Cyber Operations Rapid Assessment (CORA)

POCs: Dr. Lindsley Boiney and Dr. Clem Skorupka

MITRE

Purpose of CORA Assessment

- Guide organizations through structured review of a broad range of issues necessary to support threat-based operations
- Rapidly assess existing cybersecurity capabilities
- Raise awareness, focus attention and resources to improve cyber operations
- Provide timely, unbiased, actionable guidance to share with senior management

MITRE

CORA Methodology - Characteristics

- Lightweight (2 hours survey, 2 hours interview)
- Holistic approach (people, processes, technology)
- Unbiased feedback (tool- and technology-agnostic)
- Applicable to organizations across a broad spectrum of sizes, sectors, and capabilities
- Actionable guidance

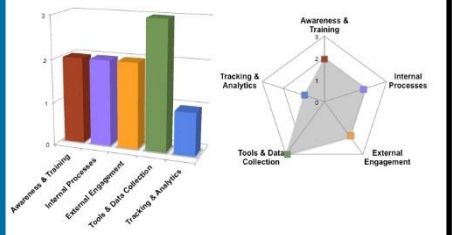
Setting Expectations

- **What the CORA methodology DOES NOT do**
  - Impose requirements or mandate responses
  - Address regulatory and compliance issues (e.g., FISMA, PCI DSS, SOX)
  - Require access to organizational logs/systems (no vulnerability assessment or pen testing)
  - Reveal sensitive data to others
  - Recommend vendor-specific tools/sensors/services
  - Perform an architectural assessment
  - Provide detailed technical guidance

CORA Focus Areas

Example Report

Organizational Capabilities



10 MITRE

Identified Strengths

- Rapid advances in cyber security tools and processes over past 2 years
- Strong support and awareness from leadership; emphasis on sophisticated threats
- High maturity on sensors and tools in place; large volume of data
- Clear, well-established procedure for escalating suspicious events
- Relevant Help Desk tickets effectively shared with SOC; SOC has complete access and full visibility
- Dedicated mailbox for users to submit tips on suspicious emails/events
- Dedicated security incident tracking system accessible to all analysts

11 MITRE

Opportunities For Improvement

- Not currently prepared to address insider threats
- Limited ability to tune sensors or customize signatures that are managed by parent organization
- Limited access to email logs (outsourced)
- Not currently able to redirect suspicious incoming emails
- Few high-value email tips received from users (mainly help desk related)
- Disparity among analyst training (some rely on out-of-the-box settings)
- Limited ability to sinkhole malicious domains via DNS
- Would benefit from DLP technologies
- Many tools, yet some not effectively used when staff expertise unavailable
- Cyber exercises include SOCs but not IT and business units
- External engagement limited by lack of staffing, documented sharing agreements, a shared repository, and standardized mechanisms

1 MITRE

THREAT AWARENESS & TRAINING

- Reduce disparity among analyst skill sets with increased and more consistent training on both tool usage and good analytic processes
- Implement user training on how/when to report suspicious targeted email attacks
- Develop capabilities to address potential insider threats
- Continue maturing cyber threat intelligence capability

EXTERNAL ENGAGEMENT

- Strive to advance from "Checker" to "Reporter": audit and report back
  - Capture indicators, including email indicators, in a more structured repository (see under Tracking & Analytics)
  - Develop clear guidelines or SOPs on what can/can't be shared with peer groups to minimize time-consuming one-by-one vetting
  - Share tips on *what to do with indicators* along with the indicators themselves
- Bolster external engagement via
  - A shared repository
  - Documented sharing agreements
  - Additional staffing (especially in cyber threat intel)
- Share lessons learned and best practices with other peer organizations
- Introduce automated mechanisms to collect and share based on standards

TOOLS & DATA COLLECTION

- Large volumes of relevant data; focus on detecting targeted APT attacks
  - Analyze quarantined AV malware samples
  - Redirect suspicious emails to designated mailbox for analysis
- Address accessibility and searchability challenges for high volume logs
  - Streamline and consolidate logs with emphasis on ability to detect targeted APT intrusion attempts (outbound traffic, mail AV logs)
- Perform risk assessment regarding BYOD usage
  - Consider tiered system of access and privileges

TRACKING & ANALYTICS

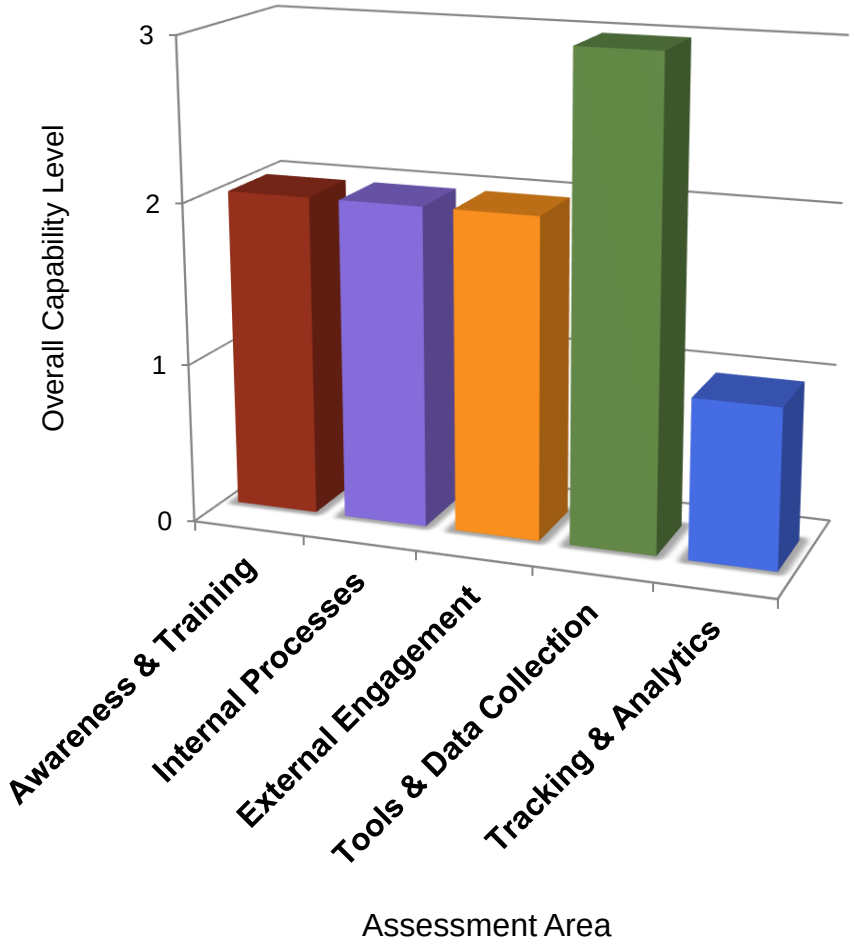
- Upgrade indicator tracking from docs/memos to spreadsheet or database
  - Begin proactively scanning for indicators, such as email indicators
  - Begin tracking all source(s) of indicators
- Upgrade incident documentation to searchable incident tracking system
  - Record relevant incident metadata in a structured format to support metrics and trending analysis
    - E.g., indicators, threat actor, targeted users, vulnerabilities, user actions (such as whether user clicked on link/attachment), detection method, how attack was stopped

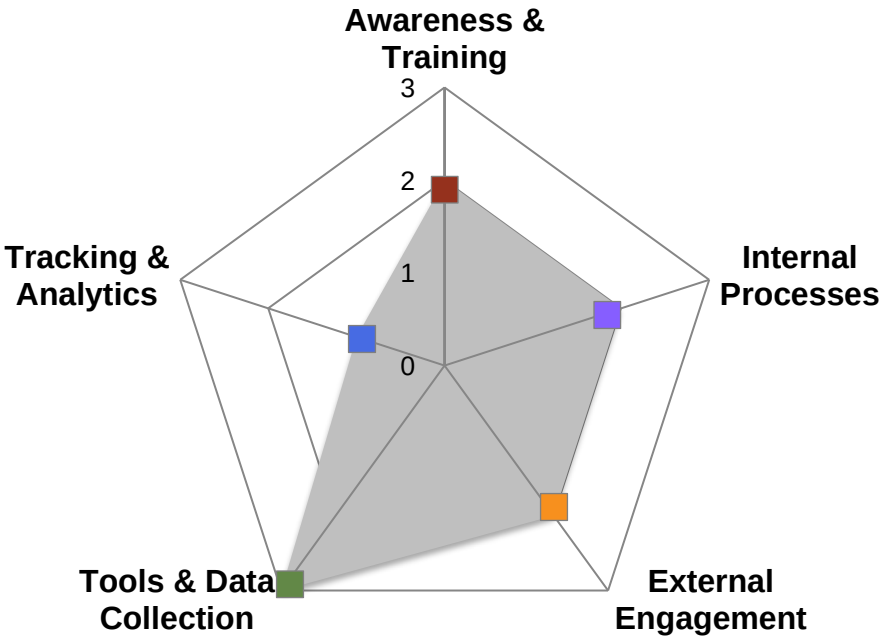
INTERNAL PROCESS & COLLABORATION

- Strongly consider in-house cyber threat intel role
  - Key to proactive detection and prevention of cyber attacks
  - Closely integrate malware and intel analysis activities (synergistic)
- Improve integration between SOC and IT groups
  - Include SOC in acquisition planning and decisions about new security tools
  - Run exercises requiring SOC and IT communication and coordination (including accessing and searching existing logs) to clarify silos, gaps, or pain points

MITRE

Notional Example: Organization X's Overall Capabilities





MITRE

Notional Example for Organization X: INTERNAL PROCESS & COLLABORATION

- **Strongly consider in-house cyber threat intelligence role**
  - Key to proactive detection and prevention of cyber attacks
  - Closely integrate malware and intel analysis activities (synergistic)

- **Improve integration between SOC and IT groups**
  - Include SOC in acquisition planning and decisions about new security tools
  - Run exercises requiring SOC and IT communication and coordination (including accessing and searching existing logs) to clarify silos, gaps, or pain points

Notional Example for Organization X: TRACKING & ANALYTICS

- **Upgrade indicator tracking from docs/memos to spreadsheet or database**
  - Begin proactively scanning for indicators, such as email indicators
  - Begin tracking all source(s) of indicators

- **Upgrade incident tracking to a searchable incident tracking system**
  - Record relevant incident metadata in a structured format to support metrics and trending analysis
    - E.g., indicators, threat actor, targeted users, vulnerabilities, user actions (such as whether user clicked on link/attachment), detection method, how attack was stopped

Notional Example for Organization X: TOOLS & DATA COLLECTION

- **Large volumes of relevant data; focus on detecting targeted APT attacks**
  - Analyze quarantined AV malware samples
  - Redirect suspicious emails to designated mailbox for analysis
- **Address accessibility and searchability challenges for high volume logs**
  - Streamline and consolidate logs with emphasis on ability to detect targeted APT intrusion attempts (outbound traffic, mail AV logs)
- **Perform risk assessment regarding BYOD usage**
  - Consider tiered system of access and privileges

Notional Example for Organization X: THREAT AWARENESS & TRAINING

- **Reduce disparity among analyst skill sets**
  - increased and more consistent training on both tool usage and good analytic processes
- **Implement user training on how/when to report suspicious targeted email attacks**
- **Develop capabilities to address potential insider threats**
- **Continue maturing cyber threat intelligence capability**

Notional Example for Organization X: EXTERNAL ENGAGEMENT

- **Strive to advance from "Checker" to "Reporter": audit and report back**
  - Capture indicators, including email indicators, in a more structured repository
  - Develop clear guidelines or SOPs on what can/can't be shared with peer groups to minimize time-consuming one-by-one vetting
  - Share tips on *what to do with indicators* along with the indicators themselves
- **Bolster external engagement via**
  - A shared repository
  - Documented sharing agreements
  - Additional staffing (especially in cyber threat intelligence)
- **Share lessons learned and best practices with other peer organizations**
- **Introduce automated mechanisms to collect and share based on standards**

Examples of Identified Strengths

- Clear, well-established procedure for escalating suspicious events
- SOC integrated with IT infrastructure
- Dedicated mailbox for user tips on suspicious emails/events
- Continuous and ongoing training for user security awareness
- High maturity on sensors and tools; collecting relevant data
- Regularly tune sensors (e.g., to reduce false positives)
- Cross-training: analysts sit together and all do some monitoring and triage
- Indicators tracked within repository that supports analytics
- Dedicated security incident tracking system accessible to all analysts
- Strong support and awareness from leadership; emphasis on sophisticated threats

Examples of Identified Opportunities For Improvement

- Not currently prepared to address insider threats
- External engagement limited by lack of: staffing, documented sharing agreements, a shared repository, standardized mechanisms
- Many tools, yet some not effectively used when staff expertise unavailable
- Limited ability to tune sensors or customize signatures that are managed by parent organization
- Limited access to email logs (outsourced)
- Not currently able to redirect suspicious incoming emails
- Limited ability to sinkhole malicious domains via DNS
- Cyber exercises include SOC but not IT and business units
- Few high-value email tips received from users (mainly help desk related)
- Disparity among analyst training (some rely on out-of-the-box settings)

Examples of Identified Recommendations

- Gain access to perimeter email logs
- Address accessibility and searchability challenges for logs
  - emphasis on detecting targeted attempts (outbound traffic, mail AV logs)
- Upgrade indicator tracking from docs/memos to database
  - Email indicators: “redirect” suspicious incoming emails to analyst mailbox
- Use signatures from peers to proactively scan for APT indicators
- Consider in-house cyber threat intel role
- Strengthen integration between IT and cyber security groups via exercises, liaison roles, tech exchanges, joint planning decisions
- Strengthen controls on network usage (2 factor authentication, forced VPN)
- Perform risk assessment regarding BYOD usage
- Strengthen user awareness training: threat bulletins, *real* examples, what to do before you click, contests…*ongoing* campaign
- Consider sharing logs, samples (indicators aren’t the only valuable data)