ManageEngine
Log360

Threat intelligence and the SIEM advantage

Why SIEM solutions are the ideal choice for gaining threat intelligence capabilities.

Introduction

Threat intelligence (TI) is the not-so-secret weapon the cybersecurity industry is using to step up its game against attacks. While it's been around for some time, only recently has threat intelligence been widely recognized. According to the SANS 2018 Cyber Threat Intelligence Survey, 81 percent of security professionals believe that investing in threat intelligence capabilities helped improve their organization's security posture—compared to 64 percent in 2016.

However, despite the rising interest, there's also a lot of debate surrounding this topic. What exactly does threat intelligence involve? What capabilities are required for an organization to claim they have a mature threat intelligence system in place? Which tools are best for providing these capabilities?

In this white paper, we'll discuss:

- Threat intelligence and its various aspects.
- How threat intelligence is incorporated into an organization's security framework.
- The advantages of using a SIEM solution to implement a comprehensive threat intelligence system in your organization.
- Enterprise use cases.

Demystifying threat intelligence

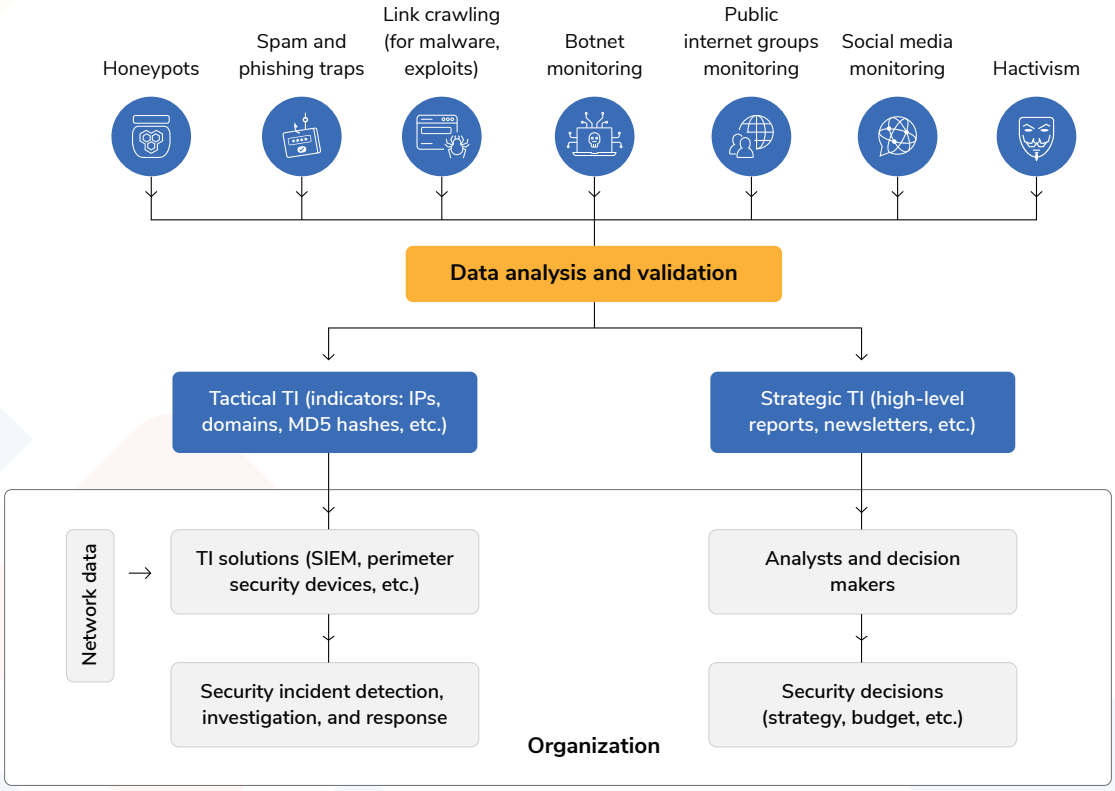
Gartner, the world's leading research and advisory company, defines threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

This definition helps us note the following aspects of threat intelligence:

- Based on a "known bad" approach, threat intelligence helps organizations detect threats based on knowledge that has been observed elsewhere in the world.
- Threat intelligence isn't just a list of bad IPs. It also includes detailed threat actor profiles, attack mechanisms, and instructions on how to respond to a threat.
- It's constantly evolving and providing information on existing and emerging threats.
- Its main goal is to better equip organizations in the fight against global threats.

The threat intelligence cycle

The definition of threat intelligence helps us appreciate what it is; however, it still doesn't address two important concerns: where does it come from? And how is it incorporated within the context of an organization's own network security? The following diagram can help us visualize the answers to these questions:



Using a combination of automated and manual techniques, threat intelligence data is gathered from all over the internet. This data is then processed by dedicated research teams who analyze and validate the information before publishing it in the form of strategic or tactical threat intelligence.

Strategic threat intelligence is intended primarily for human consumption, and it guides strategic security decisions, such as deciding which areas of cybersecurity to focus on, launching employee awareness programs for the latest threats, and so on.

Tactical threat intelligence is most commonly published in the form of threat feeds, and it's generally read by one or more security solutions. It is more useful on a day-to-day basis, as it helps organizations detect and fight security incidents in their networks. Some popular threat feeds include AlienVault OTX, FireEye iSight Threat Intelligence, and Symantec Deepsight.

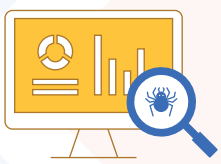
The SIEM advantage

Among the wide range of security solutions available today that provide threat intelligence features, none are as comprehensive as those offered by SIEM solutions. In fact, SIEM solutions are the most popular choice among those wishing to build threat intelligence capabilities. When it comes to threat intelligence, the following factors give SIEM solutions an edge:

Quality of threat intelligence

Security alerts are only as good as the intel they're based on. As shown in the diagram above, there's a large human effort involved in processing threat data. This means that the quality of threat intelligence can vary greatly across providers.

SIEM solutions process threat intelligence from trusted sources, and some even give you the option to add custom feeds that your organization subscribes to independently. Because many threat feeds are specific to an industry or certain types of threats, custom feeds may make more sense for your organization.

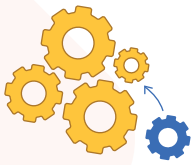


Comprehensive view of your network

Knowledge about global threats does you no good if you can't use it within the context of your own network. With a comprehensive view of all devices and applications in your network, SIEM solutions can notify you if malicious entities are detected on any system in your network.

SIEM solutions use network data results to triage alerts more effectively. They can reduce false positives by raising an alert only if a detected threat actor is engaged in specific, suspicious activity patterns.

Fewer integrations required

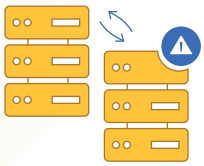


Ultimately, the goal of threat intelligence is to make the incident detection and response cycle as efficient and quick as possible. When these functions are spread across multiple solutions that don't integrate well, it defeats the purpose of threat intelligence.

SIEM solutions overcome this problem by providing most of the required functions from a single console with provisions for smooth integration where required. Once a security incident is detected, you can thoroughly investigate, manage, and respond to it. This helps expedite the incident resolution process, ensuring that your organization remains secure from any threat.

Threat intelligence and SIEM in action: Enterprise use cases

Communication with callback servers



Sometimes, if a system in your network gets infected, it may come under the control of an external server, also known as a callback or command-and-control server. This callback server can then use this system to extract sensitive data or infect other critical servers in your network.

SIEM solutions constantly scan outgoing traffic logs from your network and capture communications being sent to these types of servers. You can then launch an investigation to find out how and when the system was infected, and you can check for other potentially infected systems that have had contact with this callback server.

SQL injection attempts from malicious sources

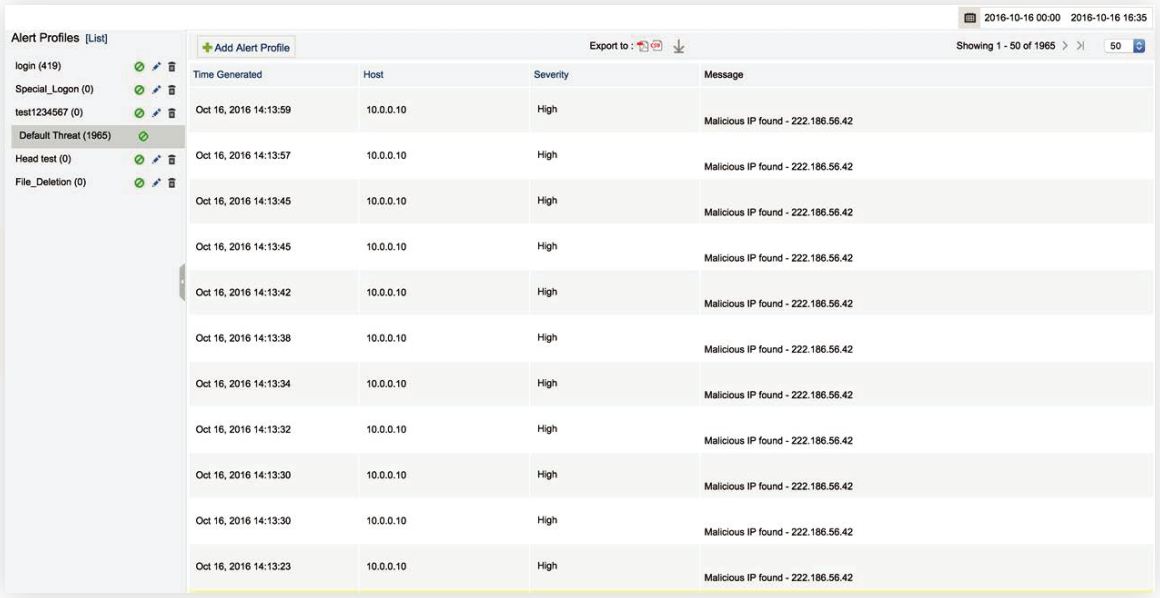
Attackers may exploit vulnerabilities in your web server and inject malicious SQL code to retrieve confidential business records from your databases. To avoid such data breaches, SIEM solutions keep an eye on all incoming connections to your web servers and flag any malicious IPs or domains. This allows you to contain the loss of important data, and identify and fix vulnerabilities in your web server.

Potential malware downloads

Attackers are always on the lookout for ways to infiltrate your network and download malware onto your systems. Since malware isn't easily distinguishable from regular software, you need to be on the lookout for attack indicators pointing to problematic software.

For example, if a known malicious actor remotely logs on to your network following a brute force attack on your organization's VPN, accesses a system in the network, and downloads software onto it, chances are this is a malware attack. SIEM solutions utilize correlation modules that can check for patterns of activity like this, allowing you to detect attacks with high accuracy and reduce false positive alerts.

Highlight: Log360's threat intelligence module



ManageEngine Log360's threat intelligence module offers these advantages:

- **Dynamic updates:** The solution's threat feed processor automatically retrieves the latest threat intelligence from highly reliable open source feeds.
- **Requires no configurations:** The threat feed alert profile is preconfigured. Log360 starts scanning your network for threats the moment you add log sources for monitoring.
- **Ability to add custom feeds:** Seamlessly add custom STIX/TAXII-based threat feeds to be compared with your network logs.

- **Correlation rule builder:** Build custom correlation rules that detect suspicious activity from a threat actor and raises alerts.
- **Powerful search engine:** Search through millions of logs in seconds, and build a log trail of any malicious actors' activity in your network.
- **Incident management:** Track the status of threat alerts using the solution's built-in ticketing console, or forward alerts to external help desk consoles.
- **Automated response:** Assign custom scripts to be triggered automatically when a threat alert is raised.

Conclusion

Threat intelligence is truly a game changer in the fight against the ever increasing number of cyberattacks that organizations face. It's a global, collaborative effort by the cybersecurity industry, and when used right, it helps organizations detect and defeat threats upon detection.

Given their comprehensive security features, SIEM solutions are the ideal choice to implement threat intelligence systems within enterprises. And with robust threat alerts, you'll be able to keep your organization secure at all times.