Cyberthreat Intelligence as a Proactive Extension to Incident Response

Cyberthreat intelligence (CTI) is one of the latest buzzwords in the information security industry. As a fairly new resource in the cybersecurity tool kit, it has not yet reached maturity, but it is used by governments, financial services, banking, insurance, retail companies, ecommerce, healthcare, manufacturing, telecommunication and energy enterprises.[1] Threat hunting is the activity associated with identifying the threats to an organization and its critical digital assets and acquiring the intelligence to combat them.

Organizations use CTI to understand the threats that have, will or are currently targeting the organization. It functions as a proactive extension to incident response by leveraging the output from existing cybersecurity monitoring tools. The information obtained from CTI is used to prepare for, prevent and identify cybersecurity threats that are trying to take advantage of valuable data. CTI can also be described as evidence-based knowledge about adversary motives, intents, capabilities, enabling environments and operations. CTI can be focused on a single cybersecurity event or a series of events or trends, and it provides advisory and reactional information to the defender.

There are many types of cyberthreats that can cause concern for an organization. Gathering and analyzing information about the source of such threats helps to combat any advanced persistent threats (APTs), distributed denial-of-service (DDoS) attacks and web application attacks (WAA) that may occur.

The resources available to counter cybersecurity threats are numerous and cover a wide range of options, including threat modelling,[2, 3, 4, 5, 6] software tools,[7, 8, 9] open-source threat information feeds[10, 11, 12, 13] and vendor services.[14] Industry surveys,[15, 16] professional associations[17, 18] and CTI guides[19, 20, 21, 22] also provide information and guidance to address threats.

The goals and objectives of CTI include reducing exposure to internal and external threats, learning the attack surface, determining dwell time from infection to detection (i.e., mean time to detection [MTTD]), enumerating the time to containment/spread prevention, and estimating the number of breaches and infections. Achieving these goals can keep an organization functioning smoothly in the face of a threat. Identifying the indicators of compromise (e.g., known attacks, incidents/events) and the attacker's

Larry G. Wlosinski, CISA, CRISC, CISM, CDPSE, CAP, CBCP, CCSP, CDP, CIPM, CISSP, ITIL v3, PMP
Is a senior consultant at Coalfire Federal. He has more than 22 years of experience in IT security and privacy and has spoken at US government and professional conferences on these topics. He has written numerous magazine and newspaper articles, reviewed various ISACA® publications, and written questions for the Certified Information Security Manager® (CISM®) and Certified in Risk and Information Systems Control® (CRISC®) examinations.

digital footprint are also important objectives for an organization to use to defend themselves. Determining threat actor behaviors and adversary tactics, motivations, infrastructure, methods, and procedures can provide strategic and tactical information that the organization can use to combat them.

These CTI goals and objectives can be difficult to achieve due to the challenges inherent in data and information gathering, technology, analysis, information sharing, management, communication, and staffing; however, it is important to understand them and, ultimately, defeat them to reduce the amount of effort needed in implementing and maintaining a CTI program.

Challenges in Data and Information Gathering

The most important components of CTI are data. The key areas of concern are data quality, the relevance of threat data, and the timeliness of threat data, and the intelligence obtained. Challenges in gathering data come in a variety of forms, and the top concerns are data quality, aggregation, validation and normalization.

Data quality refers to the cleanliness and quality of data, which can be improved by automatically identifying and removing expired indicators of compromise (IOCs), disregarding stale data and removing undependable raw data. Other factors that affect data quality include:

- CTI vendors that use an obsolete detection mechanism such as hash-based detection
- Threat applicability to certain industries
- The extensiveness of data coverage (i.e., Do the data contain useful information?)
- False threat reports filed by attackers to mislead CTI users

Data quality can be inhibited by an organization's implementation of preventive or protective measures that prohibit the revelation of data concerning classified or sensitive incidents.

Data aggregation is a challenge due to the diverse intelligence sources, differing delivery mechanisms (e.g., format, software, tools) and duplication of data. Because threat intelligence sources are diverse, they can be difficult to simplify and convert to a usable format. The huge volume of data available for aggregation, storage and efficient querying and the fact that some data may be encrypted are other factors. Location-based data (e.g., country, region) may not be relevant and should be excluded.

"DATA VALIDATION INVOLVES THE ELIMINATION OF FALSE POSITIVES, REMOVAL OF NONRELEVANT THREAT INTELLIGENCE AND DATA AUGMENTATION FOR ANALYTICS AND REPORTING."

The wide range of collection methods (i.e., automatically collected, community sourced, professional intelligence collection) also makes aggregation a challenge. Data delivery mechanisms include web-based protocols such as HyperText Transfer Protocol (HTTP) and File Transfer Protocol (FTP), which are useful for sources of information, but not all CTI systems are designed for them. Either the data sources need to provide more formats or the receiving software needs to be able to receive it by design.

Data validation involves the elimination of false positives, removal of nonrelevant threat intelligence and data augmentation for analytics and reporting. Data privacy and legal issues may also impact availability and usage of the data available.

Normalization and correlation is another challenging area due to inconsistent data formats. If one set of data is delivered as an unstructured PDF but another takes the form of Structured Threat Information Expression (STIX), identifying genuine threats can be difficult. The challenge is compounded when assembling and comparing information from internal and external data sources. There are also new vendor-specific data structure formats to consider.

Recommendations for data and information gathering include collecting the most useful intelligence, having providers prepare intelligence into a usable format and level of detail for each type of use, and avoiding wasting time and money by collecting and disseminating trivial data. Evaluating data feeds in relation to data sources (specific industry), ensuring transparency of data sources (to prevent intelligence poisoning), and establishing policies related to the unique data to be used, frequency of data by source, and targeted measurable results are also important.

Technology Challenges

The variety of technologies associated with CTI provides challenges with regard to tools, machine learning (ML) and analytics, integration and interoperability, standards, automation, and attack surfaces. The following explains each of these challenges briefly:

- **Tools**—Many cybersecurity professionals are working with outdated security information and event management (SIEM) tools and a security operations center (SOC) infrastructure that is not suited for easy data acquisition. As a result, a lack of confidence in the ability of tools to catch applicable threats requires a change in approach and methodology.
- **ML and analytics**—Translating tacit knowledge from ML will be a challenge for years to come. Containment of attacks and eradication of vulnerabilities continually grow more difficult and increase the volume of data to be processed. In addition, it is difficult to adjust ML to new tactics and techniques that exploit weaknesses in current security defenses.
- **Integration/interoperability**—Integration of malware sensor output and reports can be difficult due to incompatible software interface protocols and formats.
- **Standards**—Agreements and standardization related to data produced by many sources are not in place to aid in the implementation of an organization's CTI program. There have been some efforts to create CTI standards by the European Union Agency for Cybersecurity (ENISA),[23] but they only address certain aspects such as information sharing.
- **Automation**—The absence of automation from technical identification of targeted areas to consolidated and easy-to-understand reporting to the C-suite is a challenge for CTI managers.
- **Attack surfaces**—The attack surface has been expanding from servers, workstations and laptops and now includes mobile devices (e.g., cell phones, tablets), data hosted in the cloud, the Internet of Things (IoT) and employee information posted on social networks. As a result, better endpoint detection and response solutions are needed to aid in threat identification.

These CTI-related technologies and standards need to be compatible in order to integrate the data from data-gathering tools on the network. These tools include endpoint detection and response (EDR), SIEM, next-generation firewall (NGFW), intrusion prevention systems (IPS), antivirus (AV), web application firewall, secure web gateway (SWG), network IDS/network detection and response (NDR), antiphishing, or other messaging security software, vulnerability management and file activity monitoring.

One recommendation is to improve the ability to integrate threat intelligence data by having vendors add new interface capabilities (i.e., expand available import and export file formats) to their products to simplify interoperability and reporting.

Another recommendation includes keeping up with technology by segmenting networks and device types, such as scanners, desktops, systems, IoT devices, mobile devices, printers/copiers and other attack surfaces. Implementing a dedicated threat intelligence platform focuses a CTI program and makes implementing CTI easier.

The CTI community can work with standards organizations such as ENISA and the US National Institute of Standards and Technology (NIST) to standardize and share ML searching and correlation techniques and establish an agreed-upon set of CTI-focused data formats and logic to support interoperability between tools and data feeds.

Challenges in Data Analysis

The challenges associated with data analysis include the following:

- Detection of advanced threats (hidden, unknown, emerging), which exposes possible targets
- Identifying new adversaries that may target an industry
- Searching for applicable and actionable information
- Overcoming fatigue due to large volume and too many platforms
- Not having the tools for threat hunting investigations

Improving awareness by identifying and monitoring the applicable threat actors can help organizations address these challenges. Preparatory actions such as obtaining the right tools and data feeds, and training CTI staff on new tools, added feeds and existing organizational mechanisms, are also good practices that add to the CTI program capabilities and usefulness. Training incident response staff on CTI techniques, tools, resources and methodology also help to strengthen the organization's CTI program.

Understanding how a malware package (such as ransomware) acts to exploit vulnerabilities helps to create a threat hunting package to find the software and identify its actions. Sharing this hunting package is another way of combating automated threat actors.

Challenges Associated With Information Sharing

Information sharing between vendors and other providers is not always effective due to concerns about the potential misuse of data, the privacy of corporate data, possible data breaches, corporate liability, a lack of trust in the receiver, EU General Data Protection Regulation (GDPR) exposure, a lack of expertise in threat intelligence and a lack of value to share.

Quality vendor information can be another area of concern because the provider may not be transparent about their sources. Data provided by the producer, vendor or organization may not be as complete, applicable or inclusive as needed, and vendor reports and feeds may be focused on specific target audiences, such as government, banking and finance, cybersecurity service providers, or technology.

"QUALITY VENDOR INFORMATION CAN BE ANOTHER AREA OF CONCERN BECAUSE THE PROVIDER MAY NOT BE TRANSPARENT ABOUT THEIR SOURCES."

In addition, data from sharing groups may not be correlated; data may be just a simple feed from a dedicated data acquisition tool. There could also be significant discrepancies between intelligence estimates. The reports and observations may be stale and would contribute only to the volume, confusion and complexity of the analysis. The information shared about internal Internet Protocol (IP) sources may be of no value to other users or communities. To make matters worse, data-sharing parties may be malicious and provide false data, which could poison the CTI community data.

Recommendations to improve information sharing include vetting members of the sharing group prior to admission to the group, implementing some type of multifactor authentication (MFA) for member access, improving the categorization of the data provided (e.g., target group, event or observed dates), increasing product interoperability via multiple download formats and monitoring/validating the information submitted for sharing.

Management Challenges

The top challenges for management can be categorized as strategic, operational and technical.

Strategic challenges include not having clear priorities for investment and executives not understanding the technical issues. Operational challenges include the time-consuming effort to reconstruct attack vectors and the difficulty in identifying damage and if there are additional breaches. Technical challenges include verifying the source information to prevent false positives; prioritizing software patches, replacements and upgrades; and managing the volume of alerts to investigate.

Other management challenges include lack of budget, a lack of collaboration across departments, aligning the threats according to the needs of the organization and the organization's infrastructure, and inadequate (i.e., late, irrelevant or not actionable) strategic and operational reporting. Fortunately, there are actions that can be taken to help address these management challenges:

- Creating a budget that covers threat hunting and performing attacker investigations
- Keeping management informed of the number and types of attacks (this will help with future budget requests)
- Organize the information by type for ease of handling (e.g., credit card and financial account data, personal information, intellectual property, confidential business information, credentials and IT systems information, operational systems)
- Obtaining threat intelligence feeds after carefully investigating what is available and recommended by similar organizations
- Conducting an analysis to understanding an adversary's motivations, infrastructure (if possible) and methods of attack. Information sharing and analysis centers/organizations (ISACs/ISAOs) can help.

Two types of vendors deserving of careful research are security product and security service enterprises. Security product enterprises typically design their solutions to only support their products and may not optimize other organizations' security architectures or programs. Security services enterprises may have a regional focus, whereas CTI may need to be collected and assessed on a global basis. If this is the case, multiple sources will need to be obtained.

> "STAFFING CHALLENGES CAN BE OVERCOME BY ESTABLISHING A THREAT HUNTING TEAM, MAKING CTI A PRIORITY FOR THE SOC AND TRAINING THE SOC STAFF ON THE PURPOSE OF THE THREAT HUNTING TEAM."

The Communication Challenge

Communication between organizational stakeholders is another challenge. The security operations center (SOC) and incident response (IR) teams want intelligence alerts on newly emerging threats and adversaries delivered as soon as the information is available so they can react immediately to zero day and other types of attacks. IR and forensics teams need a comprehensive analysis of malware and cyberattacks as soon as all the details are available. Chief information security officers (CISOs) and IT managers need summary information about malware and attacks, statistics and trend data, and weekly or monthly reports. Executive managers need quarterly, high-level summaries tied to business issues and immediate assessments of breaches and security issues—especially when organization-oriented reports appear in the press. Timely and accurate information can help provide answers to questions from the chief executive officer (CEO), members of the board of directors and the press.

To minimize confusion, communication should be concise (e.g., a one-page memo or a handful of slides), be free of technical terms and jargon, explain issues in business terms (e.g., direct and indirect costs and impact on the business and reputation), and include a recommended course of action.

It is advisable to develop internal analytics for management reporting and provide actionable intelligence. Ideally, information should be prioritized, show response times, summarize the findings and present the organization's threat posture.

Also, it is a good practice for an organization to participate in ISAC/ISAO or other industry sharing groups to aid in understanding the threats, their applicability and the information available.

Staffing Challenges

There are two main CTI staffing challenges due to the increased complexity and volume of analysis and work performed. The first is having insufficient staff trained on CTI tools and resources or how to perform threat analysis (i.e., threat hunting) to utilize CTI effectively. Formal CTI training can be obtained from organizations such as the SANS Institute,[24] ENISA[25] and the EC-Council.[26]

The second challenge is maintaining staff to perform the CTI work of data gathering and analysis, running the tools, conducting risk mitigation, reporting activity, and advising management. These skills are needed and complement the incident response and forensic staff skill set.

> "BECAUSE CTI IS NOT FULLY MATURED AND THE ATTACK SURFACE IS EXPANDING, THERE ARE MANY CHALLENGES THAT NEED TO BE ADDRESSED AND SOLUTIONS TO BE IMPLEMENTED."

Staffing challenges can be overcome by establishing a threat hunting team, making CTI a priority for the SOC and training the SOC staff on the purpose of the threat hunting team. It is also helpful to train the security assessment staff on CTI and potential weaknesses, as it aids the assessment team in determining if the CTI program is current and effective.

Conclusion

The intent of CTI is to use current cybersecurity monitoring tools with additional resources such as vendor data feeds to identify the threats most applicable to an organization. Because CTI is not fully matured and the attack surface is expanding, there are many challenges that need to be addressed and solutions to be implemented. As CTI develops, AI may be used to automate some of the conversion, correlation, data enrichment, forecasting and reporting aspects of CTI. A global effort and coordinated methodology is needed to combat the many threats and threat actors that appear to be constantly increasing. The recommendations discussed can enhance a threat management program and the CTI industry in general.

The other important piece of CTI is reporting. The best intelligence reporting occurs when providers are monitored for changes to their software, services and sources, and network infrastructure is monitored for modifications that may aid or inhibit a CTI program. Vendors do not want to provide bad, incomplete, stale or erroneous intelligence, but vigilance is the key.

Endnotes

1 Cybersecurity Insiders, *2020 Threat Hunting Report*, USA, 2020, *https://www.cybersecurity-insiders.com/portfolio/2020-threat-hunting-report-download/*

2 Gumbley, J.; "A Guide to Threat Modelling for Developers," martinFowler.com, 28 May 2020, *https://martinfowler.com/articles/agile-threat-modelling.html*

3 Shevchenko, N.; T. A. Chick; P. O'Riordan; T. P. Scanlon; C. Woody; *Threat Modeling: A Summary of Available Methods*, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Pennsylvania, USA, July 2018, *https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf*

4 Gonzalez, C.; "Six Threat Modeling Methodologies: Prioritize and Mitigate Threats," Exabeam, 6 July 2020, *https://www.exabeam.com/information-security/threat-modeling/*

5 Shevchenko, N.; "Threat Modeling: 12 Available Methods." Carnegie Mellon University Software Engineering Institute, Pittsburgh, Pennsylvania, USA, 3 December 2018, *https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html*

6 *Op cit* Shevchenko, Chick, O'Riordan, Scanlon and Woody

7 Marley, K.; "Cyber Threat Hunting: Tricks and Tools You Need," Gadellnet, 23 June 2020, *https://gadellnet.com/blog/cyber-threat-hunting-tools/*
8 Shivakumar, S.; "Threat Intelligence Tools," EDUCBA, *https://www.educba.com/threat-intelligence-tools/*
9 Mohammadi, A. K.; "Ten Top Tools for Threat Hunters from Black Hat USA 2018," Authentic8, 21 August 2018, *https://blog.authentic8.com/10-tools-for-threat-hunters-from-blackhat-usa-2018/*
10 Reback, G.; "A List of the Best Open Source Threat Intelligence Feeds," logz.io, 4 May 2020, *https://logz.io/blog/open-source-threat-intelligence-feeds/*
11 Banerd, W.; "Ten of the Best Open Source Threat Intelligence Feeds," D3 Security, 30 April 2019, *https://d3security.com/blog/10-of-the-best-open-source-threat-intelligence-feeds/*
12 SENKI, "Open Source Threat Intelligence Feeds," *https://www.senki.org/operators-security-toolkit/open-source-threat-intelligence-feeds/*
13 The Cyber Threat, "Cyber Threat Intelligence Feeds," *https://thecyberthreat.com/cyber-threat-intelligence-feeds/*
14 G2, "Best Threat Intelligence Services Providers," *https://www.g2.com/categories/threat-intelligence-services*
15 Lee, R. M.; *2020 SANS Cyber Threat Intelligence (CTI) Survey*, SANS Institute, USA, February 2020, *https://www.sans.org/reading-room/whitepapers/threats/2020-cyber-threat-intelligence-cti-survey-39395*
16 Shackleford, D.; *Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey*, SANS Institute, USA, 2017, *https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/CRN360/20170314_Survey_CTI-2017_LookingGlass.pdf*
17 National Council of Information Sharing and Analysis Centers (ISACs), *https://www.nationalisacs.org/*
18 The Information Technology—Information Sharing and Analysis Center (IT-ISAC), *https://www.it-isac.org/*
19 Friedman, J.; M. Bouchard; *Definitive Guide to Cyber Threat Intelligence*, iSIGHT Partners, USA, 2015, *https://cryptome.org/2015/09/cti-guide.pdf*
20 Open Source Researchers, *The Cyber Intelligence Analyst's Cookbook*, 2020, *https://github.com/threat-hunting/awesome_Threat-Hunting/blob/master/Training%2C%20Documents%20and%20Instructions/Files/The%20Cyber%20Intelligence%20Analyst%20Cookbook%20Volume%201%202020-THlink.pdf*
21 CyberEdge Group, *The Security Intelligence Handbook*, *Third Edition*, Recorded Future, USA, 2020, *https://go.recordedfuture.com/hubfs/ebooks/security-intelligence-handbook-third-edition.pdf?utm_medium=email&_hsmi=96974607&_hsenc=p2ANqtz-8nZ7Z6uVybOhpY1UcGjy9STS6FwBSLFmyC1zjXIYaBrBcS8mePmvNcMfWyfW0VYsEa84AiGNelh6XTBbpVkcAM6XIFpwXFhcEV2RBylSjeaBxx8IQ&utm_content=96974607&utm_source=hs_automation*
22 CyberEdge Group, *The Threat Intelligence Handbook*, *Second Edition*, Recorded Future, USA, 2019, *https://paper.bobylive.com/Security/threat-intelligence-handbook-second-edition.pdf*
23 Doerr, C.; *Cyber Threat Intelligence Standards—A High-Level Overview*, Delft University of Technology, Netherlands, 16 November 2018, *https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyber-threat-intelligence-standardization.pdf*
24 SANS Institute, SANS Cybersecurity Courses and Certifications, *https://www.sans.org/cyber-security-courses/*
25 European Union Agency for Cybersecurity, Trainings for Cybersecurity Specialists, *https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists*
26 EC-Council, Certified Threat Intelligence Analyst (CTIA), *https://www.eccouncil.org/programs/threat-intelligence-training/*