Defending Against Ransomware: A Cyber Threat Intelligence Primer

Dept. No.: L512
Project No.: OVH001.A998.OP4.HE

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.

Approved For Public Release Distribution Unlimited Case Number 22-3770.

McLean, VA

Authors:
Kellyn A. Wagner Ramsdell
Matt Malone
Kristin E. Esbeck

November 2022

Table of Contents

1 Introduction

Ransomware is one of many cyber threats facing the healthcare sector, and these attacks can have immediate and widespread impacts on any organization. As noted in “The Evolution of Ransomware” (https://healthcyber.mitre.org/wp-content/uploads/2021/08/Ransomware-Paper-V2.pdf), modern ransomware operations not only lock victims out of their networks, making their files and programs inaccessible, but also often involve the theft of sensitive business information, personal identifiable information (PII), and protected health information (PHI) which may be sold to other malicious actors and used in future campaigns or even used to contact customers and/or patients directly.

Cyber threat intelligence (CTI) is intended to help an organization understand the current—as well as evolving—cyber threat landscape, and identify associated risks to the corporate network. This threat-informed defense approach can also include offering potential mitigation measures to reduce risk. CTI analysis should be actionable, timely, and tailored to an organization, with consumers ranging from senior decisionmakers (CEO, CISO, etc.) to network defenders (e.g., security operations center (SOC) analysts), as well as other business units.

A robust CTI program will generally follow the “intelligence cycle” – Planning and Direction, Collection, Processing, Analysis and Production, and Dissemination and Feedback – to ensure it is meeting the expectations of stakeholders and maturing to meet evolving demands.

This guide is intended to assist organizations interested in establishing a CTI program and those maturing an existing capability.

2 Planning and Direction – Identifying the Why and How

A CTI capability’s purpose and role within the broader cybersecurity function must be clearly defined. What questions does an organization need CTI to answer? Identifying and developing these questions determines the initial requirements that will guide a CTI capability’s operations and products. These requirements should be developed with guidance from the organization’s leadership, any current cybersecurity teams, and, particularly in a healthcare environment, clinicians using critical technologies and the teams managing them.

This process will also help identify the key stakeholders and consumers of CTI analysis, as well as help the team prioritize its various efforts. It can be used to determine the best formats and frequency of production, ranging from daily or weekly briefings to standardized written updates as needed for standing requirements as well as new/emerging issues. The requirements process can also be used to periodically assess the organization’s return on investment in its CTI capability. What products or briefings were most useful to a given stakeholder? The answers to that question provides insight on where to focus improvements.

After identifying a general purpose for the CTI function, administrative decisions need to be made. These include, but are not limited to, team composition/structure, placement within the organization, and budget. Some questions to consider include:

- Will the CTI capability be a separate business unit or housed within an existing business unit?
- Who will oversee the CTI team?
- What is the budget for this CTI capability?

- Are you intending to hire new personnel or train existing personnel? How does the budget account for the personnel/staffing considerations?
  - What levels of technical and analytic proficiency are necessary to produce finished intelligence products required by each stakeholder groups?
  - What existing technical skills already reside within the organization?
- Does the budget include considerations for training as well as tool and technology acquisition?

An important consideration is the amount of time needed to create a robust CTI function capable of supporting stakeholders with actionable, timely intelligence. The following processes take time to develop and refine, and most organizations will likely need to start with small goals for their internal CTI function and slowly increase over time. This process can take years to develop.

- Organizations in urgent need of a more advanced capability may consider hiring an outside vendor for CTI support, with the understanding an external team will likely not know the intricacies of the corporate network as well as an internal team.

3 Collection – Identifying Information Sources

A successful CTI capability will often be built upon the use of both internal as well as external data sources. Types of information collected and applied can range from indicators of compromise (such as IP addresses, email addresses, URLs, domain names, and file hashes) and observed adversary tactics and techniques (like those defined in the MITRE ATT&CK® framework; https://attack.mitre.org/) to more strategic context in terms of attacker attribution, campaigns, and goals.

Internal sources can include network logs, firewall logs, SOC alerts, suspicious emails, and other data sets that provide insight on potentially malicious activity on the organization’s cyber perimeter and, in some cases, inside the network. The CTI team can enrich this data by providing context for various stakeholders and propose defensive measures (including opening additional cybersecurity investigations and/or threat hunting initiatives). It requires close interaction with other network defenders, such as the SOC, to maintain awareness of current activity, with both/multiple teams often using network tools for overlapping purposes. If an organization does not already have a SOC, developing that capability is likely more important to the overall security of an organization than developing a CTI capability. Guidance for creating a SOC is available in MITRE’s *11 Strategies of a World Class Cybersecurity Operations Center* book (https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf).

In a healthcare delivery organization (HDO), business units responsible for medical devices may also be a key contributor to internal data sources, particularly given the unique nature of and inherent urgency in protecting these systems.

External information from free or commercial providers can detail new/emerging cyber threats, including new ransomware variants, other malware used in conjunction with ransomware operations, and new or rebranded threat groups. These data sources can include publicly available information pulled from the social media accounts of security researchers and major companies, cyber security company blogs/websites, news outlets, and industry alerts.

Government organization such as DHS/CISA, the FBI, and HHS also publish actionable alerts; organizations can review and subscribe to these at websites such as:

- HHS Health Sector Cybersecurity Coordination Center (HC3): https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- DHS/CISA “Stop Ransomware”: https://www.cisa.gov/stopransomware
- DHS/CISA “Alerts and Tips”: https://www.cisa.gov/uscert/ncas
- FBI Ransomware resources: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Commercial cyber security providers offer a range of threat-related reporting at different pricing structures; organizations should ensure these vendors provide information related to their priority CTI requirements.

Information sharing groups can be another valuable source of external CTI information for organizations, particularly in this case ones that address current threats to the healthcare sector. The Health Information Sharing and Analysis Center (H-ISAC; https://h-isac.org/), for example, provides email digests of relevant news items and, for a fee, an automated intelligence feed for members. The Cyber Health Working Group sponsored by the National Cyber-Forensics & Training Alliance (NCFTA) allows cyber professionals in healthcare organizations to directly share tactical cyber threat information (https://www.intelligence.healthcare/).

Healthcare organization should also consider either developing an in-house dark web monitoring capability or engaging with a commercial cyber firm that specialized in this area. Limited access dark web forums may contain information related to cybercriminal operations—including ransomware attacks—that may help organizations better prepare for or respond to malicious activity.

4 Processing – Information Management

Information management is a critical consideration given the potential volume of data a CTI team may acquire. Key points to consider include the types of data, how it is received (automated collection vs manual retrieval, for example), formats, and overall volume.

Many CTI teams benefit from having a threat intelligence platform (TIP) to integrate and aggregate data, so analysts can view and interact with the information. There are numerous paid and open-source TIPs organizations can use; common open-source versions include the Malware Information Sharing Platform (MISP) and OpenCTI.

The platform must be tailored by the team regardless of whether organizations use a paid or open-source TIP. This tuning process often includes vetting sources to make sure the information will help answer the team’s priority requirements and validating the data’s usability within the organization. Additional considerations include:

- Does the TIP include integrations for existing data sources?
- Can the TIP integrate with existing internal systems?
- What are the barriers to implementing the TIP?
  - Is the documentation for implementing the TIP complete?
- How long will it take the analyst(s) to tune the TIP?
- How will the TIP be maintained?
- What are the data storage requirements for the TIP?

For the healthcare sector, there may be additional policy, legal, and/or regulatory concerns associated with the storage of information, including but not limited to PII or PHI. An organization's legal and compliance representatives should be consulted to determine what specific considerations and measures need to be considered.

5 Analysis and Production

The CTI team should ensure its analysis is timely, relevant, accurate, actionable, and tailored to a specific audience; this often requires producing a blend of technical as well as non-technical narratives. Types of products can range from daily, weekly, and/or monthly written updates and briefings; ad-hoc production is also likely necessary to address newly identified or emerging threats. Understanding the needs of key stakeholders, as identified in Planning and Direction, should help shape the timing and format of CTI deliverables.

Analytic frameworks, such as the Diamond Model (https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf), the Lockheed Martin Cyber Kill Chain® (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html), and MITRE ATT&CK® (https://attack.mitre.org), can help organize analysis, meet analytic requirements, and provide a common terminology for a broad audience within the organization. These frameworks can be used to help track specific threat actors, campaigns, and malware/ransomware, and to prioritize identified threats. The CTI team should work with stakeholders to identify which framework(s) best support an organization's needs and then organize production around the identified framework.

CTI teams often use additional tools for analysis beyond the TIP and internal network defense products. Examples include link analysis tools (such as Maltego) and research platforms, such as internet infrastructure tools and social media monitoring tools.

As an organization's CTI capability matures, the team may wish to integrate structured analytic techniques and threat modelling to create deeper, more robust analysis. As with most cybersecurity disciplines, the CTI team should have training and professional development opportunities to enhance their analytic and technical skills.

6 Dissemination and Feedback

CTI product dissemination depends on the recipients, product format, data sensitivity, and any technology limitations. Some organizations prefer a "push" dissemination method, where finished CTI products are delivered automatically, while others tend towards a "pull" method, allowing customers to access a common portal or database to review and read products of interest.

- Regardless of the customer dissemination method used, the CTI team should maintain a central repository of its finished intelligence products. This database provides a historical record of cyber threats to the organization, helps measure CTI maturity over time, and serves as a training resource for new team members.

Products should be clearly marked to delineate any sensitive information; many organizations use the Traffic Light Protocol (TLP) marking system (https://www.first.org/tlp/), which consists of four main labels:

- TLP:RED – for individual recipients only; no further disclosure. Recipients may not share this information with anyone else.

- TLP:AMBER – Limited disclosure; recipients can only share this information on a need-to-know basis within their organization and, in some cases, clients.
    - TLP:AMBER+STRICT is a subcategory that limits sharing to within the organization only.
- TLP:GREEN – Limited disclosure; recipients can share this information within their community. This information can be shared with peer organizations and ISACs, for example.
- TLP:CLEAR – No disclosure limits; the information can be shared publicly without restrictions.

As noted in Section 3 Collection, the CTI team will likely need to consult with an organization's legal and compliance representatives to determine appropriate labels for different sensitive information categories, particularly related to PII, PHI, and medical device vulnerabilities.

Organization may also consider creating a standardized process for rapidly reviewing and approving the release of CTI information with peer organizations and ISACs, to help promote a community defense approach against shared cyber threats.

Consumer feedback on CTI products is critical to ensuring stakeholder needs are being met. Feedback should be designed to assess the quality, timeliness, relevance, clarity, and actionability of published CTI. It can be collected through surveys attached to CTI products, direct contact with the CTI team or its management (i.e., a designated CTI feedback email address), or periodic meetings with customer groups.

7 Process Improvement

The first step for process improvement involves documenting all internal CTI processes. This documentation provides the baseline for an assessment of the current state of a CTI program. Organizations can then review the results of feedback to identify processes and products in need of improvement. Stakeholder feedback is critical to CTI program process improvement. Addressing feedback may require streamlining production processes, acquiring new data sets, getting rid of old data sets, adding more technical knowledge to the team, or building new relationships.

Organizations can also follow a more structured assessment methodology. The United Kingdom nonprofit company CREST provides a CTI Maturity Assessment Tool organizations can use to assess their program and identify improvement opportunities. The tool is formatted as a questionnaire in a Microsoft Excel spreadsheet and provides wide coverage of the many components of a CTI program; it does not, however, go into great depth on specific improvement processes. Organizations interested in using the CREST CTI Maturity Assessment tool can access the resource here: https://www.crest-approved.org/cyber-threat-intelligence-maturity-assessment-tools/.

8 Integration Across the Organization

The CTI capability can and should be used to support a variety of functions within an organization, including incident response, defense operations, threat hunting, vulnerability management, leadership awareness/decision making, risk management, fraud prevention, brand/reputation protection, and product acquisition. Integrating with these business units throughout the CTI function's lifecycle will help ensure organizations receive the greatest return on investment. Potential questions to assess integration are listed below.

- How does CTI inform risk management decisions?
- How does CTI inform threat hunting, adversary emulation, and/or penetration testing of the organization's network?
- Are CTI findings used to inform and prioritize patch management activities?
- How does CTI analysis inform incident response processes and procedures?
- How is CTI used to inform business decisions related, but not limited to acquisitions, product development, and supply chain security?
- How is CTI used to protect research, development, testing, and evaluation projects, particularly related to medical devices?

Additional questions may apply depending on the organization's structure, activities, and business units.

9 Conclusion

A CTI capability can help organizations take a threat-informed defense approach to protecting itself from a wide range of malicious cyber activity, including ransomware. Organizations can be better prepared to prevent, detect, and respond to threats when CTI is implemented and integrated within the broader cybersecurity function. The key to a successful CTI program is having a clear mission and set of objectives, as defined by the stakeholders, and appropriate resources for associated personnel and tools. Organizations uncertain about whether to start or further develop a CTI program are encouraged to discuss this capability with their peers to gain additional perspectives, considerations, and best practices.

10 Bibliography

The MITRE Corporation, “11 Strategies of a World-Class Cybersecurity Operations Center”, McLean, VA, March 2022, https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf.