ELASTIC SECURITY

SIEM powers automated threat protection

Automated threat protection advances security maturity by enabling continuous prevention and detection of known and unknown threats, aligned with the MITRE ATT&CK matrix. The ability to thwart complex attacks with machine learning and behavior analytics. Block ransomware and malware from any infrastructure. Advance SecOps maturity to stop threats at scale.
Market dynamics and key challenges:

- Drive efficiencies across organizational boundaries with a unified data fabric and taxonomy to drive AI/ML automation
- Enables cross-stack detection via the convergence of network, host, and user data across on-premises and cloud.
- Get a step ahead of regulatory and compliance mandates.
- Enable continuous analysis of historical and archived data.

How does data normalization enable automated threat protection?	Normalizing data enables automated analytics by establishing a uniform data fabric for continuous alerting and machine learning.
Why does automated detection matter?	Finding threats early gives you the best chance to eradicate them from your ecosystem before they can inflict damage
How does threat detection stop known threats?	Reveal threats early in the attack lifecycle (before damage is done) with rules honed and shared by Elastic threat researchers and community members. Automatically enrich and corroborate alerts to prioritize the most critical attacks. Leverage threat intelligence for further fidelity.
What is the role of advanced analytics?	Machine learning and other advanced techniques help the SOC uncover unknown threats. Expose adversarial activity often missed by traditional detection methods, including malicious insiders and advanced persistent threats.

Why Elastic for automated threat protection?

Protect in depth

Elastic Security disrupts attacks with layered prevention and detection across your attack surface. The solution automates the detection of advanced threats with centralized machine learning and alerting. Elastic Agent does double duty by securing the same infrastructure from which it collects activity and state data.

Specialized expertise, ready out-of-the-box

Elastic Security arms teams to stop threats at scale with native prevention, detection, and response developed by our research engineers and community members. Prebuilt protections are aligned with MITRE ATT&CK, enabling organizations to enhance their security posture in a methodical manner.

Find out faster

Elastic's integrated Security and Observability solutions enable organizations to get ahead of compliance and security issues by gleaning automated insights into system security and application performance. This capability is made possible by ingesting a high volume and variety of data, normalizing it in a uniform manner, and activating continuous alerting.

Protect with a single agent

Organizations can power cross-telemetry detection across their environment — including host and cloud workloads — by collecting rich data with Elastic Agent. Activate built-in protections to detect threats via both localized and centralized analysis, block ransomware and malware, and take action on remote endpoints. High OS parity and robust capabilities at every licensing level meet the needs of diverse organizations.

Migrate to a modern SIEM for automated threat protection

To achieve automated threat protection for your security operations program, choose a massively scalable platform with a powerful data schema and prebuilt data integrations supporting the most innovative technologies in your enterprise stack.

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