Threat hunting

As your SOC gains maturity and establishes programs in proactive defense, threat hunting becomes a critical function. This is because advanced and sophisticated threats can get past traditional and automated cybersecurity defenses, or can be overlooked by tier 1 and 2 analysts.

Establishing a successful threat hunting program is based on your environment's data quality and your ability to surface insights generally not found through day-to-day correlation activity. You should first have a tool like Splunk Enterprise Security in place, collecting data. When data is easily collected, normalized, accessed and analyzed, this provides valuable clues for your team's threat hunters to chase down threats.

Threat hunters are skilled cybersecurity professionals who search, log, monitor, and remediate threats before they create a serious problem. They leverage a human curiosity element to investigate within enterprise security, complementing automated systems. Threat hunters also provide guidance and help establish processes for investigative techniques.

What are the benefits of an effective threat hunting program?

An effective threat hunting program reduces the time from intrusion to discovery, and in most cases limits the amount of damage that can be done by attackers. Sophisticated attacks often lurk for weeks, or even months, before discovery. On average it takes more than 200 days before most organizations discover a data breach has occurred. Attackers wait patiently to siphon off data and uncover enough confidential information or gain privileged credentials to unlock further access, setting the stage for a significant data breach and a place that no organization wants to be part of.

Threat hunting is quickly becoming a vital and favorite role in many organizational cybersecurity programs since it ensures a level of situational awareness that other methods might not reach so quickly. The benefits of enabling a threat hunting program are:

- **Proactively uncover threats**. Become aware of hidden threats and proactively identify advisories that may have found ways to establish a foothold in your organization's network.
- **Improve the speed of threat response and detection.** Ad-hoc investigation can often identify activity or patterns that may already be present in your environment.
- **Aid cybersecurity analysts in understanding the organization.** Gain a better understanding of your organization's current security state and posture and how you can defend against attacks.
- **Help achieve appropriate mitigation of threats through proper defense.** Deeper insights into your networks and systems and the threats they may face aids in establishing layered controls.
- **Reduce false positives and improves SOC efficiency.** Create hypothesis-driven, proactive, and repeatable processes. Applying human investigative techniques alongside the implementation of effective tools means false positives and reduced and efficiency in detection and resolution increased.

What are threat hunting best practices?

A threat hunter's job is to find the unknowns. Threat hunters conduct analysis through vast amounts of security data, searching for hidden malware or signs of attackers by looking for patterns of suspicious activity that may not have been uncovered by tools. They also help develop in-depth defense approaches by understanding attacker tactics and techniques so they can help prevent that type of cyberattack. They use common frameworks such as MITRE ATT&CK or Kill-Chain to help adapt them to the local environment.

Types of threat hunting

Hunters begin with a hypothesis based on security data, threat intelligence indicators or event actions. Their hypothesis steers them into a more in-depth investigation of potential risks. These deeper investigations can be structured, unstructured or ad-hoc.

Structured investigation

A structured investigation is based on threat intelligence data such as an indicator of compromise (IoC) or through tactics, techniques, and procedures (TTPs) of an attacker. Threat actors can be identified even before the attacker can cause damage to the environment by understanding the TTPs they employ. MITRE ATT&CK is a popular framework that threat hunters perform structured investigation from.

Unstructured investigation

Unstructured investigation is often started through an action or event occurring where one or more indicators of compromise (IoC) are detected. This type of event leads a threat hunter to focus on pre-event and post-detection patterns. They piece searches together with other connected incidents to build a holistic picture.

Ad-hoc investigation

Ad-hoc investigation can occur for a variety of reasons. Threat trends, active vulnerability analysis, risk assessment, or external leads. Leads can be discovered from crowd-sourced attack data which reveal the latest TTPs of current cyberthreats. A threat hunter uses these tiny clues to then search for these specific behaviors within their environment.

What threat hunting processes can I put in place?

These resources will help you implement this guidance:

- Use case: Using the MITRE ATT&CK framework in Splunk Enterprise Security