elastic

ELASTIC SECURITY

Threat hunting for SIEM

Threat hunting empowers security teams to secure an environment against advanced threats and spot gaps in automated coverage.

The practice reduces risk by spotting adversaries that may have been missed by existing security controls and identifying the limits of existing security controls and countermeasures.

Technology doesn't drive hunting, but it is a critical enabler. The shortcomings of past SIEM solutions gave many threat hunting programs no choice but to operate a standalone platform. For peak SOC efficiency and effectiveness, your SIEM should deliver the capabilities threat hunters need.

Why is threat hunting important?	Threat hunting reveals attackers who have penetrated your environment and avoided discovery. Such threats can inflict severe damage — necessitating a proactive effort to stop them.
What data do you need?	Hunters often start with a specific attacker technique — and corresponding data — in mind. Just like with an investigation, the twists and turns of a hunt can require access to further data. Automatically enriching data with threat intelligence can surface context that accelerates analysis.
Why is query speed a key consideration?	Threat hunters generate and test hypotheses in rapid succession, requiring the power to drill into data and pivot at will. A platform should allow hunters to fully focus on the task at hand by operating "at the speed of thought."
What is the role of machine learning?	Machine learning helps practitioners spot signals amongst the noise of everyday activity. It can generate evidence-based starting points for a hunt and provide insights along the way to help uncover unknown threats.

> "Super simple. Results come back in milliseconds rather than hours."
>
> **Kate Nolan, Security Data Engineer, Cisco Talos**

|

Why Elastic for threat hunting?

Arm hunters with advanced analytics

Elastic Security applies advanced analytics to help threat teams uncover lurking threats and reveal weaknesses in existing defense measures. Analytics-driven hypotheses provide a starting point for a hunt, while turnkey machine learning jobs and user and entity risk scores provide insights throughout.

Put all data within immediate reach

Elastic Security integrates with a vast ecosystem of security, observability, and IT technologies and normalizes data with an open source taxonomy, eliminating blind spots and data silos. Threat hunters can query petabytes of logs in just seconds and quickly match fresh IoCs against years of historical data. Unifying data on a single platform eliminates swivel-chair analysis, keeping practitioners in the hunt.

Leverage rich context

Elastic helps hunters determine what merits scrutiny — and what to do about it — with curated insights, context, and visualizations. It gleans information from threat intelligence, vulnerability data, and other sources. The solution nimbly surfaces relevant information and streamlines the inspection of cloud workloads and hosts.

Address gaps in automated detections

Elastic Security enables today's hunt to become tomorrow's automated protection, reflecting new observations about adversary tradecraft. Organizations can leverage a robust set of out-of-the-box detections and preventions, all mapped to MITRE ATT&CK® for simple management, as well as create custom protections.

Migrate to a modern SIEM for threat hunting

To power your threat hunting program, choose a platform that readily collects, enriches, and analyzes data by the terabyte.

Adopting a modern SIEM isn't a trivial undertaking and you'll have a lot of decisions to make along the way. But rest assured, the Elastic team and our partners have walked this road countless times, and we'd be glad to share what we've learned.

Get started by considering the most important attributes of the right SIEM solution for your organization with our SIEM Buyer's Guide.

Start your SIEM journey