La inteligencia de amenazas (TI) es el arma no tan secreta que el sector de la ciberseguridad está utilizando para fortalecer su lucha contra los ataques. Aunque existe desde hace tiempo, hasta hace poco la inteligencia de amenazas logró un amplio reconocimiento. Según la Encuesta sobre Inteligencia de Amenazas Cibernéticas de SANS 2018, el 81 por ciento de los profesionales de la seguridad creen que invertir en funciones de inteligencia de amenazas ayudó a mejorar la postura de seguridad de su organización, en comparación con el 64 por ciento en 2016.

Sin embargo, a pesar del creciente interés, también hay mucho debate en torno a este tema. ¿Qué implica exactamente la inteligencia de amenazas? ¿Qué funciones son necesarias para que una organización pueda afirmar que cuenta con un sistema de inteligencia de amenazas maduro? ¿Cuáles son las mejores herramientas para proporcionar estas funciones?

En este documento técnico discutiremos:

- La inteligencia de amenazas y sus diversos aspectos.
- Cómo se incorpora la inteligencia de amenazas al marco de seguridad de una organización.
- Las ventajas de utilizar una solución SIEM para implementar un sistema integral de inteligencia de amenazas en su organización.
- Casos de uso empresariales.

Desmitificando la inteligencia de amenazas

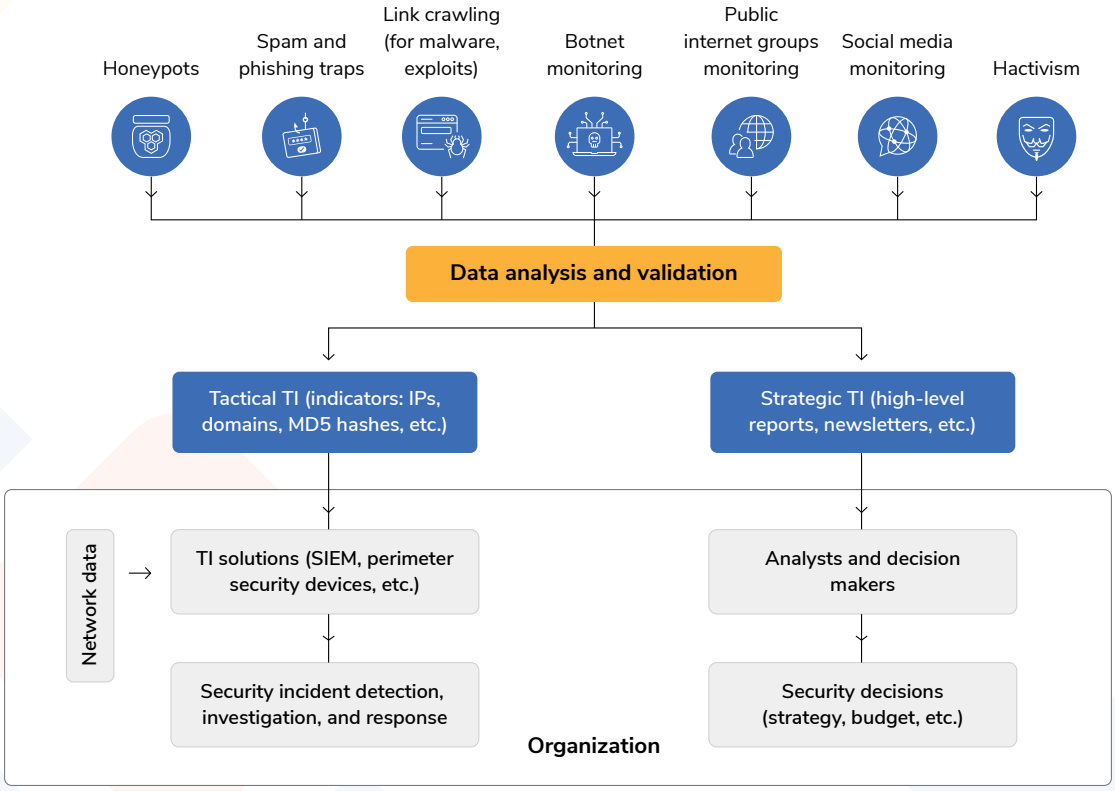
Gartner, la principal empresa de investigación y asesoramiento del mundo, define la inteligencia de amenazas como "un conocimiento basado en pruebas que incluye el contexto, los mecanismos, los indicadores, las implicaciones y los consejos procesables sobre una amenaza o un peligro existente o emergente para los activos que se puede utilizar para fundamentar las decisiones relativas a la respuesta del sujeto a dicha amenaza o peligro."

Esta definición nos ayuda a observar los siguientes aspectos de la inteligencia de amenazas

- Basada en un enfoque de "mal conocido", la inteligencia de amenazas ayuda a las organizaciones a detectar amenazas con base en lo que se ha observado en otras partes del mundo.
- La inteligencia de amenazas no sólo es una lista de IP maliciosas. También incluye perfiles detallados de atacantes, mecanismos de ataque e instrucciones sobre cómo responder a una amenaza.
- Está en constante evolución y proporciona información sobre las amenazas existentes y emergentes.
- Su principal objetivo es equipar mejor a las organizaciones para luchar contra las amenazas globales.

El ciclo de la inteligencia de amenazas

La definición de inteligencia de amenazas nos ayuda a apreciar lo que es; sin embargo, todavía no aborda dos preocupaciones importantes: ¿De dónde viene? ¿Y cómo se incorpora en el contexto de la seguridad de la red de una organización? El siguiente diagrama puede ayudarnos a visualizar las respuestas a estas preguntas:



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.

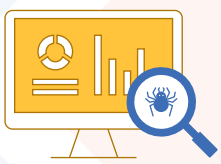
The SIEM advantage

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.

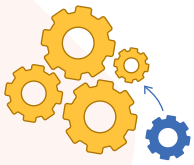


Comprehensive view of your network

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

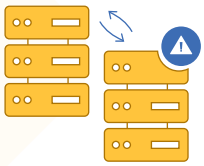


Ultimately, the goal of threat intelligence is to make the incident detection and response cycle as efficient and quick as possible. When these functions are spread across multiple solutions that don't integrate well, it defeats the purpose of threat intelligence.

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

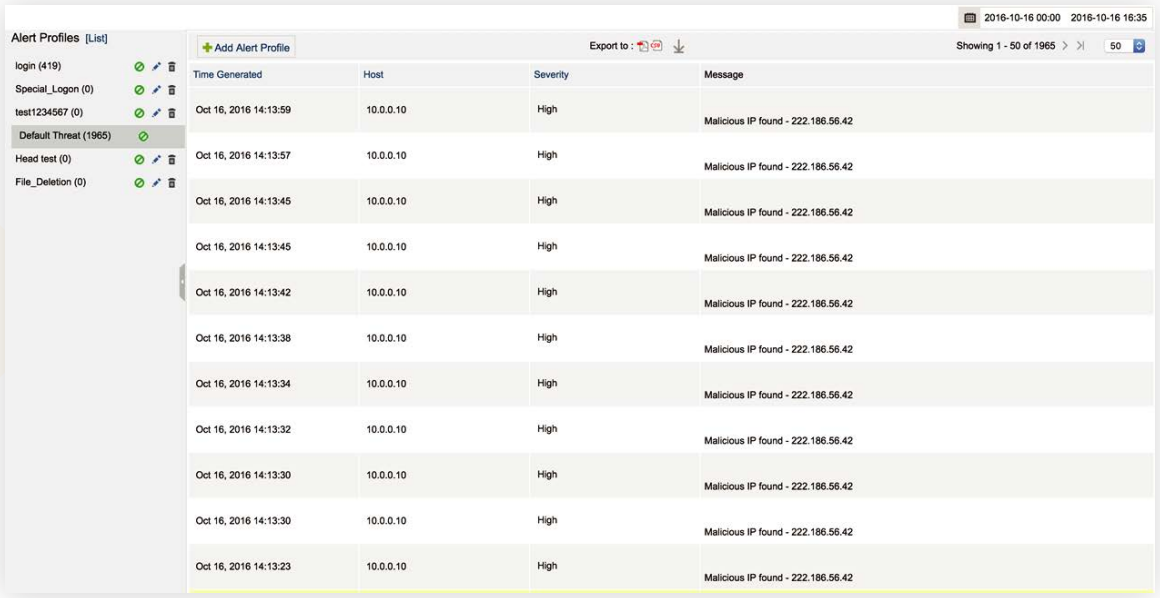
Attackers may exploit vulnerabilities in your web server and inject malicious SQL code to retrieve confidential business records from your databases. To avoid such data breaches, SIEM solutions keep an eye on all incoming connections to your web servers and flag any malicious IPs or domains. This allows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