What is SIEM?

SIEM stands for "Security Information & Event Management." In essence, it is the process of managing security and information events generated by an array of technology devices, services, and processes. This operation is accomplished through a deliberate approach of centralizing the collection, detection, investigation, and response to these events, which typically take the form of logs.

Collection

Devices generate logs that are "shipped" to a central SIEM collector.

Detection

Manual and module-based log parsing (scripting) look for keywords in the logs that may be actionable.

Collection

Security analysts then investigate select log alerts based on custom criteria and identify any correlations from other logs.

Response

IT security teams respond to the alert and remediate any issues identified.

These logs come from various disparate sources in a network and can take many formats. The overwhelming majority are structured text files with specific text strings within each file that allow your organization to parse out information based on text string matching to isolate the particular log events it's interested in.

SIEM in the Security Ecosystem

- SIEM sits in the center of End Point Detection & Response, Network Perimeter Security, and IT Compliance
- Combined with Threat Intelligence and Remediation Strategies, SIEM provides maximum impact on your IT Security posture
- Satisfy multiple controls across various compliance frameworks by deploying SIEM (PCI, NIST, SOC 2, CIS, etc.)

SIEM Use Cases

While these are not representative of all SIEM use cases, these three use cases are the three most common seen. In today's corporate environment, there are typically three main locations where work transpires:

The office or a co-location

An enterprise cloud such as Azure or AWS

At-home offices

SIEM can be deployed in all three of these scenarios to great effect and provide a massive amount of risk mitigation for the firm with a single solution.

ON PREMISE	CLOUD INFRASTRUCTURE	REMOTE WORKFORCE
Office Networks, CoLo's etc.	Azure, AWS, Google, etc.	Home Offices, Hot Sports, etc.
TYPICAL POSTURE	**TYPICAL POSTURE**	**TYPICAL POSTURE**
Log Collector + OS Agents (Installed Collectors)	S3/HTTP "Sources" Collector (Sumo+Hosted Collections)	OS Agents (Installed Collectors)
TYPICAL POSTURE	**TYPICAL POSTURE**	**TYPICAL POSTURE**
1. Setup Collector in Nework 2. Assign Ingestion Budget 3. Configure Cloud Sources	1. Create Hosted Collector 2. Assign Ingestion Budget 3. Configure Cloud Sources	1. Installed OS Agents

The RSI Security Solution

Cost-effective

No Capital Investment, no infrastructure to manage

Proven solution

Established effectiveness and reliability

Delivers fast value

Services provide tangible customer value

Cloud-native architecture

Scalable, elastic & resilient cloud architecture

Secure platform

Security first principles for peace of mind

SIEM Deployment Process

A thoughtful approach is required if your organization plans to implement SIEM in its security posture. Here is a typical 5-phase approach to rolling out SIEM with Sumo Logic.

sumo logic

SIEM Setup Process

Planning	Deployment	Trial Period	Customization	Refinement
Confirm Asset Profile	Deploy Collectors (Installed and Hosted)	Establish Baseline Ingestion Rates	Trial Converted to Full Account	Improve Log Heuristics
Design Your Deployment	Configure Log Shipping	Initial Customization (Reduce the Noise)	Finalize Alerts and Dashboards	Add New Data Sources
Estimate Ingestion Rates (GB/Day)	Confirm Data Sources and Validate Log Datasets	Finalize Ingestion Rates (GB/Day)	Develop Forensics Process for SOC	Add to Incident Response Plan

RSI Security has assessed, implemented, and currently manages SIEM operations for various clients as part of our consulting and managed security services. Even if your organization can't afford a full-time SIEM analyst team, it can easily outsource these operations at a fraction of the cost to enjoy the same benefits without the total investment required to mature them in-house with the Sumo Logic Cloud.

Want to learn more about **SIEM** and **how RSI Security can help**?

Request A Consultation Today