

SIEM

Real-time threat detection. Agent-led investigation.

Sumo Logic SIEM utilizes AI across every step of the security workflow—collect, detect, investigate, and respond—so security teams can focus on the threats that matter with fast precision.

AI is rapidly moving into every layer of security operations. While this shift offers unprecedented speed and scale, it introduces a new kind of risk: AI that investigates confidently, but incompletely. Many approaches to AI in the SOC reward velocity over verification by surfacing a verdict without disclosing what the AI could and could not see.

[Sumo Logic SIEM](#) takes a different approach. AI works across every step of the workflow—collect, detect, investigate, and respond—on top of a single, AI-ready data foundation. Rather than layering AI on top, SIEM embeds it directly into the workflow, so every verdict an analyst acts on is backed by a complete, auditable evidence trail.

With threat detection, advanced analytics, automation, and agentic capabilities working from the same trusted foundation, SIEM gives analysts Insights they can act on with confidence and evidence they can stand behind, at every stage of the kill chain.

One platform, built to work together

Sumo Logic SIEM is part of Sumo Logic's broader [Intelligent Operations Platform](#), built so AI has clean, structured data to reason over.

Intelligent Operations Platform

Data Pipelines

[Data Pipelines](#) route, filter, and transform telemetry before it reaches Log Analytics / SIEM, cutting volume without cutting the signals that matter. Teams get a single view into pipeline health, telemetry volume, and data reduction, so they can control costs and prove pipeline value without investigating each one individually, keeping the data lake clean and the signal clear.

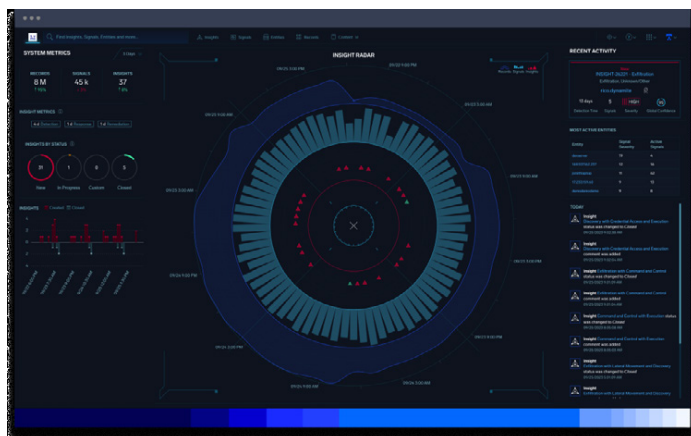
Context: Log Analytics + SIEM

Log Analytics delivers high-performance search, visualization, and root cause analysis across reliability, infrastructure, compliance, and security workflows. SIEM builds on that same foundation to add behavioral detection, agentic investigation, and automated response.

Agentic AI: Dojo AI

[Sumo Logic Dojo AI](#) puts that context to work. The SOC Analyst Agent automatically investigates Insights and delivers an evidence-backed verdict. Mobot makes that reasoning and the underlying data accessible through natural language. Sumo Logic MCP Server provides external AI clients with seamless access to SIEM context, using the same governance SOC teams already rely on.

Because SIEM sits on this same foundation, every Insight and every agent-generated verdict is backed by structured context and a complete evidence trail, not a guess. That architectural advantage, built over 15+ years of normalizing and correlating security telemetry, is something AI tools built on raw or fragmented data can't replicate.



The full workflow: verified at every step, not just fast at one of them

Gain meaningful insights to expedite TDIR

SOC teams are under constant pressure from overwhelming alert volume. Most SIEM technologies cannot keep pace with the volume and sophistication of today's attacks. Many AI SOC tools, while fast, were never given a complete data foundation to reason over, limiting the effectiveness of SOC teams even as alert handling accelerates. Sumo Logic SIEM solves these challenges across the entire TDIR workflow with AI-driven detection, investigation, and response.

Detection starts at the data layer. SIEM applies pattern and threat intelligence matching, correlation logic, machine learning-driven anomaly detection, and user and entity behavior analytics (UEBA) to every log and security event as it's ingested, filtering millions of raw records down to a focused set of Signals in near real-time. Because that detection runs on the same normalized data as every later stage, every Signal an analyst sees has already been filtered for relevance.

At the **investigation** stage of the workflow, SIEM gives analysts prioritized and contextualized threat data generated over that same foundation. It goes beyond prioritized Insights: AI-driven investigation automatically works through the Insights, complete with evidence-backed verdicts and recommended actions.

SIEM then triggers **response** playbooks, which can be built from scratch or customized from prebuilt, integration-specific templates. These playbooks run a predefined sequence of actions automatically whenever an Insight is created or closed, so response moves without waiting for manual handoffs.

The result: detection, investigation, and response all draw from the same evidence trail, so investigations move faster, and every Insight comes with the complete, auditable context analysts need to trust and verify it.

Automation analysts can trust

Analysts spend most of their day investigating Insights to separate the valid ones from the noise, manual and repetitive work that consumes the majority of a shift. SIEM applies cloud-scale and agentic AI to automate that process across the entire workflow, and does so in a way analysts can trust.

Every verdict and every action stays bound and reviewable. Confidence thresholds decide which verdicts and actions can proceed automatically and which route to an analyst first. Every

action leaves behind a full reasoning trail: the evidence reviewed, the confidence assigned, and the policy that authorized it. SOC Analyst Agent uses that trail to automate routine tasks and accelerate investigations while keeping analysts firmly in control. Mobot, the Sumo Logic assistant, gives analysts a natural language way to review, question, and act on every verdict.

Freed from the manual effort of triaging every alert, analysts can dig into Insights and verdicts and immediately begin the high-value work of threat hunting.

Solution benefits

- **Cut through alert noise:** Related Signals are grouped into Insights automatically, so analysts start every investigation with the timeline already created.
- **Scale without added overhead:** Cloud-native multi-tenancy and elasticity keep pace with more data, more Insights, and more users without adding infrastructure.
- **Free analysts to work on real threats:** Automates manual, repetitive alert triage so analysts can focus on new threats and the company's security posture.
- **Move from alert to action faster:** Enriches Insights by integrating, orchestrating, and automating actions across the security stack. Fully automated playbooks let teams quickly prioritize, investigate, and notify others of potential risks.
- **Start every investigation ahead:** SOC Analyst Agent automatically investigates Insights and delivers an evidence-backed verdict, giving analysts a head start on every Insight while keeping them in control of the final decision.
- **Trust every action:** Confidence thresholds decide which investigations SIEM completes autonomously and which route to an analyst first, and every verdict leaves behind a full reasoning trail so oversight scales right alongside automation.
- **See value from day one:** Deploys rapidly and comes with extensive out-of-the-box content, enabling security teams to realize immediate value.

The ROI of agentic SecOps

■ END-TO-END

100%

of tier-1 alerts triaged by Dojo AI

■ TIME TO VERDICT

89%

reduction in median time-to-triage

■ FASTER MTTR

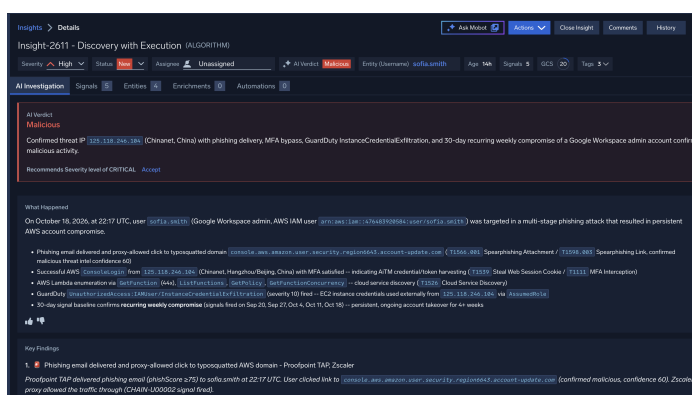
64%

reduction in MTTR on incidents

■ TIME SAVINGS

25 hrs/week

returned to each analyst



Dojo AI capabilities

- **Mobot:** Sumo Logic assistant that connects users to agents and the full context of the data through natural language and helps execute workflows directly.
- **SOC Analyst Agent:** Automatically investigates Insights, evaluates related activity and context, and prioritizes evidence-backed verdicts with clear findings, so analysts start every Insight with an investigation instead of a raw alert.
- **Log Analysis Agent:** Goes beyond query writing to guide investigations end-to-end by interpreting intent, retrieving and correlating relevant data, and helping analysts of any skill level create and manage dashboards through natural language.
- **Platform Optimization Agent:** Answers how-to questions, troubleshoots broken or inefficient queries, and helps manage

data usage and configuration through natural language.

- **Sumo Logic MCP Server:** Connects external AI clients, such as Claude Code, to SIEM and Log Analytics, with the same governance and trust as the Sumo Logic platform.

SIEM capabilities

- **Security analytics generating Signals from logs:** SIEM collects millions of logs and security-relevant data across on-prem, cloud, and multi-cloud environments. It then applies pattern and threat intelligence matching with correlation logic, statistical evaluation, and anomaly detection to filter Records down to thousands of Signals in near real-time.
- **Actionable Insights:** Insights represent the intelligent, correlated, and prioritized clustering of Signals and other data enrichments tied to associated Entities. Insights provide an automatically generated storyline containing the relevant context a security team needs to make rapid, high-confidence decisions, accelerating investigation and response time.
- **User and entity behavior analytics:** UEBA provides the typical behavior of users and entities within an organization, flagging anomalies that deviate from that established norm. UEBA bolsters detection of threats like zero-day exploits and insider activity that conventional tools might miss. Entity Timelines add a visual perspective on activity, making investigations faster and more thorough.
- **Entities and Activity Score:** An Entity (e.g., hostname, username, MAC address) is a unique actor that a Signal fires on when encountered in an incoming log. An Entity's Activity Score is the sum of severities of every Signal tied to it, and the Entity Relationship Graph visualizes how entities connect, so analysts can see the full scope of an attack at a glance.

- **Tagging and context:** Tags are metadata attached to Insights, Signals, Entities, and Rules to add context to investigations. A subset of Sumo Logic's out-of-the-box rules is natively mapped to all MITRE ATT&CK Tactics and Techniques and sub-techniques (roughly 80%), continuously managed and updated by an in-house threat engineering team.
- **MITRE ATT&CK Coverage Explorer:** Provides a comprehensive visualization of the adversary tactics, techniques, and procedures (TTPs) covered by our out-of-the-box rules. Assess detection in real-time, compare against community-wide coverage, and explore theoretical coverage to strategically align defenses with the MITRE ATT&CK framework.

- **Continuous improved detection:** Insight Trainer uses analyst feedback to refine rule accuracy over time, and Entity Criticality weighs investigations toward the assets that matter the most to a business.
- **Automated alert enrichment and notification:** Create enrichment and notification playbooks using pre-built integrations or an open integration framework for custom ones, and describe these workflows in Mobot in natural language to create, edit, or summarize them.
- **Compliance and governance:** Granular role-based permissions decide who can view, investigate, or configure SIEM, and out-of-the-box content mapped to compliance frameworks makes audit prep hassle-free.
- **Single, collaborative platform:** Modernize the SOC with a single, AI-driven intelligent SIEM that seamlessly integrates with existing tools and processes, reducing tool proliferation and complexity. SIEM provides central log management for all SecOps, ITOps, and DevOps users and use cases.
- **Community analytics:** Powered by machine learning, the Global Confidence Score estimates whether an Insight is actionable based on resolution patterns and false positives aggregated across all global Sumo Logic SIEM users.

About Sumo Logic

Sumo Logic, Inc. empowers digital organizations to transform massive amounts of data into actionable insights by unifying critical security and operational data through its Intelligent Operations Platform. Built to address the increasing complexity of modern cybersecurity and cloud operations challenges, we empower digital teams to move from reaction to readiness—combining agentic AI-powered SIEM and log analytics into a single platform to detect, investigate, and resolve modern challenges. Customers around the world rely on Sumo Logic for trusted insights to protect against security threats, ensure reliability, and gain powerful insights into their digital environments. For more information, visit www.sumologic.com.

