Cyber Threat Intelligence & the Defense Industrial Base

By: Charles DeBarber, Cybersecurity Advisor

What is Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) is an intelligence discipline that uses collection, refinement, and analysis of digital information to counter threats posed in the realm of cyberspace.

CTI helps detect and defend against cybercriminals, advanced persistent threats (APTs), and hacktivists, based on data collected internally, from open source, threat communities, or commercial products. CTI is composed of three categories: tactical, operational, and strategic.[1] Although each category is essential in its own right, this whitepaper will focus on threat intelligence sources and communities available to organizations in the Defense Industrial Base (DIB).

Why is CTI Important?

As poet John Donne famously writes, "No man is an island entire of itself."[2] It is an elegant way of saying that we never "go it alone." This thinking holds in DIB cybersecurity too, as we share the same threats and adversaries – especially with others like us. The DIB has APT groups targeting it and smaller sectors within it. By exchanging Indicators of Compromise (IoCs) and sharing intelligence regarding these APTs and cybercriminals, the DIB becomes better capable of defending its infrastructure.

Knowing an IP Address, unique user-agent string, or domain associated with an adversary can help you set up blacklists and your network monitoring to impede the adversary's efforts. CTI can potentially stop an attempted breach instantly.

Important Terminology for CTI

Here is a list of important terminology to understand CTI and what it provides.

Advanced Persistent Threat (APT) – APTs are persistent threat actors that often have the support of national or subnational groups. They can be foreign intelligence services, sophisticated cybercrime syndicates, and even extremist groups seeking notoriety. FireEye and MITRE are excellent sources for information about known APT Groups.

Indicators of Compromise (IoCs) – IoCs are pieces of metadata associated with the adversary. They can be precise IoCs (aka 'hard IoCs') as a unique e-mail address or broader IoCs that are not so unique in themselves (aka 'soft IoCs'), such as an IP Address Range.

[1] Security Intelligence at the Strategic, Operational and Tactical Levels, https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/
[2] https://www.poemhunter.com/poem/no-man-is-an-island

Cyber Kill Chain (CKC) – The CKC was developed by Lockheed Martin in 2011 and is the most popular attacker threat model used to map out the stages of 'hacking' a network. It has seven stages and is what most organizations base their CTI around.[3]

Information Sharing and Analysis Center (ISAC) – ISACs are nonprofit communities for the exchange of CTI and the promotion of cybersecurity collaboration. ISACs are excellent sources of IoCs and APT information. ISACs tailored to their communities (e.g., Electricity, Defense, Space, Healthcare) have their membership requirements.[4]

Security Information and Event Management (SIEM) – SIEMs are security suites that integrate network logs from numerous sources (e.g., IPS/IDS, Firewall Records, E-mail Enterprise, Web Traffic) to better assess and implement network management.

What Are Some Sources for CTI?

Simplified sources of CTI can be divided into three categories – *Threat Communities*, *Open Source Threat Exchanges*, and *Commercial Platforms*.

Threat Communities

FBI Infragard – The Federal Bureau of Investigation (FBI) provides a CTI and cybersecurity knowledge exchange free of charge to those with contracts with several critical infrastructure sectors. There are no membership dues for this organization.[5]

National Defense ISAC National Defense ISAC (ND-ISAC) – ND-ISAC is the intelligence sharing center for the DIB. They exchange threat intelligence, cybersecurity guidance, and are a great place for analysts to collaborate with other DIB partners to combat mutual threats facing them. This community has annual dues, and for most small companies (less than 500 employees), it costs around $3,000 a year. A company must hold a Department of Defense (DoD) contract or be a subcontractor on one to qualify for membership.[6]

Defense Industrial Base Collaborative Information Sharing Environment (DCISE) – DCISE is run by the Defense Cyber Crime Center (DC3) and offers DIB organizations an anonymous way to share CTI. Unlike the ISACs or FBI Infragard, there are reporting requirements to be part of the community.

[3] Cyber Kill Chain, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[4] Executive Order Promoting Private Sector Cybersecurity Information Sharing, White House, 2015
[5] FBI Infragard FAQ, https://www.infragardncr.org/faqs
[6] About ND-ISAC, https://www.isao.org/information-sharing-group/sector/national-defense-isac/

The DCISE community also produces FBI Flash Reports on more in-depth situations. They receive all of this at no cost.[7]

Open Threat Exchanges

AlienVault OTX – AlienVault OTX is an AT&T product. While the open threat exchange is free, its integration into your network's SIEM carries a fee. This resource is useful to see if an IP Address, e-mail address, domain, or hash has been flagged as malicious at any point. Their 'Pulses' is a threat feed where communities dump malicious data to share with the greater community, ranging from simple e-mail addresses associated with phishing scams to sophisticated state-sponsored APTs.

VirusTotal (VT) – VT is the most trusted source for malware IoCs in the industry. Although they are also a commercial product, it is free to query IoCs and get back a massive amount of data for your analysis. VT is an invaluable tool for a threat hunter and/or malware analyst.

Abuse.ch Suite – Don't let the quirky nature of the site fool you - this site is formidable. Abuse.ch is a nonprofit with a suite of CTI tools dedicated to tackling cybercrime. Its suite includes a massive malware library, blacklisted SSLs, a database of malicious URLs, and the popular Fredo Tracker that keeps an extensive list of known C2 networks.

MISP Threat Sharing – MISP (Malware Information Sharing Platform) is a CTI information exchange platform developed as shareware.

Have I Been Pwn'd? – HIBP is a popular site for finding out if your e-mail or e-mail domain has been subject to numerous data leaks over the years. For smaller organizations, the free alert webmasters can set up for their company domains is useful in combating phishing.

DomainTools – Domain Tools is an excellent resource for researching domains and can often tell you more than Internet Corporation for Assigned Names and Numbers (ICANN) alone. However, its best data (e.g., domain history, threat scoring, known subdomains) is part of its commercial version.

FireEye – FireEye is predominantly a cybersecurity assessment service but produces what is considered the best industry-wide report on APT groups.

Shodan.io – Shodan is a search engine for devices. Its scanners are "feeling out" the web around the clock to probe devices. Both cybersecurity experts and adversaries use Shodan to see what devices can be seen.

[7] Active Cyber, https://www.activecyber.net/krystal-covey-of-dcise-discusses-the-dod-dib-threat-information-sharing-program-with-active-cyber/

Commercial Platforms

Recorded Future – Recorded Future is a threat intelligence platform that can be tailored very specifically to your organization's intelligence needs and priority intelligence requirements. It has everything, from emerging threats to alerts, to doppelganger domains and uses of your trademarks.

DarkCubed (Dark3) – DarkCubed is a commercial-off-the-shelf (COTS) solution for organizations that outsource their CTI. DarkCubed provides its appliance to your network where it monitors, detects, alerts, and blocks threats based on CTI. The company has thoroughly integrated data analytics to categorize customer target sets, which makes a more sophisticated tool.

McAfee Threat Intelligence Exchange – McAfee has its suite of CTI feeds and tools and is a good option if the organization has other McAfee products (e.g., AVS, IDS/IPS, Drive Encryption, McAfee SIEM) to integrate with.

Silobreaker – Silobreaker is perhaps the broadest data aggregation tool available as it is not just for CTI, but for open-source intelligence (OSINT) in general. My personal experience with it was helping set up alerts for media or social mentions of VIP clients to assist their security staff.

Threat Intelligence Platform (TIP) – TIPs real strength is in its robust sources, but few seem unique to its platform. It is an "economy" choice for a platform and will integrate with your SIEM. It has tools that would assist in an incident response situation when trying to determine attribution (i.e., what adversaries may be behind the attack).

Digital Shadows – Digital Shadows is a platform that offers multiple services, including a threat intelligence platform to help customers understand adversaries, their behavior, and their tools. They provide weekly intelligence summaries that can be tailored to a customer's threat group.

Flashpoint – Flashpoint is currently a leader in the industry for cybercrime intelligence and supports several government contracts in that sector. Their Intelligence Platform is tailored to find the top threats to your industry and organization.

Verint – Verint integrates into a Security Operations Center's (SOC's) SIEM with constant threat intelligence metadata and methodologies. They have a strong presence in SCADA (Supervisory control and data acquisition) systems.

LogRhythm – LogRhythm is a SIEM suite based around CTI. It has a unique tool for detecting insider threat behavior with UserXDR - a user behavioral analysis tool that automatically identifies and prioritizes anomalous user behavior.

What is the best fit for my organization?

There is not a 'goldilocks solution' for everyone, but there are some important considerations:

1. If you employ a SIEM, does it have a native threat intelligence solution or offer an add-on for one? It might be more economical and practical to go with that solution.
2. Do you outsource your network defense solutions? There are multiple options for that of varying depth and cost.
3. Are you just an IT skeleton crew or a larger organization that runs an SOC or Cybersecurity Incident and Response Team (CSIRT)? Larger organizations have larger infrastructures that require larger CTI solutions.
4. How are you keeping up with emerging threats in the DIB community? No cost solutions like DCISE and FBI Infragard should be utilized by organizations of any size. ND-ISAC has annual dues. For organizations of 100+ people, it is an invaluable community to be a part of.

Disclaimer: Project Spectrum is an impartial, trusted source whose sole purpose is to protect the DIB and its supply chain. It has not been influenced by any outside vendor or compensated for any information contained in this report.

ProjectSpectrum.io Continuously Monitoring & Securing Cyber