Monitoring the Landscape of Cyberspace

By Ray Mollison

In my previous article, Building a Cadre of Cyber Intellectuals, it introduces Cyber Intelligence (CYBINT) as an intelligence discipline providing clarity to understand vulnerabilities, exploits, and threats in cybersecurity. Cyber Intelligence can help build a stronger cybersecurity posture by conceptualizing the cyberspace landscape in three levels: operational, tactical and strategic. This will provide to the decision-makers a comprehensive analysis of state actors' and non-state actors' capabilities, skillsets, and intentions of their cyber attacks.

This article will focus on Cyber Threat Intelligence (CTI), which is a sharing platform within a community on current and emerging cyber threat trends within businesses, organizations, and government entities. The future is uncertain if an impenetrable cybersecurity posture could ever exist or if there is a technical solution to stop cyber threats. It is going to take more than firewalls to stop malicious threats and attacks from penetrating computers and systems. To gain an upper hand on combating cyber threats, there is a need to understand the cyberspace landscape of vulnerabilities and exploits. The implementation of CTI could be a tangible solution to enhance the cybersecurity posture against cyber threats.

Gartner best describes Cyber Threat Intelligence as the "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard".[1] The collection of raw cyber threat information gathered to evaluate and aggregate actionable intelligence, CTI is performed through the lenses of the intelligence lifecycle: plan, collect, process, produce and disseminate information by focusing on identifying types of indicators of cyber threats such as Malware, Spear-Phishing, Password Attacks, Ransomware and Denial of Service (DOS).[2] These cyber threats are examples of what a business, organization and government entity become exposed to within their network daily. This highlights the importance in why networks need to be monitored and controlled to ensure computers and systems are secured against cyber threats.

CTI is the integration of human intelligence with technical intelligence, allowing an organization to concentrate on existing and emerging threats.[3] It is a forward leaning methodology in order to detect possible threat trends in real-time. To understand cyber threats, there are three factors to consider when assessing actors' motives, which are their Intent, Capability, and Opportunity.

- **Intent** is a malicious actor's desire to target your organization
- **Capability** is their means to do so (such as specific types of malware)
- **Opportunity** is the opening the actor needs (such as vulnerabilities, whether it be in software, hardware, or personnel)[4]

Understanding these three factors can add insight of current cyber threat activities and subsequently project future outcomes by analyzing the actors' actions, means, and needs. Defining the actors' motives will help understand their techniques, tactics, and procedures. The methodologies and motives of cyber attacks are the virtual fingerprints of cyber threats; therefore, utilizing a collaborative platform to share real-time threats will add clarity to the composition and characteristics of attacks. Using CTI, a Cyber Threat Analyst examines the actor's digital fingerprint through aggregated collection sources ranging from technical sources, open sources, and closed sources.[5]

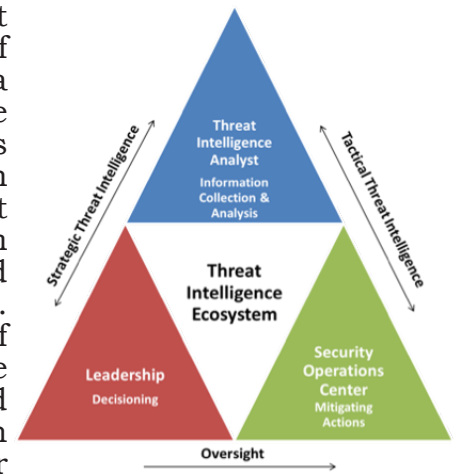
- **Technical Sources** include the Security Information and Event Manager (SIEM), Intrusion Detection Systems (IDS), firewalls, next-generation endpoint security platforms, and logs from any number of devices
- **Open Sources** such as published vendor reports, any number of free feeds of indicators, vendor vulnerability lists (Microsoft, Apple, Adobe, etc.), and media sources
- **Closed Sources** may include community mailing lists, or organizations such as Information Sharing and Analysis Center (ISACs)

There are many Threat Intelligence Platforms (TIPs) available for threat analysts to aggregate, correlate, and analyze threat data from multiple sources in real-time.[6] These platforms offer an advantage to Threat Intelligence Analysts to corroborate threat data to quantify the strength of identifying indicators of potential cyber threats. This platform is designed to be shared across small and large businesses, manufacturers, industries, banks, and government and private organizations in order to improve security within a trusted community. An example of a Threat Intelligence Platform is ThreatStream (Anomali), which was pioneered and founded by Greg Martin.[7] ThreatStream is a threat intelligence platform designed to Collect, Optimize, Integrate, and Share.[8]

- **Collect**: portal to access hundreds of threat intelligence feeds.
- **Optimize**: normalizes and optimizes intelligence, making it more actionable.
- **Integrate**: out of the box integrations with SIEMs, firewalls, and other systems.
- **Share**: offers two-way sharing and secure trusted circles for vetted collaboration.

The advantages to utilizing TIPs is that most organizations are currently using threat intelligence as a part of their cybersecurity program, where it has become valuable to their security mission, and it has become necessary to maximize the value of intelligence data.[9] TIPs have become critical to organizations that value a collaborative community and exercise innovative solutions to deter and combat cyber threats. However, there are disadvantages to using TIPs. They are overwhelmingly complex, have difficulty in platform integration with other security technologies, and suffer a lack of alignment between analyst and operational security events.[10]

The lack of professional expertise is one of the biggest hurdles to overcome in threat intelligence platforms.[11] For example, at the heart of a threat intelligence platform is the Security Operations Center (SOC) where technical information is collected in real-time. The SOC is the nucleus of threat intelligence to examine and evaluate current threat trends by technical experts who aggregate data into actionable intelligence.[12] The technical experts monitor an integration of systems in real-time from SIEMs to firewalls. The SOC will need technical experts with the right education and experience to correctly and accurately identify cyber threats. These technical experts must possess the technical knowledge and a broad range of capabilities and diversity of experiences.[13] Therefore, the pool of talent will be limited to a select few applicants making it hard to the fulfill roles and responsibilities for this position.



The figure[14] to the right details the process of threat intelligence as a visual representation. The diagram conceptualizes threat intelligence as an ecosystem referring to it as an interactive organism within interconnected communities or systems. The preservation of the Threat Intelligence Ecosystem is positioned in the center, which is governed by other pyramids: a Threat Intelligence Analyst who collects and analyzes information while the Security Operations Center monitors threats in order for the Leadership to make decisions. These pyramids fortify the epicenter of the ecosystem in conserving and preserving a healthy collection of Threat Intelligence for the Leadership to act upon. Most importantly, the Leadership will be able to understand how and what cyber threats impact the cyberspace landscape for the decision makers to accurately develop strategic and tactical intelligence frameworks. The maturity of strategic and tactical intelligence frameworks can help an organization focus their energy and resources to effectively and efficiently neutralize or degrade cyber threats while stabilizing the cyberspace ecosystem.

CTI will soon become a greater part of businesses, government and private organizations' cybersecurity portfolios, which can help identify the likelihood of future threats. The utilization of CTI can detect and prevent potential threats, which reinforce a strong cybersecurity posture by having the ability to counter threats before they materialize. The Threat Intelligence Platforms can strengthen the collection of data gathered in real-time for the intent to produce accurate and actionable intelligence reports to prepare and plan for potential cyber threats. This could lead to a stronger defensive security posture of developing Operational, Tactical, and Strategic Cyber Intelligence products that is adaptable and innovative against cyber threats. In addition, these platforms can assist in holistically comprehending the virtual landscape of potential threats deployed within cyberspace. Potential future threats will continue to grow and progressively cultivate new threats.

Ray Mollison is a field-grade officer in the Military Intelligence Readiness Command (MIRC) as an Army Reservist. He is pursuing his Master's degree in Cybersecurity at the University of South Florida. Ray enjoys working out and spending time with family.

[1]iSightpartners (2014) What is cyber threat intelligence and why do I need it? [online], http://www.isightpartners.com/ wp-content/uploads/2014/07/iSight_Parterns_What_Is_20-20_Clarity_Brief.pdf
[2]https://www.tripwire.com/state-of-security/security-data-protection/ cyber threat-intelligence/
[3]iSightpartners (2014) What is cyber threat intelligence and why do I need it? [online], http://www.isightpartners.com/ wp-content/uploads/2014/07/iSight_Parterns_What_Is_20-20_Clarity_Brief.pdf
[4]https://www.tripwire.com/state-of-security/security-data-protection/ cyber threat-intelligence/
[5]https://www.darkreading.com/vulnerabilities---threats/how-to-roll-your-own-threat-intelligence-team/a/d-id/1326445?
[6]https://en.wikipedia.org/wiki/Threat_Intelligence_Platform
[7]https://en.wikipedia.org/wiki/Threat_Intelligence_Platform
[8]https://www.anomali.com/platform/threatstream
[9]https://www.infosecurity-magazine.com/news/threat-intelligence-strategies/
[10]https://www.infosecurity-magazine.com/news/threat-intelligence-strategies/
[11]https://www.infosecurity-magazine.com/news/threat-intelligence-strategies/
[12]https://www.recordedfuture.com/security-operations-center-strategy/
[13]http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf
[14]https://semiengineering.com/threat-intelligence/

Photo credit: Tripwire.com