Threat Intelligence Programs

Why are threat intelligence programs important?

Individual threat actors and organized threat groups continue to attack financial institutions with increasingly sophisticated tools, sometimes backed by organized crime or even nation-state support. According to NIST, "Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. Given the risks that these threats present, it is increasingly important that organizations share cyber-threat information and use the community's experience to improve their security posture."[1] Properly developed and implemented **threat intelligence programs** help financial institutions gather, analyze, and act upon threat information before negative impacts occur. **Intelligence gathering and sharing** is a proactive process to stay ahead of attacks, whether it's a phishing campaign targeting employees, a ransomware event, or a nation-state threat actor probing the institution's network and systems. Without threat intelligence, institutions are effectively "flying blind" to a host of ever-changing and potentially devastating cyber threats.

Without threat intelligence, institutions are effectively "flying blind" to a host of ever-changing and potentially devastating cyber threats.

Threat intelligence program basics

Good threat intelligence programs contain four basic elements:

- **Information obtained from a trusted source,**
- **Channels to distribute information to the appropriate IT security personnel,**
- **Program to analyze and prioritize information based on the institution's own unique needs, and**
- **Acting upon applicable information in a timely manner.**

Types of threat information

NIST defines **"cyber-threat information"** as "any information that can help an organization to identify, assess, monitor, and respond to cyber-threats. These include:

- ***Indicators***, which are the system artifacts or observables that may suggest an attack is imminent, underway, or has already occurred;
- ***Tactics, techniques, and procedures (TTPs)***, which describe threat actor behavior;
- ***Security alerts, advisories, or bulletins***, which provide notification of vulnerabilities, exploits, and other security issues;
- ***Threat intelligence reports***, which are "prose documents" that describe TTPs, actors, targets, and other threat information; and
- ***Tool configurations***, which give recommendations for setting up and using automated collection, exchange, processing, analysis, and use of threat information.[2]

[1] National Institute of Standards and Technology. Johnson, Chris, Feldman, Larry, and Witte, Greg (Editors). "ITL Bulletin for May 2017: Cyber-Threat Intelligence and Information Sharing". May 2017.

[2] Ibid.

Threat intelligence resources

There are a variety of free and paid threat intelligence resources that financial institutions can leverage to gather this information. The most common sources include, but are not limited to:

- FS-ISAC and MS-ISAC: Information-sharing communities that deliver real-time alerts and sector-specific intelligence. U.S. institutions with less than $1B in assets can maintain a cost-free membership with FS-ISAC's Critical Notification Only Participant (CNOP) program.
- FBI InfraGard: Connects financial institutions with law enforcement for information sharing and early warnings
- CISA Programs and Alerts: Offers updates on vulnerabilities, malware campaigns, and best practices from the U.S. government
- Open Threat Exchange (OTX) and other community-driven threat exchange platforms
- Subscriptions to newsfeeds from industry cybersecurity websites
- Communications and alerts sent directly from applicable hardware and software vendors
- Vendor-sponsored CISO user groups

Understanding the institution's technology environment

Having a **mechanism to manage the myriad available threat information** is essential to navigate through the noise of irrelevant or untimely information. To make the most sense of threats that might impact the institution, it is important to remember a couple of key requirements. First, it is extremely beneficial to understand the institution's own operating environment. **Not all threats and vulnerabilities are applicable to every institution**, and the best way to sift through the noise that can accompany threat intelligence gathering is to understand the threats that are most relevant to your institution.

Second, when we think of potential impacts of threats, it is helpful to also understand the **interactions that assets have with one another within the institution's operating environment**. Is there an understanding of interdependencies between assets across different areas of the institution? Are there multiple areas within the institution that rely on a single application or piece of hardware (single point of failure)? Understanding not only the threats that exist, but also how these threats, if materialized, might impact overall operations is a good means of **triaging threat information and prioritizing responses and preparing recovery strategies for mission critical processes** within the institution. Because threats often require swift actions, it is important that IT security teams are well-equipped to **act upon threat intelligence information** once it's received, analyzed, and prioritized. Threat intelligence can provide timely data to enhance threat modeling activities for critical assets and can be a valuable input for incident and recovery scenario planning.

Information sharing

According to NIST, "Most organizations already produce multiple types of cyber-threat information that are available to share internally as part of their IT and security operations efforts." **When a financial institution participates in an information sharing mechanism, others benefit from "the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.** Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies." Moreover, "By correlating and analyzing cyber-threat information from multiple sources, an organization can also enrich existing information and make it more actionable. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread." Resources such as NIST Special Publication (SP) 800-150, Guide to Cyber-Threat Information Sharing, can assist institutions in forming and participating in cyber-threat information sharing activities.[3]

[3] Ibid.