sumo logic

SOLUTIONS BRIEF

Cloud SIEM

The cloud-native SIEM for cloud-native attacks

Sumo Logic Cloud SIEM is a cloud-native platform that automatically analyzes and correlates threat data, enabling security teams to efficiently and rapidly discover and resolve meaningful threats.

In the modern era of digital innovation, enterprises are rapidly embracing cloud-native architectures. While this transition offers unprecedented agility and scalability, it simultaneously introduces unique security challenges. Traditional security approaches, crafted for on-premises environments, fall short when confronted with the intricacies of cloud-native threats. Recognizing this nuanced threat landscape, Sumo Logic has pioneered a cloud-native Security Information and Event Management (SIEM) solution. Specifically engineered for cloud environments, our platform ensures that security measures evolve with cloud-native application developments. Sumo Logic Cloud SIEM enables security professionals to detect, identify, and respond to threats tailored for the cloud by offering comprehensive visibility into an organization's cloud environment. With advanced analytics, threat detection, and automation, Sumo Logic Cloud SIEM surfaces actionable insights, aiding analysts in preemptively countering cloud-native threats.

Gain meaningful insights to expedite investigations

SOC teams are under constant pressure from overwhelming alert volume. Legacy SIEM technologies can't keep pace with the volume and sophistication of today's attacks, limiting the effectiveness of SOC teams.

Gartner first identified user and entity behavioral analytics (UEBA) as a standalone category in 2013 as a recognized technology to help SOC teams reduce false positives and focus investigations on meaningful alerts. But legacy UEBA systems had many problems, including a lack of data sources, complex and time-consuming implementation, reporting complexity and lack of skilled investigators.

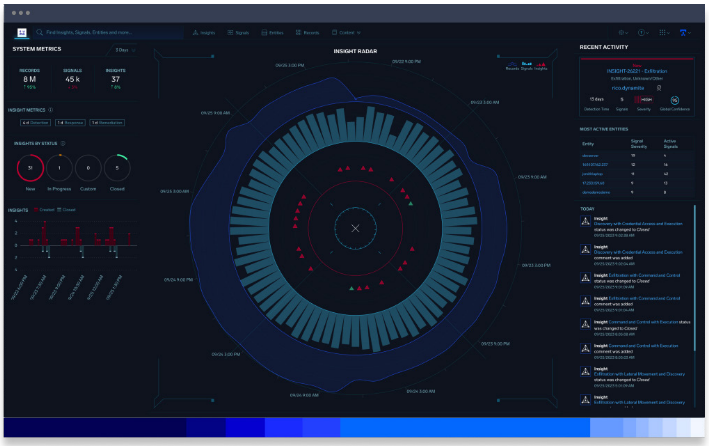
Sumo Logic Cloud SIEM alleviates these challenges with a modern solution that gives you prioritized and contextualized threat data. The platform automatically generates actionable Insights (not just prioritized alerts) and streamlines SecOp workflows with built-in event management and automated Insight enrichment. Sumo Logic's approach reimagines the needs of a SOC to answer the UEBA challenges better. The result is a solution that reduces alert fatigue, expedites investigations and improves efficiencies in your SOC processes.

The power of analytics and automation

Analysts spend most of their day investigating SIEM alerts to separate the valid ones from the noise, which is manual and time-consuming. Cloud SIEM applies cloud scale to automate this process.

The cloud-native platform provides multi-tenancy and elasticity, delivered efficiently at any scale to automate alert triage and analyze all Records to surface Insights. Insights provide critical context to complete the "story" of a potential incident and empower your security team to focus their time and attention on crucial threats to the business.

Freed from the manual effort of triaging every alert, you can dig into Sumo Logic Insights and immediately begin the high-value functions of threat investigation, response and threat hunting.



Solution benefits

- **Advanced insights:** Groups related threat Signals into Insights, automating manual triage efforts.
- **Unlimited scalability:** Cloud-native architecture provides multi-tenancy and elasticity, delivered efficiently at any scale, anytime, for all users.
- **Enhanced visibility:** Delivers context across users, networks, devices, alerts, cloud services and applications while prioritizing critical information that accelerates response times.
- **Improved SOC efficiency:** Automates manual, repetitive alert triage tasks that allow your SOC team to identify new threats and fortify the company's security posture.
- **Automated alert enrichment:** Enriches Insights by easily integrating, orchestrating, and automating actions of your stack, including enrichments and notifications. Fully automated playbooks enable Cloud SIEM customers to quickly prioritize, investigate and notify others of potential security threats.
- **Accelerated time-to-value:** Deploys rapidly and comes with extensive out-of-the-box content, enabling your SOC to experience immediate value.

The ROI of modern SecOps

Save an average of four hours per threat investigation while reducing false positives by 90% with Cloud SIEM to quickly and thoroughly understand the impact of an attack.

Cloud SIEM capabilities

Security analytics generating Signals from logs.
Cloud SIEM collects millions of logs and security-relevant data across your on-prem, cloud and multi-cloud environments. Then, it applies pattern and threat intelligence matching with correlation logic, statistical evaluation and anomaly detection to filter the 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 that contains the relevant context your security team requires to make rapid, high-confidence decisions. This modern approach dramatically accelerates a SOC team's investigation and response times.

User and entity behavior analytics
UEBA is a pivotal feature in contemporary cybersecurity. It operates by profiling the typical behaviors of users and entities within an organization, subsequently flagging anomalies that deviate from this established norm. When paired with our Cloud SIEM, UEBA bolsters detection capabilities, pinpointing potential threats like zero-day exploits and insider activities that might be missed by conventional security tools. The inclusion of features such as Entity Timelines offers a visual perspective on activities, facilitating swift and comprehensive investigations.

Entities and Activity Score
The concept of an Entity is central to the process Cloud SIEM uses to correlate Signals and create Insights. An Entity (e.g., hostname, username, MAC address, etc.) is a unique actor that a Signal fired upon when encountered in an incoming log. An Entity's Activity Score is the sum of the severities of the individual Signals associated with that Entity during the previous two weeks (by default). It can be used to limit false positives. Related Entities and Entity groups can also help scope the impact of a compromise, while the Entity Relationship Graph provides a visual representation of all the Related Entities involved.

Tagging and context
Tags are metadata you can attach to Insights, Signals, Entities and Rules which help add context to threat investigations. For example, a subset of our out-of-the-box rules are natively mapped and tagged to all 14 of the MITRE ATT&CK framework Tactics and mapped to 278 unique Techniques and sub-techniques (approximately 80% coverage) — which are continuously managed and updated by our threat engineering team in-house.

MITRE ATT&CK Coverage Explorer

The MITRE ATT&CK™ Coverage Explorer in Cloud SIEM provides a comprehensive visualization of an adversary's tactics, techniques, and procedures (TTPs) covered by our out-of-the-box rules. This dynamic page allows users to assess threat detection capabilities in real-time through the Recent Activity view, compare with community-wide coverage in the All Community Activity view, and explore the Theoretical Coverage view for insights into the full potential of implemented rules. Visualizations, filtering options, and export features empower security practitioners to optimize rule effectiveness, evaluate data sources, and strategically align defenses with the industry-standard MITRE ATT&CK framework.

Automated alert enrichment and notification

Using the Cloud SIEM Automation Service, customers can create enrichment and notification playbooks utilizing a set of pre-built integrations or leverage an open integration framework to build custom integrations.

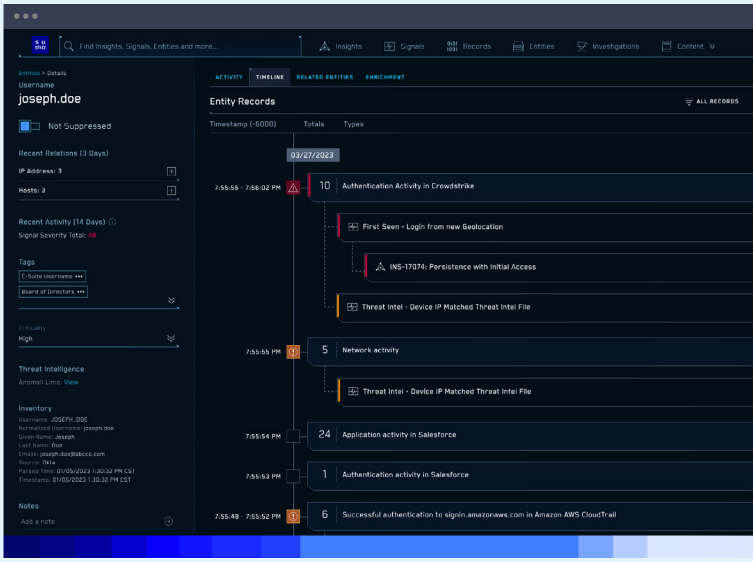
Single, collaborative platform

Sumo Logic helps modernize the SOC with a single, cloud-native SaaS platform that integrates with your existing tools and processes, reducing tool proliferation, cost and complexity. Cloud SIEM provides central log management for all your SecOps, ITOps and DevOps users and use cases.

Community analytics

A unique capability of Sumo Logic Cloud SIEM is crowd-sourced threat disposition. An Insight's Global Confidence score represents a confidence level predicted by Sumo Logic's Global Intelligence machine learning model that the Insight is actionable. The model compares closed patterns from Insights with a false positive or Resolved resolution. The model makes such comparisons broadly — across the global installed base of Cloud SIEM customers — so it can generate a Confidence score based on the patterns seen at one customer when encountered at another.

↗ Request a demo



Entities > Details

Username

joseph.doe

Not Suppressed

Recent Relations (3 Days)

IP Address: 3

Hosts: 3

Recent Activity (14 Days)

Signal Severity Total: 48

Tags

C-Suite Username

Board of Directors

Criticality

High

Threat Intelligence

Anomali Limo: View

Inventory

Username: JOSEPH_DOE
Normalized Username: joseph.doe
Given Name: Joseph
Last Name: Doe
Emails: joseph.doe@abcco.com
Source: Okta
Parsed Time: 01/05/2023 1:30:32 PM CST
Timestamp: 01/05/2023 1:30:32 PM CST

Notes

Add a note

Entity Records

Timestamp (-6000)	Totals	Types
03/27/2023		
7:55:56 - 7:56:02 PM	10	Authentication Activity in Crowdstrike
		First Seen - Login from new Geolocation
		INS-17074: Persistence with Initial Access
		Threat Intel - Device IP Matched Threat Intel File
7:55:55 PM	5	Network activity
		Threat Intel - Device IP Matched Threat Intel File
7:55:54 PM	24	Application activity in Salesforce
7:55:53 PM	1	Authentication activity in Salesforce
7:55:48 - 7:55:52 PM	6	Successful authentication to signin.amazonaws.com in Amazon AWS CloudTrail

About Sumo Logic

Sumo Logic's vision is to make the world's digital experiences reliable and secure. The Sumo Logic SaaS Analytics Log Platform provides powerful real-time analytics and insights to help practitioners and developers ensure application reliability, secure and protect against modern threats, and gain insights into their cloud infrastructures. By providing a SaaS analytics platform for cloud-native application observability and security solutions, Sumo Logic is empowering the people who power modern, digital business so they, in turn, can deliver reliable and secure digital experiences. For more information, visit www.sumologic.com.

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
855 Main Street, Redwood City, CA 94603

www.sumologic.com

Updated 10/23