MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

THREAT-INFORMED CYBERSECURITY OPERATIONS FOR HEALTHCARE DELIVERY ORGANIZATIONS

A GUIDE TO MATURING CYBER DEFENSE CAPABILITIES FOR HDOS

Dr. Clem Skorupka and Dr. Lindsley Boiney, The MITRE Corporation

NOVEMBER 2021

Executive Summary

Healthcare Delivery Organizations (HDO) face a complex set of challenges in their information technology and operational environment, with threats that can impact patient care, business operations, medical devices, facilities, protected health information, and public confidence. Understanding and being prepared to identify, prevent, detect, respond to, and recover from these threats [1] is critical to maintaining the HDO mission. The Cybersecurity Operations Center (CSOC) acts as a focal point for an HDO's cyber threat monitoring and response. MITRE has developed the Cyber Operations Rapid Assessment (CORA™) methodology, a holistic, rapid, structured approach to assessing CSOC capabilities across the people, process, and technology dimensions [2] [3], and has used this methodology to engage with a variety of public and private sector organizations to help improve their cybersecurity operations. This paper identifies the main cybersecurity challenges common to HDOs and provides a capability rubric, based on the CORA methodology, that HDO cyber leadership can employ to help assess the state of their operational cyber defenses and inform planning for future defensive capabilities. While not all HDOs have sufficient size or resources to field a full CSOC capability internally, this document can be used to help identify and structure services obtained via third parties.

Contents

Introduction

Health Delivery Organizations (HDO) face a complex set of challenges in their information technology (IT) and operational environment, with threats that can impact patient care, business operations, medical devices, facilities, protected health information (PHI), intellectual property, and public confidence. Understanding and being able to identify, prevent, detect, respond to, and recover from these threats [1] is critical to maintaining the HDO mission. MITRE has developed the Cyber Operations Rapid Assessment (CORA™) methodology, a holistic, rapid, structured approach to assessing Cybersecurity Operations Center (CSOC) capabilities across the people, process, and technology dimensions [2] [3], and has used this methodology to engage with a variety of public and private sector organizations to help improve their cybersecurity operations. In this paper we extend the CORA methodology to the HDO domain and present a capability rubric for cybersecurity operations which HDO leadership can employ to help assess the state of their operational cyber defenses and inform planning for future defensive capabilities.

The goal of this paper is to help HDOs develop their cybersecurity operational capabilities (identifying threats, monitoring, and responding). It will identify broader cybersecurity capabilities, technologies, practices, and touchpoints in the organization, such as risk management, policy, and technology practices and controls, which are integral to the organizations' operational cyber defense. The paper is not intended to identify specific incident response scenarios and procedures [4]. It will not focus on privacy practices beyond the potential impacts on privacy that data breaches can have.

WE WILL ENUMERATE THE THREATS AND CONCERNS SPECIFIC TO HDOS, SUMMARIZE THE CORA MODEL, AND THEN PRESENT BEST PRACTICES FOR HDO CYBERSECURITY OPERATIONS.

The intended audience for this paper is an HDO CSOC Manager, Chief Information Security Officer (CISO), or other cybersecurity leader interested in enhancing their cybersecurity operational capabilities. While not all HDOs have sufficient size or resources to field a full CSOC capability internally, this document can be used to help identify and structure services obtained via third parties.

In the following sections, we will enumerate the threats and concerns specific to HDOs, summarize the CORA model, and then present best practices for HDO cybersecurity operations. The final section presents a CORA-based HDO capability rubric that can be used to help organizations plan their operational cybersecurity initiatives.

What's Different About HDO Cybersecurity?

HDOs have a number of elements that make operational security particularly challenging. These include the complexity and interdependency of systems and services, the variety of technologies, applications, and networked devices, the number of organizational groups, vendors, and partners who collaborate to provide health services, and of course the overriding concern for and potential impact on patient health [5] [6]. HDO security operations must work with IT as well as Operational Technology (OT) and Health Technology Management (HTM) teams to ensure comprehensive cyber defense.

HDO Primary Threats and Concerns

Many enterprises face a range of threats that can lead to financial loss, disruption of business and services, exposure of personal information or intellectual property, and loss of reputation. But the impacts to HDOs can be even greater due to the potential for interruption of patient care, injury, and death [7]. In a clinical setting, the uninterrupted availability of services and the ability of teams of care providers to share information rapidly is vital. More specifically, threats for the HDO include [8]:

- Ransomware and extortion which can interfere with normal operations for an HDO, whether by affecting workstations, business systems, or clinical devices. Further, recovery from ransomware can be difficult and time-consuming, particularly if backup and recovery plans have not been fully exercised.
- Electronic Health Record (EHR) and Electronic Medical Record (EMR) systems can be targeted for their content. Patient records and PHI are of considerable value to some attackers, and privacy is a major concern for HDOs.
- Business/Billing systems are obvious targets for financially motivated attackers, and disruption of these systems may interfere with normal HDO operations.
- Intellectual property, such as collaborations with medical researchers from universities, biotech, and pharmaceutical companies, can be a target for theft.
- Specific regional threats may also be a concern, such as nation states targeting the medical records of individual officials at HDOs located near a seat of government or a military installation.

Additionally, HDOs have many constraints and concerns due to the nature of their mission:

- Since HDOs participate in broad networks of partners and service providers, incidents at one facility may have significant regional impact as patients and services are redirected.
- Interdependencies among systems and functions (e.g., clinical decisions and surgeries that depend on the availability and accuracy of lab reports, radiology results, and patient histories) increase the potential operational impact of threats.
- Vendor maintenance practices, regulatory and safety concerns, and the constraints on implanted or at-home devices may restrict the operational changes that can be made.
- The expected operational life of medical devices is often much longer than that of traditional IT, making it necessary to maintain many legacy devices and systems that lack current cyber protections or are built on end-of-life components that cannot be patched.
- Operational or environmental constraints, such as the need for uninterrupted access in an operating room, make the use of common controls such as multifactor authentication impractical.
- Telehealth, telemedicine [9], and remote monitoring open up a host of issues related to personally owned systems such as proper authentication, application vulnerabilities, and local network and Wi-Fi security.

HDO Teams, Partners, and Community

HDOs typically work in concert with a large number of internal teams, external vendors, and partners, including:

- Biomedical engineering
- Health systems management
- Picture archiving and communications (PACS)
- Laboratories
- Pharmacy systems
- Medical device vendors
- Healthcare system networks
- EMR/EHR
- Educational and research organizations
- Local and regional health authorities.

HDO CSOCs need points of contact and standard operating procedures (SOP) for interacting with these diverse partners and should understand the threats and potential impacts to them.

HDO Technology and Applications

HDO CSOCs need to be able to identify, monitor, and respond appropriately to threats against the following technologies:

- Medical device technology such as scanning and radiology equipment, patient monitors, infusion pumps, etc.
- Radiological Information Systems and PACS
- EMR and EHR systems
- Provisioning, ordering, and billing systems
- Pharmacy and pharmaceutical systems
- Physical and environmental control and monitoring systems, such as oxygen, elevators, temperature, refrigeration
- Public informational sites and web portals
- Telehealth facilities and applications.

CORA Overview

The CORA methodology was developed to help organizations understand how cyber threat information can best be utilized throughout their organization to improve cyber defenses. CORA identifies five major areas of cybersecurity where the proper introduction of threat information can have tremendous impact on the efficacy of defenses:

- Cyber Threat Intelligence (CTI) and External Engagement
- Threat Awareness and Training
- Tools and Data Collection
- Internal Processes
- Tracking and Analysis.

Since organizations come in different shapes and sizes, with varying missions, resources, constraints, architectures, and threat profiles, CORA considers the five areas in light of the organizational context.

The full CORA model for "generic" organizations is presented in Appendix A. In the following sections, we present guidance based on the CORA model that is tailored for HDOs.

Growing Cybersecurity Operations for HDOs

Historically, cyber attacks were often handled by the IT or networking groups within an organization in an ad hoc manner. As attacks became more prevalent, organizations built computer emergency response teams (CERT™ [10]) or computer incident response centers that staffed dedicated teams to analyze events, perform digital forensics, and coordinate recovery. Security Operations Centers (SOC) or CSOCs evolved to incorporate functions such as actively monitoring various

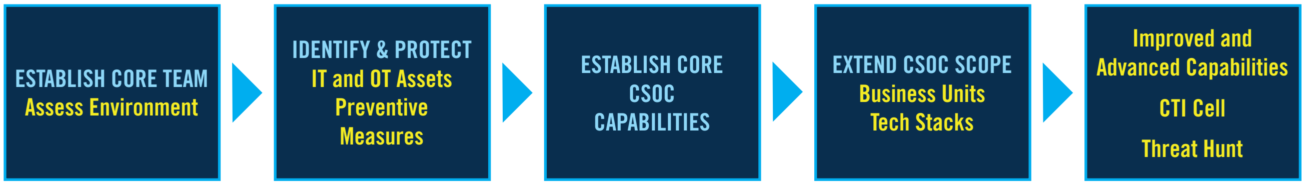

FIGURE 1: GROWING CYBERSECURITY OPERATIONS

anti-malware, firewall, and host event data feeds; performing triage, analysis, and incident response; collecting CTI, and providing situational awareness of cyber events across the organization to support consistent and efficient response [11].

Growing cybersecurity operations is an iterative process, and it takes time and focused effort to establish foundational capabilities and gradually extend them to fully encompass the HDO's environment. Furthermore, HDOs have varying resources available for cybersecurity, as well as different levels of maturity for their defensive capabilities. This section presents some strategies to help HDOs develop a roadmap for building their cyber operational capabilities. **Figure 1** describes a notional high-level approach to establishing and growing a CSOC capability.

Establish Core Team

Identify a leader or champion for the effort. This can be a CISO, a Chief Information Officer (CIO), or other direct report to senior leadership. Form a core technical team to assess current tools, processes, and capabilities and develop requirements for the CSOC. The team can engage with contractors and external consultants for technical expertise and independent analysis. The core team should also share threat landscape reports with leadership and stakeholder groups in order to raise awareness of risks and direct resources accordingly.

Identify and Protect

The core team should assess the HDO environment, identify the business units, and inventory the various IT, OT, and Health Technology assets. The team should effect changes to ensure there are basic preventive measures [12] in place such as firewalls, authentication, and anti-malware technology to reduce the overall attack surface of the HDO. Most importantly, comprehensive backup and recovery processes should be put in place and regularly exercised. Since quite often OT or biomedical engineering assets will not be managed by the IT group, all responsible groups should explicitly include cyber attack scenarios in their Continuity of Operations (COOP) plan.

Establish Core CSOC Capabilities

The core team can start by selecting a given technology stack (e.g., endpoint devices), or a given business unit (e.g., radiology), and establishing an initial set of capabilities to encompass the full cycle of monitoring, analysis, response, and recovery. The team can leverage the CORA Capability Rubric to choose "Foundational" and "Developing" capabilities to deploy (see **Figure 2**). These include network and host sensors, log collection, a security information event management (SIEM), and processes for monitoring, response, and recovery. The detection capabilities should be assessed with respect to relevant attack techniques to identify potential gaps in coverage.

HDOs must consider whether to develop capabilities in-house, leverage partnerships for shared capabilities, or outsource them. HDOs of all sizes, though particularly smaller ones, will want to strongly consider outsourcing core CSOC capabilities that require establishing and maintaining a highly skilled staff and complex technology stacks.

An important part of formalizing the CSOC is developing a Concept of Operations (CONOPS) that defines the mission, functions, relationships, and authority. The CONOPS should be socialized with stakeholders [13] and updated as the CSOC scope and capabilities grow.

Extend CSOC Scope

Use the core CSOC capabilities and processes as templates to extend the scope of the HDO's CSOC to other technology stacks and business units, such as clinical technology, EHR, or environmental systems. Each new technology or group will have its own operational constraints and concerns, so monitoring and response processes will need to be developed collaboratively with the system owners. Awareness training can also be developed that addresses the threats specific to the new business units.

Improved and Advanced Capabilities

Once the CSOC becomes established and has core capabilities in place across the main business units and technology stacks, it can look to bring in capabilities from the "Advanced" column of the CORA Capability Rubric to improve the overall security posture of the HDO. Such advanced capabilities and practices to consider include:

- Assess COOP for inclusion of cyber-triggered scenarios, such as ransomware
- Conduct tabletop exercises with IT, OT, HTM, Clinical, and other relevant groups
- Develop a process for assessing device and/or vendor risk
- Engage with external organizations such as the Healthcare Information Sharing and Analysis Center (H-ISAC), regional information sharing and analysis organizations (ISAO), and business partners to understand threats and share best practices [14]
- Consider entering cooperative defensive arrangements with regional partners for capabilities such as shared monitoring and response services [15]
- Grow a cyber threat intelligence capability/cell [16]
- Establish a "hunt team" to perform hypothesis- and intelligence-driven searches of the HDO's environment for advanced threat actors
- Deploy machine learning and advanced analytics.

Considerations for Small HDOs

Defending against cyber threats requires a broad suite of technologies, processes, and trained staff. While larger and better resourced HDOs can field a full team of a dozen or more cyber defenders and operate their own suite of defensive tools, smaller HDOs with several hundred employees or less may only have a few IT employees and no dedicated cyber defenders. This is a great challenge across most industries: security operations do not scale down well. Such smaller HDOs should consider alternative strategies to in-house security operations:

- Identify at least one lead staff responsible for identifying and procuring cybersecurity services and coordinating incident response; the lead should report to senior management
- Conduct an inventory across IT, OT, and Health Technology assets
- Conduct a cyber risk assessment to help prioritize controls and defenses

- Institute a proactive patch and vulnerability management process
- Outsource to a managed security service provider (MSSP), particularly one that specializes in HDO and small and medium business CSOC services [17] [18] [19]
- Outsource off-hours monitoring to a service provider, or alternatively implement a "pager duty" model
- Emphasize preventive measures [12]
- Train staff in cybersecurity basics [12]
- Leverage free open source intelligence from public and private sectors for threat landscape reports and emerging threat information [20] [21]
- Leverage free government resources for assessing cyber risk and reducing attack exposure [22]
- Consider partnering with a larger health provider for shared services
- Ensure good backups and exercise the restore/recovery plan.

Best CSOC Practices for HDOs in the CORA Framework

This section presents a set of recommended practices for HDO security operations, organized according to the CORA functional areas. Not all may apply or be practicable given the resources and constraints of the particular HDO [23]; some could be partially or fully outsourced to a service provider. Generally speaking, HDOs should consider outsourcing specialty functions where possible, since security operations require a broad set of skills that can be difficult to staff and maintain. MSSPs, SOC as a Service, Endpoint Detection and Response (EDR) as a Service, and SIEM as a Service are among the many options available to outsource CSOC capabilities.

Cyber Threat Intelligence and External Engagement

Threat Profile

HDOs should conduct a threat landscape assessment based on an understanding of their functions, services, and technologies. Defensive efforts should then be aligned against likely risks and potential impacts. The landscape assessment may be developed by internal staff or provided by a threat sharing organization or commercial threat intel consultant. Smaller HDOs can leverage existing open source resources such as the Health Sector Cybersecurity Coordination Center (HC3) [20] Threat Briefs [24], the CISA Cyber Resiliency Review [25], or cybersecurity vendor reporting [21].

CTI Cell

HDOs should establish a CTI capability [26] or "cell" that actively researches emerging threats relevant to the HDO, collects reporting, indicators, and analytics for the CSOC monitoring and response team to implement, and develops threat landscape reports and more detailed products to inform HDO leadership, business/clinical units, and technology groups [26]. The cell also supports the incident response process by providing intel and research for the incident responders [16]. Smaller HDOs likely cannot support a dedicated CTI cell but should allocate some staff time to this function.

Priority Intel Requirements

The HDO's CTI cell should work with leadership as well as business and technology groups to establish a set of prioritized intelligence requirements (PIR) to guide and shape intel collection and dissemination. The PIRs are informed by the HDO's risk assessment, technology, and architecture and should be updated annually.

Collaboration and Threat Sharing

Membership in a threat sharing organization can benefit HDOs at any resource or maturity level, informing defensive activities across the spectrum from tactical to strategic. HDOs should participate in the H-ISAC and other sector and regional threat-sharing collaboratives to understand emerging threats and share best defensive practices. Depending on resources available, HDOs should strive to be active members and share their own observations and analysis of malicious activity.

Threat Intel Sources

HDOs should collect threat intel from a variety of sources, including government, open source, health sector partners, and subscriptions to commercial providers.

Threat Awareness and Training

- Leadership should be informed of the overall threat landscape, including the potential risks and impacts of not fully defending against threats such as ransomware or PHI theft [27].
- HDOs should establish threat awareness and training programs for staff, patients, clinicians, and partners, to include common threats and vectors such as phishing, attacks against public facing systems, and ransomware [28].
- Defenders need to understand the HDO environment in all its complexity, including medical devices and other operational technology, and have sufficient training to understand the particular threats and appropriate response procedures. Tabletop exercises can be an effective means to improve both defenders' and operational units' understanding of different threat scenarios [29] [30] [31].

Data and Tools

Asset Management Database

HDOs need to establish an asset knowledge base of software and hardware (including OT and Health Technology) that identifies ownership, administrator, class or use, version and patch information, and configuration details [32] [33].

Architecture

HDOs should consider the use of network and application access controls to limit lateral movement and unauthorized access, such as network segmentation and zero-trust technologies [34] [35].

Endpoint Detection and Response (EDR)

EDR is an agent-based technology deployed on client systems that provides a variety of detection, query, and response capabilities. HDOs should deploy EDR on common user and system endpoints to identify malicious activity on compromised hosts and take appropriate action [36].

Passive Monitoring

HDOs should investigate and deploy passive monitoring technologies for devices and systems that cannot have security agent software installed, or that can be impacted by processing loads associated with event logging [37] [38].

SIEM

HDOs should deploy a central logging and analysis capability, such as a SIEM, to consolidate and correlate the many relevant data sources and manage the various alerts and analytics. Managing SIEMs can be complicated and require highly skilled labor, so HDOs may want to consider outsourcing this function or utilizing so-called "SIEM as a Service" offerings [39].

CTI Integration

HDOs should integrate threat feeds into their SIEM and other parts of their defensive grid in order to identify and block known malicious behavior.

Cloud Access Security Broker (CASB)

HDOs should enforce restrictions on file sharing and other potentially risky interactions with cloud services by employing CASB technology [40].

EHR, EMR

Large, pervasive systems such as EHR and EMR are comprised of many software components. HDOs should analyze their security controls, implementation, and software bill of goods to understand the potential impact of underlying vulnerabilities and exploits related to the components.

Personal Devices

HDO-issued mobile devices (e.g., smart phones, tablets, etc.) should be consistently configured and managed, and employ remote virtual desktop software for access to HDO resources and sensitive information. Personal devices or vendor-supplied devices should connect to separate network segments.

Analytics

HDOs should employ not only indicators of known malicious behavior (i.e., IP addresses, file hashes, URLs), but also use behavioral analytics to look for specific adversary tactics, techniques, and procedures (TTPs) [41]. SOC and SIEM service providers are increasingly offering "out of the box" behavioral analytics, and there are open public repositories [42] of analytics that can be leveraged.

Automated Workflow

HDOs should consider employing technologies such as Security Orchestration and Automated Response (SOAR) [43] to automate common analyst actions.

Internal Processes

CONOPS

HDOs should develop a comprehensive CONOPS, approved by HDO leadership, that describes the mission, roles, and responsibilities of the CSOC, and identifies the partner and stakeholder relationships. The CONOPS should provide high-level documentation of key processes, types of monitoring and response activities performed, and the technology employed.

Staffing

HDOs should have a core staff that includes an operations lead or CSOC manager, analysts, monitoring personnel, and systems administration/operations support sufficient to manage the sensors, SIEM, technologies, data and intel feeds, and associated analytics during normal business hours [44]. Smaller HDOs may find this impractical and should consider outsourcing to a managed service provider with a full range of capabilities [45].

24/7 Monitoring and Response

Attacks can occur any day or time, so HDOs should monitor and respond to threats 24/7. Typically, this involves full staffing during normal business hours and a reduced staff plan for off hours. If reduced staffing in-house is prohibitive, the HDO may outsource off-hours coverage. A "pager duty" rotation is another approach, though to be viable this needs to be supported by very good, high- confidence/low false positive alerts that can page the on-duty analyst.

Knowledge Management

The CSOC should employ knowledge management practices and platforms to support CSOC staff awareness of the types of medical devices, the operational impact to different targets, and up-to-date points of contact and handling procedures across different functional and clinical groups.

Vendor and Device Assessment

HDOs should establish a process to evaluate new medical devices and technologies (including upgrades) for security risk. The process should identify controls and mitigation methods to allow safe connection to the HDO networks.

Vulnerability Prioritization

HDOs should implement a vulnerability remediation prioritization scheme, such as one based on the Common Vulnerability Scoring System (CVSS) [46], in order to best manage resources and reduce risk. The CSOC CTI team should inform this process with estimates of severity and other factors based on current intelligence about active threats.

IT and OT Troubleshooting

HDOs should ensure that IT and OT groups include the possibility of cyber attack when investigating system failures and anomalies. There should be a clear notification and escalation path to the CSOC when an IT or OT group suspects malicious activity. CSOC analysts should have access to system and device trouble ticket reporting to perform correlation against other cyber events.

Exercises

HDOs should regularly exercise incident response SOPs across the different IT, OT, and stakeholder groups [29].

COOP

HDOs should have comprehensive COOP plans that explicitly consider cyber threats, including backup and recovery procedures for key HDO systems, applications, and services. There should be alternative business procedures (e.g., diversion of patients, rescheduling of patients, use of paper or alternative technology stack for data capture) for when a pervasive system such as an EHR is compromised. Assessment of COOP should employ both tabletop exercises and technical exercises (e.g., cutting over to failover system, rebuilding a service from backups).

Tracking and Analytics

Incident and Event Tracking

The HDO CSOC should implement a ticketing or case management system that captures pertinent details of attacks such as affected systems, applications and users, method detected, class of threat actor (e.g., financial, insider, benign insider, nation state), specific threat group (e.g., Ryuk), TTPs employed, and impact. These elements should be tracked in a structured format to allow for rollup reporting and trending.

Behavioral Analytics

HDOs should augment indicator-based analytics with behavioral-based analytics to identify malicious behavior. Frameworks such as ATT&CK,® and ATT&CK-ICS for operational technology, are useful for understanding adversary TTPs and provide a common language to communicate with other organizations. HDOs should develop their own analytics, as well as leverage their SIEM vendor's offerings. They can supplement with existing open source analytic repositories such as CAR [42], Elastic Query Language (EQL) [47], Sigma [48], and those available via their threat-sharing partner (e.g., the H-ISAC analytics group). Analytics should be prioritized according to a threat analysis of likely attack vectors. Analysts need to work with IT and OT groups to identify types of behavior that could be deemed suspicious (as opposed to normal system administration) in order to tune their detection signatures and analytics.

CASB and UEBA

HDOs should consider employing User Entity Behavioral Analytics (UEBA) capabilities via their CASB or cloud security management platform to identify abnormal user and system/application behavior [49] [50].

Digital Forensics

HDOs should consider engaging a digital forensics consulting group to establish a digital forensics program, and have procedures in place to preserve evidence in the event a case may involve law enforcement or litigation.

CORA Capability Rubric for HDO Cybersecurity Operations

This section describes a capability model or rubric to help HDOs assess their current CSOC capabilities and develop a roadmap for future improvements. The capabilities are grouped according to the CORA focus areas, and are presented in **Figure 2** as initial, developing, and advanced. As previously noted, HDOs vary widely in size, resources, and cyber maturity, so it is not necessary to strive for advanced capabilities across all areas. The capabilities of particular importance to Health Delivery Organizations have been presented in bold text.

	INITIAL	DEVELOPING	ADVANCED
CTI AND EXTERNAL ENGAGEMENT	No clear threat intelligence requirements	Some threat intelligence requirements, not well aligned with threat profile	Prioritized threat intelligence requirements, aligned with threat profile, approved by leadership, that drive collection activities
	No regular external threat sources	Limited and informal external threat sources (mailing list, public forum)	Variety of external threat sources to include government, open source, commercial, and sector/partner sources
	Ad hoc, informal storage of threat intelligence information (e.g., email, file store)	Simple yet structured tracking of threat intelligence (indicators and reports), e.g., spreadsheet or database	Dedicated threat intelligence platform that connects to multiple threat intelligence feeds, interfaces to SIEM and other technology, and allows analysts to track, query, and prioritize threat information
	Not member of ISAC, ISAO, or other threat-sharing organization	**Member of an ISAC (e.g., H-ISAC), ISAO, or other threat sharing organization**	**Member of multiple industry/sector-based and regional ISAC, ISAO, and threat-sharing organizations**
	Participates in threat-sharing organization as passive consumer of information for situational awareness.	Participates and actively utilizes threat information consumed from the threat-sharing organization	Participates actively, reporting sightings of attacks and producing and sharing new insights and intel from their own analysis.
	No staff time dedicated to CTI analysis	Staff time regularly dedicated to CTI	Full-time CTI staff/formal "Threat Cell" focused on CTI collection, analysis, dissemination, reporting, and collaboration
	Ad hoc, inconsistent collection, handling, analysis, and dissemination of CTI	Regular, documented CTI processes	CTI processes that encompass full intelligence lifecycle for collection, analysis, handling and dissemination, and measured for process improvement
	Limited threat intelligence reporting products produced (e.g., threat landscape report, ad hoc situation reports)	Regular threat intelligence products produced, including regular leadership threat landscape report, tailored products for CSOC team, incident-driven research products	Regular threat intelligence products, plus tailored threat reporting for specific business units, Threat Actor profiling, trending and analysis
	Limited external exchange of high-level CTI (best practices, threat landscape reports)	Exchange of semi-structured CTI (incidents, mitigations, basic indicators)	Exchange full range of CTI including indicators, signatures, analytics, malware samples, and raw data if desired

FIGURE 2: CORA CAPABILITY RUBRIC PAGES 11-15

	INITIAL	DEVELOPING	ADVANCED
TRAINING & AWARENESS	**Limited understanding of own cyber threats, or impacts and risks to HDO mission; not well propagated throughout HDO enterprise**	**Partial understanding of own cyber threats, impacts and risks to HDO mission; not well propagated throughout HDO enterprise**	**Thorough understanding of own cyber threats, as well as the potential impacts and risks to HDO mission; understanding propagated throughout HDO enterprise**
	Limited leadership buy-in for cybersecurity issues	Modest leadership buy-in for cybersecurity; not systematically influencing risk management	Leadership buy-in, support for cybersecurity; influences risk management
	Little to no employee training on cybersecurity awareness	Relatively static employee training, more on cyber hygiene than cybersecurity awareness	Ongoing, regularly updated cybersecurity awareness training of employees as "human sensor grid"
	No user threat reporting	Only ad hoc user threat reporting	Codified, supported means for user threat reporting (e.g., ticket queue, "report phishing" button in email client, web form, etc.)
	No awareness of threat of intellectual property (IP) or protected health information (PHI) theft	**Some awareness and training to include potential of IP and PHI theft**	**Researchers and clinicians briefed on specific threat scenarios focused on actual incidents and protection against IP and PHI theft**
	Unknown or little training of cyber defenders	Sporadic or ad hoc training of cyber defenders	Cyber defenders well-trained including cross-role training
	Little awareness of clinical and operational technology for cyber defenders	**Some awareness of clinical and operational technology and potential impacts of cyber threats**	**Comprehensive awareness of potential impacts to clinical and operational technology, and appropriate knowledge of environment and constraints for monitoring and response**
	Analyst expertise not captured	Analyst expertise captured inconsistently (emails, notes)	Analyst techniques and expertise consistently captured for continuity, consistency, and training new defenders

	INITIAL	DEVELOPING	ADVANCED
DATA & TOOLS	Limited in-house log/event collection	Hygiene-driven log/event collection	Threat-driven log/event collection based on likely TTPs
	Limited or ad hoc mechanisms to protect organization's data and customers' data	Incomplete mechanisms in place to protect organization's data and customers' data	Broad mechanisms in place to prevent the loss of organization's mission-critical data, as well as customers' sensitive data, such as data loss prevention, multifactor authentication, segmentation, Zero-Trust
	Incomplete, de-centralized log storage	Some logs centralized	SIEM or log aggregator - can combine and review data from across the enterprise from a single location for comprehensive analysis
	No consolidated alert or event queue for near-real time alerting	Some consolidation of alert and event data	Most alert and event data viewable, prioritized, trackable in a console "single pane of glass"
	Limited enterprise visibility	Moderate enterprise visibility	Enterprise-wide visibility into networks and systems, **OT, cloud-based assets**, and their business/mission roles
	No threat detection capabilities	Limited threat detection capabilities: network only (no host capabilities)	Instruments a variety of detection, defensive, and analysis tools: both network traffic and host inspection/ **EDR capabilities, privileged access logs, passive OT monitoring**
	Basic capabilities: firewalls, anti-malware technology	Moderate capabilities: Perimeter monitoring (e.g., web proxy logs, IDS)	Advanced capabilities: DNS sink-holing, honeypot, malware sandbox
	No visibility into or controls on cloud-based assets and services	Visibility into cloud-based assets and services, some controls	Visibility and fine-grained controls on cloud-based assets including **CASB and EUBA**
	No visibility or security controls for facility physical and environmental systems	**Some visibility and security controls for facility physical and environmental systems**	**CSOC has full visibility and security controls for facility physical and environmental systems**
	No monitoring or event logging of EHR/EMR, or other health IT systems	**Limited monitoring or event logging of EHR/EMR and other health IT systems**	**Monitoring and event logging and alerting based on threat analysis of EHR/EMR and other health IT systems**
	No monitoring of medical devices and systems	**Monitoring of some medical devices and systems**	**Monitoring, event logging, and analytics based on threat analysis of all medical devices and systems**
	No restrictions or enforcement on personal device usage to access HDO resources	**Some restrictions on personal device usage to access HDO resources**	**Organization-issued personal devices (e.g., smart phones/tablets) and/or remote virtual desktops to access HDO resources**

	INITIAL	DEVELOPING	ADVANCED
INTERNAL PROCESSES	Consistently under-resourced and/or under-staffed	Some staff functions under-represented	Resourced and staffed (or outsourced) appropriately for its size and threat profile (e.g., tiered operations, 24/7 monitoring and response, CTI, Hunt Team)
	No formal cybersecurity program (e.g., ad hoc function within IT)	Have some components of a cybersecurity program (potentially outsourced)	Has a formal cybersecurity program to include risk management, privacy, policy, user training, secure application development, asset and vulnerability management, and security operations
	No individual responsible and accountable for cybersecurity	Individual who is responsible and accountable for cybersecurity is not at senior level (e.g., not C-suite)	Has a senior leader who is responsible and accountable for cybersecurity (e.g., CISO)
	No COOP that includes cybersecurity event triggers (including ransomware)	**COOP plan that includes common cybersecurity events such as ransomware, and is partially exercised**	**COOP plan that includes cybersecurity event triggers that are considered likely based on threat analysis, and is fully exercised including system and application backup and recovery, and fallback business procedures (e.g., patient diversion, rescheduling, paper or alternative tech stack for data capture)**
	No documented CONOPS, few documented SOPs	**Some components of a CONOPS in place, most SOPs documented**	**Comprehensive, documented, approved CONOPS with mission roles, responsibilities, and interactions identified with IT, clinical groups, and external partners**
	No coordination between cybersecurity function and either IT and Health IT (EMR/EHR etc.) planning or acquisition processes	**Ad hoc, limited coordination between cybersecurity function and either IT or Health IT (EMR/EHR etc.) planning or acquisition processes**	**IT and Health IT (EMR/EHR etc.) planning and acquisition processes are informed of threat environment in time to acquire and deploy appropriate controls and defenses**
	No coordination between cybersecurity function and either OT planning or acquisition processes No prioritization of vulnerability and patch management for OT based on threat severity	**Ad hoc, limited coordination between cybersecurity function and either OT planning or acquisition processes. Some prioritization of vulnerability and patch management for OT based on threat severity guidelines**	**OT planning and acquisition processes are informed of threat environment in time to acquire and deploy appropriate controls and defenses. Prioritization of vulnerability and patch management for OT based on formal threat severity guidelines such as CVSS**
	No coordination between cybersecurity function and either telemed and OT planning or acquisition processes	**Ad hoc, limited coordination between cybersecurity function and either telemed and OT planning or acquisition processes**	**Telemed and OT planning and acquisition processes are informed of threat environment in time to acquire and deploy appropriate controls and defenses**
	No prioritization of vulnerability and patch management for IT based on threat severity	Some prioritization of vulnerability and patch management for IT based on threat severity guidelines	Prioritization of vulnerability and patch management for IT based on formal threat severity guidelines such as CVSS
	No prioritization of vulnerability and patch management for OT based on threat severity	**Some prioritization of vulnerability and patch management for OT based on threat severity guidelines**	**Prioritization of vulnerability and patch management for OT based on formal threat severity guidelines such as CVSS**
	No knowledge base of HDO systems, services, and technology and function-specific incident response procedures	**Partial knowledge base of HDO systems, services, and technology and function-specific incident response procedures**	**Full knowledge base of HDO systems, services, and technology and function-specific incident response procedures, developed in collaboration with system owners, business units, and clinicians**
	No mechanisms or SOP for OT and EHR/EMR staff to consider cyber threats as possible source of system failure or anomalies	**SOP and reporting mechanisms (e.g., ticket queue) defined for some OT and/or EHR/EMR teams to report potential cyber threat activity.**	**SOP and reporting mechanisms (e.g., ticket queue) defined for all OT and/or EHR/EMR teams to report potential cyber threat activity**
	Does not conduct cybersecurity exercises with IT, OT, and Business units	**Conducts occasional cybersecurity exercises**	**Conducts regular cybersecurity exercises with various IT, OT, and business units**
	Does not conduct cybersecurity exercises with vendors, partners, and regional government and health-related organizations and responders	**Conducts occasional cybersecurity exercises (e.g., table top exercises) with some vendors, partners, and regional government and health-related organizations and responders**	**Conducts regular cybersecurity exercises with vendors, partners, and regional government and health-related organizations and responders**

	INITIAL	DEVELOPING	ADVANCED
TRACKING & ANALYTICS	Ad hoc or no tracking of indicators	Semi-structured tracking of indicators with some contextual metadata	Systematic tracking of indicators with contextual metadata that supports queries, analytics and defensive actions (structured threat knowledge base). Employs dedicated system such as threat intelligence platform
	Ad hoc tracking of incidents	Loosely structured tracking of incidents	Dedicated incident tracking system, captures relevant incident information in structured format to support reporting, trending, and analysis
	Not able to check for presence of known indicators	Limited, ad hoc checking for presence of known indicators	Regularly checks for presence of known indicators via historical log searches, regularly scheduled queries of new logs, and near real time sensor alerts
	No or inconsistent tracking of threat information handling restrictions	Threat information tracking does not unambiguously capture handling restrictions	Organizes, tracks, and sanitizes its threat information so there are no ambiguities in handling or undue risk of exposure of sensitive information
	Ad hoc analysis and escalation	Ambiguous or incomplete analysis and escalation processes	Defined analytic processes for systematic and thorough review and escalation
	Does not write custom signatures/indicators	Occasionally writes custom signatures/indicators	Regularly write custom signatures/indicators
	No analytics	Limited analytics, such as basic historical search, and some behavioral analytics	Performs advanced analytics including traffic analysis, log analysis, historical analyses, malware analysis, host/disk/memory analysis. Supports a development lifecycle for identifying, prioritizing, testing, maintaining, and documenting analytics
	No or ad hoc defense validation	Some vulnerability scanning and pen-testing	Regular defense validation including pen-testing, Red Team and purple team exercises, and adversary emulation to test detection, analytics, and response procedures
	No detection signatures or analytics for OT (medical devices such as scanning and radiology systems, facility environmental controls, etc.)	**Limited detection signatures and analytics for OT systems**	**Detection and analytics based on threat analysis for OT systems**
	No Detection and analytics based on threat analysis for EMR/EHR systems	**Limited detection signatures and analytics for EHR/EMR**	**Detection and analytics based on threat analysis for EHR/EMR systems**
	No access to OT or EHR/EMR trouble tickets or anomalous event reporting	**Access to OT and EHR/EMR trouble tickets for incident review and analysis.**	**Correlation analysis of OT and EHR/EMR anomalous events with other cyber events (e.g., network and endpoint events)**
	Reactive-only incident investigations	Ad hoc, infrequent hypothesis-driven threat hunting activities	Regular threat-hunting activities driven by prioritized threat model and relevant CTI

References

1. National Institute of Standards and Technology, “Cybersecurity Framework: The Five Functions,” 12 05 2021. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/five-functions. [Accessed 09 2021].
2. L. Boiney, J. Connelly, C. Skorupka, S. Krueger and A. Summers, “Cyber Operations Rapid Assessment (CORA): Examining the State of Cybersecurity Assessment Methodologies and Introducing a New Alternative,” The MITRE Corp., 2015.
3. L. Boiney, “Threat-Based Cyber Operations Rapid Assessment,” in *NIST Cybersecurity Innovation Forum*, Washington, D.C., 2015.
4. J. Connolly, “Healthcare Cybersecurity Symptom Checker,” The MITRE Corp., 2021.
5. US Department of Health and Human Services/Public Health Emergency, “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,” 2020. [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx.
6. “Types of information systems used in healthcare facilities,” 2018. [Online]. Available: https://www.scott-clark.com/blog/types-of-information-systems-used-in-healthcare-facilities/.
7. US Department of Health and Human Services, “2020: A Retrospective Look at Healthcare Cybersecurity,” 2021. [Online]. Available: https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf.
8. L. Kim, “HIMSS Healthcare and Cross-Sector Cybersecurity Report,” 2020. [Online]. Available: https://www.himss.org/resources/himss-healthcare-and-cross-sector-cybersecurity-report.
9. D. Trep, “Best Practices for Telework and Telehealth Security,” [Online]. Available: https://www.hcinnovationgroup.com/population-health-management/telehealth/article/21162613/best-practices-for-telework-and-telehealth-security.
10. M. J. West-Brown, D. Stikvoort, K.P. Kossakowski, G. Killcrece, R. Ruefle and M. Zajicek, “Handbook for Computer Security Incident Response Teams,” 2003. [Online]. Available: https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf.
11. C. Zimmerman, “Ten Strategies of a World-Class Cybersecurity Operations Center,” October: The MITRE Corp., 2014.
12. US Department of Health and Human Services/Public Health Emergency, “Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations,” 2020. [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf.
13. CUE Logic, “Healthcare Cybersecurity: The Solution is SOC,” [Online]. Available: https://www.cuelogic.com/blog/healthcare-cybersecurity-soc.
14. ISAO Standards Organization, “Information Sharing Groups,” [Online]. Available: https://www.isao.org/information-sharing-groups/.
15. C. Petrozzino, “Advancing Healthcare Cybersecurity with Cyber Partnerships,” 2018. [Online]. Available: https://health.mitre.org/wp-content/uploads/2018/03/HIMSS18_Advancing_Healthcare_Cybersecurity.pdf.

16. K. Esbeck and K. W. Ramsdell, "Getting Started In Cyber Threat Intelligence," 08 2021. [Online]. Available: healthcyber.mitre.org.
17. W. Ashford, "Why Your Business Needs SOC as a Service https://www.computerweekly.com/opinion/Why-your-business-needs-SOC-as-a-service," Computer Weekly, 2021.
18. Cyberforce Q, "Specialized Cybersecurity Operations for the Healthcare Sector," [Online]. Available: https://www.cyberforceq.com/hsoc.
19. A. Wolf, "Confront Cyber Threats to Healthcare Reliably," 2019. [Online]. Available: https://www.healthcareitnews.com/news/confront-cyberthreats-healthcare-reliably-and-affordably-leverage-security-operations-center.
20. US Department of Health and Human Services/Health Sector Cybersecurity Coordination Center, "Health Sector Cybersecurity Coordination Center (HC3)," [Online]. Available: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html.
21. Fortified Health Security, "2021 Mid-Year Horizon Report: the State of Cybersecurity in Healthcare," [Online]. Available: https://go.fortifiedhealthsecurity.com/2021-Mid-Year-Horizon-Report-1.html.
22. Cybersecurity & Infrastructure Security Agency, "Cyber Hygiene Services," CISA, [Online]. Available: https://www.cisa.gov/cyber-hygiene-services.
23. US Department of Health and Human Services/Public Health Emergency, "Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations," [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf.
24. US Department of Health and Human Services Cybersecurity Program, "Ransomware Trends 2021," [Online]. Available: https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf.
25. Cybersecurity & Infrastructure Security Agency, "Assessments: Cyber Resiliency Review," 2020. [Online]. Available: https://us-cert.cisa.gov/resources/assessments.
26. Recorded Future, "How to Build a Cyber Threat Intelligence Team," 2017. [Online]. Available: https://www.recordedfuture.com/cyber-threat-intelligence-team/.
27. J. Riggi, "Why and how to incorporate cyber risk management into enterprise risk management," AHA Center for Health Innovation.
28. E. Powers, "Project Stories: Using Common Sense to Combat Threats to Privacy and Security," [Online]. Available: https://www.mitre.org/publications/project-stories/using-cyber-common-sense-to-combat-threats-to-privacy-and-security. [Accessed 16 July 2021].
29. J. Kick, "Cyber Excercise Playbook," The MITRE Corp., November 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf. [Accessed 11 September 2015].
30. T. Fersch, "Health Cyber Exercises for Patient Safety," The MITRE Corp., [Online]. Available: https://healthcyber.mitre.org/wp-content/uploads/2021/02/IDEAS-Health-Cyber-Slip-Sheet-for-PR_2021-1.pdf. [Accessed 21 July 2021].
31. T. Fersch, "Intelligence Driven Exercises and Solutions (IDEAS)," MITRE, 02 2021. [Online]. Available: https://healthcyber.mitre.org/wp-content/uploads/2021/02/IDEAS-Methodology-2021-Public-Release.pdf. [Accessed 21 July 2021].

32. M. Stone, "NIST SP 1800-5 IT Asset Management," 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf.

33. J. L. Connolly, S. Christy, R. Daldos, M. Zuk and M. Chase, "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook," 2018. [Online]. Available: https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and.

34. S. Rose, "NIST SP 800-207 Zero Trust Architecture," 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final.

35. D. H. Doherty and B. J. McKenney, "Zero Trust Architectures: Are we there yet?," 06 2021. [Online]. Available: https://www.mitre.org/publications/technical-papers/zero-trust-architectures-are-we-there-yet.

36. "Mitigations: Behavior Prevention on Endpoints," MITRE, [Online]. Available: https://attack.mitre.org/mitigations/M1040/. [Accessed 16 July 2021].

37. M. Kaouk, "A Review of Intrusion Detection Systems for Industrial Control Systems," in 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT), 2019.

38. B. Barney, "Intrusion Detection Systems: What's Missing in HIPAA Security?," Security Metrics, 2018. [Online]. Available: https://www.securitymetrics.com/blog/intrusion-detection-system-whats-missing-hipaa-security.

39. Datashield Protect, "On-Premises vs Cloud SIEM," 2020. [Online]. Available: https://www.datashieldprotect.com/blog/on-premises-vs-cloud-siem.

40. Gartner, "Gartner Glossary: Definition of Cloud Access Security Brokers," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs.

41. J. Wunder, "https://medium.com/mitre-attack/getting-started-with-attack-detection-a8e49e4960d0," The MITRE Corp.

42. The MITRE Corporation, "Cyber Analytics Repository," [Online]. Available: https://car.mitre.org.

43. "SOAR Security Automation and Orchestration Implementer Insights" 2018. [Online]. Available: https://www.iacdautomate.org/s/SAOImplementerInsights092018.pdf.

44. C. Crowley, "Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey," 2019. [Online]. Available: https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf.

45. Ponemon Institute, "Second Annual Study on The Economics of Security Operations Centers," 2020. [Online]. Available: https://www.mandiant.com/resources/economics-of-the-soc-2021-ponemon-institute-second-annual-study.

46. M. Chase and S. Coley, "Rubric for Applying CVSS to Medical Devices," 2020. [Online]. Available: https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices.

47. "EQL Analytics Library," [Online]. Available: https://eqllib.readthedocs.io/en/latest/.

48. "Sigma Rules github," [Online]. Available: https://github.com/SigmaHQ/sigma.

49. "Identify Threats with User Entity Behavioral Analytics," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics.

50. "What is UEBA?," Fortinet, [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-ueba.

51. US-CERT, "Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions," [Online]. Available: https://www.us-cert.gov/tlp.
52. The MITRE Corporation, "Awareness & Training," [Online]. Available: http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources/awareness-training.
53. C. J. Franklin, "CASB 101: Why a Cloud Access Security Broker Matters," 2020. [Online]. Available: https://www.darkreading.com/theedge/casb-101-why-a-cloud-access-security-broker-matters/b/d-id/1337302.
54. D. Bianco, "The Pyramid of Pain," [Online]. Available: https://rvasec.com/slides/2014/Bianco_Pyramid%20of%20Pain.pdf.
55. The MITRE Corp., "ATT&CK for ICS," [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Overview.
56. The MITRE Corp., "ATT&CK https://attack.mitre.org."
57. Cybersecurity & Infrastructure Security Agency, "Assessments: Cyber Resiliency Review," [Online]. Available: https://us-cert.cisa.gov/resources/assessments.
58. National Institute of Standards and Technology, "Red Team," 2015. [Online]. Available: https://csrc.nist.gov/glossary/term/Red_Team.
59. J. R. Salazar, "The Rise of Purple Teaming," 2019. [Online]. Available: https://www.darkreading.com/threat-intelligence/the-rise-of-purple-teaming/a/d-id/1334909.
60. J. Bauters, "The Rise of Adversary Emulation," 2018. [Online]. Available: https://blog.nviso.eu/2018/09/18/the-rise-of-adversary-emulation/.

Glossary

CAR	cyber analytics repository
CASB	cloud access security broker
CERT	computer emergency response team
CIO	chief information officer
CISO	chief information security officer
CONOPS	concept of operations
COOP	continuity of operations
CORA	cyber operations rapid assessment
CSOC	cybersecurity operations center
CTI	cyber threat intelligence
CVSS	common vulnerability scoring system
EDR	endpoint detection and response
EHR	electronic health record
EMR	electronic medical record
EQL	elastic query language
HC3	health sector cybersecurity coordination center
HDO	healthcare delivery organization
H-ISAC	healthcare information sharing and analysis center
HTM	health technology management
ISAC	information sharing and analysis center
ISAO	information sharing and analysis organization
IT	information technology
MSSP	managed security service provider
OT	operational technology
PACS	picture archiving and communications
PHI	protected health information
PII	personally identifiable information
PIR	prioritized intelligence requirements
SIEM	security information event management
SOAR	security orchestration, automation and response
SOC	security operations center
SOP	standard operating procedure
TLP	traffic light protocol
TTP	tactics, techniques, and procedures
UEBA	user and entity behavior analytics
URL	universal resource locator

Appendix A: CORA™ Best Practices

The CORA™ methodology [2] was developed to help organizations understand how cyber threat information can best be utilized throughout their organization to improve cyber defenses. CORA identifies five major areas of cybersecurity where the proper introduction of threat information can have tremendous impact on the efficacy of defenses:

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

Since organizations come in different shapes and sizes, with varying missions, resources, constraints, architectures, and threat profiles, CORA considers the five areas in light of such organizational context.

Cyber Threat Intelligence and External Engagement

Cyber threats evolve daily, and defensive actions taken today may not address threats that emerge tomorrow. To stay current, an organization needs to actively collect actionable, detailed information about organizationally relevant threats and threat actors. This requires an understanding of the organization itself: its mission and operations, its components, its technology, and the risks and impacts of concern. This organizational understanding drives the requirements for CTI collection.

While understanding risk requires looking within an organization, understanding threats requires external exploration and engagement. Common sources of CTI include commercial vendors, government and law enforcement agencies such as DHS and the FBI, open source, and sector communities and organizations such as ISACs and ISAOs. Threat-sharing communities such as ISACs and ISAOs are an important part of an organization's cybersecurity posture since they can provide a trusted environment for peer organizations to discuss emerging threats, share best practices, and more fully understand the potential impact of given attacks.

Participation in threat-sharing communities requires resources. Smaller or less-mature organizations may initially be passive consumers of the information that ISACs and ISAOs provide, such as threat landscape briefings and best practices for growing their foundational capabilities. As capabilities develop, organizations may become more active consumers, taking in threat indicator feeds and reports and scanning their own networks for malicious behavior. As greater capabilities and trust develop, organizations may become true contributors to the threat collective, sharing their sightings of malicious behavior and perhaps producing new threat intelligence, signatures, and analytics. This typically requires establishing a CTI cell with the ability to conduct threat research and develop a range of threat intel products to support both tactical and strategic needs [26] .

Tracking of Threat Information

Tracking and cataloging threat information, including metadata such as time of receipt, source, handling restrictions, context, and actions taken, is necessary for the following reasons:

- Indicators can have a shelf life or a limited time frame of validity, as when a malicious IP address gets re-assigned to a non-malicious entity.

- Different sources of indicators and intelligence may be of different quality, so this metadata allows identification of the most accurate and relevant information feeds. Source awareness also facilitates de-duplication of indicators that appear from multiple sources before scanning. Information from certain government or commercial sources may also have handling and sharing restrictions [21].
- Actors, motivations, and their TTPs vary, so tracking this information and linking it to associated indicators and alerts provides guidance for best response practices and "playbooks." Raw data from incidents may be re-analyzed in light of new intelligence.
- An indicator's position in the attack lifecycle or "Kill Chain" phase [22] helps determine the type and urgency of response.

The CSOC should have a well-trained team responsible for maintaining a knowledge base of its threat information. While initially a spreadsheet 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 support automated checks and defensive actions such as blacklisting. A number of security technology vendors now offer "threat information platforms" (TIP) and related technologies to support such activities [23].

CTI can come from many sources, including open source, commercial, private, and law enforcement. Care needs to be taken to handle CTI in accordance with the sources' expectations and guidelines. Mature organizations will employ a framework such as the Traffic Light Protocol (TLP) [51] to mark products for dissemination. TIPs may also have the ability to track the source of CTI, allowing analysts to comply with reporting and sharing policies and agreements.

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 personally identifiable information (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.

Organizations should have a thorough understanding of the relevant cyber threats, impacts, and risks, and this understanding must be 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 informs the user population of the types of threats and potential impacts their organization is subject to and which security policies and technical controls are in place. Employees should be given specific guidance on practices 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. Training should be provided regularly, with continuous updates as new threats emerge [52].

Enterprise Awareness

Business units, IT groups, and OT groups should be provided tailored threat intelligence reports and defensive guidance.

Defender Training and Readiness

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

Enterprise Readiness

The organization should engage in periodic, cross-organizational exercises with the CSOC using scenarios that will help refine and reinforce incident response procedures.

Tools and Data Collection

To effectively leverage CTI, organizations require a rich set of defensive tools and a collection of security-relevant logs and event data. Most organizations have basic capabilities such as border firewalls and gateway and desktop anti-malware. Defending against modern threats, however, requires additional capabilities such as endpoint detection and response (EDR), segmentation, strong authentication, server and application activity logging, network traffic monitoring, and cloud-based IT security controls and data collection. In order to know what to defend, the CSOC needs an inventory of all IT and OT assets, including owner, administrator, location, software, hardware, versions, patch levels, and security-relevant configurations. Cloud-based IT offers capabilities that can help protect an organization's assets but must be considered carefully in terms of the cost and performance associated with additional event monitoring and logging from the various cloud platforms to the SOC (or the hosting of SOC capabilities in the cloud). As more organizations shift towards cloud and multi-cloud architectures, a variety of CASB [53] and related technologies are being developed that can implement fine-grained controls and an array of event monitoring and analytics.

In order to analyze this rich set of data, organizations need a centralized collection and analysis capability such as a SIEM. Integrating CTI feeds for searching and/or blocking malicious indicators is an essential practice. Further, behavioral-based analysis capabilities are essential to move beyond indicator-based defenses [54] that can be readily bypassed by attackers.

Another challenge organizations face is the defense and monitoring of operational technology such as industrial control systems, sensors, or medical devices. OT can present a number of unique challenges and constraints beyond traditional IT, such as proprietary or "closed box" software, strict operating parameters, vendor-controlled patching and maintenance, inability to run third-party security products, limited logging capability, sensitivity to additional processing, and location and environmental constraints. OT may require specific tailored defensive approaches, such as passive monitoring, anomaly detection, and very restrictive network segmentation [55].

Advanced attackers can also potentially compromise defensive monitoring and management systems, so these should be protected via segmentation and out-of-band management approaches.

Internal Processes

Processes and policies must be in place to allow for effective planning, resource allocation, and monitoring and response across the organization. Leadership support is essential to the effectiveness of the CSOC. 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 [26], [16].

A Concept of Operations document is an important foundational document for a CSOC. The CONOPS is approved by appropriate authorities in the organization, and describes what the cybersecurity operation does, how it is staffed, what its responsibilities are, and which 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 cybersecurity team, and better define processes and points of interaction.

IT planning and acquisition processes should be fully informed of the threat environment. Requirements for security must be defined in a timely fashion to allow appropriate controls and defenses to be identified, acquired, and implemented as new technology is introduced to the organization's network.

Day-to-day SOP and incident response processes need to be both documented and informed by the current threat environment:

- Incidents should be 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.
- Firewall rules, sensor signatures, and analytics can be rapidly deployed.
- Malware analysis supports rapid turn-around indicator reporting to defenders as well as more detailed, "deep-dive" analysis.

Regular exercises should be conducted with various IT, OT, and business units to maintain readiness for high-impact scenarios and to identify gaps in existing processes and procedures [31]. These exercises also help to communicate the potential impact of different threats in a tangible way.

Particularly for complex environments, knowledge management of the variety of systems, potential impacts of attacks, POCs, and special handling procedures should be maintained and accessible for all CSOC monitoring and response staff.

Automation of common activities and workflow can help make operations more efficient and consistent. This can be accomplished via creation of SIEM "dashboards" of common analyst queries and reports, as well as implementation of Security Orchestration Automation and Response (SOAR) technologies [45].

Tracking and Analysis

In order to properly utilize threat information that has been collected and organized by the CTI Team, the CSOC must perform several important functions in addition to monitoring for threat activity: tracking of incident information, analysis, threat hunting, and defense validation.

Tracking of Incident and Event Information

The CSOC should implement a ticketing or case management system that captures pertinent details of attacks such as affected systems, applications and users, method of detection, class of threat actor (e.g. financial, insider, benign insider, nation state), specific threat group (e.g., APT13), TTPs employed, and impact. These elements should be tracked in a structured format to allow for rollup reporting and trending. Alerts and events can overload analysts, so it is important to have mechanisms in place to sort and prioritize response activity. Triage procedures can ensure the most impactful events are acted on in a timely fashion, and not overlooked by a busy analyst team.

Analysis

The CSOC threat analysts should be well-trained in a variety of disciplines and technologies, with access to additional expertise as needed via outsourcing. They require support 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 are intended to 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 need to be contextually linked to aid in quick triage and accurate handling.

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

- Traffic analysis
- Log and endpoint event analysis
- Malware analysis
- Host, disk, and memory analysis and digital 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].

To ensure a comprehensive, prioritized set of detection signatures and analytics, a CSOC should consider analyzing the set of likely threats and techniques using a framework such as ATT&CK [56]. The ATT&CK framework allows analysts to identify relevant attack threat groups and attack techniques and recommends specific detection approaches. A number of commercial tool suites map their capabilities to the ATT&CK matrix, allowing analysts to inform their detection choices. Repositories such as cyber analytics repository (CAR) [42], EQL [47] and SIGMA [48] are also sources of analytics mapped to ATT&CK TTPs.

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 [57].

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 and machine learning, and may even employ deception techniques such as honeypots/honeynets [26].

Threat Hunting

Threat hunting, or hypothesis-driven analysis, is an important aspect of analysis. In threat hunting, new intelligence, signatures, and analytics are employed to perform targeted searches for specific threat actor activity that may have been missed by the normal monitoring processes, often due to lack of information or because it was lost in the "noise" of events and alerts. Threat hunting is usually performed by a small team that constructs analytics or adapts them from open source or private repositories such as CAR [42], EQL [47], or SIGMA Rules [48].

Validating Defenses

CSOCs need to validate their defensive measures in a variety of ways. In addition to more traditional vulnerability and penetration testing exercises, mature CSOCs will regularly and systematically test detection, analysis, and response procedures via Red Team [58], Purple Team [59], and Adversary Emulation [60] exercises.

ABOUT THE AUTHORS

Clem Skorupka PhD is a Principal Cyber Threat Analyst at The MITRE Corporation. His work has spanned both operations and research, focusing on bringing new techniques and technologies to bear on problems in cybersecurity. He is a co-author of NIST's Special Publication 800-150 "Guide to Cyber Threat Information Sharing." He has worked extensively in computer security operations for MITRE, DoD and Intelligence Community environments, and civilian government sponsors, with a focus on cyber threat intelligence, attack detection, and event response.

Lindsley Boiney PhD is a Principal Cybersecurity Engineer at The MITRE Corporation, working on cybersecurity risk management and ways to improve defensive and resilient capabilities through threat-informed assessments. She emphasizes the intersection of information technology and behavioral science and believes that honing cybersecurity information sharing processes is as important as customizing tools and analytics. Dr. Boiney works across MITRE's sponsors to make it easier and faster for organizations to identify practical ways to improve their security posture and cyber resiliency; she has worked in domains including DoD Command and Control, Aviation Security, and Cybersecurity for both federal agencies and the nation's critical infrastructure.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®