elastic | The Search AI Company

Is your SIEM ready for the AI era?

You may already have a security information and event management (SIEM) solution. But is it ready to take on today's demands of flexibility, scale, and AI-fueled threats?

Most security professionals see AI's potential and are ready to adopt it into their stack...

93%

of cybersecurity professionals believe generative AI could help their cybersecurity team improve its knowledge, skills, and abilities.[1]

92%

would be willing to replace existing security technologies based on another vendor's generative AI capabilities.

78%

will increase spending for security solutions with generative AI capabilities.

The needs of SIEM have expanded. Here are the...

Key requirements for AI-driven security analytics

Eliminate blind spots

Your SIEM should broaden visibility by efficiently collecting and preparing data from across the attack surface, with telemetry from native and third-party technologies. It will need to retain years of efficiently stored data — searchable in seconds — allowing teams to uncover lurking threats and markers of newly discovered exploits. Be sure it can deploy to any infrastructure (on-prem, cloud, SaaS, hybrid, and multi-cloud) to reduce cloud lock-in.

Strengthen defenses

Today's SIEM enables the SOC to tackle new use cases by creating custom ML models, equipping threat hunters with user and entity risk scores, blocking ransomware and malware, spotting threats, and enabling host-based response — all with one agent.

Accelerate SecOps workflows

Be sure your SIEM is reducing risk and minimizing alert noise. AI-driven security analytics automates key triage steps, provides investigation steps (including a detailed description of the attack, summarization of hosts & users involved, and related MITRE ATT&CK Tactics), and streamlines admin tasks (creating/converting ingest pipelines and detection rules).

There's a lot to consider when migrating to/investing in a new SIEM. Explore our **SIEM Buyer's Guide** for help getting started.