MITRE

MTR200286 R2

MITRE TECHNICAL REPORT

Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs)

Mapping Cyber Resiliency to the ATT&CK® Framework – Revision 2

Sponsor: National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) in partnership with Air Force Research Laboratory Information Directorate (AFRL/RI)
Dept. No.: L522
Contract No.: SB-1341-14-CQ-0010
Project No.: 2721NT84-CR

Authors:
Deborah J. Bodeau
Richard D. Graubart
Linda K. Jones
Ellen R. Laderman
David Black

Bedford, MA

December 2021

Abstract

The Air Force Research Laboratory's (AFRL's) Cyber Survivability Attributes (CSA) Tool enables systems engineers to identify, evaluate gaps in, and make trade-offs among system security controls. In particular, the CSA Tool enables systems engineers to consider cyber resiliency controls. This report documents the process and results of a mapping of cyber resiliency controls, as identified in NIST SP 800-160 Vol. 2, to techniques in ATT&CK®. This mapping identifies the potential effects which the controls, properly tailored, implemented, and used, could have on adversary tactics, techniques, and procedures (TTPs). These potential effects constitute testable hypotheses, which can be used in system penetration or adversarial testing. The mapping has been incorporated into the CSA Tool.

Summary of Changes

This document updates MTR200286 to be consistent with NIST SP 800-160 v2 Revision 1 and with ATT&CK v9. It includes identification of controls and potential effects for non-cyber resiliency ATT&CK Mitigations. It includes Techniques from ATT&CK for Industrial Control Systems (ICS) as well as from ATT&CK for Enterprise.

Acknowledgments

The authors gratefully acknowledge and appreciate the contributions from Jim Reilly of the Air Force Research Laboratory, Rebecca Onuskanich of International Cyber Institute, Kenneth Colerick of Alluvion Data Solutions, Jason Rice of Quanterion Solutions, and Amy Heburn of PAR Government Systems, Dr. Ron Ross of the National Institute of Standards and Technology, and Don Faatz, Kevin Greene, Adam Hahn, Jeff Picciotto, and John Woodill of the MITRE Corporation.

Table of Contents

List of Figures

List of Tables

1 Introduction

Systems security engineers lack threat-informed guidance on selecting and tailoring controls from NIST SP 800-53 [1]. They need to give well-founded answers (i.e., answers based on analysis, preferably citing a common and reusable reference) to such questions as "This control isn't in the baseline – what good will it do, to justify the cost of adding it?" "Why is this baseline control omitted?" and "How does the collection of controls, as selected and tailored, address different adversarial threats? How well will the system mitigate a specific attack such as the SolarWinds campaign?" In the absence of guidance and reference analysis, the default is to gravitate toward a compliance mindset, in which adherence to baselines takes the place of true risk management. However, a compliance-oriented approach to selecting controls begs such questions as "Are all these controls necessary?" "How should the controls be tailored?" "How should the controls be implemented?" and "How can these controls be tested in an adversarial setting (e.g., emulating a specific attack)?"

Under the Air Force Research Laboratory (AFRL) Automated Cyber Survivability (ACS, [2]) program, AFRL's Cyber Survivability Attributes (CSA) Tool [3] enables systems engineers to identify, evaluate gaps in, and make trade-offs among system security controls. The CSA Tool also enables acquisition programs to develop test cases, using test scripts tied to adversary tactics, techniques, and procedures (TTPs) from the ATT&CK® knowledge base. In support of the ACS program in partnership with the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE), MITRE has identified the potential effects that cyber resiliency implementation approaches and controls could have on adversarial threat events. The identification of potential effects can support multiple systems security engineering (SSE) and risk management activities, including:

- Analysis, assessment, and visualization (e.g., using a heat map) of how a given control, a set of controls, or an as-built system covers a set of adversary activities or other threat events.
- Identification of possible measures of effectiveness, or definition of tests which could be performed, to validate the implementation of a control, set of controls, or requirements.

This report documents the analysis of how cyber resiliency approaches and controls could be used to reduce the risks associated with possible adversary actions, as described in the ATT&CK® for Enterprise and ATT&CK for Industrial Control Systems (ICS) Matrices. This analysis uses:

- Cyber resiliency concepts and terminology as defined in NIST SP 800-160 Vol. 2 [4] [5];

---

[1] Tailoring a control involves making selections and assignments.

[2] For brevity, the term "control" will be used to refer to control enhancements (e.g., AC-3(1)) as well as base controls (e.g., AC-3). Selection of a control enhancement assumes the selection of its base control.

[3] Terms in the ATT&CK object structures [11] – Tactics, Techniques, Mitigations – are capitalized in this document, to avoid confusion with uses in NIST SP 800-160 V2 (cyber resiliency techniques), MITRE Shield [21] (active defense techniques), and general usage (e.g., risk mitigation, threat mitigation).

[4] Appendix B identifies not only those cyber resiliency controls identified in [4], but also controls which will be added in Revision 1 [5].

[5] A CREA could similarly be performed using the attack patterns in the Common Attack Pattern Enumeration and Classification (CAPEC) repository.

- Base controls, control enhancements, and supplemental guidance in the NIST SP 800-53R5 [1], and the identification of controls which apply one or more cyber resiliency approaches in NIST SP 800-160 Vol. 2 [4] [5]; and
- Descriptions of adversary actions, mitigations, and detection methods captured in the ATT&CK knowledge base.

This introduction provides background on the source materials and describes how the material in this report can be used. Section 2 describes the analysis method, which includes defining candidate mitigations applying cyber resiliency approaches and controls, similar to the mitigations already defined by ATT&CK. (Note that, as discussed in Section 2.3 below, the candidate mitigations are not, and are not expected to become, part of the ATT&CK knowledge base.) Section 3 presents the results of the analysis, in the form of tables mapping Techniques [3] in ATT&CK for Enterprise to cyber resiliency controls and their potential effects on those techniques. Section 4 presents supporting information, including whether and how ATT&CK Mitigations map to cyber resiliency controls, descriptions of candidate mitigations for detection based on information from ATT&CK for Enterprise, and descriptions of candidate mitigations identified from the cyber resiliency concepts and controls presented in NIST SP 800-160 Vol. 2 [5]. This material has been incorporated into AFRL's CSA Tool [3]. Similarly, Section 5 presents the results of the analysis for ATT&CK for ICS, and Section 6 presents supporting information for the ATT&CK for ICS mapping.

Four appendices are also provided. Appendix A defines cyber resiliency techniques and implementation approaches, as well as effects on adversary actions, so that the user of this report does not need to consult NIST SP 800-160 Vol. 2 for definitions. Appendix B identifies, for each cyber resiliency control [4] in [5], whether and how it is used in ATT&CK mitigations and candidate mitigations. Appendix C provides Technique-specific descriptions of the candidate mitigations defined in Sections 4 and 6.

It is important to note mappings such as those presented in this document inherently have a degree of subjectivity due to experience and interpretation, and therefore are likely to evolve over time. The authors recognize this and welcome any feedback and input regarding the mapping contained within this document.

1.1 Cyber Resiliency

NIST SP 800-160 Vol. 2 [4] defines **cyber resiliency** as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." This definition was crafted, based on a variety of other definitions of resilience-related terms, to be applicable to range of subjects, including a system; a mechanism, component, or system element; a shared service, common infrastructure, or system-of-systems identified with a mission or business function; an organization; a critical infrastructure sector or a region; a system-of-systems in a critical infrastructure sector or sub-sector; and the Nation. Cyber resiliency can also be a property of a mission, business function, or a constituent task of a mission or business function. This interpretation relies on treating the task, mission, or business function as a socio-technical system (or system-of-systems). Cyber resiliency engineering builds on cybersecurity as well as other engineering disciplines, e.g., safety, reliability, or performance engineering, and is closely related to cyber survivability [6].

[6] ATT&CK for ICS does not describe detection methods but does identify data sources which could be used in detection.

As illustrated in Figure 1, different constructs are used to describe (i) the cyber resiliency problem domain – the "what" of cyber resiliency (what properties, behaviors, and capabilities are needed, based on the risk management strategy) and (ii) the cyber resiliency solution domain – the "how" of cyber resiliency (how to select and use technologies, practices, processes, and products). Constructs describing "what" – goals and objectives – are consistent with Resilience Engineering [7] and the NIST Cybersecurity Framework [8]. Constructs describing "how" include design principles, techniques, and implementation approaches. These "how" constructs are informed by other specialty engineering disciplines, including system survivability, reliability, and security.

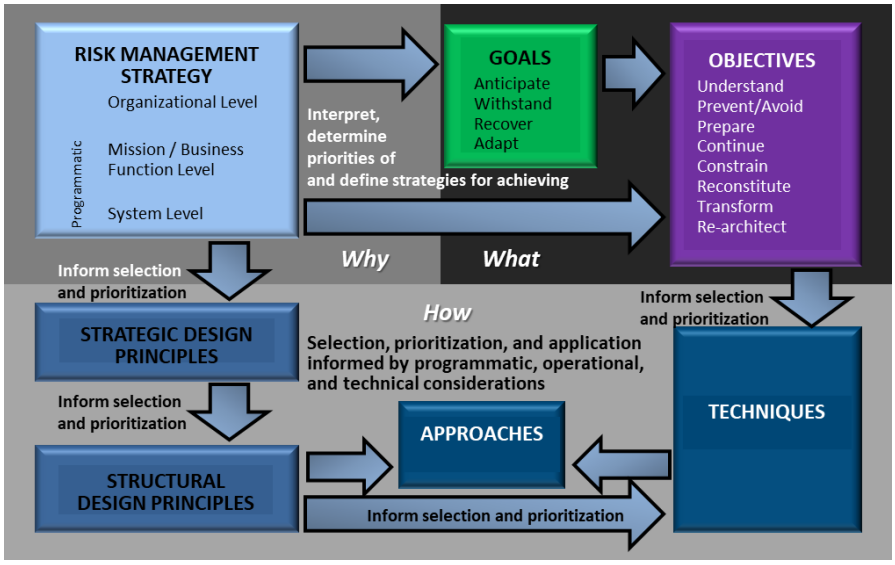

Figure 1. Cyber Resiliency Engineering Framework (CREF) (derived from [8])

NIST SP 800-160 Vol. 2 identifies controls, as defined in NIST SP 800-53R5 [1], which directly support cyber resiliency. These controls, as listed in Table E-1 of [5], apply one or more of the implementation approaches to the cyber resiliency techniques. (For reference, the implementation approaches are summarized in Appendix A of this report.)

1.2 Potential Effects on Threat Events (PETE) Analysis

A Potential Effects on Threat Events (PETE) Analysis is an analysis which uses a reserved vocabulary to describe potential effects of a capability, an action, a safeguard, or a countermeasure on a threat event or class of threat events. The vocabulary for potential effects is designed to facilitate development of tests or experiments to evaluate claims about those effects. While the vocabulary originally published in [9] and subsequently incorporated into Appendix F

[7] See https://attack.mitre.org/matrices/enterprise/. Note that the Defense Evasion column is truncated in Figure 3.

[8] The Initial Public Draft of NIST SP 800-160 Vol. 2 [22] identified cyber resiliency controls in NIST SP 800-53 R4 [28]. The CNSS baselines and overlays, as well as the CSEIG, currently cite NIST SP 800-53 R4; updates to use NIST SP 800-53 R5 are underway for these publications.

[9] The list of controls in NIST SP 800-160 Vol. 2 is emphatically *not* an overlay: it is neither desirable nor feasible to select all cyber resiliency controls for a given system. Due to interactions (e.g., dependencies, synergies, conflicts) between cyber resiliency techniques, selection of one cyber resiliency control can prioritize or preclude selection of another. As indicated in Table D-3 of NIST SP 800-160 Vol. 2 [5], one cyber resiliency technique may depend on another. For example, Adaptive Response depends on Analytic Monitoring. Therefore, architectural, or operational barriers to implementing some forms of

of NIST SP 800-160 Vol. 2 was created with adversarial and cyber threats in mind, it is largely technology-neutral and applicable to non-adversarial threats. Thus, it could be used for non-cyber threats and for threats to systems which do not include cyber elements. For reference, the definitions of the potential effects are given in Appendix A. As illustrated in Figure 2, potential effects are defined at a high level (redirect, preclude, impede, limit, expose) and at a lower level (e.g., contain, degrade, delay, and exert in support of impede).

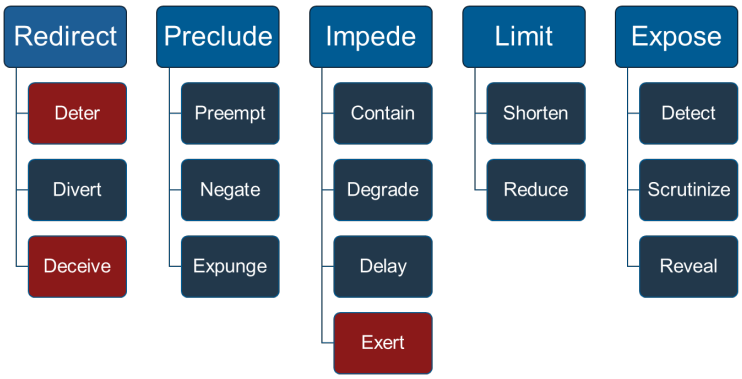

Figure 2. Potential Effects on Threat Events

One use of the high-level potential effects is in the risk management strategy for an organization, mission, or system. For example, an organization could prioritize the Limit effects for a system with high availability requirements, recognizing that the system is exposed to distributed denial of service (DDoS) attacks and must re-establish an adequate level of performance as quickly as possible. The same organization could prioritize Preclude for a system with high confidentiality and low availability requirements, accepting preventative measures which degrade performance. The lower-level effects can be used to develop metrics and testable hypotheses about system behavior (e.g., malware affects only a specified set of system resources, for Contain; capabilities are restored within a specified time period for Shorten). While these potential effects were defined with respect to adversary actions, none of them are cyber-specific and most of them apply to any threat event, independent of the threat source. The Deter, Deceive, and Exert effects are specific to adversarial actions. These adversary-specific potential effects are shown in **red** in Figure 2.

A Cyber Resiliency Effects Analysis (CREA) is a specialization of a more general Threat Effects Analysis, focusing on cyber threats and on cyber resiliency constructs or solutions. A CREA identifies the potential effects that a cyber resiliency construct (e.g., a technique, implementation approach, or design principle), mitigation ("a decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities" [5]), or solution ("a combination of technologies, architectural decisions, systems engineering processes, and operational processes, procedures, or practices which solves a problem in the

Analytic Monitoring could also be barriers to implementing Adaptive Response. Alternately, one cyber resiliency technique may conflict with or complicate the use of another. For example, some uses of Non-Persistence can interfere with Analytic Monitoring.

cyber resiliency domain" [4]) could have on an adversary. These effects could be strategic [10] or could be more tactical, i.e., related to the adversary's use of different tactics, techniques, and procedures (TTPs) to achieve specific objectives.

A CREA can use threat models and cyber resiliency constructs at different levels of abstraction. This report documents the results of a CREA which uses the Techniques defined in the ATT&CK for Enterprise and ATT&CK for ICS Matrices and cyber resiliency controls and their corresponding implementation approaches. The ATT&CK Matrices were chosen because the AFRL CSA Tool uses ATT&CK in the creation of test cases.

1.3 ATT&CK

As described in [11], MITRE ATT&CK® is a broadly-accessible knowledge base of adversary tactics and techniques based on real-world observations. These real-world observations take the form of curated data sets including publicly reported incidents, in which indicators and observables can be found. ATT&CK reflects the phases of an adversary's attack lifecycle and the platforms (e.g., Windows) adversaries are known to target, providing a taxonomy of adversarial TTPs with a focus on those used by external adversaries executing cyber-attacks against networked systems. At a high level, ATT&CK consists of the following core components:

- Tactics, denoting short-term, tactical adversary goals during an attack;
- Techniques, describing the means by which adversaries achieve tactical goals;
- Sub-Techniques, describing more specific means by which adversaries achieve tactical goals at a lower level than techniques; and
- Documented adversary usage of Techniques, their procedures, and other metadata.

In addition, for each Technique and Sub-Technique, the description in ATT&CK for Enterprise includes a discussion of detection methods [6]. The ATT&CK description may also identify Mitigations. In ATT&CK, Mitigations represent security concepts and classes of technologies that can be used to prevent a Technique or Sub-Technique from being successfully executed, based on observations in one or more of the curated data sets used to develop ATT&CK.

The Tactics and Techniques in ATT&CK for Enterprise are presented in matrix form, as illustrated in Figure 3 [7]. A similar matrix presents the Tactics and Techniques in ATT&CK for ICS. This representation lends itself to visualizations of detection or mitigation coverage. More information can be found in descriptions at attack.mitre.org, as content in the STIX 2.0 GitHub repository, or by using the TAXII server.

---

[10] Controls can be *related* in two ways. First, there is an assumed dependency of a control enhancement on its base control: NIST SP 800-53 states that "The selection and implementation of control enhancements *always* requires the selection and implementation of the base control." Second, for many controls NIST SP 800-53 identifies one or more related controls. These are controls "that impact or support the implementation of a particular control or control enhancement, address a related security or privacy capability, or are referenced in the discussion section. … When a control is designated as a related control, a corresponding designation is made on that control in its source location in the catalog to illustrate the two-way relationship." Because a control enhancement is inherently related to its base control, that base control is not listed under the enhancement's related controls.

[11] For example, SC-29, Heterogeneity, is a cyber resiliency control which applies Architectural Diversity. Related controls include AU-9, PL-8, SC-27, SC-30, and SR-3. AU-9, PL-8, and SC-27 are not cyber resiliency controls (although control enhancements for AU-9 and PL-8 are). SC-30 and SR-3 are cyber resiliency controls.

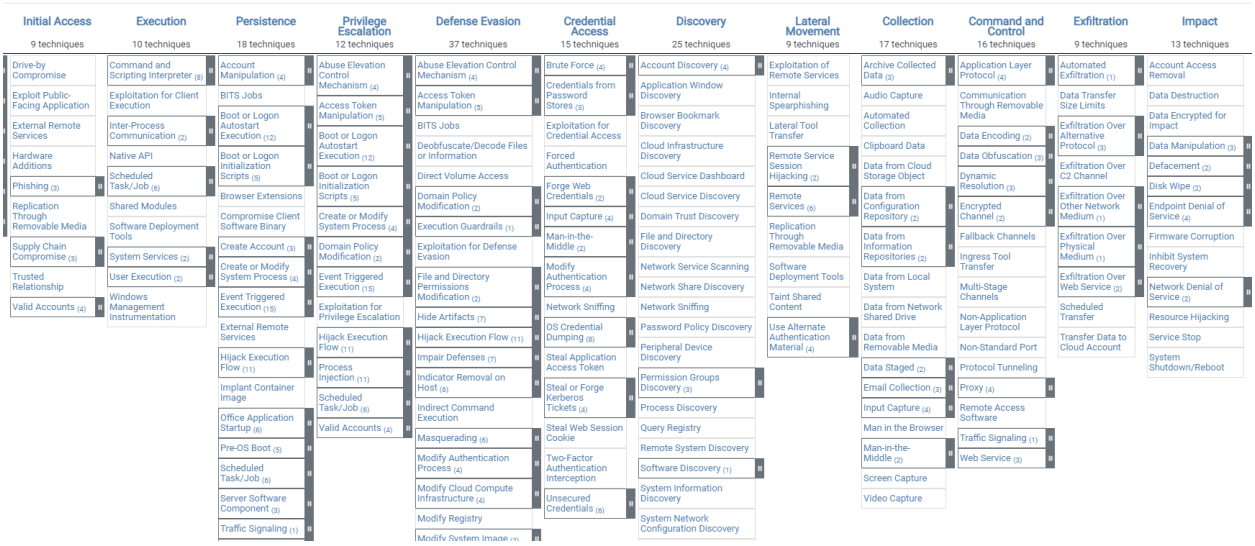

Figure 3. ATT&CK for Enterprise Matrix (Partial)

ATT&CK for Enterprise is updated twice a year. This report uses ATT&CK for Enterprise v9, which was released on April 29, 2021, and ATT&CK for ICS as described in [12].

1.4 AFRL CSA Tool

The AFRL CSA Tool provides its users – systems engineers and Program Office staff – with a customizable workflow process tool for analyzing and making trade-offs among security controls. The CSA Tool, which has Joint Staff advocacy, incorporates a database containing much of the existing Risk Management Framework (RMF) and Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253 guidance, as well as the Cyber Survivability Endorsement Implementation Guide (CSEIG, [13]). The CSA Tool database includes the controls, enhancements, and discussion of NIST SP 800-53 R5 and its predecessor NIST SP 800-53 R4 [8], the NIST 800-53 baselines, the CNSSI 1253 baselines, approved NIST and CNSSI overlays, and many unofficial, but highly useful, agency and department developed overlays. The CSA Tool also includes sample templates and detailed RMF guidance and policy documentation. As a result, the CSA Tool is able to automatically generate and consume RMF artifacts, greatly reducing the time and burden that the current manual process entails. The CSA Tool also greatly facilitates the categorization of systems relative to the overlays, baselines, and tailoring guidance for the NIST SP 800-53 controls consistent with the RMF process. The CSA Tool can be used in all phases of the system development life cycle (SDLC). Future releases will include automated support for cyber test and evaluation (CT&E). In particular, the CSA Tool will provide micro-scripts for ATT&CK Techniques.

The CSA Tool has incorporated the set of cyber resiliency controls identified in NIST SP 800-160 Vol. 2 as a starting point for identifying controls which could enable a system to mitigate risks more effectively due to advanced cyber threats, with the understanding that it is neither feasible nor cost-effective for a system to implement all of those controls [9]. One basis for analyzing trade-offs among controls for a system is the potential effects of controls on adversary

[12] See [11] for more information about ATT&CK use cases.

[13] When a cyber resiliency control is identified for a cyber hygiene or standard practice Mitigation, its use in that Mitigation is not cyber resiliency.

TTPs. A more detailed analysis of the potential effects of cyber resiliency controls on adversary activities can support visualization of potential effectiveness of the controls, trade-off analysis among controls, and development of testable claims or hypotheses about observable effects. Such claims can then be validated for a system described using the CSA Tool, using the tool's automated CT&E capabilities.

Figure 4 and Figure 5, adapted from the presentation given by AFRL at the 9th Annual Secure and Resilient Cyber Architectures Invitational, illustrate how the work documented in this report fits into the CSA Tool.

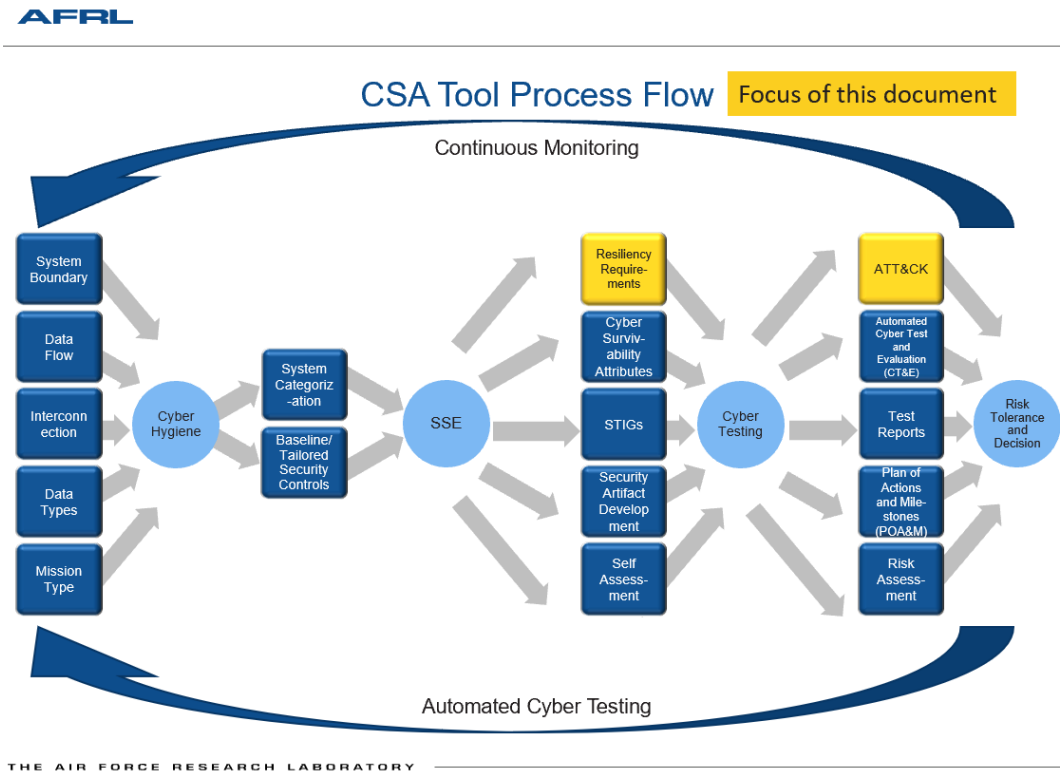

Figure 4. Cyber Resiliency-ATT&CK Mapping in the CSA Tool Process Flow

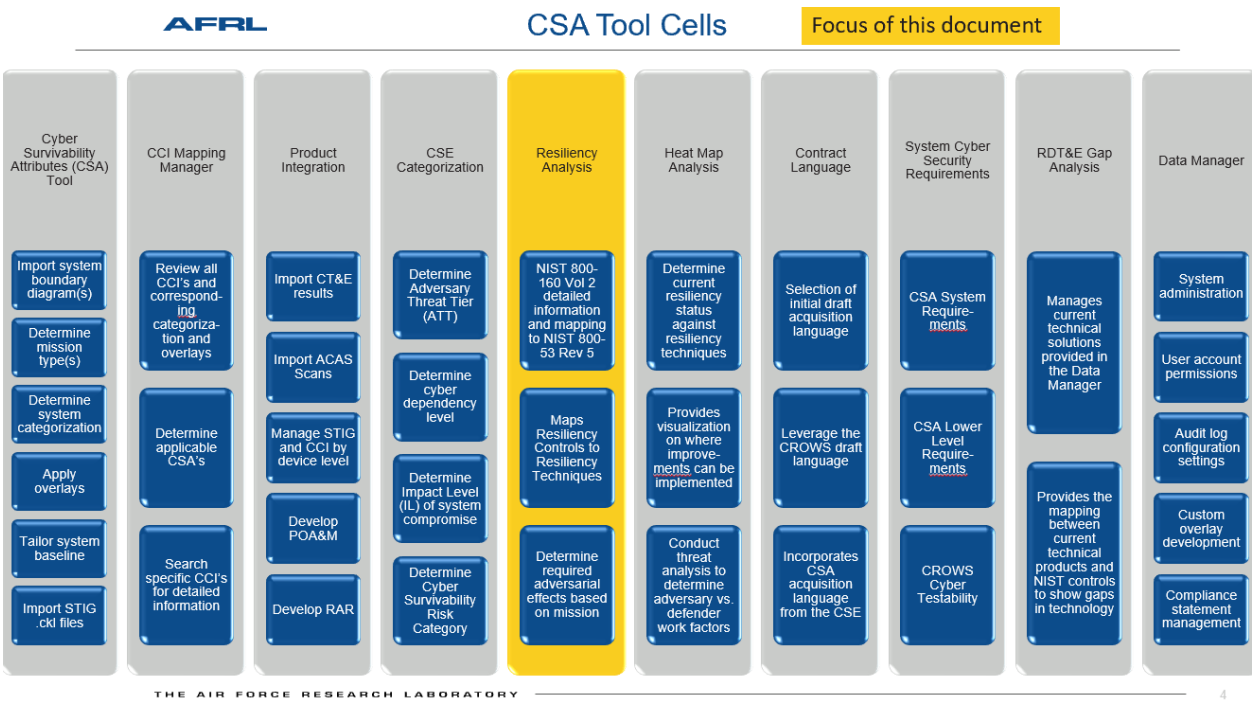

Figure 5. Cyber Resiliency-ATT&CK Mapping in the CSA Tool Cells

1.5 Limitations and Caveats

The restricted scope of the analysis presented in this paper must be understood for its results to be used correctly:

- **Based on analysis rather than observation.** The mappings of cyber resiliency controls and approaches to ATT&CK Techniques presented in this document are based on engineering analysis. This contrasts sharply with the contents of the ATT&CK for Enterprise knowledge base, which are derived from operational experience and curated data sets. The candidate mitigations defined by the Cyber Resiliency Effects Analysis for ATT&CK are not part of the ATT&CK knowledge base. Rather, they are intended to facilitate understanding of how cyber resiliency approaches and controls can be used to mitigate different Techniques.
- **Assumed use of controls.** The inclusion of a control in a system's requirements does not in itself guarantee any effect on adversary activities. Effects on threat events (whether adversarial or not) depend on (i) how the controls are specified (e.g., via Assignment statements or Selections), (ii) how the control is implemented, and (iii) how the implementation is used. Thus, the mapping tables in Sections 3 and 5 rely on the descriptions of candidate mitigations in Sections 4 and 6, respectively, and in Appendix C.
- **Direct effects only.** Only the direct effects a given control could have (in the context of an ATT&CK Mitigation or of a candidate mitigation) on an ATT&CK Technique are identified. Indirect effects are not considered. Therefore, this analysis does not consider related controls. [10] This limitation prevents the analysis from daisy-chaining into a representation of a large percentage of NIST SP 800-53R5, with no benefit to the user interested in understanding the potential effects of cyber resiliency controls on threat events. The potential effects of the non-cyber resiliency "related controls" identified for a

given cyber resiliency control in NIST SP 800-53R5 are at best indirect, will depend strongly on how the control for which they are cited is implemented and used, and are usually not themselves cyber resiliency controls [11]. Similarly, this analysis does not consider most controls which apply design principles (i.e., enhancements to SA-8), since the effects of applying a design principle are usually indirect.

- **ATT&CK Techniques but not Sub-Techniques.** The analysis in this document does not go to the level of Sub-Techniques in ATT&CK, since many Sub-Techniques are platform-specific (e.g., meaningful only for Windows). This reflects the fact that controls are intended to be technology-neutral. Sub-Techniques, while differing in technical details which are important for such ATT&CK use cases as adversary emulation, development of behavioral analytics, and maturity assessment of a Security Operations Center (SOC), do not differ significantly in the potential application of cyber resiliency approaches or controls.

Other mappings involving the ATT&CK for Enterprise Matrix, the NIST SP 800-53 controls, or both, have been developed. These are being tracked for consideration in future versions of this report and/or of the CSA Tool. These include a mapping of the NIST Cybersecurity Framework (NCF) to (version 7 of) ATT&CK [14] and a mapping of security controls to ATT&CK Techniques and Sub-Techniques published by the Center for Threat-Informed Defense (CTID) at MITRE Engenuity [15]. Both these mappings use base controls but not control enhancements. The NCF mapping identifies sub-categories which could either mitigate or detect ATT&CK Techniques. NIST SP 800-53 base controls corresponding to a sub-category are identified in the NCF as informative references; therefore, the NCF mapping could be extended to map base controls to ATT&CK Techniques. The CTID mapping identifies base controls which could mitigate ATT&CK Techniques or Sub-Techniques. (The CTID mapping does not identify controls for detection.) The CTID mapping assumes the identified controls are used to support or implement the ATT&CK Mitigations but does not identify the relationship between individual controls and Mitigations. The CTID mapping is used in at least one commercial offering of automated testing [16]. In either of these mappings, "mitigate" encompasses potential effects which, in the analysis presented in this report, fall under Preclude, Impede, and/or Limit.

---

[14] The distinction between basic, foundational, and organizational security capabilities is defined by the Center for Internet Security (CIS) in the CIS Controls (formerly the SANS Top 20 Controls). CIS characterizes the first six CIS Controls – inventory and control of hardware assets, inventory and control of software assets, continuous vulnerability management, controlled use of administrative privileges, secure configuration, and auditing – as basic. CIS defines three Implementation Groups (IGs) for use in prioritizing the sub-controls and refers to IG1 as "cyber hygiene."

[15] As defined in [25] [24], the APT is "an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives." The phrases "advanced cyber threat" and "advanced cyber adversary" are used as synonyms.

[16] For each Technique, data sources – sources of information collected by sensors or logging systems – are also identified. These are frequently technology-specific, e.g., Windows event logs. The identification of data sources is useful to the implementation of a control which implements one or more of the detection methods but is not relevant to the Cyber Resiliency Effects Analysis.

1.6 Use Cases

As noted above, the ATT&CK-cyber resiliency mapping presented in this report was developed for use in AFRL's CSA Tool. In addition, a systems engineer can use the tables in this report to answer questions such as:

- What effects could a given control or set of controls have on adversary activities? What risk-reducing benefits can be expected from implementing a specific set of controls?
    - The CSA Tool provides a visualization of the potential effects a given control or set of controls could have. Alternately, a systems engineer could search the tables in this report for those controls. The set of ATT&CK Techniques which the controls could be used to mitigate can be highlighted in an ATT&CK coverage map. (See ATT&CK® Navigator (mitre-attack.github.io).) The potential effects that the controls could have upon ATT&CK Techniques can be visualized on that coverage map.
- What controls could be used to have a given effect on adversary activities under a specific Tactic? For example, what controls could be used to Shorten the duration of adversity resulting from Impact Techniques?
    - Table 14 identifies potential effects of ATT&CK Mitigations as well as the candidate mitigations defined in this report on ATT&CK Techniques under the Impact Tactic. Controls with the potential effect of Shorten include AC-2(6), AC-2(8), AC-4(2), AC-4(3), AC-4(8), AC-7(4), CP-2(5), CP-9, CP-9(6), IR-4(2), IR-4(3), IR-4(9), IR-4(14), SA-17(9), SA-20, SA-23, SC-3, SC-5(2), SC-7(20), SC-29, SC-47, and SI-22.
- How can controls be used effectively to mitigate threats? What are the implications for implementation, use, and assessment of controls?
    - The descriptions of uses, together with the vocabulary for potential effects, explain how the controls need to be implemented and used to have the identified effects. This explanation provides systems engineers with guidance on defining requirements, making design decisions, and recommending operational procedures to achieve the desired effects. The potential effects are defined so as to facilitate the development of test cases. For example, for the Delay effect, how long does it take the ATT&CK Technique to achieve its results without the control, versus with the control implemented and used as described? The micro-scripts planned for inclusion in the CSA Tool could be used in an emulation environment or during CT&E to assess the relative effectiveness of a control.

2 Analysis Process

This section describes the analysis process used to construct the tables mapping cyber resiliency controls and approaches to the ATT&CK Techniques in Sections 3 and 5. The ATT&CK for Enterprise Tactics were analyzed one at a time, with ongoing cross checking to ensure consistency. Subsequently, the ATT&CK for ICS Tactics were analyzed one at a time, with ongoing cross checking. This process is illustrated in general terms in Figure 6. The process is described in more detail below.

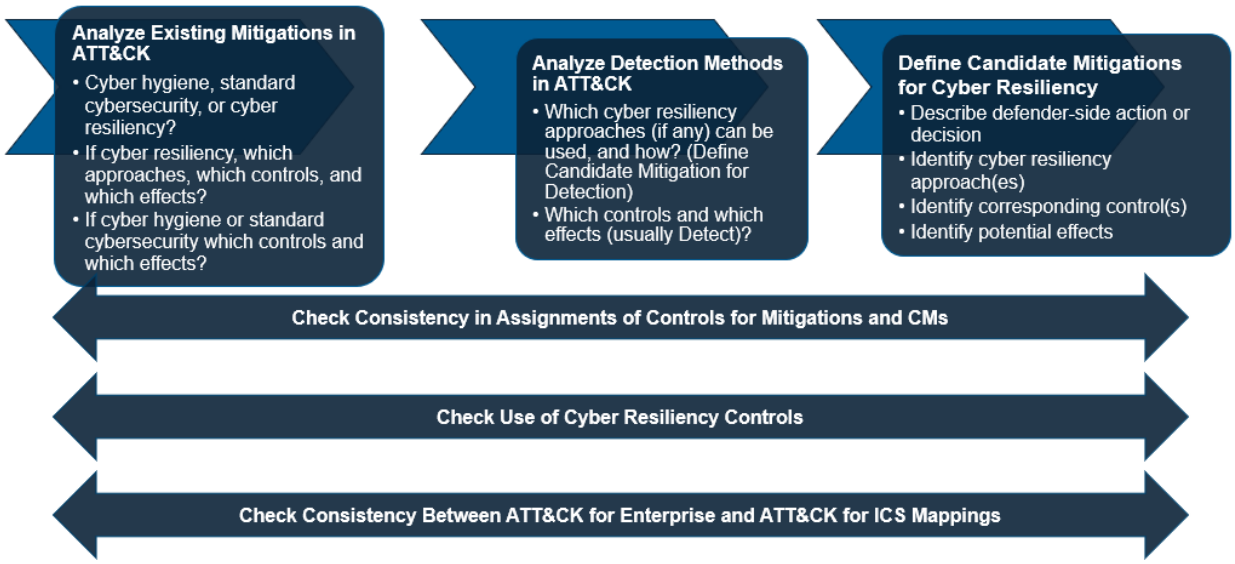

Figure 6. Overview of the Cyber Resiliency Effects Analysis Process for ATT&CK

2.1 Analysis of ATT&CK for Enterprise

Because the Techniques under a Tactic share the same purpose, they were analyzed together. For each Technique, identified Mitigations (if any) were analyzed. For a Mitigation which applies one or more cyber resiliency approaches, the analysis identified the cyber resiliency controls which can be used to implement those approaches, and the potential effects of those controls and approaches on the Technique. For a Mitigation which is characterized as standard practice or cyber hygiene, controls and potential effects were identified. Identified detection methods were analyzed and characterized in terms of whether they apply a cyber resiliency approach; if so, a candidate mitigation (CM) for detection is defined. Finally, candidate mitigations with intended effects other than detection were defined and analyzed in the same way as the existing Mitigations. Consistency checks were performed throughout, with a final sweep after all Techniques have been analyzed. This process is repeated for all Tactics, with a final consistency sweep after all the Tactics have been analyzed.

2.1.1 Existing Mitigations

As noted in Section 1.4, the inclusion of a control in a system's requirements does not in itself guarantee any effect on adversary activities. Efficacy on threat events (whether adversarial or not) depend on (i) how the control is implemented and (ii) how the implementation is used. Fortunately for this analysis, ATT&CK provides the Mitigation construct which captures the intended use of system capabilities and/or organizational processes to thwart the adversary. As

described in [11], a Mitigation identifies configurations, tools, or processes that can prevent a Technique (or Sub-Technique) from working or from having the outcome the adversary sought. A description of a Mitigation for a Technique (or Sub-Technique) enables network defenders, policymakers, or others responsible for mitigating adversarial cyber risks to take an action such as changing a policy or deploying a tool. Mitigations are vendor-agnostic, although frequently specific to a Platform (e.g., Windows).

The ATT&CK knowledge base identifies a range of Mitigations, each with an Identifier of the form M####, a Name (a very short phrase), a narrative description, and brief Descriptions of how the mitigation applies to the Techniques for which it is identified. Many of the Mitigations in the ATT&CK knowledge base do not lend themselves to applications of cyber resiliency implementation approaches. Others, however, can be said to apply one or more cyber resiliency approaches.

The analysis of a Technique began with an analysis of the Mitigations identified for that Technique in ATT&CK. Mitigations in the ATT&CK knowledge base were characterized as:

- **Cyber hygiene:** As noted in [17], there is no standard definition of the term "cyber hygiene." For purposes of this analysis, cyber hygiene is defined as "routine practices for using basic security capabilities to reduce cyber risks due to common or pervasive threats." Areas of cyber hygiene include Inventory, Protection, Configuration Management, Recovery, Monitoring, Malware Defense, and Education. Analytic and decision-making processes which are not routine (e.g., response to alerts from an intrusion detection system) are excluded from cyber hygiene but are typically standard practice.
- **Standard practice:** Practices for using basic, foundational, or organizational security capabilities to reduce cyber risks due to the threats below the level of the advanced persistent threat (APT). These practices include non-routine analytic and decision-making processes. These practices, and the controls they use, are expected to be selected and tailored as appropriate to the operational, threat, and technical environments of the system or organization, using baselines or profiles as starting points.
- **Cyber resiliency:** Practices for using security or cyber resiliency capabilities to reduce cyber risks due to advanced cyber adversaries. Cyber resiliency capabilities can be described in terms of cyber resiliency sub-objectives (see Tables 1 and D-1 of [5]) and activities [18]. However, for this analysis, they are characterized in terms of the cyber resiliency approaches they apply.

If a Mitigation was determined to apply cyber resiliency to reduce the likelihood of the Technique's success, the corresponding approach(es) were identified. The cyber resiliency control(s) which apply that approach were identified, and each control was analyzed to determine whether an implementation of it would be used by the Mitigation. The potential effects of the Mitigation on the Technique were then identified.

A given Mitigation can have multiple effects on an ATT&CK Technique, and these were assigned to the associated controls and cyber resiliency techniques by analysis. For example,

---

[17] The assignment of a combination of cyber hygiene and cyber resiliency to an A4I Mitigation relates to the Technique-specific description of the Mitigation and to the identification of associated controls; see below.

[18] This is likely a consequence of the fact that the mapping of A4I Mitigations to NIST SP 800-53R4 controls is restricted to base controls and does not include control enhancements.

M1050, Exploit Protection, can Delay, Exert, and Detect T1189, Drive-by Compromise. Two cyber resiliency controls were identified for M1050: AC-4(8), Information Flow Enforcement | Security and Privacy Policy Filters, and IR-4(13), Incident Handling | Behavior Analysis. AC-4(8) applies Integrity Checks, can delay the success of an adversary's use of Drive-by Compromise, and can also force the adversary to work harder to make that Technique succeed. AR-4(13) applies Behavior Validation and can detect an adversary's use of Drive-by Compromise as well as forcing the adversary to work harder. (Table 1 and Figure 7 in Section 3 show the results of the analysis in this example.)

It must be emphasized that the determination of whether a Mitigation can be said to apply a cyber resiliency approach, and the identification of the cyber resiliency controls which enable its use by providing capabilities which support that approach, are specific to the ATT&CK Technique for which it is identified. For example, M1047, Audit, is standard cybersecurity practice for T1053 (Scheduled Task/Job) but applies the cyber resiliency approach Provenance Tracking for T1176 (Browser Extensions) and applies Non-Persistent Information for T1574 (Hijack Execution Flow). This illustrates the fact that, for any given use of a Mitigation, only a subset of the identified cyber resiliency approaches and controls may be applicable.

Cyber resiliency analysis of ATT&CK Mitigations has been performed only for ATT&CK Techniques. Uses in Sub-Techniques are not considered. Some Mitigations may apply cyber resiliency to a Sub-Technique even if all uses at the Technique level are cyber hygiene or standard practice; however, that determination is beyond the scope of this effort.

The results of this analysis are presented in Section 4.1. Since the initial publication of this report, a mapping of security controls to ATT&CK Techniques and Sub-Techniques has been published by the Center for Threat-Informed Defense (CTID) at MITRE Engenuity [15]. The intent of and methodology for the CTID mapping [19] are different from those in this paper. However, the CTID mapping informed the analysis of cyber hygiene and standard practice Mitigations.

2.1.2 Analyze Detection Methods

Each Technique in ATT&CK for Enterprise includes a narrative discussion of detection methods. These descriptions were analyzed to identify one or more candidate mitigations for detection. The Technique-specific description of a candidate mitigation for detection was excerpted or adapted from the narrative discussion in ATT&CK.

The candidate mitigations (CMs) related to detection are expected to have the Detect, and sometimes the Scrutinize, effect on ATT&CK Techniques. These CMs rely on relatively few cyber resiliency controls. However, any one those controls can be used in different ways, depending on the Technique. As in the case of Mitigations and other CMs, the ability of a detection CM to achieve the identified effect depends strongly on how the controls are specified (via Assignment statements) and implemented, as well as on how the implementation is configured and used.

The results of this analysis are presented in Section 4.2. CMs for detection were given identifiers of the form CM2###. All CMs, although based on information provided in ATT&CK, are not part of the ATT&CK knowledge base.

[19] As noted above, the controls from NIST SP 800-53R4 identified in A4I are unchanged in NIST SP 800-53R5.

2.1.3 Define Candidate Mitigations for Cyber Resiliency

Each Technique was analyzed to identify ways in which cyber resiliency approaches and their related controls could be used to mitigate – to reduce the likelihood of success of, to detect, or to reduce the impact of – that Technique. This resulted in the definition of a new candidate mitigation or the selection and Technique-specific tailoring of a previously-defined CM. The CMs, like the ATT&CK Mitigations, are described at a high level, with more specific guidance provided for the individual techniques for which they could be effective. Therefore, the same CM could involve the use of different cyber resiliency approaches and controls in NIST SP 800-53R5, and could have different effects on the adversary, depending on how it is used to reduce the likelihood or consequences of different Techniques.

A candidate mitigation, following the pattern established by ATT&CK Mitigations, is specified by:

- An identifier. Identifiers for CMs not driven by the discussions of detection methods are given the form CM11## or CM13##. (See Section 2.6 for a discussion of the CM13## CMs.)
- A short descriptive phrase naming the action or capability.
- A brief narrative description (usually a single sentence) of the action that defenders, policymakers, systems engineers, or security program staff could take.
- A list of the approaches which could be applied to perform the action or use the capability.
- A list of the controls which could be used to provide the capability.

This information is provided in Section 4.

The Technique-specific tailoring of the CM includes:

- A brief narrative description (usually a single sentence) of the action to be taken to mitigate the Technique. These descriptions are provided in Appendix C.
- Identification of the approaches and controls used in the Technique-specific use of the CM. These are included in the mapping tables in Section 3.
- Identification of the potential effects of those controls and approaches on the Technique, using the vocabulary illustrated in Figure 2 and described in Appendix A.

The purpose of defining candidate mitigations is not to influence ATT&CK, but rather to ensure that this analysis uses a consistent method to identify which cyber resiliency approaches and controls could affect a given ATT&CK Technique, and to capture the reasoning about how effects could be achieved. The structure created by ATT&CK of an Identifier, a Name, a brief general Description, and a brief Description tailored to individual Techniques serves to improve consistency in the analysis of how defender actions or decisions could affect adversary activities as described in ATT&CK. Therefore, the Cyber Resiliency Effects Analysis for ATT&CK follows the model of ATT&CK when identifying candidate mitigations using cyber resiliency. For a Candidate Mitigation to progress to inclusion in the ATT&CK knowledge base, its effectiveness must be demonstrated in practice and reflected in a curated data set for ATT&CK.

Since the initial publication of this report, MITRE Engage – an active defense knowledge base [20] – has been published. MITRE Engage defines a set of active defense techniques which are similar to Candidate Mitigations and have been mapped to ATT&CK [21]. Analysis of the relationship between the Engage techniques and the candidate mitigations defined in this report

constitutes possible future work; that analysis may lead to definition of additional candidate mitigations.

2.1.4 Consistency Checking

Consistency checking was an ongoing process throughout the overall analysis illustrated in Figure 6 and took advantage of the fact that some Techniques are shared between two or more Tactics.

The consistency checking of the categorization of an ATT&CK Mitigation involved analyzing the "Techniques Addressed by Mitigation" table on the ATT&CK site (e.g., Audit, Mitigation M1047 - Enterprise | MITRE ATT&CK® for Audit, M1047). Identical entries were categorized identically. Note that the entries for Sub-Techniques were not examined. The results of these analyses are summarized in Table 15 in Section 4.1.

The consistency checking of CMs for detection focused on the selection and use of cyber resiliency controls in different contexts. Two controls – IR-4(13) and SI-4(2) – are used in many different detection CMs. However, they are used in different ways, depending on the candidate mitigation in question, and the specific Technique to which they are applied.

The remaining candidate mitigations (CM11## and CM13##) were analyzed individually for consistency. The internal consistency of definitions, assignment of controls, and assignment of potential effects of the CM were checked across the Techniques for which the CM is used. Not every control or cyber resiliency approach identified for a CM will be applicable to all uses of that CM. The effects which could be achieved on a Technique are specific to the use of the CM, and of the controls and cyber resiliency approaches the CM applies, for that Technique.

Consistency across CMs was also analyzed, and differentiation between similar CMs was clarified. For example, several CMs related to Deception are defined, but their uses differ.

2.1.5 Checking the Use of Cyber Resiliency Controls

For each cyber resiliency control identified in Table E-1 of [5], the Mitigations and candidate mitigations which could apply that control have been identified. The results of this analysis are included in Appendix B.

Some cyber resiliency controls are not used in any Mitigation or candidate mitigation. There are several reasons for a control not being referenced in the ATT&CK mapping, including:

- A control could be intended to address threats not represented in ATT&CK for Enterprise, e.g., insider threats, threats against ICS, threats from maintenance staff, attacks on wireless communications.
- A control could rely on policies and procedures rather than technical means.
- A control could have no effect on any specific adversary TTP, either directly or by intensifying the effectiveness of an existing Mitigation or candidate mitigation. This is particularly the case for design principles and for requirements on system development; the effects of these controls are inherently indirect.

In some cases, new CMs were identified which were then factored back into the analyses of the individual Tactics and Techniques.

2.2 Analysis ATT&CK for ICS

ATT&CK for ICS (A4I) closely parallels ATT&CK for Enterprise (A4E) but differs in several ways. A4I provides its own numbering scheme for Tactics, Techniques, and Mitigations. Roughly half the Mitigations in A4I (those with identifiers of the form M09##) correspond to Mitigations in A4E (identifiers of the form M10##); the rest (identifiers of the form M08##) are unique to A4I. Many Mitigations in A4I have associated identified controls from one or more of NIST SP 800-53R4, IEC 62443-3-3:2013, and IEC 62443-4-2:2019. (The identified controls from NIST SP 800-53R4 are unchanged in NIST SP 800-53R5.) Many of the Techniques in A4I share names with Techniques in A4E; however, the descriptions – and identified Mitigations – are different. Therefore, the A4I mappings are presented as separate tables.

This section describes the analysis approach used to construct the mapping tables.

2.2.1 Understand the Underlying Assumptions

Industrial control systems vary architecturally, depending on their uses. To make the identification of Techniques generally useful, A4I makes as few architectural assumptions as possible. These are implicit in the identification of Asset classes [12] and include:

- The architecture includes an information technology (IT) network, a separate operational technology (OT) network, and a few systems (e.g., Data Historian, Engineering Workstation) or devices (e.g., firewalls) which bridge the IT and OT networks.
- The IT network has an interface to the Internet. A demilitarized zone (DMZ) between the IT network and the Internet is standard practice.
- Examples of devices or systems on the OT network include
    - Base Process Control Systems, including input/output (I/O) servers; field controllers, remote terminal units (RTUs), programmable line controllers (PLCs), and intelligent electronic devices (IEDs); operator interfaces and monitoring; data collection (real-time and historical) and monitoring; and alarm systems;
    - Safety Instrumented Systems (SIS) and protection systems; and
    - Engineering and maintenance systems.

Human-machine interfaces (HMIs) can be part of several of these types of assets.

In general, most of the systems or devices on the OT network have limited storage, with capabilities for monitoring and self-analysis limited to providing basic health and status (H&S) data. In addition, the OT network may have limited bandwidth, or may be segmented functionally into higher-bandwidth subnets within remote facilities with lower-bandwidth connectivity between facilities. While cybersecurity products and training for the ICS domain are becoming more sophisticated, in general it should not be assumed that a well-resourced cadre of cyber defenders can operate on the OT network.

2.2.2 Look for Parallels from ATT&CK for Enterprise

The first step in analyzing an A4I Technique involves looking at whether and how the Technique relates to Techniques in A4E. Some of the A4I Techniques are executed on an organization's IT network, rather than on its OT network. If the A4I Technique resembles Techniques under an A4E Tactic, the mapping of its Mitigations and the identification of CMs are informed by the prior analysis of A4E.

Many of the CMs in the A4E mapping involve the Deception cyber resiliency technique. Options for using Deception in an ICS environment – particularly on the OT network – are more limited than in an EIT environment. Commercial offerings do exist, however, for ICS, including deceptive PLCs and HMI systems. Active engagement with an adversary, whether via a decoy system or a full-blown deception environment, are resource-intensive and potentially disruptive. In the A4I mapping, preference has been given to deception CMs which are less resource-intense (e.g., Passive Decoys rather than Active Decoys; Deception Environment limited to the IT network).

2.2.3 Map Mitigations

As in the A4E mapping, the next step in analyzing an A4I Technique involves looking at the Mitigations identified in the A4I entry for that Technique. Each Mitigation – as used for the Technique – is characterized as cyber hygiene, standard practice, cyber resiliency, or a combination of these [17]. The potential effects of the Mitigation are then identified, together with corresponding controls in NIST SP 800-53R5.

Control identification considers any controls from NIST SP 800-53R4 identified in A4I, which frequently match the controls associated with cyber hygiene practices. (See [17].) If the A4I Mitigation corresponds to an A4E Mitigation (indicated by its identifier having the form M09##), the uses of the A4E Mitigation are reviewed. In many cases, the A4I Mitigation includes actions and assumes capabilities beyond those associated with the corresponding A4E Mitigation. If one or more of the uses of the A4I Mitigation applies a different set of controls than those previously identified for A4E, those controls are reviewed. In addition, in many cases the A4I Technique-specific description of an A4I Mitigation includes both basic (i.e., cyber hygiene or standard practice) aspects and cyber resiliency aspects, but the controls identified for the A4I Mitigation focus solely on the basic aspect [18]. If controls from the A4E mapping or the controls identified from the analysis of the A4I-specific description of the Mitigation appear to be a better match for the A4I Mitigation than the R4 controls identified in A4I, they are presented in the mapping table in **bold** to indicate the divergence from the original A4I mapping.

2.2.4 Identify and Map Candidate Mitigations

As in the A4E mapping, the next step is to identify Candidate Mitigations. If A4E parallels exist, these are reviewed to identify corresponding CMs. Additional CMs are identified by analysis of the Technique description, its supporting literature, and review of information related to cyber resiliency techniques, approaches, technologies, and practices in the ICS domain. For each identified CM, a Technique-specific description is defined. (Note, however, that A4I does not include a section on Detection. Therefore, relatively few Detection CMs are identified, using parallels with A4E Techniques.) Potential effects are identified, together with corresponding controls in NIST SP 800-53R5 [19].

2.2.5 Cross-Check Consistency

Analysis of consistency of mappings for Mitigations is captured in an annotation of the listing of A4I Mitigations, as presented in Appendix B below. Consistency of mappings for CMs was ensured via review of the Technique-specific descriptions. Uses of Mitigations and CMs for A4I with corresponding A4E Mitigations and CMs were analyzed for consistency. Note, however, that the general and Technique-specific descriptions are often at different levels of detail, with the consequence that different controls may be identified.

3 Mapping Tables – ATT&CK for Enterprise

This section provides the tables mapping cyber resiliency controls and approaches to the ATT&CK Techniques. One table is provided for each ATT&CK Tactic. Rows highlighted in **green** describe ATT&CK Mitigations which apply cyber resiliency. Rows highlighted in **yellow** describe candidate mitigations. Rows that are **not highlighted** describe ATT&CK Mitigations for which no application of cyber resiliency was identified. As noted in Section 1.4 and Section 2, the potential effects of a control on a Technique depend on (i) how the control is specified (e.g., via Assignment statements or Selections), (ii) how the control is implemented, and (iii) how the implementation is used. The Technique-specific descriptions of Mitigations (found in the ATT&CK knowledge base) and the Candidate Mitigations (found in Section 4) provide guidance on use. (Control specification and implementation will depend on the system architecture and on the organization's risk management strategy.)

Figure 7 describes how the entries in the tables should be interpreted. For importation into the AFRL CSA Tool, each row was converted into one or more rows. For example, the first row for T1189 in Figure 7 became 10 rows, one row for each combination of a potential effect and a control.

ATT&CK Techniques for *Initial Access* Tactic	Mitigations (M) Identified in ATT&CK and Candidate Mitigations (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency or Other Control(s)
Drive-by Compromise (T1189)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4 (21), AC-6 (4), SC-18 (5), SC-39, CM-7 (6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4 (8)
		Behavior Validation	Detect, Exert	IR-4 (13)
	Restrict Web-Based Content (M1021)	Standard practice	Negate, Preempt	CM-7(5), SC-18, SC-7
	Update Software (M1051)	Cyber hygiene	Preempt, Negate, Expunge, Shorten	SI-2
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4 (13), SI-4 (2), SI-4 (4)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2 (12)

The Technique-specific description of M1048 applies the Predefined Segmentation approach, and could have the Contain and/or Exert effects on Drive-by-Compromise. To implement M1048, several controls as identified here must be used together.

For Drive-by-Compromise, M1021 calls for the use of adblockers and script blocking extensions. While the controls identified for this use include CM-7(5) and SC-7, which can be used to apply cyber resiliency approaches, their use here is standard practice.

Both SC-26 and SC-35 – used as described by the Technique-specific description of CM1123 – apply Misdirection. However, the use of Misdirection by these two controls has different potential effects: Negate and Contain for SC-26 vs. Detect and Scrutinize for SC-35. In addition, the use of SC-35 in the Active Decoys CM applies Dynamic Segmentation and Isolation, with the potential effect of Contain.

Figure 7. How to Read the Tactic Tables

Some Techniques fall under multiple Tactics. For example, T1133, External Remote Services, falls under both Initial Access and Persistence. The information for such Techniques is repeated under all Tactics.

3.1 Reconnaissance

The adversary's goal for the 10 Techniques under the Reconnaissance Tactic is to gather information they can use in future operations.

Table 1. Reconnaissance Tactic (TA0043): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Reconnaissance*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
Active Scanning (T1595)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive	SC-26
		Architectural Diversity	Divert, Exert	SC-29
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16)
		Obfuscation	Degrade, Exert	SC-28 (1), SC-30, SC-30(5)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Host Information (T1592)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive	SC-26
		Architectural Diversity	Divert, Exert	SC-29
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Conceal Resources from Discovery (CM1160)	Obfuscation	Degrade, Exert	SC-28 (1), SC-30, SC-30(5)
Gather Victim Identity Information (T1589)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Exert	AT-2(1), AT-2(5)
		Self-Challenge	Exert	AT-2(1), AT-3(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Network Information (T1590)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26

ATT&CK Technique (*Reconnaissance*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Gather Victim Org Information (T1591)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
Phishing for Information (T1598)	User Training (M1017)	Dynamic Threat Awareness	Preempt, Negate, Exert, Detect	AT-2(5)
		Standard practice	Negate, Exert	PL-4(1)
	Adversarial Simulation (CM1107)	Dynamic Threat Awareness, Self-Challenge	Preempt	AT-2(1), AT-3(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
	Active Decoys (CM1123)	Misdirection, Forensic and Behavioral Analysis	Detect	SC-35
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Search Closed Sources (T1597)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, CA-8(2)
	Collaborate to Counter Adversaries (CM1161)	Disinformation, Tainting	Deceive, Detect	SC-30(4), SI-20
		Dynamic Threat Awareness	Detect	PM-16
	Restrict Supply Chain Exposures (CM1162)	Obfuscation, Supply Chain Diversity	Exert	SR-3(2)
		Disinformation	Deceive	SR-7

ATT&CK Technique (*Reconnaissance*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
		Self-Challenge	Detect	SR-6(1), SR-7
Search Open Technical Databases (T1596)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, CA-8(2)
	Restrict Supply Chain Exposures (CM1162)	Obfuscation, Supply Chain Diversity	Exert	SR-3(2)
		Disinformation	Deceive	SR-7
		Self-Challenge	Detect	SR-6(1), SR-7
Search Open Websites / Domains (T1593)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
Search Victim-Owned Websites (T1594)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)

3.2 Resource Development

The adversary's goal for the seven Techniques under the Resource Development Tactic is to establish resources they can use to support operations.

Table 2. Resource Development Tactic (TA0042): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Resource Development*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
Acquire Infrastructure (T1583)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Present Deceptive Information (CM1101)	Disinformation	Preempt, Detect	SC-30(4)
	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, CA-8(2)
	Collaborate to Counter Adversaries (CM1161)	Dynamic Threat Awareness	Detect	PM-16
	Pre-Compromise (M1056)	Standard practice	Exert	SC-38

ATT&CK Technique (*Resource Development*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
Compromise Accounts (T1586)	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	AU-13, AU-13 (3), RA-5(4), RA-10
Compromise Infrastructure (T1584)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect, Scrutinize, Reveal	AU-13, AU-13 (3), PM-16, RA-5(4), RA-10
Develop Capabilities (T1587)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	PM-16, RA-10
Establish Accounts (T1585)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(5), AT-3(3)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	AU-13, AU-13 (3), RA-5(4), RA-10
Obtain Capabilities (T1588)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(5), AT-3(3)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	PM-16, RA-10
Stage Capabilities (T1608)	Pre-Compromise (M1056)	Standard practice	Exert	SC-38
	Restrict Supply Chain Exposures (CM1162)	Integrity Checks, Provenance Tracking	Detect	SR-5, SR-11
		Monitoring and Damage Assessment	Detect	SR-6(1), SR-10
		Forensic and Behavioral Analysis	Detect, Scrutinize	SR-10

ATT&CK Technique (*Resource Development*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
		Predefined Segmentation	Contain	CM-7(7)
	Monitor External Sources (CM2043)	Monitoring and Damage Assessment, Dynamic Threat Awareness	Detect	PM-16, RA-10

3.3 Initial Access

The adversary's goal for the nine Techniques under the Initial Access Tactic is to get into the enterprise network.

Table 3. Initial Access Tactic (TA0001): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
Drive-by Compromise (T1189)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-18 (5), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
		Behavior Validation	Detect, Exert	IR-4(13)
	Restrict Web-Based Content (M1021)	Standard practice	Negate, Preempt	CM-7(5), SC-18, SC-7
	Update Software (M1051)	Cyber hygiene	Preempt, Negate, Expunge, Shorten	SI-2
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2(12)
Exploit Public-Facing	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-18 (5), SC-39, CM-7(6)

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
Application (T1190)	Exploit Protection (M1050)	Standard practice	Negate, Exert, Detect	SC-7(17), SI-7
	Network Segmentation (M1030)	Standard practice	Degrade, Preempt, Contain, Reduce	SC-7(29), SC-7(22)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Exert	AC-6(2)
	Update Software (M1051)	Cyber hygiene	Preempt, Negate, Exert	SI-2
	Vulnerability Scanning (M1016)	Cyber hygiene	Detect, Reveal, Shorten	RA-5
	Monitor Logs (CM2004)	Behavior Validation	Detect	AU-6
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Adversarial Simulation (CM1107)	Self-Challenge	Preempt	CA-8, CA-8(2)
External Remote Services (T1133)	Disable or Remove Feature or Program (M1042)	Restriction	Preempt, Negate	CM-7(2)
	Limit Access to Resource Over Network (M1035)	Standard practice	Preempt, Exert	AC-6, AC-3, AC-17
	Multi-factor Authentication (M1032)	Standard practice	Exert, Preempt	IA-2(1), IA-2(2), IA-2(6)
	Network Segmentation (M1030)	Predefined Segmentation	Preempt, Contain, Exert	AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Shorten	SC-10, SI-14(3)
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Degrade, Preempt	SC-23(3)

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Hardware Additions (T1200)	Limit Access to Resource over Network (M1035)	Trust-Based Privilege Management	Preempt	AC-6(3), AC-6(10)
	Limit Hardware Installation (M1034)	Restriction	Preempt, Negate	CM-8(3)
	Authenticate Devices (CM1125)	Obfuscation, Integrity Checks	Preempt, Negate	IA-3(1)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment	Detect	CM-8(3)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Preempt	SC-30(4)
Phishing (T1566)	Antivirus/Antimalware (M1049)	Cyber hygiene	Detect, Expunge, Shorten	AC-4, SI-3, AT-2, AT-3
	Network Intrusion Prevention (M1031)	Standard practice	Detect, Negate	SI-4(4), SC-44, SI-8
	Restrict Web-Based Content (M1021)	Standard practice	Contain, Exert, Preempt	AC-4(8), CM-7(5), SC-7(8)
	User Training (M1017)	Dynamic Threat Awareness	Negate, Exert	AT-2(1), AT-2(3), AT-2(5)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Preempt	SC-30(4)
	Detonation Chamber (CM1103)	Forensic and Behavioral Analysis	Detect, Scrutinize	SC-44
		Misdirection	Divert, Negate	SC-44
		Predefined Segmentation	Contain, Delay, Exert	SC-44
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35, SC-44
		Dynamic Segmentation and Isolation	Contain	SC-35, SC-44
Replication Through Removable Media (T1091)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Limit Hardware Installation (M1034)	Cyber hygiene	Preempt, Negate, Exert	MP-7, MP-6, SC-41

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
	Virtual Sandbox (CM1109)	Non-Persistent Services	Preempt Shorten	SC-7(20)
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Supply Chain Compromise (T1195)	Update Software (M1051)	Cyber hygiene	Negate, Shorten, Detect	SI-2
	Vulnerability Scanning (M1016)	Integrity Checks	Preempt, Detect	SA-9(7)
		Provenance Tracking	Detect, Scrutinize	SR-4(3), SR-4(4)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
		Integrity Checks, Provenance Tracking	Detect	CM-14, SR-4(3)
	Software Stress Testing (CM2010)	Self-Challenge	Detect	SR-6(1)
	Physical Inspection (CM2011)	Integrity Checks	Detect	SR-9, SR-10
	Component Provenance Validation (CM1105)	Provenance Tracking	Detect, Delay, Exert	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4)
	Supply Chain Diversity (CM1106)	Supply Chain Diversity	Exert	PL-8(2), SR-3(1), SR-3(2)
Trusted Relationship (T1199)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7, SC-7(21)
	User Account Control (M1052)	Standard practice	Preempt, Exert, Detect	AC-2(6), AC-6(8), AC-6(9), CM-11(2)
	Monitor Trusted Parties (CM2012)	Dynamic Threat Awareness	Detect	PM-16
		Behavior Validation	Detect	SI-10(3)
		Provenance Tracking	Detect	PM-30(1)
Valid Accounts (T1078)	Application Developer Guidance (M1013)	Standard practice	Preempt, Exert	AT-3, IA-5(7), SA-8
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Trust-Based Privilege Management, Consistency Analysis	Preempt	AC-6(7)
		Disinformation	Exert	SC-30(4)

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
	Present Deceptive Information (CM1101)	Tainting	Detect	SI-20
	Cross Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

3.4 Execution

The adversary's goal for the twelve Techniques under the Execution Tactic is to get malicious code running on an enterprise system.

Table 4. Execution Tactic (TA0002): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Command and Scripting Interpreter (T1059)	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2), SC-3(3)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(4), CM-7(5)
	Privileged Account Management (M1026)	Standard practice	Negate, Degrade, Exert	AC-6(7)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(13)
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)
		Non-Persistent Information	Expunge	SI-14, SI-14(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26, SI-3(10)
Container Administration Command (T1609)	Execution Prevention (M1038)	Non-Persistent Services, Provenance Tracking	Negate, Exert	SI-14(1)
	Limit Access to Resource over Network (M1035)	Standard practice	Degrade, Exert	CM-2, CM-2(2)
	Privileged Account Management (M1026)	Cyber hygiene	Exert	CM-2
	Execution Restriction (CM1111)	Attribute-Based Usage Restriction	Degrade, Exert	AC-3(13)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12), SI-4(16)
Deploy Container (T1610)	Limit Access to Resource Over Network (M1035)	Standard practice	Exert	CM-7(1)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7, SC-7(21), SC-7(29)
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert	AC-6(7)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Degrade, Exert	AC-6
		Trust-Based Privilege Management	Degrade, Exert	AC-6(5)
		Restriction	Degrade, Exert	CM-7(2)
	Analyze Logs (CM2005)	Sensor Fusion and Analysis	Detect	SI-4(16)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Exploitation for Client Execution (T1203)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Negate, Delay, Degrade, Exert	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Exploit Protection (M1050)	Standard practice	Negate, Detect, Exert	AC-4, SI-4, SI-7(17)
	Detonation Chamber (CM1103)	Predefined Segmentation	Negate	SC-44

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Scrutinize, Detect	IR-4(12)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Inter-Process Communication (T1559)	Application Isolation and Sandboxing (M1048)	Standard practice	Negate, Preempt, Detect, Contain	AC-4(21), AC-6(4), SC-39
	Behavior Prevention on Endpoint (M1040)	Restriction	Exert, Preempt	CM-7(2)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Privileged Account Management (M1026)	Standard practice	Negate, Degrade, Exert	AC-6(7)
	Software Configuration (M1054)	Standard practice	Preempt, Negate, Exert	CM-7(1)
	Monitor Use of Libraries and Utilities (CM2040)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4), SI-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
		Monitoring and Damage Assessment	Detect	SI-4(11), SI-4(13)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Native API (T1106)	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Host-Local Event Correlation (CM2022)	Sensor Fusion and Analysis	Detect	IR-4(13), SI-4(16)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Scheduled Task/Job (T1053)	Audit (M1047)	Standard practice	Detect	RA-5, AU-6
	Operating System Configuration (M1028)	Standard practice	Preempt, Exert	CM-6
	Privileged Account Management (M1026)	Standard practice	Preempt, Degrade, Exert	AC-6(7)
	User Account Management (M1018)	Standard practice	Preempt	AC-6(1)

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Detect, Scrutinize	SC-26
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Shared Modules (T1129)	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Execution Restriction (CM1111)	Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	AC-3(13)
	Host-Local Event Correlation (CM2022)	Sensor Fusion and Analysis	Detect	IR-4(13), SI-4(16)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Software Deployment Tools (T1072)	Active Directory Configuration (M1015)	Standard practice	Preempt, Exert	AC-6(5)
	Multi-factor Authentication (M1032)	Standard practice	Negate, Exert	IA-2(1), IA-2(2), IA-2(6)
	Network Segmentation (M1030)	Standard practice	Exert, Contain	SC-7(11), SC-7(21), AC-4
	Password Policies (M1027)	Standard practice	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Exert	AC-6(5)
	Remote Data Storage (M1029)	Predefined Segmentation, Trust-	Exert	AC-6(4)

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Based Privilege Management		
	Update Software (M1051)	Standard practice	Exert, Preempt	MA-6, MA-3(6), RA-5
	User Account Management (M1018)	Trust-Based Privilege Management, Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
	User Training (M1017)	Cyber hygiene	Negate	AC-3, AT-3
	Isolate or Contain Selected Applications or Components (CM1133)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	CM-7(6)
		Predefined Segmentation	Contain	CM-7(6)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Monitor Trusted Parties (CM2012)	Dynamic Threat Awareness	Detect	PM-16
		Dynamic Resource Awareness	Detect	SI-4(17)
		Provenance Tracking	Detect	PM-30(1)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5), AU-6(3)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
System Services (T1569)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Exert	AC-6(8)

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	SC-34, AC-3(15)
	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
User Execution (T1204)	Execution Prevention (M1038)	Standard practice	Preempt, Exert	CM-2, CM-3, CM-5, CM-6, CM-7, CM-8
	Network Intrusion Prevention (M1031)	Standard practice	Detect, Negate	SI-4(4)
	Restrict Web-Based Content (M1021)	Integrity Checks	Preempt, Exert	AC-4(8)
	User Training (M1017)	Cyber hygiene	Preempt	AT-2
	Minimize Local Functionality (CM1119)	Restriction	Contain, Preempt	CM-7(2), SC-25
	Identify External Malware (CM1136)	Monitoring and Damage Assessment	Detect	SC-35
		Forensic and Behavioral Analysis	Scrutinize	SC-35

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Windows Management Instrumentation (T1047)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Degrade, Delay, Exert	AC-6(5)
		Trust-Based Privilege Management	Negate, Degrade, Delay, Exert	AC-6(7)
		Consistency Analysis	Degrade, Delay, Exert	AC-6(7)
	User Account Management (M1018)	Standard practice	Negate	AC-6(1), AC-6(7)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Exert	AC-6
		Trust-Based Privilege Management	Exert	AC-6(5)
		Restriction	Exert	CM-7(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26

ATT&CK Technique (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26

3.5 Persistence

The adversary's goal for the 19 Techniques under the Persistence Tactic is to maintain access to systems across restarts, changed credentials, and other interruptions which could otherwise curtail their access.

Table 5. Persistence Tactic (TA0003): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
Account Manipulation (T1098)	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Delay, Preempt	AC-4(21), SC-7, SC-7(21)
	Operating System Configuration (M1028)	Standard practice	Exert, Negate	CM-5, CM-6, CM-7
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(2)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
BITS Jobs (T1197)	Filter Network Traffic (M1037)	Standard practice	Negate, Preempt, Exert	AC-4, SC-7
	Operating System Configuration (M1028)	Standard practice	Negate	CM-5, CM-6, CM-7, CM-7(2)
	User Account Management (M1018)	Standard practice	Negate	AC-4(12), AC-4(21), AC-4(17), AC-4(8)

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Boot or Logon Autostart Execution (T1547)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Negate	SI-14(2)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Boot or Logon Initialization Scripts (T1037)	Restrict File and Directory Permissions (M1022)	Standard practice	Preempt	AC-3(11), AC-3(15)
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	AC-6, CM-6
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Negate	SI-14(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Browser Extensions (T1176)	Audit (M1047)	Provenance Tracking	Detect, Negate	AU-10(2)
	Execution Prevention (M1038)	Standard practice	Preempt, Exert	CM-7(2), CM-7(5)
	Limit Software Installation (M1033)	Standard practice	Preempt, Exert	CM-11(2), CM-11(3)
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-2
	Update Software (M1051)	Cyber hygiene	Negate, Shorten	SI-2
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Compromise Client Software Binary (T1554)	Code Signing (M1045)	Provenance Tracking	Detect	SI-7(15)
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Detect, Scrutinize	IR-4(12)
	Software Integrity Check (CM2009)	Integrity Checks	Detect, Scrutinize	SI-7(1), SI-7(6)
Create Account (T1136)	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Network Segmentation (M1030)	Standard practice	Negate, Exert	SC-7, AC-4
	Operating System Configuration (M1028)	Standard practice	Exert, Preempt	CM-5, CM-6, CM-7
	Privileged Account Management (M1026)	Standard practice	Exert, Preempt	AC-6(1), AC-6(2)
	Check Policy Consistency (CM1129)	Consistency Analysis	Degrade, Exert, Detect	CA-7(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Create or Modify System Process (T1543)	Audit (M1047)	Consistency Analysis	Detect	CA-7(5)
	Limit Software Installation (M1033)	Standard practice	Preempt, Exert	CM-11(2), CM-5(6)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-2(7), SC-2
	User Account Management (M1018)	Standard practice	Negate	AC-6, AC-6(5)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
Event Triggered Execution (T1546)	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
External Remote Services (T1133)	Disable or Remove Feature or Program (M1042)	Restriction	Preempt, Negate	CM-7(2)
	Limit Access to Resource Over Network (M1035)	Standard practice	Preempt, Exert	AC-6, AC-3, AC-17

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Multi-factor Authentication (M1032)	Standard practice	Exert, Preempt	IA-2(1), IA-2(2), IA-2(6)
	Network Segmentation (M1030)	Predefined Segmentation	Preempt, Contain, Exert	AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Expunge, Shorten	SC-10, SI-14(3)
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Exert, Preempt	SC-23(3)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Hijack Execution Flow (T1574)	Audit (M1047)	Non-Persistent Information	Preempt, Exert	SI-14(2)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Restrict File and Directory Permissions (M1022)	Integrity Checks	Preempt, Exert	SC-34
	Restrict Library Loading (M1044)	Standard practice	Preempt, Negate, Exert	CM-7(4)
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	CM-6
	Update Software (M1051)	Standard practice	Exert, Preempt, Shorten	MA-6, MA-3(6)
	User Account Control (M1052)	Standard practice	Negate, Exert	AC-2(6), AC-6(8), AC-6(9), CM-11(2)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
		Dynamic Segmentation and Isolation	Contain	SC-35
	Validate Data Properties (CM1137)	Integrity Checks	Detect	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Implant Internal Image (T1525)	Audit (M1047)	Integrity Checks	Detect	SI-7, SI-7(1)
	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15)
	Privileged Account Management (M1026)	Standard practice	Negate, Exert	AC-6(1)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Office Application Startup (T1137)	Disable or Remove Feature or Program (M1042)	Standard practice	Exert, Negate	CM-7(2)
	Software Configuration (M1054)	Standard practice	Negate	CM-7(1)
	Update Software (M1051)	Standard practice	Exert, Negate	MA-6, MA-3(6)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6, SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
Pre-OS Boot (T1542)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-6, SI-7, SI-7(1), SI-7(9)
	Privileged Account Management (M1026)	Standard practice	Preempt	AC-2(6)
	Update Software (M1051)	Standard practice	Exert, Preempt, Negate	MA-6, MA-3(6), SI-2
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Shorten	SI-14(1)
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Detect	IR-4(12)
	Hardware-Based Protection of Firmware (CM1154)	Integrity Checks	Negate, Preempt	SC-51
	Host-Local Event Correlation (CM2022)	Sensor Fusion and Analysis	Detect	IR-4(13), SI-4(16)
Scheduled Task/Job (T1053)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)
	Operating System Configuration (M1028)	Standard practice	Exert, Preempt	CM-5, CM-6, CM-7
	Privileged Account Management (M1026)	Standard practice	Negate, Degrade, Exert	AC-6(7)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6(5), AC-3(7)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect, Scrutinize	SC-26
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Server Software Component (T1505)	Audit (M1047)	Integrity Checks	Detect	SI-7, SI-7(1)
	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15)
	Privileged Account Management (M1026)	Standard practice	Exert, Preempt	AC-6(5)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Sensor Fusion and Analysis	Detect	SI-4(16)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
Traffic Signaling (T1205)	Filter Network Traffic (M1037)	Standard practice	Exert	SC-7(11)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Exert	SC-10, SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Valid Accounts (T1078)	Application Developer Guidance (M1013)	Standard practice	Exert, Preempt	AT-3, IA-5(7), SA-8
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Trust-Based Privilege Management, Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

3.6 Privilege Escalation

The adversary's goal for the 13 Techniques under the Privilege Escalation Tactic is to gain higher-level permissions on a system or network than those obtained by previous TTPs in their campaign.

Table 6. Privilege Escalation Tactic (TA0004): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
Abuse Elevation Control Mechanism (T1548)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5, RA-5(10), AU-6(5)
	Execution Prevention (M1038)	Purposing	Negate	CM-7(5)
	Operating System Configuration (M1028)	Standard practice	Negate	SI-7, AC-6(8), CM-5, CM-6, CM-7
	Privileged Account Management (M1026)	Cyber hygiene	Negate	AC-2(7), AC-6(7)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate	AC-24

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	User Account Control (M1052)	Standard practice	Preempt	AC-2(6), AC-6(8), AC-6(9), CM-11(2)
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32 (1)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Access Token Manipulation (T1134)	Privileged Account Management (M1026)	Standard practice	Preempt	AC-6(5), AC-3(7)
	User Account Management (M1018)	Cyber hygiene	Negate, Exert	AC-3(15)
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-26, SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32 (1)
	Enhanced Authentication (CM1126)	Adaptive Management, Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
		Architectural Diversity, Design Diversity, Adaptive Management	Delay, Exert	CP-13
		Path Diversity	Delay, Exert	SC-47
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SC-16(1), SC-16(3)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment,	Detect	SC-26

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
Boot or Logon Autostart Execution (T1547)		Forensic and Behavioral Analysis		
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Negate	SI-14(2)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Boot or Logon Initialization Scripts (T1037)	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-3(15)
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	CM-6
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Negate	SI-14(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Create or Modify System Process (T1543)	Audit (M1047)	Consistency Analysis	Detect	CA-7(5)
	Limit Software Installation (M1033)	Standard practice	Negate, Preempt	CM-11(2), CM-5(6)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-2(7), SC-2
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
Escape to Host (T1611)	Application Isolation and Sandboxing (M1048)	Restriction	Contain, Exert	CM-7(2)
	Execution Prevention (M1038)	Non-Persistent Services	Negate, Exert	SC-34, SC-34(1)
	Privileged Account Management (M1026)	Attribute-Based Usage Restriction	Exert	AC-6
	Analyze Logs (CM2005)	Sensor Fusion and Analysis	Detect	SI-4(16)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Event Triggered Execution (T1546)	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Passive Decoys (CM1104)	Misdirection	Deceive, Negate, Contain	SC-26
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7, SI-7(1)
	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-18

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
Exploitation for Privilege Escalation (T1068)				(5), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
		Behavior Validation	Detect, Exert	IR-4(13)
		Synthetic Diversity, Restriction	Preempt, Exert	SI-16
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Negate	PM-16, RA-3(3)
	Update Software (M1051)	Standard practice	Exert, Preempt	SI-2, MA-3(6), RA-5
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal [20]	SI-20
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Shorten	SI-14(1)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Domain Policy Modification (T1484)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)
	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Lock Down Visibility or Access (CM1149)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(11)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
Hijack Execution Flow (T1574)	Audit (M1047)	Non-Persistent Information	Preempt, Exert	SI-14(2)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Restrict File and Directory Permissions (M1022)	Integrity Checks	Preempt, Exert	SC-34

[20] The Reveal effect is currently identified only for some uses of CM1101. Reveal can be an effect if the organization uses the PM-16 control, which is cited by M1019, CM2012, and CM1301, to share threat information it develops with other organizations, rather than simply being a consumer of threat information developed by other organizations.

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Restrict Library Loading (M1044)	Standard practice	Preempt, Negate	CM-5, CM-7(4), CM-7(5)
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	CM-6
	Update Software (M1051)	Standard practice	Preempt	SI-2, MA-3(6), RA-5
	User Account Control (M1052)	Standard practice	Preempt	AC-2(6), AC-6(8), AC-6(9), CM-11(2)
	User Account Management (M1018)	Standard practice	Negate	AC-6
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Validate Data Properties (CM1137)	Integrity Checks	Detect	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Process Injection (T1055)	Behavior Prevention on Endpoint (M1040)	Standard practice	Negate	CM-7(2)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Degrade	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Degrade	AC-6(8)
	Dynamically Relocate and Refresh Processing (CM1150)	Functional Relocation of Cyber Resources	Shorten	SC-30(3)
		Non-Persistent Services	Shorten	SI-14(1)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es)	Potential Effects on ATT&CK Technique	Control(s)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Scheduled Task/Job (T1053)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)
	Operating System Configuration (M1028)	Standard practice	Negate, Exert	CM-6
	Privileged Account Management (M1026)	Standard practice	Negate, Exert	AC-2(7), AC-6(7)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6(5), AC-3(7)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect, Scrutinize	SC-26
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Valid Accounts (T1078)	Application Developer Guidance (M1013)	Standard practice	Preempt, Exert	AT-3, IA-5(7), SA-8
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	AC-6(7)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

3.7 Defense Evasion

The adversary's goal for the 39 Techniques under the Defense Evasion Tactic is to avoid detection. Many of the Techniques under Defense Evasion also appear under other Tactics.

Table 7. Defense Evasion Tactic (TA0005): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Abuse Elevation Control	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Mechanism (T1548)	Execution Prevention (M1038)	Purposing	Negate	CM-7(5)
	Operating System Configuration (M1028)	Standard practice	Preempt, Exert	SI-7, AC-6(8), CM-5, CM-6, CM-7
	Privileged Account Management (M1026)	Cyber hygiene	Preempt, Exert	AC-2(7), AC-6(7), AC-17(4)
	Restrict File and Directory Permissions (M1022)	Standard practice	Preempt, Exert	AC-2(7), SC-2
	User Account Control (M1052)	Standard practice	Negate, Exert	AC-2(6), AC-6(8), AC-6(9), CM-11(2)
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32 (1)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Access Token Manipulation (T1134)	Privileged Account Management (M1026)	Standard practice	Preempt, Exert	AC-2(7), AC-6(7), AC-17(4)
	User Account Management (M1018)	Standard practice	Preempt, Exert	AC-6(5), AC-6(10)
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-26, SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Partition Host (CM1118)	Predefined Segmentation	Delay, Negate, Contain	SC-2, SC-2(1), SC-32, SC-32 (1)
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SC-16(1), SC-16(3)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
BITS Jobs (T1197)	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	AC-4, SC-7

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Operating System Configuration (M1028)	Standard practice	Negate, Exert	CM-5, CM-6, CM-7, CM-7(2)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-4(12), AC-4(21), AC-4(17), AC-4(8)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Build Image on Host (T1612)	Audit (M1047)	Integrity Checks	Detect	SI-7, SI-7(1)
	Limit Access to Resource over Network (M1035)	Standard practice	Degrade, Exert	CM-2, CM-2(2)
	Network Segmentation (M1030)	Predefined Segmentation	Negate, Degrade, Exert	SC-7, SC-7(22), SC-7(29)
	Privileged Account Management (M1026)	Cyber hygiene	Exert	CM-2
	Execution Restriction (CM1111)	Attribute-Based Usage Restriction	Degrade, Exert	AC-3(12)
	Lock Down Visibility or Access (CM1149)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(11)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Deobfuscate/Decode Files or Information (T1140)	Application- or Utility-Specific Data Removal (CM1110)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Integrity Checks	Detect	SI-7(1), SI-7(7)
		Dynamic Reconfiguration	Expunge	IR-4(2)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Host-Local Event Correlation (CM2022)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(16)
Deploy Container (T1610)	Limit Access to Resource Over Network (M1035)	Standard practice	Exert	CM-7(1)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7, SC-7(21), SC-7(29)
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert	AC-6(7)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Degrade, Exert	AC-6
		Trust-Based Privilege Management	Degrade, Exert	AC-6(5)
		Restriction	Degrade, Exert	CM-7(2)
	Analyze Logs (CM2005)	Sensor Fusion and Analysis	Detect	SI-4(16)
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Direct Volume Access (T1006)	Present Decoy Data (CM1113)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
Execution Guardrails (T1480)	Do Not Mitigate (M1055)	Standard practice	—	—
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Exploitation for Defense Evasion (T1211)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Exert	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
		Synthetic Diversity, Restriction	Preempt, Exert	SI-16
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Negate	PM-16, RA-3(3)
	Update Software (M1051)	Cyber hygiene	Preempt, Negate, Expunge, Shorten	SI-2, MA-3(6), RA-5
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
File and Directory Permissions Modification (T1222)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	AC-6(8)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-3(15)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Domain Policy Modification (T1484)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)
	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Lock Down Visibility or Access (CM1149)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(11)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
Hide Artifacts (T1564)	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Hijack Execution Flow (T1574)	Audit (M1047)	Non-Persistent Information	Preempt, Exert	SI-14(2)
	Execution Prevention (M1038)	Purposing	Negate, Delay, Degrade, Exert	CM-7(5)
	Restrict File and Directory Permissions (M1022)	Integrity Checks	Preempt, Exert	SC-34
	Restrict Library Loading (M1044)	Standard practice	Preempt, Exert, Negate	CM-2
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	CM-6

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Update Software (M1051)	Cyber hygiene	Preempt, Exert	SI-2, MA-3(6), RA-5
	User Account Control (M1052)	Standard practice	Preempt, Exert	AC-2(6), AC-6(8), AC-6(9),CM-11(2)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-3, AC-6(10)
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
	Validate Data Properties (CM1137)	Integrity Checks	Detect	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Impair Defenses (T1562)	Restrict File and Directory Permissions (M1022)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-6(1)
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	CM-6
	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-6(1)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Indicator Removal on Host (T1070)	Encrypt Sensitive Information (M1041)	Obfuscation	Degrade, Exert	AU-9(3), SC-8(4), SC-28 (1)
	Remote Data Storage (M1029)	Predefined Segmentation	Degrade, Exert	AU-9(2)
		Non-Persistent Information	Degrade, Exert	SI-14(2)
		Integrity Checks	Degrade, Exert	AU-9(6)
	Restrict File and Directory Permissions (M1022)	Trust-Based Privilege Management	Degrade, Exert	AU-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Defend Audit Data (CM1158)	Integrity Checks	Negate	AU-9(1)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Indirect Command Execution (T1202)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Sensor Fusion and Analysis	Detect	SI-4(16)
Masquerading (T1036)	Code Signing (M1045)	Provenance Tracking	Detect	SI-7(15)
	Execution Prevention (M1038)	Restriction	Preempt, Exert	CM-7(4)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-3(15), AC-3(11), AC-6
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Modify Authentication Process (T1556)	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)
	Operating System Configuration (M1028)	Standard practice	Negate, Exert	AC-3(15), AC-3(11), AC-6
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Degrade, Exert, Shorten	AC-6(7)
	Privileged Process Integrity (M1025)	Standard practice	Negate, Exert	SI-7(3), SI-7(6)
	Enhanced Authentication (CM1126)	Adaptive Management, Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
		Architectural Diversity, Design Diversity, Adaptive Management	Delay, Exert	CP-13
		Path Diversity	Delay, Exert	SC-47
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Modify Cloud Compute Infrastructure (T1578)	Audit (M1047)	Standard practice	Detect, Exert	RA-5, RA-5(10), AU-6(5)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6(5), AC-3(7)
	Centralize and Analyze Instance Logging (CM2023)	Sensor Fusion and Analysis	Detect	AU-6(5), IR-4(4)
Modify Registry (T1112)	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	CM-6

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Modify System Image (T1601)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-7, SI-7(1), SI-7(6), SI-7(9)
	Code Signing (M1045)	Provenance Tracking	Preempt	SI-7(15), SR-4(3)
	Credential Access Protection (M1043)	Standard practice	Delay, Exert	IA-5(7), SC-28 (1)
	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(5)
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SC-16(1), SC-16(3)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services, Non-Persistent Information, Provenance Tracking	Expunge, Exert, Shorten	SI-14(1)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7(6)
Network Boundary Bridging (T1599)	Credential Access Protection (M1043)	Standard practice	Delay, Exert	IA-5, SC-29 (1)
	Filter Network Traffic (M1037)	Adaptive Management	Degrade, Reduce	AC-4(3)
		Dynamic Reconfiguration	Degrade, Reduce	IR-4(2)
		Monitoring and Damage Assessment	Detect	SI-4(4)
	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(5)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services, Non-Persistent Information	Expunge, Exert, Shorten	SI-14(1)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Enhance via Heterogeneity (CM1305)	Architectural Diversity	Exert	AU-9(7), SC-29, SC-29 (1)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Obfuscated Files or Information (T1027)	Antivirus/Antimalware (M1049)	Cyber hygiene	Detect, Expunge, Shorten	AC-4, SI-3, SC-44
	Detonation Chamber (CM1103)	Forensic and Behavioral Analysis	Detect, Scrutinize	SC-44
	Application- or Utility-Specific Data Removal (CM1110)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Integrity Checks	Detect	SI-7(1), SI-7(7)
		Dynamic Reconfiguration	Expunge	IR-4(2)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Pre-OS Boot (T1542)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-6, SI-7, SI-7(1), SI-7(9)
	Privileged Account Management (M1026)	Standard practice	Negate, Exert	AC-3(15)
	Update Software (M1051)	Cyber hygiene	Preempt, Exert	SI-2, MA-3(6), RA-5
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Information	Expunge, Shorten	SI-14(1)
	Hardware-Based Protection of Firmware (CM1154)	Integrity Checks	Negate, Preempt	SC-51

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Endpoint Scrutiny (CM2019)	Forensic and Behavioral Analysis	Detect	IR-4(12)
Process Injection (T1055)	Behavior Prevention on Endpoint (M1040)	Standard practice	Negate, Exert	CM-7(2)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Degrade	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Degrade	AC-6(8)
	Dynamically Relocate and Refresh Processing (CM1150)	Functional Relocation of Cyber Resources	Shorten	SC-30(3)
		Non-Persistent Services	Shorten	SI-14(1)
	Defend Against Memory Attacks (CM1152)	Synthetic Diversity, Temporal Unpredictability	Negate, Exert	SI-16
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Process Analysis (CM2014)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Rogue Domain Controller (T1207)	Validate Data Quality (CM1130)	Integrity Checks	Detect, Shorten	SI-7(1)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Rootkit (T1014)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Calibrate Administrative Access (CM1164)	Attribute-Based Usage Restriction	Exert	AC-6
		Trust-Based Privilege Management	Exert	AC-6(5)
		Restriction	Exert	CM-7(2)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Signed Binary Proxy Execution (T1218)	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(7)
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	AC-6(8)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2), SC-3(3)
	Execution Prevention (M1038)	Standard practice	Preempt, Exert	CM-7
	Exploit Protection (M1050)	Standard practice	Negate, Detect, Exert	AC-4, SI-4, SI-7(17)
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)
		Non-Persistent Information	Expunge	SI-14, SI-14(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Signed Script Proxy Execution (T1216)	Execution Prevention (M1038)	Standard practice	Preempt, Exert	CM-7
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)
		Non-Persistent Information	Expunge	SI-14, SI-14(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	SI-4(2)
	Monitor Script Execution (CM2029)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Subvert Trust Controls (T1553)	Execution Prevention (M1038)	Purposing	Negate, Exert	CM-7(5)
	Operating System Configuration (M1028)	Standard practice	Preempt, Exert	CM-2
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert, Degrade	CM-6
	Software Configuration (M1054)	Provenance Tracking	Negate, Exert	AC-4(17)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Expunge, Shorten	SC-23(3), SI-14(2), SI-21
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
	Analyze Logs (CM2005)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
	Software Integrity Check (CM2009)	Integrity Checks	Detect	SI-7(6)
Template Injection (T1221)	Antivirus/Antimalware (M1049)	Predefined Segmentation	Negate, Contain	SC-44
	Disable or Remove Feature or Program (M1042)	Restriction	Negate, Degrade	CM-7(2)
	Network Intrusion Prevention (M1031)	Predefined Segmentation	Negate, Contain	SC-44
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Detect	SC-26
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Traffic Signaling (T1205)	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	SC-7(11)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Exert	SC-10, SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Trusted Developer Utilities Proxy Execution (T1127)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2), SC-3(3)
	Execution Prevention (M1038)	Purposing	Exert, Preempt	CM-7(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Unused/Unsupported Cloud Regions (T1535)	Software Configuration (M1054)	Attribute-Based Usage Restriction	Negate	AC-3(13)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6, SI-4(11)
Use Alternate Authentication Material (T1550)	Privileged Account Management (M1026)	Standard practice	Degrade, Exert	AC-6(7)
	User Account Management (M1018)	Standard practice	Negate, Degrade, Exert	AC-6
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Exert	SC-23(3), SI-14(2), SI-21
		Temporal Unpredictability	Exert	SC-23(3)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
	Cross Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)
Valid Accounts (T1078)	Application Developer Guidance (M1013)	Standard practice	Preempt, Exert	AT-3, IA-5(7), SA-8
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Preempt	AC-6(7)

ATT&CK Technique (*Defense Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)
	Present Deceptive Information (CM1101)	Disinformation	Exert	SC-30(4)
		Tainting	Detect	SI-20
	Cross Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)
Virtualization/Sandbox Evasion (T1497)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35
Weaken Encryption (T1600)	Execution Restriction (CM1111)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-3(13)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services, Non-Persistent Information, Provenance Tracking	Expunge, Exert, Shorten	SI-14(1)
XSL Script Processing (T1220)	Execution Prevention (M1038)	Standard practice	Preempt, Exert	CM-7(2)
	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Quarantine or Delete Suspicious Files (CM1132)	Provenance Tracking	Detect	SR-4(3)
		Dynamic Segmentation and Isolation	Contain, Delay, Degrade, Exert	CM-7(6)
		Non-Persistent Information	Expunge	SI-14(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

3.8 Credential Access

The adversary's goal for the 15 Techniques under the Credential Access Tactic is to steal credentials (e.g., account names, passwords) for future use.

Table 8. Credential Access Tactic (TA0006): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Credential Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Brute Force (T1110)	Account Use Policies (M1036)	Standard practice	Delay, Exert	AC-2(11), AC-7
	Multi-factor Authentication (M1032)	Standard practice	Delay, Exert, Negate	IA-2(1), IA-2(2), IA-2(6)
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	User Account Management (M1018)	Standard practice	Shorten, Expunge	AC-2(3), AC-2(6), AC-2(8)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Design Diversity (CM1128)	Design Diversity	Delay, Exert	SA-17(9)
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Check Policy Consistency (CM1129)	Consistency Analysis	Degrade, Exert	CA-7(5)
Credentials from Password Stores (T1555)	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Exploitation for Credential Access (T1212)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Delay, Preempt	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert	AC-4(8)
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Negate	PM-16, RA-3(3)

ATT&CK Technique (*Credential Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Update Software (M1051)	Cyber hygiene	Exert, Preempt	SI-2, MA-3(6), RA-5
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Forced Authentication (T1187)	Filter Network Traffic (M1037)	Standard practice	Exert, Negate	AC-4
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	AC-2(12)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment	Detect	AC-2(12)
Input Capture (T1056)	Trusted Path (CM1120)	Predefined Segmentation	Negate, Contain	SC-11
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12), SI-4(16)
		Dynamic Resource Awareness	Detect	SI-4(16)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Adversary-in-the-Middle (T1557)	Disable or Remove Feature or Program (M1042)	Restriction	Negate, Exert	CM-7(2), SC-3(3)
	Filter Network Traffic (M1037)	Provenance Tracking	Negate, Exert	SC-7(11), SI-10(5)
	Limit Access to Resource Over Network (M1035)	Trust-Based Privilege Management	Negate, Exert	AC-6(3)
	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Degrade, Exert	SC-7, SC-7(21), SC-7(22)
	User Training (M1017)	Cyber hygiene	Negate	AT-3

ATT&CK Technique (*Credential Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Modify Authentication Process (T1556)	Multi-factor Authentication (M1032)	Standard practice	Negate, Exert, Delay	IA-2(1), IA-2(2)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-3(15)
	Operating System Configuration (M1028)	Standard practice	Delay, Exert, Preempt	CM-5, CM-6, CM-7
	Privileged Account Management (M1026)	Consistency Analysis, Trust-Based Privilege Management	Negate, Delay, Degrade, Exert	AC-6(7)
	Privileged Process Integrity (M1025)	Standard practice	Negate, Exert	CM-7
	Enhanced Authentication (CM1126)	Adaptive Management, Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
		Architectural Diversity, Design Diversity, Adaptive Management	Delay, Exert	CP-13
		Path Diversity	Delay, Exert	SC-47
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Network Sniffing (T1040)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Exert	SC-8(1)

ATT&CK Technique (*Credential Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Multi-factor Authentication (M1032)	Standard practice	Negate, Preempt, Exert	IA-2(1), IA-2(2)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Privileged Account Monitoring (CM2017)	Monitoring and Damage Assessment	Detect	AU-6(8)
OS Credential Dumping (T1003)	Active Directory Configuration (M1015)	Standard practice	Preempt, Exert	AC-2, AC-2(1), IA-5
	Credential Access Protection (M1043)	Standard practice	Preempt, Exert	IA-5, SC-29 (1)
	Operating System Configuration (M1028)	Restriction	Preempt	CM-7(2)
	Password Policies (M1027)	Cyber hygiene	Exert	IA-5
	Privileged Account Management (M1026)	Cyber hygiene	Exert, Negate	AC-2(7), AC-6(7)
	Privileged Process Integrity (M1025)	Restriction	Preempt	CM-7(2)
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3
	Hide Sensitive Information (CM1135)	Obfuscation	Delay, Exert	SC-28 (1)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Adversarial Simulation (CM1107)	Self-Challenge	Preempt	CA-8, CA-8(2)
Steal Application Access Token (T1528)	Audit (M1047)	Standard practice	Detect, Shorten, Expunge, Negate	RA-5, RA-5(10), AU-6(5)
	Restrict Web-Based Content (M1021)	Trust-Based Privilege Management	Negate, Exert	AC-6(4)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6(5)
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3

ATT&CK Technique (*Credential Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Hunt for Malicious Processes (CM2048)	Forensic and Behavioral Analysis	Detect	IR-5
Steal or Forge Kerberos Tickets (T1558)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Exert	SC-30
	Active Directory Configuration (M1015)	Standard practice	Contain, Exert, Negate, Expunge	SC-7(20), IA-5(13)
	Password Policies (M1027)	Cyber hygiene	Exert	IA-5
	Privileged Account Management (M1026)	Cyber hygiene	Exert, Degrade	AC-2(7), AC-6(7)
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Exert	SC-30(4)
Steal Web Session Cookie (T1539)	Multi-factor Authentication (M1032)	Standard practice	Exert, Delay	IA-2(1), IA-2(2)
	Software Configuration (M1054)	Non-Persistent Information	Degrade, Exert	SI-14(2), SI-21
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Expunge, Shorten	SI-14(2)
Two-Factor Authentication Interception (T1111)	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3
	Monitor Logs (CM2004)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
Unsecured Credentials (T1552)	Active Directory Configuration (M1015)	Standard practice	Preempt, Exert	SC-7(20)
	Audit (M1047)	Standard practice	Detect	RA-5, AU-6(5)
	Encrypt Sensitive Information (M1041)	Calibrated Defense-in-Depth, Obfuscation	Negate, Degrade, Exert	SC-28 (1), IA-2(6)
	Filter Network Traffic (M1037)	Restriction	Negate, Degrade, Exert	SC-3(3)
	Operating System Configuration (M1028)	Standard practice	Negate, Preempt	CM-5, CM-6, CM-7
	Password Policies (M1027)	Cyber hygiene	Delay, Exert, Preempt, Negate	IA-5
	Privileged Account Management (M1026)	Standard practice	Preempt, Exert	AC-2(7), AC-6(7)

ATT&CK Technique (*Credential Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-2(7), SC-2
	Update Software (M1051)	Cyber hygiene	Preempt, Exert	SI-2, MA-3(6), RA-5
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Partition Host (CM1118)	Predefined Segmentation	Contain, Delay, Exert	SC-2, SC-2(1), SC-32, SC-32 (1)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)

3.9 Discovery

The adversary's goal for the 27 Techniques under the Discovery Tactic is to learn about the enterprise's information environment, e.g., network segments, network nodes or endpoint systems, operating systems (OSs), applications, accounts, and trust relationships.

Table 9. Discovery Tactic (TA0007): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Account Discovery (T1087)	Operating System Configuration (M1028)	Standard practice	Negate, Exert	CM-5, CM-6, CM-7
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Reveal, Scrutinize	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Application Window Discovery (T1010)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Browser Bookmark Discovery (T1217)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Cloud Infrastructure Discovery (T1580)	User Account Management (M1018)	Trust-Based Privilege Management	Degrade	AC-6
		Consistency Analysis	Exert	AC-6(7)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Degrade, Exert	SC-26
		Architectural Diversity	Deceive, Divert, Degrade, Exert	SC-29
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
Cloud Service Dashboard (T1538)	User Account Management (M1018)	Trust-Based Privilege Management	Degrade	AC-6
		Consistency Analysis	Exert	AC-6(7)
	Monitor Logs (CM2004)	Monitoring and Damage Assessment	Detect	AU-6
Cloud Service Discovery (T1526)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Degrade, Exert	SC-26
		Architectural Diversity	Deceive, Divert, Degrade, Exert	SC-29
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Container and Resource Discovery (T1613)	Network Segmentation (M1030)	Predefined Segmentation	Negate, Degrade, Exert	SC-7, SC-7(21)
	Limit Access to Resource Over Network (M1035)	Standard practice	Preempt, Exert	AC-6, AC-3, AC-17
	User Account Management (M1018)	Attribute-Based Usage Restriction	Degrade	AC-6
		Consistency Analysis	Exert	AC-6(7)

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Defend Audit Data (CM1158)	Predefined Segmentation	Negate, Exert	AU-9(2)
	Centralize and Analyze Instance Logging (CM2023)	Sensor Fusion and Analysis	Detect	AU-6(5), IR-4(4)
Domain Trust Discovery (T1482)	Audit (M1047)	Consistency Analysis	Exert	CA-7(5)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7
	Present Deceptive Information (CM1101)	Disinformation	Delay, Deter, Deceive, Exert	SC-30(4)
		Tainting	Detect, Scrutinize	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
File and Directory Discovery (T1083)	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Delay	SC-26
	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Network Service Scanning (T1046)	Disable or Remove Feature or Program (M1042)	Standard practice	Preempt, Negate, Exert	CM-7(2)
	Network Intrusion Prevention (M1031)	Standard practice	Detect, Negate	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7
	Passive Decoys (CM1104)	Misdirection	Divert, Deceive, Delay	SC-26

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Network Share Discovery (T1135)	Passive Decoys (CM1104)	Misdirection	Divert, Deceive, Delay	SC-26
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Network Sniffing (T1040)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-8(1)
	Multi-factor Authentication (M1032)	Standard practice	Exert, Delay	IA-2(1), IA-2(2)
	Conceal or Randomize Network Traffic (CM1148)	Obfuscation, Contextual Unpredictability	Delay, Exert	SC-8(5), SC-30
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt	SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Password Policy Discovery (T1201)	Password Policies (M1027)	Cyber hygiene	Delay, Exert	IA-5
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Peripheral Device Discovery (T1120)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Permission Groups Discovery (T1069)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Process Discovery (T1057)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Query Registry (T1012)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Remote System Discovery (T1018)	Passive Decoys (CM1104)	Misdirection	Divert, Deceive, Delay	SC-26
	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Software Discovery (T1518)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Information Discovery (T1082)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Degrade, Exert	SC-30(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
System Location Discovery (T1614)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Physically Relocate Resources (CM1156)	Asset Mobility	Expunge, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13)
System Network Configuration Discovery (T1016)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Degrade, Exert	SC-30(4)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Network Connections Discovery (T1049)	Conceal Resources from Discovery (CM1160)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Owner/User Discovery (T1033)	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Services	Shorten	AC-12
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Service Discovery (T1007)	Lock Down Thin Nodes (CM1115)	Restriction	Preempt	SC-25
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
System Time Discovery (T1124)	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2), SI-4(4)

ATT&CK Technique (*Discovery*)	Mitigations(M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Virtualization/Sandbox Evasion (T1497)	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Active Decoys (CM1123)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
		Dynamic Segmentation and Isolation	Contain	SC-35

3.10 Lateral Movement

The adversary's goal for the nine Techniques under the Lateral Movement Tactic is to move from system to system within the enterprise environment.

Table 10. Lateral Movement Tactic (TA0008): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Exploitation of Remote Services (T1210)	Application Isolation and Sandboxing (M1048)	Predefined Segmentation	Contain, Delay, Preempt	AC-4(21), AC-6(4), SC-39, CM-7(6)
	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Exploit Protection (M1050)	Integrity Checks	Delay, Exert, Detect	AC-4(8)
		Behavior Validation	Detect	IR-4(13)
		Synthetic Diversity, Restriction	Preempt, Exert	SI-16
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), SC-3, SC-7
	Privileged Account Management (M1026)	Standard practice	Degrade, Exert	AC-6(7), AC-2(7), AC-17(4)
	Threat Intelligence Program (M1019)	Dynamic Threat Awareness	Exert, Negate	PM-16, RA-3(3)
	Update Software (M1051)	Cyber hygiene	Negate, Preempt, Expunge, Exert	SI-2, MA-3(6), RA-5
	Vulnerability Scanning (M1016)	Cyber hygiene	Detect	RA-5, SI-4(22)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Endpoint Behavior Analysis (CM2003)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)

ATT&CK Technique (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Internal Spearphishing (T1534)	Present Deceptive Information (CM1101)	Disinformation	Deceive	SC-30(4)
		Tainting	Detect	SI-20
	Enhance User Preparedness (CM1159)	Dynamic Threat Awareness	Detect	AT-2(1), AT-2(3), AT-2(5), AT-3(3)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Lateral Tool Transfer (T1570)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Negate, Exert	SI-4(4), SI-4(5)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Reconfiguration	Contain, Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Dynamic Segmentation, and Isolation	Contain, Shorten, Reduce	SC-7(20)
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25
		Non-Persistent Information	Preempt	SC-25
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(24)
Remote Service Session Hijacking (T1563)	Disable or Remove Feature or Program (M1042)	Standard practice	Preempt, Exert	CM-7(2)

ATT&CK Technique (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7
	Privileged Account Management (M1026)	Standard practice	Degrade, Exert	AC-6(7), AC-2(7), AC-17(4)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6(5), AC-3(7), AC-12, AC-17
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Services	Expunge, Shorten	AC-12
	Refresh Sessions or Connections (CM1146)	Non-Persistent Connectivity	Preempt, Shorten	SI-14(3)
		Temporal Unpredictability	Preempt, Shorten	SC-23(3), SC-30(2)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Remote Services (T1021)	Multi-factor Authentication (M1032)	Standard practice	Exert, Negate	IA-2(1), IA-2(2)
	User Account Management (M1018)	Consistency Analysis, Trust-Based Privilege Management	Delay, Exert	AC-6(7)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Reconfiguration	Contain, Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Dynamic Segmentation, and Isolation	Contain, Shorten, Reduce	SC-7(20)
	Modulate Information Flows (CM1153)	Predefined Segmentation, Trust-Based Privilege Management	Negate, Exert	SC-7(15)

ATT&CK Technique (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
Replication Through Removable Media (T1091)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Limit Hardware Installation (M1034)	Cyber hygiene	Preempt, Negate, Exert	MP-7, MP-6, SC-41
	Virtual Sandbox (CM1109)	Non-Persistent Services	Preempt, Shorten	SI-14
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Software Deployment Tools (T1072)	Active Directory Configuration (M1015)	Standard practice	Preempt, Exert	AC-6(5)
	Multi-factor Authentication (M1032)	Standard practice	Negate, Exert, Delay, Contain	IA-2(1), IA-2(2)
	Network Segmentation (M1030)	Standard practice	Contain, Degrade, Exert	AC-4(21), SC-7
	Password Policies (M1027)	Cyber hygiene	Negate, Exert	IA-5
	Privileged Account Management (M1026)	Cyber hygiene	Exert	AC-6(7), AC-2(7), AC-17(4)
	Remote Data Storage (M1029)	Predefined Segmentation, Trust-Based Privilege Management	Exert	AC-6(4)
	Update Software (M1051)	Cyber hygiene	Preempt, Exert	SI-2
	User Account Management (M1018)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	AC-6(7)
		Consistency Analysis	Degrade, Exert, Shorten, Reduce	AC-6(7)
	User Training (M1017)	Cyber hygiene	Negate, Exert	AT-3
	Isolate or Contain Selected Applications or Components (CM1133)	Trust-Based Privilege Management	Degrade, Exert, Shorten, Reduce	CM-7(6)
		Predefined Segmentation	Contain	CM-7(6)

ATT&CK Technique (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Refresh Selected Applications or Components (CM1134)	Non-Persistent Services	Expunge, Shorten	SI-14(1)
	Monitor Trusted Parties (CM2012)	Dynamic Threat Awareness	Detect	PM-16
		Dynamic Resource Awareness	Detect	SI-4(17)
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5), AU-6(3)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Taint Shared Content (T1080)	Execution Prevention (M1038)	Standard practice	Detect, Preempt, Exert	CM-7(2)
	Exploit Protection (M1050)	Standard practice	Negate, Detect, Exert	RA-5, SI-3
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-2(7), SC-2
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Predefined Segmentation	Contain, Divert, Delay, Degrade, Exert	SC-7(21)

ATT&CK Technique (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Disinformation	Delay, Degrade, Exert	SC-30(4)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26, SI-3(10)
	Validate Data Properties (CM1137)	Integrity Checks	Negate, Detect	SI-7
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Use Alternate Authentication Material (T1550)	Privileged Account Management (M1026)	Standard practice	Negate, Delay, Exert	AC-6(7)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6(5), AC-3(7)
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Exert	SC-23(3), SI-14(2), SI-21
		Temporal Unpredictability	Exert	SC-23(3)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-10
	Cross Enterprise Account Usage Analysis (CM2013)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

3.11 Collection

The adversary's goal for the 17 Techniques under the Collection Tactic is to gather information for future use – primarily for Exfiltration, but also for Credential Access.

Table 11. Collection Tactic (TA0009): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Archive Collected Data (T1560)	Audit (M1047)	Sensor Fusion and Analysis	Detect	AU-6(5)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Audio Capture (T1123)	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Dynamically Disable or Suspend (CM1121)	Non-Persistent Connectivity	Preempt, Delay	SC-15 (1)
		Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
Automated Collection (T1119)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-28 (1)
	Remote Data Storage (M1029)	Predefined Segmentation	Delay	AU-9(2) [21], SC-7(21)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources, Temporal Unpredictability	Negate, Delay, Degrade, Exert	SC-30(3)
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Defend Against Data Mining (CM1157)	Monitoring and Damage Assessment, Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges	Delay, Degrade, Exert, Detect	AC-23
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

[21] AU-9(2) applies only to audit information.

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Clipboard Data (T1115)	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(5)
Data from Cloud Storage Object (T1530)	Audit (M1047)	Standard practice	Detect	RA-5, AU-6
	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-28 (1)
	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	SC-7(11), AC-4
	Multi-factor Authentication (M1032)	Standard practice	Negate, Exert	IA-2(1), IA-2(2)
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Dynamic Privileges	Delay, Exert	IA-2(13), IA-10
	Restrict File and Directory Permissions (M1022)	Standard practice	Preempt, Exert	AC-3(15), AC-2(7)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6, AC-2(2)
	Cloud Account Monitoring (CM2016)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Data from Configuration Repository (T1602)	Encrypt Sensitive Information (M1041)	Obfuscation	Delay, Degrade, Preempt	SC-28 (1)
	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	AC-4, AC-4(8)
	Network Intrusion Prevention (M1031)	Standard practice	Detect	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	SC-7, SC-7(21)
	Software Configuration (M1054)	Standard practice	Negate, Preempt, Exert	CM-7(1)
	Update Software (M1051)	Cyber hygiene	Negate, Preempt, Expunge	SI-2
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Detect	SC-30(4)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Data from Information Repositories (T1213)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6
	User Training (M1017)	Standard practice	Negate, Exert	AT-3

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Adversarial Simulation (CM1107)	Self-Challenge	Negate	SI-19(8)
	Minimize Data Retention or Lifespan (CM1124)	Non-Persistent Information	Delay, Exert, Preempt	SI-14(2), SI-21
	Hide Sensitive Information (CM1135)	Obfuscation	Preempt, Negate, Exert	SI-19(4)
	Privileged Account Monitoring (CM2017)	Monitoring and Damage Assessment	Detect	AU-6(8)
	Account Monitoring (CM2021)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
	Dynamic Account Management (CM1117)	Dynamic Reconfiguration	Contain, Shorten, Reduce	AC-2(6)
		Dynamic Privileges	Exert, Delay	AC-2(6), AC-2(8)
Data from Local System (T1005)	Partition Host (CM1118)	Predefined Segmentation	Contain, Degrade, Exert	SC-2, SC-2(1), SC-32, SC-32 (1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Hide Sensitive Information (CM1135)	Obfuscation	Delay, Degrade, Preempt	SC-28 (1)
Data from Network Shared Drive (T1039)	Partition Host (CM1118)	Predefined Segmentation	Contain, Degrade, Exert	SC-32
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
		Tainting	Scrutinize, Reveal	SI-20
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt	SI-14(3)
	Hide Sensitive Information (CM1135)	Obfuscation	Delay, Degrade, Preempt	SC-28 (1)

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Data from Removable Media (T1025)	Minimize Local Functionality (CM1119)	Restriction	Preempt, Contain	SC-25
	Dynamically Disable or Suspend (CM1121)	Adaptive Management, Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Data Staged (T1074)	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources, Temporal Unpredictability	Preempt, Delay, Degrade, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
Email Collection (T1114)	Audit (M1047)	Sensor Fusion and Analysis	Detect	RA-5(10), AU-6(5)
	Encrypt Sensitive Information (M1041)	Obfuscation	Degrade, Exert	SC-8(4)
	Multi-factor Authentication (M1032)	Standard practice	Negate, Exert	IA-2(1), IA-2(2)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Tainting	Scrutinize, Reveal	SI-20
	Enhanced Authentication (CM1126)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13)
	Monitor Specific Servers (CM2034)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Command Line Use (CM2038)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Input Capture (T1056)	Trusted Path (CM1120) [22]	Predefined Segmentation	Contain	SC-11
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Dynamic Resource Awareness	Detect	SI-4(16)
	Present Deceptive Information (CM1101)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30(4)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Browser Session Hijacking (T1185)	User Account Management (M1018)	Attribute-Based Usage Restriction	Negate, Exert	AC-3(13)
	User Training (M1017)	Cyber hygiene	Negate, Exert, Detect	AT-3
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Dynamically Disable or Suspend (CM1121)	Non-Persistent Connectivity	Preempt, Delay	SC-15 (1)
		Dynamic Reconfiguration	Preempt, Delay	AC-2(8)

[22] Note that this mitigation applies to the capture of credentials, and not to keylogging or other input capture of more general data types. Thus, it mitigates only part of the Input Capture Technique.

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Adversary-in-the-Middle (T1557)	Disable or Remove Feature or Program (M1042)	Restriction	Negate, Exert	CM-7(2), SC-3(3)
		Cyber hygiene	Negate, Exert	SC-41
	Filter Network Traffic (M1037)	Restriction	Negate, Exert	SC-3(3)
	Limit Access to Resource Over Network (M1035)	Trust-Based Privilege Management	Negate, Exert	AC-6(3)
	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Contain, Degrade, Exert	SC-7, SC-7(21), SC-7(22)
	User Training (M1017)	Cyber hygiene	Detect	AT-3
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Active Deception (CM1131)	Dynamic Reconfiguration	Contain, Delay, Degrade, Exert	IR-4(2)
		Adaptive Management	Contain, Delay, Degrade, Exert	AC-4(3), IR-4(3)
		Misdirection	Contain, Divert, Delay, Degrade, Exert	SC-26
		Monitoring and Damage Assessment	Detect	SC-26
		Forensic and Behavioral Analysis	Detect, Scrutinize	SC-26
Screen Capture (T1113)	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Dynamic Resource Awareness	Detect	SI-4(16)
Video Capture (T1125)	Dynamically Disable or Suspend (CM1121)	Adaptive Management, Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
	Trusted Path (CM1120)	Predefined Segmentation	Contain, Delay, Exert	SC-11

ATT&CK Technique (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Application- or Utility-Specific Monitoring (CM2020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Logs (CM2005)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Dynamic Resource Awareness	Detect	SI-4(16)

3.12 Command and Control

The adversary's goal for the 16 Techniques under the Command and Control Tactic is to communicate with systems they have compromised. Command and Control is used to direct actions using Techniques under the Credential Access, Privilege Escalation, Discovery, Lateral Movement, Collection, Exfiltration, and Impact Tactics.

Table 12. Command and Control Tactic (TA0011): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Application Layer Protocol (T1071)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Preempt	SI-3, SI-4(4), SI-4(5)
	Isolate or Contain Selected Applications or Components (CM1133)	Predefined Segmentation, Dynamic Segmentation, and Isolation	Preempt, Negate, Contain, Exert	CM-7(6)
		Predefined Segmentation	Preempt, Negate, Contain, Exert	SC-7(21)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8), AC-4(12)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Communication Through Removable Media (T1092)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Operating System Configuration (M1028)	Restriction	Preempt	CM-7(2)
	Virtual Sandbox (CM1109)	Non-Persistent Services	Preempt, Shorten	SI-14
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Data Encoding (T1132)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4), SI-4(10)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Data Obfuscation (T1001)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4), SI-4(10)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Dynamic Resolution (T1568)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Restrict Web-Based Content (M1021)	Disinformation	Negate	SC-30(4)
		Monitoring and Damage Assessment,	Detect	SC-26

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Maintain Deception Environment (CM1102)	Forensic and Behavioral Analysis		
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
Encrypted Channel (T1573)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	SSL/TLS Inspection (M1020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(10), SI-4(25)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4), SI-4(10)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(10), SI-4(25)
Fallback Channels (T1008)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Maintain Deception Environment (CM1102)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Refresh Sessions or Connections (CM1146)	Non-Persistent Connectivity	Degrade, Exert	SI-14(3)
		Temporal Unpredictability	Degrade, Exert	SC-30(2)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Ingress Tool Transfer (T1105)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8), AC-4(12)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Multi-Stage Channels (T1104)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Refresh Sessions or Connections (CM1146)	Non-Persistent Connectivity	Degrade, Exert	SI-14(3)
		Temporal Unpredictability	Degrade, Exert	SC-30(2)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8), AC-4(12)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Non-Application Layer Protocol (T1095)	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	CM-7
	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Network Segmentation (M1030)	Predefined Segmentation	Negate, Degrade, Exert, Preempt	SC-7(3), SC-7(5), SI-4(4)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Non-Standard Port (T1571)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Network Segmentation (M1030)	Predefined Segmentation	Negate, Contain	AC-4(21), SC-7
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Protocol Tunneling (T1572)	Filter Network Traffic (M1037)	Standard practice	Preempt, Exert	AC-4(8)
	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11)
		Behavior Validation	Detect	IR-4(13)
		Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
Proxy (T1090)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	SI-3, SI-4(4), SI-4(5)
	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	SC-7(11), AC-4
	SSL/TLS Inspection (M1020)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(10), SI-4(25)
	Defend Enclave Boundaries (CM1151)	Predefined Segmentation	Negate, Exert	AC-4(21), SC-7(21), SC-7(22)
		Integrity Checks	Negate, Exert	AC-4(8)
		Provenance Tracking	Negate, Exert	AC-4(17)
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
		Predefined Segmentation	Negate, Exert	SC-46
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Remote Access Software (T1219)	Execution Prevention (M1038)	Standard practice	Negate, Degrade, Exert	CM-7(5)
	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	SC-7(11), AC-4
	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	AC-4, SI-3, SI-4(4), SI-4(5)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Detect	SC-26
	Lock Down Thin Nodes (CM1115)	Non-Persistent Services	Preempt	SC-25

ATT&CK Technique (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Non-Persistent Information	Preempt	SC-25, SC-34(1)
		Restriction	Preempt	SC-25
		Integrity Checks	Preempt	SC-34
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Traffic Signaling (T1205)	Filter Network Traffic (M1037)	Standard practice	Negate, Exert	AC-3(8), SC-7
	Passive Decoys (CM1104)	Misdirection	Deceive, Detect	SC-26
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Preempt, Exert	SC-10, SI-14(3)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
Web Service (T1102)	Network Intrusion Prevention (M1031)	Standard practice	Detect, Exert	AC-4, SI-3, SI-4(4), SI-4(5)
	Restrict Web-Based Content (M1021)	Standard practice	Negate, Degrade, Exert	SC-7(8)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Detect	SC-26
	Cross-Enterprise Behavior Analysis (CM2018)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)

3.13 Exfiltration

The adversary's goal for the nine Techniques under the Exfiltration Tactic is to steal information collected from enterprise systems by sending it to an adversary-chosen destination.

Table 13. Exfiltration Tactic (TA0010): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Exfiltration*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Automated Exfiltration (T1020)	Adversarial Simulation (CM1107)	Self-Challenge	Detect	CA-8, SC-7(10)
	Covert Signaling (CM1112)	Tainting	Detect, Scrutinize	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Inspect and Analyze Network Traffic (CM2002)	Monitoring and Damage Assessment	Detect	AU-6, SI-4(4), SI-4(18)
Data Transfer Size Limits (T1030)	Network Intrusion Prevention (M1031)	Standard practice	Negate, Detect	SI-4(4), SI-4(5), SI-4(11)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(18), IR-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)

ATT&CK Technique (*Exfiltration*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Exfiltration Over Alternative Protocol (T1048)	Filter Network Traffic (M1037)	Standard practice	Negate, Detect	AC-4, SI-4(4), SI-4(5)
	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect, Negate	SI-4(4)
	Network Segmentation (M1030)	Predefined Segmentation	Degrade, Delay, Exert	SC-7, SC-7(3), SC-7(5), SI-4(4)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(18), IR-4(13)
Exfiltration Over C2 Channel (T1041)	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment, Behavior Validation	Detect, Negate	SI-4(4)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt, Shorten, Reduce	SC-7(10), SC-10, SI-14(3)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)

ATT&CK Technique (*Exfiltration*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Analyze Network Traffic Content (CM2041)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
Exfiltration Over Other Network Medium (T1011)	Operating System Configuration (M1028)	Cyber hygiene	Negate, Preempt	CM-7(1), SC-7(15)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Minimize Duration of Connection or Session (CM1127)	Non-Persistent Connectivity	Delay, Preempt, Shorten, Reduce	SC-7(10), SC-10, SI-14(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Monitor Specific Files (CM2035)	Monitoring and Damage Assessment	Detect	AU-6
Exfiltration Over Physical Medium (T1052)	Disable or Remove Feature or Program (M1042)	Restriction	Exert, Preempt	CM-7(2)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Host Event Detection (CM2007)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Removable Device Usage Detection (CM2008)	Monitoring and Damage Assessment	Detect	CM-8(3)
Exfiltration Over Web Service (T1567)	Restrict Web-Based Content (M1021)	Standard practice	Negate	SC-7(8), CM-7(4), CM-7(5), SC-7(10)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26

ATT&CK Technique (*Exfiltration*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(18)
Scheduled Transfer (T1029)	Network Intrusion Prevention (M1031)	Monitoring and Damage Assessment	Detect	SI-4(4)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Modulate Information Flows (CM1153)	Design Diversity, Replication	Negate, Exert	AC-4(27), AC-4(30)
		Orchestration	Exert	AC-4(29)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6, IR-4(13)
	Analyze Outgoing Traffic Patterns (CM2042)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(18), IR-4(13)
Transfer Data to Cloud Account (T1537)	Filter Network Traffic (M1037)	Standard practice	Negate	AC-4(12), AC-4(17), AC-4(8)
	Password Policies (M1027)	Standard practice	Exert, Delay	IA-2(1), IA-2(8), IA-5
	User Account Management (M1018)	Standard practice	Degrade, Exert, Negate	AC-6, AC-2(2)
	Covert Signaling (CM1112)	Tainting	Detect, Reveal	SI-20
	Present Decoy Data (CM1113)	Disinformation, Misdirection	Deceive, Degrade	SC-30(4), SC-26
		Tainting	Detect, Scrutinize	SI-20
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23

ATT&CK Technique (*Exfiltration*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Cloud Account Monitoring (CM2016)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)

3.14 Impact

The adversary's goal for the 13 Techniques under the Impact Tactic is to have an adverse effect – other than data theft – on enterprise systems, and hence on enterprise operations.

Table 14. Impact Tactic (TA0040): Techniques, Mitigations, and Cyber Resiliency

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
Account Access Removal (T1531)	Use Alternate Communications (CM1140)	Path Diversity	Shorten, Reduce	AC-7(4), SC-47
	Dynamic Account Management (CM1117)	Dynamic Privileges, Dynamic Reconfiguration	Shorten, Reduce	AC-2(6)
		Dynamic Reconfiguration	Shorten, Reduce	AC-2(8)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Data Destruction (T1485)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Validate Data Quality (CM1130)	Integrity Checks	Detect	SA-9(7), SI-7(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Dynamically Reprovision (CM1139)	Adaptive Management	Shorten, Reduce	AC-4(3)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
	Reconstruct Compromised Assets (CM1141)	Information Diversity	Exert, Reduce	SI-22
		Fragmentation	Exert, Reduce	SI-23
		Replication	Exert, Reduce	SC-36
		Dynamic Reconfiguration	Reduce, Shorten	IR-4(9)
	Switch to Protected Hot Shadow (CM1142)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Contain, Exert	AC-4(2)
		Integrity Checks	Negate, Exert	AC-4(8)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
Data Encrypted for Impact (T1486)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9, CP-9(8)
		Replication	Shorten, Reduce	CP-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Fragment Information (CM1114)	Fragmentation	Delay, Exert	SI-23
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
		Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
	Perform Mission Damage Assessment (CM1122)	Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Dynamically Reprovision (CM1139)	Adaptive Management	Shorten, Reduce	AC-4(3)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
	Reconstruct Compromised Assets (CM1141)	Information Diversity	Exert, Reduce	SI-22
		Fragmentation	Exert, Reduce	SI-23
		Replication	Exert, Reduce	SC-36
		Dynamic Reconfiguration	Reduce, Shorten	IR-4(9)
	Switch to Protected Hot Shadow (CM1142)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Contain, Exert	AC-4(2)
		Integrity Checks	Negate, Exert	AC-4(8)
		Dynamic Reconfiguration,	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
Data Manipulation (T1565)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Exert	AC-4(2), AC-4(21), SC-7(29)
	Encrypt Sensitive Information (M1041)	Obfuscation	Degrade, Exert	SC-28 (1)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Degrade, Exert	AC-2(11)
	Remote Data Storage (M1029)	Standard practice	Exert, Reduce	CP-9
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Negate, Contain	SC-26

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
	Trusted Path (CM1120)	Predefined Segmentation	Negate, Contain	SC-11
	Validate Data Properties (CM1137)	Integrity Checks	Delay, Degrade, Exert	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Validate Output Data (CM1155)	Integrity Checks	Detect, Reduce	SI-15
	Analyze File Contents (CM2006)	Forensic and Behavioral Analysis	Detect	SR-10
Defacement (T1491)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Obfuscation, Protected Backup and Restore, Integrity Checks	Exert	CP-9(8)
		Replication	Shorten, Reduce	CP-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)
	Validate Data Quality (CM1130)	Integrity Checks	Detect	SA-9(7), SI-7(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Disk Wipe (T1561)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Dynamic Data Location (CM1116)	Functional Relocation of Cyber Resources	Preempt	SC-30(3)
		Temporal Unpredictability	Preempt, Exert	SC-30(3)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
	Host Event Detection (CM2007)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternative Data Sources (CM1138)	Information Diversity	Reduce, Shorten	SI-22
		Dynamic Reconfiguration	Contain, Reduce, Shorten	IR-4(2)
	Dynamically Reprovision (CM1139)	Adaptive Management	Shorten, Reduce	AC-4(3)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
	Reconstruct Compromised Assets (CM1141)	Protected Backup and Restore	Exert, Reduce	CP-9
		Information Diversity	Exert, Reduce	SI-22
		Fragmentation	Exert, Reduce	SI-23
		Replication, Distributed Functionality	Exert, Reduce	SC-36
		Dynamic Reconfiguration	Reduce, Shorten	IR-4(9)
	Switch to Protected Hot Shadow (CM1142)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Contain, Exert	AC-4(2)
		Integrity Checks	Negate, Exert	AC-4(8)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce	SC-29
		Design Diversity	Shorten, Reduce	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Defend Failover and Recovery (CM1145)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
Endpoint Denial of Service (T1499)	Filter Network Traffic (M1037)	Adaptive Management	Degrade, Reduce	AC-4(3), SC-7(11)
	Maintain Deception Environment (CM1102)	Misdirection	Deceive, Divert	SC-26
		Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30(4)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Resource Allocation, Adaptive Management	Degrade, Reduce	AU-5(3), IR-4(2), SC-7(20)
	Partition Host (CM1118)	Predefined Segmentation	Degrade, Reduce	SC-2, SC-32
	Defend Against DoS (CM1147)	Dynamic Resource Allocation, Surplus Capacity	Shorten, Reduce	SC-5(2)
		Monitoring and Damage Assessment	Detect	SC-5(3)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
Firmware Corruption (T1495)	Boot Integrity (M1046)	Integrity Checks	Detect	SI-7, SI-7(9), SI-7(10)
	Privileged Account Management (M1026)	Trust-Based Privilege Management	Negate, Exert	AC-6(5), CM-5(5)
	Update Software (M1051)	Cyber hygiene	Preempt, Exert	SI-2
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce	SC-29
		Design Diversity	Shorten, Reduce	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Activate Alternate (CM1144)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Specialization	Shorten, Reduce, Exert	SA-20, SA-23
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Defend Failover and Recovery (CM1145)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
	Hardware-Based Protection of Firmware (CM1154)	Integrity Checks	Negate, Preempt	SC-51
Inhibit System Recovery (T1490)	Data Backup (M1053)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	CP-9(6)
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	CP-9(8)
	Operating System Configuration (M1028)	Standard practice	Negate	CM-5, CM-6, CM-7, CM-7(2)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Monitor the File System (CM2033)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration,	Shorten, Reduce	CP-2(5)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
		Adaptive Management, Orchestration		
	Activate Alternate (CM1144)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Specialization	Shorten, Reduce, Exert	SA-20, SA-23
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)
	Defend Failover and Recovery (CM1145)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
Network Denial of Service (T1498)	Filter Network Traffic (M1037)	Adaptive Management	Degrade, Reduce	AC-4(3)
		Provenance Tracking	Degrade, Reduce	SC-7(11)
	Dynamically Restrict Traffic or Isolate Resources (CM1108)	Dynamic Resource Allocation, Adaptive Management	Degrade, Reduce	AU-5(3), IR-4(2), SC-7(20)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13)
	Switch to Alternate System or Component (CM1143)	Replication	Degrade, Reduce	SC-22

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
	Defend Against DoS (CM1147)	Dynamic Resource Allocation, Surplus Capacity	Shorten, Reduce	SC-5(2)
		Monitoring and Damage Assessment	Detect	SC-5(3)
Resource Hijacking (T1496)	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Monitor Network Usage (CM2047)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)
	Dynamically Reprovision (CM1139)	Dynamic Reconfiguration	Shorten	IR-4(2)
		Dynamic Segmentation and Isolation	Reduce	SC-7(20)
	Dynamically Disable or Suspend (CM1121)	Adaptive Management	Preempt, Delay	SC-15 (1)
		Dynamic Reconfiguration	Preempt, Delay	AC-2(8)
Service Stop (T1489)	Network Segmentation (M1030)	Predefined Segmentation	Contain, Shorten, Reduce	IR-4(14), SC-3, SC-7(29)
	Restrict File and Directory Permissions (M1022)	Standard practice	Negate, Exert	AC-2(11)
	Restrict Registry Permissions (M1024)	Standard practice	Negate, Exert	AC-6, CM-6
	User Account Management (M1018)	Standard practice	Negate, Exert	AC-6
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13)
	Monitor Platform Status (CM2044)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Process Monitoring (CM2015)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)

ATT&CK Technique (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Cyber Resiliency Control(s) if Any
System Shutdown/Reboot (T1529)	Passive Decoys (CM1104)	Misdirection	Deceive, Divert, Detect	SC-26
	Perform Mission Damage Assessment (CM1122)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Alternate System or Component (CM1143)	Architectural Diversity	Shorten, Reduce, Exert	SC-29
		Design Diversity	Shorten, Reduce, Exert	SA-17(9)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)

4 Mitigations and Candidate Mitigations for ATT&CK for Enterprise

As noted in Section 1.4 and as discussed in Section 2, neither a cyber resiliency implementation approach nor a security control per se has a potential effect on an adversary TTP or other threat event – it is the way cyber resiliency approaches and controls are *implemented and used* that can produce an effect. In the Cyber Resiliency Effects Analysis for ATT&CK, descriptions of possible uses of cyber resiliency approaches and controls are captured via ATT&CK Mitigations or via candidate mitigations (CMs). As noted in Section 2, a Mitigation or CM is given an identifier and a name (a short phrase); these appear in the mapping tables in Section 3. This section provides further information on the Mitigations and CMs.

4.1 Mitigations

As discussed in Section 2.1, the ATT&CK knowledge base identifies 42 enterprise mitigations. These are listed in Table 15. For brevity, neither the short description nor the Technique-specific descriptions are listed; for more details, https://attack.mitre.org/mitigations/enterprise/ provides the authoritative source. The Technique-specific uses are characterized as cyber hygiene, standard practice, or cyber resiliency. For those uses which apply cyber resiliency, the corresponding cyber resiliency approaches and controls are identified. (When a cyber resiliency control is not used to apply an associated cyber resiliency approach, the use is identified as standard practice. This situation arises when the Mitigation description is not specific enough to determine how an approach applies.) It should be noted that the number of Techniques to which a Mitigation applies varies widely. For example, M1036, Account Use Policies, applies only to T1110, Brute Force (and its Sub-Techniques), while M1047, Audit, applies directly to 18 different Techniques (and indirectly to more, by its use for one or more Sub-Techniques).

Table 15. Mitigations and Their Cyber Resiliency Applicability

ID	Name	Controls	Discussion
M1013	Application Developer Guidance	AT-3, IA-5(7), SA-8	All uses are standard practice.
M1015	Active Directory Configuration	AC-2, AC-2(1), AC-6(5), AC-6(7), IA-5(13), SC-7(20), SC-7(30)	All uses are standard practice.
M1016	Vulnerability Scanning	RA-5, SA-9(7), SA-11(4), SI-4(22), SR-4(3), SR-4(4)	Uses of RA-5 in T1190 and T1210 are cyber hygiene. For T1195, SA-9(7) and SA-11(4) apply Integrity Checks, while SR-4(3) and SR-4(4) apply Provenance Tracking.
M1017	User Training	AT-2, AT-2(1), AT-2(3), AT-2(4), AT-2(5), AT-3, PL-2(1)	Many uses are cyber hygiene, using AT-2. Use for T1598 applies a combination of standard practice, using PL-2(1), and Dynamic Threat Awareness, using AT-2(5). Use for T1072 is standard practice and applies AT-3. Use for T1213 is standard practice and applies AT-2 and AT-2(4). Use for T1566 applies Dynamic Threat Awareness, via AT-2(1), AT-2(3), and AT-2(5).

ID	Name	Controls	Discussion
M1018	User Account Management	AC-2, AC-2(3), AC-2(6), AC-2(8), AC-3(7), AC-3(13), AC-4(12), AC-4(21), AC-4(17), AC-4(8), AC-6, AC-6(1), AC-6(5), AC-6(7), AC-12, AC-17	Most uses are standard practice. However, some uses involve analysis to determine how best to manage user accounts consistent with the principle of least privilege. These include applications of Consistency Analysis and/or Trust-Based Privilege Management using AC-6 or AC-6(7), and applications of Attribute-Based Usage Restriction using AC-3(13) or AC-6(1).
M1019	Threat Intelligence Program	PM-16, RA-3(3)	All uses apply Dynamic Threat Awareness via PM-16 and RA-3(3).
M1020	SSL/TLS Inspection	IR-4(13), SI-4(10), SI-4(25)	All uses apply Monitoring and Damage Assessment via IR-4(13), SI-4(10), and SI-4(25); the SI-4 control enhancements enable examination of SSL and TLS traffic.
M1021	Restrict Web-Based Content	AC-4(8), AC-6(4), AC-6(7), CM-7(5), SC-18, SC-7, SC-7(8), SC-7(10), SC-30(4)	Most uses are standard practice. Some uses apply Trust-Based Privilege Management, using AC-6(4) or AC-6(7). Some uses apply Integrity Checks, using AC-4(8). T1568 applies Disinformation, using SC-30(4).
M1022	Restrict File and Directory Permissions	AC-2(7), AC-2(11), AC-3(11), AC-3(15), AC-24, AU-9(6), SC-2, SC-34	Descriptions range from high-level (e.g., “enforce least privilege”) to technology-specific (e.g., strictly editing the sudoesrs file). Many uses are standard practice and use combinations of AC-2(7), AC-2(11), AC-3(11), AC-3(15), AC-24, and SC-2, depending on whether privileged accounts are considered (AC-2(7), SC-2). Some uses apply Integrity Checks, using SC-34. Use for T1562 applies Attribute-Based Usage Restriction, using AC-6(1). Use for T1070 applies Trust-Based Privilege Management, using AU-9(6).
M1024	Restrict Registry Permissions	AC-6, CM-6	All uses are standard practice.
M1025	Privileged Process Integrity	CM-7, CM-7(2), SI-7(3), SI-7(6)	Some uses are standard practice. Use for T1003 applies Restriction and CM-7(2).
M1026	Privileged Account Management	AC-2(7), AC-6, AC-6(2), AC-6(5), AC-6(7), AC-6(8), AC-17(4), CM-5(5)	Some uses are cyber hygiene; many are standard practice. However, uses involve analysis to determine how best to manage privileged accounts consistent with the principle of least privilege. These apply Trust-Based Privilege Management, using some combination of AC-6, AC-6(2), AC-6(5), AC-6(7), or CM-5(5), and/or Attribute-Based Usage Restriction using AC-6(8).
M1027	Password Policies	IA-2(1), IA-2(8), IA-5	All uses are either cyber hygiene or standard practice, using IA-5. T1537 also uses IA-2(1) and IA-2(8) as standard practice.

ID	Name	Controls	Discussion
M1028	Operating System Configuration	AC-6(8), CM-5, CM-6, CM-7, CM-7(2)	Most uses are cyber hygiene or standard practice, using one or more of CM-5, CM-6, CM-7. Some uses apply Restriction, using CM-7(2); some also apply Attribute-Based Usage Restriction, using AC-6(8).
M1029	Remote Data Storage	AU-9(2), AU-9(6), AC-6(4), CP-9, SC-7(21), SI-4(2)	Some uses are standard practice, using CP-9 but not necessarily applying cyber resiliency. For audit data, AU-9(2) is used to apply Predefined Segmentation, and AU-9(6) to apply Integrity Checks. Other uses apply Predefined Segmentation and Trust-Based Privilege Management, using AC-6(4), Predefined Segmentation using SC-7(21), or Non-Persistent Information using SI-4(2).
M1030	Network Segmentation	AC-4, AC-4(2), AC-4(21), AU-9(2), IR-4(12), SC-3, SC-7, SC-7(21), SC-7(22), SC-7(29)	Most uses of Network Segmentation are applications of Predefined Segmentation, with considerable variation in the controls used. However, some are more appropriately considered to be standard practice. Use for T1489 (AU-9(2), IR-4(12), and SC-7(29)) applies Predefined Segmentation to the intrusion detection, analysis, and response system.
M1031	Network Intrusion Prevention	PM-16(1), SI-3, SI-4, SI-4(4), SI-4(5)	Almost all uses of M1031 are standard practice, relying on signatures (SI-4 and its enhancements). Uses that are not solely reliant on signatures include T1557, which applies Monitoring and Damage Assessment, Behavior Validation using SI-4(4), and T1221, which applies Predefined Segmentation using SC-44.
M1032	Multi-factor Authentication	IA-2(1), IA-2(2), IA-2(6)	All uses are standard practice. Note that the effectiveness of this Mitigation can be enhanced by including IA-2(6), which applies Path Diversity and Calibrated Defense-in-Depth.
M1033	Limit Software Installation	CM-5(6), CM-11(2), CM-11(3)	All uses are standard practice.
M1034	Limit Hardware Installation	CM-8(3), MP-6, MP-7, SC-41	Most uses apply cyber hygiene. Use for T1200 applies Restriction, using CM-8(3).
M1035	Limit Access to Resource Over Network	AC-3, AC-6, AC-6(3), AC-6(10), AC-17, CM-2, CM-2(2), CM-7(1)	Most uses are standard practice, except T1557, which applies Trust-Based Privilege Management, using AC-6(3) and T1200, using AC-6(3) and AC-6(10).
M1036	Account Use Policies	AC-2(11), AC-7	All uses are standard practice.
M1037	Filter Network Traffic	AC-3(8), AC-4, AC-4(3), IR-4(2), SC-7, SC-7(11), SI-4(4), SI-10(5)	Most uses are standard practice, using AC-4 and SC-7. (While SC-7 is a cyber resiliency control, its use in this context is not specifically cyber resiliency.) However, some uses apply one or more of Restriction, Provenance Tracking, Adaptive Management, Dynamic Reconfiguration, and Monitoring and Damage Assessment.

ID	Name	Controls	Discussion
M1038	Execution Prevention	CM-2, CM-3, CM-5, CM-6, CM-7, CM-7(4), CM-7(5), CM-8, SC-34, SI-14(1)	Most uses are standard practice, using application control tools (and some combination of CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, and SI-3). Some uses apply Purposing, using CM-7(4) or CM-7(5) or Non-Persistent Services, using SC-34 or SI-14(1).
M1039	Environment Variable Permissions	N/A	This Mitigation is used only for Sub-Techniques. All uses are Standard practice.
M1040	Behavior Prevention on Endpoint	CM-7(2)	Most uses are standard practice. Use for T1559 applies Restriction.
M1041	Encrypt Sensitive Information	AU-9(3), IA-2(6), SC-8(1), SC-8(4), SC-28(1)	All uses apply Obfuscation, using or more of SC-8(1), SC-8(4), SC-28 (1), IA-2(6), and (solely for audit information) AU-9(3).
M1042	Disable or Remove Feature or Program	CM-7, CM-7(2), SC-3(3), SC-41	Some uses are cyber hygiene, CM-7, and in some cases SC-41. Multiple uses apply Restriction via CM-7(2); some also use SC-3(3).
M1043	Credential Access Protection	IA-5, IA-5(7), SC-28 (1), SC-29 (1)	All uses are standard practice.
M1044	Restrict Library Loading	CM-7, CM-7(4), CM-7(5)	Use for T1574 applies Purposing, using CM-7(5). All other uses are for Sub-Techniques and were not analyzed.
M1045	Code Signing	CM-7(5), SI-7(15), SR-4(3)	Uses apply Provenance Tracking and use SI-7(15). SR-4(3) applies when the vendor is involved.
M1046	Boot Integrity	SI-6, SI-7, SI-7(1), SI-7(6), SI-7(9), SI-7(10)	This mitigation uses Integrity Checks in multiple ways.
M1047	Audit	AC-6(7), AU-6, AU-6(5), AU-10(2), CA-7(5), RA-5, RA-5(10), SI-7, SI-7(1), SI-14(2)	The general description of M1047 (Audit) is cyber hygiene, applying AU-6 and/or RA-5: “Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.” However, many of the uses involve analysis beyond the routine practices of cyber hygiene, making them standard practice. And some of the uses of M1047 go well beyond the “audits or scans” in the general description, applying a range of cyber resiliency implementation approaches.
M1048	Application Isolation and Sandboxing	AC-4(21), AC-6(4), SC-18 (5), SC-39, CM-7(2), CM-7(6)	The use of M1048 is standard practice for T1559, Inter-Process Communication. Most other uses apply Predefined Segmentation – selected from AC-4(21), AC-6(4), SC-18 (5) [23], SC-39, and CM-7(6), depending on the ATT&CK Technique. For T1610, the Mitigation uses Restriction – CM-7(2).
M1049	Antivirus/Antimalware	AC-4, SI-3, AT-2, AT-3, SC-44	All uses except T1221 are cyber hygiene, applying AC-4 and SI-3. Phishing also uses AT-2 and AT-3. The use of detonation chambers for T1221 relies on Predefined Segmentation, using SC-44.

[23] SC-18 (5) applies only for browser attacks, i.e., for T1189 and T1203.

ID	Name	Controls	Discussion
M1050	Exploit Protection	SI-16, AC-4, AC-4(8), IR-4(13), SI-4, SI-7, SC-7(17)	Uses of security applications that look for behavior used during exploitation apply Behavior Validation and use IR-4(13). Control flow integrity checking applies Integrity Checking and uses AC-4(8). Web application firewalls, allowlisting, and basic use of the Microsoft Enhanced Mitigation Experience Toolkit (EMET) or Windows Defender Exploit Guard (WDEG) are standard practice. Some uses of WDEG apply Restriction and Synthetic Diversity, using SI-16.
M1051	Update Software	MA-3(6), RA-5, SI-2	All uses are cyber hygiene and apply SI-2. Patch management involves MA-3(6) and may also involve RA-5.
M1052	User Account Control	AC-2(6), AC-6(8), AC-6(9), CM-11(2), MA-3(6), RA-5, SI-2	All uses are standard practice.
M1053	Data Backup	CP-9, CP-9(6)	All uses rely on Protected Backup and Restore (CP-9) and Replication (CP-9(6)). Uses for T1490 and T1491 also apply Protected Backup and Restore, Obfuscation, and Integrity Checks, using CP-9(8).
M1054	Software Configuration	AC-3(13), AC-4(17), CM-7(1)	Some uses (T1137, T1602) are standard practice and apply CM-7(1). Use for T1553 applies Provenance Tracking, using AC-4(17) [24]. Use for T1535 applies Attribute-Based Usage Restriction, using AC-3(13). Use for T1539 applies Non-Persistent Information, using SI-14(2) and SI-21.
M1055	Do Not Mitigate	N/A	Standard practice for T1480; not used for any other Technique or Sub-Technique.
M1056	Pre-Compromise	SC-38	All uses are standard practice, using SC-38, Operations Security.

4.2 Candidate Mitigations for Detection

As discussed in Section 2.2, each ATT&CK Technique includes a narrative discussion of detection methods. Some of those detection methods are cyber hygiene – they can be performed routinely using basic capabilities expected of any enterprise system [17]. Others are standard practice – non-routine uses of such capabilities, or using capabilities which, while beyond the basic, are expected to be provided by enterprise systems based on good risk management practice [25]. Finally, many of the detection methods discussed in ATT&CK apply cyber resiliency implementation approaches. These approaches primarily fall under the Analytic Monitoring cyber resiliency technique (Monitoring and Damage Assessment, Sensor Fusion, and Analysis, and Forensic and Behavioral Analysis); however, some fall under Substantiated

[24] The mitigation cites HTTP Public Key Pinning; while that mechanism has been deprecated in favor of Certificate Transparency (CT), CT is also an application of Provenance Tracking.

[25] "Standard cybersecurity" can be identified with the RMF baselines, Cybersecurity Maturity Model Certification (CMMC) level 3, the NIST Cybersecurity Framework (NCF, [8], and the Center for Internet Security (CIS) Controls [26], with the understanding that the controls, capabilities, and practices defined by these standards are intended to be tailored to reflect the organizational, operational, technical, and risk environments in which they are applied.

Integrity (Integrity Checks, Behavior Validation). CMs for detection are presented in Table 16. Technique-specific descriptions are given in Appendix C, Table TBD.

Table 16. Candidate Mitigations, Cyber Resiliency Controls, and Approaches for Detection

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2002	**Inspect and Analyze Network Traffic**	AC-2(12), AU-6, IR-4(13), SI-4(2), SI-4(4), SI-4(10), SI-4(18)	Analyze network traffic for unusual data flows. Traffic inspection and analysis can be performed at the enterprise boundary, at internal boundaries between enclaves, or within enclaves.	Monitoring and Damage Assessment
CM2003	**Endpoint Behavior Analysis**	AC-2(12)	Analyze the behavior of endpoint (i.e., end-user, client) systems for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2004	**Monitor Logs**	AU-6, IR-4(13), SI-4(2), SI-4(11)	Monitor system and application logs for anomalous or suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2005	**Analyze Logs**	AC-2(12), SI-4(13), SI-4(16)	Analyze logs (individually or with some correlation across logs) for anomalous or suspicious patterns of behavior.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Dynamic Resource Analysis, Behavior Validation
CM2006	**Analyze File Contents**	SR-10	Analyze contents of specific files or types of files for suspicious contents.	Forensic and Behavioral Analysis
CM2007	**Host Event Detection**	CM-8(3), IR-4(13), SI-4(2)	Detect anomalous or unauthorized events on hosts (e.g., servers, endpoint systems).	Monitoring and Damage Assessment, Behavior Validation
CM2008	**Removable Device Usage Detection**	CM-8(3)	Detect anomalous or unauthorized events involving use of removable devices.	Monitoring and Damage Assessment
CM2009	**Software Integrity Check**	SI-7, SI-7(1), SI-7(6), CM-14, SR-4(3)	Perform integrity checks (e.g., using checksums, hashes, or digital signatures) on software, software certificates, or metadata.	Integrity Checks, Provenance Tracking
CM2010	**Software Stress Testing**	SR-6(1)	Perform software stress testing (e.g., using out-of-bounds input values) prior to installation.	Self-Challenge
CM2011	**Physical Inspection**	SR-9, SR-10	Perform physical inspection of hardware components for indicators of tampering.	Integrity Checks

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2012	**Monitor Trusted Parties**	PM-16, PM-30(1), SI-4(17)	Monitor the behavior and status (e.g., change in ownership) of second or third parties.	Dynamic Resource Awareness, Dynamic Threat Awareness, Behavior Validation
CM2013	**Cross Enterprise Account Usage Analysis**	AU-6(3), SI-4(16)	Analyze user account usage across the enterprise for anomalies or suspicious behavior.	Sensor Fusion and Analysis
CM2014	**Process Analysis**	IR-4(13), SI-4(2)	Analyze process attributes or behavior for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment
CM2015	**Process Monitoring**	AU-6, IR-4(13), SI-4(2)	Monitor the behavior of processes for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
CM2016	**Cloud Account Monitoring**	AC-2(12)	Monitor activity associated with cloud accounts for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
CM2017	**Privileged Account Monitoring**	AU-6(8)	Monitor and analyze activity associated with privileged accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment
CM2018	**Cross-Enterprise Behavior Analysis**	AU-6(3), AU-6(5)	Correlate and analyze behavior of multiple systems.	Sensor Fusion and Analysis
CM2019	**Endpoint Scrutiny**	IR-4(12)	Scrutinize the contents and behavior patterns of an endpoint system.	Forensic and Behavioral Analysis
CM2020	**Application- or Utility-Specific Monitoring**	IR-4(13), SI-4(2)	Monitor and analyze events in the context of a specific application or utility.	Monitoring and Damage Assessment, Behavior Validation
CM2021	**Account Monitoring**	AC-2(12), IR-4(13), SI-4(2)	Monitor and analyze activity associated with user accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
CM2022	**Host-Local Event Correlation**	IR-4(13), SI-4(16)	Correlate and analyze events occurring on a single host.	Sensor Fusion and Analysis, Monitoring and Damage Assessment

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2023	**Centralize and Analyze Instance Logging**	AU-6(5), IR-4(4)	Centralize instance logging in a cloud or container environment and analyze.	Sensor Fusion and Analysis
CM2029	**Monitor Script Execution**	IR-4(13), SI-4(2), SI-4(13)	Monitor for the execution of scripts which are unknown or used in suspicious ways.	Monitoring and Damage Assessment
CM2033	**Monitor the File System**	IR-4(13), SI-4(2), SI-4(24)	Monitor the file system to identify the unexpected presence and atypical use of files of specific types, or atypical patterns of access.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Behavior Validation
CM2034	**Monitor Specific Servers**	IR-4(13), SI-4(2)	Monitor specific servers for anomalous or suspicious uses or access attempts.	Monitoring and Damage Assessment
CM2035	**Monitor Specific Files**	AU-6	Monitor the use of specific files or directories for anomalous or suspicious uses or access attempts.	Behavior Validation, Monitoring and Damage Assessment
CM2038	**Monitor Command Line Use**	IR-4(13), SI-4(2), SI-4(4), SI-4(13)	Monitor use of the command line interface for use of common utilities (part of the system or installed by the adversary), looking for suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2040	**Monitor Use of Libraries and Utilities**	IR-4(13), SI-4(2), SI-4(4), SI-4(13)	Monitor the use of libraries and utilities which are commonly used to support adversary actions.	Monitoring and Damage Assessment
CM2041	**Analyze Network Traffic Content**	IR-4(13), SI-4(10), SI-4(25)	Analyze the contents of network traffic.	Monitoring and Damage Assessment, Behavior Validation
CM2042	**Analyze Outgoing Traffic Patterns**	IR-4(13), SI-4(18)	Analyze outgoing traffic for patterns of behavior which could indicate adversary communications.	Monitoring and Damage Assessment, Behavior Validation
CM2043	**Monitor External Sources**	AU-13, AU-13 (3), PM-16, RA-5(4), RA-10	Monitor and analyze external information sources for indicators of adversary activities, especially those targeting the organization.	Monitoring and Damage Assessment, Dynamic Threat Awareness
CM2044	**Monitor Platform Status**	IR-4(13), SI-4(2)	Monitor the status of platforms (e.g., user endpoints, servers, network devices).	Monitoring and Damage Assessment

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2047	**Monitor Network Usage**	IR-4(13), SI-4(11), SI-4(13)	Monitor network usage for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2048	**Hunt for Malicious Processes**	IR-5	Hunt for applications or processes which display specific malicious or suspect behaviors.	Forensic and Behavioral Analysis

4.3 Candidate Mitigations with Other Direct Potential Effects

A variety of candidate mitigations – not derived from the curated data sets which inform ATT&CK – have been defined to describe how cyber resiliency approaches and controls can be used to have effects other than purely detection on different Techniques. These are presented in Table 17. Technique-specific descriptions are given in Appendix C. Note that a Technique-specific application of a candidate mitigation may apply only a subset of the identified controls.

Table 17. Candidate Mitigations with Direct Potential Effects Other Than Detection

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1101	**Present Deceptive Information**	SC-30(4), SI-20	Present deceptive information about systems, data, processes, and users. Monitor uses or search for presence of that information.	Disinformation, Tainting
CM1102	**Maintain Deception Environment**	SC-7(21), SC-26, SC-30(4)	Maintain a distinct subsystem or a set of components specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Disinformation, Predefined Segmentation
CM1103	**Detonation Chamber**	SC-44	Use a dynamic execution environment to handle potentially harmful incoming data.	Forensic and Behavioral Analysis, Misdirection, Predefined Segmentation
CM1104	**Passive Decoys**	SC-26, SC-29	Use factitious systems or resources to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities.	Misdirection, Architectural Diversity
CM1105	**Component Provenance Validation**	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4), SR-11(3)	Validate the provenance of system components.	Integrity Checks, Provenance Tracking

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1106	**Supply Chain Diversity**	PL-8(2), SR-3(1), SR-3(2)	Provide multiple distinct supply chains for system components.	Supply Chain Diversity
CM1107	**Adversarial Simulation**	AT-2(1), AT-3(3), CA-8, CA-8(1), CA-8(2), SC-7(10), SI-19(8)	Simulate adversary activities to test the effectiveness of system protections and detection mechanisms.	Self-Challenge
CM1108	**Dynamically Restrict Traffic or Isolate Resources**	AU-5(3), IR-4(2), SC-7(20)	Dynamically reconfigure networking to restrict network traffic or isolate resources.	Dynamic Resource Allocation, Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation, and Isolation
CM1109	**Virtual Sandbox**[26]	SC-7(20), SI-14	Use virtualization to create a controlled execution environment, which is expunged after execution terminates.	Non-Persistent Services, Dynamic Segmentation, and Isolation
CM1110	**Application- or Utility-Specific Data Removal**	IR-4(2), IR-4(13), SI-4(2), SI-7(1), SI-7(7)	Analyze files and data structures specific to an application or utility for anomalies and delete.	Monitoring and Damage Assessment, Integrity Checks, Dynamic Reconfiguration
CM1111	**Execution Restriction**	AC-3(12), AC-3(13)	Restrict the sources of executables or the locations in which execution can occur.	Attribute-Based Usage Restriction
CM1112	**Covert Signaling**	SI-20	Use hidden logic to enable exfiltrated data to signal its location or embed hidden data which can be the subject of a search.	Tainting
CM1113	**Present Decoy Data**	SC-26, SC-30(4), SI-20	Present plausible but factitious data assets to attract the adversary. Monitor uses of those assets or search for presence of decoy information.	Disinformation, Misdirection, Tainting
CM1114	**Fragment Information**	SI-23	Fragment information and distribute across multiple locations.	Fragmentation

[26] This could be subsumed into M1048, Application Isolation and Sandboxing. However, ATT&CK does not identify M1048 for T1091.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1115	**Lock Down Thin Nodes**	SC-25, SC-34, SC-34(1)	Minimize local functionality and disallow writable storage.	Non-Persistent Services, Non-Persistent Information, Restriction, Integrity Checks
CM1116	**Dynamic Data Location**	SC-30(3)	Dynamically move data resources.	Functional Relocation of Cyber Resources, Temporal Unpredictability
CM1117	**Dynamic Account Management**	AC-2(6), AC-2(8)	Dynamically update an account's authorizations or privileges.	Dynamic Privileges, Dynamic Reconfiguration
CM1118	**Partition Host**	SC-2, SC-2(1), SC-32, SC-32 (1)	Partition a host (e.g., server, endpoint system) into separate logical domains.	Predefined Segmentation
CM1119	**Minimize Local Functionality**	CM-7(2), SC-25	Construct or configure systems or applications to minimize their inherent functionality.	Restriction
CM1120	**Trusted Path**	SC-11	Provide an isolated communications path between the user and security functions.	Predefined Segmentation
CM1121	**Dynamically Disable or Suspend**	AC-2(8), SC-15 (1)	Terminate processes or disable capabilities upon triggering conditions.	Adaptive Management, Dynamic Reconfiguration
CM1122	**Perform Mission Damage Assessment**	CP-2(8), RA-9, SI-4(1), SI-7, SI-7(1)	Determine the mission consequences of adversary activities (e.g., which resources can be relied on; how quickly, how completely, and with what confidence mission-essential services, data, and communications can be restored from backups or alternative resources).	Sensor Fusion and Analysis, Mission Dependency and Status Visualization, Integrity Checks
CM1123	**Active Decoys**	SC-26, SC-35, SC-44	Use one or more factitious systems or other resources to identify malicious sites, interact with the adversary, actively probe for malicious code, and observe adversary TTPs [27].	Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation, and Isolation

[27] CM1123 supports M1038, Execution Prevention.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1124	**Minimize Data Retention or Lifespan**	SC-23(3), SI-14(2), SI-21	Minimize the lifespan or retention of data, and ensure that deleted data cannot be retrieved.	Non-Persistent Information, Temporal Unpredictability
CM1125	**Authenticate Devices**	IA-3(1)	Authenticate a device before establishing a connection to it.	Obfuscation, Integrity Checks
CM1126	**Enhanced Authentication**	IA-2(13), IA-10, CP-13, SC-47	Use situation-specific, risk-adaptive, or out-of-band authentication.	Adaptive Management, Calibrated Defense-in-Depth, Architectural Diversity, Design Diversity, Path Diversity, Dynamic Privileges
CM1127	**Minimize Duration of Connection or Session**	AC-12, SC-7(10), SC-10, SI-14(3)	Minimize the time period for which a connection remains open or a session remains active, requiring reauthorization to reestablish connectivity.	Non-Persistent Services, Non-Persistent Connectivity
CM1128	**Design Diversity**	SA-17(9)	Use multiple designs to implement the same functionality.	Design Diversity
CM1129	**Check Policy Consistency**	CA-7(5)	Ensure that policies are applied consistently across systems, applications, and services.	Consistency Analysis
CM1130	**Validate Data Quality**	SA-9(7), SI-7(1)	Validate data quality (e.g., integrity, consistency, correctness).	Integrity Checks
CM1131	**Active Deception**	AC-4(3), IR-4(2), IR-4(3), SC-7(21), SC-26, SC-30(4), SI-3(10)	Maintain an internal deception environment, divert suspicious traffic to that environment, interact with and analyze behavior to determine whether it is malicious and to investigate adversary TTPs.	Dynamic Reconfiguration, Adaptive Management, Misdirection, Monitoring and Damage Assessment, Forensic and Behavioral Analysis
CM1132	**Quarantine or Delete Suspicious Files**	SR-4(3), CM-7(6), SI-14, SI-14(2)	Move and make inaccessible, or delete, suspicious files.	Provenance Tracking, Dynamic Segmentation and Isolation, Non-Persistent Information
CM1133	**Isolate or Contain Selected Applications or Components**	CM-7(6), SC-7(21)	Isolate or contain (e.g., using internal firewalls or virtual environments) selected applications or components, based on risk profiles.	Trust-Based Privilege Management, Predefined Segmentation, Dynamic Segmentation, and Isolation

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1134	**Refresh Selected Applications or Components**	SI-14(1), SI-14(2)	Refresh software, firmware, or data from a trusted source.	Non-Persistent Services, Non-Persistent Information
CM1135	**Hide Sensitive Information**	SC-28 (1), SI-19(4)	Conceal (e.g., via encryption or data hiding) or remove sensitive information (including metadata).	Obfuscation
CM1136	**Identify External Malware**	SC-35	Identify and redirect malware found on external systems.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation, and Isolation
CM1137	**Validate Data Properties**	PL-8(1), SC-16(1), SC-16(3), SI-7, SI-7(1)	Validate data properties (including binaries, metadata, and cryptographic bindings) to defend against modification or fabrication.	Integrity Checks, Calibrated Defense-in-Depth
CM1138	**Switch to Alternative Data Sources**	SI-22, IR-4(2)	Switch to one or more alternative data sources to ensure adequate data quality or rebuild destroyed data.	Information Diversity, Dynamic Reconfiguration
CM1139	**Dynamically Reprovision**	AC-4(3), IR-4(2), SC-7(20)	Reconfigure or reallocate resources to route around damage.	Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation, and Isolation
CM1140	**Use Alternate Communications**	AC-7(4), SC-47	Use alternative communications paths.	Path Diversity
CM1141	**Reconstruct Compromised Assets**	SC-36, SI-22, SI-23, IR-4(9), CP-9	Reconstruct assets (e.g., files, software components) which have been damaged, destroyed, or modified in a way that makes them suspect.	Information Diversity, Fragmentation, Distributed Functionality, Protected Backup and Restore, Replication, Dynamic Reconfiguration
CM1142	**Switch to Protected Hot Shadow**	AC-4(2), AC-4(8), CP-2(5), CP-9(6), IR-4(2)	Switch (failover) to a duplicate system in a protected enclave which, subject to additional quality controls on data and software updates, mirrors the system which has been compromised.	Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication, Predefined Segmentation, Integrity Checks

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1143	**Switch to Alternate System or Component**	CP-2(5), IR-4(2), SA-17(9), SC-22, SC-29	Switch (failover) to another system or component which provides roughly equivalent functionality in a different way.	Architectural Diversity, Design Diversity, Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication
CM1144	**Activate Alternate**	CP-2(5), IR-4(2), SA-17(9), SA-20, SA-23, SC-29	Activate an alternate system or component (e.g., from a war-time reserve) which provides roughly equivalent function in a novel or specialized way, and failover.	Architectural Diversity, Design Diversity, Dynamic Reconfiguration, Adaptive Management, Orchestration, Specialization
CM1145	**Defend Failover and Recovery**	AC-2(6), IR-4(2), IR-4(3), SC-7(20), SC-48, SC-48 (1), SI-4(1)	Increase sensor activity and restrict privileges to defend against an adversary taking advantage of failover or recovery activities.	Adaptive Management, Dynamic Reconfiguration, Orchestration, Functional Relocation of Sensors, Dynamic Segmentation and Isolation, Mission Dependency and Status Visualization, Dynamic Privileges
CM1146	**Refresh Sessions or Connections**	SC-23(3), SC-30(2), SI-14(3)	Terminate and re-establish sessions or network connections unpredictably to disrupt adversary use.	Non-Persistent Connectivity, Temporal Unpredictability
CM1147	**Defend Against DoS**	AC-4(3), SC-5(2), SC-5(3)	Adapt to reduce the impacts of denial-of-service attacks.	Dynamic Resource Allocation, Surplus Capacity, Monitoring and Damage Assessment
CM1148	**Conceal or Randomize Network Traffic**	SC-8(5), SC-30	Conceal (via encryption or insertion of fabricated traffic) or randomize network traffic patterns.	Obfuscation, Contextual Unpredictability
CM1149	**Lock Down Visibility or Access**	AC-3(11)	Restrict the visibility of or access to data based on the nature or attributes of that data.	Attribute-Based Usage Restriction
CM1150	**Dynamically Relocate and Refresh Processing**	SC-30(3), SI-14(1)	Suspend a process and re-instantiate it in a different location.	Functional Relocation of Cyber Resources, Non-Persistent Services

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1151	**Defend Enclave Boundaries**	AC-4(8), AC-4(12), AC-4(17), AC-4(21), SC-7(21), SC-7(22), SC-46	Maintain distinct enclaves based on security characteristics and defend the enclave boundary.	Predefined Segmentation, Integrity Checks, Provenance Tracking
CM1152	**Defend Against Memory Attacks**	SI-16	Provide defenses against attacks against system memory.	Synthetic Diversity, Temporal Unpredictability
CM1153	**Modulate Information Flows**	AC-4(27), AC-4(29), AC-4(30), SC-7(15), SC-46	Use controlled interfaces and communications paths to provide access to risky capabilities.	Predefined Segmentation
CM1154	**Hardware-Based Protection of Firmware**	SC-51	Use hardware-based protections for firmware.	Integrity Checks
CM1155	**Validate Output Data**	SI-15	Validate information output from processes or applications against defined criteria.	Integrity Checks
CM1156	**Physically Relocate Resources**	SC-30(3)	Physically move resources (e.g., storage devices, servers, end-user devices), with concomitant changes to network location.	Asset Mobility
CM1157	**Defend Against Data Mining**	AC-23	Enforce access restrictions and provide alerting to defend against data mining.	Monitoring and Damage Assessment, Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges
CM1158	**Defend Audit Data**	AU-9(1), AU-9(2), AU-9(3), AU-9(6)	Provide mechanisms to protect audit data from modification or observation.	Integrity Checks, Predefined Segmentation
CM1159	**Enhance User Preparedness**	AT-2(1), AT-2(3), AT-2(5), AT-3(3)	Keep users, administrators, and operators aware of existing and emerging threats and attack techniques they can counter in practice.	Dynamic Threat Awareness, Self-Challenge

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1160	**Conceal Resources from Discovery**	SC-7(16), SC-28 (1), SC-30, SC-30(5)	Protect locations of system components from discovery through common tools and techniques, via hiding or relocation.	Obfuscation, Functional Relocation of Cyber Resources
CM1161	**Collaborate to Counter Adversaries**	PM-16, SC-30(4), SI-20	Collaborate with other entities to counter adversary activities.	Disinformation, Tainting, Dynamic Threat Awareness
CM1162	**Restrict Supply Chain Exposures**	CM-7(7), PM-30(1), SR-3(2), SR-5, SR-6(1), SR-7, SR-10, SR-11	Limit adversaries' ability to determine or manipulate the organization's cyber supply chain.	Obfuscation, Disinformation, Self-Challenge, Supply Chain Diversity
CM1163	**Redefine System**	IR-4(10), SC-27, SC-29, SR-5(1)	Redefine the system in terms of components, interfaces, and dependencies.	Orchestration, Architectural Diversity, Supply Chain Diversity, Evolvability, Replication
CM1164	**Calibrate Administrative Access**	AC-6, AC-6(5), CM-7(2)	Configure administrator access to resources based on active defense strategies.	Attribute-Based Usage Restriction, Trust-Based Privilege Management, Restriction

4.4 Candidate Mitigations with Intensifying Potential Effects

Finally, some candidate mitigations have been defined which could be used in conjunction with CMs presented in Table 17 to increase the effectiveness of those CMs. The effects of these CMs on ATT&CK Techniques are indirect, resulting from the intensified effectiveness of other CMs. These additional "intensifier" CMs are presented in Table 18. Technique-specific descriptions are given in Appendix C, Table 22. Because their potential effects depend so strongly on whether other CMs have been applied, these CMs are currently not included in the mapping tables in Section 3.

Table 18. Candidate Mitigations with Intensifying Potential Effects

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1301	**Dynamic Threat Awareness and Response**	CA-7(3), RA-3(2), RA-3(3), RA-3(4), RA-5(10), RA-10, PM-16, PM-16 (1)	Use awareness of the current threat landscape to inform threat hunting and threat-adaptive defenses.	Adaptive Management, Sensor Fusion and Analysis, Dynamic Threat Awareness
CM1302	**Mission-Oriented Cyber Situational Awareness**	SI-4(1), SI-4(2)	Maintain awareness of mission dependencies and the current status of mission-critical assets to inform threat-adaptive responses.	Sensor Fusion and Analysis, Mission Dependency and Status Visualization

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1303	**Integrated Non-Disruptive Response**	SI-4(3), SI-4(7), SI-7(5)	Integrate automated and human-directed response to suspicious events to minimize disruption.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Adaptive Management
CM1304	**Enhance via Unpredictability**	SC-30(2), SI-19(6)	Enhance the effectiveness of defender actions by using capabilities unpredictably.	Contextual Unpredictability, Temporal Unpredictability
CM1305	**Enhance via Heterogeneity**	AU-9(7), CP-11, SC-29, SC-29 (1)	Increase barriers to adversary effectiveness by providing architecturally diverse system components.	Architectural Diversity
CM1306	**Lock Down Usage**	AC-3(12), AC-6(10), CM-5(5), CM-5(6), CM-7(4)	Restrict access to applications and configurations as part of the installation process, and narrowly restrict modifications or other uses of privileged functions.	Attribute-Based Usage Restriction, Trust-Based Privilege Management
CM1307	**Enhance via Layered Protections**	PL-8(1), SC-3(5)	Provide similar capabilities or mechanisms at multiple architectural layers.	Calibrated Defense-in-Depth
CM1308	**Separate Environments with Specific Risks**	AU-6(8), CM-4(1), SC-7(13)	Provide environments separate from the operational environment for activities with specific risks.	Monitoring and Damage Assessment, Predefined Segmentation
CM1309	**Vulnerability-Oriented Cyber Situational Awareness**	RA-5(6), RA-5(8), RA-5(10)	Maintain awareness of the vulnerability posture over time to inform calibration of detection as well as proactive responses.	Sensor Fusion and Analysis
CM1310	**Protect Distributed Processing and Storage**	SC-36 (1), SC-36 (2)	Provide supporting protections for distributed processing and distributed or replicated storage.	Behavior Validation, Replication
CM1311	**Enhance via Isolation**	SC-3(2), SC-39 (2), SC-50	Enhance the effectiveness of, or confidence in, security functions via system mechanisms for isolation.	Predefined Segmentation, Dynamic Segmentation, and Isolation

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1312	**Enhance Isolation via Hardware Features**	SC-3(1), SC-39 (1), SC-49, SC-50	Enhance the effectiveness of, or confidence in, isolation by using underlying hardware features.	Predefined Segmentation, Dynamic Segmentation, and Isolation
CM1313	**Validate or Assess Control Effectiveness in Practice**	CP-4(5), CP-9(1), SI-19(8)	Validate or assess the effectiveness of controls as implemented and used in practice.	Self-Challenge, Protected Backup and Restore, Integrity Checks
CM1314	**Enhance via Automation**	CA-7(6) , PE-6(2), PM-16(1), RA-5(6), SI-4(2), SI-4(3), SI-4(7), SI-7(5)	Use automation to increase the effectiveness or quality of capabilities and practices.	Adaptive Management, Monitoring and Damage Assessment, Sensor Fusion and Analysis, Dynamic Threat Awareness, Integrity Checks, Behavior Validation
CM1315	**Maintain a War-Time Reserve**	RA-9, SA-20, SA-23, SR-5(1)	Maintain a reserve of critical components, both special-purpose and acquired, for use in a crisis situation.	Mission Dependency and Status Visualization, Specialization, Replication
CM1316	**Enhance via Coordination**	CP-2(1), IR-4(10), IR-4(11)	Coordinate across the organization and with external stakeholders to increase the effectiveness or timeliness of capabilities and practices.	Adaptive Management, Orchestration

5 Mapping Tables – ATT&CK for ICS

This section provides the tables mapping cyber resiliency controls and approaches to the Techniques in ATT&CK for ICS. One table is provided for each ATT&CK Tactic, following the same color-coding conventions as ATT&CK for Enterprise. However, as discussed in Section 2.2, ATT&CK for ICS identifies controls for Mitigations. These are in plain font. Additional controls identified by the Cyber Resiliency Effects Analysis are in **bold**.

For each Tactic, the relationships of the A4I Techniques – to Techniques in A4E and, as relevant, to other A4I Techniques – are briefly discussed.

5.1 Initial Access Tactic

In the 13 Techniques under Initial Access, the adversary is trying to get into the ICS environment.

Relationships: The Initial Access Tactic in A4I reflects elements of A4E under multiple Tactics, not simply Initial Access. Data Historian Compromise (T0810) and Engineering Workstation Compromise (T0818) basically are examples of Lateral Movement – the adversary already has a presence in the IT environment and compromises a data historian or engineering workstation to gain a foothold into the control system environment. Drive-by Compromise (T0817) is similar to the corresponding A4E Technique, since it involves an attack on the IT network; no users on the OT network should be accessing the internet via a web browser. Other Techniques with corresponding A4E Techniques of the same name include Exploit Public-Facing Application (T0819) with T1190, Exploitation of Remote Services (T0866) with T1210, External Remote Services (T0822) with T1133, Remote Services (T0886) with T1021, Replication Through Removable Media (T0847) with T1091, and Supply Chain Compromise (T0862) with T1195. Spearphishing Attachment (T0865) corresponds to a sub-technique under Phishing for Information (T1598) and Phishing (T1566). No A4E Technique corresponds to Internet Accessible Device (T0883), Rogue Master (T0848), and Wireless Compromise (T0860).

Table 19. Initial Access Tactic for ICS

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Data Historian Compromise (T0810)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Disable or Remove Feature or Program (M0942)	Standard practice	Preempt, Negate, Degrade, Exert	CM-7

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Restriction	Preempt, Negate, Degrade, Exert	**CM-7(2)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), AC-4(21), SC-7, SC-7(21), SC-7(22), SC-7(29)**
	Software Configuration (M0954)	Standard practice	Preempt, Negate, Degrade, Exert	CM-7
	Adversarial Simulation (CM1207)	Self-Challenge	Preempt	CA-8,CA-8(2)
	Active Decoys (CM1223)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Monitor Logs (CM2104)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
Drive-by Compromise (T0817)	Application Isolation and Sandboxing (M0948)	Cyber hygiene	Contain, Exert	SI-3
		Predefined Segmentation	Contain, Exert	**AC-4(21), AC-6(4), SC-18 (5), SC-39, CM-7(6)**, SI-3
	Exploit Protection (M0950)	Restriction	Delay, Exert	SI-16
		Integrity Checks	Delay, Exert	**AC-4(8)**
		Behavior Validation	Detect, Exert	**IR-4(13)**
	Restrict Web-Based Content (M0921)	Standard practice	Negate, Preempt	**CM-7(5)**, SC-18, **SC-7**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Expunge, Shorten	SI-2
	Active Decoys (CM1223)	Misdirection	Deceive, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Dynamic Segmentation and Isolation	Contain	SC-35
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Endpoint Behavior Analysis (CM2103)	Monitoring and Damage Assessment	Detect	AC-2(12)
Engineering Workstation Compromise (T0818)	Antivirus/Antimalware (M0949)	Cyber hygiene	Detect, Expunge, Shorten	**AC-4, AT-2, AT-3, CM-4,** SI-3
	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Disable or Remove Feature or Program (M0942)	Standard practice	Preempt	CM-7
	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Delay, Exert	SC-28
		Obfuscation	Negate, Delay, Exert	**SC-28(1)**
	Limit Hardware Installation (M0934)	Cyber hygiene	Preempt	MP-7
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), AC-4(21), SC-7, SC-7(22), SC-7(29)**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Degrade, Exert	SI-2
	Adversarial Simulation (CM1207)	Self-Challenge	Preempt	CA-8, CA-8(1), CA-8(2)
	Active Decoys (CM1223)	Misdirection	Deceive, Negate, Contain	SC-26

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Misdirection	Detect, Scrutinize	SC-35
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Monitor Logs (CM2104)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
Exploit Public-Facing Application (T0819)	Application Isolation and Sandboxing (M0948)	Predefined Segmentation	Contain, Exert	**AC-4(21), AC-6(4), SC-18(5), SC-39, CM-7(6)**
	Exploit Protection (M0950)	Standard practice	Negate, Exert, Detect	**SC-7(17), SI-7,** SI-16
	Network Segmentation (M0930)	Standard practice	Degrade, Contain	AC-3
		Predefined Segmentation	Degrade, Preempt, Contain, Reduce	**AC-4(2), SC-7(29), SC-7(22)**
	Privileged Account Management (M0926)	Cyber hygiene	Negate, Exert	AC-2
		Trust-Based Privilege Management	Negate, Exert	**AC-6(5)**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Exert	SI-2
	Vulnerability Scanning (M0916)	Cyber hygiene	Detect, Reveal, Shorten	RA-5
	Present Deceptive Information (CM1201)	Disinformation	Delay, Deter, Deceive, Exert	SC-30 (4)
	Maintain Deception Environment (CM1202)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Monitor Logs (CM2104)	Behavior Validation	Detect	AU-6
Exploitation of Remote Services (T0866)	Application Isolation and Sandboxing (M0948)	Predefined Segmentation	Contain, Delay, Preempt	**AC-4(21), AC-6(4), SC-39, CM-7(6)**
		Restriction	Exert, Preempt	**CM-7(2)**

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Disable or Remove Feature or Program (M0942)	Cyber hygiene	Exert, Preempt	CM-7, **SC-41**
	Exploit Protection (M0950)	Integrity Checks	Delay, Exert, Detect	**AC-4(8)**
		Behavior Validation	Detect	**IR-4(13)**
		Synthetic Diversity, Restriction	Preempt, Exert	SI-16
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-3, SC-7, SC-7(22), SC-7(29)**
	Privileged Account Management (M0926)	Standard practice	Degrade, Exert	AC-2
		Trust-Based Privilege Management	Degrade, Exert	**AC-6(5)**
	Threat Intelligence Program (M0919)	Dynamic Threat Awareness	Exert, Preempt	**PM-16, RA-3(3)**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Degrade, Exert	SI-2
	Vulnerability Scanning (M0916)	Cyber hygiene	Detect, Reveal, Shorten	RA-5
	Maintain Deception Environment (CM1202)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Endpoint Behavior Analysis (CM2103)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
	Monitor Network Usage (CM2147)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)
External Remote Services (T0822)	Account Use Policies (M0936)	Standard practice	Negate, Delay, Exert	**AC-2(11), AC-7**, IA-5

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Disable or Remove Feature or Program (M0942)	Standard practice	Preempt, Negate, Degrade, Exert	CM-7
		Restriction	Preempt, Negate, Degrade, Exert	**CM-7(2)**
	Limit Access to Resource Over Network (M0935)	Standard practice	Preempt, Exert	AC-3, **AC-6, AC-17**, SC-7
	Multi-factor Authentication (M0932)	Standard practice	Negate, Exert	IA-2, **IA-2(1), IA-2(2), IA-2(6)**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Preempt, Contain, Exert	**AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)**
	Password Policies (M0927)	Cyber hygiene	Degrade, Exert	IA-5
	Enhanced Authentication (CM1226)	Calibrated Defense-in-Depth, Path Diversity	Delay, Exert	IA-2(13), IA-10
	Minimize Duration of Connection or Session (CM1227)	Non-Persistent Connectivity	Preempt, Shorten	SC-10, SI-14 (3)
	Monitor Logs (CM2104)	Monitoring and Damage Assessment, Behavior Validation	Detect	AU-6
Internet Accessible Device (T0883)	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Preempt, Contain, Exert	**AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)**
	Maintain Deception Environment (CM1202)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Monitor Logs (CM2104)	Behavior Validation	Detect	AU-6

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Remote Services (T0886)	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(7), AC-3(13)**
		Cyber hygiene	Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Preempt, Contain, Exert	**AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)**
	Password Policies (M0927)	Cyber hygiene	Degrade, Exert	IA-5
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Maintain Deception Environment (CM1202)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Dynamically Restrict Traffic or Isolate Resources (CM1208)	Dynamic Reconfiguration	Contain, Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Dynamic Segmentation, and Isolation	Preempt, Contain, Shorten, Reduce	SC-7(20)

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Modulate Information Flows (CM1253)	Predefined Segmentation, Trust-Based Privilege Management	Negate, Exert	SC-7(15)
	Cross-Enterprise Behavior Analysis (CM2118)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
Replication Through Removable Media (T0847)	Disable or Remove Feature or Program (M0942)	Restriction	Exert, Preempt	**CM-7(2)**
		Cyber hygiene	Exert, Preempt	CM-7
	Limit Hardware Installation (M0934)	Cyber hygiene	Preempt, Negate, Exert	MP-7, **MP-6, SC-41**
	Operating System Configuration (M0928)	Cyber hygiene	Exert	CM-7
		Restriction	Exert, Preempt	**CM-7(2)**
	Virtual Sandbox (CM1209)	Non-Persistent Services	Preempt, Shorten	SC-7(20)
		Dynamic Segmentation and Isolation	Delay, Contain	SC-7(20)
	Removable Device Usage Detection (CM2108)	Monitoring and Damage Assessment	Detect	CM-8(3)
Rogue Master (T0848)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Negate, Degrade, Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
		Provenance Tracking	Negate, Delay, Degrade, Exert	**AC-4(17)**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Preempt, Contain, Exert	**AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)**

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	**AC-3(13)**
		Provenance Tracking	Negate, Delay, Degrade, Exert	**AC-4(17)**
	Adversarial Simulation (CM1207)	Self-Challenge	Preempt	CA-8, CA-8(1), CA-8(2)
	Active Decoys (CM1223)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
		Misdirection	Detect, Scrutinize	SC-35
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Spearphishing Attachment (T0865)	Antivirus/Antimalware (M0949)	Cyber hygiene	Detect, Expunge, Shorten	**AC-4, AT-2, AT-3, CM-4,** SI-3
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
	Restrict Web-Based Content (M0921)	Standard practice	Negate, Preempt	**CM-7(5),** SC-18, **SC-7**
	User Training (M0917)	Cyber hygiene	Negate, Degrade, Exert	AT-2
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Detect	SC-30 (4)
	Enhance User Preparedness (CM1259)	Dynamic Threat Awareness	Negate, Degrade, Exert, Detect	AT-2(1), AT-2(3), AT-2(5)
	Analyze Network Traffic Content (CM2141)	Monitoring and Damage Assessment, Behavior Validation	Detect	SI-4(13)
Supply Chain Compromise (T0862)	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **CM-14**
		Provenance Tracking	Detect	**CM-14, SI-7(15), SR-4, SR-4(1), SR-4(2)**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Expunge, Shorten	SI-2
	Audit (M0947)	Integrity Checks	Shorten	**CM-14,** SI-7, **SI-7(6), SI-**

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
				7(12), SI-7(15)
	Vulnerability Scanning (M0916)	Cyber hygiene	Detect, Reveal, Shorten	RA-5
		Integrity Checks	Detect, Reveal, Shorten	**SA-9(7), SA-11(4)**
	Supply Chain Management (M0817)	Standard practice	Negate, Degrade, Exert	SR-12
	Restrict Supply Chain Exposures (CM1262)	Integrity Checks, Provenance Tracking	Detect	SR-5, SR-11
		Monitoring and Damage Assessment	Detect	SR-6(1), SR-10
		Forensic and Behavioral Analysis	Detect	SR-10
		Predefined Segmentation	Contain	CM-7(7)
	Software Integrity Check (CM2109)	Integrity Checks	Detect	SI-7, SI-7(1)
		Integrity Checks, Provenance Tracking	Detect	CM-14, SR-4(3)
	Software Stress Testing (CM2110)	Self-Challenge	Detect	SR-6(1)
	Physical Inspection (CM2111)	Integrity Checks	Detect	SR-9, SR-10
	Component Provenance Validation (CM1205)	Provenance Tracking	Detect, Delay, Exert	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4)
		Integrity Checks	Detect, Exert	SR-11(3)
Wireless Compromise (T0860)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
	Encrypt Network Traffic (M0808)	Standard practice	Negate, Degrade, Exert	SC-8
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**

ATT&CK Technique (*Initial Access*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
		Calibrated Defense-in-Depth	Negate, Degrade, Exert	**PL-8(1)**
		Architectural Diversity	Negate, Degrade, Exert	**SC-29**
		Obfuscation, Integrity Checks	Negate, Degrade, Exert	**IA-3(1)**
	Minimize Wireless Signal Propagation (M0806)	Standard practice	Negate, Degrade, Exert	SC-40
		Obfuscation	Negate, Degrade, Exert	**SC-40(2)**

5.2 Execution Tactic

In the nine Techniques under the Execution Tactic, the adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.

Relationships: Techniques with A4E counterparts include Command-Line Interface (T0807), which has some similarities with Command and Scripting Interpreter (T1059); Execution through API (T0871), which is related to Native API (T1106); Hooking (T0874), which corresponds to T1056.004, Credential API Hooking, a sub-technique of Input Capture; Native API (T0834), which relates to Native API (T1106) and to Execution through API (T0871); Scripting (T0853), related to Command and Scripting Interpreter (T1059) and Command-Line Use (T0807); User Execution (T0863), which corresponds to T1204. Change Operating Mode (T0858) [28] has no A4E counterparts.

Table 20. Execution Tactic for ICS

ATT&CK Techniques (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Change Operating Mode (T0858)	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(13)**
		Cyber hygiene	Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23

[28] T0858 is related to Activate Firmware Update Mode, T0800, under the Inhibit Response Function Tactic.

ATT&CK Techniques (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(22), SC-7(29)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13)
Command-Line Interface (T0807)	Disable or Remove Feature or Program (M0942)	Standard practice	Negate, Degrade, Exert	CM-7
		Restriction	Preempt	**CM-7(2)**
	Execution Prevention (M0938)	Cyber hygiene	Negate, Degrade, Exert	SI-3
		Restriction	Preempt	**CM-7(2)**
		Purposing	Preempt	**CM-7(4)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
	Monitor Command Line Use (CM2138)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(13)
Execution through API (T0871)	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(13)**
		Cyber hygiene	Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**

ATT&CK Techniques (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Execution Prevention (M0938)	Cyber hygiene	Negate, Degrade, Exert	SI-3
		Restriction	Preempt	**CM-7(2)**
	Host-Local Event Correlation (CM2122)	Monitoring and Damage Assessment	Detect	IR-4(13)
Graphical User Interface (T0823)	Limit Access to Resource Over Network (M0935)	Standard practice	Preempt, Exert	AC-3, **AC-6, AC-17**, SC-7
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
Hooking (T0874)	Restrict Library Loading (M0944)	Standard practice	Exert	**CM-7**
		Purposing	Preempt, Exert	**CM-7, CM-7(4)**
	Audit (M0947)	Integrity Checks	Detect, Shorten	**CM-14**, SI-7, **SI-7(6), SI-7(12), SI-7(15)**
	Analyze Logs (CM2105)	Monitoring and Damage Assessment	Detect	AC-2(12), SI-4(16)
		Dynamic Resource Awareness	Detect	SI-4(16)
Modify Controller Tasking (T0821)	Audit (M0947)	Integrity Checks	Detect, Shorten	**CM-14**, SI-7, **SI-7(6), SI-7(12)**
		Provenance Tracking	Detect, Exert	**SI-7(15)**
	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(6)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
Native API (T0834)	Execution Prevention (M0938)	Cyber hygiene	Negate, Degrade, Exert	SI-3
		Restriction	Preempt	**CM-7(2)**
	Host-Local Event Correlation (CM2122)	Monitoring and Damage Assessment	Detect	IR-4(13)
Scripting (T0853)	Application Isolation and Sandboxing (M0948)	Standard practice	Contain, Delay	SI-3
		Predefined Segmentation	Contain, Delay, Preempt	**AC-4(21), AC-6(4), SC-39, CM-7(6)**

ATT&CK Techniques (*Execution*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Disable or Remove Feature or Program (M0942)	Standard practice	Exert, Preempt	CM-7
		Restriction	Exert, Preempt	**CM-7(2)**
	Execution Prevention (M0938)	Cyber hygiene	Negate, Degrade, Exert	SI-3
		Restriction	Preempt	**CM-7(2)**
		Purposing	Preempt	**CM-7(4)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
	Monitor Script Execution (CM2129)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(13)
User Execution (T0863)	Antivirus/Antimalware (M0949)	Cyber hygiene	Detect, Expunge, Shorten	**AC-4, AT-2, AT-3, CM-4,** SI-3
	Code Signing (M0945)	Integrity Checks	Detect	**CM-14,** SI-7
		Provenance Tracking	Negate, Exert	**SI-7(15)**
		Trust-Based Privilege Management	Negate, Exert	**CM-7(5)**
	Execution Prevention (M0938)	Cyber hygiene	Negate, Degrade, Exert	SI-3
		Restriction	Preempt	**CM-7(2)**
		Purposing	Preempt	**CM-7(4)**
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
	Restrict Web-Based Content (M0921)	Standard practice	Negate, Preempt	SC-18
		Integrity Checks	Preempt, Exert	**AC-4(8)**
		Trust-Based Privilege Management	Negate, Degrade, Exert	**CM-7(5)**
	User Training (M0917)	Cyber hygiene	Negate, Degrade, Exert	AT-2
		Standard practice	Negate, Degrade, Exert	**AT-2(4)**
	Enhance User Preparedness (CM1259)	Dynamic Threat Awareness	Negate, Degrade, Exert, Detect	AT-2(1), AT-2(3), AT-2(5)
	Application- or Utility-Specific Monitoring (CM2120)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)

5.3 Persistence Tactic

In the five Techniques under Persistence, the adversary is trying to maintain their foothold in the ICS environment.

Relationships: Modify Program (T0889) is somewhat related to Modify System Process (T1543). Module Firmware (T0839) and System Firmware (T0857) have some similarity with Firmware Corruption (T1495), though T1495 is more oriented to denial-of-service. Project File Infection (T0873) is similar to Data Manipulation (T1565) and Modify Program (T0889). Valid Accounts (T0859) corresponds to T1078.

Table 21. Persistence Tactic for ICS

ATT&CK Techniques (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Modify Program (T0889)	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1)**
	Code Signing (M0945)	Integrity Checks	Detect	**CM-14,** SI-7
		Provenance Tracking	Detect	**CM-14, SI-7(15)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
Module Firmware (T0839)	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Encrypt Network Traffic (M0808)	Standard practice	Negate, Degrade, Exert	SC-8
		Obfuscation, Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Negate, Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Boot Integrity (M0946)	Integrity Checks	Detect	**SI-6**, SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **SI-7(1), CM-14**

ATT&CK Techniques (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Provenance Tracking	Detect	**CM-14, SI-7(15), SR-4, SR-4(1), SR-4(3)**
	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Delay, Exert	SC-28
		Obfuscation	Negate, Delay, Exert	**SC-28(1)**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), SC-3, SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Hardware-Based Protection of Firmware (CM1254)	Integrity Checks	Negate, Preempt	SC-51
Project File Infection (T0873)	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(6)**
		Standard practice	Negate, Exert	**SC-28(3)**
	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Exert	SC-28
		Obfuscation, Integrity Checks	Negate, Exert	**SC-28(1)**
	Restrict File and Directory Permissions (M0922)	Trust-Based Privilege Management	Negate, Delay, Exert	AC-6
	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Validate Data Properties (CM1237)	Integrity Checks	Delay, Degrade, Exert, Detect	SI-7, SI-7(1)
System Firmware (T0857)	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3

ATT&CK Techniques (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Encrypt Network Traffic (M0808)	Standard practice	Negate, Degrade, Exert	SC-8
		Obfuscation, Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Negate, Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Boot Integrity (M0946)	Integrity Checks	Detect	**SI-6**, SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Code Signing (M0945)	Integrity Checks	Detect	**CM-14,** SI-7, **SI-7(1), SI-7(6)**
		Provenance Tracking	Detect	**CM-14, SI-7(15), SR-4, SR-4(1), SR-4(2)**
	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Delay, Exert	SC-28
		Obfuscation	Negate, Delay, Exert	**SC-28(1)**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), SC-3, SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, **AC-4, AC-4(1),** SC-7
		Integrity Checks	Negate, Contain, Degrade, Exert	**AC-4(8)**
	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Hardware-Based Protection of Firmware (CM1254)	Integrity Checks	Negate, Preempt	SC-51
Valid Accounts (T0859)	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3

ATT&CK Techniques (*Persistence*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Account Use Policies (M0936)	Standard practice	Negate, Delay, Exert	**AC-2(11), AC-7**, IA-5
	Active Directory Configuration (M0915)	Standard practice	Negate, Exert	**AC-2, AC-2(1)**
		Consistency Analysis	Negate, Delay, Degrade, Exert	**AC-6(7)**
	Application Developer Guidance (M0913)	Standard practice	Preempt, Exert	AT-3**, IA-5(7), SA-8**
	Multi-factor Authentication (M0932)	Standard practice	Negate, Exert	IA-2, **IA-2(1), IA-2(2), IA-2(6)**
	Password Policies (M0927)	Cyber hygiene	Degrade, Exert	IA-5
	Privileged Account Management (M0926)	Cyber hygiene	Negate, Exert	AC-2
		Trust-Based Privilege Management	Negate, Exert	**AC-6(5)**
		Trust-Based Privilege Management, Consistency Analysis	Negate, Exert	**AC-6(7)**
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
		Trust-Based Privilege Management, Consistency Analysis	Negate, Exert	**AC-6(7)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, **AC-4, AC-4(1),** SC-7
	Audit (M0947)	Standard practice	Detect	SI-7
		Consistency Analysis	Detect	**CA-7(5)**
	Present Deceptive Information (CM1201)	Disinformation	Exert	SC-30 (4)
		Tainting	Detect	SI-20
	Cross Enterprise Account Usage Analysis (CM2113)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

5.4 Privilege Escalation Tactic

In the two Techniques under Privilege Escalation, the adversary is trying to obtain higher-level permissions.

Relationships: Exploitation for Privilege Escalation (T0890) corresponds to T1068. Hooking (T0874) also appears under Execution.

Table 22. Privilege Escalation Tactic for ICS

ATT&CK Techniques (*Privilege Escalation*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Exploitation for Privilege Escalation (T0890)	Application Isolation and Sandboxing (M0948)	Cyber hygiene	Contain	SI-3
		Predefined Segmentation	Contain, Delay, Preempt	**AC-4(21), AC-6(4), SC-39, CM-7(6)**
	Exploit Protection (M0950)	Integrity Checks	Delay, Exert, Detect	**AC-4(8)**
		Behavior Validation	Detect	**IR-4(13)**
		Synthetic Diversity, Restriction	Preempt, Exert	SI-16
	Threat Intelligence Program (M0919)	Dynamic Threat Awareness	Exert, Preempt	PM-16, RA-3(3)
	Update Software (M0951)	Cyber hygiene	Exert, Preempt	SI-2
		Standard practice	Exert, Preempt	**MA-3(6), RA-5**
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30 (4)
		Tainting	Exert, Scrutinize, Reveal	SI-20
	Refresh Selected Applications or Components (CM1234)	Non-Persistent Information	Expunge, Shorten	SI-14 (1)
	Endpoint Behavior Analysis (CM2103)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Hooking (T0874)	Restrict Library Loading (M0944)	Purposing	Preempt, Exert	**CM-7, CM-7(4)**
	Audit (M0947)	Integrity Checks	Detect, Shorten	**CM-14**, SI-7, **SI-7(6), SI-7(12), SI-7(15)**
	Analyze Logs (CM2105)	Monitoring and Damage Assessment	Detect	AC-2(12), SI-4(16)
		Dynamic Resource Awareness	Detect	SI-4(16)

5.5 Evasion Tactic

In the six Techniques under Privilege Escalation, the adversary is trying to avoid being detected.

Relationships: Change Operating Mode (T0858) also appears under Execution. Exploitation for Evasion (T0820) is similar to Exploitation for Defense Evasion (T1211); however, the assets affected by this technique do not accommodate the Active Deception CM. Indicator Removal on Host (T0872) corresponds to T1070, Masquerading (T0849) to T1076, and Rootkit (T0851) to T1014. Spoof Reporting Message (T0856) has no corresponding A4E Technique.

Table 23. Evasion Tactic for ICS

ATT&CK Techniques (*Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Change Operating Mode (T0858)	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-3, **AC-3(12), AC-3(13)**
		Cyber hygiene	Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(22), SC-7(29)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Exploitation for Evasion (T0820)	Application Isolation and Sandboxing (M0948)	Cyber hygiene	Contain, Exert	SI-3
		Predefined Segmentation	Contain, Exert	**AC-4(21), AC-6(4), SC-39, CM-7(6)**
		Cyber hygiene	Negate, Exert	AC-2

ATT&CK Techniques (*Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Privileged Account Management (M0926)	Trust-Based Privilege Management	Negate, Exert	**AC-6(5)**
	Exploit Protection (M0950)	Synthetic Diversity, Restriction	Delay, Exert	SI-16
		Integrity Checks	Delay, Exert	**AC-4(8)**
		Behavior Validation	Detect, Exert	**IR-4(13)**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Expunge, Shorten	SI-2
	Threat Intelligence Program (M0919)	Dynamic Threat Awareness	Exert, Preempt	**PM-16, RA-3(3)**
Indicator Removal on Host (T0872)	Restrict File and Directory Permissions (M0922)	Trust-Based Privilege Management	Negate, Delay, Exert	AC-6
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
	Monitor the File System (CM2133)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Masquerading (T0849)	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(6)**
		Provenance Tracking	Detect	**SI-7(15)**
	Execution Prevention (M0938)	Cyber hygiene	Negate, Degrade, Exert	SI-3
		Restriction	Preempt	**CM-7(2)**
		Purposing	Preempt	**CM-7(4)**
	Restrict File and Directory Permissions (M0922)	Attribute-Based Usage Restriction	Negate, Delay, Exert	AC-6
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Monitor the File System (CM2133)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
		Sensor Fusion and Analysis	Detect	SI-4(24)
Rootkit (T0851)	Code Signing (M0945)	Integrity Checks	Detect, Negate	SI-7, **SI-7(1), SI-7(6)**
	Audit (M0947)	Integrity Checks	Shorten	SI-7, **SI-7(6), SI-7(12), SI-7(15)**

ATT&CK Techniques (*Evasion*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Spoof Reporting Message (T0856)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Negate, Degrade, Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
		Provenance Tracking	Negate, Delay, Degrade, Exert	**AC-4(17)**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Negate, Contain, Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	**AC-3(13)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)

5.6 Discovery Tactic

In the five Techniques under Discovery, the adversary is trying to figure out the ICS environment.

Relationships: Network Connection Enumeration (T0840) is similar to Remote System Discovery (T1018) and System Network Connections Discovery (T1016). Network Sniffing (T0842) corresponds to T1040, and Remote System Discovery (T0846) to T1018. Remote

System Information Discovery (T0888) includes elements of System Information Discovery (T1082) and Peripheral Device Discovery (T1120).

Table 24. Discovery Tactic for ICS

ATT&CK Techniques (*Discovery*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Network Connection Enumeration (T0840)	Mitigation Limited or Not Effective (M0816)	Not applicable	—	—
	Passive Decoys (CM1204)	Misdirection	Divert, Deceive, Delay	SC-26
	Conceal Resources from Discovery (CM1260)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2115)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Network Sniffing (T0842)	Encrypt Network Traffic (M0808)	Cyber hygiene	Negate, Degrade, Exert	SC-8
		Obfuscation	Negate, Degrade, Exert	**SC-8(1)**
	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Multi-factor Authentication (M0932)	Standard practice	Negate, Exert	IA-2, **IA-2(1), IA-2(2)**
		Calibrated Defense-in-Depth	Negate, Exert	**IA-2(6)**
	Network Segmentation (M0930)	Standard practice	Negate, Contain, Exert	AC-3
		Predefined Segmentation	Preempt, Contain, Exert	**SC-7, SC-7(21), SC-7(22)**
	Privileged Account Management (M0926)	Standard practice	Degrade, Exert	AC-2
		Trust-Based Privilege Management	Degrade, Exert	**AC-6(5)**
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30 (4)
		Tainting	Detect, Scrutinize	SI-20
	Enhanced Authentication (CM1226)	Calibrated Defense-in-Depth, Path Diversity	Degrade, Exert	IA-2(13)

ATT&CK Techniques (*Discovery*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Conceal or Randomize Network Traffic (CM1248)	Obfuscation, Contextual Unpredictability	Delay, Exert	SC-8(5), SC-30
	Privileged Account Monitoring (CM2117)	Monitoring and Damage Assessment	Detect	AU-6(8)
Remote System Discovery (T0846)	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Disable or Remove Feature or Program (M0942)	Cyber hygiene	Preempt	CM-7, **SC-41**
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), AC-4(21), SC-7, SC-7(22)**
	Passive Decoys (CM1204)	Misdirection	Divert, Deceive, Delay	SC-26
	Conceal Resources from Discovery (CM1260)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2115)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Remote System Information Discovery (T0888)	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Disable or Remove Feature or Program (M0942)	Cyber hygiene	Preempt	CM-7, **SC-41**
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), AC-4(21), SC-7, SC-7(22)**
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Detect	SC-30(4)

ATT&CK Techniques (*Discovery*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Conceal Resources from Discovery (CM1260)	Obfuscation, Functional Relocation of Cyber Resources	Degrade, Exert, Shorten	SC-7(16), SC-30, SC-30(5)
	Process Monitoring (CM2115)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Wireless Sniffing (T0887)	Encrypt Network Traffic (M0808)	Cyber hygiene	Negate, Degrade, Exert	SC-8
		Obfuscation	Negate, Degrade, Exert	**SC-8(1)**
	Minimize Wireless Signal Propagation (M0806)	Standard practice	Negate, Degrade, Exert	SC-40
		Obfuscation	Negate, Degrade, Exert	**SC-40(2)**

5.7 Lateral Movement Tactic

In the six Techniques under Lateral Movement, the adversary is trying to move through the ICS environment.

Relationships: Default Credentials (T0812) is similar to T1078.001, Valid Accounts: Default Accounts. Since T0812 involves vendor default passwords, Present Deceptive Information and Cross Enterprise Usage Analysis (used for T1078) are not relevant. Exploitation of Remote Services (T0866) and Remote Services (T0886) have already appeared under Initial Access. Lateral Tool Transfer (T0867) is similar to the corresponding Technique in A4E (T1570). Valid Accounts (T0859) has already appeared under Persistence and is similar to the corresponding Technique in A4E (T1078).

Table 25. Lateral Movement Tactic for ICS

ATT&CK Techniques (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Default Credentials (T0812)	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
	Password Policies (M0927)	Cyber hygiene	Preempt, Exert	IA-5
	Application Developer Guidance (M0913)	Standard practice	Preempt, Exert	AT-3, **IA-5(7), SA-8**

ATT&CK Techniques (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Exploitation of Remote Services (T0866)	Application Isolation and Sandboxing (M0948)	Predefined Segmentation	Contain, Delay, Preempt	**AC-4(21), AC-6(4), SC-39, CM-7(6)**
	Disable or Remove Feature or Program (M0942)	Restriction	Exert, Preempt	**CM-7(2)**
		Cyber hygiene	Exert, Preempt	CM-7, SC-41
	Exploit Protection (M0950)	Integrity Checks	Delay, Exert, Detect	**AC-4(8)**
		Behavior Validation	Detect	**IR-4(13)**
		Synthetic Diversity, Restriction	Preempt, Exert	SI-16
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), AC-4(21), SC-3, SC-7, SC-7(21), SC-7(22)**
	Privileged Account Management (M0926)	Standard practice	Degrade, Exert	AC-2
		Trust-Based Privilege Management	Degrade, Exert	**AC-6(5)**
	Threat Intelligence Program (M0919)	Dynamic Threat Awareness	Exert, Preempt	**PM-16, RA-3(3)**
	Update Software (M0951)	Cyber hygiene	Preempt, Negate, Degrade, Exert	SI-2
	Vulnerability Scanning (M0916)	Cyber hygiene	Detect, Reveal, Shorten	RA-5
	Maintain Deception Environment (CM1202)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Endpoint Behavior Analysis (CM2103)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)

ATT&CK Techniques (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Monitor Network Usage (CM2147)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)
Lateral Tool Transfer (T0867)	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
		Monitoring and Damage Assessment	Detect	**SI-4(4)**
		Dynamic Threat Awareness	Degrade, Exert, Detect	**PM-16(1)**
	Maintain Deception Environment (CM1202)	Monitoring and Damage Assessment, Forensic and Behavioral Analysis	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Monitor the File System (CM2133)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(24)
Program Download (T0843)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3, **CM-5, CM-6**
		Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(7)**
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(6)**
		Standard practice	Contain, Exert	AC-3

ATT&CK Techniques (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Network Segmentation (M0930)	Predefined Segmentation	Contain, Exert	**AC-4(2), SC-3, SC-7, SC-7(21)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, **AC-4, AC-4(1),** SC-7
		Integrity Checks	Negate, Contain, Degrade, Exert	**AC-4(8)**
	Audit (M0947)	Integrity Checks	Detect, Shorten	**CM-14**, SI-7, **SI-7(6), SI-7(12)**
		Provenance Tracking	Detect, Exert	**SI-7(15)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
Remote Services (T0886)	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(7), AC-3(13)**
		Cyber hygiene	Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Preempt, Contain, Exert	**AC-4(21), AC-4(2), SC-7, SC-7(21), SC-7(22)**
	Password Policies (M0927)	Cyber hygiene	Degrade, Exert	IA-5
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
		Monitoring and Damage Assessment,	Detect	SC-26

ATT&CK Techniques (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Maintain Deception Environment (CM1202)	Forensic and Behavioral Analysis		
		Misdirection	Deceive, Divert	SC-26
		Predefined Segmentation	Negate, Contain	SC-7(21)
		Disinformation	Deceive	SC-30 (4)
	Dynamically Restrict Traffic or Isolate Resources (CM1208)	Dynamic Reconfiguration	Contain, Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Dynamic Segmentation and Isolation	Preempt, Contain, Shorten, Reduce	SC-7(20)
	Modulate Information Flows (CM1253)	Predefined Segmentation, Trust-Based Privilege Management	Negate, Exert	SC-7(15)
	Cross-Enterprise Behavior Analysis (CM2118)	Sensor Fusion and Analysis	Detect	AU-6(3), AU-6(5)
Valid Accounts (T0859)	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
	Account Use Policies (M0936)	Standard practice	Negate, Delay, Exert	**AC-2(11), AC-7**, IA-5
	Active Directory Configuration (M0915)	Standard practice	Negate, Exert	**AC-2, AC-2(1)**
		Consistency Analysis	Negate, Delay, Degrade, Exert	**AC-6(7)**
	Application Developer Guidance (M0913)	Standard practice	Preempt, Exert	AT-3**, IA-5(7), SA-8**
	Multi-factor Authentication (M0932)	Standard practice	Negate, Exert	IA-2, **IA-2(1), IA-2(2), IA-2(6)**
	Password Policies (M0927)	Cyber hygiene	Degrade, Exert	IA-5
	Privileged Account Management (M0926)	Cyber hygiene	Negate, Exert	AC-2
		Trust-Based Privilege Management	Negate, Exert	**AC-6(5)**
		Trust-Based Privilege Management, Consistency Analysis	Negate, Exert	**AC-6(7)**

ATT&CK Techniques (*Lateral Movement*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
		Trust-Based Privilege Management, Consistency Analysis	Negate, Exert	**AC-6(7)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, **AC-4, AC-4(1),** SC-7
	Audit (M0947)	Standard practice	Detect	SI-7
		Consistency Analysis	Detect	**CA-7(5)**
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Exert	SC-30 (4)
		Tainting	Detect	SI-20
	Cross Enterprise Account Usage Analysis (CM2113)	Sensor Fusion and Analysis	Detect	AU-6(3), SI-4(16)

5.8 Collection Tactic

In the 10 Techniques under Collection, the adversary is trying to gather data of interest and domain knowledge on the ICS environment to inform their goal.

Relationships: A number of the Techniques are similar to those of the same name in A4E, including Automated Collection (T0802) and T1119, Data from Information Repositories (T0811) and T1213, Man in the Middle (T0830) and T1557, and Screen Capture (T0852) and T1113. However, differences can be noted: For Automated Collection, T1119 uses M1041, Encrypt Sensitive Information, and M1029, Remote Data Storage. Those mitigations are not used in A4I since they are not applicable to operational data on controllers and relays. Many of the Candidate Mitigations for T1119 are similarly inapplicable (e.g., Dynamic Data Location, Fragment Information). Active uses of Deception for T1557 are inapplicable in A4I. No A4E Technique corresponds to Detect Operating Mode (T0868), I/O Image (T0877), Monitor Process State (T0801), Point & Tag Identification (T0861), and Program Upload (T0845). Wireless Sniffing (T0887) has been covered under Discovery.

Table 26. Collection Tactic for ICS

ATT&CK Techniques (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Automated Collection (T0802)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), AC-4(21), SC-7, SC-**

ATT&CK Techniques (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
				7(21), SC-7(22), SC-7(29)
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30 (4)
		Tainting	Scrutinize, Reveal	SI-20
	Passive Decoys (CM1204)	Misdirection	Deceive, Detect	SC-26
	Endpoint Behavior Analysis (CM2103)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12)
Data from Information Repositories (T0811)	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Delay, Exert	SC-28
		Obfuscation	Negate, Delay, Exert	**SC-28(1)**
	Privileged Account Management (M0926)	Cyber hygiene	Negate, Exert	AC-2
		Trust-Based Privilege Management	Negate, Exert	**AC-6(5)**
	Restrict File and Directory Permissions (M0922)	Trust-Based Privilege Management	Negate, Delay, Exert	AC-6
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
		Trust-Based Privilege Management, Consistency Analysis	Negate, Exert	**AC-6(7)**
	User Training (M0917)	Cyber hygiene	Negate, Degrade, Exert	AT-2
	Audit (M0947)	Consistency Analysis	Negate, Exert	**AC-6(7)**
	Present Deceptive Information (CM1201)	Disinformation	Deceive, Delay, Degrade, Exert	SC-30 (4)
		Tainting	Scrutinize, Reveal	SI-20
	Account Monitoring (CM2121)	Monitoring and Damage Assessment, Behavior Validation	Detect	AC-2(12), IR-4(13)
Detect Operating Mode (T0868)	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	AC-3, **AC-3(12), AC-3(13)**
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2

ATT&CK Techniques (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Negate, Degrade, Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Passive Decoys (CM1204)	Misdirection	Deceive	SC-26
I/O Image (T0877)	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Passive Decoys (CM1204)	Monitoring and Damage Assessment	Detect	SC-26
		Misdirection	Deceive, Divert	SC-26
Man in the Middle (T0830)	Communication Authenticity (M0802)	Standard practice	Detect	SC-8, SC-23
	Out-of-Band Communications Channel (M0810)	Path Diversity	Shorten, Detect	SC-37
		Integrity Checks	Shorten, Detect	**SI-7**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
		Obfuscation, Integrity Checks	Negate, Degrade, Exert	**IA-3(1)**

ATT&CK Techniques (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Disable or Remove Feature or Program (M0942)	Standard practice	Preempt, Negate, Degrade, Exert	CM-7**, CM-7(1), SC-41**
		Restriction	Preempt, Negate, Degrade, Exert	**CM-7(2)**
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**SC-7, SC-7(21), SC-7(22)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Audit (M0947)	Standard practice	Negate, Contain, Degrade, Exert	**AC-4, AC-6**
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(4), SI-4(25)
Monitor Process State (T0801)	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(4), SI-4(25)
Point & Tag Identification (T0861)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Negate, Degrade, Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3

ATT&CK Techniques (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Present Deceptive Information (CM1201)	Disinformation	Exert	SC-30 (4)
		Tainting	Detect	SI-20
	Passive Decoys (CM1204)	Misdirection	Deceive	SC-26
Program Upload (T0845)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3, **CM-5, CM-6**
		Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(7)**
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), SC-3, SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, **AC-4, AC-4(1),** SC-7
		Integrity Checks	Negate, Contain, Degrade, Exert	**AC-4(8)**

ATT&CK Techniques (*Collection*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Passive Decoys (CM1204)	Misdirection	Deceive, Detect	SC-26
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
Screen Capture (T0852)	Application- or Utility-Specific Monitoring (CM2120)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
	Analyze Logs (CM2105)	Monitoring and Damage Assessment	Detect	AC-2(12)
		Dynamic Resource Awareness	Detect	SI-4(16)
Wireless Sniffing (T0887)	Encrypt Network Traffic (M0808)	Cyber hygiene	Negate, Degrade, Exert	SC-8
		Obfuscation	Negate, Degrade, Exert	**SC-8(1)**
	Minimize Wireless Signal Propagation (M0806)	Standard practice	Negate, Degrade, Exert	SC-40
		Obfuscation	Negate, Degrade, Exert	**SC-40(2)**

5.9 Command and Control Tactic

In the three Techniques under Collection, the adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to the ICS environment.

Relationships: Commonly Used Port (T0885) has some similarity to Application Layer Protocol (T1071) in A4E. Connection Proxy (T0884) is similar to Proxy (T1090). Standard Application Layer Protocol (T0869) is similar to Application Layer Protocol (T1071).

Table 27. Command and Control Tactic for ICS

ATT&CK Techniques (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Commonly Used Port (T0885)	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Disable or Remove Feature or Program (M0942)	Restriction	Exert, Preempt	**CM-7(2)**
		Cyber hygiene	Exert, Preempt	CM-7, **SC-41**
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4

ATT&CK Techniques (*Command and Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Monitoring and Damage Assessment	Detect	**SI-4(4)**
		Dynamic Threat Awareness	Degrade, Exert, Detect	**PM-16(1)**
	Network Segmentation (M0930)	Standard practice	Negate, Contain, Degrade, Exert	AC-3
		Predefined Segmentation	Preempt, Negate, Degrade, Exert	**AC-4(2), AC-4(21), SC-7, SC-7(22)**
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4)
	Analyze Network Traffic Content (CM2141)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(10), SI-4(25)
Connection Proxy (T0884)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
		Monitoring and Damage Assessment	Detect	**SI-4(4)**
		Dynamic Threat Awareness	Degrade, Exert, Detect	**PM-16(1)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	SSL/TLS Inspection (M0920)	Monitoring and Damage Assessment	Detect	**IR-4(13), SI-4(10), SI-4(25)**
Standard Application Layer Protocol (T0869)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Network Intrusion Prevention (M0931)	Standard practice	Negate, Degrade, Exert	SI-4
	Network Segmentation (M0930)	Standard practice	Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), AC-4(21), SC-7, SC-7(22)**
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(4), SI-4(10)
	Analyze Network Traffic Content (CM2141)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(10), SI-4(25)

5.10 Inhibit Response Function Tactic

In the 13 Techniques under Inhibit Response Function, the adversary is trying to prevent safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.

Relationships: Many of the Techniques under this Tactic have no corresponding A4E Technique. These include Activate Firmware Update Mode (T0800), Alarm Suppression (T0878), Block Command Message (T0803), Block Reporting Message (T0804), and Block Serial COM (T0805). Some correspond to Techniques under the Impact Tactic in A4E: Data Destruction (T0809), corresponding to T1485; Denial of Service (T0814), corresponding to T1499 (and to a lesser extent T1498); and Device Restart/Shutdown (T0816), corresponding to System Shutdown/Reboot (T1529). Rootkit (T0851) has appeared under Evasion. System Firmware (T0857) has appeared under Persistence.

Table 28. Inhibit Response Function Tactic for ICS

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Activate Firmware Update Mode (T0800)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3, **CM-5, CM-6**
		Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(13)**
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
		Standard practice	Negate, Degrade, Exert	**AC-3, AC-17, CM-5, CM-6**
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13)

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Alarm Suppression (T0878)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-3, SC-7, SC-7(21), SC-7(29)**
	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Detect	SC-37
	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Block Command Message (T0803)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Detect	SC-37
	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Block Reporting Message (T0804)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Detect	SC-37
	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Block Serial COM (T0805)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Detect	SC-37
	Static Network Configuration (M0814)	Cyber hygiene	Negate	CM-7
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Data Destruction (T0809)	Privileged Account Management (M0926)	Standard practice	Degrade, Exert	AC-2
		Trust-Based Privilege Management	Degrade, Exert	**AC-6(5)**
	Restrict File and Directory Permissions (M0922)	Trust-Based Privilege Management	Negate, Delay, Exert	AC-6
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Replication	Shorten, Reduce	**CP-9(6)**
	Validate Data Quality (CM1230)	Integrity Checks	Detect	SA-9(7), SI-7(1)
	Perform Mission Damage Assessment (CM1222)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Switch to Protected Hot Standby (CM1242)	Replication	Shorten, Reduce	CP-9(6)
		Predefined Segmentation	Contain, Exert	AC-4(2)
		Integrity Checks	Negate, Exert	AC-4(8)
		Dynamic Reconfiguration	Shorten, Reduce	IR-4(2)
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	CP-2(5)

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Process Monitoring (CM2115)	Monitoring and Damage Assessment, Behavior Validation	Detect	IR-4(13), SI-4(2)
Denial of Service (T0814)	Watchdog Timers (M0815)	Behavior Validation, Adaptive Management	Detect, Shorten	SC-36(1)
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Detect	SC-26
	Defend Against DoS (CM1247)	Adaptive Management	Shorten	AC-4(3)
		Surplus Capacity, Dynamic Resource Allocation	Shorten	SC-5(2)
		Monitoring and Damage Assessment	Detect	SC-5(3)
Device Restart/Shutdown (T0816)	Disable or Remove Feature or Program (M0942)	Cyber hygiene	Negate, Degrade, Exert	CM-7
		Restriction	Preempt	**CM-7(2)**
	Authorization Enforcement (M0800)	Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(13)**
		Cyber hygiene	Exert	AC-3
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(22), SC-7(29)**
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Manipulate I/O Image (T0835)	Mitigation Limited or Not Effective (M0816)	Not applicable	—	—
	Passive Decoys (CM1204)	Misdirection	Divert, Deceive, Delay	SC-26
Modify Alarm Settings (T0838)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3, **CM-5, CM-6**
		Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(13)**
	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
		Standard practice	Negate, Degrade, Exert	**AC-3, CM-5, CM-6**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(22), SC-7(29)**

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Rootkit (T0851)	Code Signing (M0945)	Integrity Checks	Detect, Negate	SI-7, **SI-7(1), SI-7(6)**
	Audit (M0947)	Integrity Checks	Shorten, Detect	**CM-14,** SI-7, **SI-7(6), SI-7(12), SI-7(15)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
Service Stop (T0881)	Network Segmentation (M0930)	Standard practice	Contain, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-3, SC-7, SC-7(22), SC-7(29)**
	Restrict File and Directory Permissions (M0922)	Attribute-Based Usage Restriction	Negate, Delay, Exert	AC-6
	Restrict Registry Permissions (M0924)	Attribute-Based Usage Restriction	Negate, Delay, Exert	AC-6
	User Account Management (M0918)	Cyber hygiene	Delay, Exert	AC-2
		Trust-Based Privilege Management, Consistency Analysis	Negate, Exert	**AC-6(7)**
	Monitor Platform Status (CM2144)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2)
System Firmware (T0857)	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Encrypt Network Traffic (M0808)	Obfuscation	Negate, Degrade, Exert	SC-8, **SC-8(1)**
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3

ATT&CK Techniques (*Inhibit Response Function*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Architectural Diversity	Negate, Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Boot Integrity (M0946)	Integrity Checks	Detect	**SI-6**, SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Code Signing (M0945)	Integrity Checks	Detect	**CM-14,** SI-7, **SI-7(1), SI-7(6)**
		Provenance Tracking	Detect	**CM-14, SI-7(15), SR-4, SR-4(1), SR-4(2)**
	Encrypt Sensitive Information (M0941)	Obfuscation	Negate, Delay, Exert	SC-28, **SC-28(1)**
	Network Segmentation (M0930)	Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), SC-3, SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, **AC-4, AC-4(1),** SC-7
		Integrity Checks	Negate, Contain, Degrade, Exert	**AC-4(8)**
	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Hardware-Based Protection of Firmware (CM1254)	Integrity Checks	Negate, Preempt	SC-51

5.11 Impair Process Control Tactic

In the five Techniques under Impair Process Control, the adversary is trying to manipulate, disable, or damage physical control processes.

Relationships: While Brute Force I/O (T0806) does not correspond directly to an A4E Technique, some overlap with Endpoint Denial of Service (T1499) can be found. Similarly, Modify Parameter (T0836) has some overlap with Date Manipulation (T1565). Module Firmware (T0839) has some similarity with Firmware Corruption (T1495), though T1495 is more oriented to denial-of-service. No A4E Techniques correspond to Spoof Reporting Message (T0856) or Unauthorized Command Message (T0855).

Table 29. Impair Process Control Tactic for ICS

ATT&CK Techniques (*Impair Process Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
Brute Force I/O (T0806)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Cyber hygiene	Negate, Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**AC-4(2), SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Cyber hygiene	Negate, Degrade, Exert	AC-3, SC-7
		Adaptive Management	Shorten	**AC-4(3), SI-4(7)**
	Dynamically Restrict Traffic or Isolate Resources (CM1208)	Dynamic Reconfiguration	Degrade, Reduce	IR-4(2), SC-7(20)
	Monitor Network Usage (CM2147)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(11), SI-4(13)
Modify Parameter (T0836)	Authorization Enforcement (M0800)	Standard practice	Negate, Degrade, Exert	AC-3, **CM-5, CM-6**
		Attribute-Based Usage Restriction	Negate, Degrade, Exert	**AC-3(12), AC-3(7)**
	Audit (M0947)	Integrity Checks	Negate, Detect	SI-7, **SI-7(1), SI-7(6), SI-7(12)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Validate Data Properties (CM1237)	Integrity Checks	Delay, Degrade, Exert	SI-7, SI-7(1)
		Calibrated Defense-in-Depth	Delay, Degrade	PL-8(1)
	Validate Output Data (CM1255)	Integrity Checks	Detect, Reduce	SI-15
	Analyze File Contents (CM2106)	Forensic and Behavioral Analysis	Detect	SR-10
Module Firmware (T0839)	Human User Authentication (M0804)	Cyber hygiene	Negate, Degrade, Exert	IA-2
	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23

ATT&CK Techniques (*Impair Process Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Encrypt Network Traffic (M0808)	Standard practice	Negate, Degrade, Exert	SC-8
		Obfuscation, Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
	Access Management (M0801)	Cyber hygiene	Delay, Degrade, Exert	AC-3
		Architectural Diversity	Negate, Delay, Degrade, Exert	**SC-29**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Boot Integrity (M0946)	Integrity Checks	Detect	**SI-6**, SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Code Signing (M0945)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(6), CM-14**
		Provenance Tracking	Detect	**CM-14, SI-7(15), SR-4, SR-4(1), SR-4(3)**
	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Delay, Exert	SC-28
		Obfuscation	Negate, Delay, Exert	**SC-28(1)**
	Network Segmentation (M0930)	Cyber hygiene	Negate, Contain, Degrade, Exert	AC-3
		Predefined Segmentation	Negate, Contain, Degrade, Exert	**AC-4(2), SC-3, SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
	Audit (M0947)	Integrity Checks	Detect	SI-7, **SI-7(1), SI-7(9), SI-7(10)**
	Hardware-Based Protection of Firmware (CM1254)	Integrity Checks	Negate, Preempt	SC-51
Spoof Reporting Message (T0856)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**

ATT&CK Techniques (*Impair Process Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
		Provenance Tracking	Negate, Delay, Degrade, Exert	**AC-4(17)**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Cyber hygiene	Negate, Contain, Degrade, Exert	AC-3
		Predefined Segmentation	Contain, Exert	**SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	**AC-3(13)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)
Unauthorized Command Message (T0855)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Exert	**SC-29**
	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
		Provenance Tracking	Negate, Delay, Degrade, Exert	**AC-4(17)**
	Software Process and Device Authentication (M0813)	Standard practice	Negate, Degrade, Exert	IA-9, **IA-3**
	Network Segmentation (M0930)	Standard practice	Negate, Contain, Degrade, Exert	AC-3

ATT&CK Techniques (*Impair Process Control*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es), if Any	Potential Effects on ATT&CK Technique	Control(s)
		Predefined Segmentation	Contain, Exert	**SC-7, SC-7(21), SC-7(29)**
	Filter Network Traffic (M0937)	Standard practice	Negate, Contain, Degrade, Exert	AC-3, SC-7
		Attribute-Based Usage Restriction	Negate, Delay, Degrade, Exert	**AC-3(13)**
	Passive Decoys (CM1204)	Misdirection	Deceive, Divert, Negate, Contain	SC-26
	Inspect and Analyze Network Traffic (CM2102)	Monitoring and Damage Assessment	Detect	IR-4(13), SI-4(2), SI-4(4)

5.12 Impact Tactic

In the 12 Techniques under Impact, the adversary is trying to manipulate, disable, or damage physical control processes.

Relationships: Almost all of the Techniques under this Tactic have no counterpart in A4E. These include Damage to Property (T0879), Denial of Control (T0813), Denial of View (T0815), Loss of Control (T0827), Loss of Productivity and Revenue (T0828), Loss of Protection (T0837), Loss of Safety (T0880), Loss of View (T0829), Manipulation of Control (T0831), Manipulation of View (T0832), and Theft of Operational Information (T0882). Loss of Availability (T0826) has some similarities to Endpoint Denial of Service (T1499).

Table 30. Impact Tactic for ICS

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Damage to Property (T0879)	Network Allowlists (M0807)	Standard practice	Negate, Degrade, Exert	AC-3
	Mechanical Protection Layers (M0805)	Calibrated Defense-in-Depth	Preempt, Negate, Exert	**PL-8(1), SA-8(3)**
		Standard practice	Detect	**PE-14(2)**
		Restriction	Preempt, Negate, Exert	**SA-8(2)**
		Architectural Diversity	Preempt, Negate, Exert	**CP-13**
	Safety Instrumented Systems (M0812)	Predefined Segmentation	Negate, Contain, Degrade, Exert	**SC-7**
		Architectural Diversity	Detect, Negate	**SC-29**

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Standard practice	Negate, Degrade, Reduce	**CP-12, IR-4(5)**
	Perform Mission Damage Assessment (CM1222)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Emergency Shutdown (CM1275)	Dynamic Reconfiguration	Shorten, Reduce	IR-4(2), IR-4(3)
		Architectural Diversity	Exert	SC-29
		Standard practice	Shorten, Reduce	CP-2, PE-10, SC-24
	Safe Mode Restart (CM1276)	Adaptive Management	Reduce	CP-12
	Coordinate Responses to Adversity (CM1277)	Consistency Analysis	Shorten, Reduce	CP-2(1)
		Orchestration	Shorten, Reduce	CP-2(5)
		Self-Challenge	Shorten, Reduce	CP-4(5)
		Standard practice	Shorten, Reduce	IR-4, PM-8, PM-9, PM-11, PM-16
Denial of Control (T0813)	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Redundancy of Service (M0811)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Design Diversity	Exert	**CP-11**
		Replication	Shorten, Reduce	**CP-9(6)**
		Predefined Segmentation	Exert	**AC-4(2)**
		Integrity Checks	Exert	**AC-4(8)**
		Dynamic Reconfiguration	Shorten, Reduce	**IR-4(2)**
		Dynamic Reconfiguration, Adaptive	Shorten, Reduce	**CP-2(5)**

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Management, Orchestration		
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
	Defend Failover and Recovery (CM1245)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
	Emergency Shutdown (CM1275)	Dynamic Reconfiguration	Shorten, Reduce	IR-4(2), IR-4(3)
		Architectural Diversity	Exert	SC-29
		Standard practice	Shorten, Reduce	CP-2, PE-10, SC-24
	Safe Mode Restart (CM1276)	Adaptive Management	Reduce	CP-12
	Coordinate Responses to Adversity (CM1277)	Consistency Analysis	Shorten, Reduce	CP-2(1)
		Orchestration	Shorten, Reduce	CP-2(5)

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Denial of View (T0815)	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Redundancy of Service (M0811)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Design Diversity	Negate, Exert	**CP-11**
		Replication	Negate, Shorten, Reduce	**CP-9(6)**
		Predefined Segmentation	Shorten, Reduce	**AC-4(2)**
		Integrity Checks	Exert	**AC-4(8)**
		Dynamic Reconfiguration	Exert	**IR-4(2)**
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	**CP-2(5)**
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
	Defend Failover and Recovery (CM1245)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
Loss of Availability (T0826)	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Redundancy of Service (M0811)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Design Diversity	Shorten, Reduce	**CP-11**
		Replication	Negate, Shorten, Reduce	**CP-9(6)**
		Predefined Segmentation	Exert	**AC-4(2)**
		Integrity Checks	Exert	**AC-4(8)**
		Dynamic Reconfiguration	Shorten, Reduce	**IR-4(2)**
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	**CP-2(5)**
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
	Defend Failover and Recovery (CM1245)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Reconfiguration,	Detect	IR-4(2)

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Functional Relocation of Sensors		
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
	Defend Against DoS (CM1247)	Dynamic Resource Allocation, Surplus Capacity	Shorten, Reduce	SC-5(2)
		Monitoring and Damage Assessment	Detect	SC-5(3)
Loss of Control (T0827)	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Redundancy of Service (M0811)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Design Diversity	Negate, Shorten, Reduce	**CP-11**
		Replication	Shorten, Reduce	**CP-9(6)**
		Predefined Segmentation	Exert	**AC-4(2)**
		Integrity Checks	Exert	**AC-4(8)**
		Dynamic Reconfiguration	Shorten, Reduce	**IR-4(2)**
		Dynamic Reconfiguration, Adaptive Management, Orchestration	Shorten, Reduce	**CP-2(5)**
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
	Emergency Shutdown (CM1275)	Dynamic Reconfiguration	Shorten, Reduce	IR-4(2), IR-4(3)
		Architectural Diversity	Degrade, Exert	SC-29
		Standard practice	Shorten, Reduce	CP-2, PE-10, SC-24
	Safe Mode Restart (CM1276)	Adaptive Management	Reduce	CP-12
	Coordinate Responses to Adversity (CM1277)	Consistency Analysis	Shorten, Reduce	CP-2(1)
		Orchestration	Shorten, Reduce	CP-2(5)
		Self-Challenge	Shorten, Reduce	CP-4(5)
		Standard practice	Shorten, Reduce	IR-4, PM-8, PM-9, PM-11, PM-16
Loss of Productivity and Revenue (T0828)	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
	Perform Mission Damage Assessment (CM1222)	Mission Dependency and Status Visualization	Detect, Scrutinize	CP-2(8), RA-9
		Sensor Fusion and Analysis, Mission Dependency and Status Visualization	Detect, Scrutinize	SI-4(1)
		Integrity Checks	Detect, Scrutinize	SI-7, SI-7(1)
	Coordinate Responses to Adversity (CM1277)	Consistency Analysis	Shorten, Reduce	CP-2(1)
		Orchestration	Shorten, Reduce	CP-2(5)
		Self-Challenge	Shorten, Reduce	CP-4(5)
		Standard practice	Shorten, Reduce	IR-4, PM-8, PM-9, PM-11, PM-16

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Loss of Protection (T0837)	Monitor Health and Status of Protective Systems (CM2124)	Monitoring and Damage Assessment, Sensor Fusion, and Analysis	Detect	PM-31
Loss of Safety (T0880)	Mechanical Protection Layers (M0805)	Calibrated Defense-in-Depth	Preempt, Negate, Exert	**PL-8(1), SA-8(3)**
		Monitoring and Damage Assessment	Detect	**PE-14(2)**
		Restriction	Preempt, Negate, Exert	**SA-8(2)**
		Architectural Diversity	Preempt, Negate, Exert	**CP-13**
	Safety Instrumented Systems (M0812)	Predefined Segmentation	Negate, Contain, Degrade, Exert	**SC-7**
		Architectural Diversity	Detect, Negate	**SC-29**
		Standard practice	Negate, Degrade, Reduce	**CP-12, IR-4(5)**
	Monitor Health and Status of Protective Systems (CM2124)	Monitoring and Damage Assessment, Sensor Fusion, and Analysis	Detect	PM-31
Loss of View (T0829)	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Redundancy of Service (M0811)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Design Diversity	Negate, Shorten, Reduce	**CP-11**
		Replication	Shorten, Reduce	**CP-9(6)**
		Predefined Segmentation	Exert	**AC-4(2)**
		Integrity Checks	Exert	**AC-4(8)**
		Dynamic Reconfiguration	Shorten, Reduce	**IR-4(2)**
		Dynamic Reconfiguration, Adaptive	Shorten, Reduce	**CP-2(5)**

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Management, Orchestration		
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
Manipulation of Control (T0831)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Exert	**SC-29**
	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
	Defend Failover and Recovery (CM1245)	Adaptive Management, Dynamic Reconfiguration, Orchestration	Shorten, Reduce, Exert	IR-4(3)
		Functional Relocation of Sensors	Detect	SC-48, SC-48 (1)
		Dynamic Reconfiguration, Functional Relocation of Sensors	Detect	IR-4(2)

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
		Dynamic Segmentation and Isolation	Shorten, Reduce, Contain, Exert	SC-7(20)
		Mission Dependency and Status Visualization	Detect	SI-4(1)
		Dynamic Privileges	Contain, Exert	AC-2(6)
	Emergency Shutdown (CM1275)	Dynamic Reconfiguration	Shorten, Reduce	IR-4(2), IR-4(3)
		Architectural Diversity	Exert	SC-29
		Standard practice	Shorten, Reduce	CP-2, PE-10, SC-24
	Safe Mode Restart (CM1276)	Adaptive Management	Reduce	CP-12
	Coordinate Responses to Adversity (CM1277)	Consistency Analysis	Shorten, Reduce	CP-2(1)
		Orchestration	Shorten, Reduce	CP-2(5)
Manipulation of View (T0832)	Communication Authenticity (M0802)	Standard practice	Negate, Degrade, Exert	SC-8, SC-23
		Provenance Tracking	Negate, Degrade, Exert	**AU-10(2)**
		Integrity Checks	Negate, Degrade, Exert	**SC-8(1)**
		Architectural Diversity	Exert	**SC-29**
	Out-of-Band Communications Channel (M0810)	Path Diversity	Negate, Shorten, Reduce	SC-37
	Data Backup (M0953)	Protected Backup and Restore	Shorten, Reduce	CP-9
		Standard practice	Exert	**IR-3**
		Replication	Shorten, Reduce	**CP-9(6)**
		Protected Backup and Restore, Obfuscation, Integrity Checks	Exert	**CP-9(8)**
Theft of Operational	Operational Information Confidentiality (M0809)	Obfuscation	Exert	SC-30
		Integrity Checks	Exert, Detect	**AC-4(8)**

ATT&CK Techniques (*Impact*)	Mitigation (M) Identified in ATT&CK or Candidate Mitigation (CM)	Cyber Resiliency Implementation Approach(es) if Any	Potential Effects on ATT&CK Technique	Control(s)
Information (T0882)	Data Loss Prevention (M0803)	Monitoring and Damage Assessment	Detect	**SC-7(10)**
	Encrypt Sensitive Information (M0941)	Standard practice	Negate, Delay, Exert	SC-28
		Obfuscation	Negate, Delay, Exert	**SC-28(1)**
	Restrict File and Directory Permissions (M0922)	Trust-Based Privilege Management	Negate, Delay, Exert	AC-6
	Present Deceptive Information (CM1201)	Disinformation	Deceive	SC-30(4)

6 Mitigations and Candidate Mitigations for ATT&CK for ICS

This section parallels Section 4, for ATT&CK for ICS. Table 31 lists the Mitigations defined in the ATT&CK for ICS (A4I) knowledge base. Columns 1-2 are taken from Mitigations - attackics (mitre.org). Most A4I Mitigations have an associated control identified from NIST SP 800-53R4; these are in column 3. Since these are base controls related to cyber hygiene or standard practice, they are unchanged in R5. Each A4I Mitigation is characterized in terms of the cyber resiliency approaches (if any) it applies (if any), or as cyber hygiene or standard cybersecurity practice; this is captured in column 4. Many A4I Mitigations (those with identifiers of the form M09##) correspond directly to Mitigations defined in the ATT&CK for Enterprise (A4E) knowledge base. Some also correspond to Candidate Mitigations (CMs) in the ATT&CK for Enterprise mapping. The relationship between an A4I Mitigation, A4E Mitigations and CMs, and cyber resiliency is discussed in the final column. In addition, discussion of proposed changes to the assignment of controls is included in the final column.

Table 31. ATT&CK for ICS Mitigations

Name	ID	R4 Control	R5 Control(s)	Discussion
Access Management	M0801	AC-3	AC-3, **SC-29**	"All devices or systems changes, including all administrative functions, should require authentication" applies cyber hygiene. "Consider using access management technologies to enforce authorization … especially when the device does not inherently provide strong authentication and authorization functions" applies Architectural Diversity, SC-29
Account Use Policies	M0936	IA-5	**AC-2(11), AC-7**, IA-5	In A4I, applies to External Account Services and Valid Accounts; in A4E, applies to Brute Force. IA-5 is questionable. Specific login times, etc.: AC-2(11). Login attempt lockouts: AC-7
Active Directory Configuration	M0915	None	**AC-2, AC-2(1), AC-6(5), AC-6(7)**	In A4E, Trust-Based Privilege Management, uses AC-6(5) for T1072, Software Deployment Tools; other are standard practice, AC-2 and AC-2(1). In A4I, Trust-Based Privilege Management using AC-6(7) applies to Valid Accounts.
Antivirus/Antimalware	M0949	SI-3	SI-3, **CM-4, AC-4, AT-2, AT-3**	In A4E, T1566, Phishing, uses AC-4, SI-3, AT-2, AT-3. CM-4 supports validation of products in a test environment, which is not part of the A4E Mitigation.
Application Developer Guidance	M0913	AT-3	AT-3**, IA-5(7), SA-8**	This mitigation is standard practice. (The recommended additional controls are not cyber resiliency but are standard practice.)

Name	ID	R4 Control	R5 Control(s)	Discussion
Application Isolation and Sandboxing	M0948	SI-3	SI-3, **AC-4(21), AC-6(4), CM-7(2), CM-7(6), SC-18(5), SC-39**	The assignment of SI-3 (Malicious Code Protection) seems inappropriate, except for Drive-by Compromise. In A4E, the use of M1048 is standard practice for T1559, Inter-Process Communication. Most other uses apply Predefined Segmentation, using one or more of AC-4(21), AC-6(4), SC-18 (5), SC-39, and CM-7(6), depending on the ATT&CK Technique. For T1610, the Mitigation uses Restriction – CM-7(2). In A4I, the uses are for TTPs on the IT network, and can apply Predefined Segmentation.
Audit	M0947	SI-7	**AC-4, AC-6, AC-6(7), CM-14, RA-5**, SI-7, **SI-7(6), SI-7(12), SI-7(15)**	Note that this mitigation does not refer to audit in the sense of the AU control family. It involves a variety of forms of scrutiny. Scans are cyber hygiene, RA-5. Integrity Checks are SI-7 and its enhancements.
Authorization Enforcement	M0800	AC-3	AC-3, **AC-3(12), AC-3(13), CM-5, CM-6**	Basic use of access control mechanisms is cyber hygiene, using AC-3 and sometimes CM-5 and CM-6. Role-based access control applies Trust-Based Privilege Management and/or Attribute-Based Usage Restriction, using AC-3(12) and AC-3(13).
Boot Integrity	M0946	SI-7	**SI-6**, SI-7, **SI-7(1), SI-7(9), SI-7(10)**	All uses apply Integrity Checks.
Code Signing	M0945	SI-7	**CM-7(5), CM-14, SC-28(3),** SI-7, **SI-7(1), SI-7(15), SR-4, SR-4(1), SR-4(3)**	Uses of code signing in A4I involve greater variation than in A4E. Uses which restrict the installation of software or firmware based on digital signatures apply Provenance Tracking and some combination of CM-14, SI-7(15), SR-4(1), and SR-4(3). (The SR controls apply when the vendor is involved.) Uses which rely on digital signatures to check that assets have not been changed apply Integrity Checks and some combination of SI-7, SI-7(1), and SI-7(6). For T0863, User Execution, CM-7(5) applies, in addition to CM-14, SI-7, and SI-7(15). For T0873, SC-28(3) applies to the protection of cryptographic keys.
Communication Authenticity	M0802	SC-8, SC-23	SC-8, SC-23, **SC-8(1), AU-10(2), SC-29**	Uses involving protocol checking are standard practice, using SC-8 and SC-23. Uses involving digital signatures apply Integrity Checks and SC-8(1) together with Provenance Tracking and AU-10(2). Uses involving bump-in-the-wire devices or VPNs apply Architectural Diversity and SC-29.

Name	ID	R4 Control	R5 Control(s)	Discussion
Data Backup	M0953	CP-9	CP-9, **CP-9(6), CP-9(8), IR-3**	CP-9, CP-9(6), and CP-9(8), as used in the mitigation, apply cyber resiliency. (A more generic use of CP-9, with no protection of backups, is cyber hygiene.) The mitigation differs from its counterpart in A4E in its use of maintaining and exercising incident response plans; IR-3 is standard practice.
Data Loss Prevention	M0803	None	**SC-7, SC-7(10)**	SC-7(10) applies Monitoring and Damage Assessment to identify exfiltration attempts, and Non-Persistent Connectivity to thwart such attempts. In so doing, it relies on its base control, SC-7, which applies Predefined Segmentation.
Disable or Remove Feature or Program	M0942	CM-7	CM-7, **CM-7(1), CM-7(2), SC-41**	Removing or restricting features or functions applies Restriction, using CM-7(2), which involves CM-7 as cyber hygiene; removal can Preempt, while restricting can Negate, Degrade, or Exert. Closing ports and protocols uses CM-7, CM-7(1), and SC-41 as standard practice.
Encrypt Network Traffic	M0808	SC-8	SC-8, **SC-8(1)**	SC-8, which is standard practice, by itself does not specify encryption. SC-8(1) calls for cryptographic protection. For T0860, Wireless Compromise, and for System Firmware and Module Firmware, the use applies Integrity Checks. Other uses apply Obfuscation. (System Firmware and Module Firmware use both Obfuscation and Integrity Checks.)
Encrypt Sensitive Information	M0941	SC-28	SC-28, **SC-28(1)**	SC-28 is standard practice in most cases, cyber hygiene in the case of removable devices and media. SC-28(1) applies Obfuscation and sometimes Integrity Checks.
Execution Prevention	M0938	SI-3	SI-3, **CM-7(2), CM-7(4)**	SI-3 (Malicious Code Protection) is cyber hygiene. CM-7(2) applies Restriction. CM-7(4) applies Purposing and is used in conjunction with CM-7(2) for uses of execution prevention or application control tools.
Exploit Protection	M0950	SI-16	SI-16, **AC-4(8), IR-4(13), SI-7, SC-7(17)**	SI-16 applies Restriction and, when linked with EMET or WDEG, Synthetic Diversity. For Drive-By Compromise, T1189, A4E provides a more detailed description, mapped to AC-4(8) and IR-4(13). In A4E, SI-16 is used only in CM1152, Defend Against Memory Attacks, for T1055.

Name	ID	R4 Control	R5 Control(s)	Discussion
Filter Network Traffic	M0937	AC-3, SC-7	AC-3, **AC-3(13), AC-4, AC-4(1), AC-4(3), AC-4(8), AC-4(17),** SC-7, **SI-4(7)**	Basic filtering via allowlists and denylists are cyber hygiene, using AC-3 and SC-7. (While SC-7 is a cyber resiliency control, its use in this context is not specifically cyber resiliency.) More nuanced filtering can apply Adaptive Management, Attribute-Based Usage, Restriction, Trust-Based Privilege Management, Integrity Checks, or Provenance Tracking.
Human User Authentication	M0804	IA-2	**AC-3**, **AC-17, CM-5, CM-6,** IA-2	IA-2 is cyber hygiene. AC-3, AC-17, CM-5, and CM-6 are standard practice.
Limit Access to Resource Over Network	M0935	AC-3, SC-7	AC-3, **AC-6, AC-17**, SC-7	All uses are standard practice. Some uses in A4E are described in greater detail and thus apply different controls.
Limit Hardware Installation	M0934	MP-7	MP-7	MP-7 is cyber hygiene. Some uses in A4E are described in greater detail and thus apply different controls.
Mechanical Protection Layers	M0805	None	**PL-8(1), SA-8(3), PE-14(2), SA-8(2), CP-13**	This Mitigation applies Calibrated Defense-in-Depth, Restriction, and Architectural Diversity. It is supported by PE-14(2), which is standard practice.
Minimize Wireless Signal Propagation	M0806	SC-40	SC-40, **SC-40(2)**	SC-40 is standard practice. SC-40(2) applies Obfuscation.
Mitigation Limited or Not Effective	M0816	None	—	This Mitigation is a placeholder.
Multi-factor Authentication	M0932	IA-2	IA-2, **IA-2(1), IA-2(2), IA-2(6)**	Use of Multi-Factor Authentication is standard practice. The use of a separate device (IA-2(6)) applies Path Diversity and Calibrated Defense-in-Depth, and significantly enhances the effectiveness of the Mitigation.
Network Allowlists	M0807	AC-3	AC-3, **AC-4(17)**	Most uses are standard practice, where descriptions are of the form “Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services”. Provenance Tracking is used in a few cases (e.g., T0848).
Network Intrusion Prevention	M0931	SI-4	**PM-16(1),** SI-4, **SI-4(4)**	SI-4 is standard practice. For Commonly Used Port, Connection Proxy, and Lateral Tool Transfer, SI-4(4) applies Monitoring and Damage Assessment, and looks for C2 protocol signatures, which are maintained as current by applying Dynamic Threat Awareness and PM-16(1).

Name	ID	R4 Control	R5 Control(s)	Discussion
Network Segmentation	M0930	AC-3	AC-3, **AC-4(2), AC-4(21), SC-3, SC-7, SC-7(21), SC-7(22), SC-7(29)**	The uses of AC-3 in this mitigation are standard practice rather than cyber hygiene. Most uses (e.g., "Segment operational network") of the mitigation apply Predefined Segmentation (and sometimes Integrity Checks), via SC-7 and/or its control enhancements. Some uses also apply enhancements to AC-4 (Information Flow Enforcement). More specifically, • Uses of Predefined Segmentation to mitigate observation, collection, or exfiltration of information apply AC-4(2), AC-4(21), SC-7, and SC-7(22). • Uses of Predefined Segmentation to mitigate manipulation apply AC-4(2), SC-7, SC-7(22), and SC-7(29). • Uses of Predefined Segmentation to mitigate attacks on security functions apply AC-4(2), SC-3, SC-7(21), and SC-7(29).
Operating System Configuration	M0928	CM-7	CM-7, **CM-7(2)**	CM-7 is cyber hygiene. Use of the mitigation for T0847 applies Restriction, CM-7(2).
Operational Information Confidentiality	M0809	None	**SC-30**	As noted in the mitigation description, the uses of Obfuscation must be applied carefully to avoid interfering with critical processes. Apply the *Make Deception and Unpredictability Effects User-Transparent* Cyber Resiliency Design Principle.
Out-of-Band Communications Channel	M0810	SC-37	SC-37, **SI-7**	The mitigation applies Path Diversity (SC-37) by providing an out-of-band communications channel. Its use against MitM also applies Integrity Checks.
Password Policies	M0927	IA-5	IA-5	IA-5 is cyber hygiene.
Privileged Account Management	M0926	AC-2	AC-2, **AC-6(5)**	Uses of this do apply AC-2, as standard practice. However, they either apply least privilege or minimized permissions, using AC-6(5), Trust-Based Privilege Management.
Redundancy of Service	M0811	CP-9	**AC-4(2), AC-4(8), CP-2(5),** CP-9, **CP-9(6), CP-11, IR-4(2)**	The mitigation applies many of the controls from CM1142, Switch to Protected Hot Shadow.CP-11 relates to the use of the Parallel Redundancy Protocol. Note that Predefined Segmentation (AC-4(2)) and Integrity Checks (AC-4(8)) are not essential to the mitigation but will greatly enhance its effectiveness.

Name	ID	R4 Control	R5 Control(s)	Discussion
Restrict File and Directory Permissions	M0922	AC-6	AC-6	The mitigation applies Trust-Based Privilege Management or Attribute-Based Usage Restriction, depending on the A4I Technique. Note that there is considerably less variation across the detailed descriptions for M0922 than there is for the corresponding A4E Mitigation.
Restrict Library Loading	M0944	CP-7	**CM-7, CM-7(4)**	CM-7, Least Functionality, is standard practice. CM-7(4) applies Purposing.
Restrict Registry Permissions	M0924	AC-6	AC-6	The mitigation applies Attribute-Based Usage Restriction.
Restrict Web-Based Content	M0921	SC-18	**CM-7(5),** SC-18, **SC-7**	The uses of CM-7(5) and SC-7 in this mitigation are standard practice.
SSL/TLS Inspection	M0920	None	**IR-4(13), SI-4(10), SI-4(25)**	The mitigation applies Monitoring and Damage Assessment, via IR-4(13), and via the two SI-4 control enhancements to enable inspection of SSL/TLS traffic.
Safety Instrumented Systems	M0812	None	**SC-7, SC-29, CP-12, IR-4(5)**	The mitigation applies SC-7 and Predefined Segmentation, together with Architectural Diversity (SC-29). Note that no control in NIST SP 800-53R5 specifies a Safety Instrumented System (SIS). The cyber resiliency controls and approaches cited here enhance the effectiveness of the SIS. CP-12, Safe Mode, and IR-4(5), Incident Handling | Automatic Disabling of System, are not cyber resiliency controls, but should be standard practice.
Software Configuration	M0954	CM-7	CM-7	Unlike A4E, A4I uses this mitigation sparingly and without variations as cyber hygiene.
Software Process and Device Authentication	M0813	IA-9	IA-9, **IA-3, IA-3(1), PL-8(1), SC-29**	Standard practice when uses are of the form “Devices should authentical all messages” or “Authenticate connections.” Note that these uses typically involve IA-3 (Device I&A) as well as IA-9 (Service I&A). When cryptographic protection is also involved, the mitigation applies Obfuscation and Integrity Checks, sometimes subsuming A4E CM1125, Authenticate Devices, IA-3(1). For Wireless Compromise, M0813 also applies Calibrated Defense-in-Depth (PL-8(1)) and Architectural Diversity (SC-29).
Static Network Configuration	M0814	CM-7	CM-7	All uses are cyber hygiene, CM-7.

Name	ID	R4 Control	R5 Control(s)	Discussion
Supply Chain Management	M0817	SA-12	SA-12	The described use of SA-12 is standard practice.
Threat Intelligence Program	M0919	None	**PM-16, RA-3(3)**	M0919 applies Dynamic Threat Awareness, using PM-16 and RA-3(3).
Update Software	M0951	SI-2	SI-2, **MA-3(6), RA-5**	SI-2 is cyber hygiene. Patch management – which may involve non-routine activities, so is standard practice – involves MA-3(6) and RA-5.
User Account Management	M0918	AC-2	AC-2, **AC-6(7)**	AC-2 is cyber hygiene. Some uses include AC-6(7), Trust-Based Privilege Management and Consistency Checking.
User Training	M0917	AT-2	AT-2, **AT-2(4)**	AT-2 is cyber hygiene. AT-2(4) is standard practice. The controls for M0917 are a subset of those for M1017.
Vulnerability Scanning	M0916	RA-5	RA-5, **SA-9(7), SA-11(4), SR-4(3), SR-4(4)**	RA-5 is cyber hygiene and SA-11(4) is standard practice. For Supply Chain Compromise, SA-9(7) applies Integrity Checks, while SR-4(3) and SR-4(4) apply Provenance Tracking.
Watchdog Timers	M0815	None	**SI-4(2), SI-4(7), SI-4(16)**	SI-4(2) and SI-4(7) apply Monitoring and Damage Assessment. SI-4(16) applies Dynamic Resource Awareness and enables discernment of whether lack of responsiveness is due to lack of expected stimuli from other system elements.

Table 32 lists the Candidate Mitigations defined for ATT&CK for ICS.

Table 32. Candidate Mitigations for ATT&CK for ICS

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1201	**Present Deceptive Information**	SC-30(4), SI-20	Present deceptive information about systems, data, processes, and users. Monitor uses or search for presence of that information.	Disinformation, Tainting
CM1202	**Maintain Deception Environment**	SC-7(21), SC-26, SC-30(4)	Maintain a distinct subsystem or a set of components specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Disinformation, Predefined Segmentation

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1204	**Passive Decoys**	SC-26, SC-29	Use factitious systems or resources to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities.	Misdirection
CM1205	**Component Provenance Validation**	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4), SR-11(3)	Validate the provenance of system components.	Provenance Tracking
CM1207	**Adversarial Simulation**	CA-8, CA-8(1), CA-8(2), SC-7(10)	Simulate adversary activities to test the effectiveness of system protections and detection mechanisms.	Self-Challenge
CM1208	**Dynamically Restrict Traffic or Isolate Resources**	AU-5(3), IR-4(2), SC-7(20)	Dynamically reconfigure networking to restrict network traffic or isolate resources.	Dynamic Resource Allocation, Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation and Isolation
CM1209	**Virtual Sandbox**	SC-7(20), SI-14	Use virtualization to create a controlled execution environment, which is expunged after execution terminates.	Non-Persistent Services, Dynamic Segmentation and Isolation
CM1222	**Perform Mission Damage Assessment**	CP-2(8), RA-9, SI-4(1), SI-7, SI-7(1)	Determine the mission consequences of adversary activities.	Sensor Fusion and Analysis, Mission Dependency and Status Visualization, Integrity Checks
CM1223	**Active Decoys**	SC-26, SC-35, SC-44, SA-23	Use one or more factitious systems or other resources to identify malicious sites, interact with the adversary, actively probe for malicious code, and observe adversary TTPs.	Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation and Isolation, Specialization
CM1226	**Enhanced Authentication**	IA-2(13), IA-10, CP-13, SC-47	Use situation-specific, risk-adaptive, or out-of-band authentication.	Adaptive Management, Calibrated Defense-in-Depth, Architectural Diversity, Design Diversity, Path Diversity, Dynamic Privileges

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1227	**Minimize Duration of Connection or Session**	AC-12, SC-7(10), SC-10, SI-14 (3)	Minimize the time period for which a connection remains open or a session remains active, requiring reauthorization to reestablish connectivity.	Non-Persistent Services, Non-Persistent Connectivity
CM1230	**Validate Data Quality**	SA-9(7), SI-7(1)	Validate data quality (e.g., integrity, consistency, correctness).	Integrity Checks
CM1234	**Refresh Selected Applications or Components**	SI-14 (1)	Refresh software, firmware, or data from a trusted source.	Non-Persistent Services, Non-Persistent Information, Provenance Tracking
CM1237	**Validate Data Properties**	PL-8(1), SC-16(1), SC-16(3), SI-7, SI-7(1)	Validate data properties (including binaries, metadata, and cryptographic bindings) to defend against modification or fabrication.	Integrity Checks, Calibrated Defense-in-Depth
CM1242	**Switch to Protected Hot Standby**	AC-4(2), AC-4(8), CP-2(5), CP-9(6), IR-4(2)	Switch (failover) to a duplicate system in a protected enclave which, subject to additional quality controls on data and software updates, mirrors the system which has been compromised.	Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication, Predefined Segmentation, Integrity Checks
CM1245	**Defend Failover and Recovery**	AC-2(6), IR-4(2), IR-4(3), SC-7(20), SC-48, SC-48 (1), SI-4(1)	Increase sensor activity and restrict privileges to defend against an adversary taking advantage of failover or recovery activities.	Adaptive Management, Dynamic Reconfiguration, Orchestration, Functional Relocation of Sensors, Dynamic Segmentation and Isolation, Mission Dependency and Status Visualization, Dynamic Privileges
CM1247	**Defend Against DoS**	AC-4(3), SC-5(2), SC-5(3)	Adapt to reduce the impacts of denial-of-service attacks.	Dynamic Resource Allocation, Adaptive Management, Surplus Capacity, Monitoring and Damage Assessment

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1248	**Conceal or Randomize Network Traffic**	SC-8(5), SC-30	Conceal (via encryption or insertion of fabricated traffic) or randomize network traffic patterns.	Obfuscation, Contextual Unpredictability
CM1253	**Modulate Information Flows**	AC-4(27), AC-4(29), AC-4(30), SC-7(15), SC-46	Use controlled interfaces and communications paths to provide access to risky capabilities or to filter communications between enclaves.	Orchestration, Design Diversity, Replication, Predefined Segmentation, Trust-Based Privilege Management
CM1254	**Hardware-Based Protection of Firmware**	SC-51	Use hardware-based protections for firmware.	Integrity Checks
CM1255	**Validate Output Data**	SI-15	Validate information output from processes or applications against defined criteria.	Integrity Checks
CM1259	**Enhance User Preparedness**	AT-2(1), AT-2(3), AT-2(5), AT-3(3)	Keep users, administrators, and operators aware of existing and emerging threats and attack techniques they can counter in practice.	Dynamic Threat Awareness, Self-Challenge
CM1260	**Conceal Resources from Discovery**	SC-7(16), SC-28(1), SC-30, SC-30(5)	Protect network addresses of system components that are part of managed interfaces from discovery through common tools and techniques, via hiding or relocation.	Obfuscation, Functional Relocation of Cyber Resources
CM1262	**Restrict Supply Chain Exposures**	CM-7(7), SR-3(2), SR-5, SR-6(1), SR-7, SR-10, SR-11	Restrict adversaries' ability to determine or manipulate the organization's cyber supply chain.	Orchestration, Obfuscation, Disinformation, Self-Challenge, Supply Chain Diversity, Replication, Predefined Segmentation, Integrity Checks, Provenance Tracking
CM1275	**Emergency Shutdown**	IR-4(2), IR-4(3), SC-29	Shut down physical processes safely.	Dynamic Reconfiguration, Architectural Diversity

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1276	**Safe Mode Restart**	CP-12	Reboot devices and restart physical processes safely.	Adaptive Management, Restriction
CM1277	**Coordinate Responses to Adversity**	CP-2(1), CP-2(5), CP-4(5)	Coordinate responses to adversity to minimize impacts on service delivery.	Consistency Analysis, Orchestration, Self-Challenge
CM2102	**Inspect and Analyze Network Traffic**	IR-4(13), SI-4(2), SI-4(4), SI-4(10), SI-4(25)	Analyze network traffic for unusual data flows.	Monitoring and Damage Assessment, Behavior Analysis
CM2103	**Endpoint Behavior Analysis**	AC-2(12)	Analyze the behavior of endpoint (i.e., end-user, client) systems for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2104	**Monitor Logs**	AU-6, IR-4(13), SI-4(2), SI-4(11)	Monitor system and application logs for anomalous or suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2105	**Analyze Logs**	AC-2(12), SI-4(13), SI-4(16)	Analyze logs (individually or with some correlation across logs) for anomalous or suspicious patterns of behavior.	Monitoring and Damage Assessment, Dynamic Resource Awareness, Behavior Validation
CM2106	**Analyze File Contents**	SR-10	Analyze contents of specific files or types of files for suspicious contents.	Forensic and Behavioral Analysis
CM2108	**Removable Device Usage Detection**	CM-8(3)	Detect anomalous or unauthorized events involving use of removable devices.	Monitoring and Damage Assessment
CM2109	**Software Integrity Check**	SI-7, SI-7(1), SI-7(6), CM-14, SR-4(3)	Perform integrity checks (e.g., using checksums, hashes, or digital signatures) on software, software certificates, or metadata.	Integrity Checks, Provenance Tracking
CM2110	**Software Stress Testing**	SR-6(1)	Perform software stress testing (e.g., using out-of-bounds input values) prior to installation.	Self-Challenge

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2111	**Physical Inspection**	SR-9, SR-10	Perform physical inspection of hardware components for indicators of tampering.	Integrity Checks
CM2113	**Cross Enterprise Account Usage Analysis**	AU-6(3), SI-4(16)	Analyze user account usage across the enterprise for anomalies or suspicious behavior.	Sensor Fusion and Analysis
CM2115	**Process Monitoring**	IR-4(13), SI-4(2)	Monitor the behavior of processes for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
CM2117	**Privileged Account Monitoring**	AC-6(8)	Monitor and analyze activity associated with privileged accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment
CM2118	**Cross-Enterprise Behavior Analysis**	AU-6(3), AU-6(5)	Correlate and analyze behavior of multiple systems.	Sensor Fusion and Analysis
CM2120	**Application- or Utility-Specific Monitoring**	IR-4(13), SI-4(2)	Monitor and analyze events in the context of a specific application or utility.	Monitoring and Damage Assessment, Behavior Validation
CM2121	**Account Monitoring**	AC-2(12), IR-4(13), SI-4(2)	Monitor and analyze activity associated with user accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
CM2122	**Host-Local Event Correlation**	IR-4(13), SI-4(16)	Correlate and analyze events occurring on a single host.	Sensor Fusion and Analysis, Monitoring and Damage Assessment
CM2124	**Monitor Health and Status of Protective Systems**	PM-31	Monitor the health and status of protective systems.	Monitoring and Damage Assessment, Sensor Fusion and Analysis
CM2129	**Monitor Script Execution**	IR-4(13), SI-4(2), SI-4(13)	Monitor for the execution of scripts which are unknown or used in suspicious ways.	Monitoring and Damage Assessment

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2133	**Monitor the File System**	IR-4(13), SI-4(2), SI-4(24)	Monitor the file system to identify the unexpected presence and atypical use of files of specific types, or atypical patterns of access.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Behavior Validation
CM2138	**Monitor Command Line Use**	IR-4(13), SI-4(2), SI-4(4), SI-4(13)	Monitor use of the command line interface for use of common utilities (part of the system or installed by the adversary), looking for suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
CM2141	**Analyze Network Traffic Content**	IR-4(13), SI-4(25)	Analyze the contents of network traffic.	Monitoring and Damage Assessment, Behavior Validation
CM2144	**Monitor Platform Status**	IR-4(13), SI-4(2)	Poll platforms (e.g., user endpoints, servers, network devices) and other devices to determine their status.	Monitoring and Damage Assessment
CM2147	**Monitor Network Usage**	IR-4(13), SI-4(11), SI-4(13)	Monitor network usage for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation

7 Conclusion

This paper documents the initial results of a Cyber Resiliency Effects Analysis for ATT&CK for Enterprise and ATT&CK for ICS. AFRL has used the tables in Sections 3 and 5 to create a set of ordered lists of the form <ATT&CK Technique, control, cyber resiliency approach, potential effect, Mitigation or CM> for incorporation into the CSA Tool knowledge base. Each row in the list represents a statement of the form "this control, by applying this cyber resiliency approach, can have this effect on this Technique, as long as it is used as described by the identified Mitigation or candidate mitigation." The potential effects can be used to develop test cases for systems without and with the controls implemented and used as described by the Mitigations or CMs.

The use cases for this analysis are driven by the use cases for the CSA Tool, and include systems security engineering (SSE), development of automated test cases for cyber test and evaluation (CT&E), and identification of capability gaps in Department of Defense (DoD) systems as a motivation for research planning. The results of this analysis have not yet been examined to answer such questions as which effects are most frequently identified, which effects are under-represented, which cyber resiliency approaches are most frequently identified, which approaches provide the broadest range of potential effects, or which approaches could potentially affect adversary TTPs under the most Tactics. While such an examination could identify capability gaps meriting further research, it must be qualified carefully: This analysis was driven by the ATT&CK for Enterprise knowledge base, which was designed for a different set of use cases. In particular, adversary TTPs which have not yet been observed "in the wild" (i.e., in a real-world environment) are not included, even if a Red Team or a group of cyber researchers has defined such novel TTPs.

In addition, because the ATT&CK knowledge base includes descriptions of detection methods, many of which apply one or more cyber resiliency approaches to Analytic Monitoring, the Detect effect may be disproportionately represented in this analysis. By contrast, the Reveal effect, which involves threat information sharing with other organizations (control PM-16), depends on organizational commitment to such sharing, and has an indirect effect on any specific Technique, is probably under-represented in this analysis. Similarly, some cyber resiliency techniques (e.g., Diversity) and implementation approaches are more structural than functional; given the strong operational orientation of the ATT&CK knowledge base, these are probably under-represented in this analysis.

This analysis did not include ATT&CK for Mobile. Additional possible directions for future work include alignment and integration with the CTID control mapping, MITRE D3FEND, and MITRE Engage. Because ATT&CK, D3FEND, and Engage will continue to evolve, systems security engineers are encouraged to track changes and update the analysis as needed.

8 References

[1] Joint Task Force, "NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations," 23 September 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[2] J. Reilly, *Automated Cyber Survivability (ACS),* Rome, NY: AFRL RIGA, 2019.

[3] J. Reilly, *Cyber Survivability Attributes: CSA Tool (8ABW-2019-2267),* Rome, NY: Air Force Research Laboratory, 2019.

[4] NIST, "NIST SP 800-160 Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach," 27 November 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

[5] NIST, "NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber Resilient Systems: A Systems Security Engineering Approach," December 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

[6] D. Bodeau, R. Graubart, and E. Laderman, "Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes: Enabling Controls, Requirements, Solutions, and Metrics to Be Identified (MP 190668, PR 19-02172-10)," September 2019. [Online]. Available: https://www.mitre.org/sites/default/files/pdf/CR-Cyber-Survivability.pdf.

[7] A. M. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," *IEEE Systems Journal, Vol. 3, No. 2*, June 2009.

[8] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment (MTR 130432, PR 13-4173)," November 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf.

[10] D. Bodeau and R. Graubart, "A Framework for Describing and Analyzing Cyber Strategies and Strategic Effects (MTR 140346, PR 14-3407)," The MITRE Corporation, Bedford, MA, 2014.

[11] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, "MITRE ATT&CK: Design and Philosophy, MP180360R1," March 2020. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

[12] O. Alexander, M. Belisle and J. Steele, "MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy, MP01055863, PR 19-03307-03," March 2020. [Online]. Available: https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT%26CK_for_ICS_-_Philosophy_Paper.pdf.

[13] JCS, "Cyber Survivability Endorsement Implementation Guide, Version 2.0," 14 February 2020. [Online].

[14] T. Gregg and M. Long, “Framework for Improving Critical Infrastructure Cybersecurity/ATT&CK™ Mapping, PR 19-3442,” The MITRE Corporation, McLean, VA, 2019.

[15] J. Baker and T. Bergeron, “Security Control Mappings: A Bridge to Threat-Informed Defense,” MITRE-Engenuity, 15 December 2020. [Online]. Available: https://medium.com/mitre-engenuity/security-control-mappings-a-bridge-to-threat-informed-defense-2e42a074f64a.

[16] AttackIQ, “Security Optimization Journey Blueprint, Phase 1: Automated Security Validation,” 2021. [Online]. Available: https://attackiq.com/blueprints/automated-security-validation/.

[17] D. Bodeau, R. Graubart, J. Fitzpatrick, D. Johnson, D. Mann and J. R. Woodill, “Defining Cyber Hygiene to Enable Trade-off Analysis, MTR200593, PR 21-1315,” The MITRE Corporation, Bedford, MA, 2021.

[18] D. Bodeau, R. Graubart, R. McQuaid, and J. Woodill, “Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods (MTR 180314, PR 18-2579),” September 2018. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

[19] MITRE Engenuity, “Mapping Methodology,” Center for Threat-Informed Defense ATT&CK Control Framework Mappings, 14 December 2020. [Online]. Available: https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings/blob/master/docs/mapping_methodology.md.

[20] The MITRE Corporation, “MITRE Engage,” 2021. [Online]. Available: https://engage.mitre.org/.

[21] The MITRE Corporation, “Complete ATT&CK® Mapping,” 2020. [Online]. Available: https://shield.mitre.org/attack_mapping/mapping_all.

[22] NIST, “Draft NIST Special Publication 800-160 Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach,” 4 September 2019. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft-fpd.pdf.

[23] National Security Agency, “NSA/CSS Technical Cyber Threat Framework V2,” 13 November 2018. [Online]. Available: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf.

[24] NIST, “NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View,” March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[25] CNSS, “Committee on National Security Systems (CNSS) Glossary (CNSS Instruction No. 4009),” 26 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/openDoc.cfm?hldYMe6UHW4ISXb8GFGURw==.

[26] CIS, “CIS Controls V7.1,” 1 April 2019. [Online]. Available: https://learn.cisecurity.org/cis-controls-download.

[27] D. Bodeau, R. Graubart, R. McQuaid, and J. Woodill, “Cyber Resiliency Metrics Catalog (MTR 180450),” The MITRE Corporation, Bedford, MA, 2018.

[28] NIST, “NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations,” April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[29] The MITRE Corporation, “Shields Up: A Good Cyber Defense Is an Active Defense,” August 2020. [Online]. Available: https://www.mitre.org/publications/project-stories/shields-up-a-good-cyber-defense-is-an-active-defense.

[30] Office of Cybersecurity and Communications, Federal Network Resilience Division, “Securing High Value Assets, Version 1.1,” July 2018. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf.

[31] NIST, “NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171,” 2 February 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.

Appendix A Definitions

Table 33, adapted from Appendix F of NIST SP 800-160 Vol. 2, defines the potential effects on adversary activities.

Table 33. Definitions of Potential Effects on Adversary Activities

INTENDED EFFECT	DESCRIPTION
Redirect (includes deter, divert, and deceive)	Direct threat events away from defender-chosen resources.
Deter	Discourage the adversary from undertaking further activities by instilling fear (e.g., of attribution or retribution) or doubt that those activities would achieve intended effects (e.g., that targets exist).
Divert	Direct the threat event toward or away from defender-chosen resources.
Deceive	Lead the adversary to believe false information about individuals, systems, missions, organizations, defender capabilities, or TTPs.
Preclude (includes expunge, preempt, and negate)	Ensure that the threat event does not have an impact.
Expunge	Remove resources that are known to be or are suspected of being unsafe, incorrect, or corrupted.
Preempt	Forestall or avoid conditions under which the threat event could occur or on which an attack is predicated.
Negate	Create conditions under which the threat event cannot be expected to result in an impact.
Impede (includes contain, degrade, delay, and exert)	Make it more difficult for threat events to cause adverse impacts or consequences.
Contain	Restrict the effects of the threat event to a limited set of resources.
Degrade	Decrease the expected consequences of the threat event.
Delay	Increase the amount of time needed for the threat event to result in adverse impacts.
Exert	Increase the level of effort or resources needed for an adversary to achieve a given result.
Limit (includes shorten and reduce)	Restrict the consequences of realized threat events by limiting the damage or effects they cause in terms of time, system resources, and/or mission or business impacts.
Shorten	Limit the duration of adverse consequences of a threat event.
Reduce	Decrease the degree of damage from a threat event. Degree of damage can have two dimensions: breadth (i.e., number of affected resources) and depth (i.e., level of harm to a given resource).
Expose (includes detect, scrutinize, and reveal)	Reduce risk due to ignorance of threat events and possible replicated or similar threat events in the same or similar environments.
Detect	Identify threat events or their effects by discovering or discerning the fact that an event is occurring, has occurred, or (based on indicators, warnings, and precursor activities) is about to occur.
Scrutinize	Analyze threat events and artifacts associated with threat events to develop indicators, determine sources of events, assess damage, and identify patterns of exploiting vulnerabilities, predisposing conditions, and weaknesses.
Reveal	Share information about risk factors and the relative effectiveness of remediation approaches with partners, stakeholder community, or the general public.

The informal descriptions of cyber resiliency techniques and approaches in Table 34 are tailored from [4] [5] for readability, with *notes in italics* of how cyber resiliency techniques and approaches could relate to other technologies and practices used by an organization. See Appendix F of [4] for the complete definition and examples of technologies and practices for each approach, and for guidance on where in a notional layered architecture each approach could be used.

Table 34. Cyber Resiliency Techniques and Approaches

TECHNIQUES	APPROACHES
Adaptive Response Implement agile courses of action to manage risks. *Inform courses of action with situational awareness and predictive analytics for increased agility.* *All approaches can leverage virtualization and are compatible with zero trust architecture (ZTA) and cloud computing strategies. All approaches can also be applied to processes and reporting within a Security Operations Center (SOC), and to the use of deception.*	**Dynamic Reconfiguration** Definition: Make changes to individual systems, system elements, components, or sets of resources to change functionality or behavior without interrupting service. Informal description: Change how resources are – or can be – used. *Reconfiguration needs to be executed without significantly degrading or interrupting service.*
	Dynamic Resource Allocation Definition: Change the allocation of resources to tasks or functions without terminating critical functions or processes. Informal description: Change how much of a resource can be used. *Reallocate resources to tasks or functions without terminating critical functions or processes*.
	Adaptive Management Definition: Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment. Informal description: Change in response to change. *Manage how mechanisms can be used based on changes in the operational environment as well as changes in the threat environment*.
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way. *Systems can accumulate vast amounts of monitoring or logging data. Use monitoring data strategically to inform defensive activities.*	**Monitoring and Damage Assessment** Definition: Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, to look for precursor conditions or indicators of other threat events, and to detect and assess damage from adversity. Informal description: Look for indications that something might be awry and what damage might have occurred. *Leverage Continuous Diagnostics and Monitoring (CDM) and other monitoring capabilities, including those related to health and status (H&S). Integrate with threat hunting and insider threat monitoring.*
	Sensor Fusion and Analysis Definition: Fuse and analyze monitoring data and analysis results from different information sources or at different times together with externally provided threat intelligence. Informal description: Put the pieces together – from many different sources. *Consider all possible sources of monitoring information, including CDM, H&S, physical access logs, and insider threat monitoring.*
	Forensic and Behavioral Analysis Definition: Analyze indicators and adversary TTPs, including observed behavior as well as malware and other artifacts left behind by adverse events.

TECHNIQUES	APPROACHES
	Informal description: Analyze adversary activities and artifacts to develop understanding and attribution of adversary goals, capabilities, and practices. *Ensure that policies and practices are in place to capture evidence and support analysis.*
Contextual Awareness Construct and maintain current representations of the posture of missions or business functions considering threat events and courses of action. *Maintain cyber situational awareness to support mission continuity.*	**Dynamic Resource Awareness** Definition: Maintain current information about resources, status of resources, and resource connectivity. Informal description: Maintain awareness of systems' performance and security posture. *Integrate network performance, system performance, and continuous diagnostics as part of situational awareness.*
	Dynamic Threat Awareness Definition: Maintain current information about threat actors, indicators, and potential, predicted, and observed adverse events. Informal description: Maintain current awareness of threats – observed and anticipated. *Ensure that the organization's Security Operations Center (SOC) ingests cyber threat intelligence.*
	Mission Dependency and Status Visualization Definition: Maintain a useful current visualization of the status of missions or business functions, dependencies on resources, and the status of those resources with respect to threats. Informal description: Maintain an up-to-date cyber operational picture. *Maintain an up-to-date dependency map for mission essential or business essential functions. Integrate resource and threat awareness into situational awareness and enable focused visualization for high value assets and infrastructure services.*
Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner. *Lack of coordination introduces fragility and creates exposures to threats.*	**Calibrated Defense-in-Depth** Definition: Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value. Informal description: Don't expect one defense to suffice – but apply layered defenses based on risk. *Avoid creating single points of failure. Do not make the adversary's job easy.*
	Consistency Analysis Definition: Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps. Informal description: Minimize opportunities for the system's security capabilities to be used incompletely or inconsistently. *Over time, changing access policies for information, allowable uses of capabilities, and dependencies among systems and components can produce fragility and provide adversaries with opportunities.*
	Orchestration Definition: Coordinate modifications to and the ongoing behavior of mechanisms and processes at different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps. Informal description: Coordinate security capabilities at different layers, and in different systems or components, to avoid coverage gaps or interference.

TECHNIQUES	APPROACHES
	Orchestrate updates of capabilities and policies – in particular, for identity, credentialing, and access management (ICAM) – across systems. Orchestrate monitoring across architectural layers. Use a cyber playbook to orchestrate incident response efforts.
	Self-Challenge Definition: Affect mission/business processes or system elements adversely in a controlled manner to validate the effectiveness of protections and to enable proactive response and improvement. Informal description: Validate the effectiveness of capabilities and processes in action. *Use tabletop exercises (TTXs), Red Teams, penetration testing, or automated fault injection throughout the system lifecycle and with different scopes.*
Deception Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary. *Apply deception strategically, tactically, or both. Ensure that cyber risk governance and SOC operations allow for deception and maintain deception resources. Deception can support analysis and attribution of adversary TTPs, and the development of cyber threat intelligence.*	**Obfuscation** Definition: Hide, transform, or otherwise make information unintelligible to the adversary. Informal description: Make information hard for the adversary to find and understand. *Encryption is a key method for obfuscation.*
	Disinformation Definition: Provide deliberately misleading information to adversaries. Informal description: Lie to adversaries. *Typical forms of disinformation include decoy accounts and decoy credentials.*
	Misdirection Definition: Maintain deception resources or environments and direct adversary activities there. Informal description: Direct adversary activities to deception environments or resources. *Commercial products can be used to create and maintain a deception network, but ongoing effort is needed to keep it current, engage with adversaries, and analyze adversary TTPs.*
	Tainting Definition: Embed covert capabilities in resources. Informal description: Cause what adversaries steal to give them away or otherwise harm them. *Enable exfiltrated data to "phone home."*
Diversity Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities. *Enterprise systems often include some diversity incidentally, as a result of procurements by different programs or at different times. Poorly managed, this can be costly and*	**Architectural Diversity** Definition: Use multiple sets of technical standards, different technologies, and different architectural patterns. Informal description: Use different technical architectures. *An organization can use, for example, both Windows and Linux. An organization's cloud strategy can involve multiple cloud infrastructures.*
	Design Diversity Definition: Use different designs within a given architecture to meet the same requirements or provide equivalent functionality. Informal description: Provide multiple ways to meet requirements.

TECHNIQUES	APPROACHES
create security risks; well managed, it can make an adversary's job harder. *Due to reliance on common libraries and infrastructures, diversity can be more apparent than real; therefore, analysis is needed to verify the extent of diversity.*	*Within the context of a given architecture, parallel design teams can solve the same problem in different ways, thus producing different attack surfaces.*
	Synthetic Diversity Definition: Transform implementations of software to produce a variety of instances. Informal description: Use automation to tweak software implementations. *For example, use randomizing compilers or address space layout randomization.*
	Information Diversity Definition: Provide information from different sources or transform information in different ways. Informal description: Use multiple sources for the same information. *Use of information from different sources can reveal adversary injection or modification.*
	Path Diversity Definition: Provide multiple independent paths for command, control, and communications. Informal description: Do not rely on a single mode of communication. *In particular, ensure alternative lines of communications for incident response and for continuity of an organization's essential functions.*
	Supply Chain Diversity Definition: Use multiple independent supply chains for critical components. Informal description: Look for ways to avoid relying on a single supply chain. *Determine when and how to use supply chain diversity as part of the organization's supply chain risk management (SCRM) strategy. Note that the use of shared libraries and common components can make supply chain diversity more apparent than real.*
Dynamic Positioning Distribute and dynamically relocate functionality or system resources. *Use moving target defenses to make an adversary's job harder.*	**Functional Relocation of Sensors** Definition: Relocate sensors or reallocate responsibility for specific sensing tasks to look for indicators of adverse events. Informal description: Keep your eyes moving. *Relocating sensors compensates for blind spots and makes it harder for an adversary to hide.*
	Functional Relocation of Cyber Resources Definition: Change the location of cyber resources that provide functionality or information, either by moving the assets or by transferring functional responsibility. Informal description: Keep your cyber resources moving. *Make the adversary's discovery and network mapping efforts go stale quickly.*
	Asset Mobility Definition: Securely move physical resources. Informal description: Don't pin your physical resource down. *This approach is applicable to cyber-physical and tactical systems.*
	Fragmentation Definition: Partition information and distribute it across multiple components. Informal description: Create an information jigsaw puzzle.

TECHNIQUES	APPROACHES
	Manage fragmented data to ensure its ongoing quality, minimize its exposure, and minimize performance inefficiencies.
	Distributed Functionality Definition: Decompose a function or application into smaller functions and distribute those functions across multiple components. Informal description: Use fine-grained control of resource use. *Distributed functionality can be used with micro-segmentation and ZTA.*
Non-Persistence Generate and retain resources as needed or for a limited time. *Reduce the attack surface in the temporal dimension and reduce costs with just-in-time provisioning.*	**Non-Persistent Information** Definition: Refresh information periodically, or generate information on demand, and delete it when no longer needed. Informal description: Limit how long information is exposed. *Determine how temporary "temporary" files are.*
	Non-Persistent Services Definition: Refresh services periodically or generate services on demand and terminate services when no longer needed. Informal description: Don't let a service run indefinitely – it may have been compromised while running. *Instantiating services on demand and expunging them when inactive can be a performance management strategy as well.*
	Non-Persistent Connectivity Definition: Establish connections on demand and terminate connections when no longer needed. Informal description: Don't leave a communications line open. *Leverage software-defined networking (SDN), particularly in a ZTA.*
Privilege Restriction Restrict privileges based on attributes of users and system elements as well as on environmental factors. *Apply existing capabilities more stringently and integrate ZT technologies.*	**Trust-Based Privilege Management** Definition: Define, assign, and maintain privileges based on established trust criteria consistent with principles of least privilege. Informal description: Apply principles of least privilege. *Separate roles and responsibilities, use dual authorization.*
	Attribute-Based Usage Restriction Definition: Define, assign, maintain, and apply usage restrictions on cyber resources based on the criticality of missions or business functions and other attributes (e.g., data sensitivity). Informal description: Restrict use narrowly. *Avoid treating a system or an application as a Swiss Army knife.*
	Dynamic Privileges Definition: Elevate or decrease privileges assigned to a user, process, or service based on transient or contextual factors. Informal description: Make privileges context-sensitive. *Make access and usage decisions based on the current state and recent history.*
Realignment	**Purposing**

TECHNIQUES	APPROACHES
Structure systems and resource uses to meet mission or business function needs, to reduce current and anticipated risks, and to accommodate evolution of the technical, operational, and threat environments. *Look for restructuring opportunities related to new systems and programs, as well as planned upgrades to existing systems.*	Definition: Ensure cyber resources are used consistently with mission or business function purposes and approved uses, thereby avoiding unnecessary sharing and complexity. Informal description: Ensure resources are used consistently with mission or business function purposes and approved uses. *Avoid "mission creep," which can increase a system's attack surface.*
	Offloading Definition: Offload supportive but non-essential functions to other systems or to an external provider that is better able to perform the functions securely. Informal description: Offload functions when an external provider can do a better job. *Offloading reduces the attack surface and motivates ongoing consideration of what's essential.*
	Restriction Definition: Remove or disable unneeded functionality or connectivity. Informal description: Lock capabilities down. *Lock it down, even though that reduces agility and leaves some capabilities unused.*
	Replacement Definition: Replace low-assurance or poorly understood components with more trustworthy ones. Informal description: Replace what can't be trusted. *Some components are best simply discarded, particularly in light of supply chain risks. However, the decommissioning and replacement processes need to be secure.*
	Specialization Definition: Modify the design of, augment, or configure critical cyber resources uniquely for the mission or business function to improve trustworthiness. Informal description: Build special-purpose components or develop "special sauce." *Prevent the adversary from being able to mirror your system.*
	Evolvability Definition: Provide mechanisms and structure resources to enable the system to be maintained, modified, extended, or used in new ways without increasing security or mission risk. Informal description: Don't commit to an unchanging architecture. *Expect a broader range of "plug and play" capabilities over time.*
Redundancy Provide multiple protected instances of critical resources. *Redundancy is integral to system resilience, but it must be managed carefully to avoid redundant vulnerabilities and an increased attack surface.*	**Protected Backup and Restore** Definition: Back up information and software (including configuration data and virtualized resources) in a way that protects its confidentiality, integrity, and authenticity, and enable safe and secure restoration in case of disruption or corruption. Informal description: Back up resources securely and defend the restore process from adversary exploitation. *Keep in mind that transitions are often periods of exposure, and backups can be compromised.*
	Surplus Capacity

TECHNIQUES	APPROACHES
	Definition: Maintain extra capacity for information storage, processing, or communications. Informal description: Don't skimp on resources – provide surge capacity. *Where possible, use diverse resources to provide surplus capacity.*
	Replication Definition: Duplicate hardware, information, backups, or functionality in multiple locations and keep them synchronized. Informal description: Replicate capabilities in multiple locations and keep them synchronized. *Where possible, replicate capabilities using diverse resources.*
Segmentation Define and separate system elements based on criticality and trustworthiness. *Reduce the adversary's scope for lateral movement or command and control (C2).*	**Predefined Segmentation** Definition: Define enclaves, segments, micro-segments, or other restricted types of resource sets based on criticality and trustworthiness so that they can be protected separately and, if necessary, isolated. Informal description: Define enclaves, segments, or micro-segments to protect them separately. *Predefined enclaves and micro-segmentation facilitate risk-calibrated use of other security and cyber resiliency techniques.*
	Dynamic Segmentation and Isolation Definition: Change the configuration of enclaves or protected segments, or isolate resources while minimizing operational disruption. Informal description: Isolate resources dynamically to reduce transient risks. *Consider software-defined networking (SDN) and network function virtualization (NFV), consistent with ZT principles, particularly for high value assets.*
Substantiated Integrity Ascertain whether critical system elements have been corrupted. *Verify that you actually have what you think you have.*	**Integrity Checks** Definition: Apply and validate checks of the integrity or quality of information, components, or services, to guard against surreptitious modification. Informal description: Check for modifications to data and software. *Integrity checks can be applied to information, metadata, components, or services.*
	Provenance Tracking Definition: Identify and track the provenance of data, software, or hardware elements. Informal description: Verify the source of what you depend on. *Make provenance tracking part of SCRM.*
	Behavior Validation Definition: Validate the behavior of a system, service, device, or individual user against defined or emergent criteria (e.g., requirements, patterns of prior usage). Informal description: Validate behavior against defined or emergent criteria. *Learn what's normal and what's suspicious. Coordinate with insider threat mitigation.*
Unpredictability Make changes randomly or unpredictably. *Keep the adversary guessing.*	**Temporal Unpredictability** Informal description: Change behavior or state at times that are determined randomly or by complex functions. Informal description: Keep the adversary from extrapolating from past events.

TECHNIQUES	APPROACHES
	Don't let the present duplicate the past.
	Contextual Unpredictability Definition: Change behavior or state in ways that are determined randomly or by complex functions. Informal description: *Keep the adversary from extrapolating from similar events.* *Don't let the adversary take advantage of consistency.*

Appendix B Cyber Resiliency Controls

The following table indicates, for each cyber resiliency control identified in NIST SP 800-160 Vol. 2, the ATT&CK Mitigations and the candidate mitigations which use the control to apply one or more of the identified cyber resiliency approaches. As discussed in Section 2.5, some cyber resiliency controls are not used by any Mitigation or candidate mitigation, because their effects are indirect (e.g., design principles), they involve policies and procedures rather than technical capabilities, or they are intended to address threats not represented in the ATT&CK matrices. Also, some Mitigations apply controls identified as cyber resiliency, but do not use those controls to apply a cyber resiliency approach; these are not identified in Table 35.

Table 35. Mitigations and Candidate Mitigations Using Cyber Resiliency Controls

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
Access Control			
AC-2(6)	Account Management | Dynamic Privilege Management	Privilege Restriction [Dynamic Privileges] Adaptive Response [Dynamic Reconfiguration]	CM1117, CM1145, CM1245
AC-2(8)	Account Management | Dynamic Account Management	Adaptive Response [Dynamic Resource Allocation, Dynamic Reconfiguration, Adaptive Management] Privilege Restriction [Dynamic Privileges]	CM1117, CM1121
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CM2002, CM2003, CM2005, CM2016, CM2021, CM2103, CM2105, CM2121
AC-3(2)	Access Enforcement | Dual Authorization	Privilege Restriction [Trust-Based Privilege Management]	[not referenced – intended to address insider threats]
AC-3(7)	Access Enforcement | Role-Based Access Control	Privilege Restriction [Attribute-Based Usage Restriction]	M0800
AC-3(11)	Access Enforcement | Restrict Access to Specific Information Types	Privilege Restriction [Attribute-Based Usage Restriction]	CM1149
AC-3(12)	Access Enforcement | Assert and Enforce Application Access	Privilege Restriction [Attribute-Based Usage Restriction]	M0800, CM1111, CM1306
AC-3(13)	Access Enforcement | Attribute-Based Access Control	Privilege Restriction [Attribute-Based Usage Restriction]	M0800, M0937, M1018, M1054, CM1111
AC-4(2)	Information Flow Enforcement | Processing Domains	Segmentation [Predefined Segmentation]	M0811, M0930, M1030, CM1142
AC-4(3)	Information Flow Enforcement | Dynamic Information Flow Control	Adaptive Response [Dynamic Reconfiguration, Adaptive Management]	M0937, M1037, CM1131, CM1139, CM1147, CM1247

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
AC-4(8)	Information Flow Enforcement | Security and Privacy Policy Filters	Substantiated Integrity [Integrity Checks]	M0811, M0937, M0950, M1021, M1050, CM1142, CM1151, CM1242
AC-4(12)	Information Flow Enforcement | Data Type Identifiers	Substantiated Integrity [Integrity Checks]	CM1151
AC-4(17)	Information Flow Enforcement | Domain Authentication	Substantiated Integrity [Provenance Tracking]	M0807, M0937, M1054, CM1151
AC-4(21)	Information Flow Enforcement | Physical or Logical Separation of Information Flows	Segmentation [Predefined Segmentation]	M0930, M0948, M1030, M1048, CM1151
AC-4(27)	Information Flow Enforcement | Redundant/Independent Filtering Mechanisms	Diversity [Design Diversity] Redundancy [Replication]	CM1153, CM1253
AC-4(29)	Information Flow Enforcement | Filter Orchestration Engines	Coordinated Protection [Orchestration]	CM1153, CM1253
AC-4(30)	Information Flow Enforcement | Filter Mechanisms Using Multiple Processes	Diversity [Design Diversity] Redundancy [Replication]	CM1153, CM1253
AC-6	Least Privilege	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction]	M0922, M0924, M1018, M1026, M1028, CM1164
AC-6(1)	Least Privilege | Authorize Access to Security Functions	Privilege Restriction [Attribute-Based Usage Restriction]	M1018, M1022
AC-6(2)	Least Privilege | Non-Privileged Access for Nonsecurity Functions	Privilege Restriction [Trust-Based Privilege Management] Realignment [Purposing]	M1026
AC-6(3)	Least Privilege | Network Access to Privileged Commands	Privilege Restriction [Trust-Based Privilege Management]	M1035
AC-6(4)	Least Privilege | Separate Processing Domains	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction] Segmentation [Predefined Segmentation]	M0948, M1021, M1029, M1048
AC-6(5)	Least Privilege | Privileged Accounts	Privilege Restriction [Trust-Based Privilege Management]	M0926, M1026, CM1164
AC-6(6)	Least Privilege | Privileged Access by Non-Organizational Users	Privilege Restriction [Trust-Based Privilege Management]	[not referenced – addresses threats not covered by ATT&CK]
AC-6(7)	Least Privilege | Review of User Privileges	Coordinated Protection [Consistency Analysis] Privilege Restriction [Trust-Based Privilege Management]	M0915, M0918, M0947, M1018, M1021, M1026
AC-6(8)	Least Privilege | Privilege Levels for Code Execution	Privilege Restriction [Attribute-Based Usage Restriction, Dynamic Privileges]	M1026

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	Privilege Restriction [Attribute-Based Usage Restriction, Trust-Based Privilege Management]	M1035, CM1306
AC-7(4)	Unsuccessful Logon Attempts | Use of Alternate Authentication Factor	Diversity [Path Diversity]	CM1140
AC-12	Session Termination	Non-Persistence [Non-Persistent Services]	CM1127, CM1227
AC-23	Data Mining Protection	Analytic Monitoring [Monitoring and Damage Assessment] Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges]	CM1157
Audit and Accountability			
AU-5(3)	Response to Audit Processing Failures | Configurable Traffic Volume Thresholds	Adaptive Response [Dynamic Resource Allocation, Adaptive Management]	CM1108, CM1208
AU-6	Audit Record Review, Analysis, and Reporting	Adaptive Response [Adaptive Management] Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CM2002, CM2004, CM2015, CM2035, CM2104
AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Repositories	Analytic Monitoring [Sensor Fusion and Analysis]	CM2013, CM2018, CM2113, CM2118
AU-6(5)	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	Analytic Monitoring [Sensor Fusion and Analysis]	CM2018, CM2023, CM2118
AU-6(6)	Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring	Analytic Monitoring [Sensor Fusion and Analysis]	[not referenced – addresses threats not covered by ATT&CK]
AU-6(8)	Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands	Analytic Monitoring [Monitoring and Damage Assessment] Segmentation [Predefined Segmentation]	CM2017, CM1308, CM2117
AU-6(9)	Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources	Analytic Monitoring [Sensor Fusion and Analysis]	[not referenced – addresses threats not covered by ATT&CK]
AU-9(1)	Protection of Audit Information | Hardware Write-Once Media	Substantiated Integrity [Integrity Checks]	CM1158
AU-9(2)	Protection of Audit Information | Store on Separate Physical Systems and Components	Segmentation [Predefined Segmentation]	M1029, M1030, CM1158
AU-9(3)	Protection of Audit Information | Cryptographic Protection	Substantiated Integrity [Integrity Checks]	M1041, CM1158

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
AU-9(5)	Protection of Audit Information | Dual Authorization	Privilege Restriction [Trust-Based Privilege Management]	[not referenced – intended to address insider threats]
AU-9(6)	Protection of Audit Information | Read-Only Access	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction] Substantiated Integrity [Integrity Checks]	M1022, M1029, CM1158
AU-9(7)	Protection of Audit Information | Store on Component with Different Operating System	Diversity [Architectural Diversity]	CM1305
AU-10(2)	Non-Repudiation | Validate Binding of Information Producer Identity	Substantiated Integrity [Provenance Tracking]	M0802, M1047
AU-13	Monitoring for Information Disclosure	Adaptive Response [Adaptive Management] Analytic Monitoring [Monitoring and Damage Assessment]	CM2043
AU-13(3)	Monitoring for Information Disclosure | Unauthorized Replication of Information	Analytic Monitoring [Monitoring and Damage Assessment]	CM2043
Awareness and Training			
AT-2(1)	Awareness Training | Practical Exercises	Contextual Awareness [Dynamic Threat Awareness] Coordinated Protection [Self-Challenge]	M1017, CM1107, CM1159, CM1259
AT-2(3)	Awareness Training | Social Engineering and Mining	Contextual Awareness [Dynamic Threat Awareness]	M1017, CM1159, CM1259
AT-2(5)	Awareness Training | Advanced Persistent Threat	Contextual Awareness [Dynamic Threat Awareness]	M1017, CM1159, CM1259
AT-3(3)	Role-Based Training | Practical Exercises	Contextual Awareness [Dynamic Threat Awareness] Coordinated Protection [Self-Challenge]	CM1107, CM1159, CM1259
Assessment, Authorization, and Monitoring			
CA-7(3)	Continuous Monitoring | Trend Analyses	Contextual Analysis [Dynamic Resource Awareness, Dynamic Threat Awareness]	CM1301
CA-7(5)	Continuous Monitoring | Consistency Analysis	Coordinated Protection [Consistency Analysis]	M1047, CM1129
CA-7(6)	Continuous Monitoring | Automation Support for Monitoring	Analytic Monitoring [Monitoring and Damage Assessment]	CM1314
CA-8	Penetration Testing	Coordinated Protection [Self-Challenge]	CM1107, CM1207

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
CA-8(1)	Penetration Testing | Independent Penetration Agent or Team	Coordinated Protection [Self-Challenge]	CM1107, CM1207
CA-8(2)	Penetration Testing | Red Team Exercises	Coordinated Protection [Self-Challenge]	CM1107, CM1207
CA-8(3)	Penetration Testing | Facility Penetration Testing	Coordinated Protection [Self-Challenge]	[not referenced – addresses threats not covered by ATT&CK]
Configuration Management			
CM-2(7)	Baseline Configuration | Configure Systems and Components for High-Risk Areas	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis] Realignment [Restriction]	[not referenced – addresses threats not covered by ATT&CK]
CM-4(1)	Impact Analyses | Separate Test Environments	Segmentation [Predefined Segmentation]	CM1308
CM-5(4)	Access Restrictions for Change | Dual Authorization	Privilege Restriction [Trust-Based Privilege Management]	M1026
CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation	Privilege Restriction [Trust-Based Privilege Management]	CM1306
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	Privilege Restriction Trust-Based Privilege Management]	CM1306
CM-7(2)	Least Functionality | Prevent Program Execution	Realignment [Restriction]	M0928, M0938, M0942, M0948, M1025, M1026, M1028, M1040, M1042, M1048, CM1119, CM1164
CM-7(4)	Least Functionality | Unauthorized Software	Realignment [Purposing]	M0944, CM1306
CM-7(5)	Least Functionality | Authorized Software	Privilege Restriction [Trust-Based Privilege Management] Realignment [Purposing]	M0938, M0945, M1038, M1044
CM-7(6)	Least Functionality | Confined Environments with Limited Privileges	Privilege Restriction [Trust-Based Privilege Management] Segmentation [Predefined Segmentation, Dynamic Segmentation, and Isolation]	M0948, M1048, CM1132, CM1133
CM-7(7)	Least Functionality | Code Execution in Protected Environments	Segmentation [Predefined Segmentation]	CM1162, CM1262
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	Analytic Monitoring [Monitoring and Damage Assessment]	M1034, CM2007, CM2008, CM2108
CM-14	Signed Components	Substantiated Integrity [Integrity Checks, Provenance Tracking]	M0945, M0947, CM2009, CM2109
Contingency Planning			

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
CP-2(1)	Contingency Plan | Coordinate with Related Plans	Coordinated Protection [Consistency Analysis]	CM1316, CM1277
CP-2(5)	Contingency Plan | Continue Missions and Business Functions	Coordinated Protection [Orchestration] Adaptive Response [Dynamic Reconfiguration, Adaptive Management]	M0811, CM1142, CM1143, CM1144, CM1242, CM1277
CP-2(8)	Contingency Plan | Identify Critical Assets	Contextual Awareness [Mission Dependency and Status Visualization]	CM1122, CM1222
CP-4(5)	Self-Challenge	Coordinated Protection [Self-Challenge]	CM1313, CM1277
CP-8(3)	Telecommunications Services | Separation of Primary And Alternate Providers	Diversity [Architectural Diversity]	[not referenced – addresses threats not covered by ATT&CK]
CP-9	System Backup	Redundancy [Protected Backup and Restore]	M0811, M0953, M1053, CM1141
CP-9(1)	System Backup | Testing for Reliability And Integrity	Coordinated Protection [Self-Challenge] Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]	CM1313
CP-9(6)	System Backup | Redundant Secondary System	Redundancy [Replication]	M0811, M0953, M1053, CM1142, CM1242
CP-9(7)	System Backup | Dual Authorization	Privilege Restriction [Trust-Based Privilege Management]	[not referenced – intended to address insider threats]
CP-9(8)	System Backup | Cryptographic Protection	Deception [Obfuscation] Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]	M0953, M0153
CP-11	Alternate Communications Protocols	Diversity [Architectural Diversity, Design Diversity]	M0811, CM1305
CP-12	Safe Mode	Adaptive Response [Adaptive Management] Realignment [Restriction]	CM1276
CP-13	Alternative Security Mechanisms	Diversity [Architectural Diversity, Design Diversity] Adaptive Response [Adaptive Management]	M0805, CM1126, CM1226
Identification and Authentication			

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
IA-2(6)	Identification And Authentication | Access to Accounts - Separate Device	Diversity [Path Diversity] Coordinated Protection [Calibrated Defense-in-Depth, Orchestration]	M0932, M1041
IA-2(13)	Identification and Authentication | Out-of-Band Authentication	Diversity [Path Diversity] Coordinated Protection [Calibrated Defense-in-Depth, Orchestration] Segmentation [Predefined Segmentation]	CM1126, CM1226
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]	M0813, CM1125
IA-10	Adaptive Authentication	Adaptive Response [Adaptive Management] Privilege Restriction [Dynamic Privileges] Coordinated Protection [Calibrated Defense-in-Depth]	CM1126, CM1226
Incident Response			
IR-4(2)	Incident Handling | Dynamic Reconfiguration	Adaptive Response [Dynamic Reconfiguration] Dynamic Positioning [Functional Relocation of Sensors]	M0811, M1037, CM1108, CM1110, CM1131, CM1138, CM1139, CM1142, CM1143, CM1144, CM1145, CM1208, CM1242, CM1245, CM1275
IR-4(3)	Incident Handling | Continuity of Operations	Adaptive Response [Dynamic Reconfiguration, Adaptive Management] Coordinated Protection [Orchestration]	CM1131, CM1145, CM1245, CM1275
IR-4(4)	Incident Handling | Information Correlation	Coordinated Protection [Orchestration] Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Threat Awareness]	CM2023
IR-4(9)	Incident Handling | Dynamic Response Capability	Adaptive Response [Dynamic Reconfiguration]	CM1141
IR-4(10)	Incident Handling | Supply Chain Coordination	Coordinated Protection [Orchestration]	CM1163, CM1316

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
IR-4(11)	Incident Handling | Integrated Incident Response Team	Adaptive Response [Dynamic Reconfiguration, Adaptive Management] Analytic Monitoring [Forensic and Behavioral Analysis] Coordinated Protection [Orchestration]	CM1316
IR-4(12)	Incident Handling | Malicious Code and Forensic Analysis	Analytic Monitoring [Forensic and Behavioral Analysis] Segmentation [Predefined Segmentation]	M1030, CM2019
IR-4(13)	Incident Handling | Behavior Analysis	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	M0920, M0950, M1020, M1050, CM1110, CM2002, CM2007, CM2014, CM2015, CM2020, CM2021, CM2022, CM2029, CM2033, CM2034, CM2038, CM2040, CM2042, CM2041, CM2044, CM2047, CM2102, CM2104, CM2115, CM2120, CM2121, CM2122, CM2129, CM2133, CM2138, CM2141, CM2144, CM2147
IR-5	Incident Monitoring	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]	CM2048
Maintenance			
MA-4(4)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions	Segmentation [Predefined Segmentation]	[not referenced – addresses threats not covered by ATT&CK]
Physical and Environmental Protection			
PE-3(5)	Physical Access Control | Tamper Protection	Substantiated Integrity [Integrity Checks]	[not referenced – addresses threats not covered by ATT&CK]
PE-6	Monitoring Physical Access	Analytic Monitoring [Monitoring and Damage Assessment]	[not referenced – addresses threats not covered by ATT&CK]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
PE-6(2)	Monitoring Physical Access | Automated Intrusion Recognition and Responses	Analytic Monitoring [Monitoring and Damage Assessment] Adaptive Response [Adaptive Management] Coordinated Protection [Orchestration]	CM1314
PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Systems	Analytic Monitoring [Monitoring and Damage Assessment] Coordinated Protection [Calibrated Defense-in-Depth]	[not referenced – addresses threats not covered by ATT&CK]
PE-9(1)	Power Equipment and Cabling | Redundant Cabling	Redundancy [Replication]	[not referenced – addresses threats not covered by ATT&CK]
PE-11(1)	Emergency Power | Alternate Power Supply - Minimal Operational Capability	Redundancy [Replication]	[not referenced – addresses threats not covered by ATT&CK]
PE-11(2)	Emergency Power | Alternate Power Supply - Self-Contained	Redundancy [Replication]	[not referenced – addresses threats not covered by ATT&CK]
PE-17	Alternate Work Site	Redundancy [Replication]	[not referenced – addresses threats not covered by ATT&CK]
Planning			
PL-8(1)	Security and Privacy Architecture | Defense in Depth	Coordinated Protection [Calibrated Defense-in-Depth]	M0805, M0813, CM1307, CM1137, CM1237
PL-8(2)	Security and Privacy Architecture | Supplier Diversity	Diversity [Supply Chain Diversity]	CM1106
Program Management			
PM-7(1)	Enterprise Architecture | Offloading	Realignment [Offloading]	[not referenced – relies on procedures and measures beyond the technical system]
PM-16	Threat Awareness Program	Contextual Awareness [Dynamic Threat Awareness]	M0919, M1019, CM2012, CM1161, CM1301, CM2043
PM-16(1)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	Contextual Awareness [Dynamic Threat Awareness]	M0931, CM1301, CM1314
PM-30(1)	Supply Chain Risk Management | Suppliers of Critical or Mission-Essential Items	Substantiated Integrity [Provenance Tracking]	CM1162, CM2012
PM-31	Continuous Monitoring Strategy	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion, and Analysis]	CM2124

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
PM-32	Purposing	Realignment [Purposing]	[not referenced – relies on procedures and measures beyond the technical system]
Risk Assessment			
RA-3(2)	Risk Assessment | Use of All-Source Intelligence	Contextual Awareness [Dynamic Threat Awareness]	CM1301
RA-3(3)	Risk Assessment | Dynamic Threat Awareness	Contextual Awareness [Dynamic Threat Awareness] Adaptive Response [Adaptive Management]	M0919, M1019, CM1301
RA-3(4)	Risk Assessment | Predictive Cyber Analytics	Contextual Awareness [Dynamic Threat Awareness]	CM1301
RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	Analytic Monitoring [Monitoring and Damage Assessment]	CM2043
RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	Analytic Monitoring [Monitoring and Damage Assessment] Privilege Restriction [Attribute-Based Usage Restriction]	[not referenced – addresses threats not covered by ATT&CK]
RA-5(6)	Vulnerability Monitoring and Scanning | Automated Trend Analyses	Analytic Monitoring [Sensor Fusion and Analysis]	CM1309, CM1314, CM1414
RA-5(8)	Vulnerability Monitoring and Scanning | Review Historic Audit Logs	Analytic Monitoring [Sensor Fusion and Analysis]	CM1309
RA-5(10)	Vulnerability Monitoring and Scanning | Correlate Scanning Information	Analytic Monitoring [Sensor Fusion and Analysis]	CM1301, CM1309
RA-9	Criticality Analysis	Contextual Awareness [Mission Dependency and Status Visualization] Realignment [Offloading]	CM1122, CM1315, CM1222
RA-10	Threat Hunting	Analytic Monitoring [Monitoring and Damage Assessment] Contextual Awareness [Dynamic Threat Awareness]	CM2043, CM1301
System and Services Acquisition			
SA-3(2)	System Development Lifecycle | Use of Live or Operational Data	Segmentation [Predefined Segmentation]	[not referenced – applies to development environment]
SA-8(2)	Security and Privacy Engineering Principles | Least Common Mechanism	Realignment [Offloading, Restriction]	M0805
SA-8(3)	Security and Privacy Engineering Principles | Modularity and Layering	Coordinated Protection [Calibrated Defense-in-Depth] Realignment [Specialization] Segmentation [Predefined Segmentation]	M0805

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SA-8(4)	Security and Privacy Engineering Principles | Partially Ordered Dependencies	Coordinated Protection [Consistency Analysis]	[not referenced – applied during system design]
SA-8(7)	Security and Privacy Engineering Principles | Reduced Complexity	Realignment [Purposing, Specialization]	[not referenced – applied during system design]
SA-8(8)	Security and Privacy Engineering Principles | Secure Evolvability	Coordinated Protection [Orchestration] Realignment [Evolvability]	[not referenced – applied during system design]
SA-8(13)	Security and Privacy Engineering Principles | Minimized Security Elements	Realignment [Purposing, Restriction]	[not referenced – applied during system design]
SA-8(16)	Security and Privacy Engineering Principles | Self-Reliant Trustworthiness	Adaptive Response [Adaptive Management] Segmentation [Dynamic Segmentation and Isolation] Substantiated Integrity [Integrity Checks]	[not referenced – applied during system design]
SA-8(17)	Security and Privacy Engineering Principles | Secure Distributed Composition	Dynamic Positioning [Distributed Functionality]	[not referenced – applied during system design]
SA-8(18)	Security and Privacy Engineering Principles | Trusted Communications Channels	Privilege Restriction [Attribute-Based Usage Restriction]	[not referenced – applied during system design]
SA-8(19)	Security and Privacy Engineering Principles | Continuous Protection	Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]	[not referenced – applied during system design]
SA-8(31)	Security and Privacy Engineering Principles | Secure System Modification	Realignment [Evolvability]	[not referenced – applied during system design]
SA-9(7)	External System Services | Organization-Controlled Integrity Checking	Substantiated Integrity [Integrity Checks]	M0916, CM1016, CM1130, CM1230
SA-11(2)	Developer Testing and Evaluation | Threat Modeling And Vulnerability Analysis	Contextual Awareness [Dynamic Threat Awareness]	[not referenced – requirement on development]
SA-11(5)	Developer Testing and Evaluation | Penetration Testing	Coordinated Protection [Self-Challenge]	[not referenced – requirement on development]
SA-11(6)	Developer Testing and Evaluation | Attack Surface Reviews	Realignment [Replacement]	[not referenced – requirement on development]
SA-15(5)	Development Process, Standards, and Tools | Attack Surface Reduction	Realignment [Replacement]	[not referenced – requirement on development]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SA-17(6)	Developer Security Architecture and Design | Structure for Testing	Realignment [Evolvability]	[not referenced – requirement on development]
SA-17(8)	Developer Security Architecture and Design | Orchestration	Coordinated Protection [Orchestration]	[not referenced – applies to system design]
SA-17(9)	Developer Security Architecture and Design | Design Diversity	Diversity [Design Diversity]	CM1128, CM1143, CM1144
SA-20	Customized Development of Critical Components	Realignment [Specialization]	CM1144, CM1315
SA-23	Specialization	Realignment [Specialization]	CM1144, CM1315, CM1223
System and Communications Protection			
SC-2	Separation of System and User Functionality	Segmentation [Predefined Segmentation]	CM1118
SC-2(1)	Separation of System and User Functionality | Interfaces for Non-Privileged Users	Segmentation [Predefined Segmentation]	CM1118
SC-3	Security Function Isolation	Segmentation [Predefined Segmentation]	M0930, M1030
SC-3(1)	Security Function Isolation | Hardware Separation	Segmentation [Predefined Segmentation]	CM1312
SC-3(2)	Security Function Isolation | Access and Flow Control Functions	Segmentation [Predefined Segmentation]	CM1311
SC-3(3)	Security Function Isolation | Minimize Nonsecurity Functionality	Realignment [Restriction]	M1037, M1042
SC-3(5)	Security Function Isolation | Layered Structures	Coordinated Protection [Orchestration] Segmentation [Predefined Segmentation] Realignment [Offloading]	CM1307
SC-5(2)	Denial-of-Service Protection | Capacity, Bandwidth, and Redundancy	Adaptive Response [Dynamic Resource Allocation] Redundancy [Surplus Capacity]	CM1147, CM1247
SC-5(3)	Denial-of-Service Protection | Detection and Monitoring	Analytic Monitoring [Monitoring and Damage Assessment]	CM1147, CM1247
SC-7	Boundary Protection	Segmentation [Predefined Segmentation]	M0803, M0812, M0930, M1030

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SC-7(10)	Boundary Protection | Prevent Exfiltration	Analytic Monitoring [Monitoring and Damage Assessment] Non-Persistence [Non-Persistent Information, Non-Persistent Connectivity] Coordinated Protection [Self-Challenge]	M0803, CM1107, CM1127, CM1207, CM1227
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	Substantiated Integrity [Provenance Tracking]	M1037
SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	Segmentation [Predefined Segmentation]	CM1308
SC-7(15)	Boundary Protection | Network Privilege Accesses	Realignment [Offloading] Segmentation [Predefined Segmentation] Privilege Restriction [Trust-Based Privileged Management]	CM1153, CM1253
SC-7(16)	Boundary Protection | Prevent Discovery of Components And Devices	Deception [Obfuscation] Dynamic Positioning {Functional Relocation of Cyber Resources]	CM1160, CM1260
SC-7(20)	Boundary Protection | Dynamic Isolation and Segregation	Segmentation [Dynamic Segmentation and Isolation] Adaptive Response [Dynamic Reconfiguration]	CM1108, CM1109, CM1139, CM1145, CM1208, CM1209, CM1245
SC-7(21)	Boundary Protection | Isolation of System Components	Segmentation [Predefined Segmentation]	M0930, M1029, M1030, CM1102, CM1131, CM1133, CM1151, CM1202
SC-7(22)	Boundary Protection | Separate Subnets for Connecting to Different Security Domains	Segmentation [Predefined Segmentation]	M0930, CM1151
SC-7(29)	Boundary Protection | Separate Subnets to Isolate Functions	Segmentation [Predefined Segmentation]	M0930, M1030
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]	M0802, M0808, M1041
SC-8(4)	Transmission Confidentiality and Integrity | Conceal or Randomize Communications	Deception [Obfuscation] Unpredictability [Contextual Unpredictability]	M1041
SC-8(5)	Transmission Confidentiality and Integrity | Protected Distribution System	Substantiated Integrity [Integrity Checks] Segmentation [Predefined Segmentation]	CM1148, CM1248

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SC-10	Network Disconnect	Non-Persistence [Non-Persistent Connectivity]	CM1127, CM1227
SC-11	Trusted Path	Segmentation [Predefined Segmentation] Substantiated Integrity [Provenance Tracking]	CM1120
SC-15(1)	Collaborative Computing Devices | Physical or Logical Disconnect	Non-Persistence [Non-Persistent Connectivity]	CM1121
SC-16(1)	Transmission Of Security and Privacy Attributes | Integrity Verification	Substantiated Integrity [Integrity Checks]	CM1137, CM1237
SC-16(3)	Transmission Of Security and Privacy Attributes | Cryptographic Binding	Substantiated Integrity [Integrity Checks]	CM1137, CM1237
SC-18(5)	Mobile Code | Allow Execution Only in Confined Environments	Segmentation [Dynamic Segmentation and Isolation]	M0948, M1048
SC-22	Architecture And Provisioning for Name/Address Resolution Service	Redundancy [Replication]	CM1143
SC-23(3)	Session Authenticity | Unique System-Generated Session Identifiers	Non-Persistence [Non-Persistent Information] Unpredictability [Temporal Unpredictability]	CM1124, CM1146
SC-25	Thin Nodes	Realignment [Offloading, Restriction] Non-Persistence [Non-Persistent Services, Non-Persistent Information]	CM1115, CM1119
SC-26	Decoys	Deception [Misdirection] Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]	CM1102, CM1104, CM1113, CM1123, CM1131, CM1202, CM1204, CM1223
SC-27	Platform-Independent Applications	Diversity [Architectural Diversity] Realignment [Evolvability]	CM1163
SC-28(1)	Protection Of Information at Rest | Cryptographic Protection	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]	M0941, M1041, CM1135, CM1160, CM1260
SC-29	Heterogeneity	Diversity [Architectural Diversity]	M0801, M0802, M0812, M0813, CM1104, CM1143, CM1144, CM1163, CM1305, CM1204, CM1275
SC-29(1)	Heterogeneity | Virtualization Techniques	Diversity [Architectural Diversity] Non-Persistence [Non-Persistent Services]	CM1305

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SC-30	Concealment and Misdirection	Deception [Obfuscation, Misdirection]	M0809, CM1148, CM1160, CM1248, CM1260
SC-30(2)	Concealment and Misdirection | Randomness	Unpredictability [Temporal Unpredictability, Contextual Unpredictability]	CM1146, CM1304
SC-30(3)	Concealment and Misdirection | Change Processing and Storage Locations	Dynamic Positioning [Functional Relocation of Cyber Resources, Asset Mobility] Unpredictability [Temporal Unpredictability]	CM1116, CM1150, CM1156
SC-30(4)	Concealment and Misdirection | Misleading Information	Deception [Disinformation]	M1021, CM1101, CM1102, CM1113, CM1131, CM1161, CM1201, CM1202
SC-30(5)	Concealment and Misdirection | Concealment of System Components	Deception [Obfuscation]	CM1160, CM1260
SC-32	System Partitioning	Segmentation [Predefined Segmentation]	CM1118
SC-32(1)	System Partitioning | Separate Physical Domains for Privileged Functions	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]	CM1118
SC-34	Non-Modifiable Executable Programs	Substantiated Integrity [Integrity Checks]	M1022, M1038, CM1115
SC-34(1)	Non-Modifiable Executable Programs | No Writable Storage	Non-Persistence [Non-Persistent Information]	CM1115, M1038
SC-34(2)	Non-Modifiable Executable Programs | Integrity Protection On Read-Only Media	Substantiated Integrity [Integrity Checks]	[not referenced – addresses threats not covered by ATT&CK]
SC-35	External Malicious Code Identification	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis] Deception [Misdirection] Segmentation [Dynamic Segmentation and Isolation]	CM1123, CM1136, CM1223
SC-36	Distributed Processing and Storage	Dynamic Positioning [Distributed Functionality, Functional Relocation of Cyber Resources] Redundancy [Replication]	CM1141
SC-36(1)	Distributed Processing and Storage | Polling Techniques	Adaptive Response [Adaptive Management] Substantiated Integrity [Behavior Validation]	CM1310

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SC-36(2)	Distributed Processing and Storage | Synchronization	Coordinated Protection [Orchestration] Redundancy [Replication]	CM1310
SC-37	Out-Of-Band Channels	Diversity [Path Diversity]	M0810
SC-39	Process Isolation	Segmentation [Predefined Segmentation, Dynamic Segmentation, and Isolation]	M0948, M1048
SC-39(1)	Process Isolation | Hardware Separation	Segmentation [Predefined Segmentation, Dynamic Segmentation, and Isolation]	CM1312
SC-39(2)	Process Isolation | Separation Execution Domains Per Thread	Segmentation [Predefined Segmentation, Dynamic Segmentation, and Isolation]	CM1311
SC-40(2)	Wireless Link Protection | Reduce Detection Potential	Deception [Obfuscation]	M0806
SC-40(3)	Wireless Link Protection | Imitative or Manipulative Communications Deception	Deception [Obfuscation] Unpredictability [Temporal Unpredictability, Contextual Unpredictability]	[not referenced – addresses threats not covered by ATT&CK]
SC-44	Detonation Chambers	Segmentation [Predefined Segmentation] Analytic Monitoring [Forensic and Behavioral Analysis] Deception [Misdirection]	M1031, M1049, CM1103, CM1123, CM1223
SC-46	Cross Domain Policy Enforcement	Segmentation [Predefined Segmentation]	CM1151, CM1153, CM1253
SC-47	Alternate Communication Paths	Diversity [Path Diversity]	CM1126, CM1140, CM1226
SC-48	Sensor Relocation	Dynamic Positioning [Functional Relocation of Sensors]	CM1145, CM1245
SC-48(1)	Sensor Relocation | Dynamic Relocation of Sensors Or Monitoring Capabilities	Dynamic Positioning [Functional Relocation of Sensors]	CM1145, CM1245
SC-49	Hardware-Enforced Separation and Policy Enforcement	Segmentation [Predefined Segmentation]	CM1312
SC-50	Software-Enforced Separation and Policy Enforcement	Segmentation [Predefined Segmentation]	CM1311, CM1312
SC-51	Hardware-Based Protection	Substantiated Integrity [Integrity Checks]	CM1154, CM1254
System and Information Integrity			
SI-3(10)	Malicious Code Protection | Malicious Code Analysis	Analytic Monitoring [Forensic and Behavioral Analysis]	CM1131

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SI-4(1)	System Monitoring | System-Wide Intrusion Detection System	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Mission Dependency and Status Visualization]	CM1122, CM1145, CM1302, CM1222, CM1245
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	Analytic Monitoring [Monitoring and Damage Assessment] Contextual Awareness [Mission Dependency and Status Visualization] Substantiated Integrity [Behavior Validation]	M0815, M1029, CM1110, CM1302, CM1314, CM2002, CM2004, CM2007, CM2014, CM2015, CM2020, CM2021, CM2029, CM2033, CM2034, CM2038, CM2040, CM2044, CM2102, CM2104, CM2115, CM2120, CM2121, CM2129, CM2133, CM2138, CM2144
SI-4(3)	System Monitoring | Automated Tool and Mechanism Integration	Analytic Monitoring [Sensor Fusion and Analysis] Adaptive Response [Adaptive Management]	M1016, CM1303, CM1314
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	M0931, M1016, M1031, CM2002, CM2038, CM2040, CM2102, CM2138
SI-4(7)	System Monitoring | Automated Response to Suspicious Events	Analytic Monitoring [Monitoring and Damage Assessment] Adaptive Response [Adaptive Management]	M0815, M0937, CM1303, CM1314
SI-4(10)	System Monitoring | Visibility of Encrypted Communications	Analytic Monitoring [Monitoring and Damage Assessment]	M0920, M1020, CM2002, CM2102
SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies	Analytic Monitoring [Monitoring and Damage Assessment]	CM2004, CM2047, CM2104, CM2147
SI-4(13)	System Monitoring | Analyze Traffic and Event Patterns	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CM2005, CM2029, CM2038, CM2040, CM2041, CM2047, CM2105, CM2129, CM2138, CM2147
SI-4(16)	System Monitoring | Correlate Monitoring Information	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Resource Awareness]	CM2005, CM2013, CM2022, CM2105, CM2113, CM2122
SI-4(17)	System Monitoring | Integrated Situational Awareness	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Resource Awareness]	CM2012

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SI-4(18)	System Monitoring | Analyze Traffic and Covert Exfiltration	Analytic Monitoring [Monitoring and Damage Assessment]	CM2002, CM2042
SI-4(24)	System Monitoring | Indicators of Compromise	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion, and Analysis]	CM2033, CM2133
SI-4(25)	System Monitoring | Optimize Network Traffic Analysis	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion, and Analysis]	M0920, M1020, CM2041, CM2102, CM2141, CM2141
SI-6	Security and Privacy Function Verification	Substantiated Integrity [Integrity Checks]	M0946, M1046
SI-7	Software, Firmware, and Information Integrity	Substantiated Integrity [Integrity Checks]	M0810, M0945, M0946, M0947, M0950, M1046, M1047, CM1122, CM1137, CM2009, CM1237, CM2109
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	Substantiated Integrity [Integrity Checks]	M0945, M0946, M1046, M1047, CM1110, CM1122, CM1130, CM1137, CM2009, CM1222, CM1230, CM1237, CM2109
SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations	Substantiated Integrity [Integrity Checks] Adaptive Response [Adaptive Management]	CM1303, CM1314
SI-7(6)	Software, Firmware, and Information Integrity | Cryptographic Protection	Substantiated Integrity [Integrity Checks]	M0947, M1042, M1046, CM2009, CM2109
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	Substantiated Integrity [Integrity Checks] Analytic Monitoring [Monitoring and Damage Assessment]	CM1110
SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process	Substantiated Integrity [Integrity Checks]	M0946, M1046
SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	Substantiated Integrity [Integrity Checks]	M0946, M1046
SI-7(12)	Software, Firmware, and Information Integrity | Integrity Verification	Substantiated Integrity [Integrity Checks]	M0947
SI-7(15)	Software, Firmware, and Information Integrity | Code Authentication	Substantiated Integrity [Provenance Tracking]	M0945, M0947, M1045
SI-10(3)	Information Input Validation |Predictable Behavior	Substantiated Integrity [Behavior Validation]	[not referenced – addresses threats not covered by ATT&CK]

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SI-10(5)	Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats	Substantiated Integrity [Provenance Tracking]	M1037
SI-14	Non-Persistence	Non-Persistence [Non-Persistent Services]	CM1109, CM1132, CM1209
SI-14(1)	Non-Persistence | Refresh from Trusted Sources	Non-Persistence [Non-Persistent Services, Non-Persistent Information] Substantiated Integrity [Provenance Tracking]	M1038, CM1134, CM1150, CM1234
SI-14(2)	Non-Persistence | Non-Persistent Information	Non-Persistence [Non-Persistent Information]	M1047, M1054, CM1124, CM1132, CM1134
SI-14(3)	Non-Persistence | Non-Persistent Connectivity	Non-Persistence [Non-Persistent Connectivity]	CM1127, CM1146, CM1227
SI-15	Information Output Filtering	Substantiated Integrity [Integrity Checks]	CM1155, CM1255
SI-16	Memory Protection	Diversity [Synthetic Diversity] Realignment [Restriction] Unpredictability [Temporal Unpredictability]	M0950, M1050, CM1152
SI-19(4)	De-Identification | Removal, Masking, Encryption, Hashing, or Replacement of Direct Identifiers	Deception [Obfuscation]	CM1135
SI-19(6)	De-Identification | Differential Privacy	Deception [Obfuscation] Uncertainty [Contextual Uncertainty]	CM1304
SI-19(8)	De-Identification | Motivated Intruder	Coordinated Protection [Self-Challenge]	CM1107, CM1313
SI-20	Tainting	Deception [Tainting]	CM1101, CM1112, CM1113, CM1161, CM1201
SI-21	Information Refresh	Non-Persistence [Non-Persistent Information]	M1054, CM1124
SI-22	Information Diversity	Diversity [Information Diversity]	CM1138, CM1141
SI-23	Information Fragmentation	Dynamic Positioning [Fragmentation]	CM1114, CM1141
Supply Chain Risk Management			
SR-3(1)	Supply Chain Controls and Processes | Diverse Supply Base	Diversity [Supply Chain Diversity]	CM1106
SR-3(2)	Supply Chain Controls and Processes | Limitation Of Harm	Diversity [Supply Chain Diversity] Deception [Obfuscation]	CM1106, CM1162, CM1262
SR-4	Provenance	Substantiated Integrity [Provenance Tracking]	M0945, CM1105, CM1205

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	MITIGATIONS AND CANDIDATE MITIGATIONS (CMs)
SR-4(1)	Provenance | Identity	Substantiated Integrity [Provenance Tracking]	M0945, CM1105, CM1205
SR-4(2)	Provenance | Track and Trace	Substantiated Integrity [Provenance Tracking]	CM1105, CM1205
SR-4(3)	Provenance | Validate as Genuine And Not Altered	Substantiated Integrity [Integrity Checks, Provenance Tracking]	M0916, M0945, M1045, CM1105, CM1132, CM2009, CM1205, CM2109
SR-4(4)	Provenance | Supply Chain Integrity – Pedigree	Substantiated Integrity [Provenance Tracking]	M0916, CM1105, CM1205
SR-5	Acquisition Strategies, Tools, and Methods	Substantiated Integrity [Integrity Checks, Provenance Tracking] Deception [Obfuscation]	CM1162, CM1262
SR-5(1)	Acquisition Strategies, Tools, and Methods | Adequate Supply	Redundancy [Replication] Diversity [Supply Chain Diversity]	CM1163, CM1315
SR-6(1)	Supplier Assessments and Reviews | Testing and Analysis	Coordinated Protection [Self-Challenge] Analytic Monitoring [Monitoring and Damage Assessment]	CM1162, CM2010, CM1262, CM2110
SR-7	Supply Chain Operations Security	Deception [Obfuscation, Disinformation, Self-Challenge]	CM1162, CM1262
SR-9	Tamper Resistance and Detection	Substantiated Integrity [Integrity Checks]	CM2011, CM2111
SR-9(1)	Tamper Resistance and Detection | Multiple Phases of System Development Life Cycle	Substantiated Integrity [Integrity Checks] Deception [Obfuscation]	[not referenced – addresses threats not covered by ATT&CK]
SR-10	Inspection of Systems or Components	Substantiated Integrity [Integrity Checks] Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]	CM1162, CM2006, CM2011, CM2106, CM2111
SR-11	Component Authenticity	Substantiated Integrity [Integrity Checks, Provenance Tracking]	CM1162, CM1262
SR-11(3)	Component Authenticity | Anti-Counterfeit Scanning	Substantiated Integrity [Integrity Checks]	CM1105, CM1205

Appendix C Specific Descriptions of Candidate Mitigations

The following tables amplify the tables in Sections 4 and 6. For each Candidate Mitigation (CM), a specific description is given for each Technique for which it could be used. Some controls, most notably IR-4(13) and SI-4(2) for detection, are used by multiple CMs; however, the uses – and hence the tailoring of those controls (and of their base controls, in the case of control enhancements) – differ, depending on the description of the CM.

Table 36. CMs for Detection – Technique-Specific Descriptions

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2002	**Inspect and Analyze Network Traffic**	AC-2(12), AU-6, IR-4(13), SI-4(2), SI-4(4), SI-4(10), SI-4(18)	Analyze network traffic for unusual data flows. Traffic inspection and analysis can be performed at the enterprise boundary, at internal boundaries between enclaves, or within enclaves.	Monitoring and Damage Assessment, Behavior Analysis
Discussion: Patterns of network traffic – e.g., pairings of message sources and destinations, message contents – are generally predictable, with variations based on time of day, day of week, or other known factors. Changes in traffic to or from a specific destination can be an indicator of malicious activity, as can some specific message characteristics (e.g., message size, message contents, message structure). Traffic inspection and analysis can be performed at the enterprise boundary, at internal boundaries between enclaves, or within enclaves. Baseline patterns must be established, and analysis is needed to determine whether the anomalies are due to events external to the system (e.g., failures in supporting infrastructures, natural disasters). This CM focuses on patterns of data flows and message characteristics, rather than on deep analysis of message contents. That analysis of message contents is the focus of CM2041.				
T1002 (Data Compressed): Look for compressed files in transit.				
T1022 (Data Encrypted): Look for encrypted files in transit.				
T1027 (Obfuscated Files or Information): Use network intrusion detection systems and email gateway filtering to identify compressed and encrypted attachments and scripts. Payloads delivered over an encrypted connection from a website require encrypted network traffic inspection.				
T1030 (Data Transfer Size Limits): Look at outgoing packet destinations.				
T1040 (Network Sniffing): Identify changes in information flows within an enclave indicating an adversary is performing a Adversary-in-the-Middle attack to capture network traffic. Monitor for ARP spoofing and gratuitous ARP broadcasts.				
T1046 (Network Scanning Service): Monitor for process use of the networks and inspect intra-network flows to detect port scans.				
T1047 (Windows Management Instrumentation): Monitor network traffic for WMI connections; the use of WMI in environments that do not typically use WMI may be suspect.				
T1071 (Application Layer Protocol), T1132 (Data Encoding), T1001 (Data Obfuscation), T1573 (Encrypted Channel), T1008 (Fallback Channels), T1105 (Ingress Tool Transfer), T1571 (Non-Standard Port), T1572 (Protocol Tunneling), T1090 (Proxy), T1219 (Remote Access Software): Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.				

T1095 (Non-Application Layer Protocol): Analyze network traffic for ICMP messages or other protocols that contain abnormal data or are not normally seen within or exiting the network. Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server).
T1114 (Email Collection): Look for Detect volumes of email with the "X-MS-Exchange-Organization-Auto-Forwarded" header without a corresponding number of emails that match the appearance of a forwarded message.
T1187 (Forced Authentication): Monitor for SMB traffic to unknown external systems and for unusual SMB traffic.
T1189 (Drive-by Compromise): Inspect URLs for known-bad domains, use reputation-based analytics, or look for known malicious scripts.
T1207 (Rogue Domain Controller): Monitor and analyze network traffic associated with data replication between domain controllers as well as to/from non-domain controller hosts.
T1205 (Traffic Signaling): Record network packets sent to and from the system, looking for extraneous packets that do not belong to established flows.
T1557 (Adversary-in-the-Middle): Monitor network traffic for anomalies associated with known MiTM behavior.
T1568 (Dynamic Resolution): Look for pseudo-randomly generated domain names and check for recently registered names or for rarely visited domains.
T1590 (Gather Victim Network Information): Monitor for anomalous traffic patterns, large or unexpected data transfers, and other activity that may reveal the presence of an adversary.
T1595 (Active Scanning): Analyze network traffic for indications of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet).
T1599 (Network Boundary Bridging): Monitor network traffic on both interfaces of border network devices, looking for traffic that should be prohibited by the intended network traffic policy enforcement for the border network device.
T1602 (Data from Configuration Repository): Identify network traffic sent or received by untrusted hosts or networks that solicits and obtains the configuration information of the queried device.
T1612 (Build Image on Host): Monitor for network communication with anomalous IP addresses that have never been seen before in the environment which could indicate the download of malicious code.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2003	**Endpoint Behavior Analysis**	AC-2(12)	Analyze the behavior of endpoint (i.e., end-user, client) systems for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation

Discussion: A variety of behaviors on an endpoint system can be observed and analyzed, either by the endpoint system (if it has the capacity) or by another system in the enterprise. This analysis typically uses logs, which are accumulated as part of basic hygiene (using AU-2). Analysis can feed forensics (CM2019). It can be aggregated across multiple endpoints and analyzed in light of network behavior; thus, the results of this CM can feed into CM2018.
T1068 (Exploitation for Privilege Escalation): Look for software crashes, abnormal process behavior, or unexpected files written to disk.
T1187 (Forced Authentication): Monitor creation and modification of .LNK, .SCF, or any other files on systems and within virtual environments that contain resources that point to external network resources.
T1189 (Drive-by Compromise): Look for suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic.

T1203 (Exploitation for Client Execution): Look for abnormal behavior of the browser or Office processes.				
T1210 (Exploitation of Remote Services): Look for suspicious files written to disk, evidence of Process Injection for attempts to hide execution, and evidence of Discovery.				
T1212 (Exploitation for Credential Access): Look for behavior on the system that might indicate successful compromise, such as abnormal behavior of processes.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2004	**Monitor Logs**	AU-6, IR-4(13), SI-4(2), SI-4(11)	Monitor system and application logs for anomalous or suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
Discussion: Devices, OSs, services, and applications perform logging to facilitate performance analysis and improvement. Those logs can be monitored for indicators of anomalous or suspicious behavior. Such indicators can be used to trigger defensive responses.				
T1003 (Credential Dumping): Monitor domain controller logs for replication requests and other unscheduled activity.				
T1053 (Scheduled Task): Configure event logging for scheduled task creation and changes. Monitor scheduled task creation from common utilities using command-line invocation, process execution from identified services.				
T1110 (Brute Force): Monitor authentication logs for system and application login failures of valid accounts.				
T1111 (Two-Factor Authentication Interception): Monitor for installation of a driver, setting a hook, or usage of particular API calls associated with polling to intercept keystrokes.				
T1133 (External Remote Services): Collect authentication logs for remote services and analyze for unusual access patterns, windows of activity, and access outside of normal business hours.				
T1137 (Office Application Startup): Collect process execution information including process IDs (PID) and parent process IDs (PPID) and look for abnormal chains of activity resulting from Office processes. Non-standard process execution trees may also indicate suspicious or malicious behavior.				
T1190 (Exploit Public-Facing Application): Monitor application logs for abnormal behavior.				
T1535 (Unused/Unsupported Cloud Regions): Monitor system logs to review activities occurring across all cloud environments and regions. Configure alerting to notify of activity in normally unused regions or if the number of instances active in a region goes above a certain threshold.				
T1538 (Cloud Service Dashboard): Monitor account activity logs to see actions performed and activity associated with the cloud service management console.				
T1564 (Hide Artifacts): Monitor event and authentication logs for records of hidden artifacts being used.				
T1569 (System Services): Monitor command files for unfamiliar launch agents or launch daemons.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2005	**Analyze Logs**	AC-2(12), SI-4(13), SI-4(16)	Analyze logs (individually or with some correlation across logs) for anomalous or suspicious patterns of behavior.	Monitoring and Damage Assessment, Dynamic Resource Awareness, Behavior Validation
Discussion: Devices, OSs, services, and applications perform logging to facilitate performance analysis and improvement. Those logs can be analyzed individually or monitored to trigger correlation analysis. By contrast with log monitoring (CM2004), log analysis is usually part of a larger investigatory effort (e.g., a SOC function).				

T1056 (Input Capture): Analyze logs to search for API calls which, in conjunction with other information such as new files written to disk and unusual processes, could indicate keylogging.
T1113 (Screen Capture): Monitor for image files written to disk, and correlate with other events to identify suspected malicious activity.
T1125 (Video Capture): Monitor for image files written to disk, and correlate with other events to identify suspected malicious activity.
T1133 (External Remote Services): Analyze authentication logs for unusual access patterns, windows of activity, and access outside of normal business hours.
T1202 (Indirect Command Execution): Monitor and analyze logs from host-based detection mechanisms, such as Sysmon, for events such as process creations that include or are resulting from parameters associated with invoking programs/commands/files and/or spawning child processes/network connections.
T1222 (File and Directory Permissions Modification): Investigate attempts to modify ACLs and file/directory ownership; compare against baseline knowledge for how systems are typically used and correlate modification events with other indications of malicious activity where possible.
T1484 (Domain Policy Modification): Analyze logs for changes to directory service objects.
T1505 (Server Software Component): Monitor application logs for abnormal behavior that may indicate suspicious installation of application software components.
T1548 (Abuse Elevation Control Mechanism): Analyze logs to look for any process API calls for behavior that may be indicative of Process Injection and unusual loaded DLLs through DLL Search Order Hijacking, which indicate attempts to gain access to higher privileged processes.
T1553 (Subvert Trust Controls): Analyze Autoruns data for oddities and anomalies, specifically malicious files attempting persistent execution by hiding within auto-starting locations.
T1609 (Container Administration Command): Analyze logs to look at container administration service activities and executed commands.
T1610 (Deploy Container): Correlate and analyze logs across container clusters, looking for suspicious or unknown container images.
T1611 (Escape to Host): Correlate and analyze logs across container clusters, looking for suspicious or unknown container images.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2006	**Analyze File Contents**	SR-10	Analyze contents of specific files or types of files for suspicious contents.	Forensic and Behavioral Analysis
T1154 (Trap): Monitor the contents of command files for suspicious or overly broad trap commands.				
T1565 (Data Manipulation): Inspect important application binary file hashes, locations, and parameters for suspicious or unexpected values.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2007	**Host Event Detection**	CM-8(3), IR-4(13), SI-4(2)	Detect anomalous or unauthorized events on hosts (e.g., servers, endpoint systems).	Monitoring and Damage Assessment, Behavior Validation
T1052 (Exfiltration Over Physical Medium): Detect processes that execute when removable media are mounted.				

T1055 (Process Injection): Monitor DLL/PE file events, specifically creation of these binary files as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process.				
T1200 (Hardware Additions): Detect devices connected to system ports.				
T1561 (Disk Wipe): Look for attempts to read/write to sensitive locations like the partition boot sector or BIOS parameter block/superblock. Monitor for unusual kernel driver installation activity.				
T1610 (Deploy Container), T1611 (Escape to Host): Monitor for the deployment of suspicious or unknown container images and pods in the host environment.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2008	**Removable Device Usage Detection**	CM-8(3)	Detect anomalous or unauthorized events involving use of removable devices.	Monitoring and Damage Assessment
T1052 (Exfiltration Over Physical Medium): Monitor file accesses (particularly write, append, or modify) on removable devices or media.				
T1091 (Replication Through Removable Media): Monitor file accesses (particularly read and execute) on removable devices or media.				
T1092 (Communication Through Removable Media): Monitor file access on removable media. Detect processes that execute when removable media is mounted.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2009	**Software Integrity Check**	SI-7, SI-7(1), SI-7(6), CM-14, SR-4(3)	Perform integrity checks (e.g., using checksums, hashes, or digital signatures) on software, software certificates, or metadata.	Integrity Checks, Provenance Tracking
T1601 (Modify System Image): Compare the checksum of the operating system file with the checksum of a known good copy from a trusted source, if possible; if not, download a copy of the file to a trusted computer to calculate the checksum with software that is not compromised.				
T1195 (Supply Chain Compromise): Perform integrity checks on as-delivered software (including updates) upon arrival.				
T1543 (Create or Modify System Process): Monitor for changes to system processes that do not correlate with known software, patch cycles, etc., including by comparing results against a trusted system baseline.				
T1553 (Subvert Trust Controls): Collect and analyze signing certificate metadata on software that executes within the environment to look for unusual certificate characteristics and outliers. Periodically baseline registered Subject Interface Packages (SIPs) and trust providers (Registry entries and files on disk), specifically looking for new, modified, or non-Microsoft entries.				
T1554 (Compromise Client Software Binaries): Collect and analyze signing certificate metadata and check signature validity on software that executes within the environment.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2010	**Software Stressing**	SR-6(1)	Perform software stress testing (e.g., using out-of-bounds input values) prior to installation.	Self-Challenge

T1195 (Supply Chain Compromise): Perform stress testing on as-delivered software (including updates) upon arrival.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2011	**Physical Inspection**	SR-9, SR-10	Perform physical inspection of hardware components for indicators of tampering.	Integrity Checks

T1195 (Supply Chain Compromise): Perform physical inspection of hardware component packaging, and spot-check components, upon delivery.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2012	**Monitor Trusted Parties**	PM-16, PM-30(1), SI-4(17)	Monitor the behavior and status (e.g., change in ownership) of second or third parties.	Dynamic Resource Awareness, Dynamic Threat Awareness, Behavior Validation, Provenance Tracking

T1072 (Software Deployment Tools): Monitor the status of third-party software providers.

T1199 (Trusted Relationship): Monitor the behavior of, and track behavioral indicators for, trusted second or third parties.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2013	**Cross Enterprise Account Usage Analysis**	AU-6(3), SI-4(16)	Analyze account usage across the enterprise for anomalies or suspicious behavior.	Sensor Fusion and Analysis

Discussion: Systems, applications, and devices often share accounts for users, administrators, or services. This differs from Account Monitoring (CM2021) in that it involves looking across the different places on which the same account is used, analyzing patterns of use, and looking at a broader range of account types.

T1078 (Valid Accounts): Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts (e.g., one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours). Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

T1550 (Use Alternate Authentication Material): Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours. Activity may be from interactive login sessions or process ownership from accounts being used to execute binaries on a remote system as a particular account. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2014	**Process Analysis**	IR-4(13), SI-4(2)	Analyze process attributes or behavior for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment

T1055 (Process Injection): Analyze process behavior to determine if a process is performing actions it usually does not, such as opening network connections, reading files, or other suspicious actions that could relate to post-compromise behavior.				
T1134 (Access Token Manipulation): Look for inconsistencies between the various fields that contain parent process identification.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2015	**Process Monitoring**	AU-6, IR-4(13), SI-4(2)	Monitor the behavior of processes for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
Discussion: The phrase "monitor processes" appears frequently in the descriptions of detection methods in ATT&CK for Enterprise. Abnormal behavior of processes can indicate misuse and can indicate the potential for subsequent harmful events.				
T1002 (Data Compressed): Monitor processes for use of data compression utilities.				
T1005 (Data from Local System): Monitor processes for behavior typical of collection.				
T1006 (Direct Volume Access): Monitor processes and command-line arguments for actions that could be taken to copy files from the logical drive and evade common file system protections.				
T1011 (Exfiltration Over Other Network Medium): Monitor for processes that normally require user-driven events to access the network (for example, a web browser opening with a mouse click or key press) but access the network without such.				
T1012 (Query Registry): Monitor processes and command-line arguments for invocation of utilities used to query the Registry.				
T1020 (Automated Exfiltration): Monitor processes' file access patterns and network behavior.				
T1022 (Data Encrypted): Monitor processes for use of data encryption utilities.				
T1029 (Scheduled Transfer): Monitor process file access patterns and network behavior, looking for unrecognized processes or scripts that appear to be traversing file systems and sending network traffic.				
T1037 (Boot or Logon Initialization Scripts): Monitor running process for actions that could be indicative of abnormal programs or executables running upon logon.				
T1039 (Data from Network Shared Drive): Monitor processes for behavior typical of collection.				
T1047 (Windows Management Instrumentation): Perform process monitoring to capture command-line arguments of "wmic" and detect commands that are used to perform remote behavior.				
T1074 (Data Staged): Monitor processes for actions that could be taken to collect and combine files.				
T1080 (Taint Shared Content): Monitor processes that are executed from removable media for malicious or abnormal activity such as network connections due to Command and Control and possible network Discovery techniques.				
T1087 (Account Discovery), T1010 (Application Window Discovery), T1482 (Domain Trust Discovery), T1083 (File and Directory Discovery), T1135 (Network Share Discovery), T1120 (Peripheral Device Discovery), T1069 (Permission Groups Discovery), T1057 (Process Discovery), T1018 (Remote System Discovery), T1518 (Software Discovery), T1082 (System Information Discovery), T1016 (System Network Configuration Discovery), T1049 (System Network Connections Discovery), T1033 (System Owner/User Discovery), T1007 (System Service Discovery): Monitor processes and command-line arguments for actions that could be taken to gather system and network information.				

T1105 (Ingress Tool Transfer): Monitor for unusual processes with external network connections creating files on-system.
T1112 (Modify Registry): Monitor processes and command-line arguments for actions that could be taken to change or delete information in the Registry.
T1114 (Email Collection): Monitor processes for actions that could be taken to gather local email files.
T1119 (Automated Collection): Monitor processes for behavior typical of collection.
T1127 (Trusted Developer Utilities Proxy Execution): Monitor the execution and arguments of trusted developer utilities (e.g., MSBuild.exe, dnx.exe, rcsi.exe, WinDbg.exe, cdb.exe, and tracker.exe).
T1136 (Create Account): Monitor for processes associated with account creation.
T1173 (Dynamic Data Exchange): Monitor for spawning of unusual processes (such as cmd.exe) from Microsoft Office applications.
T1176 (Browser Extensions): Monitor processes to detect browsers communicating with a C2 server.
T1183 (Audio Capture): Monitor processes for interaction with the microphone, recording devices, or recording software.
T1201 (Password Policy Discovery): Monitor processes for tools and command line arguments that may indicate they are being used for password policy discovery.
T1216 (Signed Script Proxy Execution): Monitor script processes, such as cscript, that may be used to proxy execution of malicious files.
T1217 (Browser Bookmark Discovery): Monitor processes and command-line arguments for actions that could be taken to gather browser bookmarks.
T1218 (Signed Binary Proxy Execution): Monitor processes for signed binaries that may be used to proxy execution of malicious files.
T1220 (XSL Script Processing): Monitor the execution and arguments of msxsl.exe and wmic.exe.
T1485 (Data Destruction): Monitor the execution and command-line parameters of binaries that could be involved in data destruction activity. Monitor for the creation of suspicious files as well as high unusual file modification activity. In particular, look for large quantities of file modifications in user directories and under system directories.
T1486 (Data Encrypted for Impact): Monitor the execution and command line parameters of binaries involved in data destruction activity. Monitor for the creation of suspicious files as well as unusual file modification activity. In particular, look for large quantities of file modifications in user directories. Look for the execution of utilities commonly used for data destruction, such as SDelete.
T1489 (Service Stop): Monitor processes and command-line arguments to see if critical processes are terminated or stop running.
T1490 (Inhibit System Recovery): Monitor the execution and command line parameters of binaries involved in inhibiting system recovery.
T1491 (Defacement): Monitor internal and external websites for unplanned content changes. Monitor application logs for abnormal behavior that may indicate attempted or successful exploitation. Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection. Web Application Firewalls may detect improper inputs attempting exploitation.
T1495 (Firmware Corruption): Monitor the execution and command line parameters of binaries involved in inhibiting system recovery.
T1505 (Server Software Component): Process monitoring may be used to detect server components that perform suspicious actions such as running cmd.exe or accessing files.

T1529 (System Shutdown / Reboot): Monitor the execution and command line parameters of binaries involved in shutting down or rebooting systems.

T1531 (Account Access Removal): Monitor the execution and command line parameters of binaries involved in deleting accounts or changing passwords. Monitor for changes to a user account outside normal business hours, from remote locations, etc.

T1546 (Event Triggered Execution): Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process. Look for abnormal process behavior that may be due to a process loading a malicious DLL.

T1562 (Impair Defenses): Monitor processes to see if security tools or logging services are killed or stop running, or otherwise show signs of being tampered with.

T1574 (Hijack Execution Flow): Monitor processes for unusual activity (e.g., a process that does not use the network begins to do so, abnormal process call trees).

T1612 (Build Image on Host): Monitor for unexpected Docker image build requests to the Docker daemon on hosts in the environment.

T1614 (System Location Discovery): Monitor processes for actions that could be taken to gather system location information.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2016	**Cloud Account Monitoring**	AC-2(12)	Monitor activity associated with cloud accounts for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation

T1530 (Data from Cloud Storage Object): Monitor for patterns of account behavior involving privilege escalation to obtain access to cloud data objects, and for unusual queries.

T1537 (Transfer Data to Cloud Account): Monitor account activity for attempts to share data, snapshots, or backups with untrusted or unusual accounts on the same cloud service provider, and for anomalous file transfer activity between accounts and to untrusted VPCs.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2017	**Privileged Account Monitoring**	AU-6(8)	Monitor and analyze activity associated with privileged accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment

T1040 (Network Sniffing): Monitor administrative logins, configuration changes, and changes to device images.

T1213 (Data from Information Repositories): Monitor and alert on access to information repositories by privileged users.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2018	**Cross-Enterprise Behavior Analysis**	AU-6(3), AU-6(5)	Correlate and analyze behavior of multiple systems.	Sensor Fusion and Analysis

T1021 (Remote Services): Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity.

T1072 (Software Deployment Tools): Analyze behavior of third-party software, as well as interactions between that software and system software, and correlate logs from third-party applications and software deployment systems with other system logs.
T1098 (Account Manipulation): Correlate changes to accounts or account objects across the enterprise.
T1102 (Web Service): Use host data that can relate unknown or suspicious process activity using a network connection to supplement any existing indicators of compromise based on malware command and control signatures and infrastructure or the presence of strong encryption.
T1104 (Multi-Stage Channels): Correlate host and network data to relate unknown or suspicious process activity using a network connection with any existing indicators of compromise based on malware command and control signatures and infrastructure.
T1115 (Clipboard Data): Correlate monitoring of clipboard use and other suspicious or non-user-driven activity.
T1552 (Unsecured Credentials): Correlate monitoring across the enterprise to look for anomalous uses of credentials.
T1556 (Modify Authentication Process): Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services. Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2019	**Endpoint Scrutiny**	IR-4(12)	Scrutinize the contents and behavior patterns of an endpoint system.	Forensic and Behavioral Analysis

T1203 (Exploitation for Client Execution): Look for suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.
T1542 (Pre-OS Boot): Use disk check, forensic utilities, and data from device drivers (i.e., processes and API calls) to reveal anomalies that warrant deeper investigation.
T1554 (Compromise Client Software Binaries): Look for changes to client software that do not correlate with known software or patch cycles. Consider monitoring for anomalous behavior from client applications, such as atypical module loads, file reads/writes, or network connections.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2020	**Application- or Utility-Specific Monitoring**	IR-4(13), SI-4(2)	Monitor and analyze events in the context of a specific application or utility.	Monitoring and Damage Assessment, Behavior Validation

Discussion: ATT&CK for Enterprise identifies a variety of circumstances under which different applications or utilities can be monitored for indications of adversary activity.
T1025 (Data from Removable Media): Monitor for data collection through Windows Management Instrumentation and PowerShell.
T1025 (Data from Removable Media): Monitor for remote access tools with built-in features that can interact directly with the Windows API to gather data.
T1074 (Data Staged): Monitor for data staging through Windows Management Instrumentation and PowerShell.
T1074 (Data Staged): Monitor for remote access tools with built-in features that can interact directly with the Windows API to stage data.

T1087 (Account Discovery): Monitor for the use of remote access tools or Windows system management tools to obtain system and network information.
T1010 (Application Window Discovery): Monitor for the use of remote access tools or Windows system management tools to obtain system and network information.
T1217 (Browser Bookmark Discovery): Monitor for the use of remote access tools or Windows system management tools to obtain system and network information.
T1482 (Domain Trust Discovery): Monitor for the use of remote access tools or Windows system management tools to obtain system and network information.
T1083 (File and Directory Discovery): Monitor for the use of remote access tools or Windows system management tools to obtain system and network information.
T1135 (Network Share Discovery): Monitor for the use of remote access tools or Windows system management tools to obtain system and network information.
T1113 (Screen Capture): Monitor the use of API calls to obtain image data.
T1114 (Email Collection): Monitor for data collection through Windows Management Instrumentation and PowerShell.
T1125 (Video Capture): Monitor the use of API calls to obtain video or camera data.
T1137 (Office Application Startup): Collect process execution information including process IDs and parent process IDs and look for abnormal chains of activity resulting from Office processes.
T1176 (Browser Extensions): Inventory and monitor browser extension installations that deviate from normal, expected, and benign extensions.
T1185 (Browser Session Hijacking): Monitor for process injection against browser applications.
T1197 (BITS Jobs): Monitor usage of the BITSAdmin tool; monitor and analyze network activity generated by BITS.
T1204 (User Execution): Monitor for applications which, with user interaction, an adversary can use to download malware (e.g., compression applications).
T1218 (Signed Binary Proxy Execution): Compare recent invocations of signed binaries that may be used to proxy execution with prior history of known good arguments and loaded files to determine anomalous and potentially adversarial activity. Monitor for legitimate programs used in suspicious ways, like msiexec.exe downloading an MSI file from the Internet, which may be indicative of an intrusion.
T1221 (Template Injection): Analyze process behavior to determine if an Office application is performing actions, such as opening network connections, reading files, spawning abnormal child processes (e.g., PowerShell), or other suspicious actions that could relate to post-compromise behavior.
T1526 (Cloud Service Discovery): Monitor cloud service usage for anomalous behavior that may indicate adversarial presence within the environment.
T1534 (Internal Spearphishing): Analyze internal emails or patterns of email traffic to identify possible internal spearphishing.
T1559 (Inter-Process Communication): Monitor uses of IPC for potentially malicious behavior.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2021	**Account Monitoring**	AC-2(12), IR-4(13), SI-4(2)	Monitor and analyze activity associated with user accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment, Behavior Validation

Discussion: Individual user accounts can be monitored for unusual or suspicious patterns of behavior. In contrast with CM2013, this monitoring typically occurs in the context of a single system or application, rather than across the enterprise.
T1098 (Account Manipulation): Monitor for use of credentials at unusual times or to unusual systems or services.
T1213 (Data from Information Repositories): Monitor and alert on users that are retrieving and viewing a large number of documents and pages in an information repository.
T1525 (Implant Internal Image): Monitor interactions with images and containers by users to identify ones that are added or modified anomalously.
T1556 (Modify Authentication Process): Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts.
T1563 (Remote Service Session Hijacking): Monitor for user accounts logged into systems they would not normally access or access patterns to multiple systems over a relatively short period of time.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2022	**Host-Local Event Correlation**	IR-4(13), SI-4(16)	Correlate and analyze events occurring on a single host.	Sensor Fusion and Analysis, Monitoring and Damage Assessment
T1106 (Native API): Correlate other events with behavior surrounding API function calls using API monitoring to evaluate behavior.				
T1140 (Deobfuscate/Decode Files of Information): Monitor the execution file paths and command-line arguments for common archive file applications and extensions, such as those for Zip and RAR archive tools, and correlate with other suspicious behavior to reduce false positives from normal user and administrator behavior.				
T1199 (Execution Through Module Load): Correlate other events with behavior surrounding module loads using API monitoring and suspicious DLLs written to disk.				
T1542 (Pre-OS Boot): Log changes to boot records, BIOS, and EFI, which can be performed by API calls, and compare against known good behavior and patching.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2023	**Centralize and Analyze Instance Logging**	AU-6(5), IR-4(4)	Centralize instance logging in a cloud or container environment and analyze.	Sensor Fusion and Analysis
T1578 (Modify Cloud Compute Infrastructure): Establish centralized logging for the activity of cloud compute infrastructure components. Monitor for suspicious sequences of events, such as the creation of multiple snapshots within a short period of time or the mount of a snapshot to a new instance by a new or unexpected user.				
T1613 (Container and Resource Discovery): Establish centralized logging for the activity of container and cluster components. Monitor logs for actions that could be taken to gather information about container infrastructure, including the use of discovery API calls by new or unexpected users.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2029	**Monitor Script Execution**	IR-4(13), SI-4(2), SI-4(13)	Monitor for the execution of scripts which are unknown or used in suspicious ways.	Monitoring and Damage Assessment
T1006 (Direct Volume Access): Log and analyze the use of PowerShell scripts.				

T1037 (Boot or Logon Initialization Scripts): Monitor logon scripts for unusual access by abnormal users or at abnormal times.
T1059 (Command and Scripting Interpreter): Monitor for execution of scripts that may be related to other suspicious behavior occurring on the system, e.g., running out of cycle from patching or other administrator functions.
T1216 (Signed Script Proxy Execution): Monitor script processes, such as cscript, and command-line parameters for scripts like PubPrn.vbs that may be used to proxy execution of malicious files.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2033	**Monitor the File System**	IR-4(13), SI-4(2), SI-4(24)	Monitor the file system to identify the unexpected presence and atypical use of files of specific types, or atypical patterns of access.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Behavior Validation

T1036 (Masquerading): Monitor for mismatches between file names and file hashes; for files with known names but in unusual locations; files that are modified outside of an update or patch; and indications of common characters that may indicate an attempt to trick users into misidentifying the file type.
T1039 (Data from Network Shared Drive): Monitor the file system on a network shared drive for atypical patterns of access.
T1056 (Input Capture): Monitor the Registry and file system for changes indicating driver installs or the addition of a Custom Credential Provider.
T1071 (Indicator Removal on Host): Monitor the file system to detect improper deletion or modification of indicator files.
T1074 (Data Staged): Monitor publicly writeable directories, central locations and commonly used staging directories for compressed or encrypted data.
T1105 (Ingress Tool Transfer): Monitor for file creation and files transferred into the network.
T1137 (Office Application Startup): Collect and analyze events related to Registry key creation and modification for keys that could be used for Office-based persistence.
T1490 (Inhibit System Recovery): Monitor the registry for changes associated with system recovery features.
T1548 (Abuse Elevation Control Mechanism): Monitor the file system for files that have the setuid or setgid bits set.
T1555 (Credentials from Password Stores): Monitor system calls, file read events, and processes for suspicious activity that could indicate searching for a password. File read events should be monitored surrounding known password storage applications.
T1560 (Archive Collected Data): Monitor for writing of files with extensions and/or headers associated with compressed or encrypted file types. Detection efforts may focus on follow-on exfiltration activity, where compressed or encrypted files can be detected in transit with a network intrusion detection or data loss prevention system analyzing file headers.
T1564 (Hide Artifacts): Monitor the file system for hidden attribute usage and for creation of hidden files.
T1570 (Lateral Tool Transfer): Monitor for file creation and files transferred within a network using protocols such as SMB.
T1574 (Hijack Execution Flow): Monitor file systems for moving, renaming, replacing, or modifying DLLs.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM2034	**Monitor Specific Servers**	IR-4(13), SI-4(2)	Monitor specific servers for anomalous or suspicious uses or access attempts.	Monitoring and Damage Assessment
T1114 (Email Collection): Monitor for unusual processes connecting to an email server within a network, or unusual access patterns or authentication attempts on public-facing webmail servers.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2035	**Monitor Specific Files**	AU-6	Monitor the use of specific files or directories for anomalous or suspicious uses or access attempts.	Behavior Validation, Monitoring and Damage Assessment
T1011 (Exfiltration Over Other Network Medium): Monitor for and investigate changes to host adapter settings, such as addition and/or replication of communication interfaces.				
T1053 (Scheduled Task): Monitor Windows Task Scheduler stores for change entries related to scheduled tasks that do not correlate with known software, patch cycles, etc.				
T1080 (Taint Shared Content): Frequently scan shared network directories for malicious files, hidden files, .LNK files, and other file types that may not typically exist in directories used to share specific types of content.				
T1546 (Event Triggered Execution): Monitoring for additions or modifications of mechanisms in event repositories that could be used to trigger event-based execution, especially the addition of abnormal commands such as execution of unknown programs, opening network sockets, or reaching out across the network.				
T1569 (System Services): Monitor for changes to service Registry entries that do not correlate with known software, patch cycles, etc.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2038	**Monitor Command Line Use**	IR-4(13), SI-4(2), SI-4(4), SI-4(13)	Monitor use of the command line interface for use of common utilities (part of the system or installed by the adversary), looking for suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
T1002 (Data Compression): Monitor the command line for arguments indicating the use of compression utilities.				
T1003 (Credential Dumping): Monitor command-line arguments for program execution that may be indicative of credential dumping.				
T1022 (Data Encryption): Monitor the command line for arguments indicating the use of encryption utilities.				
T1025 (Data from Removable Media): Monitor command-line arguments for actions that could be taken to collect files from a system's connected removable media.				
T1027 (Obfuscated Files or Information): Flag and analyze commands containing indicators of obfuscation and known suspicious syntax such as uninterpreted escape characters like "'^'" and """".				
T1059 (Command and Scripting Interpreter): Monitor command-line arguments for script execution and subsequent behavior.				
T1059 (Command Line Use): Capture command-line interface activities through proper logging of process execution with command-line arguments.				
T1074 (Data Staged): Monitor command-line arguments for actions that could be taken to collect and combine files.				

T1114 (Email Collection): Monitor command-line arguments for actions that could be taken to gather local email files.
T1124 (System Time Discovery): Monitor the command-line interface to detect instances of net.exe or other command-line utilities being used to gather system time or time zone.
T1134 (Access Token Manipulation): Detect token manipulation by auditing command-line activity. Specifically, analysts should look for use of the runas command.
T1216 (Signed Script Proxy Execution): Monitor command-line parameters for scripts like PubPrn.vbs that may be used to proxy execution of malicious files.
T1569 (System Services): Monitor for command-line invocation of tools capable of modifying services that do not correlate with known software, patch cycles, etc.
T1614 (System Location Discovery): Monitor processes for actions that could be taken to gather system location information.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2040	**Monitor Use of Libraries and Utilities**	IR-4(13), SI-4(2), SI-4(4), SI-4(13)	Monitor the use of libraries and utilities which are commonly used to support adversary actions.	Monitoring and Damage Assessment

T1022 (Data Encryption): Monitor for the use of utilities which perform encryption, decryption, or verification of file signatures (e.g., crypt32.dll).
T1173 (Dynamic Data Exchange): Monitor for Microsoft Office applications loading DLLs and other modules not typically associated with the application.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2041	**Analyze Network Traffic Content**	IR-4(13), SI-4(10), SI-4(25)	Analyze the contents of network traffic.	Monitoring and Damage Assessment, Behavior Validation

T1001 (Data Obfuscation): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1008 (Fallback Channels): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1030 (Data Transfer Size Limits): Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.
T1041 (Exfiltration over C2 Channel): Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.
T1048 (Exfiltration over Alternative Protocol): Analyze packet contents for protocols that do not match the port.
T1071 (Application Layer Protocol): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1090 (Proxy): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.

T1095 (Non-Application Layer Protocol): Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.
T1105 (Ingress Tool Transfer): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1132 (Data Encoding): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1219 (Remote Access Software): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1571 (Non-Standard Port): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1572 (Protocol Tunneling): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1573 (Encrypted Channel): Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.
T1598 (Phishing for Information): Monitor for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Monitor for references to uncategorized or known-bad sites in email. Monitor social media traffic for suspicious activity, including messages requesting information as well as abnormal file or data transfers (especially those involving unknown, or otherwise suspicious accounts).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2042	**Analyze Outgoing Traffic Patterns**	IR-4(13), SI-4(18)	Analyze outgoing traffic for patterns of behavior which could indicate adversary communications.	Monitoring and Damage Assessment, Behavior Validation

T1029 (Scheduled Transfer): Look for network connections to the same destination that occur at the same time of day for multiple days.
T1030 (Data Transfer Size Limits): Look for patterns of fixed-size outgoing packets, particularly at regular intervals or using a long connection.
T1048 (Exfiltration over Alternative Protocol): Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server).
T1102 (Web Service): Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server).
T1567 (Exfiltration Over Web Service): Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM2043	**Monitor External Sources**	AU-13, AU-13 (3), PM-16, RA-5(4), RA-10	Monitor and analyze external information sources for indicators of adversary activities, especially those targeting the organization.	Monitoring and Damage Assessment, Dynamic Threat Awareness
T1584 (Compromise Infrastructure): Monitor threat intelligence sources, and any other sources the organization uses covertly (e.g., on the Dark Web), for indications that external infrastructures have been compromised.				
T1585 (Establish Accounts): Monitor social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization.				
T1586 (Compromise Accounts): Monitor social media activity related to your organization. Suspicious activity may include personas claiming to work for your organization or recently modified accounts making numerous connection requests to accounts affiliated with your organization.				
T1587 (Develop Capabilities): Monitor threat intelligence sources, and any other sources the organization uses covertly (e.g., on the Dark Web), for indications (e.g., recruiting specific skills) that an adversary is developing capabilities which could be used against organizational systems.				
T1588 (Obtain Capabilities): Monitor threat intelligence sources, and any other sources the organization uses covertly (e.g., on the Dark Web), for indications that an adversary is obtaining capabilities which could be used against organizational systems.				
T1608 (Stage Capabilities): Monitor threat intelligence sources, and any other sources the organization uses covertly (e.g., on the Dark Web), for indications that an adversary is staging capabilities which could be used against organizational systems.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2044	**Monitor Platform Status**	IR-4(13), SI-4(2)	Monitor the status of platforms (e.g., user endpoints, servers, network devices) and other devices.	Monitoring and Damage Assessment
Discussion: The status of individual platforms (e.g., user endpoints, servers, network devices) and other devices (e.g., controllers, printers) can be monitored via polling, periodically or at random intervals. More detailed status information can be obtained by querying or examining settings, registries, and directories.				
T1011 (Exfiltration Over Other Network Medium): Look for and investigate changes to host adapter settings.				
T1014 (Rootkit): Monitor for the existence of unrecognized DLLs, devices, services, and changes to the Master Boot Record (MBR).				
T1037 (Boot or Logon Initialization Scripts): Look for files added or modified by unusual accounts outside of normal administration duties, and monitor running processes for actions that could be indicative of abnormal programs or executables running upon logon.				
T1112 (Modify Registry): Enable Registry Auditing on specific keys to produce an alertable event whenever a value is changed. Look for changes to Registry entries that load software on Windows startup that do not correlate with known software, patch cycles, etc., as well as additions or changes to files within the startup folder.				
T1489 (Service Stop): Monitor Registry edits for modifications to services and startup programs that correspond to services of high importance. Look for changes to service Registry entries that do not correlate with known software, patch cycles, etc.				
T1496 (Resource Hijacking): Monitor resource usage to determine anomalous activity associated with malicious hijacking of computer resources such as CPU, memory, and graphics processing resources.				

T1547 (Boot or Logon Autostart Execution): Monitor Registry changes that are not correlated with known updates, patches, or other planned administrative activity.				
T1599 (Network Boundary Bridging): Monitor the border network device's configuration to validate that the policy enforcement sections are what was intended. Look for rules that are less restrictive, or that allow specific traffic types that were not previously authorized.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2047	**Monitor Network Usage**	IR-4(13), SI-4(11), SI-4(13)	Monitor network usage for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation
T1041 (Exfiltration Over Command and Control Channel): Look for processes utilizing the network that do not normally have network communication or have never been seen before.				
T1011 (Exfiltration Over Other Network Medium): Monitor network usage to identify processes using the network that are unknown or ones that do not normally use the network.				
T1030 (Data Transfer Size Limits): Monitor network usage to identify processes using the network that are unknown or ones that do not normally use the network.				
T1048 (Exfiltration Over Alternative Protocol): Monitor network usage to identify processes using the network that are unknown or ones that do not normally use the network.				
T1210 (Exploitation of Remote Services): Monitor network usage to look for unusual network traffic that may indicate additional tools transferred to the system.				
T1496 (Resource Hijacking): Monitor for suspicious use of network resources associated with cryptocurrency mining software.				
T1498 (Network Denial of Service): Use network throughput monitoring tools to detect sudden increases in network or service utilization; perform real-time, automated, and qualitative study of the network traffic to identify a sudden surge in one type of protocol.				
T1499 (Endpoint Denial of Service): Use network throughput monitoring tools to detect sudden increases in network or service utilization; perform real-time, automated, and qualitative study of the network traffic to identify a sudden surge in one type of protocol.				
T1559 (Inter-Process Communication): Monitor for potentially malicious uses of IPC.				
T1572 (Protocol Tunneling): Monitor for systems listening and/or establishing external connections using ports/protocols commonly associated with tunneling, and for processes commonly associated with tunneling, such as Plink and the OpenSSH client.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2048	**Hunt for Malicious Processes**	IR-5	Hunt for applications or processes which display specific malicious or suspect behaviors.	Forensic and Behavioral Analysis
T1528 (Steal Application Access Token): Hunt for apps which steal or use application access tokens using the tools available in the Cloud Access Security Broker (CASB), identity provider, or resource provider.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**

CM2102	**Inspect and Analyze Network Traffic**	IR-4(13), SI-4(2), SI-4(4), SI-4(10), SI-4(25)	Analyze network traffic for unusual data flows.	Monitoring and Damage Assessment, Behavior Analysis
Discussion: Patterns of network traffic – e.g., pairings of message sources and destinations, message contents – are generally predictable, with variations based on time of day, day of week, or other known factors. Changes in traffic to or from a specific destination can be an indicator of malicious activity, as can some specific message characteristics (e.g., message size, message contents, message structure). Traffic inspection and analysis can be performed at the enterprise boundary, at internal boundaries between enclaves, or within enclaves. Baseline patterns must be established, and analysis is needed to determine whether the anomalies are due to events external to the system (e.g., failures in supporting infrastructures, natural disasters). This CM focuses on patterns of data flows and message characteristics, rather than on deep analysis of message contents. That analysis of message contents is the focus of CM2141.				
T0801 (Monitor Process State): Analyze network traffic to look for transmission of such information as OPC tags, historian data, or PLC block information to unusual or unexpected destinations (e.g., a server or a workstation which does not ordinarily receive such information).				
T0804 (Block Reporting Message): Analyze network traffic to look for divergence from normal patterns of reporting messages, which could indicate a device failure or blocking of reporting messages.				
T0810 (Data Historian Compromise): Analyze network traffic to and from the data historian, looking for unusual patterns.				
T0818 (Engineering Workstation Compromise): Analyze network traffic to and from engineering workstations, looking for unusual patterns.				
T0817 (Drive-by Compromise): Inspect URLs for known-bad domains, use reputation-based analytics, or look for known malicious scripts.				
T0830 (Man in the Middle): Monitor network traffic for anomalies associated with known MiTM behavior.				
T0845 (Program Upload): Monitor network traffic to watch for program uploads from relays, PLCs, or other devices which are not expected to transmit such information.				
T0848 (Rogue Master): Analyze network traffic to watch for anomalous patterns of control server communications.				
T0855 (Unauthorized Command Message): Analyze network traffic to watch for unusual patterns of command messages (e.g., a burst of unrelated messages from the same source, a burst of identical messages from multiple sources).				
T0856 (Spoof Reporting Message): Analyze network traffic to watch for unusual patterns of reporting messages (e.g., a burst of unrelated messages from the same source, a burst of identical messages from multiple sources). While these can indicate actual problems, they can also be the result of adversarial message spoofing.				
T0869 (Standard Application Layer Protocol): Analyze network traffic to watch for unusual usage patterns for commonly used protocols.				
T0877 (I/O Image): Analyze network traffic from controllers to watch for messages containing an I/O image.				
T0885 (Commonly Used Port): Analyze network traffic to watch for unusual usage patterns for commonly used ports.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2103	**Endpoint Behavior Analysis**	AC-2(12)	Analyze the behavior of endpoint (i.e., end-user, client) systems for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation

Discussion: A variety of behaviors on an endpoint system can be observed (e.g., logged) and analyzed, either by the endpoint system itself (usually as part of analyzing its health and status) or by another system or enclave on the network (e.g., a SOC). This analysis typically uses logs, which are accumulated as part of basic hygiene (using AU-2).				
T0802 (Automated Collection): Look for suspicious use of native control protocols and tools available in the control systems environment.				
T0817 (Drive-by Compromise): Look for suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic.				
T0866 (Exploitation of Remote Services): Look for suspicious files written to disk, evidence of Process Injection for attempts to hide execution, and evidence of Discovery.				
T0890 (Exploitation for Privilege Escalation): Look for software crashes, abnormal process behavior, or unexpected files written to disk.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2104	**Monitor Logs**	AU-6, IR-4(13), SI-4(2), SI-4(11)	Monitor system and application logs for anomalous or suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
Discussion: Devices, OSs, services, and applications perform logging to facilitate performance analysis and improvement. Those logs can be monitored for indicators of anomalous or suspicious behavior. Such indicators can be used to trigger defensive responses.				
T0810 (Data Historian Compromise): Monitor the data historian logs for indications of unusual behavior.				
T0818 (Engineering Workstation Compromise): Monitor engineering workstation logs for indications of unusual behavior.				
T0819 (Exploit Public-Facing Application): Monitor application logs for abnormal behavior.				
T0883 (Internet Accessible Device): Monitor device logs of internet-accessible devices for anomalies.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2105	**Analyze Logs**	AC-2(12), SI-4(13), SI-4(16)	Analyze logs (individually or with some correlation across logs) for anomalous or suspicious patterns of behavior.	Monitoring and Damage Assessment, Dynamic Resource Awareness, Behavior Validation
Discussion: Devices, OSs, services, and applications perform logging to facilitate performance analysis and improvement. Those logs can be analyzed individually or monitored to trigger correlation analysis. By contrast with log monitoring (CM2104), log analysis is usually part of a larger investigatory effort (e.g., a SOC function).				
T0852 (Screen Capture): Monitor the HMI system log for image files written to disk, and correlate with other events to identify suspected malicious activity.				
T0874 (Hooking): Analyze logs to search for API calls which, in conjunction with other information such as new files written to disk and unusual processes, could indicate hooking.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2106	**Analyze File Contents**	SR-10	Analyze contents of specific files or types of files for suspicious contents.	Forensic and Behavioral Analysis

T0836 (Modify Parameter): Inspect device or application parameters for suspicious or unexpected values.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2108	**Removable Device Usage Detection**	CM-8(3)	Detect anomalous or unauthorized events involving use of removable devices.	Monitoring and Damage Assessment

T0847 (Replication Through Removable Media): Monitor file accesses (particularly read and execute) on removable devices or media.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2109	**Software Integrity Check**	SI-7, SI-7(1), SI-7(6), CM-14, SR-4(3)	Perform integrity checks (e.g., using checksums, hashes, or digital signatures) on software, software certificates, or metadata.	Integrity Checks, Provenance Tracking

T0862 (Supply Chain Compromise): Perform integrity checks on as-delivered software (including updates) upon arrival.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2110	**Software Stress Testing**	SR-6(1)	Perform software stress testing (e.g., using out-of-bounds input values) prior to installation.	Self-Challenge

T0862 (Supply Chain Compromise): Perform stress testing on as-delivered software (including updates) upon arrival.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2111	**Physical Inspection**	SR-9, SR-10	Perform physical inspection of hardware components for indicators of tampering.	Integrity Checks

T0862 (Supply Chain Compromise): Perform physical inspection of hardware component packaging, and spot-check components, upon delivery.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2113	**Cross Enterprise Account Usage Analysis**	AU-6(3), SI-4(16)	Analyze user account usage across the enterprise for anomalies or suspicious behavior.	Sensor Fusion and Analysis

Discussion: Systems, applications, and devices often share accounts for users, administrators, or services. This differs from Account Monitoring (CM2121) in that it involves looking across the different places on which the same account is used, analyzing patterns of use, and looking at a broader range of account types.

T0859 (Valid Accounts): Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts (e.g., one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours). Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2115	**Process Monitoring**	IR-4(13), SI-4(2)	Monitor the behavior of processes for indications of unusual, unauthorized, or suspicious use.	Monitoring and Damage Assessment, Behavior Validation
Discussion: System processes and common application processes display behavior that is consistent over time. Anomalies in process behavior can indicate compromise of the processes or modification of the data they rely on. Automated tools support monitoring, ideally in near-real-time (SI-4(2)); however, in some environments (e.g., processes on relays in an ICS), asynchronous analysis may be used to avoid operational disruption.				

T0809 (Data Destruction): Monitor the execution and command-line parameters of processes that could be involved in data destruction activity. Monitor for the creation of suspicious files as well as high unusual file modification activity.

T0840 (Network Connection Enumeration): On HMI systems, engineering workstations, data historians, or other end-user workstations, monitor processes and command-line arguments for actions that could be taken to gather system and network information.

T0842 (Remote System Discovery): On HMI systems, engineering workstations, data historians, or other end-user workstations, monitor processes and command-line arguments for actions that could be taken to gather system and network information.

T0888 (Remote System Information Discovery): On HMI systems, engineering workstations, data historians, or other end-user workstations, monitor processes and command-line arguments for actions that could be taken to gather system and network information.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2117	**Privileged Account Monitoring**	AC-6(8)	Monitor and analyze activity associated with privileged accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment

T0842 (Network Sniffing): Monitor administrative logins, configuration changes, and changes to device images.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2118	**Cross-Enterprise Behavior Analysis**	AU-6(3), AU-6(5)	Correlate and analyze behavior of multiple systems.	Sensor Fusion and Analysis

T0886 (Remote Services): Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2120	**Application- or Utility-Specific Monitoring**	IR-4(13), SI-4(2)	Monitor and analyze events in the context of a specific application or utility.	Monitoring and Damage Assessment, Behavior Validation

T0852 (Screen Capture): Monitor the use of API calls on an HMI system to obtain image data.

T0863 (User Execution): Monitor for applications which, with user interaction, an adversary can use to download malware (e.g., compression applications).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2121	**Account Monitoring**	AC-2(12), IR-4(13), SI-4(2)	Monitor and analyze activity associated with user accounts for indications of unusual or suspicious use.	Monitoring and Damage Assessment, Behavior Validation

Discussion: Individual user accounts can be monitored for unusual or suspicious patterns of behavior. In contrast with CM2113, this monitoring typically occurs in the context of a single system or application, rather than across the enterprise.

T1213 (Data from Information Repositories): Monitor and alert on users that are retrieving and viewing a large number of documents and pages in an information repository.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2122	**Host-Local Event Correlation**	IR-4(13), SI-4(16)	Correlate and analyze events occurring on a single host.	Sensor Fusion and Analysis, Monitoring and Damage Assessment

T0834 (Native API): Correlate other events with behavior surrounding API function calls using API monitoring to evaluate behavior.

T0871 (Execution through API): Correlate other events with behavior surrounding API function calls using API monitoring to evaluate behavior.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2124	**Monitor Health and Status of Protective Systems**	PM-31	Monitor the health and status of protective systems.	Monitoring and Damage Assessment, Sensor Fusion, and Analysis

Discussion: A variety of protective systems can be integrated into the larger industrial control system to provide protections against physical faults and failures, as well as against improper (e.g., mis-timed, out-of-bounds) commands or control parameters. In IT systems, security subsystems or services are examples of protective systems. If monitoring of the health and status of such systems, or of specific functions they perform, is part of the organization's Continuous Monitoring Strategy, unexpected changes which could be precursors to failure as well as trends over time which could indicate degradation of protective capabilities could be identified.

T0837 (Loss of Protection): Monitor the health and status of protective system functions.

T0880 (Loss of Safety): Monitor the health and status of constituent elements of Safety Instrumented Systems (SIS).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2129	**Monitor Script Execution**	IR-4(13), SI-4(2), SI-4(13)	Monitor for the execution of scripts which are unknown or used in suspicious ways.	Monitoring and Damage Assessment

T0853 (Scripting): Monitor for execution of scripts that may be related to other suspicious behavior occurring on the system, e.g., running out of cycle from patching or other administrator functions.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2133	**Monitor the File System**	IR-4(13), SI-4(2), SI-4(24)	Monitor the file system to identify the unexpected presence and atypical use of files of specific types, or atypical patterns of access.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Behavior Validation
Discussion: File system monitoring can detect evidence of misuse, malware installation, deletion or modification of files expected to remain present, and other indicators of compromise. In an ICS environment, file system monitoring is most tractable on servers and workstations; it is less feasible on controllers and other devices.				
T0849 (Masquerading): Monitor for mismatches between file names and file hashes; for files with known names but in unusual locations; files that are modified outside of an update or patch; and indications of common characters that may indicate an attempt to trick users into misidentifying the file type.				
T0867 (Lateral Tool Transfer): Monitor for file creation and files transferred within a network using protocols such as SMB.				
T0872 (Indicator Removal on Host): Monitor the file system to detect improper deletion or modification of indicator files.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2138	**Monitor Command Line Use**	IR-4(13), SI-4(2), SI-4(4), SI-4(13)	Monitor use of the command line interface for use of common utilities (part of the system or installed by the adversary), looking for suspicious behavior.	Monitoring and Damage Assessment, Behavior Validation
T0807 (Command-Line Interface): Capture command-line interface activities through proper logging of process execution with command-line arguments.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2141	**Analyze Network Traffic Content**	IR-4(13), SI-4(25)	Analyze the contents of network traffic.	Monitoring and Damage Assessment, Behavior Validation
T0865 (Spearphishing Attachment): Look for suspicious email activity, such as numerous accounts receiving messages from a single unusual/unknown sender. Look for references to uncategorized or known-bad sites in email.				
T0869 (Standard Application Layer Protocol): Look for unusual contents of message traffic using commonly used protocols (e.g., unusually long strings in message fields).				
T0885 (Commonly Used Port): Look for unusual contents of message traffic, or patterns of messages to different destinations, using commonly used ports.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM2144	**Monitor Platform Status**	IR-4(13), SI-4(2)	Poll platforms (e.g., user endpoints, servers, network devices) and other devices to determine their status.	Monitoring and Damage Assessment

Discussion: The status of individual platforms (e.g., user endpoints, servers, network devices) and other devices (e.g., controllers, printers) can be monitored via polling, periodically or at random intervals.				
T0800 (Activate Firmware Update Mode): Poll devices for health and status periodically or at random intervals, to determine whether any appear to be in firmware update mode.				
T0878 (Alarm Suppression): Poll devices for health and status periodically or at random intervals, to elicit alarm data which might have been suppressed.				
T0803 (Block Command Message): Poll devices for health and status periodically or at random intervals, to determine whether they are in the state expected based on command messages which have been sent.				
T0804 (Block Reporting Message): Poll devices for health and status periodically or at random intervals, to gather data which ordinarily would have been expected to appear in a reporting message.				
T0805 (Block Serial COM): Poll devices via serial COM for health and status periodically or at random intervals, to determine whether serial COM has been blocked.				
T0816 (Device Restart/Shutdown): Poll devices for health and status periodically or at random intervals, to determine whether they are shut down.				
T0838 (Modify Alarm Settings): Poll devices for health and status periodically or at random intervals, to check what their alarm settings are.				
T0851 (Rootkit): Scan devices periodically to look for indications of rootkit installation.				
T0858 (Change Operating Mode): Scan devices periodically to identify device operating mode.				
T0881 (Service Stop): Scan devices periodically to check whether expected services are running or have been stopped.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM2147	**Monitor Network Usage**	IR-4(13), SI-4(11), SI-4(13)	Monitor network usage for anomalous behavior.	Monitoring and Damage Assessment, Behavior Validation
Discussion: Patterns of network usage – the volume of message traffic or the size of messages, particularly in the context of specific message sources and destinations – are generally predictable, with variations based on time of day, day of week, or other known factors. Unusually high volumes of traffic (or a significant decrease in traffic volume) to or from a specific destination can be an indicator of malicious activity. Baseline patterns must be established, and analysis is needed to determine whether the anomalies are due to events external to the system (e.g., failures in supporting infrastructures, natural disasters).				
T0806 (Bute Force I/O): Monitor network usage to look for high volumes of traffic sent to a single device.				
T0866 (Exploitation of Remote Services): Monitor network usage to look for unusual network traffic that may indicate additional tools transferred to a specific system.				

Table 37. CMs with Direct Potential Effects Other Than Detection – Technique-Specific Descriptions

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1101	**Present Deceptive Information**	SC-30(4), SI-20	Present deceptive information about systems, data, processes, and users. Monitor uses or search for presence of that information.	Disinformation, Tainting

Discussion: Deceptive information [SC-30(4)] can take a variety of forms, including codewords and cover stories; fabricated persona, accounts, credentials, or registry entries; the contents of fabricated files, directories, or registries; dummy processes with which an adversary could interact; and information provided for inclusion in external data stores. An initial effort is taken to create deceptive information. After that, no further action needs to be taken by cyber defenders, although the effectiveness of the deceptive information will degrade over time if it is not maintained. Monitoring for the use of the deceptive information can enable detection, particularly if the information is tainted (e.g., includes distinctive characteristics or steganographic encoding [SI-20]). Care must be exercised to ensure that users and mission or business functions do not use the deceptive information.
T1012 (Query Registry): Present false information in about the operating system, configuration, software, and security in the registry.
T1016 (System Network Configuration Discovery): Present false information about network configurations.
T1033 (System Owner/User Discovery): Create a false user identity and run processes under that identity.
T1056 (Input Capture): Have a deceptive user enter false credential information and track the use of that information.
T1068 (Exploitation for Privilege Escalation): Create a false user identity and run processes under that identity.
T1069 (Permission Groups Discovery): Create dummy groups, or identify dummy accounts within existing groups, for which changes or uses will trigger an alert.
T1078 (Valid Accounts): Create dummy accounts, for which any changes or uses will trigger an alert.
T1082 (System Information Discovery): Present false system information, e.g., via a shadow system registry.
T1087 (Account Discovery): Create dummy accounts and track their use within the system.
T1098 (Account Manipulation): Create dummy accounts, for which any changes or uses will trigger an alert.
T1110 (Brute Force), T1552 (Unsecured Credentials): Create false credentials, and track their use within the system.
T1114 (Email Collection): Place deceptive information in email repositories, making it inaccessible to normal users.
T1119 (Automated Collection): Provide deceptive information
T1190 (Exploit Public-Facing Application): Present deceptive information about software, data structures, or locations.
T1200 (Hardware Additions): Present disinformation about the hardware used in organizational systems.
T1210 (Exploitation of Remote Services): Present disinformation about the capabilities offered via remote services.
T1213 (Data from Information Repositories): Place deceptive information in repositories, making it inaccessible to normal users.
T1222 (File and Directory Permissions Modification): Create dummy files and directories, for which any changes to permissions will trigger an alert.
T1482 (Domain Trust Discovery): Include information about non-existent domains in the domain trust data store and set auditing to alert when an attempt is made to access information in those domains.
T1526 (Cloud Service Discovery): Present deceptive information about cloud services (e.g., dummy services).
T1534 (Internal Spearphishing): Create dummy email / messaging accounts and monitor for their use.
T1555 (Credentials from Password Stores): Plant decoy credentials across an array of locations to increase the chances of an adversary finding and using them.

T1566 (Phishing): Create dummy email / messaging accounts and monitor for their use.

T1583 (Acquire Infrastructure): Create decoy domains, using a decoy persona, to prevent adversaries from creating domains that could be mistaken for the organization's domain. Monitor for attempts to acquire decoy domains (e.g., via queries to decoy persona used to create such domains).

T1589 (Gather Victim Identity Information): Provide false information about the identities or attributes of individual users or customers. Monitor for use of false information.

T1591 (Gather Victim Org Information): Provide false information about the organization (e.g., fabricated roles, responsibilities, or reporting structures) to mislead an adversary. Monitor for use or external presence of false information.

T1592 (Gather Victim Host Information): Present false information about any system characteristics which legitimate enterprise services do not need, to mislead adversaries probing for such information. Monitor for use of false information about a host (e.g., attempt to access a decoy file or use a decoy service).

T1593 (Search Open Websites / Domains): Create decoy persona and content about those persona, linking across multiple open websites to construct a well-rounded view of them. Monitor for use of decoy persona.

T1594 (Search Victim-Owned Websites): Deploy a decoy website to support a deception operation or as part of the organization's deception strategy. Search for, and monitor for use of, false information placed on a deceptive website.

T1595 (Active Scanning): Present false information about any network characteristics which legitimate enterprise services do not need, to mislead adversaries scanning for such information.

T1596 (Search Open Technical Databases): Provide false information about an organization's systems, networks, or uses of technology to open technical databases. Search for, and monitor for use of, false information placed in open technical databases.

T1598 (Phishing for Information): Create decoy user accounts to mislead adversaries and cause them to reveal their information-gathering. Monitor decoy user accounts for adversary interaction.

T1602 (Data from Configuration Repository): Create configuration data related to dummy device types and monitor for attempts to discover such devices.

T1614 (System Location Discovery): Create decoy user or administrator accounts with false information implying a different physical location for the end-user device (e.g., time zone, keyboard layout, language setting).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1102	**Maintain Deception Environment**	SC-7(21), SC-26, SC-30(4)	Maintain a distinct subsystem or a set of components specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Disinformation, Predefined Segmentation

Discussion: A deception environment can replicate all or portions of an existing system or subsystem, possibly supplemented with system elements which are not present in the operational environment. Alternately, a deception environment can be a distinctly different system, with the goal of deceiving the adversary about the true nature of the operational environment. In either case, factitious (artificially created or developed) information is used to populate the deception environment [SC-30(4)], as are active or passive decoys [SC-26]. Commercial cyber deception products can facilitate the creation and maintenance of a deception environment. Note, however, that effective use of a deception environment involves ongoing effort, and care must be taken to avoid interference with operations. Therefore, some separation between the deception environment and other resources is enforced [SC-7(21)].

T1008 (Fallback Channels): Maintain a deception environment to look for adversary C2 using fallback channels.

T1014 (Rootkit): Maintain a deception environment to look for adversary use of rootkits.
T1021 (Remote Services), T1210 (Exploitation of Remote Services): Maintain a deception environment to serve as a target for remote services. For example, implement a decoy system running a remote service (such as telnet, SSH, and VNC) and see if the adversary attempts to login to the service.
T1036 (Masquerading): Maintain a deception environment to look for evidence of masquerading.
T1112 (Modify Registry): Maintain a deception environment to look for evidence of registry modifications.
T1190 (Exploit Public-Facing Application): Maintain a public-facing deception environment to attract adversaries seeking to exploit public-facing applications.
T1197 (BITS Jobs): Maintain a deception environment to look for BITS tasks, which an adversary can use to download, execute, and clean up after running malicious code.
T1202 (Indirect Command Execution): Maintain a deception environment to look for evidence of indirect command execution.
T1497 (Virtualization/Sandbox Evasion): Maintain a deception environment and monitor for indications of virtualization or sandbox evasion, such as suspicious processes being spawned that gather a variety of system information.
T1499 (Endpoint Denial of Service): Maintain a deception environment to serve as a target for denial-of-service attacks.
T1547 (Boot or Logon Autostart Execution): Maintain a deception environment to look for evidence of unauthorized software being executed as part of system boot or logon.
T1562 (Impair Defenses): Maintain a deception environment to look for adversary attempts to impair defenses.
T1568 (Dynamic Resolution): Maintain a deception environment to look for adversary C2 using dynamic resolution.
T1570 (Lateral Tool Transfer): Maintain a deception environment to look for tool transfer to, from, and within that environment.
T1590 (Gather Victim Network Information): Maintain a decoy network that contains systems which are easily discoverable by and appealing to an adversary. Monitor for use of false information about network services or configurations.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1103	**Detonation Chamber**	SC-44	Use a dynamic execution environment to handle potentially harmful incoming data.	Malware and Forensic Analysis, Misdirection, Predefined Segmentation
Discussion: A detonation chamber [SC-44] can be used to open files or execute applications, thereby limiting potential damage and facilitating analysis of malware.				
T1027 (Obfuscated Files or Information): Use a detonation chamber to open compressed and encrypted attachments.				
T1203 (Exploitation for Client Execution): Use a detonation chamber for execution of web browsers, Office applications, and common third-party applications.				
T1566 (Phishing): Use a detonation chamber to open email attachments.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM1104	**Passive Decoys**	SC-26, SC-29	Use factitious systems or resources to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities.	Misdirection, Architectural Diversity
Discussion: Factitious – artificially created or developed – systems or other resources (e.g., devices, files, services, applications) can be deployed to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities [SC-26]. This is a lower-overhead approach than a full-blown deception environment. The decoys are passive insofar as defenders do not use them to interact with the adversary; however, to be plausible, decoy systems need to run processes, decoy services and applications need to interact with the file system, and decoy files may need to be updated periodically. Some decoys can be architecturally different from the operational resources [SC-29], further deceiving the adversary and (when the adversary is more familiar with the architecture of the decoy) leading the adversary to focus on the decoy.				
T1018 (Remote System Discovery): Make a factitious system easily discoverable by other systems on the network.				
T1037 (Boot or Logon Initialization Scripts): Trick the adversary into installing boot or logon scripts onto a decoy system.				
T1046 (Network Service Scanning): Trick the adversary into targeting decoy services.				
T1053 (Scheduled Task/Job): Enable admin access on a system to see if the adversary utilizes that access to create scheduled tasks to launch their malware or tools.				
T1070 (Indicator Removal on Host): Trick the adversary into removing duplicate, shadow copies of logs or captured files which could provide indicators.				
T1083 (File and Directory Discovery): Trick the adversary into identifying decoy file systems to target.				
T1102 (Web Service): Create deceptive instances of Web services software to trick the adversary into targeting those.				
T1135 (Network Share Discovery): Trick the adversary into identifying decoy shared files or directories to target.				
T1205 (Traffic Signaling): Create deceptive ports (or identify selected unused ports as deceptive) for which attempted use will generate an alert.				
T1219 (Remote Access Software): Create deceptive instances of commonly used software to trick the adversary into targeting those with remote access tools. Install remote access tools on decoy systems across the network to see if the adversary uses these tools for command and control.				
T1221 (Template Injection): Trick the adversary into identifying decoy template files to target.				
T1484 (Domain Policy Modification): Create decoy Group Policy Objects (GPOs) and track the adversary's use of them.				
T1486 (Data Encrypted for Impact): Trick the adversary into encrypting data resources which are not operationally used.				
T1491 (Defacement): Trick the adversary into modifying visual content which is not operationally used.				
T1529 (System Shutdown / Reboot): Deploy a decoy system to see if an adversary attempts to shutdown or reboot the device.				
T1543 (Create or Modify System Process): Trick the adversary into installing or modifying a system process on a decoy system.				

T1547 (Boot or Logon Autostart Execution): Trick the adversary into installing software to execute upon boot or logon on a decoy system.
T1561 (Disk Wipe): Trick the adversary into wiping disks which are not operationally used.
T1565 (Data Manipulation): Trick the adversary into modifying or manipulating data which is not used operationally.
T1580 (Cloud Infrastructure Discovery): Deploy a diverse set of decoy systems to impact an adversary's level of effort or focus of investigation during reconnaissance activity against a cloud infrastructure.
T1592 (Gather Victim Host Information): Deploy a diverse set of decoy systems to impact an adversary's level of effort or focus of investigation during reconnaissance. Monitor for attempts to interact with a decoy system or network.
T1595 (Active Scanning): Deploy a diverse set of decoy systems to impact an adversary's level of effort or focus of investigation during reconnaissance. Monitor for attempts to interact with a decoy system or network.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1105	**Component Provenance Validation**	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4), SR-11(3)	Validate the provenance of system components.	Provenance Tracking
T1195 (Supply Chain Compromise): Perform processes to identify the source(s), scan for counterfeiting, determine the security posture, and validate the integrity of software components, as documented in the SCRM Plan.				
T1200 (Hardware Additions): Perform tracking, and spot-checks of, the provenance of hardware components, as documented in the SCRM Plan.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1106	**Supply Chain Diversity**	PL-8(2), SR-3(1), SR-3(2)	Provide multiple distinct supply chains for system components.	Supply Chain Diversity
T1195 (Supply Chain Compromise): Include processes to ensure multiple distinct supply chains for software components in the SCRM Plan.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1107	**Adversarial Simulation**	AT-2(1), AT-3(3), CA-8, CA-8(1), CA-8(2), SC-7(10), SI-19(8)	Simulate adversary activities to test the effectiveness of system protections and detection mechanisms.	Self-Challenge
T1003 (Credential Dumping): Conduct credential dumping attacks as part of a Red Team attack scenario.				
T1020 (Automated Exfiltration): Use automated tools to exercise system capabilities intended to protect against or to detect exfiltration.				
T1190 (Exploit Public-Facing Application): Simulate attempts to exploit public-facing applications in order to detect and remove weaknesses.				
T1213 (Data from Information Repositories): Use Red Team exercises to determine the susceptibility of repositories to data collection.				

T1583 (Acquire Infrastructure): Use services that may aid in tracking of newly acquired domains, such as WHOIS databases and/or passive DNS. In some cases, it may be possible to pivot on known pieces of domain registration information to uncover other infrastructure purchased by the adversary. Consider monitoring for domains created with a similar structure to your own, including under a different TLD.				
T1596 (Search Open Technical Databases): Use a decoy persona to engage with online communities or to purchase or download information about the organization and review that information for exposure.				
T1597 (Search Closed Sources): Use a false persona to obtain information from closed data sources.				
T1598 (Phishing for Information): Simulate phishing attempts and other uses of social engineering to challenge users to apply their training, recognize suspicious interactions, and respond (e.g., report) appropriately.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1108	**Dynamically Restrict Traffic or Isolate Resources**	AU-5(3), IR-4(2), SC-7(20)	Dynamically reconfigure networking to restrict network traffic or isolate resources.	Dynamic Resource Allocation, Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation, and Isolation
T1021 (Remote Services): Dynamically isolate subnets, servers, or specific components to restrict the use of remote services.				
T1498 (Network Denial of Service): Restrict network traffic if audit logging information about such traffic is determined to exceed logging storage capacity.				
T1499 (Endpoint Denial of Service): Restrict network traffic to an endpoint if audit logging information about such traffic is determined to exceed logging storage capacity, or if an authentication failure threshold is exceeded.				
T1570 (Lateral Tool Transfer): Dynamically restrict the use of file sharing protocols or isolate subnets, servers, or specific components.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1109	**Virtual Sandbox [29]**	SC-7(20), SI-14	Use virtualization to create a controlled execution environment, which is expunged after execution terminates.	Non-Persistent Services, Dynamic Segmentation, and Isolation
T1091 (Replication Through Removable Media): Use a virtual sandbox for execution of files on removable media.				
T1092 (Communication Through Removable Media): Use a virtual sandbox to read files on removable media, to inspect for executable files or scripts that could be used for C2.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1110	**Application- or Utility-Specific Data Removal**	IR-4(2), IR-4(13), SI-4(2), SI-7(1), SI-7(7)	Analyze files and data structures specific to an application or utility for anomalies and delete.	Monitoring and Damage Assessment, Integrity Checks, Dynamic Reconfiguration

[29] This could be subsumed into M1048, Application Isolation and Sandboxing. However, ATT&CK does not identify M1048 for T1091.

T1027 (Obfuscated Files or Information): Identify and delete files and data structures which have been obfuscated and for which provenance (e.g., user, system) is not verifiable.				
T1140 (Deobfuscate/Decode Files or Information): Inventory and analyze application files to locate obfuscated files (e.g., files for which contents cannot be determined by simple pattern matches, such as .txt files not containing any common words) not created by the user or the system and delete.				
T1196 (Control Panel Items): Inventory and analyze Control Panel items to locate and delete unregistered and potentially malicious files.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1111	**Execution Restriction**	AC-3(12), AC-3(13)	Restrict the sources of executables, the locations in which execution can occur, or other constraints on execution access.	Attribute-Based Usage Restriction
T1199 (Execution Through Module Load): Limit DLL module loads to specific directories to protect against module loads from unsafe paths.				
T1600 (Weaken Encryption): Block execution of untrusted software.				
T1601 (Modify System Image): Block execution of untrusted software.				
T1609 (Container Administration Command): Restrict remote management of containers.				
T1612 (Build Image on Host): Restrict the authority to build a container image and/or the set of registries from which an image may be drawn.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1112	**Covert Signaling**	SI-20	Use hidden logic to enable exfiltrated data to signal its location or embed hidden data which can be the subject of a search.	Tainting
T1020 (Automated Exfiltration): Embed hidden logic in data that detects the data's presence on a non-enterprise system and transmits a warning message to the enterprise.				
T1074 (Data Staged): Embed hidden data in data assets which are likely to be targets for exfiltration, so that internal searches for staged data can be performed.				
T1114 (Email Collection): Embed hidden logic in data that detects the data's presence on a non-enterprise system and transmits a warning message to the enterprise.				
T1567 (Exfiltration Over Web Service): Embed hidden logic in data that detects the data's presence on a non-enterprise system and transmits a warning message to the enterprise.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1113	**Present Decoy Data**	SC-26, SC-30(4), SI-20	Present plausible but factitious data assets to attract the adversary. Monitor uses of those assets or search for presence of decoy information.	Disinformation, Misdirection, Tainting

Discussion: Decoy data assets [SC-26] typically take the form of files, sets of related files (e.g., directories), or tokens. They contain – or in themselves constitute – deceptive information [SC-30(4)], and may contain data, steganographic encoding, or other characteristics which make their misuse evident [SI-20]. These data assets can be created and managed in parallel with data assets used as part of normal operations.
T1006 (Direct Volume Access): Create decoy files and search for evidence that they have been copied or exfiltrated, to discern whether an adversary has accessed them directly (bypassing file system access controls).
T1011 (Exfiltration Over Other Network Medium): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1020 (Automated Exfiltration): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1029 (Scheduled Transfer): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1030 (Data Transfer Size Limits): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1041 (Exfiltration Over C2 Channel): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1048 (Exfiltration Over Alternative Protocol): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1052 (Exfiltration Over Physical Medium): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1134 (Access Token Manipulation): Present fabricated access tokens (possibly in conjunction with decoy resources) and look for evidence that they have been modified to enable access to resources.
T1537 (Transfer Data to Cloud Account): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1558 (Steal or Forge Kerberos Tickets): Present fabricated Kerberos tickets and track their use.
T1567 (Exfiltration Over Web Service): Lead the adversary to expend time and effort on and risk exposure by exfiltrating false data assets; enable the defender to track where exfiltrated data goes.
T1589 (Gather Victim Identity Information): Create decoy user accounts or decoy persona to mislead adversaries and cause them to reveal their information-gathering. Monitor for use of decoy accounts, decoy persona, or deliberately created false information about user or customer identities.
T1590 (Gather Victim Network Information): Seed decoy content into network service configuration files which may be consumed during an adversary's reconnaissance activity. Monitor for use of false information.
T1591 (Gather Victim Org Information): Create a decoy persona (see DTE0015) and seed information about that persona's personal accounts on systems. Monitor for use of decoy persona or false information about the organization.
T1592 (Gather Victim Host Information): Provide decoy content to give the false impression about the system's content or purpose when an adversary performs system information discovery. Monitor for use or external presence of false information.
T1594 (Search Victim-Owned Websites): Provide decoy content (e.g., directories, files) which an adversary could use.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1114	**Fragment Information**	SI-23	Fragment information and distribute across multiple locations.	Fragmentation

T1002 (Data Compressed): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1011 (Exfiltration Over Other Network Medium): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1020 (Automated Exfiltration): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1029 (Scheduled Transfer): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1030 (Data Transfer Size Limits): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1041 (Exfiltration Over Command and Control Channel): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1048 (Exfiltration Over Alternative Protocol): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1052 (Exfiltration Over Physical Medium): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1119 (Automated Collection): Lead the adversary to expend time and effort on locating and reassembling data across the file system.				
T1213 (Data from Information Repositories): Lead the adversary to expend time and effort on locating and reassembling data from a fragmented information repository.				
T1486 (Data Encrypted for Impact): Lead the adversary to expend time and effort on locating enough data fragments that encrypting them (and thus making them unusable) will have an operational impact.				
T1537 (Transfer Data to Cloud Account): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
T1567 (Exfiltration Over Web Service): Lead the adversary to expend time and effort on reassembling data, and risk exposure by exfiltrating a larger number of data fragments.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1115	**Lock Down Thin Nodes**	SC-25, SC-34, SC-34(1)	Minimize local functionality and disallow writable storage.	Non-Persistent Services, Non-Persistent Information, Restriction, Integrity Checks
T1007 (System Service Discovery): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.				
T1012 (Query Registry): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.				
T1033 (System Owner/User Discovery): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.				
T1037 (Boot or Logon Initialization Scripts): Use thin (e.g., diskless) nodes to prevent software or scripts which could autostart upon boot or logon from being installed.				
T1057 (Process Discovery): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.				
T1083 (File and Directory Discovery): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.				

T1120 (Peripheral Device Discovery): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.

T1219 (Remote Access Software): Use thin (e.g., diskless) nodes to prevent an adversary from installing remote access software on an endpoint client system.

T1518 (Software Discovery): Use thin (e.g., diskless) nodes to make the adversary's attempts to learn about the endpoint futile.

T1547 (Boot or Logon Autostart Execution): Use thin (e.g., diskless) nodes to prevent software or scripts which could autostart upon boot or logon from being installed.

T1554 (Compromise Client Software Binary): Use thin (e.g., diskless) nodes to prevent binaries (which could be modified by an adversary) from being permanently resident on an endpoint client system.

T1562 (Impair Defenses): Use thin (e.g., diskless) nodes to prevent an adversary from manipulating defenses on an endpoint client system.

T1564 (Hide Artifacts): Use thin (e.g., diskless) nodes to prevent an adversary from hiding artifacts on an endpoint client system.

T1570 (Lateral Tool Transfer): Use thin (e.g., diskless) nodes to prevent tools from being transferred to an endpoint client system.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1116	**Dynamic Data Location**	SC-30(3)	Dynamically move data resources.	Functional Relocation of Cyber Resources, Temporal Unpredictability

T1074 (Data Staged): Dynamically move data resources to disrupt collection processes.

T1083 (File and Directory Discovery): Dynamically move data resources to make outdated the information the adversary obtains from file or directory discovery.

T1119 (Automated Collection): Dynamically move data resources to disrupt automated collection processes.

T1485 (Data Destruction), T1486 (Data Encrypted for Impact), T1491 (Defacement): Dynamically move data resources to disrupt attempts to destroy or modify data.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1117	**Dynamic Account Management**	AC-2(6), AC-2(8)	Dynamically update an account's authorizations or privileges.	Dynamic Privileges, Dynamic Reconfiguration

T1213 (Data from Information Repositories): Dynamically change an account's privileges to access data in an information repository.

T1531 (Account Access Removal): Dynamically reset or change an account's authorizations.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1118	**Partition Host**	SC-2, SC-2(1), SC-32, SC-32 (1)	Partition a host (e.g., server, endpoint system) into separate logical domains.	Predefined Segmentation

T1005 (Data from Local System): Partition storage or file systems on a host to restrict access based on host-local process attributes.

T1009 (Data from Shared Network Drive): Partition storage or file systems on a shared network resource so that access controls can be applied with more granularity.

T1499 (Endpoint Denial of Service): Partition an endpoint system so that DoS attacks can be restricted to a single domain.				
T1548 (Abuse Elevation Control Mechanism), T1134 (Access Token Manipulation): Partition a system to limit the scope within which a process with elevated privileges can act.				
T1552 (Unsecured Credentials): Partition a system so that searches for improperly stored credentials are restricted.				
T1561 (Disk Wipe): Partition a disk to limit the extent of destructive wiping or corruption.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1119	**Minimize Local Functionality**	CM-7(2), SC-25	Construct or configure systems or applications to minimize their inherent functionality.	Restriction
T1025 (Data from Removable Media): Prevent endpoint systems from using removable media.				
T1059 (Command and Scripting Interpreter): Minimize the available storage and capabilities, so that an adversary cannot drop a file to disk for future execution.				
T1151 (Space after Filename): Minimize the available storage and capabilities, so that an adversary cannot drop a file to disk for future execution.				
T1183 (Audio Capture): Physically remove or disable a system's microphone and web camera so that audio capture is not possible.				
T1204 (User Execution): Prevent endpoint systems from downloading files, so that a user cannot inadvertently execute malware.				
T1216 (Signed Script Proxy Execution): Minimize the available storage and capabilities, so that an adversary cannot drop a file to disk for future execution.				
T1218 (Signed Binary Proxy Execution): Minimize the available storage and capabilities, so that an adversary cannot drop a file to disk for future execution.				
T1220 (XSL Script Processing): Minimize the available storage and capabilities, so that an adversary cannot drop a file to disk for future execution.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1120	**Trusted Path**	SC-11	Provide an isolated communications path between the user and security functions.	Predefined Segmentation
T1056 (Input Capture): Provide a trusted path for credential input.				
T1565 (Data Manipulation): Provide a trusted path to protect against malicious data manipulation.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1121	**Dynamically Disable or Suspend**	AC-2(8), SC-15 (1)	Terminate processes or disable capabilities upon triggering conditions.	Adaptive Management, Dynamic Reconfiguration
T1028 (Windows Remote Management): Disable remote management capabilities in response to detection of anomalous behavior.				
T1183 (Audio Capture): Disable audio capture in response to detection of anomalous behavior.				
T1185 (Browser Session Hijacking): Terminate an inactive or suspicious browser session.				

T1496 (Resource Hijacking): Terminate processes which appear to be hijacking system resources.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1122	**Perform Mission Damage Assessment**	CP-2(8), RA-9, SI-4(1), SI-7, SI-7(1)	Determine the mission consequences of adversary activities (e.g., which resources can be relied on; how quickly, how completely, and with what confidence mission-essential services, data, and communications can be restored from backups or alternative resources).	Sensor Fusion and Analysis, Mission Dependency and Status Visualization, Integrity Checks
Discussion: Damage assessment is intended to determine which resources can be relied on; how quickly, how completely, and with what confidence services, data, and communications can be restored from backups or alternative resources. Damage assessment is also intended to determine when to shut down systems before they cause further harm. Mission damage assessment translates this information into mission terms, e.g., which mission-essential functions are degraded and how long the degradation will last. Note that CP-2(8) and RA-9 are not crucial to CM1122, but significantly enhance the effectiveness of its use.				
T1485 (Data Destruction): Determine mission consequences of data destruction.				
T1486 (Data Encrypted for Impact), T1561.001 (Disk Content Wipe): Determine mission consequences of data made unavailable.				
T1489 (Service Stop): Determine mission consequences of services being stopped or disabled.				
T1490 (Inhibit System Recovery): Determine mission consequences of a to-be-recovered system being kept offline.				
T1499 (Endpoint Denial of Service): Determine mission consequences of services offered via an endpoint system being degraded or unavailable.				
T1529 (System Shutdown / Reboot): Determine whether system shutdown and reboot have mission consequences.				
T1561 (Disk Wipe): Determine mission consequences of data and/or services made unavailable.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1123	**Active Decoys**	SC-26, SC-35, SC-44	Use one or more factitious systems or other resources to identify malicious sites, interact with the adversary, actively probe for malicious code, and observe adversary TTPs. [30]	Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation, and Isolation

[30] CM1123 supports M1038, Execution Prevention.

Discussion: Decoy systems or other resources (e.g., devices, files, services, applications) can be operated to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities [SC-26]. This is a lower-overhead approach than a full-blown deception environment but involves more effort than passive decoys. Defenders use active decoys to interact with the adversary. Some interactions can be designed to identify malicious code on external systems [SC-35], using detonation chambers [SC-44].

T1176 (Browser Extensions): Use a honeyclient to identify sources of malicious browser extensions, so these can inform denylists.

T1189 (Drive-by Compromise): Use a honeyclient to visit sites commonly visited by organization staff to identify sources of malware.

T1497 (Virtualization/Sandbox Evasion): Use a honeyclient to identify adversary attempts to determine whether they are in a virtual or sandbox environment.

T1566 (Phishing): Use a honeyclient to open links in email to ensure they are non-malicious, prior to delivery to the end user.

T1574 (Hijack Execution Flow): Use a honeyclient to identify potentially malicious software which could be executed via hijacking.

T1598 (Phishing for Information): Investigate sites to which links are offered (e.g., via email, via links on commonly visited pages) to determine whether those sites are malicious or are used by malicious actors.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1124	**Minimize Data Retention or Lifespan**	SC-23(3), SI-14(2), SI-21	Minimize the lifespan or retention of data and ensure that deleted data cannot be retrieved.	Non-Persistent Information, Temporal Unpredictability

T1133 (External Remote Services): Generate random session identifiers that are good for one-time use.

T1213 (Data from Information Repositories): Define and enforce policies about retaining data unnecessarily.

T1539 (Steal Web Session Cookie): Minimize the lifespan of web session cookies.

T1550 (Use Alternate Authentication Material): Refresh alternate authentication material as needed; prevent caching of such information.

T1553 (Subvert Trust Controls): Periodically delete – and thus force to be regenerated – security attributes or root certificates.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1125	**Authenticate Devices**	IA-3(1)	Authenticate a device before establishing a connection to it.	Obfuscation, Integrity Checks

T1200 (Hardware Additions): Use cryptographically protected bi-directional authentication before establishing a connection to a device.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1126	**Enhanced Authentication**	IA-2(13), IA-10, CP-13, SC-47	Use situation-specific, risk-adaptive, or out-of-band authentication.	Adaptive Management, Calibrated Defense-in-Depth, Architectural Diversity, Design Diversity, Path Diversity, Dynamic Privileges

T1040 (Network Sniffing): Use out-of-band authentication to complicate the adversary's efforts to capture authenticators.

T1098 (Account Manipulation): Use out-of-band authentication to make adversary manipulation of credentials more difficult.				
T1110 (Brute Force): Use out-of-band authentication to thwart brute force guessing of authenticators.				
T1114 (Email Collection): Use out-of-band authentication to thwart adversary efforts to access and collect email.				
T1133 (External Remote Services): Use out-of-band authentication to make adversary efforts to use external remote services more difficult.				
T1134 (Access Token Manipulation): Use adaptive authentication to challenge the adversary's manipulation of access tokens.				
T1530 (Data from Cloud Storage Object): Use adaptive or out-of-band authentication to restrict access to cloud resources and cloud storage API.				
T1550 (Use Alternate Authentication Material): Use adaptive authentication to challenge the adversary's use of alternate authentication material.				
T1556 (Modify Authentication Process): Use out-of-band and adaptive authentication to thwart the adversary's efforts to modify the authentication process.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1127	**Minimize Duration of Connection or Session**	AC-12, SC-7(10), SC-10, SI-14(3)	Minimize the time period for which a connection remains open or a session remains active, requiring reauthorization to reestablish connectivity.	Non-Persistent Services, Non-Persistent Connectivity
T1033 (System Owner/User Discovery): Minimize session duration to shorten the period during which an adversary can discover users.				
T1039 (Data from Network Shared Drive): Minimize the duration of a connection to a network shared drive.				
T1041 (Exfiltration Over C2 Channel), T1011 (Exfiltration Over Other Network Medium): Minimize the duration of or unpredictably interrupt connections to reduce the amount of information the adversary can exfiltrate.				
T1133 (External Remote Services): Minimize the duration of or unpredictably interrupt services which allow users to connect to internal enterprise network resources from external locations, thus forcing off an adversary who has obtained access to a one-time authenticator.				
T1205 (Traffic Signaling): Minimize the duration a port remains open.				
T1563 (Remote Service Session Hijacking): Minimize the duration of remote service sessions to restrict adversary movement.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1128	**Design Diversity**	SA-17(9)	Use multiple designs to implement the same functionality.	Design Diversity
T1110 (Brute Force): Use different hashing schemes for passwords used by different services.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1129	**Check Policy Consistency**	CA-7(5)	Ensure that policies are applied consistently across systems, applications, and services.	Consistency Analysis

T1110 (Brute Force): Check that password policies are applied consistently to cloud-based applications. Policies applied to the use of cloud services should be consistent with policies for using enterprise-internal services.

T1136 (Create Account): Check that policies regarding account creation and permissions are applied consistently within a local system, a domain, or cloud services. Perform regular audits of domain and local system accounts to identify suspicious accounts that may have been created by an adversary. Monitor for accounts assigned to admin roles that go over a certain threshold of known admins.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1130	**Validate Data Quality**	SA-9(7), SI-7(1)	Validate data quality (e.g., integrity, consistency, correctness).	Integrity Checks

T1207 (Rogue Domain Controller): Baseline and periodically analyze the Configuration partition of the Active Directory (AD) schema and alert on creation of nTDSDSA objects. Leverage AD directory synchronization to monitor changes to directory state using AD replication cookies.

T1485 (Data Destruction): Periodically validate the quality of stored data, including data in cloud storage, to determine whether data has been destroyed.

T1491 (Defacement): Periodically validate the quality of stored data, including data in cloud storage, particularly data used to present public-facing information or services, to determine whether it has been modified or destroyed.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1131	**Active Deception**	AC-4(3), IR-4(2), IR-4(3), SC-7(21), SC-26, SC-30(4), SI-3(10)	Maintain an internal deception environment, divert suspicious traffic to that environment, interact with and analyze behavior to determine whether it is malicious and to investigate adversary TTPs.	Dynamic Reconfiguration, Adaptive Management, Misdirection, Monitoring and Damage Assessment, Forensic and Behavioral Analysis

Discussion: Active deception goes beyond the maintenance of a deception environment (CM1102) to enable defenders to interact with, and analyze the behavior of, adversaries. The MITRE Engage framework (Engage Home (mitre.org)) identifies a variety of Activities defenders can perform as part of active deception.

T1028 (Windows Remote Management): Use active deception to investigate uses of WinRM.

T1047 (Windows Management Instrumentation): Use active deception to investigate uses of WMI.

T1059 (Command and Scripting Interpreter): Use active deception to investigate potential abuse of command or script interpreters.

T1059 (Command Line Interface): Use active deception to investigate potential abuse of the Command Line Interface.

T1072 (Software Deployment Tools): Use active deception to investigate suspicious or anomalous behavior related to third-party software.

T1080 (Taint Shared Content): Use active deception to trick the adversary into tainting shared content in a deception environment.

T1106 (Native API): Use active deception to investigate potential abuse of the Windows API.

T1129 (Shared Modules): Use active deception to investigate potential abuse of the Windows module loader.

T1203 (Exploitation for Client Execution): Use active deception to investigate potential exploitation of vulnerabilities that enable arbitrary code execution.

T1211 (Exploitation for Defense Evasion): Use active deception to investigate how the adversary uses exploitation for defense evasion.

T1216 (Signed Script Proxy Execution): Use active deception to investigate potential abuse of signed scripts that support proxy execution.

T1218 (Signed Binary Proxy Execution): Use active deception to investigate potential abuse of signed binaries that support proxy execution.

T1480 (Execution Guardrails): Use active deception to interact with malware, in order to determine the conditions under which malware will execute.

T1557 (Adversary-in-the-Middle): Use active deception to investigate the adversary's Adversary-in-the-Middle attack methods and targets.

T1569 (System Services): Use active deception to investigate potential abuse of service creation and execution.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1132	**Quarantine or Delete Suspicious Files**	SR-4(3), CM-7(6), SI-14, SI-14(2)	Move and make inaccessible, or delete, suspicious files.	Provenance Tracking, Dynamic Segmentation and Isolation, Non-Persistent Information

T1059 (Command and Scripting Interpreter): Identify and quarantine files containing scripts of unknown provenance.

T1216 (Signed Script Proxy Execution): Intercept execution of specific signed scripts to identify and either move and make inaccessible, or delete, files of unknown provenance.

T1218 (Signed Binary Proxy Execution): Intercept execution of specific Windows utilities to identify and either move and make inaccessible, or delete, files of unknown provenance.

T1220 (XSL Script Processing): Intercept execution of commands related to XSL scripting to identify and either move and make inaccessible, or delete, files of unknown provenance.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1133	**Isolate or Contain Selected Applications or Components**	CM-7(6), SC-7(21)	Isolate or contain (e.g., using internal firewalls or virtual environments) selected applications or components, based on risk profiles.	Trust-Based Privilege Management, Predefined Segmentation, Dynamic Segmentation, and Isolation

T1071 (Application Layer Protocol): Isolate or contain in a designated enclave selected applications, so that exploitation of application layer protocols for C2 can be stopped at the internal boundary.

T1072 (Software Deployment Tools): Isolate or contain third-party applications or software deployment systems.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1134	**Refresh Selected Applications or Components**	SI-14(1), SI-14(2)	Refresh software, firmware, or data from a trusted source.	Non-Persistent Services, Non-Persistent Information, Provenance Tracking

T1037 (Boot or Logon Initialization Scripts): Periodically refresh the software and configuration settings on an endpoint system from a trusted source external to the system, to remove malware configured to execute automatically upon boot or logon.

T1068 (Exploitation for Privilege Escalation): Periodically refresh software and configuration settings to restore privileges to the minimal set associated with the software.

T1072 (Software Deployment Tools): Periodically refresh third-party applications or software development systems from a trusted source.				
T1137 (Office Application Startup): Periodically refresh an endpoint's installation of Office applications from a trusted source external to the system (e.g., a gold copy on a protected server).				
T1525 (Implant Internal Image): Periodically refresh cloud container images from a trusted source.				
T1543 (Create or Modify System Process), T1542 (Pre-OS Boot): Periodically refresh system firmware or system-level processes from a trusted source external to the system (e.g., a gold copy on a protected server).				
T1546 (Event Triggered Execution): Revert a system to a verified baseline on a frequent, recurring basis in order to remove adversary persistence mechanisms.				
T1547 (Boot or Logon Autostart Execution): Store good copies of registry startup keys and restore them on a frequent basis.				
T1599 (Network Boundary Bridging): Periodically refresh the firmware, software, and/or configuration files on a network boundary device from a trusted source.				
T1600 (Weaken Encryption): Periodically refresh the firmware, software, and settings on a network device to expunge the effects of weakened encryption.				
T1601 (Modify System Image): Periodically refresh the firmware and software on an embedded network device from a trusted source external to the system.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1135	**Hide Sensitive Information**	SC-28 (1), SI-19(4)	Conceal (e.g., via encryption or data hiding) or remove sensitive information (including metadata).	Obfuscation
T1003 (OS Credential Dumping): Encrypt credential data in system files and caches.				
T1005 (Data from Local System): Encrypt or hide files (e.g., hidden password-protected folders) on a local system.				
T1039 (Data from Network Shared Drive): Encrypt or conceal files on network drives.				
T1213 (Data from Information Repositories): Remove, mask, encrypt, hash, or replace identifiers or other highly sensitive information in a dataset.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1136	**Identify External Malware**	SC-35	Identify and redirect malware found on external systems.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation, and Isolation
T1204 (User Execution): Identify malware downloaded as a result of user actions and redirect its traffic to a deception environment.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**

CM1137	**Validate Data Properties**	PL-8(1), SC-16(1), SC-16(3), SI-7, SI-7(1)	Validate data properties (including binaries, metadata, and cryptographic bindings) to defend against modification or fabrication.	Integrity Checks, Calibrated Defense-in-Depth
T1080 (Taint Shared Content): Track metadata on shared network directories, e.g., via a cryptographic hash, and compare libraries that are loaded at process execution time against previous executions to detect differences that do not correlate with patching or updates.				
T1134 (Account Token Manipulation): Use and validate cryptographic bindings of attributes to account tokens.				
T1565 (Data Manipulation): Build data quality (e.g., correctness, consistency) checks into multiple locations in mission, business, or system workflows to ensure that data has not been manipulated.				
T1574 (Hijack Execution Flow): Track library metadata, such as a cryptographic hash, and compare libraries that are loaded at process execution time against previous executions to detect differences that do not correlate with patching or updates.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1138	**Switch to Alternative Data Sources**	SI-22, IR-4(2)	Switch to one or more alternative data sources to ensure adequate data quality or rebuild destroyed data.	Information Diversity, Dynamic Reconfiguration
T1485 (Data Destruction): Use an alternative data source to create new versions of data that was destroyed in storage.				
T1486 (Data Encrypted for Impact): Use an alternative data source to create new versions of data that was destroyed in storage.				
T1561 (Disk Wipe): Use an alternative data source to create new versions of data that was destroyed in storage.				
T1565 (Data Manipulation): Build the capability to use alternative data sources into mission, business, or system workflows, as a cross-check against fabricated or modified data.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1139	**Dynamically Reprovision**	AC-4(3), IR-4(2), SC-7(20)	Reconfigure or reallocate resources to route around damage.	Adaptive Management, Dynamic Reconfiguration
T1485 (Data Destruction), T1486 (Data Encrypted for Impact), T1561 (Disk Wipe): Reconfigure resources to remove dependence on data which has been made useless or unavailable.				
T1496 (Resource Hijacking): Reconfigure resources to isolate components which appear to have been hijacked or usurped.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1140	**Use Alternate Communications**	AC-7(4), SC-47	Use alternative communications paths.	Path Diversity
T1531 (Account Access Removal): Use alternate communications paths (e.g., phone) to notify administrators of account access disruption.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**

CM1141	**Reconstruct Compromised Assets**	SC-36, SI-22, SI-23, IR-4(9), CP-9	Reconstruct assets (e.g., files, software components) which have been damaged, destroyed, or modified in a way that makes them suspect.	Information Diversity, Fragmentation, Distributed Functionality, Protected Backup and Restore, Replication, Dynamic Reconfiguration
T1485 (Data Destruction): Reconstruct damaged or destroyed files from information fragments, redundant copies, or alternative information sources, and reconfigure systems to use the reconstructed resources.				
T1486 (Data Encrypted for Impact): Reconstruct encrypted data from information fragments, redundant copies, or alternative information sources, and reconfigure systems to use the reconstructed resources.				
T1561 (Disk Wipe): Reconstruct disk contents from information fragments, redundant copies, or alternative information sources, and reconfigure systems to use the reconstructed resources. [31]				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1142	**Switch to Protected Hot Shadow**	AC-4(2), AC-4(8), CP-2(5), CP-9(6), IR-4(2)	Switch (failover) to a duplicate system in a protected enclave which, subject to additional quality controls on data and software updates, mirrors the system which has been compromised.	Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication, Predefined Segmentation, Integrity Checks
T1561 (Disk Wipe): Orchestrate the switch to a protected hot shadow system in a protected enclave on which the destroyed data is mirrored, recognizing that the additional protections may mean some data is not as current or complete as on the primary system.				
T1485 (Data Destruction): Orchestrate the switch to a protected hot shadow system in a protected enclave on which the destroyed data is mirrored, recognizing that the additional protections may mean some data is not as current or complete as on the primary system.				
T1486 (Data Encrypted for Impact): Orchestrate the switch to a protected hot shadow system in a protected enclave on which the affected data is mirrored, recognizing that the additional protections may mean some data is not as current or complete as on the primary system.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1143	**Switch to Alternate System or Component**	CP-2(5), IR-4(2), SA-17(9), SC-22, SC-29	Switch (failover) to another system or component which provides roughly equivalent functionality in a different way.	Architectural Diversity, Design Diversity, Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication
T1498 (Network Denial of Service): Switch to an alternate system that provides name and address resolution services, e.g., an alternate domain name system (DNS) server.				
T1561 (Disk Wipe): Switch to another system or component which provides the functionality of the system or component which has been rendered unusable.				
T1495 (Firmware Corruption): Switch to another system or component which provides the functionality of the system or component for which firmware has been corrupted.				

[31] Note that this Candidate Mitigation depends on the use of CM-8, CP-10, and SC-27, which are standard practice.

T1490 (Inhibit System Recovery): Switch to another system or component which provides the functionality of the system or component for which recovery is inhibited.

T1529 (System Shutdown / Reboot): Switch to another system or component which provides the functionality of the system or component which the adversary repeatedly puts through shutdown and/or reboot.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1144	**Activate Alternate**	CP-2(5), IR-4(2), SA-17(9), SA-20, SA-23, SC-29	Activate an alternate system or component (e.g., from a war-time reserve) which provides roughly equivalent function in a novel or specialized way, and failover.	Architectural Diversity, Design Diversity, Dynamic Reconfiguration, Adaptive Management, Orchestration, Specialization

T1490 (Inhibit System Recovery): Activate an alternate system or component which provides the functionality of the impaired system or component, so that the adversary's attempts to interfere with recovery of that component are wasted.

T1495 (Firmware Corruption): Activate an alternate system or component which provides the functionality of the system or component for which recovery is inhibited but does so in a way the adversary has not previously seen.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1145	**Defend Failover and Recovery**	AC-2(6), IR-4(2), IR-4(3), SC-7(20), SC-48, SC-48 (1), SI-4(1)	Increase sensor activity and restrict privileges to defend against an adversary taking advantage of failover or recovery activities.	Adaptive Management, Dynamic Reconfiguration, Orchestration, Functional Relocation of Sensors, Dynamic Segmentation and Isolation, Mission Dependency and Status Visualization, Dynamic Privileges

T1490 (Inhibit System Recovery): Defend against attempts to prevent recovery.

T1561 (Disk Wipe): Defend the failover to an alternate system or storage location.

T1495 (Firmware Corruption): Defend the failover to an alternate system or storage location.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1146	**Refresh Sessions or Connections**	SC-23(3), SC-30(2), SI-14(3)	Terminate and re-establish sessions or network connections unpredictably to disrupt adversary use.	Non-Persistent Connectivity, Temporal Unpredictability

T1008 (Fallback Channels): Refresh external connections unpredictably to disrupt the adversary's use of fallback C2 channels.

T1104 (Multi-Stage Channels): Refresh external connections unpredictably to disrupt the adversary's use of multi-stage C2 channels.

T1563 (Remote Service Session Hijacking): Refresh sessions unpredictably to disrupt session hijacking.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM1147	**Defend Against DoS**	AC-4(3), SC-5(2), SC-5(3)	Adapt to reduce the impacts of denial-of-service attacks.	Dynamic Resource Allocation, Adaptive Management, Surplus Capacity, Monitoring and Damage Assessment
T1498 (Network Denial of Service): Dynamically reallocate surplus network capacity or redundant network resources to adapt to denial-of-service attacks.				
T1499 (Endpoint Denial of Service): Dynamically reallocate surplus platform capacity or redundant platform resources on an endpoint system to adapt to denial-of-service attacks.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1148	**Conceal or Randomize Network Traffic**	SC-8(5), SC-30	Conceal (via encryption or insertion of fabricated traffic) or randomize network traffic patterns.	Obfuscation, Contextual Unpredictability
T1040 (Network Sniffing): Insert fabricated network traffic to mislead the adversary.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1149	**Lock Down Visibility or Access**	AC-3(11)	Restrict the visibility of or access to data or a capability based on the nature or attributes of that data or capability.	Attribute-Based Usage Restriction
T1484 (Domain Policy Modification): Restrict the ability to modify Group Policy Objects (GPOs) to administrators.				
T1612 (Build Image on Host): Restrict the ability to build a container image.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1150	**Dynamically Relocate and Refresh Processing**	SC-30(3), SI-14(1)	Suspend a process and re-instantiate it in a different location.	Functional Relocation of Cyber Resources, Non-Persistent Services
T1055 (Process Injection): Capture process status data and relocate the process, refreshing it from a trusted source.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1151	**Defend Enclave Boundaries**	AC-4(8), AC-4(12), AC-4(17), AC-4(21), SC-7(21), SC-7(22), SC-46	Maintain distinct enclaves based on security characteristics and use stringent filtering [32] to defend the enclave boundary.	Predefined Segmentation, Integrity Checks, Provenance Tracking
T1008 (Fallback Channels): Restrict information channels at the enclave boundary.				
T1043 (Non-Standard Port): Enforce stringent filtering at enclave boundaries to defend against modifications to standard port/protocol pairings and attempts to bypass filtering.				

[32] Stringent filtering – using well-defined rules to check the structure, provenance, and integrity of transmitted information – goes beyond simple configuration settings for firewalls and access control mechanisms. However, uses of this Candidate Mitigation do not involve cross-domain or layered solutions; those are considered in CM1153.

T1071 (Application Layer Protocol): Enforce stringent filtering on information entering or leaving a protected enclave, to defend against C2 information flows.

T1095 (Non-Application Layer Protocol): Enforce stringent filtering on information entering or leaving a protected enclave, to defend against C2 information flows.

T1572 (Protocol Tunneling): Enforce stringent filtering on information entering or leaving a protected enclave, to defend against C2 information flows.

T1090 (Proxy): Enforce stringent filtering on information entering or leaving a protected enclave, to defend against C2 information flows.

T1104 (Multi-Stage Channels): Enforce stringent filtering at the enclave boundary to prevent the transfer of remote access tools into the enclave, and to limit systems communicating to unknown locations on the Internet.

T1105 (Ingress Tool Transfer): Enforce stringent filtering on information entering a protected enclave, to defend against tool transfer.

T1573 (Encrypted Channel): Enforce stringent filtering on encrypted information flows at the boundaries of a protected enclave.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1152	**Defend Against Memory Attacks**	SI-16	Provide defenses against attacks against system memory.	Synthetic Diversity, Temporal Unpredictability

T1055 (Process Injection): Provide data execution protections or other defenses (e.g., ASLR) against adversary injection of code into running processes.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1153	**Modulate Information Flows**	AC-4(27), AC-4(29), AC-4(30), SC-7(15), SC-46	Use controlled interfaces and communications paths to provide access to risky capabilities or to filter communications between enclaves.	Orchestration, Design Diversity, Replication, Predefined Segmentation, Trust-Based Privilege Management

T1001 (Data Obfuscation): Use layered controlled interfaces to catch obfuscated C2 data before it transits the enclave boundary.

T1020 (Automated Exfiltration): Use layered controlled interfaces to control traffic between enclaves, and hence to impede automated exfiltration of data.

T1021 (Remote Services): Use a dedicated, managed interface for networked privileged accesses to remote services.

T1079 (Scheduled Transfer): Use layered controlled interfaces to control traffic between enclaves, and hence to impede exfiltration of data which relies on scheduled data transfer.

T1071 (Application Layer Protocol), T1095 (Non-Application Layer Protocol), T1572 (Protocol Tunneling), T1090 (Proxy): Use one or more controlled interfaces to catch protocol-layer data before it transits the enclave boundary.

T1104 (Multi-Stage Channels): Use layered controlled interfaces to catch different stages of C2 channel use before information transits the enclave boundary.

T1567 (Exfiltration Over Web Service): Use layered controlled interfaces to control traffic between enclaves, and hence to impede exfiltration of data which relies on existing, legitimate Web services.

T1570 (Lateral Tool Transfer): Use layered controlled interfaces to prevent tools from being transferred between enclaves.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1154	**Hardware-Based Protection of Firmware**	SC-51	Use hardware-based protections for firmware.	Integrity Checks
T1495 (Firmware Corruption): Use hardware-based write protection for firmware.				
T1542 (Pre-OS Boot): Use hardware-based write protection for firmware used pre-OS boot.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1155	**Validate Output Data**	SI-15	Validate information output from processes or applications against defined criteria.	Integrity Checks
T1565 (Data Manipulation): Validate information output from processes or applications against defined criteria to check whether an adversary has manipulated inputs or logic.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1156	**Physically Relocate Resources**	SC-30(3)	Physically move resources (e.g., storage devices, servers, end-user devices), with concomitant changes to network location.	Asset Mobility
T1614 (System Location Discovery): Physically move resources to make the adversary's determination of location outdated.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1157	**Defend Against Data Mining**	AC-23	Enforce access restrictions and provide alerting to defend against data mining.	Monitoring and Damage Assessment, Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges
T1213 (Data from Information Repositories): Enhance access restrictions on data repositories (e.g., by limiting the number or frequency of queries) and provide alerting to defend against data mining.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1158	**Defend Audit Data**	AU-9(1), AU-9(2), AU-9(3), AU-9(6)	Provide mechanisms to protect audit data from modification or observation.	Integrity Checks, Predefined Segmentation, Attribute-Based Usage Restriction
T1070 (Indicator Removal on Host): Use write-once storage for audit data to defend against the adversary's attempts to delete or modify audit logs.				
T1613 (Container and Resource Discovery): Encrypt container logs and store them on a separate component or system with read-only access.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**

CM1159	**Enhance User Preparedness**	AT-2(1), AT-2(3), AT-2(5), AT-3(3)	Keep users, administrators, and operators aware of existing and emerging threats and attack techniques they can counter in practice.	Dynamic Threat Awareness, Self-Challenge
T1528 (Steal Application Access Token): Train users on how to recognize and report third-party applications requesting authorization can create "Human Sensors" that help detect application token theft.				
T1534 (Internal Spearphishing): Train and exercise users so that they can serve as “human sensors” for internal spearphishing, able to detect suspicious behavior from other uses.				
T1585 (Establish Accounts): Train and exercise users so that they can serve as “human sensors,” able to detect suspicious external persona trying to interact with them.				
T1586 (Compromise Accounts): Train and exercise users so that they can serve as “human sensors,” able to detect suspicious behavior from external users or organizations.				
T1589 (Gather Victim Identity Information): Keep users and administrators apprised of ways that an adversary can gather, correlate, and aggregate information about them. Offer them practices for analyzing their on-line presence for potential exposure of personal or sensitive information.				
T1598 (Phishing for Information): Train and exercise users so that they can serve as “human sensors,” able to detect suspicious interactions from external sources.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1160	**Conceal Resources from Discovery**	SC-7(16), SC-28 (1), SC-30, SC-30(5)	Protect network addresses of system components that are part of managed interfaces from discovery through common tools and techniques, via hiding or relocation.	Obfuscation, Functional Relocation of Cyber Resources
T1018 (Remote System Discovery): Conceal the location of remote systems, or periodically change their network addresses.				
T1049 (System Network Connections Discovery): Conceal (e.g., via redirection) the network connections to or from a compromised system.				
T1120 (Peripheral Device Discovery): Conceal the location of peripheral devices, or periodically change their network addresses.				
T1135 (Network Share Discovery): Conceal shared drives so they are not easily discoverable or relocate them periodically to invalidate the adversary’s discovery data.				
T1592 (Gather Victim Host Information): Conceal information about externally-visible hosts.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1161	**Collaborate to Counter Adversaries**	PM-16, SC-30(4), SI-20	Collaborate with other entities to counter adversary activities.	Disinformation, Tainting, Dynamic Threat Awareness
T1583 (Acquire Infrastructure): Collaborate with other entities (e.g., services that track, query, and monitor domain name registration information) to track adversary infrastructure acquisition across multiple DNS infrastructures.				

T1597 (Search Closed Sources): Collaborate with other entities (e.g., threat intelligence vendors, other service suppliers, equipment, and software suppliers) to provide false information about the organization's systems, technology uses, or employees.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1162	**Restrict Supply Chain Exposures**	CM-7(7), PM-30(1), SR-3(2), SR-5, SR-6(1), SR-7, SR-10, SR-11	Restrict adversaries' ability to determine or manipulate the organization's cyber supply chain.	Orchestration, Obfuscation, Disinformation, Self-Challenge, Supply Chain Diversity, Replication, Predefined Segmentation, Integrity Checks, Provenance Tracking

T1596 (Search Open Technical Databases): Acquire system components using indirection (e.g., multiple trusted third parties), acquire components which will not be used, and analyze open technical databases to determine what information about the organization's cyber supply chain is available to adversaries.

T1597 (Search Closed Sources): Acquire system components using indirection (e.g., multiple trusted third parties), acquire components which will not be used, and analyze closed sources to determine what information about the organization's cyber supply chain is available.

T1608 (Stage Capabilities): In a safe environment, perform analysis and testing of software or configuration settings downloaded from Web services (e.g., GitHub, Pastebin) to determine that it does not include staged malware.

T1195 (Supply Chain Compromise): Acquire system components for which provenance and constituent elements can be identified, either by the source vendor / integrator or via analysis in a safe environment.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1163	**Redefine System**	IR-4(10), SC-27, SC-29, SR-5(1)	Redefine the system in terms of components, interfaces, and dependencies.	Orchestration, Architectural Diversity, Supply Chain Diversity, Evolvability, Replication

T1195 (Supply Chain Compromise): Redefine the system based on information about known or suspected compromised components.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1164	**Calibrate Administrative Access**	AC-6, AC-6(5), CM-7(2)	Configure administrator access to resources based on active defense strategies.	Attribute-Based Usage Restriction, Trust-Based Privilege Management, Restriction

T1014 (Rootkit): Remove admin access in an attempt to force an adversary to perform privilege escalation to install a rootkit.

T107 (Windows Management Instrumentation): Remove admin access from the local user to prevent an adversary from being able to utilize WMI.

T1610 (Deploy Container): Restrict the authority to deploy containers using role-based access control (RBAC).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1201	**Present Deceptive Information**	SC-30(4), SI-20	Present deceptive information about systems, data, processes, and users. Monitor uses or search for presence of that information.	Disinformation, Tainting

Discussion: Deceptive information [SC-30(4)] can take a variety of forms, including codewords and cover stories; fabricated persona, accounts, credentials, or registry entries; fabricated files, directories, or registries; and dummy processes with which an adversary could interact. An initial effort is taken to create deceptive information. After that, no further action needs to be taken by cyber defenders, although the effectiveness of the deceptive information will degrade over time if it is not maintained. Monitoring for the use of the deceptive information can enable detection, particularly if it is tainted (e.g., includes distinctive characteristics or steganographic encoding [SI-20]). Care must be exercised to ensure that users and mission or business functions do not use the deceptive information.

T0802 (Automated Collection): Present deceptive information on devices that could be targeted for automation.

T0811 (Data from Information Repositories): Present deceptive information in information repositories (e.g., false specifications, schematics, or diagrams of control system layouts, devices, and processes).

T0819 (Exploit Public-Facing Application): Present deceptive information about software, data structures, or locations.

T0842 (Network Sniffing): Insert network traffic presenting false credentials, for which any attempted uses will trigger an alert.

T0859 (Valid Accounts): Create dummy accounts, for which any changes or uses will trigger an alert.

T0861 (Point & Tag Identification): Present false but plausible point and tag values, and track whether they are used or transmitted anywhere.

T0865 (Spearphishing Attachment): Create decoy or dummy email accounts and monitor for spearphishing attempts.

T0882 (Theft of Operational Information): Present deceptive operational information, e.g., on a workstation which is not authorized for operational use.

T0888 (Remote System Information Discovery): Present false system information, e.g., via a shadow system registry.

T0890 (Exploitation for Privilege Escalation): Create a false user identity and run processes under that identity.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1202	**Maintain Deception Environment**	SC-7(21), SC-26, SC-30(4)	Maintain a distinct subsystem or a set of components specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.	Monitoring and Damage Assessment, Forensic and Behavioral Analysis, Misdirection, Disinformation, Predefined Segmentation

Discussion: A deception environment can replicate all or portions of an existing system or subsystem, possibly supplemented with system elements which are not present in the operational environment. Alternately, a deception environment can be a distinctly different system, with the goal of deceiving the adversary about the true nature of the operational environment. In either case, factitious (artificially created or developed) information is used to populate the deception environment [SC-30(4)], as are active or passive decoys [SC-26]. Commercial cyber deception products can facilitate the creation and maintenance of a deception environment, including in the ICS domain. Note, however, that effective use of a deception environment involves ongoing effort, and care must be taken to avoid interference with operations. (For example, a DoS attack on a system in a deception environment could degrade network performance.) Therefore, deception environments are more likely to be deployed in the IT than in the OT environment. In any case, some separation between the deception environment and other resources is enforced [SC-7(21)].

T0819 (Exploit Public-Facing Application): Maintain a public-facing deception environment to attract adversaries seeking to exploit public-facing applications.

T0866 (Exploitation of Remote Services): Maintain an internal deception environment to serve as a target for attacks involving remote services.

T0867 (Lateral Tool Transfer): Maintain a deception environment to look for tool transfer to, from, and within that environment.

T0883 (Internet Accessible Device): Include an internet-accessible device in an internal deception environment to watch for attacks against such devices.

T0886 (Remote Services): Maintain an internal deception environment to serve as a target for attacks involving remote services.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1204	**Passive Decoys**	SC-26, SC-29	Use factitious systems or resources to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities.	Misdirection

Discussion: Factitious – artificially created or developed – systems or other resources (e.g., devices, files, services, applications) can be deployed to decoy adversary attacks away from operational resources, to increase the adversary's workload, or to observe adversary activities [SC-26]. This is a lower-overhead approach than a full-blown deception environment. The decoys are passive insofar as defenders do not use them to interact with the adversary; however, to be plausible, decoy systems need to run processes, decoy services and applications need to interact with the file system, and decoy files may need to be updated periodically. Some decoys can be architecturally different from the operational resources [SC-29], further deceiving the adversary and (when the adversary is more familiar with the architecture of the decoy) leading the adversary to focus on the decoy; however, architectural diversity is more difficult in an OT environment. In an ICS environment (and particularly on the OT network), passive decoys are less likely to cause problems than active decoys.

T0802 (Automated Collection): Maintain a decoy control device or server with false operational data to serve as a target for automated collection.

T0807 (Command-Line Interface): Maintain a decoy system with a command line interface and monitor it for indications of unauthorized command-line use.

T0814 (Denial of Service): Maintain a decoy system or device as a target for denial-of-service attacks.

T0821 (Modify Controller Tasking): Maintain a decoy controller and monitor it for indications of unauthorized modifications of tasking.

T0823 (Graphical User Interface): Maintain a decoy system with a GUI and monitor it for indications of unauthorized commands via the GUI.

T0835 (Manipulate I/O Image): Maintain a decoy PLC and check periodically whether its input or output image table matches observed inputs and outputs.

T0836 (Modify Parameter): Make a factitious system and observe whether any of its key operating parameters change.

T0840 (Network Connection Enumeration): Maintain decoy devices and systems on the network, with sufficient network activity among them to make them appear interesting.

T0842 (Remote System Discovery): Make a factitious system easily discoverable by other systems on the network.

T0843 (Program Download): Maintain a decoy controller and monitor it for evidence that an unauthorized program has been downloaded.

T0849 (Masquerading): Maintain a decoy system and monitor it for evidence of masquerading.

T0851 (Rootkit): Maintain a decoy system and monitor it for indications of rootkit installation.

T0853 (Scripting): Maintain a decoy system and monitor it for indications of malicious use of scripting.

T0855 (Unauthorized Command Message): Maintain decoy control system devices to trick an adversary into sending false control messages which could have an Impact. While most devices will not be capable of determining the possibility of Impact, a specially crafted decoy could.

T0856 (Spoof Reporting Message): Maintain a decoy master station, management / engineering workstation, or other outstation to serve as a recipient of reporting messages, and to respond to such messages with a query for a follow-on report or to correlate the messages it receives with messages received by other outstations.

T0858 (Change Operating Mode): Maintain decoy devices (programmable controllers) on the network and monitor them for unexpected changes in operating mode.

T0861 (Point & Tag Identification): Operate a decoy system (e.g., a Data Historian, Control Server, or Human-Machine Interface system) which maintains false but plausible point and tag values.

T0868 (Detect Operating Mode): Maintain decoy devices (programmable controllers) on the network and configure them differently from normal devices to mislead the adversary about operating modes.

T0872 (Indicator Removal on Host): Maintain a decoy system (e.g., an HMI system or SIS) and monitor it for indications such as removal of event logs.

T0873 (Project File Infection): Maintain decoy project files and monitor for modification.

T0877 (I/O Image): Maintain decoy devices and monitor traffic from them that indicates transmission of an I/O image.

T0889 (Modify Program): Place decoy controllers on the OT network and check periodically to see whether they are modified.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1205	**Component Provenance Validation**	SR-4, SR-4(1), SR-4(2), SR-4(3), SR-4(4), SR-11(3)	Validate the provenance of system components.	Provenance Tracking

T0862 (Supply Chain Compromise): Define and execute processes to identify the source(s), scan for counterfeiting, determine the security posture, and validate the integrity of software components, as documented in the SCRM Plan.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1207	**Adversarial Simulation**	CA-8, CA-8(1), CA-8(2), SC-7(10)	Simulate adversary activities to test the effectiveness of system protections and detection mechanisms.	Self-Challenge

T0810 (Data Historian Compromise): Explore ways to compromise a data historian as part of a Red Team exercise.

T0818 (Engineering Workstation Compromise): Explore ways to compromise an engineering workstation as part of a Red Team exercise.

T0848 (Rogue Master): Set up a rogue master as part of a Red Team exercise to determine whether and how well control messages can be detected and discarded.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1208	**Dynamically Restrict Traffic or Isolate Resources**	AU-5(3), IR-4(2), SC-7(20)	Dynamically reconfigure networking to restrict network traffic or isolate resources.	Dynamic Resource Allocation, Adaptive Management, Dynamic Reconfiguration, Dynamic Segmentation, and Isolation

T0806 (Brute Force I/O): Dynamically isolate devices which appear to be performing a brute force I/O attack (e.g., sending a high volume of traffic, particularly at times when the device is expected to be quiescent), or reconfigure traffic filtering to drop all traffic from a given address associated with such an attack.

T0886 (Remote Services): Dynamically isolate subnets, servers, or specific components to restrict the use of remote services.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1209	**Virtual Sandbox**	SC-7(20), SI-14	Use virtualization to create a controlled execution environment, which is expunged after execution terminates.	Non-Persistent Services, Dynamic Segmentation, and Isolation

T0847 (Replication Through Removable Media): Use a virtual sandbox for execution of files on removable media.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1222	**Perform Mission Damage Assessment**	CP-2(8), RA-9, SI-4(1), SI-7, SI-7(1)	Determine the mission consequences of adversary activities.	Sensor Fusion and Analysis, Mission Dependency and Status Visualization, Integrity Checks

Discussion: Damage assessment is intended to determine which resources can be relied on; how quickly, how completely, and with what confidence services, data, and communications can be restored from backups or alternative resources. Damage assessment is also intended to determine when to shut down systems before they cause further harm. Mission damage assessment translates this information into mission terms, e.g., which mission-essential functions are degraded and how long the degradation will last. Note that CP-2(8) and RA-9 are not crucial to CM1222, but significantly enhance the effectiveness of its use.

T0809 (Data Destruction): Determine mission consequences of data destruction.

T0828 (Loss of Productivity and Revenue): Determine the potential consequences for productivity and revenue of planned responses to adversity, based on analysis of affected systems, services, and supporting infrastructures.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1223	**Active Decoys**	SC-26, SC-35, SC-44, SA-23	Use one or more factitious systems or other resources to identify malicious sites, interact with the adversary, actively probe for malicious code, and observe adversary TTPs.	Forensic and Behavioral Analysis, Misdirection, Dynamic Segmentation and Isolation, Specialization

T0810 (Data Historian Compromise): Maintain a decoy data historian, actively engaging with the adversary.

T0818 (Engineering Workstation Compromise): Maintain a decoy engineering workstation, actively engaging with the adversary.

T0817 (Drive-by Compromise): Use a honeyclient to visit sites commonly visited by organization staff to identify sources of malware.

T0848 (Rogue Master): Maintain decoy outstations to trick an adversary's rogue master into sending detectable messages.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1226	**Enhanced Authentication**	IA-2(13), IA-10, CP-13, SC-47	Use situation-specific, risk-adaptive, or out-of-band authentication.	Adaptive Management, Calibrated Defense-in-Depth, Architectural Diversity, Design Diversity, Path Diversity, Dynamic Privileges

T0822 (External Remote Services): Use out-of-band authentication to make adversary efforts to use external remote services more difficult.

T0842 (Network Sniffing): Use out-of-band authentication to complicate the adversary's efforts to capture authenticators.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1227	**Minimize Duration of Connection or Session**	AC-12, SC-7(10), SC-10, SI-14 (3)	Minimize the time period for which a connection remains open or a session remains active, requiring reauthorization to reestablish connectivity.	Non-Persistent Services, Non-Persistent Connectivity

T0822 (External Remote Services): Minimize the duration of or unpredictably interrupt services which allow users to connect to internal enterprise network resources from external locations, thus forcing off an adversary who has obtained access to a one-time authenticator. This also applies to situations in which a vendor needs access for a limited timeframe.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1230	**Validate Data Quality**	SA-9(7), SI-7(1)	Validate data quality (e.g., integrity, consistency, correctness).	Integrity Checks

T0809 (Data Destruction): Periodically validate the quality of stored data to determine whether data has been destroyed.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1234	**Refresh Selected Applications or Components**	SI-14 (1)	Refresh software, firmware, or data from a trusted source.	Non-Persistent Services, Non-Persistent Information, Provenance Tracking

T0890 (Exploitation for Privilege Escalation): Periodically refresh software and configuration settings to restore privileges to the minimal set associated with the software.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM1237	**Validate Data Properties**	PL-8(1), SC-16(1), SC-16(3), SI-7, SI-7(1)	Validate data properties (including binaries, metadata, and cryptographic bindings) to defend against modification or fabrication.	Integrity Checks, Calibrated Defense-in-Depth
T0836 (Modify Parameter): Build data quality (e.g., correctness, consistency) checks into multiple locations in mission, business, or system workflows to ensure that parameters have not been manipulated.				
T0873 (Project File Infection): Apply data quality checking (e.g., consistency, correctness) to project files on a periodic basis.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1242	**Switch to Protected Hot Standby**	AC-4(2), AC-4(8), CP-2(5), CP-9(6), IR-4(2)	Switch (failover) to a duplicate system in a protected enclave which, subject to additional quality controls on data and software updates, mirrors the system which has been compromised.	Dynamic Reconfiguration, Adaptive Management, Orchestration, Replication, Predefined Segmentation, Integrity Checks
T0809 (Data Destruction): Orchestrate the switch to a protected hot shadow system in a protected enclave on which the destroyed data is mirrored, recognizing that the additional protections may mean some data is not as current or complete as on the primary system.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1245	**Defend Failover and Recovery**	AC-2(6), IR-4(2), IR-4(3), SC-7(20), SC-48, SC-48 (1), SI-4(1)	Increase sensor activity and restrict privileges to defend against an adversary taking advantage of failover or recovery activities.	Adaptive Management, Dynamic Reconfiguration, Orchestration, Functional Relocation of Sensors, Dynamic Segmentation and Isolation, Mission Dependency and Status Visualization, Dynamic Privileges
Discussion: Manage failover and recovery activities to minimize adversary interference with them and to ensure that the adversary cannot take advantage of them to penetrate backup or newly restored systems. This can involve temporarily defining and protecting enclaves for systems being restored; changing privileges on backup systems; increasing, relocating, and tailoring sensing; and presenting more detailed information via visualization. Note that failover and recovery can be in response to disruptive events which may not be caused by (or may not be attributable to) an adversary; even accidental or environmental disruptions can provide opportunities for an adversary to establish a new foothold. Failover and recovery efforts need to be orchestrated to ensure that privileges and protections on backup, activated standby, and recovered systems are consistent, since adversaries can take advantage of gaps or inconsistencies.				
T0813 (Denial of Control): Manage failover and recovery activities to limit the adversary's ability to interfere with process control actions. It may be necessary to "wall off" portions of the OT network or to isolate specific devices.				
T0815 (Denial of View): During failover and recovery activities, watch for and respond to transient gaps or anomalies in status and reporting messages, treating these as indicators of possible compromise.				
T0826 (Loss of Availability): Manage failover and recovery activities for an essential component or system (e.g., HMI system), to ensure that an adversary cannot seize the opportunity to establish a fresh foothold.				

T0831 (Manipulation of Control): During failover and recovery activities, watch for and respond to anomalous or unexpected behavior, treating such behavior as indicators of adversary manipulation.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1247	**Defend Against DoS**	AC-4(3), SC-5(2), SC-5(3)	Adapt to reduce the impacts of denial-of-service attacks.	Dynamic Resource Allocation, Adaptive Management, Surplus Capacity, Monitoring and Damage Assessment

Discussion: If a system has surplus capacity (e.g., bandwidth, storage, processing), that capacity can be reallocated dynamically to compensate for DoS. This is meaningful for endpoint systems (e.g., servers, workstations), for virtual systems (e.g., in a cloud environment), and for networks.

T0814 (Denial of Service): Dynamically reallocate surplus capacity or redundant resources to adapt to denial-of-service attacks.

T0806 (Loss of Availability): Dynamically reallocate surplus capacity or redundant resources to adapt to denial-of-service attacks.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1248	**Conceal or Randomize Network Traffic**	SC-8(5), SC-30	Conceal (via encryption or insertion of fabricated traffic) or randomize network traffic patterns.	Obfuscation, Contextual Unpredictability

T0842 (Network Sniffing): Insert fabricated network traffic to mislead the adversary.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1253	**Modulate Information Flows**	AC-4(27), AC-4(29), AC-4(30), SC-7(15), SC-46	Use controlled interfaces and communications paths to provide access to risky capabilities or to filter communications between enclaves.	Orchestration, Design Diversity, Replication, Predefined Segmentation, Trust-Based Privilege Management

T0886 (Remote Services): Use a dedicated, managed interface for networked privileged accesses to remote services.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1254	**Hardware-Based Protection of Firmware**	SC-51	Use hardware-based protections for firmware.	Integrity Checks

T0839 (Module Firmware): Use hardware-based write protection for module firmware.

T0857 (System Firmware): Use hardware-based write protection for system firmware.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1255	**Validate Output Data**	SI-15	Validate information output from processes or applications against defined criteria.	Integrity Checks

T0836 (Modify Parameter): Validate information output from processes or applications against defined criteria, since invalid output may indicate that an adversary has modified a parameter.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM1259	**Enhance User Preparedness**	AT-2(1), AT-2(3), AT-2(5), AT-3(3)	Keep users, administrators, and operators aware of existing and emerging threats and attack techniques they can counter in practice.	Dynamic Threat Awareness, Self-Challenge
T0863 (User Execution): Train users about current and emerging tactics to entice users into executing malware.				
T0865 (Spearphishing Attachment): Train users about spearphishing tactics, providing up-to-date examples.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1260	**Conceal Resources from Discovery**	SC-7(16), SC-28(1), SC-30, SC-30(5)	Protect network addresses of system components that are part of managed interfaces from discovery through common tools and techniques, via hiding or relocation.	Obfuscation, Functional Relocation of Cyber Resources
T0840 (Network Connections Enumeration): Conceal the location of remote systems, or periodically change their network addresses.				
T0842 (Remote System Discovery): Conceal the location of remote systems, or periodically change their network addresses.				
T0888 (Remote System Information Discovery): Conceal the location of remote systems, or periodically change their network addresses.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1262	**Restrict Supply Chain Exposures**	CM-7(7), SR-3(2), SR-5, SR-6(1), SR-7, SR-10, SR-11	Restrict adversaries' ability to determine or manipulate the organization's cyber supply chain.	Orchestration, Obfuscation, Disinformation, Self-Challenge, Supply Chain Diversity, Replication, Predefined Segmentation, Integrity Checks, Provenance Tracking
T0862 (Supply Chain Compromise): Acquire system components for which provenance and constituent elements can be identified, either by the source vendor / integrator or via analysis in a safe environment.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1275	**Emergency Shutdown**	IR-4(2), IR-4(3), SC-29	Shut down physical processes safely.	Dynamic Reconfiguration, Architectural Diversity
Discussion: Plan for and provide mechanisms for safe emergency shutdown (IR-4(2), IR-4(3)), ensuring that safety is central to contingency planning (CP-2). Emergency shutdown can involve power shutdown (using PE-10), other physical switches, messages, and commands issued via a keyboard or GUI. Recovery will be facilitated if the system fails in a known state (SC-24). Multiple, different shutdown mechanisms (SC-29) can make an adversary's job harder.				
T0813 (Denial of Control): Use physical or other mechanisms to shut down process controllers or systems from which operators are locked out.				
T0827 (Loss of Control): Use physical or other mechanisms to shut down misbehaving process controllers or systems safely.				

T0831 (Manipulation of Control): Use physical or other mechanisms to shut down misbehaving process controllers or systems safely.

T0879 (Damage to Property): Execute emergency shutdowns in such a way as to minimize damage to equipment, infrastructure, and the surrounding environment.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1276	**Safe Mode Restart**	CP-12	Reboot devices and restart physical processes safely.	Adaptive Management, Restriction
Discussion: Plan for and provide mechanisms for safe rebooting of devices and safe restarting of physical processes. Safe restart can involve restricting the use of functionality or using functions differently than in normal operations. Note that this mitigation is most effective if CM1275 has already been applied.				

T0813 (Denial of Control): Safely reboot process controllers or systems from which operators have been locked out.

T0827 (Loss of Control): Safely reboot process controllers or systems from which operators have been locked out, restarting physical processes in constrained environments.

T0831 (Manipulation of Control): Safely reboot process controllers or systems safely, restarting physical processes in constrained environments.

T0879 (Damage to Property): Restrict functionality and increase monitoring of health and status in order to restart physical processes safely.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1277	**Coordinate Responses to Adversity**	CP-2(1), CP-2(5), CP-4(5)	Coordinate responses to adversity to minimize impacts on service delivery.	Consistency Analysis, Orchestration, Self-Challenge
Discussion: Plan for, establish processes, and provide resources to ensure that responses to adversity minimize loss of productivity, revenue, or reputation. Loss of productivity can result from cyber-attacks against the organization or its systems but can also arise from loss of infrastructure services (e.g., power loss) or from the determination that some critical component, service, or infrastructure element is potentially malicious. Tabletop exercises, particularly joint exercises, can greatly enhance the plans, verify that processes can be followed, and determine whether resources to execute plans are actually available. Most of this involves efforts at the mission or business process level or at the organizational level, rather than at the system level, and is part of enterprise risk management (ERM). Organizational use of this mitigation will also apply IR-4, PM-8, Critical Infrastructure Plan, PM-9, Risk Management Strategy, PM-11, Mission and Business Process Definition, and PM-16, Threat Awareness Program (used to share information with external stakeholders rather than as an application of Dynamic Threat Awareness), but those uses are standard practice rather than cyber resiliency. At the system level, this is reflected in contingency planning.				

T0827 (Loss of Control): Plan for scenarios in which control of critical systems or components is lost.

T0828 (Loss of Productivity and Revenue): Plan for disruptions to productivity resulting from a broad range of possible adversity, including cyber-attacks, loss of infrastructure services, and determination that some critical component, service, or infrastructure element is potentially malicious.

T0831 (Manipulation of Control): Plan for scenarios in which an adversary manipulates control of critical systems or components.

T0879 (Damage to Property): Plan for potential damage to equipment, infrastructure, or the surrounding environment resulting from issues with control systems.

Table 38. CMs with Indirect Potential Effects – Technique-Specific Descriptions

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1301	**Dynamic Threat Awareness and Response**	CA-7(3), RA-3(2), RA-3(3), RA-3(4), RA-5(10), RA-10, PM-16, PM-16 (1)	Use awareness of the current threat landscape to inform threat hunting and threat-adaptive defenses.	Adaptive Management, Sensor Fusion and Analysis, Dynamic Threat Awareness

Discussion: This CM is used for threat hunting (particularly under Defense Evasion and Command and Control) and when mitigations or candidate mitigations can be calibrated based on threat information (e.g., information flow controls can be reconfigured). Depending on the use, effects can include Detect, Reveal, Exert, and/or Shorten.

Examples of uses for Command and Control include:

- T1071 (Application Layer Protocol): Use up-to-date threat information and warnings to hunt for threats and inform the adaptive use of isolation and enclave boundary defense.
- T1573 (Encrypted Channel), T1008 (Fallback Channels), T1105 (Ingress Tool Transfer), T1104 (Multi-Stage Channels), T1095 (Non-Application Layer Protocol), T1572 (Protocol Tunneling), T1090 (Proxy): Use up-to-date threat information and warnings to hunt for threats and inform the adaptive use of enclave boundary defense.
- T1219 (Remote Access Software), T1205 (Traffic Signaling), T1102 (Web Service): Use up-to-date threat information and warnings to hunt for threats. (Note that this uses only Dynamic Threat Awareness, for a Detect effect.)

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1302	**Mission-Oriented Cyber Situational Awareness**	SI-4(1), SI-4(2)	Maintain awareness of mission dependencies and the current status of mission-critical assets to inform threat-adaptive responses.	Sensor Fusion and Analysis, Mission Dependency and Status Visualization

Discussion: This CM can be used in conjunction with CMs which use Adaptive Management, Functional Relocation of Sensors, Functional Relocation of Cyber Resources, Dynamic Privileges, or Dynamic Segmentation and Isolation. Its effect is Detect.

Specifically, this CM can be used in conjunction with CM1108 (Dynamically Restrict Traffic or Isolate Resources), CM1116 (Dynamic Data Location), CM1117 (Dynamic Account Management), CM1121 (Dynamically Disable or Suspend), CM1133 (Isolate or Contain Selected Applications or Components), CM1139 (Dynamically Reprovision), and CM1150 (Dynamically Relocate and Refresh Processing).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1303	**Integrated Non-Disruptive Response**	SI-4(3), SI-4(7), SI-7(5)	Integrate automated and human-directed response to suspicious events to minimize disruption.	Monitoring and Damage Assessment, Sensor Fusion and Analysis, Adaptive Management

Discussion: This CM can be used with any CM which has a dynamic aspect, as long as there is a detection CM which informs the use of that dynamic CM. Its effects, which are indirect, can be Detect, Shorten, or Reduce.

Specifically, this CM can be used in conjunction with CM1108 (Dynamically Restrict Traffic or Isolate Resources), CM1116 (Dynamic Data Location), CM1117 (Dynamic Account Management), CM1121 (Dynamically Disable or Suspend), CM1133 (Isolate or Contain Selected Applications or Components), CM1139 (Dynamically Reprovision), and CM1150 (Dynamically Relocate and Refresh Processing).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1304	**Enhance via Unpredictability**	SC-30(2), SI-19(6)	Enhance the effectiveness of defender actions by using capabilities unpredictably.	Contextual Unpredictability, Temporal Unpredictability

Discussion: SC-30(2) can be used with any CM which has a dynamic aspect, as long as unpredictability will not interfere with successful mission operations. Its effects, which are indirect, can be Degrade, Delay, Exert, or Shorten, depending on the CM which it is used to enhance. Specifically, SC-30(2) can be used in conjunction with CM1108 (Dynamically Restrict Traffic or Isolate Resources), CM1116 (Dynamic Data Location), CM1117 (Dynamic Account Management), CM1121 (Dynamically Disable or Suspend), CM1133 (Isolate or Contain Selected Applications or Components), CM1139 (Dynamically Reprovision), and CM1150 (Dynamically Relocate and Refresh Processing).

The mechanism of adding non-deterministic noise to the results of a query or computation, while defined in terms of personally identifiable information in SI-19(6), can be used more broadly to thwart adversary attempts to extract and correlate sensitive information. Specifically, an extension of SI-19(6) can be used in conjunction with CM1101 (Present Deceptive Information) against T1213 (Data from Information Repositories).

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1305	**Enhance via Heterogeneity**	AU-9(7), CP-11, SC-29, SC-29 (1)	Increase barriers to adversary effectiveness by providing architecturally diverse system components.	Architectural Diversity, Design Diversity

Discussion: AU-9(7), SC-29, and SC-29(1) can be used whenever architecturally diverse components (e.g., platforms with different operating systems) can make the adversary's job harder, by requiring them to do more discovery and to develop attack tools specific to the different components. This is particularly relevant to ATT&CK Techniques (or Sub-Techniques) which are specific to a single Platform (e.g., T1559, Inter-Process Communication, is specific to Windows). The effects can be Delay or Exert.

For example, in Defense Evasion:

- T1070 (Indicator Removal on Host): Store audit data for a system with one operating system on another system, with a different operating system, to make restriction of write access to and/or remote storage of audit data more effective.
- T1599 (Network Boundary Bridging): Monitor network traffic on both interfaces of border network devices with out-of-band packet capture or network flow data, using a different device than the one in question.

This CM can also enhance deception activities, in particular CM1102, CM1104, and CM1131.

CP-11 can be used to enhance the effectiveness of response activities, in particular CM1143, CM1145, and CM1147.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM1306	**Lock Down Installation**	AC-3(12), AC-6(10), CM-5(5), CM-5(6), CM-7(4)	Restrict access to applications and configurations as part of the installation process, and narrowly restrict modifications or other uses of privileged functions.	Attribute-Based Usage Restriction, Trust-Based Privilege Management

Discussion: This CM can be used in conjunction with Mitigations and CMs which address adversary actions which escalate privileges or modify components or configurations during installation.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1307	**Enhance via Layered Protections**	PL-8(1), SC-3(5)	Provide similar capabilities or mechanisms at multiple architectural layers.	Calibrated Defense-in-Depth

Discussion: This CM can be used in conjunction with CMs for which similar capabilities can be provided at different architectural layer. Its effects can be Degrade, Delay, or Exert.

For example:

T1119 (Automated Collection): Fragment, relocate, segment, or impose multiple access controls on stored data at multiple levels (e.g., directory, file, record). (Use in conjunction with CM1114, CM1116, and/or M1029.)

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1308	**Separate Environments with Specific Risks**	AU-6(8), CM-4(1), SC-7(13)	Provide environments separate from the operational environment for activities with specific risks.	Monitoring and Damage Assessment, Predefined Segmentation

Discussion: Several activities present risks to the operational environment and can be made less risky by providing separate environments. These include:

- Audit analysis. AU-6(8) can be used in conjunction with CMs in which analysis of logs, audit trails, and adversary artifacts can be performed in a separate environment (e.g., CM2038). The goal is to perform analysis without compromising information about the fact or results of the analysis. Other CMs which could be made more effective include CM1158 and CM2005.
- Malware analysis and other computer network defense (CND) operations. A separate environment for malware analysis can prevent it from infecting systems in the operational environments, and a separate environment for developing defender tools can protect those tools against adversary discovery and development of countermeasures. SC-7(13) can be used with CM1136 as well as with IR-4(12) and SI-3(1).
- Analysis in a test or evaluation environment, to determine whether a component which could be added to the system contains malicious logic. The goal is to reduce supply chain risks. CM-4(1) can be used with CM2009, CM2010, and CM2011, as well as with SA-11(5).

The effects of CM1308 are indirect, and can be Negate, Degrade, and/or Exert.

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)

CM1309	**Vulnerability-Oriented Cyber Situational Awareness**	RA-5(6), RA-5(8), RA-5(10)	Maintain awareness of the vulnerability posture over time to inform calibration of detection as well as proactive responses.	Sensor Fusion and Analysis
Discussion: This CM can be used in conjunction with CMs which have a dynamic aspect (see CM1303), or which use tailorable information flow controls (e.g., CM1151). Its effect (which is indirect) is Detect.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1310	**Protect Distributed Processing and Storage**	SC-36 (1), SC-36 (2)	Provide supporting protections for distributed processing and distributed or replicated storage.	Behavior Validation, Replication
Discussion: This CM can be used in conjunction with CM1141, CM1142, and/or CM1143. Its effects can be Negate, Degrade, and/or Exert.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1311	**Enhance via Isolation**	SC-3(2), SC-39 (2), SC-50	Enhance the effectiveness of, or confidence in, security functions via system mechanisms for isolation.	Predefined Segmentation, Dynamic Segmentation, and Isolation
Discussion: This CM can be used with CMs which address adversary tampering with security functions, including functions which could manipulate or delete logs. Its effects can be Negate, Degrade, and/or Exert.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1312	**Enhance Isolation via Hardware Features**	SC-3(1), SC-39 (1), SC-49	Enhance the effectiveness of, or confidence in, isolation by using underlying hardware features.	Predefined Segmentation, Dynamic Segmentation, and Isolation
Discussion: This CM can be used with CMs involving Predefined Segmentation and Dynamic Segmentation and Isolation. Its effects can be Negate, Degrade, and/or Exert. Its effects can be Negate, Degrade, and/or Exert.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**
CM1313	**Validate or Assess Control Effectiveness in Practice**	CP-4(5), CP-9(1), SI-19(8)	Validate or assess the effectiveness of controls as implemented and used in practice.	Self-Challenge, Protected Backup and Restore, Integrity Checks
Discussion: CP-4(5) can be used with CMs for restoration or reconstitution of cyber assets or functionality, including CM1161, CM1138, CM1139, CM1141, CM1142, CM1143, and CM1145. CP-9(1) enhances the effectiveness of M1053. For SI-19(8), perform analysis of datasets which have been defensively manipulated to make some sensitive information impossible to retrieve or reconstruct (e.g., de-identified data) to determine whether the sensitive data can be found or reconstructed.				
Identifier	**Name**	**Controls**	**Description**	**Cyber Resiliency Approach(es)**

CM1314	**Enhance via Automation**	CA-7(6) , PE-6(2), PM-16(1), RA-5(6), SI-4(2), SI-4(3), SI-4(7), SI-7(5)	Use automation to increase the effectiveness or quality of capabilities and practices.	Adaptive Management, Monitoring and Damage Assessment, Sensor Fusion and Analysis, Dynamic Threat Awareness
Discussion: Automation – including the use of artificial intelligence or machine learning – can be used to make the use of other controls more effective, or to make the results of those uses higher-quality (e.g., more accurate, current, or available). This is particularly the case for automation related to analysis of and response to monitored events or behaviors. CA-7(6) can enhance the effectiveness of all Mitigations and CMs that apply Monitoring and Damage Assessment (i.e., M1047, all CM20## Candidate Mitigations), as well as CM1158, by making the results of monitoring higher-quality. PE-6(2) can enhance the effectiveness of some CMs that apply Sensor Fusion and Analysis (i.e., CM2005, CM2018, CM2023), by monitoring physical access. RA-5(6). The (indirect) effect of CA-7(6), PE-6(2), SI-4(2), SI-4(3) is Detect. The (indirect) effect of SI-4(7) and SI-7(5) is Shorten.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1315	**Maintain a War-Time Reserve**	RA-9, SA-20, SA-23, SR-5(1)	Maintain a reserve of critical components, both special-purpose and acquired, for use in a crisis situation.	Mission Dependency and Status Visualization, Specialization, Replication
Discussion: This CM supports CM1141, CM1143, CM1144, and CM1163.				

Identifier	Name	Controls	Description	Cyber Resiliency Approach(es)
CM1316	**Enhance via Coordination**	CP-2(1), IR-4(10), IR-4(11)	Coordinate across the organization and with external stakeholders to increase the effectiveness or timeliness of responsive capabilities and practices.	Adaptive Management, Orchestration
Discussion: CP-2(1) can be applied to ensure coordination in advance of response efforts. IR-4(10) and IR-4(11) involve coordination of response efforts applying Orchestration so that actions using Adaptive Management are minimally disruptive. This CM supports organization-internal responses to suspicious activities via CM1108, CM1121, CM1126, CM1142, CM1143, and CM1143. It also supports coordination beyond the organization via CM1161 and CM1162.				

Appendix D Acronyms

- A4E ATT&CK for Enterprise
- A4I ATT&CK for ICS
- ACL Access Control List
- AD Active Directory
- AFRL Air Force Research Laboratory
- API Application Interface
- APT Advanced Persistent Threat
- BIOS Basic Input/Output System
- BITS (Windows) Background Intelligent Transfer Service
- C2 Command and Control
- CDM Continuous Diagnostics and Monitoring
- CHM Compiled HTML
- CIS Center for Internet Security
- CM Candidate Mitigation
- CMMC Cybersecurity Maturity Model Certification
- CMSTP (Microsoft) Connection Manager Profile Installer
- CNSS Committee on National Security Systems
- CNSSI CNSS Instruction
- COM Component Object Model
- CPL Control Panel
- CPU Central Processing Unit
- CREA Cyber Resiliency Effects Analysis
- CREF Cyber Resiliency Engineering Framework
- CSA Cyber Survivability Attributes (or Attribute)
- CSEIG Cyber Survivability Endorsement Implementation Guide
- CSS Central Security Service
- CT&E Cyber Test and Evaluation
- CTID Center for Threat-Informed Defense
- DCE/RPC Distributed Computing Environment/Remote Procedure Call
- DCOM Distributed COM

- DDE Dynamic Data Exchange
- DLL Dynamic Link Library
- DMZ Demilitarized Zone
- DNS Domain Name System
- DoD Department of Defense
- DoS Denial of Service
- EFI Extensible File Interface
- EIT Enterprise Information Technology
- FPD Final Public Draft
- H&S Health and Status
- HMI Human-Machine Interface
- I/O Input/Output
- ICS Industrial Control System(s)
- IdAM Identity and Access Management
- IED Intelligent Electronic Device
- IPC Inter-Process Communication
- IT Information Technology
- JCS Joint Chiefs of Staff
- LLMBR Link-Local Multicast Name Resolution
- .LNK Link (file extension)
- LSA Local Security Authority
- LSASS LSA Subsystem Service
- MBR Master Boot Record
- MS Microsoft
- MSI Microsoft Installer
  (now known as Windows Installer, but file extensions still have the form .msi)
- NBT-NS NetBIOS Name Service
- NCCoE (NIST) National Cybersecurity Center of Excellence
- NCF NIST Cybersecurity Framework
- NFV Network Function Virtualization
- NIST National Institute of Standards and Technology
- NSA National Security Agency
- NTCTF NSA/CSS Technical Cyber Threat Framework

- OS Operating System
- OT Operational Technology
- PLC Programmable Line Controller
- RAR Roshal Archive (file format)
- RMF Risk Management Framework
- RTU Remote Terminal Unit
- SCRM Supply Chain Risk Management
- SDLC System Development Life Cycle
- SDN Software-Defined Networking
- SIP Subject Interface Package
- SIS Safety Instrumented System(s)
- SMB Server Message Block
- SP (NIST) Special Publication
- SSE Systems Security Engineering
- STIX™ Structured Threat Information eXpression
- TAXII™ Trusted Automated eXchange of Indicator Information
- TTPs Tactics, Techniques, and Procedures
- TTX Tabletop Exercise
- VPN Virtual Private Network
- XSL eXtensible Stylesheet Language
- ZT Zero Trust
- ZTA Zero Trust Architecture

NOTICE

This technical data was produced for the U. S.

Government under contract SB-1341-14-CQ-0010, and is subject to the Rights in Data-General Clause 52.227-14, Alt. IV (DEC 2007)