CYBER OPERATIONS RAPID ASSESSMENT (CORA) QUESTIONNAIRE

Thank you for your interest in this questionnaire. This multiple-choice set of items should require less than two hours to complete. The interview team will reserve 1.5 hours with you to review your responses and allow time for questions, discussion, and elaboration on your responses.

ORGANIZATIONAL CONTEXT

1. What is your industry sector?

(Check all that apply)

☐ Biotech/pharmaceutical
☐ Defense industry
☐ Government
☐ Financial services
☐ Technology
☐ University
☐ Transportation
☐ Manufacturing
☐ Utilities
☐ Healthcare
☐ Energy production
☐ Other: _______________________
☐ Retail
☐ Legal

2. Approximately how many employees are in the organization?

Number of employees: _______________________

3. Which best describes the cyber security team's geographical distribution?

Geographically distributed: Yes or No

Multinational: Yes or No

4. The organization has policies for flexible work practices in terms of:

(Check all that apply)

☐ Working remotely ☐ Using bring-your-own-devices (BYOD) ☐ Neither

5. How long has your organization been dedicating resources to cyber security?

☐ Within the last year ☐ 1-3 years ☐ 3-5 years ☐ More than 5 years

6. Please indicate whether your organization employs full-time cyber security staff.

☐ N/A
☐ 1-5 full time staff
☐ 5-20 full time staff
☐ Other: _______________________

7. Which of the following groups are considered to pose significant potential threats to your organization?

(Check all that apply)

☐ Criminal organizations
☐ Hacktivist groups
☐ Employee error (unintentional)
☐ Insider threats (intentional)
☐ Nation state sponsored groups
☐ Terrorist groups
☐ Accident/natural disaster
☐ Other: _______________________

8. What are your primary cyber impact concerns?

(Check all that apply)

☐ Mission disruption/Denial of service
☐ Operational data integrity
☐ Financial loss
☐ Reputation loss
☐ Personally identifiable information loss
☐ Availability (communications, command and control)
☐ Intellectual property loss (designs, patents, formulas, research, etc.)
☐ Other: _______________________

9. Our systems or networks are at significant risk for cyber attack.

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

10. Which of the following are important third party dependencies for your organization?

(Check all that apply)

☐ Software vendors
☐ Hardware/parts suppliers
☐ Outsourced IT services
☐ Other: _______________________
☐ Business partners

11. Our organization has confidence in the cyber security of our third party dependencies.

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

12. Please indicate which external Infrastructure you consider critical to your organization's mission. For those checked, please indicate whether contingency plans are established (such as alternate sources, backup systems or different processes).

(Check all that apply)	*Contingency plan established*
☐ Power grid	Yes or No
☐ Internet	Yes or No
☐ Telecommunications/phone	Yes or No
☐ Financial networks	Yes or No
☐ Transportation	Yes or No
☐ Water	Yes or No
☐ Other: ______________________	Yes or No

THREAT AWARENESS & TRAINING

1. Our organization's senior management consistently emphasizes the importance of cyber security.

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

2. Senior management understands the current cyber threat environment

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

3. Which best describes the nature of training for existing cyber security analyst roles?

☐ Training is essentially non-existent
☐ Training occurs sporadically and content is variable
☐ Training is well-defined, focusing on tool usage
☐ Training is well-defined, focusing on tool usage *and* good analytic process

4. Which best describes the nature of cross-training between functions (such as incident response, threat intel, malware analysis, or tool development)?

☐ There is no cross-training between functions
☐ Cross-training occurs for some functions
☐ There is significant cross-training involving most or all of these functions

5. Most users are sophisticated about detecting spear phishing and other kinds of intrusion attempts.

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

6. How often does the organization provide any user security awareness training?

(Check all that apply)

☐ Training is never provided
☐ Training is only provided in response to a specific threat
☐ Training is *offered* at least annually
☐ Training is *required* at least annually
☐ Training is *continuous* and *ongoing* (bulletins, advisories, posters, emails, etc.)

7. How often do you receive actionable tips from users?

☐ Never ☐ Rarely ☐ Sometimes ☐ Frequently

8. Which best describes the organization’s policies regarding user behaviors on the network?

☐ There are no policies
☐ The organization has a few rules regarding particularly extreme behaviors
☐ The organization has many rules that describe acceptable network behaviors
☐ There is mandatory user security training to reinforce policies

9. What controls are in place regarding what users may do or not do?

(Check all that apply)

☐ Laptop encryption
☐ 2 factor authentication
☐ DLP (data loss prevention)/exfiltration control
☐ Forced VPN
☐ Other: ______________________

10. How often does cyber security share current threat information with users?

☐ Never ☐ Rarely ☐ Sometimes ☐ Frequently

TOOLS & DATA COLLECTION

1. What types of cyber security tools and sensors are currently being used?

(Check all that apply)

☐ Asset management
☐ Anti-virus software
☐ Email spam filter
☐ Honeypot
☐ Web content filter/proxy
☐ Host forensics
☐ Network firewall
☐ Malware sandbox
☐ Netflow tool
☐ Malware indicator scanning tool
☐ SIEM or central log aggregator
☐ Network intrusion detection/protection system
☐ Exploit prevention tools (e.g. Microsoft’s EMET)
☐ Other: ______________________

2. In terms of asset management, which assets are tracked (in a spreadsheet, database, etc.)?

(Check all that apply)

☐ We have limited IT asset tracking
☐ Mobile devices (cell phones, USB drives, etc.)
☐ Common infrastructure assets (such as servers, network devices, etc.)
☐ End-user assets (desktops, laptops, etc.)
☐ Mission assets (specialized and/or standalone systems)

3. We have clear guidance in place for log data capture and access (e.g., what is to be collected, for how long, by whom, and how accessed).

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

4. For each of the types of logs below, please indicate who **owns/maintains** the data (cyber security, IT, business unit, vendor), the **accessibility** of the data, and the **searchability** of the data.

	What office owns/maintains? (N/A if not maintained)	*Accessibility (time/effort to obtain logs)*	*Searchability (time/effort to find info in logs)*
Mail logs		easy/moderate/difficult	easy/moderate/difficult
Proxy logs		easy/moderate/difficult	easy/moderate/difficult
Firewall logs		easy/moderate/difficult	easy/moderate/difficult
DNS logs		easy/moderate/difficult	easy/moderate/difficult
Netflow records		easy/moderate/difficult	easy/moderate/difficult
Anti-virus (AV) detection logs		easy/moderate/difficult	easy/moderate/difficult
Network access logs		easy/moderate/difficult	easy/moderate/difficult
Packet capture		easy/moderate/difficult	easy/moderate/difficult
Application and server logs		easy/moderate/difficult	easy/moderate/difficult
Other: ____________		easy/moderate/difficult	easy/moderate/difficult

5. For logs that are more difficult to access, what are the primary challenges?

(Check all that apply)

☐ Outsourced, not provided by vendor
☐ Logs not kept long enough
☐ Logs not well organized or indexed
☐ Must fill out request form and wait
☐ Logs inconsistent
☐ Must rely on informal social network
☐ Must log into separate server to view
☐ Other: ______________________
☐ Others don't recognize the important role of logs, so they are not reliably kept

6. Does the cyber security team have access to Help Desk tickets to review for potential indicators?

☐ There is no reliable access
☐ They have access to help desk tickets - but no regular process for review and escalation
☐ They have access to help desk tickets - and a process for review and escalation

7. What mechanisms exist for users to submit tips on potentially suspicious emails or other suspicious events?

☐ There is no mechanism
☐ Users have developed their own mechanisms
☐ There is a standard mechanism (e.g., a dedicated mailbox), but no process for review and escalation
☐ There is a standard mechanism (e.g., a dedicated mailbox), and a process for review and escalation

INTERNAL PROCESS & COLLABORATION

1. Does the organization have someone responsible for information security, such as a CISO (Chief Information Security Officer)?

Yes or No

2. Does the organization have a CONOPS (concept of operations) for cyber security operations?

Yes or No

3. There is regular communication between the cyber security team and the following groups:

(Check all that apply)

☐ Senior management
☐ Business/ mission unit
☐ IT infrastructure
☐ Users
☐ Corporate security

4. How often does a member of the cyber security team (whether CISO or other) brief the organization's senior management?

(Check all that apply)

☐ Weekly
☐ Monthly
☐ Quarterly
☐ When a threat or incident affects operations
☐ Other: ______________________

5. Is the cyber security team consulted when departments are planning to acquire or deploy new tools and systems?

☐ There is virtually no coordination with cyber security regarding new tools/systems
☐ There is ***occasionally*** coordination with cyber security regarding new tools/systems
☐ There is ***usually*** coordination with cyber security regarding new tools/systems
☐ Other: _________________________

6. Who performs each of the following functions for your organization?

	We don't have this function	*Function is outsourced*	*In-house cyber security team*	*In-house IT team*
Patch and configuration management	☐	☐	☐	☐
Incident response	☐	☐	☐	☐
Tune/customize tools (e.g., firewall, IDS)	☐	☐	☐	☐
Malware analysis	☐	☐	☐	☐
Cyber threat intel	☐	☐	☐	☐

7. For existing functions, please indicate the level of communication and cooperation between each pair. "Low" means the functions are stovepiped (they do not interact); "Medium" means there is ad hoc (occasional, as needed) communication; "High" means the functions are well integrated.

a. Overall cyber security team and IT infrastructure groups

☐ N/A ☐ Low (stovepiped) ☐ Medium (ad hoc) ☐ High (integrated)

b. Incident response and tools tuning/customization

☐ N/A ☐ Low (stovepiped) ☐ Medium (ad hoc) ☐ High (integrated)

c. Malware analysis and tools/tuning customization

☐ N/A ☐ Low (stovepiped) ☐ Medium (ad hoc) ☐ High (integrated)

d. Malware analysis and cyber threat intelligence

☐ N/A ☐ Low (stovepiped) ☐ Medium (ad hoc) ☐ High (integrated)

e. Cyber threat intelligence and tools tuning/customization

☐ N/A ☐ Low (stovepiped) ☐ Medium (ad hoc) ☐ High (integrated)

8. How easy is it to take each of the following courses of action in response to threats/incidents?

	N/A or unknown	*Very difficult*	*Somewhat difficult*	*Neutral (not easy or difficult)*	*Somewhat easy*	*Very easy*
Engage with ISP (as in DOS attack)	☐	☐	☐	☐	☐	☐
Analyze malware	☐	☐	☐	☐	☐	☐
Engage with law enforcement	☐	☐	☐	☐	☐	☐
Redirect incoming emails (without deleting)	☐	☐	☐	☐	☐	☐
Delete emails	☐	☐	☐	☐	☐	☐
Update signatures via IDS/IPS	☐	☐	☐	☐	☐	☐
Block traffic via firewall	☐	☐	☐	☐	☐	☐
Revise automated user policies (such as removable media controls)	☐	☐	☐	☐	☐	☐
Blackhole or sinkhole domains via DNS	☐	☐	☐	☐	☐	☐
Examine a specific device or system (without wiping it)	☐	☐	☐	☐	☐	☐
Remotely wipe a specific device or system (such as a mobile device)	☐	☐	☐	☐	☐	☐
Push emergency patch or configuration	☐	☐	☐	☐	☐	☐

9. How rapidly can the cyber security group alert the organization (including users) to a significant threat?

□ Less than an hour □ 1 – 4 hours □ Within 24 hours □ Longer than 24 hours

10. Our organization has a clear, well-established procedure for escalating suspicious events.

□ Unsure □ Strongly disagree □ Disagree □ Neither agree nor disagree □ Agree □ Strongly agree

11. The organization conducts cyber exercises to practice coordinated response among cyber defenders, IT infrastructure owners, and business unit or mission system owners.

□ Unsure □ Strongly disagree □ Disagree □ Neither agree nor disagree □ Agree □ Strongly agree

TRACKING & ANALYTICS

1. Which best describes how your organization tracks cyber threat indicators?

□ Not tracked □ In a watchlist or spreadsheet □ In a database □ Other: ____________________

2. If any indicators are tracked, what types of indicators?

(Check all that apply)

□ IPs
□ URLs
□ Domains
□ File hashes
□ Email addresses
□ Email headers
□ Other: _______________________

3. If indicators are tracked, what contextual detail is collected?

(Check all that apply)

□ Attribution
□ Date added
□ Description (why bad)
□ Role in kill chain/attack lifecycle
□ Valid time window
□ Related incidents
□ Indicator type
□ Confidence level
□ Source(s)
□ Actions taken
□ Related campaigns
□ Other: _______________________

4. How does your organization check for known threat indicators?

(Check all that apply)

□ N/A □ Near real time sensor alerts □ Scheduled queries of new logs
□ Historical log search □ Ad hoc/manual queries □ Other: _______________________

5. Which best describes your organization's tracking of cyber attacks/incidents?

□ There is none
□ There is manual tracking of attacks/incidents, not easily accessible to all analysts
□ We track attacks/incidents routinely with some tools (wiki, spreadsheet)
□ We have a dedicated security attack/incident tracking system that is accessible to all analysts

6. Does the organization collect attack/incident data on the following?

(Check all that apply)

□ Number of incidents
□ Detection method
□ Affected assets
□ How attack was stopped, if prevented
□ Whether vulnerability patched or not
□ Impact of incident, if not prevented
□ Whether user(s) clicked on link or attachment
□ Attributed threat actor(s)
□ Other: _____________________

7. Which of the following types of analytics are performed?

(Check all that apply)

□ Historical analyses
□ Attribution
□ Dynamic analysis/sandboxing
□ Network traffic analysis
□ Reverse engineering of binaries
□ Memory forensics
□ Data mining for new signs of attack (proactive)
□ Trending (on activity, timing, adversary groups)

8. Which best describes your knowledge management of cyber security expertise?

☐ Expertise is shared verbally but not usually documented

☐ Expertise is informally documented (for example, events or lessons learned are shared via emails, instant messages)

☐ Some expertise and judgments are documented (for example, event or shift logs), but usually with little explanation

☐ Analyst expertise and judgments are well-documented and accessible to other analysts

9. Our organization regularly tunes our sensors (e.g., by removing noisy indicators).

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

10. Our organization regularly writes custom signatures/indicators.

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

11. Our organization regularly develops its own (non-vendor) techniques to detect cyber threat activity.

☐ Unsure ☐ Strongly disagree ☐ Disagree ☐ Neither agree nor disagree ☐ Agree ☐ Strongly agree

12. What other threat information does your organization routinely retain?

(Check all that apply)

☐ Malware samples and analyses ☐ Intel notes, analyses and reports

☐ Threat actor or campaign tactics, techniques and procedures ☐ Other: ______________________

EXTERNAL ENGAGEMENT

1. Other than patching publicized vulnerabilities, how does your organization learn about potential threats?

(Check all that are used regularly)

☐ Help desk tickets

☐ Vendor reports

☐ Open source reports

☐ Government and law enforcement tips

☐ Tips from users (suspicious email or activity)

☐ Threat sharing peers' tips

☐ Other: ______________________

2. Does your organization belong to any threat sharing groups such as an ISAO (information sharing and analysis organization)?

(Check all that apply)

☐ No

☐ Industry based group

☐ Regionally based group

☐ Other: ______________________

The following questions pertain to participation in any ISAO (Information Sharing and Analysis Organization), such as a regional or industry based threat sharing group.

3. What are your organization's reasons for participating in ISAO threat sharing?

(Check all that apply)

☐ Build our reputation

☐ Learn best practices

☐ Build relationships

☐ Protect our customers

☐ Training

☐ Improve our cyber security capabilities/posture

☐ Share and pool resources (feeds, samples, analyses, etc.)

☐ Learn about advanced adversary tactics, techniques, procedures

☐ Broaden cyber security situational awareness

☐ Other: ______________________

4. What kinds of information are *__currently__* shared within the ISAO group? What do you *__wish__* were shared?

	Currently shared	*Would like to be shared*
Indicators	□	□
Incidents	□	□
Vulnerabilities	□	□
Threat analysis	□	□
Consolidated threat intel feeds	□	□
Defensive measures/courses of action	□	□
Malware samples	□	□
Log files	□	□
Lessons learned and best practices	□	□
Reviews of product vendors	□	□
Points of contact	□	□
Other: ______________________	□	□

5. Please indicate the mechanism(s) used for ISAO sharing.

(Check all that apply)

□ Telecom or VTC
□ Forum or chat room
□ Email distribution list
□ Private communications
□ Automated feeds (e.g., STIX and TAXII)
□ Face to face meetings
□ Shared repository (for indicators, samples, etc.)
□ Other: ______________________
□ Wiki
□ Portal

6. Please describe what your organization does with shared information.

(Check all that apply)

□ Manually ingest indicators
□ Automatically ingest indicators
□ Scan once for new indicators
□ Improve training
□ Perform analyses
□ Write reports
□ Brief management
□ Create signature/indicator for ongoing scan
□ Other: _________________

7. Information from ISAO members is *actionable* for our organization's threat detection and defense operations.

□ Unsure □ Strongly disagree □ Disagree □ Neither agree nor disagree □ Agree □ Strongly agree

8. Our organization is comfortable sharing information with ISAO members.

□ Unsure □ Strongly disagree □ Disagree □ Neither agree nor disagree □ Agree □ Strongly agree

9. Which of the options below best describes your organization's role in the ISAO?

□ Member: We receive peer-reported threat information for our situational awareness
□ Checker: We scan our networks for peer-reported threats, but don't report findings
□ Reporter: We scan our networks for peer-reported threats, and report back our findings
□ Contributor: We scan for peer reported threats and also contribute new indicators
□ Mentor: We are a primary contributor of trusted threat information

10. Is there anything limiting what threat information you share with the ISAO?

(Check all that apply)

□ Threat sharing mechanisms are not easy to use
□ Lack of effective sharing agreements
□ Legal issues
□ Internal vetting process/approvals
□ Lack of confidence in our information's value/relevance
□ Level of trust
□ Manpower/resource constraints
□ Competition
□ Concerns about reputation
□ Other: ______________________