sumo logic

SIEM evaluation guide

Safeguarding your future

SIEM evaluation guide

The Security Information and Event Management (SIEM) market is at a critical juncture, rife with disruptions and innovations that require serious reevaluation of your current SIEM solution. Enterprises must navigate this volatile landscape, questioning whether their SIEM can keep pace with emerging threats and organizational needs. It's crucial to maintain a forward-looking perspective regarding the efficacy of security tools instead of reevaluating after a breach has already occurred, when it is too late. This guide is your roadmap to cutting through the noise, giving you confidence that your security posture goes beyond adequate into exceptional.

The first step in this journey is recognizing what might trigger your team to examine your SIEM more closely.

Recent security incidents and pen tests should be a wake-up call. They expose glaring vulnerabilities and gaps that organizations can no longer ignore and highlights critical capabilities you might need going forward in your solution.

Regulatory requirements and changes aren't just bureaucratic hurdles—they're crucial mandates that require robust security measures to avoid crippling penalties.

Growth initiatives whether expanding into new markets or adopting cutting-edge technologies, demand a security solution that can scale and adapt.

Budget cycles offer a prime opportunity to invest wisely in security rather than continuing with outdated or inadequate solutions.

Industry mergers and acquisitions these force you to confront whether your SIEM can withstand the shockwaves of market consolidation and still provide robust protection.

How to use this guide

This guide draws from various authoritative sources, including critical capabilities defined by various analyst firms for SIEM, Sumo Logic customer insights, and our expert analysis. This multifaceted approach ensures you comprehensively understand the SIEM market's current and future trends.

Five steps to evaluate your SIEM:

1. Are you collecting the right logs?
2. How is data transformed in your SIEM?
3. Does your SIEM offer advanced analytics?
4. Does your SIEM offer effective investigation?
5. Does your SIEM facilitate response?

Who are you?

CISO

Steps one, two, and five are key to optimizing budget and security tooling with a SIEM solution while delivering confidence, visibility, and robust protection in order to safeguard your organization's future.

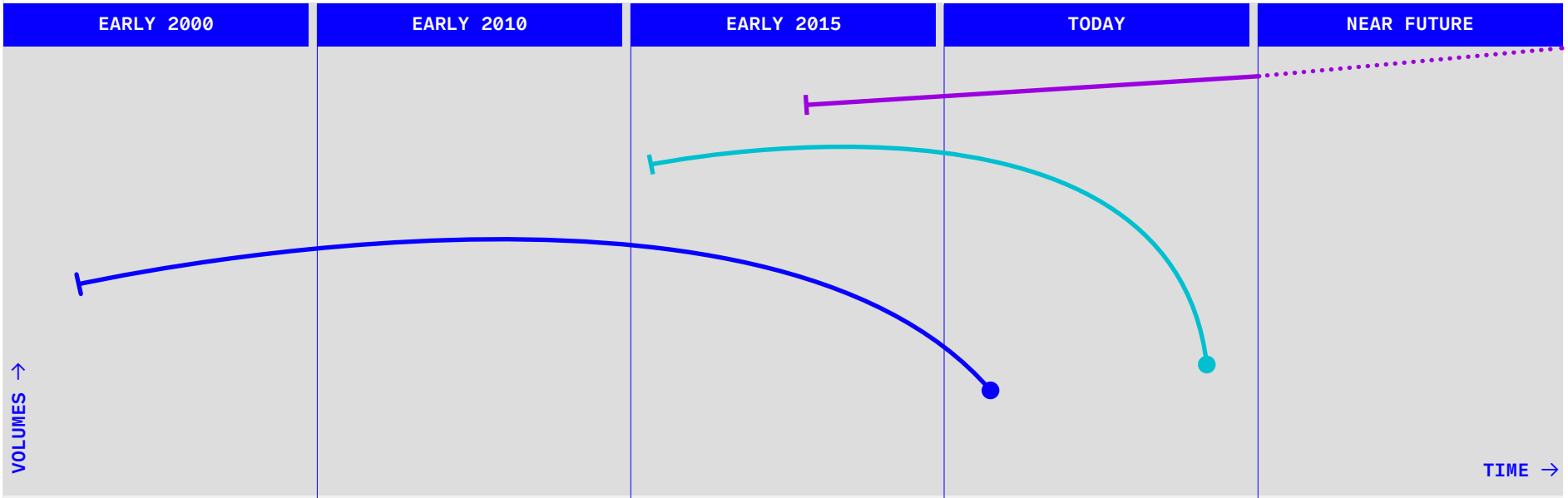
SOC MANAGER

Steps three, four, and five outline the necessary advanced analytics, investigation and collaboration capabilities to efficiently detect threats and enable you and your team to continually secure your organization.

SECURITY ANALYST

Steps four and five take a closer look at how ease of use and rapid, accurate insights from your SIEM solution can speed investigations and remediation, and reduce false positives.

What generation of SIEM do you have?



1st gen

Reactive search

ALERTS + LOGS
+ CORRELATIONS

Initially focused on basic log management and simple correlation capabilities, relying on manual log analysis for threat identification.

2nd gen

Near real-time

+ INDEXING

Introduced improved correlation engines, dashboards, and basic incident response workflows, enhancing visibility and response times.

3rd gen

Real-time analysis

+ BEHAVIORAL ANALYTICS
+ AUTOMATION

Featured real-time monitoring, integration with external threat intelligence feeds, and User Behavior Analytics (UBA) for insider threat detection.

4th gen

Scale and performance

+ CLOUD-NATIVE SCALE

Integrated advanced analytics, machine learning, and SOAR capabilities, with better support for cloud environments and hybrid infrastructures.

5th gen

Predictive security

+ AI-POWERED + DEVSECOPS
+ CONTEXT-DRIVEN INSIGHT

The fifth generation SIEM blends AI-driven insights, DevSecOps practices, and automated remediation, offering predictive threat detection and natural language interface..

Fifth generation SIEM

On the horizon, the fifth generation SIEM represents a significant advancement over the previous generation. It incorporates AI-driven insights providing recommendations and predictive threat detection and response, a unified platform for holistic security management, DevSecOps integration to embed security across development lifecycles, and automated remediation to contain and mitigate threats swiftly. Furthermore, fifth generation SIEM solutions incorporate large language models (LLMs) allowing a broader set of DevSecOps teams to interface with the solution using natural language and serve up recommended actions, correlate with real time threat intelligence, facilitate multi-stage detections, and provide custom insights tailored to their organization. If your SIEM is fifth-gen ready, excellent; otherwise, you may want to reevaluate your SIEM solution.

With over ten years of log analytics leadership and over one thousand security customers, we have created this evaluation guide as a resource for you to objectively evaluate your current SIEM solution. Using the provided criteria and associated scorecard, you will come away with the comprehensive understanding needed to drive the decision process for replacing your existing SIEM.

5 steps to evaluate your SIEM

At the core of evaluating your SIEM is ensuring that it can address threat detection, investigation, and response (TDIR) challenges.

1 Are you collecting the right logs?

Logs are the most fundamental and naturally generated artifact of digital computing.

Effective log collection is the cornerstone of a robust SIEM solution and when investigating an incident all critical logs need to be online, available, and part of your analysis.

In today's complex IT environments, data are generated from many sources, including on-premises systems, cloud services, SaaS applications, network devices, your security and intrusion prevention stack and of course endpoints. This data is the foundation for all subsequent threat detection, investigation, and response activities. However, the challenge lies in aggregating this diverse data accurately and efficiently. Scalability and speed are hallmarks of cloud-native SaaS solutions and must rise to the top of the list when evaluating SIEM log collection capabilities.

Also critical, solutions that provide licensing and consumption that enable you to effectively store and analyze all your enterprise-wide logs can cut hours and even days out of investigations that would otherwise require data staging, processing, and preparation before you can drive analytics and insights.

A robust SIEM solution must seamlessly integrate with various data sources, support real-time data ingestion, and handle multiple data formats, including vendor-agnostic, open-source collection technologies such as OpenTelemetry, to provide a comprehensive and unified security view. Without these components of data collection and consumption, teams are left with common challenges such as visibility gaps, integration complexity, and data quality issues.

Comprehensive data collection is essential to ensure that no critical data are missed and your security team has the information to detect and respond to threats promptly and effectively.

LOG COLLECTION EVALUATION CRITERIA

Comprehensive source integration

Ensure the SIEM can collect data from all relevant sources, including on-premises, cloud, and hybrid environments. This includes logs, network flows, endpoint data, and data from various SaaS applications.

Real-time data ingestion

Verify that the SIEM can ingest data in real time to ensure timely threat detection to respond quickly to emerging threats.

Support for diverse data types

The SIEM should support a wide range of data types, including logs, events, metrics, and other relevant data formats, to provide a holistic view of your organization's security posture.

Log storage and data retention

Check that security log data are stored securely with AES 256 encryption at rest and TLS encryption in transit, and retained for up to seven years or pursuant to regulatory bodies in your industry.

Log economics

Make sure your SIEM includes log economics and flexible pricing of security data to keep critical data flowing to the SIEM while mitigating cost overruns; optimally, your SIEM will include pricing per scan versus ingest-based pricing models.

MUST-HAVE CAPABILITY ACCORDING TO GARTNER®

Collection of infrastructure details and security-relevant data from a wide range of assets located on-premises and/or in cloud infrastructure.

STANDARD CAPABILITY ACCORDING TO GARTNER®

Gartner capability (standard): Allow for the collection of event data from disparate event sources, using multiple mechanisms (log stream, API, file processing) for the purposes of threat detection, use cases, reporting, and incident investigation.

Gartner, "Security Information and Event Management Magic Quadrant," Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.

2 How is data transformed in your SIEM?

Once collected, the SIEM transforms the data into a format that enables effective analysis and action.

Data transformation involves normalization, enrichment, and correlation processes that convert raw data into meaningful insights. In information security, analysts often face the daunting task of making sense of vast amounts of data from diverse sources. Without proper transformation, this data can remain fragmented and difficult to analyze.

Normalization is paramount for understanding network activities. It transforms disparate data from various sources into a unified format or schema that simplifies analysis. Despite many solutions touting normalization capabilities, their implementations often fail in effectiveness and ease of use. Normalization is the backbone of detection engineering, threat hunting, and security operations, converting raw messages into standardized records for seamless querying and analysis.

Not all schemas are created equal. The strength of normalization lies in the use of parsers and mappers to handle both structured and unstructured data. Parsers decode and extract crucial information from raw data, converting it into a readable, structured format. Mappers then align this data with a predefined schema, ensuring uniformity across diverse data sources. This process is especially critical when dealing with unstructured data, which can vary wildly in format and content yet contain some of the most critical, custom application insights.

Enrichment enhances normalized data with contextual information, such as threat intelligence feeds and asset data, helping analysts understand its significance and making detecting and responding to threats easier. Enriching valuable context to records makes them more informative and actionable. For example, command-line data enriched with threat intelligence can identify known malicious commands, improving detection accuracy and investigations.

DATA TRANSFORMATION EVALUATION

Effectiveness of normalization
Ensure the SIEM consistently and accurately applies a common schema and mapping field names.

Parser and mapper quality
Check the accuracy of parsers, efficiency of mappers, and ease of parser updates.

Performance and scalability
Evaluate processing speed, ability to handle large data volumes, unstructured data, and efficient resource use.

Integration capabilities
Assess compatibility with various data sources, API and plugin support, and interoperability with existing systems.

Contextual data integration
The SIEM must have robust integration of threat intelligence feeds and asset data.

Accuracy and relevance
Check the precision and relevance of the contextual information added during the SIEM data transformation process.

Ease of use
Check if the user interface is intuitive, the configuration is simple and flexible, the SIEM provides automation and investigation triggers, and offers robust support.

Impact on detection and response
Ensure the SIEM offers options to improve detection accuracy and investigation efficiency.

Performance and scalability
The SIEM must efficiently process data volumes and scale elastically with data volume growth.

MUST-HAVE CAPABILITY ACCORDING TO GARTNER®

Provide SIEM vendor content and facility for client-created content in areas including: analytics, data normalization, collection, and enrichment.

STANDARD CAPABILITY ACCORDING TO GARTNER®

Normaliztion, enrichment, and risk-score data from third-party systems.

Gartner, "Security Information and Event Management Magic Quadrant," Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.

3 Does your SIEM offer advanced analytics?

Data analytics powers the detection of sophisticated cyber threats within a SIEM solution.

Advanced analytics capabilities, including AI-driven threat detection and insight management, use machine learning to analyze large data volumes and identify patterns that traditional methods might miss. SIEM solutions incorporating machine learning models enhance threat detection by adapting to new threat patterns and improving over time.

User and entity behavior analytics is crucial in modern SIEM solutions, offering deeper insights into user and entity activities. By creating detailed profiles of normal behavior, UEBA can more accurately identify deviations that may indicate security threats, thus detecting sophisticated threats that traditional monitoring might miss.

Entity-centric detection and correlation and pattern recognition are key components of effective threat detection. By linking data from various sources, SIEM solutions can detect complex attack patterns that individual data points might not reveal. SaaS-based SIEM solutions offer significant benefits in maintaining, updating, and creating detection rules, including a customizable rules engine that aligns the SIEM solution with an organization's unique security posture. Another key aspect of the SaaS delivery model is the ability to instantly incorporate new and updated detection rules curated by expert threat research teams to keep security content current to help secure against emerging attacks.

Incorporating these AI-driven features ensures a SIEM solution can handle the dynamic nature of modern cybersecurity threats, providing security teams with the necessary tools to protect their organizations. The SaaS model further enhances this capability by keeping the SIEM solution updated with the latest advancements in threat detection and analytics, ensuring continuous protection against emerging threats.

ADVANCED ANALYTICS EVALUATION CRITERIA

Anomaly detection
Verify the SIEM highlights deviations from normal user and system behavior, crucial for identifying potential security incidents.

Behavioral analysis
Assess how well the SIEM monitors user and entity activities to detect unusual behavior, aiding in identifying unknown and insider threats.

Holistic view
Ensure the UEBA capabilities provide a comprehensive view of activities across users and entities, identifying correlations that single-point monitoring might miss for insider threat detection.

Enhanced contextual analysis and awareness
Review how the SIEM incorporates various data sources for more accurate threat detection and uses contextual information for risk assessment, alert prioritization, and reducing false positives.

Entity profiling and behavior baselines
Determine if the SIEM builds comprehensive profiles and establishes baselines for each entity, improving anomaly detection.

Continuous updates and reduced maintenance
Validate the SIEM is a true SaaS solution to ensure detection rules and models are updated with the latest threat intelligence, reducing maintenance burden.

AI-infused capabilities
Check that the SIEM has AI interwoven into its capabilities, such as AI-powered log clustering and noise reduction, automatically adjusting for seasonality and reducing alert fatigue.

Scalability and flexibility
Assess how well the solution scales resources based on demand for optimal performance and cost-efficiency.

Transparency and ease of customization
Ensure the SIEM allows for easy rule construction and operation visibility, with a user-friendly interface for customization.

Predefined rules and templates
Apprise the provided library of customizable predefined rules and templates for tailored detection strategies.

Rule testing and simulation
Review the ability to test and simulate rules before deployment to ensure performance and accuracy.

MUST-HAVE CAPABILITY ACCORDING TO GARTNER®

Ability for end-users to self-develop, modify, and maintain threat detection use cases utilizing correlation-, analytic-, and signature-based methods.

STANDARD CAPABILITY ACCORDING TO GARTNER®

Advanced analytic capabilities using user and entity behavior analytics (UEBA) and data sciences (i.e., supervised and unsupervised machine learning, deep learning/recurrent neural networks).

Threat intelligence platform (TIP) capabilities to manage intelligence and supply contextual information about threats.

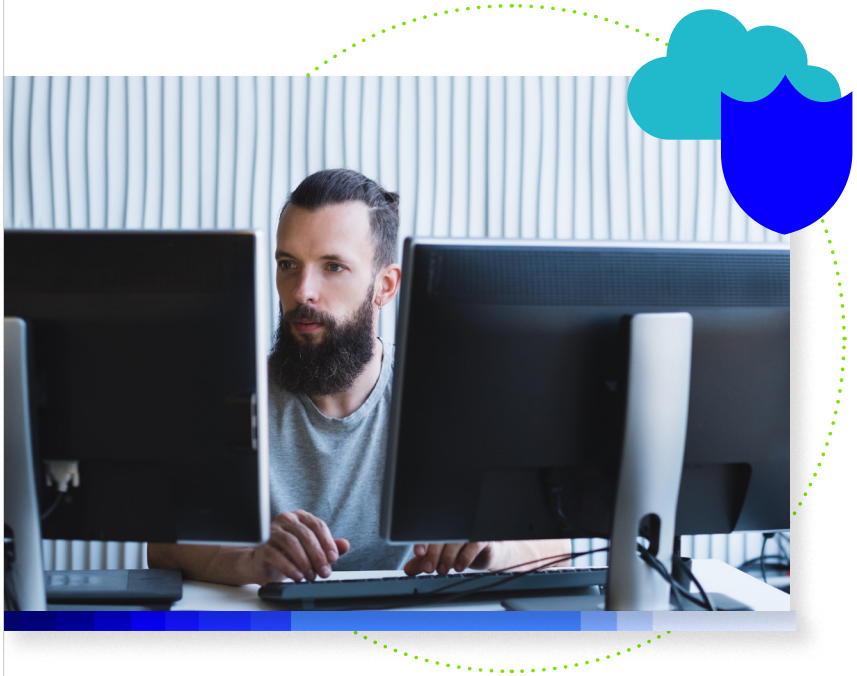
Gartner, "Security Information and Event Management Magic Quadrant," Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.

4 Does your SIEM offer effective investigation?

Identifying potential threats is only the beginning.

Effective threat investigation is crucial for understanding these threats' full scope and impact. This process involves detailed analysis, root cause identification, and efficient alert management to address genuine threats while minimizing false positives promptly.

Security investigation features in a SIEM solution should support detailed analysis of security incidents, including drilling down into events, viewing detailed timelines, and correlating related events across different data sources. Root cause analysis is essential for identifying the underlying cause of a security incident, understanding its origin and spread, and preventing future occurrences. Effective alert triage and false positive reduction ensure that security teams focus on genuine threats.



INVESTIGATION EVALUATION CRITERIA

Identifying initial compromise
Ensure the SIEM helps trace incidents back to the initial point of compromise, identifying the first affected system or user and how the threat entered the environment.

Tracking threat propagation
Assess the provided tools to track the lateral movement of the threat within the network, identifying affected systems and understanding the attacker's methods.

Determining impact
Verify the SIEM helps quantify the full impact of the incident, including data exfiltration, system downtime, and potential regulatory implications, to inform effective response and remediation.

Alert prioritization
Confirm the SIEM prioritizes alerts based on severity and potential impact, helping analysts focus on critical threats first.

Contextual information
Determine if alerts include relevant details about affected assets, involved users, and associated threat intelligence to help analysts quickly assess relevance and urgency.

Automated triage
Check the automated triage capabilities use a combination of machine learning and predefined rules to reduce analysts' time spent on initial alert assessments by automatically classifying and prioritizing alerts.

False positive reduction
Validate that the SIEM minimizes false positives by refining detection rules and incorporating analyst feedback to ensure that alerts are meaningful and actionable, reduce alert fatigue, and improve efficiency.

Rapid root cause identification
Ensure the SIEM features and includes powerful analytics to sift through vast amounts of data and provide complete visibility across on-premises and cloud environments. This includes custom searches via an in-built query engine, the ability to instantly query structured and unstructured data, and machine learning to reduce and deduplicate repeat logs.

MUST-HAVE CAPABILITY ACCORDING TO GARTNER®

Provision of case management and support of incident response activities.

STANDARD CAPABILITY ACCORDING TO GARTNER®

Orchestration and automation of tasks and workflows to enhance investigations and limit the impact of incidents.

Gartner, "Security Information and Event Management Magic Quadrant," Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.

5 Does your SIEM facilitate response?

Collaboration is essential for effectively managing and responding to security incidents in cybersecurity.

Especially when incidents and breaches can occur at an application level. Kubernetes containers, GitHub repositories, or insecure cloud infrastructure components can all be exploited during an attack, but these are not typically monitored or maintained by security teams. Furthermore, with resource-constrained teams across all three DevSecOps teams, leveraging powerful automation is critical for speed and efficiency.

As such, a SIEM solution that facilitates teamwork and communication can significantly enhance a security team's efficiency and effectiveness through features like customizable dashboards, automated reporting, compliance tracking, and streamlined response processes. Additionally, a SIEM solution's response capabilities are vital for promptly and effectively managing incidents, including predefined and customizable incident response workflows, automation and orchestration of repetitive tasks, and tools for post-incident reviews to continuously improve the security posture. What used to be considered a separate solution, Security Orchestration and Automated Response (SOAR) is increasingly becoming table stakes for SIEM functionality.

A SIEM dashboard provides real-time visualizations of security data to efficiently monitor the organization's security posture. Reports are crucial in communicating findings, progress, and outcomes to stakeholders within and outside the organization. Compliance features in a SIEM ensure adherence to regulatory requirements and industry standards, which is crucial for avoiding penalties and maintaining trust. Overall, robust response capabilities are essential for effectively managing and mitigating security incidents.

COLLABORATION EVALUATION CRITERIA

Customizable dashboards
Review users' ability to create dashboards to display key metrics, trends, and alerts relevant to their role, with real-time updates for prompt responses to threats.

Single source of truth
Verify your SIEM gathers all critical data in one place, enabling DevSecOps practices and boosting cross-team collaboration. Also pursue pricing and consumption models that provide unlimited users, to enable all relevant teams to leverage the solution.

Role-based access controls and views
Ensure permissions can be assigned by role to enable access for authorized users, with information tailored for each team member, enhancing data relevance and usability.

Automated and custom reporting
Check that automated report generation ensures consistency and saves time, while custom reports cater to specific needs like compliance audits or executive summaries, featuring visual summaries and detailed data.

Regulatory compliance
Assess how well the SIEM facilitates data collection, retention, and reporting for regulations such as GDPR, HIPAA, and PCI-DSS, with comprehensive audit trails for transparency.

Compliance dashboards and reports
Evaluate specialized tools for monitoring and demonstrating regulatory adherence.

Incident response workflows
Ensure predefined and customizable workflows guide analysts through security incidents.

Automation and orchestration
Check how well the SIEM integrates with log analytics platforms and external SOAR tools to automate response actions and improve efficiency, and ensure orchestration supports human-in-the-middle workflow designs.

Collaboration tools
Validate the SIEM facilitates effective communication and coordination during incident response with shared workspaces and real-time chat.

Post-incident reviews
Ensure the solution supports analysis of response effectiveness, identifying areas for improvement, and updating response plans for continuous enhancement.

MUST-HAVE CAPABILITY ACCORDING TO GARTNER®

Report generations to support business, compliance, and audit needs as needed.

STANDARD CAPABILITY ACCORDING TO GARTNER®

Storing of essential security event data long term and making it available for searching.

Fully featured security orchestration automation response (SOAR) functionality.

Gartner, "Security Information and Event Management Magic Quadrant," Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.

Rating system based on evaluation criteria

How to interpret your results:

Score 0 - 30	Consider a new solution
Score 31 - 40	Adequate coverage
Score 41 - 50	Your current SIEM provides adequate security coverage

SIEM Scorecard

CAPABILITY	IDEAL SIEM CAPABILILITIES	CURRENT SIEM CAPABILITIES		POINTS
DATA COLLECTION	• Cloud-native SIEM • Multi-cloud and on-prem collection • Out-of-the-box connectors • Support for structured and unstructured data	Limited data sources, manual integration required.	0-3 points	
		Supports multiple data sources, some automation in integration.	4-7 points	
		Comprehensive data collection, and seamless integration with all relevant sources.	8-10 points	
DATA TRANSFORMATION	• Automatic alert triage and threat correlation • Multiple Threat Intelligence feeds • 100's of app integrations, parsing, and normalization • Automated & playbook enrichment • Raw data storage for search	Basic normalization, minimal enrichment.	0-3 points	
		Effective normalization, good enrichment capabilities.	4-7 points	
		Advanced normalization and enrichment, robust correlation.	8-10 points	
DATA ANALYTICS	• User and Entity Behavior Analytics • Pre-built and customizable rules • AI-powered rule tuning • Peer benchmarking	Basic analytics, limited detection capabilities.	0-3 points	
		Advanced analytics, good behavioral analysis.	4-7 points	
		AI-driven analytics, comprehensive behavioral analysis, highly customizable rules.	8-10 points	
INVESTIGATION	• Cloud-native SIEM • Multi-cloud and on-prem collection • Out-of-the-box connectors • Support for structured and unstructured data	Basic investigation tools, limited root cause analysis.	0-3 points	
		Good investigation tools and effective root cause analysis.	4-7 points	
		Advanced investigation capabilities, robust root cause analysis, strong forensics.	8-10 points	
RESPONSE	• Automatic alert triage and threat correlation • Multiple Threat Intelligence feeds • 100's of app integrations, parsing, and normalization • Automated & playbook enrichment • Raw data storage for search	Basic case management, minimal collaboration tools.	0-3 points	
		Good case management and some collaboration features.	4-7 points	
		Comprehensive case management, strong integration with SOAR, excellent collaboration tools.	8-10 points	
			TOTAL SCORE	

Consider a new solution (0-30)

A low SIEM evaluation score indicates significant underperformance in critical areas, exposing your organization to substantial security risks, operational inefficiencies, and potential regulatory non-compliance. Immediate action is required to address these deficiencies, including reconfiguring the existing system, investing in additional training for your security team, or considering more capable alternative solutions to meet your security needs better and enhance your overall security posture.

Adequate coverage (31-40)

A medium score indicates that the SIEM solution is functional but has notable limitations affecting optimal security operations, adequately covering basic requirements but lacking advanced capabilities for comprehensive threat detection, analysis, and response. This score suggests that while the solution performs reasonably well in data collection and basic analytics, it falls short in advanced threat investigation and seamless integration with other security tools. To address these limitations, consider incremental improvements, integrating supplementary tools, or gradually transitioning to a more robust solution to meet the increasing complexity of modern cyber threats.

Great security foundation (41-50)

A high score in your SIEM evaluation indicates excellent performance across key functionalities, effectively supporting your security needs with comprehensive data collection, advanced analytics, and seamless integration with other security tools. This level of performance signifies a robust security posture capable of proactively addressing modern cyber threats and includes advanced features such as real-time threat detection, AI-driven analytics, and strong collaboration tools. To maintain and enhance this performance, consider leveraging your high-performing SIEM for a comprehensive DevSecOps strategy, ensuring continuous security monitoring, rapid threat response, and enhanced collaboration between development, security, and operations teams.

Ready to evaluate Sumo Logic Cloud SIEM?

Book a demo

About Sumo Logic

Sumo Logic, Inc. unifies and analyzes enterprise data, translating it into actionable insights through one AI-powered cloud-native log analytics platform. This single source of truth enables Dev, Sec and Ops teams to simplify complexity, collaborate efficiently and accelerate data-driven decisions that drive business value. More than 2,400 customers around the world rely on the Sumo Logic SaaS Log Analytics Platform for trusted insights to ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. **For more information, visit www.sumologic.com.**

Disclaimer:
Gartner, Security Information and Event Management Magic Quadrant, Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.

sumo logic