Federated Analysis of Cyber Threats (FACT)

Capstone Overview

Jackson Wynn

July 2015

One of five U.S. Air Force Air and Space Operations Centers (AOCs)

http://www.mitre.org/publications/project-stories/smaller-computer-footprint-in-air-force-operations-centers-boosts-effectiveness

MITRE

Federated Analysis of Cyber Threats (FACT)

- **Explores the exchange of cyber threat intelligence developed from cyber incident analysis and response**
  - Exchange of threat indicators and adversary TTPs among mission partners
  - Cyber incident reporting
  - Mitigation best practices released to acquisition organizations
  - Distribution of cyber playbook and mission model data

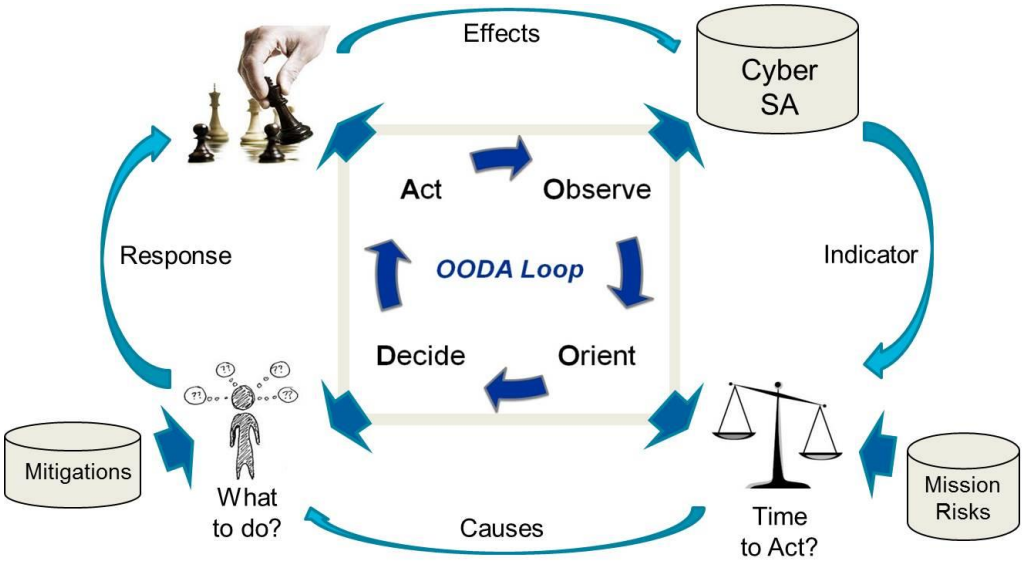
- **Imports and exports cyber threat intelligence in an industry-standard XML format (STIX™)**

Approved for Public Release: 15-2008

Distribution Unlimited.

Modeling the Decision Lifecycle: Observe, Orient, Decide, Act (OODA)[1] Loop

"In order to win, we should operate at a faster tempo or rhythm than our adversaries..." Col John Boyd[2]

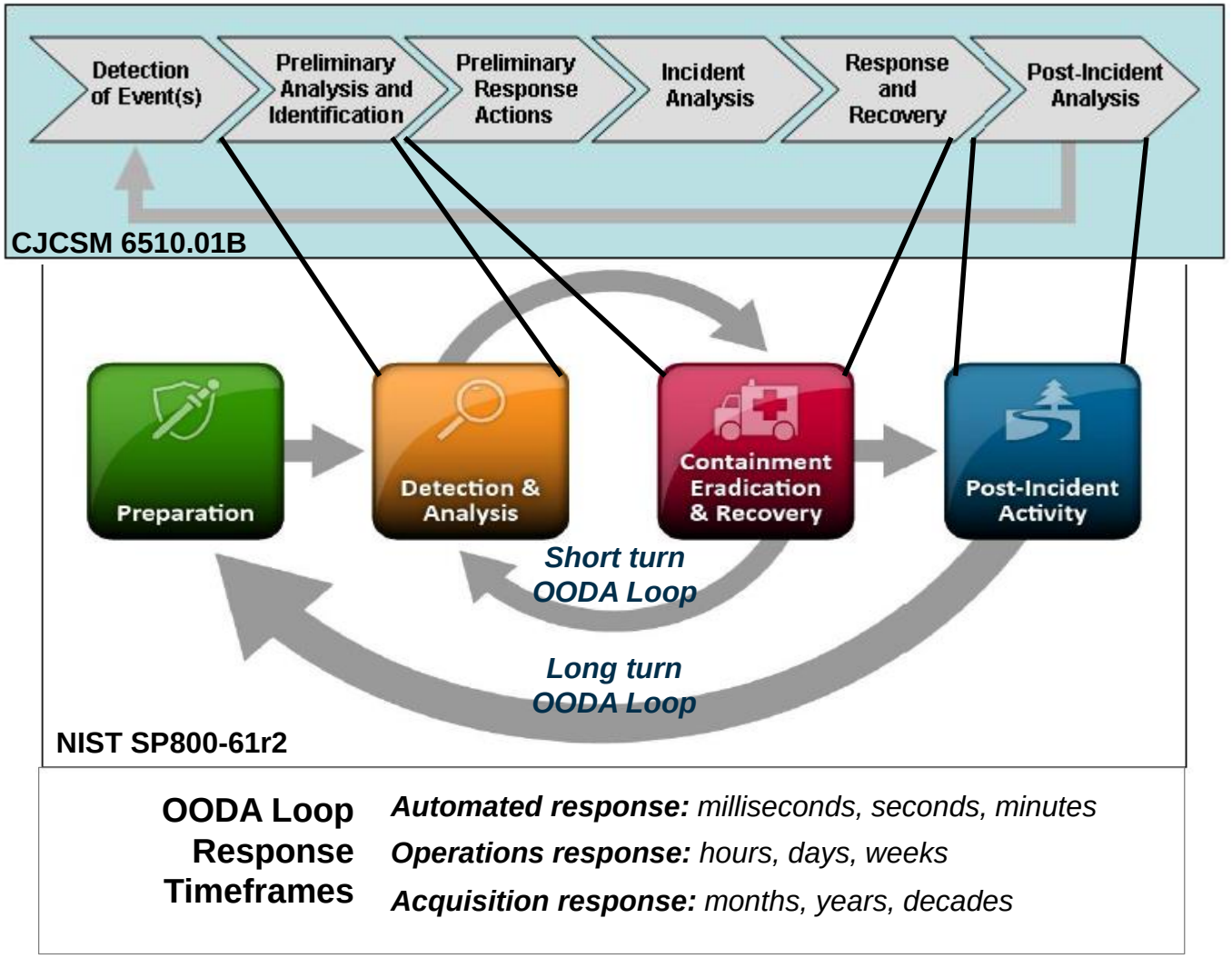


The time from initial indicator to response is a Key Performance Parameter (KPP)

[1]Observe, Orient, Decide, Act (OODA) loop: https://en.wikipedia.org/wiki/OODA_loop

[2]Boyd, J., "Patterns of Conflict", presentation, December 1986. http://www.dnipogo.org/boyd/patterns_ppt.pdf

OODA Loops in Cyber Incident Handling



OODA Loop Response Timeframes	***Automated response:*** *milliseconds, seconds, minutes*
	Operations response: *hours, days, weeks*
	Acquisition response: *months, years, decades*

FACT Tool Use Cases

- **Tool support for Information Security Analysis Teams (ISATs)**
  - Support identification of TTPs and potential mission impacts with a tempo that allows mitigations to be enacted without disrupting mission operations
  - Respond to intrusions more effectively using team structures that leverage federated analysis capabilities, enabled through information sharing
    - Reachback to leverage national assets that provide malware analysis and reverse engineering, coordinated response, etc.

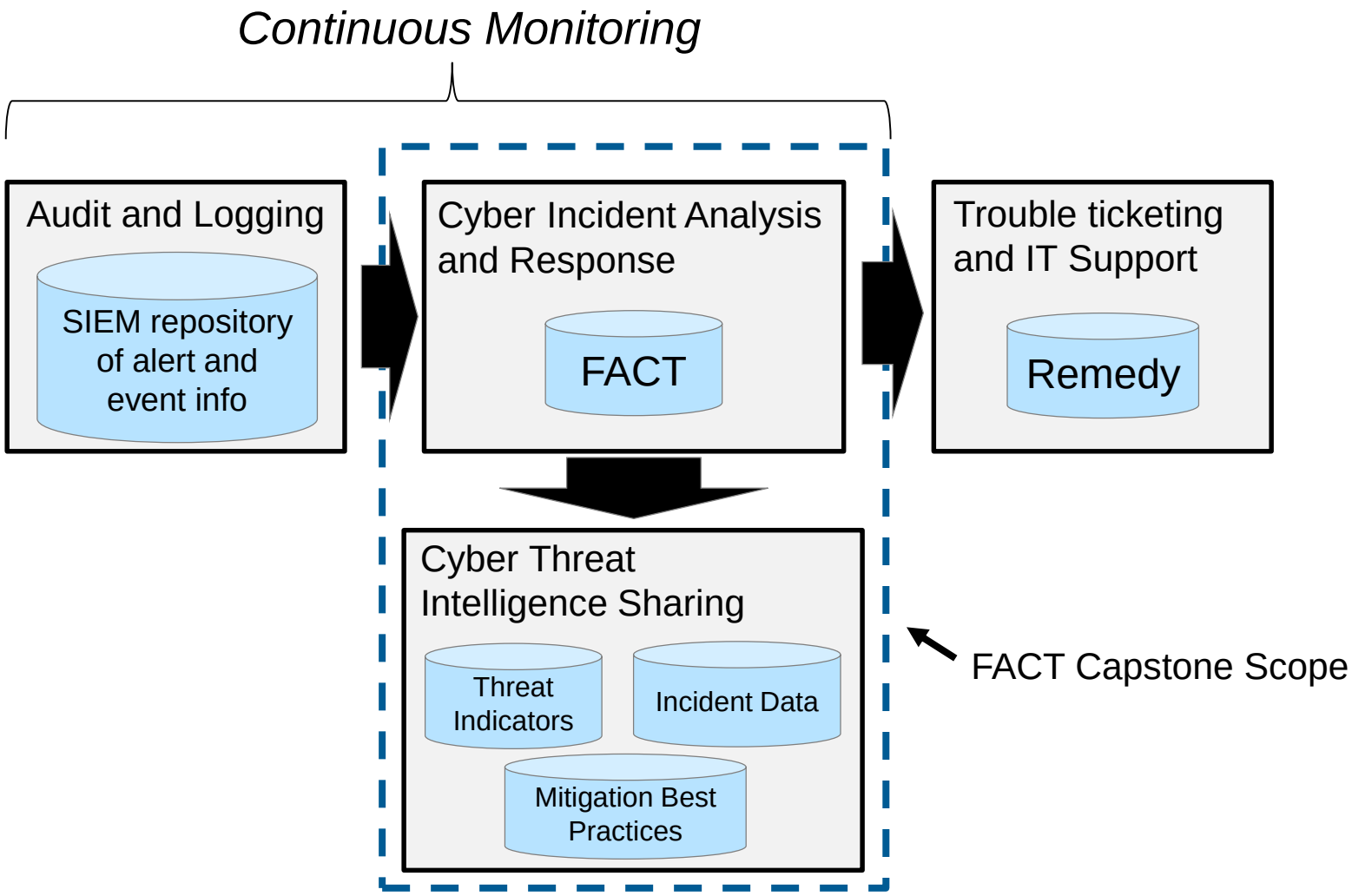
Navy Cyber Defense Operations Command

http://www.defense.gov/news/newsarticle.aspx?id=119470

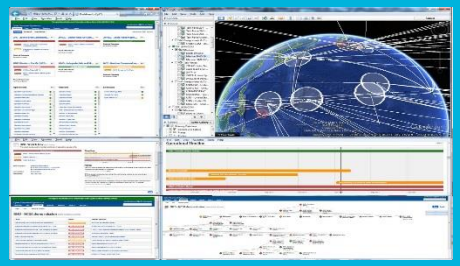
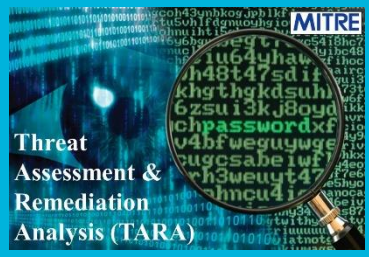
U.S. Army Cyber Command

http://cybersecuritydojo.com/2015/03/28/

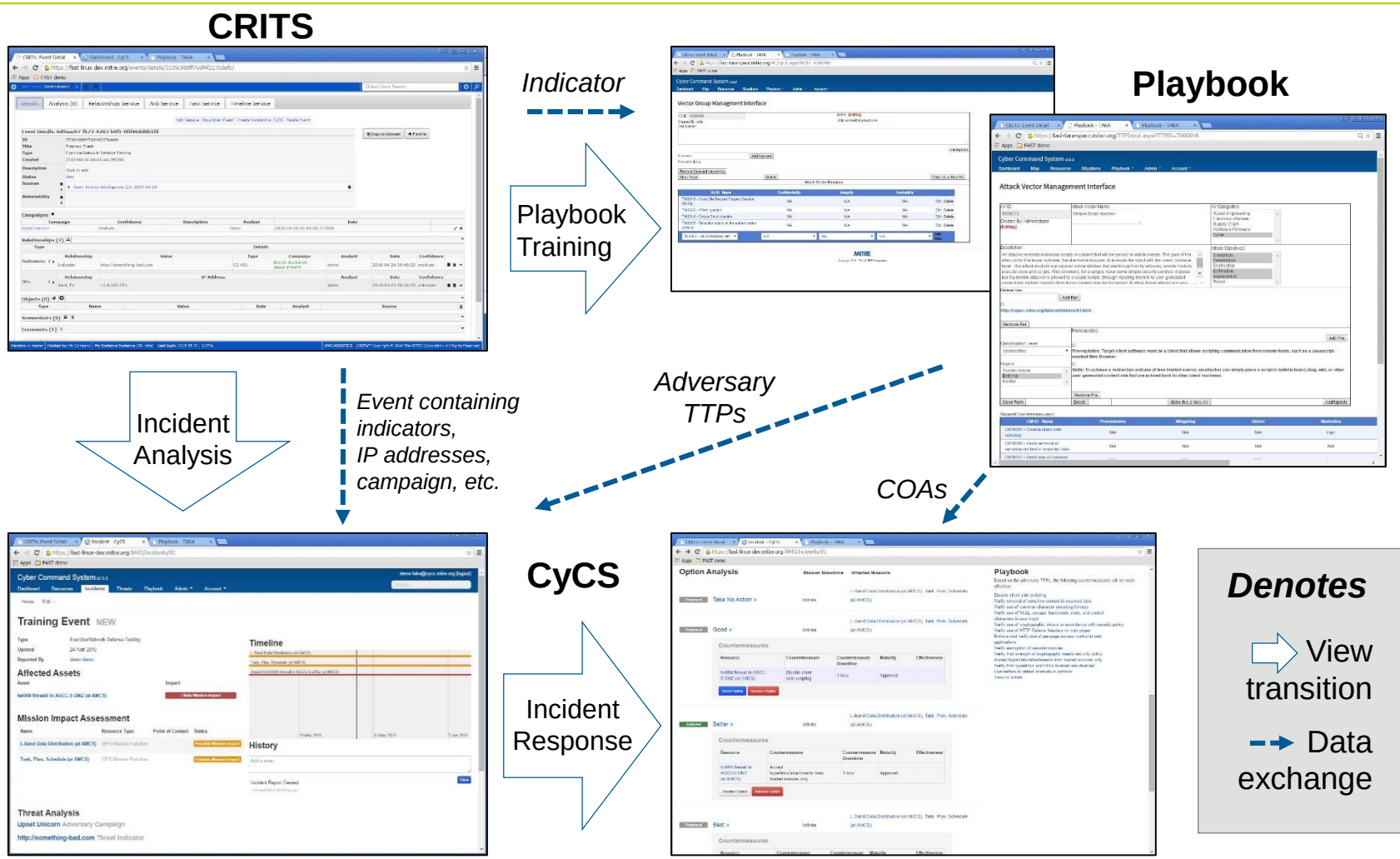
FACT Operational Context



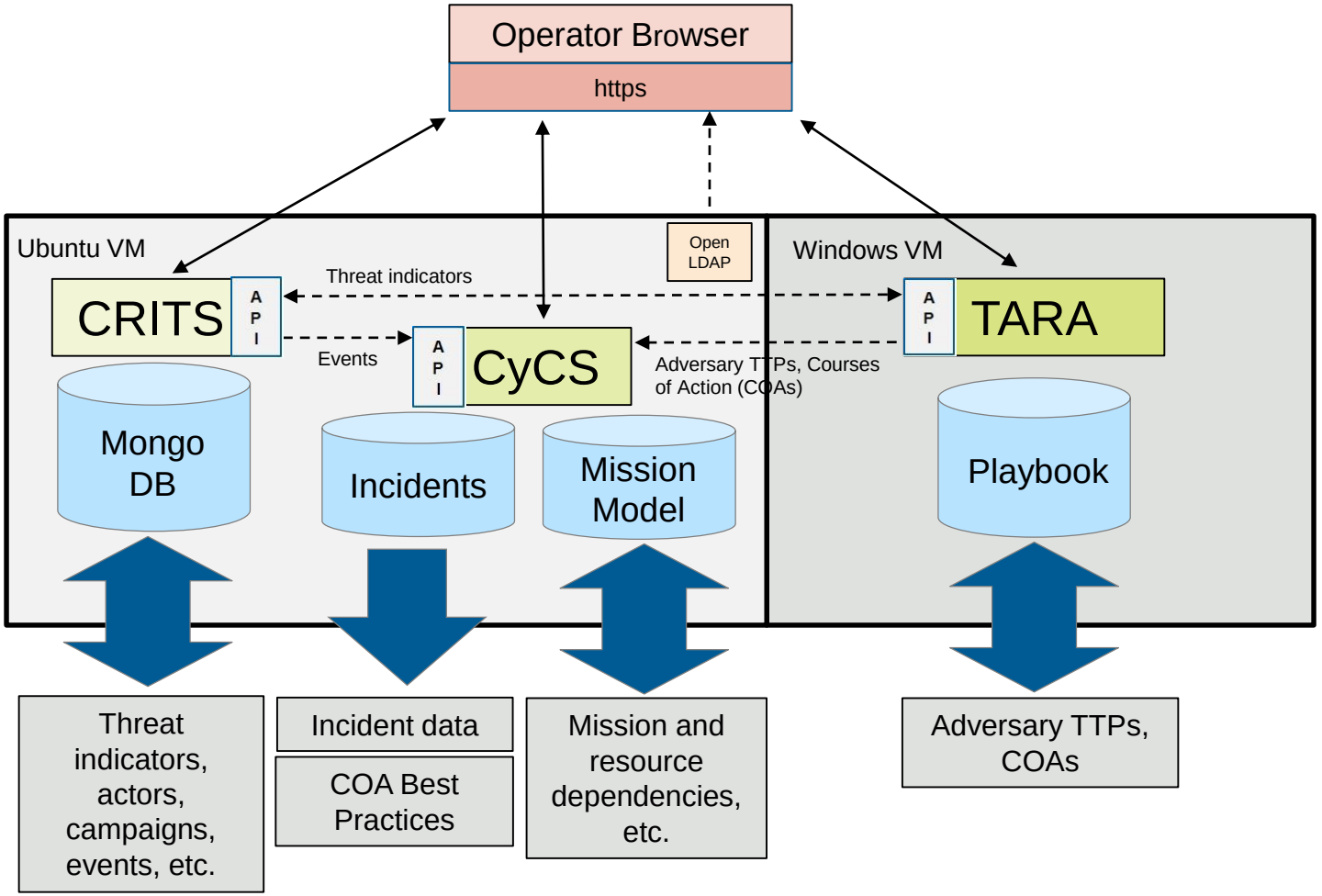
MITRE-Developed Tools Integrated into FACT: CRITS, CyCS, and TARA

CRITS	CyCS	TARA Playbook
		
Collaborative Research into Threats (CRITS) Used to analyze SIEM and sensor data to identify and correlate cyber threat indicators with campaigns (intrusion sets) and threat actors	**Cyber Command System (CyCS)** Used to assess mission impact based on a mission model reflecting the mission's functional decomposition and allocation to cyber resources	**Threat Assessment and Remediation Analysis (TARA)** Used to store cyber threat indicators, adversary TTPs, and defensive countermeasures to support analysis of threats and selection of alternative Courses of Action (COAs) in response to cyber incidents

Tool Functional Integration

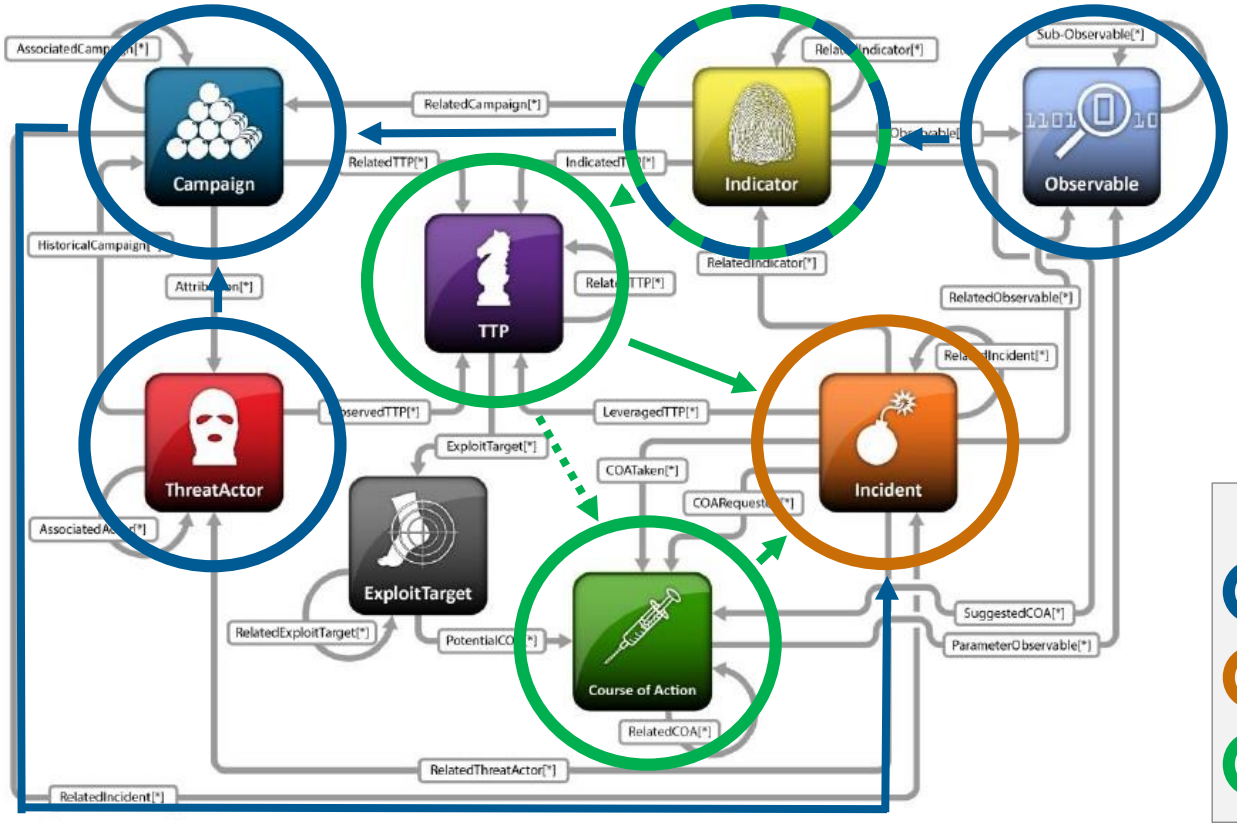


FACT “As Is” Architecture



STIX™ as a Unifying Data Model

CRITS, CyCS, and TARA each support subsets of the STIX™ data model, making STIX™ a unifying influence in the integration of these tools



The STIX™ Data Model
http://stix.mitre.org/

Legend

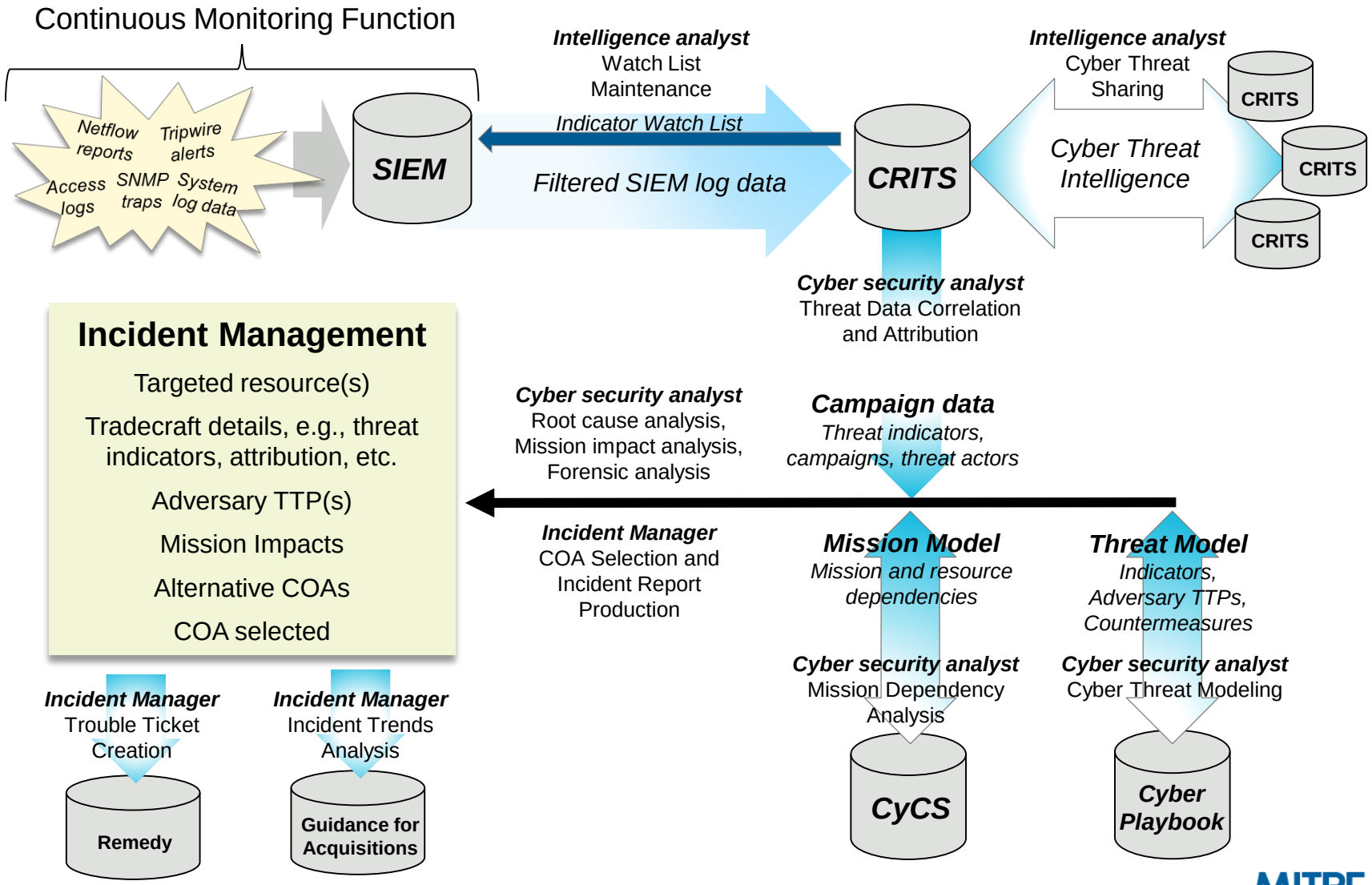
- Maintained, imported, exported in CRITS
- Maintained, exported from CyCS
- Maintained, imported, exported in TARA

MITRE

Benefits

- **Faster operator response to cyber-attack, with better understanding of mission impacts and mitigations**
  - Use of CRITS facilitates correlation of threat indicators with known bad actors and targeted cyber resources.
  - Integration of CRITS with CyCS expands awareness of the potential mission impact(s) resulting from compromise of cyber resources.
  - Use of a playbook promotes systematic analysis of alternative courses of actions (COAs) when responding to cyber threats
- **Long term objective to establish a federated repository of cyber threat intelligence that can be shared within the DoD community**
  - Sharing of cyber threat intelligence with mission partners is prerequisite to development of proactive cyber defensive strategies
  - Use of industry standard data models and exchange formats (STIX™) promotes interoperability with commercial products
- **Acquisition of more resilient systems that implement "tried and true" mitigations for real-world cyber attacks**
  - Mitigation best practices applied operationally can inform acquisition community of potential gaps and areas for improvement

ISAT Use of FACT Tools in Cyber Incident Analysis and Response



MITRE