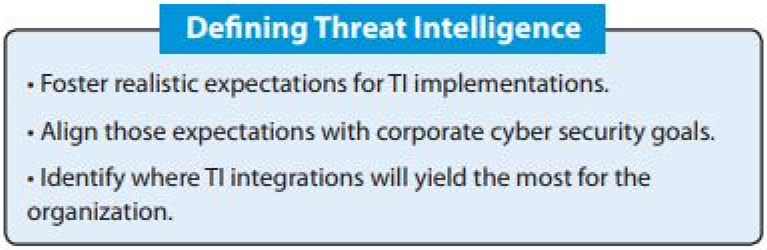
What Is Threat Intelligence?

Threat Intelligence 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:



Defining Threat Intelligence

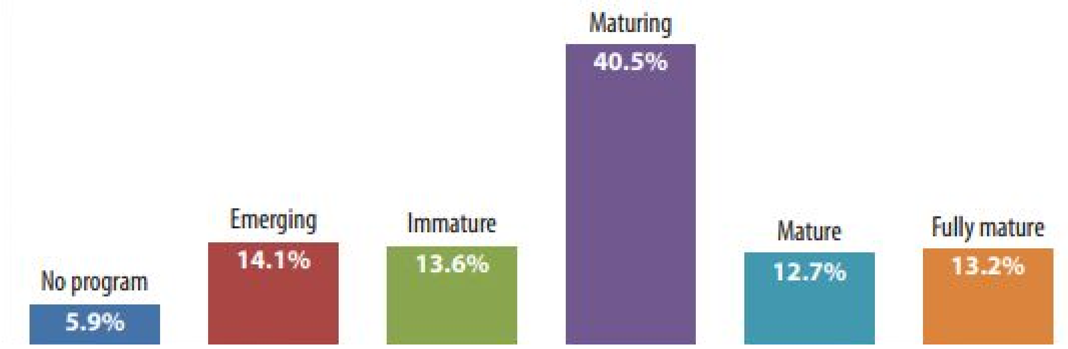
- Foster realistic expectations for TI implementations.
- Align those expectations with corporate cyber security goals.
- Identify where TI integrations will yield the most for the organization.

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.

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

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).



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.

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?”

Terminology

Advanced persistent threat (APT): A targeted cyberattack that leverages multiple tactics to gain network access and remain undetected for extended periods.

Application programming interface (API): A set of documented commands, functions, and protocols that allow software programs to communicate and share data.

Attribution: Linking an attack to a specific threat actor.

Command and control (C&C) server: A server operated by a threat actor to provide instructions to bots or to communicate with compromised systems inside the network. Also known as a CnC or C2 server.

Cyber threat intelligence: Knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise.

Distributed denial of service (DDoS) attack: A cyberattack intended to disable a targeted network or host by flooding it with requests from multiple computers.

Hacktivist: A threat actor who uses cyberattacks to express political or ideological beliefs or to damage opponents.

Honeypot: an Internet-connected computer that simulates the activities of servers or users in order to collect malware files and emails used in attack campaigns.

Incident response (IR) team: The team responsible for investigating and analyzing data breaches and other cyberattacks. Also known as a computer incident response team (CIRT) or a security incident response team (SIRT).

Indicator of compromise (IOC): An artifact or event associated with attacks or data breaches.

Mass attack: An attack launched at a large number of potential victims rather than at a specific target. network operations center (NOC): A facility for monitoring and controlling computer and telecommunications networks.

Personally identifiable information (PII): Information that can be used to identify or represent individuals, including names, addresses, and financial and medical records.

Pivot: (verb) To investigate a potential attack by starting with an initial indicator of compromise and finding related indicators and events.

Sandboxing: Running an unknown file in an isolated virtual execution environment in order to detect malicious behaviors. A form of dynamic analysis.

Security information and event management (SIEM): A system or application that collects and correlates security alerts and events.

Security operations center (SOC): A facility for monitoring security alerts and events, initiating investigations, and remediating damage.

Signature: A unique identifier of a file or other artifact potentially associated with an attack.

Software development kit (SDK): A set of software development libraries and tools that facilitate the integration of an application with other programs.

Spear Phishing: Phishing campaigns directed at selected individuals within a targeted organization.

Tactics, techniques and procedures (TTPs): Patterns of activities and methods associated with specific threat actors or groups of threat actors.

Tradecraft: Operational techniques used in intelligence to obtain information from adversaries without detection.