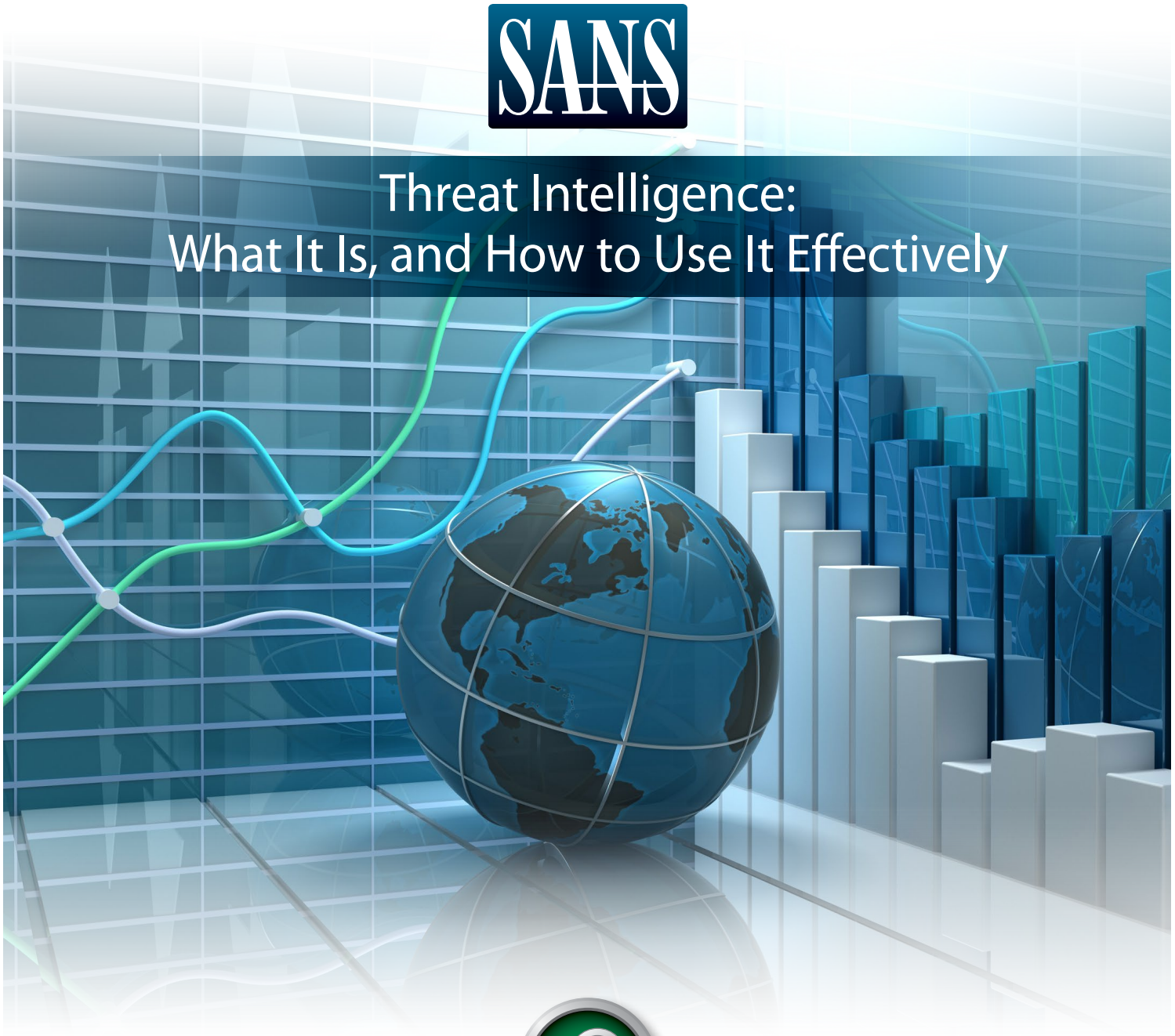

Threat Intelligence: What It Is, and How to Use It Effectively

A SANS Whitepaper

Written by Matt Bromiley

September 2016

Sponsored by
NSFOCUS

Executive Summary

In today's cyber landscape, decision makers constantly question the value of their security investments, asking whether each dollar is helping secure the business. Meanwhile, cyber attackers are growing smarter and more capable every day. Today's security teams often find themselves falling behind, left to analyze artifacts from the past to try to determine the future. As organizations work to bridge this gap, threat intelligence (TI) is growing in popularity, usefulness and applicability.

In its simplest form, TI is the process of understanding the threats to an organization based on available data points. But it goes beyond simply collecting data points; there must also be an understanding of how the data relates to the organization. Teams must combine data points with contextual information to determine relevant threats to the business. Furthermore, TI is useful to an organization only if it is actionable. If a team cannot determine how to best respond, combat or mitigate a threat to the organization, then the information provides little, if any, value.

This whitepaper seeks to help decision makers determine whether their organization is ready to incorporate TI into their security program or, for more mature organizations already leveraging TI, how to use it more effectively. We examine the following key points:

Defining TI

How to define TI for your organization, while ensuring that you set appropriate expectations.

Sourcing TI

How to source valuable TI, and best combine internal and external sources to meet your organizational needs.

Making TI actionable

How to implement intelligence findings throughout the organization versus just collecting data points.

TI can be an expensive undertaking. This whitepaper does not assume that an organization has the budget for a large, dedicated TI task force. Instead, it focuses on techniques for integrating and acting upon TI—information that should be of value to organizations of all sizes. It is prudent for all organizations to be aware of the current threats confronting them and do their best to protect the business by implementing a TI strategy.

What Is Threat Intelligence?

TI is the process of acquiring, via multiple sources, knowledge about threats to an environment. In May 2013, Gartner analyst Rob McMillan put forth an excellent explanation of TI as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."[1]

As an organization seeks to hone its information security team and harden its security posture, it is a natural step to consider the use of TI. Detecting incidents sooner, and potentially even preventing them, is the overall goal of TI. Mature information security teams often see TI as a way to bolster the environment and prepare for both known and unknown threats. As competitors suffer data breaches, executives and key stakeholders are coming to perceive cyber threats as imminent. Today, they simply want to know whether their organization is protected. However, TI should not be integrated into an organization's defenses without first defining what it is. Only with a clear definition can an organization do the following:

Part of defining TI is deciding what it is not. TI is not simply a list of atomic indicators that an attacker used at one point in time, without additional context into how the attack worked.

Defining Threat Intelligence

- Foster realistic expectations for TI implementations.
- Align those expectations with corporate cyber security goals.
- Identify where TI integrations will yield the most for the organization.

For example, consider an organization whose TI program consists of subscribing to external data feeds. The expectation would be that someone on the team will be tasked with maintaining those feeds. The organization may take things a step further and require the staffer who gathers the feed data to ensure that it is pushed out to the enterprise. However, the organization must also address questions such as "Where in the enterprise should those feeds be deployed?" and "Will information in the feeds compel actions such as reconfiguring perimeter defenses to detect specific attacks?" We will discuss the relevancy of TI in a later section.

Another organization might implement TI by building and maintaining a deep understanding of various threat groups and their tactics, techniques and procedures (TTPs). The information security team would be expected to understand who exactly may be targeting the organization and how they plan to do so. This advanced definition may come with the expectation that the organization is actively consuming and acting upon TI and prepared to combat advanced attackers.

[1] "Definition: Threat Intelligence," Gartner, www.gartner.com/doc/2487216/definition-threat-intelligence

Part of defining TI is deciding what it is not. TI is not simply a list of atomic indicators that an attacker used at one point in time, without additional context into the workings of the attack. It is not dated information that fails to help the organization protect itself or understand its attackers. And it is not a data source that is ignored. In the next section, we evaluate these and other points to highlight the importance of TI to an organization.

The Importance of Threat Intelligence

Executives increasingly see TI as a valuable tool. In the 2016 SANS Cyber Threat Intelligence Survey,[2] only 6 percent of survey respondents said they did not have a TI program in place, while 40 percent characterized their programs as immature but improving. Even more concerning, 27 percent of respondents admitted that their TI program either is just getting started or in an immature state (see Figure 1).

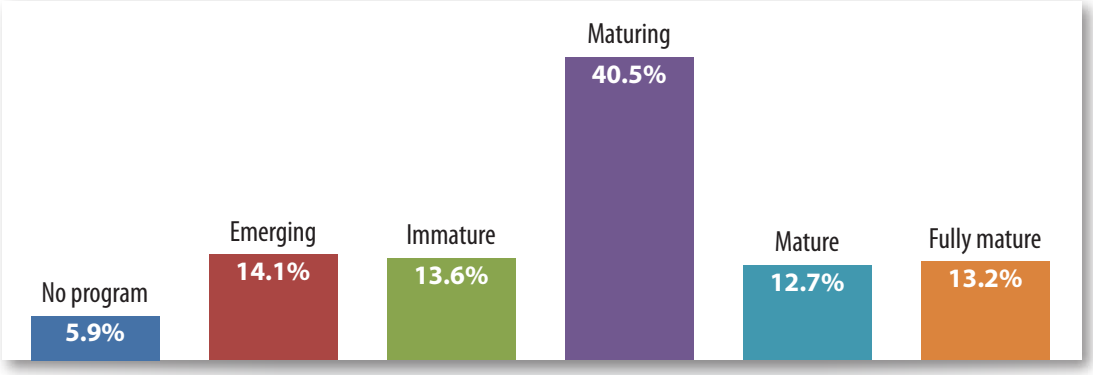

Figure 1. Maturity of CTI Programs[3]

In fact, the perception of TI is turning from one of luxury to necessity as information security professionals come to realize that attackers often have a better understanding of their organization's networks than they do. Oftentimes, as organizations uncover details from a breach, they find that the attackers successfully and quietly moved throughout the network without being detected—even with detection mechanisms in place.

[2] "The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing," August 2016, www.sans.org/reading-room/whitepapers/bestprac/state-cyber-threat-intelligence-survey-cti-important-maturing-37177

[3] "The SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing," August 2016, www.sans.org/reading-room/whitepapers/bestprac/state-cyber-threat-intelligence-survey-cti-important-maturing-37177, p. 3, Figure 2.

Attackers are evading whitelists, gaining privileged access and abusing network devices to maintain persistence. To keep up, teams are leveraging multiple tools to help them hunt for threats and detect them throughout their networks. Many have become convinced that, properly implemented, TI is one of the more valuable tools to help them better understand their attackers.

The growing embrace of TI programs is also a sign that information security leaders are gaining ground in their efforts to make key stakeholders more aware of the overall threat landscape. Security practitioners have been warning organizations about imminent threats for years, often saying breaches are not a matter of if, but when. It says something about growing security awareness that so many organizations are now willing to fund TI efforts in the hope that they will provide insight into an attacker group and their TTPs. In the 2016 SANS Incident Response Survey, 72 percent of organizations reported that they use TI within their environment.[4] In effect, organizations are confronting the questions "What if this happens to us?" and "Are we prepared?"

[4] "Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey," June 2016, www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047

Sources of Threat Intelligence

The first step for an organization that decides to enhance its information security capabilities with TI is to choose the sources of the intelligence. Sources can be grouped into two high-level categories: internal and external.

Internal Threat Intelligence

Data points and information that are garnered from within the organization itself constitute internal TI. As enterprises experience exploit kits, malware infections and other daily issues that can seem random and unconnected, they have an opportunity to build a profile of their environment by organizing such information into meaningful content. That process also gives the information security team the opportunity to learn how to turn unrelated or simple events into "enterprise intelligence."

The first step for an organization that decides to enhance its information security capabilities with TI is to choose the sources of the intelligence.

Oftentimes, gathering internal information is much easier than organizing and interpreting it. Many organizations strive to send mountains of data to a central aggregation point, such as a SIEM system. The central aggregation point must be tuned to accept the various types of data, and data must be indexed and available for query by the information security team. The team must also ensure that specific data points are being collected and alerted upon.

Consider, for example, a ransomware infection delivered via spearphishing that encrypts a file share, disrupting the normal course of business and potentially causing a financial loss. Despite those negatives, the organization does not consider ransomware a targeted threat, because the situation can be easily remediated. However, by applying a TI lens to the situation, the information security team may be able to identify the path the malware took to infect the original host and what chokepoints along that path failed to detect the malware.

The team can also identify the vulnerabilities exploited by the malware and observe the ease with which the malware could spread internally. By polling its aggregated logs, the team could identify whether the malware caused additional damage, still yet unknown. It could also use a trivial exercise to identify gaps in its data aggregation effort and put additional collectors at those data collection points. Building and maintaining a history of incidents within an organization is a critical first step toward building a successful internal TI team.

By cataloging details of the incidents, such as attack paths, vulnerabilities, malware and other network indicators, an internal team can start to recognize similarities between attack groups or malware families. This internal growth can also help the organization identify weak points, critical assets and priorities for security policy implementation.

External Threat Intelligence

Quite simply, this is intelligence that an organization acquires from outside itself. External TI can be further broken into multiple subgroups, including the following:

- Data subscriptions, also known as feeds
- Commonality, such as by industry or geographic location
- Relationships with government and law enforcement
- Crowdsourced platforms

Because external TI is often not specific to the organization, the security team must spend time evaluating the applicability of the intelligence. Some recommendations are included in Figure 2.

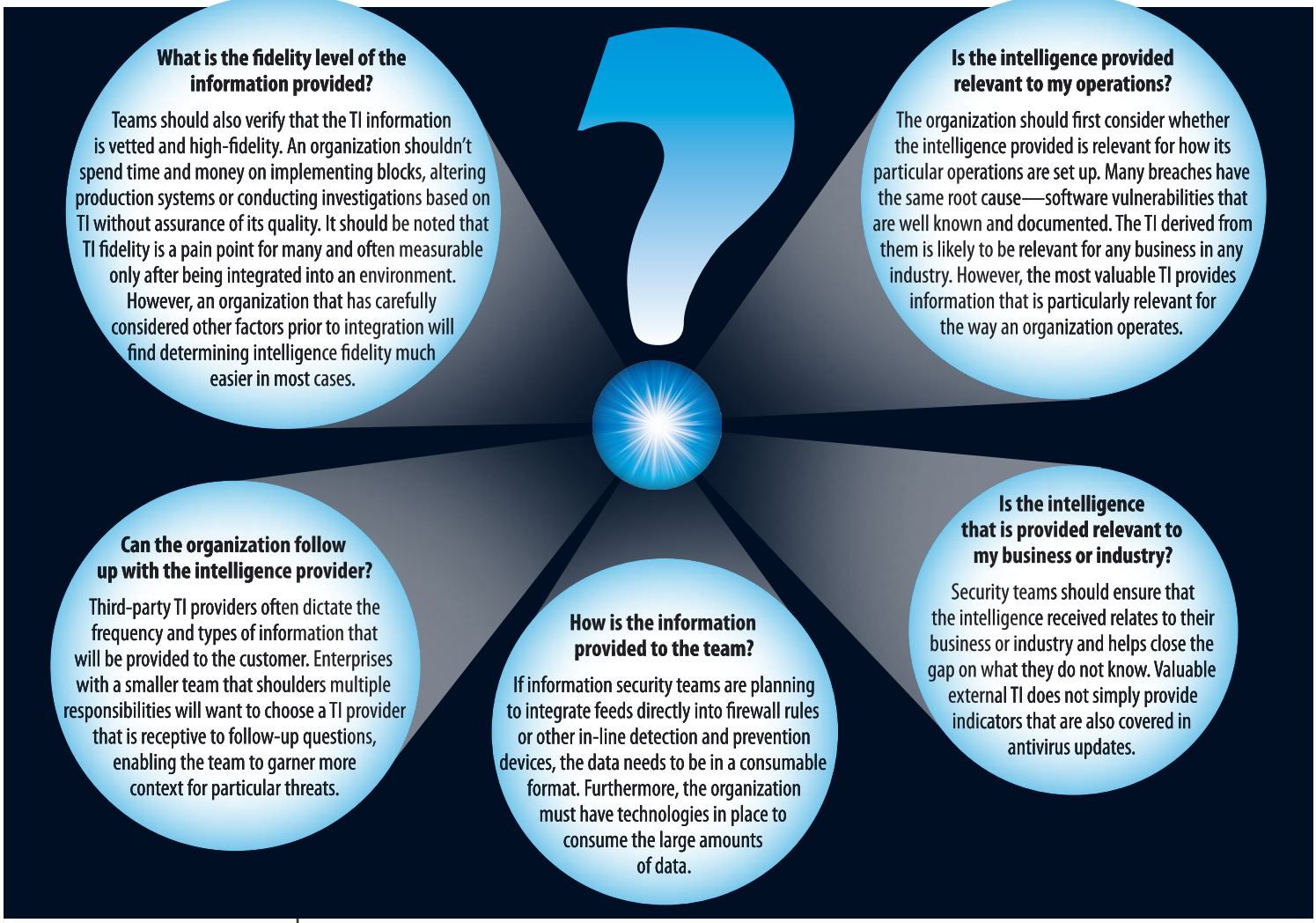

Figure 2. Choosing an External TI Provider

Data Feeds

Many TI vendors offer data feeds that set up a delivery mechanism for specific types of data at pre-determined intervals. These are widely used by information security organizations today (see Figure 3).

Are you using threat intelligence (TI) feeds to speed detection and response? ***Select the most appropriate.***

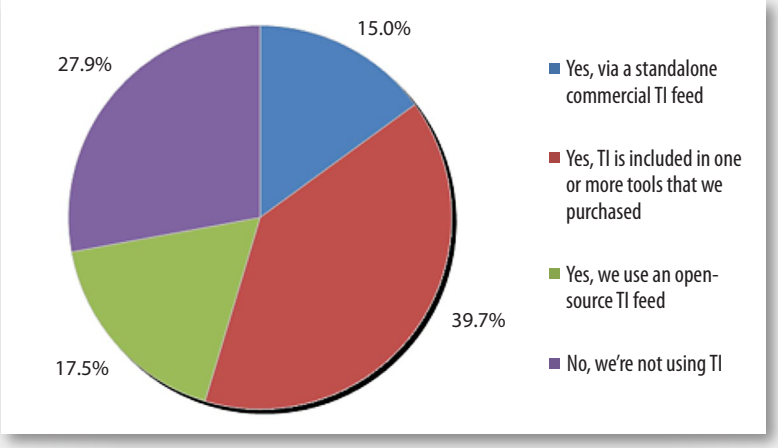

Figure 3. Use of Threat Intelligence Feeds[5]

Data feed sources can be further separated into subgroups and delivered in the following ways:

- Emails delivered at an interval, such as hourly, daily or weekly
- Subscriptions that provide lists of indicators, also delivered at intervals in various formats, such as JSON or CSV
- Scripts that utilize APIs to extract information from a data source, such as a database or website
- "Special releases," such as a public report from a TI provider

The value of a feed is realized only when the receiving organization *implements* the data provided into its tools, including firewalls, SIEM systems, endpoint agents and network-based security technologies. Data feeds may also include attacker TTPs or research reports. All of it must be consumed and acted upon by the receiving organization to extract its value.

[5] "Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey," June 2016, www.sans.org/reading-room/whitepapers/incident/incident-response-capabilities-2016-2016-incident-response-survey-37047, p. 14, Figure 9.

Open-source threat intelligence (OSINT) feeds are available as well. Some organizations that monitor for attacker activity, such as vulnerability scanning or spam emails, aggregate their data and provide it for free. Being low cost (possibly even free) and easy to ingest, OSINT feeds can provide value to organizations. Data is often made available in multiple formats, similar to commercial feeds.

But OSINT feeds have pros and cons. They are largely automated and can cause an increase in false positives. Furthermore, OSINT feeds are rarely investigation-driven and frequently rely on attackers performing a specific set of activities. However, as many attackers often exploit well-known vulnerabilities, OSINT feeds may help protect against groups scanning for these.

One reason crowdsourced platforms have become popular is that they may provide anonymous access methods. This may be useful for organizations that want to get particular TI but not reveal their company name and perhaps raise suspicions that they have been breached.

Commonality

Attack groups often target industries or services as a whole, as well as company by company. Organizations with similar interests, such as the financial community, have created industry-specific groups that facilitate the sharing of information. These groups, including Information Sharing and Analysis Centers (ISACs), often present findings or intelligence with higher fidelity than feeds. ISACs also help facilitate bidirectional sharing of information between the public and private sectors.

Relationships with Government and Law Enforcement

Many organizations also receive some form of TI and other benefits from relationships with government and law enforcement. For example, InfraGard is a partnership between the FBI and the private sector that provides a forum for private industry and law enforcement to confidentially share information about threats.

Law enforcement agencies have also been known to provide TI to organizations, but this knowledge often arises from evidence that a breach has occurred and can be accompanied by a request for further investigation. In some cases, the information provided by law enforcement is limited due to ongoing investigations or pending litigation.

Crowdsourced Platforms

Crowdsourced TI platforms can resemble commonality sharing but serve as hubs between multiple types of entities. One reason crowdsourced platforms have become popular is that they may provide anonymous access methods. This may be useful for organizations that want to get particular TI but not reveal their company name and perhaps raise suspicions that they have been breached.

As with data feeds, only a small portion of the breadth of information and intelligence in a crowdsourced platform may be applicable to the acquiring organization. For example, a crowdsourced platform may provide information on an advanced threat group that is actively targeting organizations in the energy sector and provide a description of TTPs, malware and high-fidelity signatures. For an organization in the retail industry, this industry-specific information may not prove to be useful in mitigating threats.

One potential drawback with crowdsourced TI platforms is that the value of the intelligence will suffer if members are minimally involved or the data they share is generic or misleading. If data is not curated or the platform is not well maintained, data could be misclassified. An organization relying on this approach may get unreliable information and waste time and resources looking for a nonexistent threat. When examining crowdsourced TI, organizations should analyze the frequency of information posted, the number of members and the reputation of the group maintaining the platform.

Combining External and Internal Sources

Both external and internal TI sources have potential applicability, but true TI harmony exists when an organization uses both sources simultaneously. This complementary nature is illustrated in Figure 4.

Figure 4. A Combined TI Approach

Although internal TI sources are better able to provide information that is highly relevant to the organization, external TI sources can help alert the organization to threats it was not previously aware of. These sources can also provide additional context the organization may not have. When external TI is coupled with internal TI, the organization may be able to shorten the time from infection to detection, and from detection to remediation.

Once an organization has laid the groundwork for a TI implementation by defining it, identifying sources and setting expectations, it must take steps to make TI actionable. Examples include:

- Incorporating TI into an organization's security posture
- Using TI to help drive investigations and response
- Using TI to look into the past and possibly see things that were missed in the absence of the TI
- Using TI to look into the future

Incorporating TI into Your Security Posture

One of the most logical places to begin acting upon TI is with the organization's overall security plan—its security posture. Security posturing often begins with determining what the business needs to protect and implementing policies and procedures to do so. TI can help the organization understand which areas of the business attackers are most likely to target and use that insight to more effectively protect key assets. For example, a hospitality chain may receive TI about an attack group that is targeting vulnerable payment card systems. The chain can then build continuity and contingency plans around high-value, essential targets. In this way, TI can help promote security measures such as the implementation of two-factor authentication or network segmentation.

An organization might also use TI to identify potentially critical assets that had not been internally perceived as vulnerable. Let's say that the hospitality chain receives TI showing that an attack group is attempting to compromise reservation systems to gain information on potential victims' whereabouts. Previously, reservations may have been seen as arbitrary data and not a critical asset.

Of course, this does not mean that TI should be the only benchmark of defense. It merely complements other ways of identifying the portions of a network or enterprise that need protection, as part of a well-balanced information security team's efforts.

Using TI to Help Drive Investigations and Response

A second important way for TI to give rise to action is to incorporate it into the information security and incident response (IR) team's daily activities. An organization's investigative teams, often comprising analysts, engineers and administrators, have a deep understanding of the organization's environment. They can quickly act on the information provided via TI to begin detecting compromises and better protect the environment. When an incident occurs, useful TI can help the IR team understand something about the threat actors and how they are conducting their attack.

For example, advanced attackers often follow regimens that make them easily distinguishable from other attack groups. TI can guide the IR team on which hosts to examine, what type of malware to look for, and what methods an attacker might be using to maintain persistence after infected machines have been powered down.

Using TI to Look into the Future

As organizations mature and TI becomes an integral part of day-to-day operations, advanced security teams can start to use TI to understand what the next threats will likely be. TI can help the security team identify changes in attacks and trends in attacker TTPs and plan accordingly for those changes. For example, attackers have recently increased their skills and utilization of Windows PowerShell. Attackers are adding tools and techniques to their arsenals that take advantage of the built-in scripting platform. Organizations can use the change in trends via TI analysis to identify what may be the next attack vector. They can use this knowledge to take proactive steps, such as increasing system logging or disabling unused technologies at the enterprise level.

Conclusion

TI is not a simple checkbox item. Establishing a program that learns about and acts upon threats to the organization takes time and effort. More often than not, teams that have put in the time have recognized a high return on their investment.

The first step is to define what TI means to the organization, keeping in mind that definition that will differ by company, industry, organization size and many other factors. This first step enables the information security team to establish measurable expectations, which will not only aid in determining whether the team has completed its tasks, but also help guide the team as it builds its program. As teams assess external TI offerings and capabilities, having a clear goal in mind helps them make the right decisions and acquire the pertinent information.

The relative importance of TI is a matter each organization must weigh against its budget, security plans and current capabilities. Everyone in information security wants the best of any technology and an unlimited budget, but few get all they want. In many cases, adding TI to the security program may seem like a long-term goal. However, being informed about the tools available—how they can help and how they can be implemented—will help a team prioritize goals and do its best to protect the business.

About the Author

Matt Bromiley, a SANS GIAC Advisory Board member who holds the GCFA and GNFA certifications, is an up-and-coming forensics instructor. A senior consultant at a major incident response and forensic analysis company, he has experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, and network forensics, as well as memory analysis and network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, sharing with others and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

NSFOCUS

NSFOCUS was founded in 2000 to provide enterprise-level network security solutions and services primarily in the Asia/Pacific market. The new NSFOCUS International Business Division (IBD) brings advanced security solutions to the Americas, Europe, the Middle East, and Southeast Asia.

Its research and development teams focus on vulnerability analysis, threat understanding and security intelligence, while providing core technical support for NSFOCUS products, solutions and services. This long-term commitment has helped its customers maintain high levels of business operations and ensured that its online business systems always remain available.

With offices in the United States, Japan, Europe, China and Southeast Asia, NSFOCUS supports more than 27,000 customers, including four of the five largest financial institutions and some of the largest telecom carriers, data centers, cloud service providers, managed security services providers and enterprises in the world.