elastic

ELASTIC SECURITY

Continuous monitoring for SIEM

Continuous monitoring delivers powerful operational awareness, streamlined security analysis, and ongoing visual feedback. Achieving visibility across your environment is among the first — and most essential — steps to securing your organization.

The continuous monitoring use case is deceptively simple:

- Collect security-relevant data of any kind
- Normalize the data to enable uniform analysis
- View the data as you see fit with prebuilt and custom visualizations

Despite "security" and "monitoring" constituting the first and last letters of SIEM, most organizations have become inured to the shortcomings of solutions that fail to deliver on this promise. Eliminate blind spots and data silos with a SIEM that supports the modern SOC.

Why is visibility vital for security operations?	Attackers prod for weaknesses. Prepare your defenses by achieving comprehensive operational awareness.
Why does data normalization matter?	Data normalization enables uniform analysis, expediting SOC processes and clearing the way for automated analytics.
How does monitoring drive performance?	You can't improve what you don't measure. Monitoring puts a lens on business and security results.
How is data management relevant to monitoring?	Direct access to long-term archives equips the SOC to analyze trends, meet compliance requirements, and stop advanced threats.
How can monitoring spur results beyond the SOC?	With integrated functionality for security, development, and operations teams, collaborate across organizational boundaries.

> "Countless cybersecurity weaknesses are rooted in poor visibility and inadequate search capabilities."
>
> **Armando Seay, Co-Founder, MISI**

 |

Why Elastic for continuous monitoring?

Everything you know, all in one place

Centralize data distributed across clouds and geographies. Elastic Security collects and prepares data via integrations developed by Elastic engineers, partners, and community contributors. It gathers rich host and user data and provides entity insights (e.g., risky users, critical assets) for enhanced visibility. It also delivers visibility into cloud infrastructure and applications, host and activity and context, network activity, IoT and OT data, and more.

View your data, your way

Elastic Security enables uniform analysis of diverse technologies with an open data schema. Harness purpose-built visualizations and quickly craft and share your own. Update an entire dashboard with a simple filter. Account for business context to enhance command.

Harness rich observability data

Advance SecOps maturity, harden DevOps and DevSecOps processes, and optimize operations with integrated security and observability. Observations like increased CPU usage could reveal adversary activity. Grant additional teams access to a dataset in a controlled manner.

Start small, scale up

Arm analysts with an order of magnitude more data — without breaking your budget. Retain and analyze years of archives in searchable, low-cost object stores. With resource-based pricing, ensure that licensing doesn't get in the way of good security practices.

Migrate to a modern SIEM for continuous monitoring

To achieve continuous monitoring 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

 |

elastic