Cyber Operations Rapid Assessment (CORA)

A Guide to Best Practices for Threat-Informed Cyber Security Operations

Dr. Clem Skorupka
Dr. Lindsley Boiney

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

Department No.: J83D
Project No.: 25MSR615-BB

Document No: 15-2971
Bedford, MA

MITRE

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introduction

Actionable threat intelligence plays a critical role in cyber defense, from helping to protect systems and data, to protecting organizations, industries, and even countries. A number of recent highly-publicized breaches has led to considerable activity in both the public and private sector to enhance capabilities to collect, utilize, and share cyber threat information [1], [2]. Many organizations, however, struggle with introducing threat intelligence into their defenses, relying predominantly on static defensive measures and compliance-oriented processes. Transitioning to a threat-informed posture is not easy, and change needs to occur across the triad of people, processes and technologies.

In a previous paper [3] we introduced the CORA (Cyber Operations Rapid Assessment) methodology, which was developed to study issues and best practices in cyber information sharing. In addition, it serves as an engagement tool for assessing and improving threat-informed security defenses. CORA identifies five major areas of cyber security where the proper introduction of threat information can have tremendous impact on the efficacy of defenses:

- External Engagement
- Tools and Data Collection
- Tracking and Analysis
- Internal Processes
- Threat Awareness and Training

This paper captures the underlying assumptions of the CORA methodology by describing what a robust, threat-informed cyber security program looks like. We identify a selection of key practices in each of the above five areas. We defined a “Threat-Informed Cyber Security Operation” (TICSO), as one that successfully incorporates threat information into its regular security practices, and thereby enhances both its tactical and strategic defensive capabilities.

Given the vast literature for cyber security recommendations and guidance, an additional goal of this paper is to provide references to resources and further guidance to assist organizations in achieving their goal of a threat-informed defensive posture.

Organizational Context

Organizations vary widely in terms of size, mission, industry, threat profile, and the relative maturity of their cyber defensive operations. These differences lead to distinct challenges in terms of leveraging, sharing, or generating new threat intelligence.

Newer cyber defensive operations can experience a range of “growing pains,” such as lack of experienced staff, incomplete sensor coverage, or inefficient communication channels between cyber defenders and IT infrastructure or business units. Geographically dispersed and international operations present unique challenges such as distributed operations groups that may span time zones and languages, differing standard operating procedures, and NDAs that prevent full information disclosure among analysts.

Cyber defense of any kind takes resources, and many smaller or lesser resourced organizations may not be able to execute every recommendation described in this paper. CORA is designed such that tailored recommendations can be provided to meet the needs of a range of organizations.

External Engagement

Fundamental to a threat-informed defensive posture is external engagement: going beyond the borders of one's organization to collect intelligence about pertinent threats and emerging attack vectors, establishing relationships with regional and industry groups to share best practices, and reporting and sharing information with government, law enforcement, and peers. External engagement supports proactive and responsive tactical defenses, as well as fully threat-informed strategic risk management.

Collection and Prioritized Intelligence Requirements

There is an ever-growing amount of cyber threat information available, with varying degrees of quality. The TICSO collects cyber threat intelligence and information from a variety of sources including open source reporting by researchers and consultants [4], [5] government and law enforcement sources (USCERT, INFRG), fee-for-service threat intel feeds from vendors [6], and industry sector and regional threat sharing communities such as ISACs and ISAOs [7], [8], [9], [10]. The TICSO focuses collection efforts on the most relevant information by defining prioritized intelligence requirements (PIR), and continuously evaluating the quality of intelligence from different sources in terms of relevance, timeliness, and accuracy. Examples of PIRs include

- Threats and threat actors that have attacked your specific organization previously
- Vulnerabilities and exploits that pertain to technology specific to your organization or industry
- Threats and attacks against industry/sector peers or business partners

Relationships and Threat Information Sharing Collaboratives

In order to gain a full and balanced picture of its threat environment and requisite defensive practices, the TICSO relies not only on its own research and commercial vendors, but also engages with industry, sector, and regional peer groups to share in their specific insights and viewpoints. These relationships can be informal (such as participation in a mailing list or public forum) to formal (signed mutual NDAs, or an organization's membership framework agreement). A TICSO in a given industry sector will have joined an ISAC or ISAO at a level commensurate with its size and resources, as well as a regional collaborative, such as the ACSC [8] or the NCX [9].

In any given information exchange community, participation of the members can vary greatly. In cyber-sharing collaboratives, participation is generally governed by two factors: resources and organizational maturity. CORA defines five levels of participation in threat-sharing bodies:

- Member (consuming information for situation awareness purposes)
- Checker (using group-provided indicators to scan its networks and systems)

- Reporter (reporting back results of scans for group-provided indicators)
- Contributor (reporting new indicators about different attacks on its own networks)
- Leader (providing new intelligence and advanced analytics, and mentors less mature organizations)

The TICSO is an active participant in its community, not only consuming information but reporting back at the Checker or Contributor level. The TICSO is resourced appropriately for its size and threat profile, and has matured its processes to overcome the most common obstacles to threat sharing [11]. It has established scanning of threat information and reporting back as part of its standard procedures; it organizes, tracks, and sanitizes its threat information so that there are no ambiguities in handling or undue risk of exposure of sensitive information; resources permitting, it performs advanced analytics and generates new threat intelligence which it shares with its partners.

What to Collect and Share

The TICSO collects and shares a number of different types of cyber security information [12] including

- Threat activity analysis reports for specific attack groups
- Exploit and vulnerability information
- Specific indicators of compromise (IOC) or attack activity such as phishing email addresses, IP addresses and URLs of malicious sites, host-based indicators such as files, registry keys, and process elements associated with attacks
- Samples of malware used in targeted attacks
- Industry best practices, recommended courses of action, and remediation guidance
- Feedback and value of information provided by others

Emerging Standards and Technologies

To deal with the ever-increasing amount of cyber information available, the TICSO automates manual processes where possible. Essential to this is standards-based technology, so the TICSO considers threat sharing and analysis platforms that will leverage emerging standards to allow for rapid response and interoperability [13], [14]. ISACs and other entities looking to improve the timeliness of their intelligence sharing will also look to standards-based technology to automate their processes where possible.

Tools and Data Collection

In order to utilize the threat intelligence it gathers, the TICSO collects pertinent logs and system data in addition to instrumenting a variety of detection, defensive, and analysis tools.

Threat-informed Collection

Common security elements such as firewalls and anti-malware technology are important defensive components, but a threat-informed defense will call for additional measures and information-collecting capabilities to counter the range of sophisticated threats. Defensive cyber efforts, including log analysis, should be driven by the TICSO's unique risk profile, which will dictate the information needed to identify malicious activity from likely attacks.

Adversaries commonly attack enterprises via phishing emails that carry malware or links to malicious websites. Therefore the TICSO will have access to incoming mail logs in order to scan for known-malicious sender addresses, and other details characteristic of attackers.

In terms of intrusion sensors, the TICSO deploys a combination of both network traffic (e.g., IDS, packet capture) and host-inspection (e.g. HIDS / remote forensics) capabilities to allow analysts to look for suspicious activity, such as network connections to command and control sites, or malware traces such as registry keys or file hashes.

Non-standard Sources

DNS, the Domain Name Service, is usually thought of as an IT infrastructure necessity, however it is also a rich source of information for cyber security analysts to detect fast-flux botnet activity [15], malicious domains, and even act as a defense via the technique of DNS sink-holing [16]. The more advanced TICSO will employ these tactics as well as honeypot and malware sandbox tools.

Available, Searchable

The TICSO not only collects the requisite data, but it is organized to be searchable and readily accessible to all cyber defenders. Many organizations employ log aggregator and/or SIEM technology [17]. The TICSO has policy and guidelines to define requirements for logging of security relevant logs across their IT infrastructure [18]. These practices allow analysts to review data from across the enterprise from a single location rather than logging in multiple places, and support rapid and comprehensive analysis.

Enterprise Visibility

Besides security-specific data such as firewalls and IDS, the TICSO has full visibility into its networks and systems, with readily accessible network maps, system/asset data, patch-levels, applications and versions, and role of systems in the organization's mission [19]. This information is used to readily assess which system was involved in a potential attack, and to inform escalation and prioritization processes. This view of the enterprise informs the systematic and comprehensive deployment of defenses.

Human Sensor Grid

Users are an invaluable resource in cyber defense, often able to notice suspicious phishing emails or unusual system behavior when technological defenses have failed. The TICSO provides means for users to report such activity, and also accesses IT trouble tickets for signs of anomalies that might be potential compromises [20].

Tracking and Analytics

In order to properly utilize threat information that has been collected, the TICSO must perform two important functions: tracking of information and analysis.

Tracking of Threat Information

Tracking or cataloging threat information, to include not just the information itself but also metadata such as time of receipt, source, handling restrictions, context, and actions taken, is necessary task for the following reasons:

- Information from government or commercial sources may have handling and sharing restrictions [21].
- Indicators and intelligence from different sources may be of different quality, so tracking of sources allows one to identify the most accurate and relevant information feeds.
- Indicator's appearance in attack lifecycle or "Kill Chain" phase [22] helps determine type and urgency of response.
- Raw data from incidents may be re-analyzed in light of new intelligence
- Multiple sources may provide the same indicators, so de-duplication avoids scanning for the same indicator twice and may lead to broader understanding of the activity.
- Indicators can have a "shelf life" or a certain time frame of validity, e.g. when a malicious IP address gets re-assigned to a non-malicious entity
- Actors, motivations, and their Tactics, Techniques, and Procedures (TTP's) vary, so tracking this information and linking it to associated indicators and alerts provides guidance for best response practices and "Playbooks".

The TICSO has a well-trained team responsible for maintaining a knowledge base of its threat information. While initially a spreadsheet or less structured approach may work, most organizations find it imperative to develop a structured knowledge base that allows an analyst to track all of the above-mentioned attributes as well as perform queries, analytics, and even feed automated checks and defensive actions such as blacklisting. A number of security technology vendors now offer "threat management platforms" and related technologies to support such activities [23].

Analytics

The analysts of the TICSO are well-trained in a variety of disciplines and technologies, and have access to as-needed expertise via outsourcing. They are supported in their efforts via an organized threat knowledge base and ready access to a full range of security logs, alerts, and enterprise system information. The analysis efforts generate both timely tactical information for defenders, as well as threat analysis products to inform defensive planning and risk management.

Intrusion alerts presented to responders are contextually-linked to aid in quick triage and accurate handling.

Analysts have a large toolbox of analysis techniques and utilities to perform actions such as

- Traffic analysis
- Log analysis
- Malware analysis
- Host, disk, and memory analysis and forensics

Local observations and incidents are studied in detail to understand which defenses were most effective, and to identify patterns and commonalities that are indicative of targeted attacks. Malware analysts maintain a repository of samples used in attacks against the organization. Attacks are reviewed for historical trends, to identify attacker groups and techniques, and to better develop detection and other defenses.

Analysts define consistent processes for all efforts to ensure systematic and thorough review of intelligence, alerts, and incident observations. For incidents with the potential for high impact, particular emphasis is given to root-cause analysis as opposed to a more traditional “wipe system and move on” approach [24].

DevOps, where programmers and developers work closely together with analysts and defenders to rapidly turn out tailored detection and defense capabilities, is a very effective approach to defending against sophisticated attackers that can regularly bypass generic protections [25].

Larger and well-resourced organizations can pursue longer term questions such as the “who” and the “why” relevant to activity they are investigating. In addition, these types of organizations can perform more advanced analytics such as statistical analysis and anomaly detection, machine learning, and may even employ deception techniques such as honeypots / honeynets [26].

Internal Processes and Collaboration

The TICSO, having collected a broad range of threat information, utilizes this information to the fullest extent by establishing clear, efficient processes to communicate information and effect changes in defenses across the enterprise.

Leadership Support

Leadership support is essential to the overall effectiveness of the TICSO. When presented with clear information about the threat environment mapped to the potential impacts and risks to the organization, decision makers can manage those risks by providing sufficient resources for defense, and communicating the priority of cyber defense to all stakeholders [27], [28], [29].

The TICSO provides clear and timely situation reports about high-impact threats and incidents, as well as regular threat analyses that can inform planning, risk management and investments in defenses.

Concept of Operations (CONOPS) and Communications

The TICSO has a Concept of Operations (CONOPS) document that captures its mission, scope and structure. The CONOPS is approved by appropriate authorities in the organization, and describes what the cyber security operation does, how it is staffed, what its responsibilities are, and what groups and entities it regularly interacts with within and outside the enterprise. The CONOPs allows other groups to understand the purpose and function of the cyber security team, and better define processes and points of interaction.

IT Planning and Acquisition

IT planning and acquisition processes are fully informed of the threat environment. Requirements for security are defined in a timely fashion so as to allow for appropriate defenses to be implemented.

Courses of Action and Process

The TICSO is able to quickly act on new threat information, through efficient processes that allow for ready changes and updates to common defenses. In the TICSO:

- Incidents are triaged and escalated according to clear criteria about the potential threat and impact to the organization.
- Vulnerability and patch management processes are prioritized according to threat and impact, and critical patches and workarounds can be deployed according to pre-set criteria such as targeted attacks and Zero-Day exploits.
- Firewalls rules and sensor signatures can be rapidly deployed.
- Malware analysis supports rapid turn-around indicator reporting to defenders as well as more detailed, “deep-dive” analysis

Exercises

The TICSO conducts regular exercises with various IT and business units to maintain readiness for high-impact scenarios and to identify gaps in existing processes and procedures. These exercises also help to communicate in the potential impact of different threats in a tangible way [30], [31].

Threat Awareness and Training

Threats come from a range of actors, from “hacktivists” and criminal organizations to insiders and nation states. Attacks can lead to financial loss, operational failure, loss of reputation, theft of intellectual property, and breach of PII or PHI. The likelihood and consequent risk of each of these scenarios will depend on the nature of the organization, the activity of the different threat actors, and the security controls the organization has in place.

The TICSO has a thorough understanding of its relevant cyber threats, impacts, and risks, and this understanding is propagated throughout the enterprise via clear and consistent communications and training to employees, business units, IT groups, and leadership.

Employee Training: Human Sensor Grid

Training is employed to inform the user population of the types of threats and potential impacts their organization is subject to and what security policies and technical controls are in place. Employees are given specific guidance as to what practices help to minimize risk and how to identify and report suspicious activity. User training that is informed by current threat intelligence, in conjunction with clear efficient reporting mechanisms, establishes a “Human Sensor Grid” that complements technological defenses. The TICSO provides training regularly, with continuous updates as new threats emerge.

Enterprise Awareness

Business units, IT groups, and technical operations groups (e.g. SCADA, ICS, PLC) are provided specialized threat intelligence reports and defensive guidance tailored to their needs.

Defender Training and Readiness

The TICSO's cyber defenders are aware of the overall mission of their enterprise, and interact with different business groups to better understand their missions and technical practices. They engage in training [32] and cross-training to enhance the depth and breadth of their skills and knowledge. Analysts' techniques, knowledge, and judgements are captured and shared to assure continuity and consistency as well as aid in training new defenders.

References

[1] The White House, "Executive Order - Promoting Private Sector Cybersecurity Information Sharing," 13 February 2015. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari [Accessed 21 January 2021].

[2] C. Johnson, L. Badger, D. Waltermire, J. Snyder, C Skorupka, "NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing," U.S. Department of Commerce, 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-150/final. [Accessed 11 September 2015].

[3] C. Skorupka, J. Connelly and A. Summers, "Cyber Operations Rapid Assessment (CORA): Examining the State of Cybersecurity Assessment Methodologies and Introducing a New Alternative," The MITRE Corporation, 2015.

[4] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," 19 February 2013. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [Accessed 21 January 2021].

[5] Crowdstrike, "Global Threat Intel Report," 6 February 2015. [Online]. Available: http://www.crowdstrike.com/global-threat-report-2014/. [Accessed 21 January 2021].

[6] R. McMillian and P. Khushby, "Market Guide for Security Threat Intelligence Services," Gartner, 14 October 2014. [Online]. Available: https://www.gartner.com/doc/2874317/market-guide-security-threat-intelligence. [Accessed 11 September 2015].

[7] National Council of ISACs, "Member ISACs," ISAC Council, [Online]. Available: http:// https://www.nationalisacs.org/member-isacs. [Accessed 21 January 2021].

[8] Advanced Cyber Security Center, "Advanced Cyber Security Center Homepage," [Online]. Available: http://www.acscenter.org/. [Accessed 11 September 2015].

[9] National Cyber Exchange (formerly Western Cyber Exchange), "Changing the Equation," [Online]. Available: http://www.wcyberx.org/. [Accessed 21 January 2021].

[10] Health Information Trust Alliance, "Health Information Trust Alliance Homepage," [Online]. Available: https://hitrustalliance.net/. [Accessed 11 September 2015].

[11] K. Peretti, "Cyber Threat Intelligence: To Share or Not to Share - What are the Real Concerns?," Bloomberg BNA, 1 September 2014. [Online]. Available: http://www.alston.com/Files/Publication/09a5e602-0f0c-4635-b5eb-685811791486/Presentation/PublicationAttachment/629e5e52-4200-422a-a3e1-6fa39e6b2ff5/Bloomberg%20BNA_KPeretti_LDennig_Cyber%20Threat%20Intel%208%2029%2014.pdf. [Accessed 11 September 2015].

[12] C. Johnson, L. Badger and D. Waltermire, "NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing Section 4.1.2," U.S. Department of Commerce, 2015. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf. [Accessed 11 September 2015].

[13] Oasis Open, "Introduction to STiX," [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro /. [Accessed 21 January 2021].

[14] The MITRE Corporation, "Collaborative Research Into Threats (CRITs)," [Online]. Available: http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/collaborative-research-into-threats-crits. [Accessed 11 September 2015].

[15] ICANN Security and Stability Advisory Committee, "SAC 025: SSAC Advisory on Fast Flux Hosting and DNS," 2008. [Online]. Available: https://www.icann.org/en/system/files/files/sac-025-en.pdf. [Accessed 11 September 2015].

[16] Infosec Institute, "Understanding DNS Sinkholes - A Weapon Against Malware," 26 June 2014. [Online]. Available: http://resources.infosecinstitute.com/dns-sinkhole/. [Accessed 11 September 2015].

[17] K. Scarfone, "Introduction to SIEM Services and Products," TechTarget, [Online]. Available: http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products. [Accessed 11 September 2015].

[18] K. Kent and M. Souppaya, "Special Publication 800-92: Guide to Computer Security Log Management"," NIST, September 2006. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf. [Accessed 11 September 2015].

[19] C. Osborne, "Execs admit 'blind spots' hurt network security: report," ZDnet, 1 June 2015. [Online]. Available: http://www.zdnet.com/article/execs-admit-blind-spots-hurts-network-security-report/. [Accessed 11 September 2015].

[20] The MITRE Corporation, "Awareness & Training," [Online]. Available: http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources/awareness-training. [Accessed 11 September 2015].

[21] US-CERT, "Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions," [Online]. Available: https://cisa.gov/tlp. [Accessed 21 January 2021].

[22] E. Hutchins, M. Cloppert and e. al., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin, [Online]. Available: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf. [Accessed 11 September 2015].

[23] T. Wilson, "Threat Intelligence Platforms: The Next 'Must-Have' for Harried Security Operations Teams," Dark Reading, June 2 2015. [Online]. Available: http://www.darkreading.com/threat-intelligence-platforms-the-next-must-have-for-harried-security-operations-teams/d/d-id/1320671. [Accessed 11 September 2015].

[24] ISACA, "Responding to Targeted Cyberattacks," 2013. [Online]. Available: http://www.infosecurityeurope.com/__novadocuments/68602?v=635526169065300000. [Accessed 11 September 2015].

[25] C. Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, October: The MITRE Corporation, 2014.

[26] S. Garfinkel, "All About Honeypots and Honeynets," CSO Online, 1 May 2003. [Online]. Available: http://www.csoonline.com/article/2115901/data-protection/all-about-

honeypots-and-honeynets.html. [Accessed 11 September 2015].

[27] Department of Homeland Security, "Cyber Risk Management Primer for CEOs," [Online]. Available: http://cisa.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf. [Accessed 21 January 2021].

[28] National Association of Corporate Directors, "Cyber-Risk Oversight Handbook," 10 June 2014. [Online]. Available: https://www.nacdonline.org/cyber. [Accessed 11 September 2015].

[29] NIST, "Cybersecurity Framework," 2015, 1 July. [Online]. Available: http://www.nist.gov/cyberframework/. [Accessed 11 September 2015].

[30] NIST, "Special Publication 800-84: Guide to Test, Training, and Excercise Programs for IT Plans and Capabilities," September 2006. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf. [Accessed 11 September 2015].

[31] J. Kick, "Cyber Excercise Playbook," The MITRE Corporation, November 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf. [Accessed 11 September 2015].

[32] Open Security Training, "Open Security Training," [Online]. Available: http://opensecuritytraining.info/. [Accessed 11 September 2015].