sumo logic

WHITEPAPER

Cloud SIEM Buyer's Guide

The essential requirements to modernize your security operations

Security analysts have a lot of responsibilities, and when it comes to daily security operations, ensuring that there isn't a security incident that will interrupt the flow of business or put customer data at risk is priority number one.

To aid in this goal, security operations center (SOC) teams have adopted many tools to the organization's cybersecurity stack, including security information and event management (SIEM) solutions to help with log collection, threat hunting, and investigation efforts.

When it comes to security investigations, experts recommend aiming to meet the 1-10-60 rule:

1 minute to detect, 10 minutes to investigate and 60 minutes to remediate.[i] That means security analysts should aim to investigate threats in 10 minutes to effectively combat sophisticated cyberattacks and avoid the damage a successful breach can inflict on an organization's reputation and bottom line.

However, the reality is that even with existing SIEM investments, SOC teams are challenged with time consuming and complex investigation cycles. In fact, according to Ponemon research it takes security teams an average of 280 days to detect and containa breach.[ii]

Selecting the right SIEM solution will make a big impact in advancing your computer security incident response plan (CSIRP). The goal is to have a SIEM you can trust and rely upon to accelerate and automate your efforts, so you have success in protecting and defending your organization.

Whether you're looking for your first SIEM solution or are considering a new one, this buyer's guide will provide helpful guidance on the critical considerations for selecting a modern cloud SIEM that will provide your organization with the best fit now and in the years to come.

The purpose of SIEM solutions

The first concept of SIEM was created in the late 90's as network and security teams looked for ways to consolidate the event log information from their various devices to a central location. The centralized logging function of SIEM started as security information management (SIM) that provides organizations with data log collection and aggregation. This served as a central repository for all event logs that were generated in an environment. The core goal of the SIM was log monitoring and retention to address compliance requirements.

As technology evolved, central data collection wasn't enough. SOC analysts wanted to apply logic to the data to define patterns of known bad activity and receive real-time alerts that this activity was happening rather than only responding following a postmortem analysis. This gave rise to security event management (SEM).

SEM allowed the data to be analyzed with matching lists, mapping network traffic, grouping critical systems, and even joining various events and alerts together to look for a sequence of activity instead of individual events. SEM also introduced features for managing investigations through case management and response workflows. This included grouping related alerts to a case, assigning cases to a user or team, and then tracking the activity and information until the investigation could be closed with an outcome.

Understandably, the natural pairing between SIM and SEM solutions provided the origination for today's SIEM market. While SIEM often describes a tool for SOC analysts that collects event data and log information and then analyzes and prioritizes the data collected from security events, almost every SOC must still invest in several tools to optimize the event prioritization and response efforts. In fact, 45% of organizations use more than 20 tools when specifically investigating and responding to a cybersecurity incident.[iii]

However, the high volume of disconnected tools creates complex security environments that diminish efficiency and introduces challenges for SOC teams to manage enterprise incident response processes.

Indeed, with today's SIEM tools, security teams face many challenges that must be addressed with a modern SIEM approach.

Trends driving the imperative for a modern, cloud SIEM approach

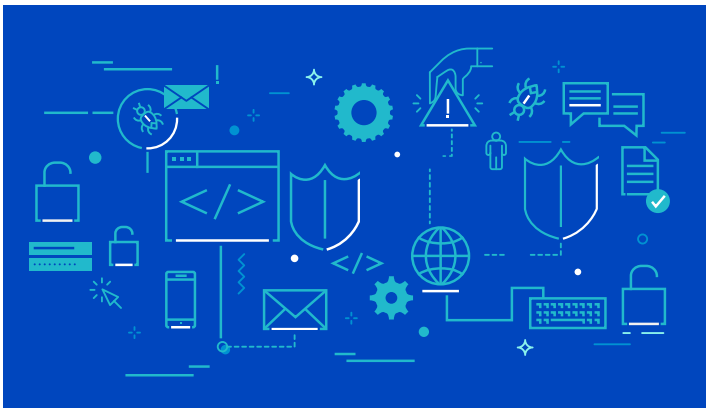
Increasing the enterprise data security footprint with cloud adoption

Undoubtedly, the way companies conduct business has changed significantly since SIEM solutions were first introduced. Business-enabling technologies and systems like cloud storage and services have been innovating at a breakneck pace. As a result, SOC teams have needed to continually redefine their plans for security monitoring and investigations to adapt.

Cloud migration spending is growing significantly with 32% of total IT budgets being allocated to cloud computing in 2021.[iv] This has introduced the imperative for security visibility across an organization's infrastructure; however, more than one-third (33%) of security professionals cite the lack of threat visibility across both on-prem and cloud environments as the greatest challenge with their existing SIEM solution.[v]

Monitoring the ever-expanding attack surface

As one would guess, cloud adoption and migrating apps to the cloud have shifted the threat landscape, creating an exponentially expanded attack surface. This has introduced distributed networks, giving cybercriminals more avenues whereby they can launch their attacks on companies. Think of all the possibilities available to attackers with mobile and IoT devices, multi-cloud environments, containers, and modern applications, such as load balancers, virtual private cloud (VPC) flows, and microservices.



Consequently, the expanded corporate attack surface has created one of the greatest pressure points for organizations to establish security monitoring and real-time intelligence. In fact, 67% of security professionals said their increase in the number of security alerts stems from new and evolving threats, while 55% blame the increase in their cloud infrastructure.[vi]

Legacy and even newer SIEM solutions weren't built with a cloud-native architecture, which means they can't readily monitor this attack surface. This limited support for diverse data sources and

locations inhibits your ability to tie in all your data types across all of your on-prem and cloud environments.

Managing the crushing volume of security alerts

While SIEM solutions fill the need of collecting logs and analyzing them for potential threats, in common cases, SOC teams are getting buried under a mountain of tens of thousands of daily alerts. As a result, 83% of security stakeholders indicate that their team suffers from "alert fatigue" due to the high volume of security alerts. Addressing this massive volume with human capital is also unrealistic. The majority (75%) of organizations report they would need to hire three or more analysts to address their security alerts in the same day.[vii]

However, with the pervasive shortage of trained security professionals, hiring additional staff is not even an option as a potential solution for organizations to manually investigate and triage their never-ending onslaught of alerts.

The simple truth is, with existing SIEM solutions there are simply too many alerts. Security teams can't get to all of them, which leads to CSIRP processes that are slow and inefficient—not to mention the advanced persistent threats (APTs) and other attacks that are missed and left unfettered to do their damage.

83%

Security stakeholders indicate their team suffers from "alert fatigue" due to the high volume of security alerts

Cloud SIEM selection criteria

No doubt, SIEM solutions are powerful products with a lot of "bells and whistles." Ultimately, your SIEM must provide the capabilities to address your biggest security need: to identify indicators of compromise (IOCs) quickly and accurately across your entire corporate infrastructure.

It's important to segment your SIEM evaluation into sections that take a close look at the solution's ability to manage data sources across your organization's infrastructure, including your multi-cloud and on-premises investments. Your SIEM also must readily scale and provide automation to handle the in-depth analytics that deliver the actionable intelligence you need.

Evaluating the solution's capabilities across the following areas will ensure it provides a strong fit for your organization's needs.

Requirement #1: Take your SIEM to the cloud for scalability and management efficiency

There is so much that a SIEM must do to be effective, so, as a starting point, it's important to make a firm decision on the solution's architecture to ensure it can scale to meet the demands that will be put on it. That decision should be laser-focused on selecting a cloud-native solution.

As SIEM vendors sprinted to bring cloud offerings to market, many "SaaS-ified" their solution by porting the software code to a cloud-hosted environment. This approach gave vendors a way to support the cloud and join the "cloud revolution," but this approach doesn't support the true scalability requirements that organizations should expect from their SIEM solution.

The distinction between a cloud-native and cloud-based solution is especially important, because only cloud-native technology can provide the performance and simplicity SOC teams require to scale for big data analytics that addresses an organization's wide range of security use cases—from user monitoring to network traffic analysis, privileged user activity, and more. For a SIEM to provide accuracy in detecting anomalous activity and advanced attacks, organizations will want to ingest all of the data from across their infrastructure footprint, including structured, unstructured, and streamed data.

When you think about the scalability requirements through that lens, it provides a better understanding of the magnitude of scale your solution should provide. In terms of numbers, a cloud-native solution should support processing hundreds of petabytes of data per day.

Selecting a solution that is built in the cloud also minimizes the attack exposure to the SIEM. While an on-premises SIEM can potentially be accessed and compromised from many entry points, selecting a cloud-native SIEM narrows security down to one service to monitor.

Requirement #2: Quickly identify IOCs and gain automated insights

Attackers can gain access to your data and environment from any unsuspecting avenue, so a modern cloud SIEM solution should support ingestion from your company-wide data sources. And, when it comes to data sources, to say there are a lot is an understatement.

From your servers and HVAC controls in the data center to your keycard access to protected areas—all of your data should be monitored. Then, there are your security controls, such as your firewall, IDS/IPS, endpoint security, and more that should be

covered. Finally, your multi-cloud services, data workloads, and the traffic connections made between them and the Internet, as well as what they're reaching out to should be monitored by your SIEM. If your SIEM can't hook into all this data, then it should be removed from your vendor short list.

A cloud-native architecture also adds value here as it provides an API-driven approach, which makes data integrations easy. This is especially important because third-party integrations are a key factor to gain quick insights.

In addition to ensuring your SIEM can support all of the data ingestion, it's essentially important that the solution provides analytics capabilities that go well beyond traditional SIEM correlation rules to free you from the manual effort of triaging every alert for validity. The right SIEM solution should apply the power of analytics and automation to reduce your alert funnel from millions down to a couple hundred, for example, to accelerate and streamline your efforts in detecting those "needle in a haystack" IOCs.

Solution requirements

- Empowers your organization to ingest security-relevant data from cloud, on-premises, and hybrid architectures to effectively provide comprehensive security monitoring and detection across your whole infrastructure.
- Automates alert triage using advanced analysis techniques, such as pattern and threat intelligence matching with correlation logic, statistical evaluation, and anomaly detection to filter the raw records down to meaningful Signals in near real-time.
- Automates level 1 and 2 security analyst workflows with intelligent, correlated, and prioritized clustering of events and other data enrichments for analysts to immediately respond.
- Performs correlation analysis on data that covers longer time periods; for example, alerts should cover up to 30 days of historical data to surface the true high-priority detections.

Requirement #3: Serves as a single platform that unifies teams and consolidates tools

Because today's traditional SIEM has provided limited analytics that only goes so far, typically leaving security analysts with an overwhelming number of alerts, SOC teams have looked to separate correlation tools to try to fill the gap. SOC teams have invested in network traffic analysis (NTA), endpoint security, threat intelligence, and other tools, however the result is a piecemeal and complex process.

According to Ponemon research, the greater the number of tools a security team uses creates an adverse effect on their ability to detect and respond to an incident. Their study found that SOC teams with more than 50 tools ranked 8% lower in their ability to detect and 7% lower in their ability to respond to an attack.[viii]

Your cloud SIEM solution should help mitigate the overload of tools by allowing you to use a single platform that provides these capabilities.

Solution requirements

- Provides a single platform that provides capabilities for log management, metrics, SIEM, NTA, and alert triage and prioritization with investigation workflows.
- Unifies your development and security staff with a solution that allows all users to work together with the same consistent and trusted data set, without incurring additional per user licensing fees.
- Includes integrated threat intelligence feeds that enrich the solution's analytics at no additional charge. Look for feeds such as, CrowdStrike threat intelligence, TAXII intel sharing, and YARA rules from GitHub.

Requirement #4: Powerful and simple user interfaces that streamlines your workflows

Legacy SIEM solutions have often had a reputation as being significantly complex and only usable by security staff with advanced training. Your ideal modern SIEM, should set a new standard—one that provides clear and purpose-built user interfaces along with built-in workflows that are designed for simplicity and ease of use by your entire security team to solve a wide range of use cases.

A SIEM that makes it easy to navigate through a threat investigation, without requiring a "data analytics PhD" will provide your team with a highly effective security tool that can be thoroughly leveraged across security operations.

Solution requirements

- Includes a powerful search interface to quickly find the information you need.
- Features a modern, purpose-built security interface designed for security analysts.
- Provides streamlined SecOps workflows designed with a prioritization-based process that enables analysts to intuitively verify alerts and investigate incidents.
- Delivers pre-built and supports customizable queries across all of your data and analytics that let you distill high-priority events from large data volumes.

Requirement #5: Native coverage for multi-cloud and on-premises environments

It is probably self-evident, but still important call out that your SIEM solution must provide full coverage support for your infrastructure. Providing support for a single cloud environment or specific set of supported applications is not sufficient as this will

lock you into a fixed investment that doesn't support the flexibility for you to make infrastructure changes as you continue your digital transformation initiatives.

Just as the market has seen enterprise environments change significantly in the past decade, there will surely be more changes in the future. Ensuring your SIEM provides broad coverage will make it easy to expand your SIEM's integrations in the future if your organization decides to expand its cloud infrastructure investments.

Solution requirements

- Provides complete cloud coverage to unify your security analytics and investigations across Amazon Web Services, Azure, and Google Cloud.
- Simplifies the data connection process with turnkey integrations that can be activated by an API key.
- Readily supports creating custom correlations across your data sources.

Requirement #6: Easy-to-use with fast time-to-value

Every SIEM requires content in order to function. Legacy SIEM solutions have typically required organizations to make a significant time investment, upfront, to develop content during the initial solution purchase and implementation phases. However, thereafter, few companies have had the time or resources required to develop new use cases following their SIEM purchase, resulting in an under-utilized product or one that has become "shelf ware."

Digital transformation has made corporate infrastructures incredibly dynamic and continuously evolving. As a result, content development for your SIEM use cases must be simple and effective. Your chosen solution should include out-of-the box content for your security and compliance use cases. In addition, creating custom content and integrating new security sources should be a straightforward effort to ensure you can readily support new use cases as your environment inevitably changes. Ultimately, the capabilities for this requirement should enable your organization to go from initial set up to uncovering meaningful security insights within days.

Solution requirements

- Provides fast, SaaS-delivered platform startup and simple, intuitive management that allows your SOC team to experience value in days.
- Features effective out-of-the box content for cloud and on-premises security, PCI and other compliance requirements.
- Supports custom rule creation to help you develop new use cases, over time, that address your organization's specific needs.
- Provides comprehensive support for products, vendors, rules, and applications.
- Makes it easy to train and onboard users by providing online and onsite certification courses, high-quality product documentation, and an intuitive user interface with built-in help tips.

Requirement #7: Architected using security best practices

Entrusting your data to a third-party service provider requires rigorous security measures, so taking your SIEM to the cloud means it must apply airtight security best practices that provide the assurance that your data is safe from compromise.

Your SIEM vendor must demonstrate that they have applied best-of-breed technologies and stringent operational processes to ensure that your data is completely safe at all times.

Solution requirements

- Built in the cloud, the platform must demonstrate a strong commitment to data security. The vendor should provide their processes and details across several areas:
  - Logical data separation
  - Physical security of the cloud data centers
  - Encryption of data in transit and at rest
  - Account creation
  - Authentication mechanisms
  - User level security
  - Node security
  - Vulnerability and testing program
  - Vendor's access to your data
  - Data redaction and deletion
- Look for validations from compliance attestations and certifications that help speak to the vendors' commitment to data security, including:
  - FedRAMP authorized (moderate impact level)
  - PCI DSS 3.2.1 Service Provider Level 1
  - SOC 2 Type 2 audit report
  - HIPAA Security Rule Attestation of Compliance
  - ISO 27001 certification
  - CSA STAR Level 2 certification

Requirement #8: Provides high ROI with cloud-friendly licensing model

A SIEM is an essential solution for the SOC and should be considered a long-term investment. Therefore, it's important to consider the upfront and on-going costs as part of your selection criteria.

Many CISOs and security analysts have witnessed their company's data grow much faster than anticipated. This is to be expected as a byproduct of our "digital era." Undoubtedly, your data volumes will continue to grow as well. Likewise, ingesting all of your organization's data is a valuable security approach to ensure your

SIEM has the breadth of data to uncover harder-to-detect APT traffic. All of these data requirements should be considered when it comes to your SIEM costs.

Most SIEM solutions are priced by a one-size-fits-all data volume model—the more data you ingest and analyze, the more expensive your costs. This price prohibitive model is not optimized for the real-world flexibility for your SOC team to analyze data across different use cases, variability, or retention requirements. Inevitably, this approach forces you to make a trade-off to not analyze all your data, which, in turn, creates security blind spots and impedes you from getting full value from their data.

Instead, your vendor should provide a flexible, value-based pricing model. By leveraging this model, you can avoid the common analytics tradeoffs and enjoy an economical platform with predictable costs.

Solution requirements

- Provides a pricing model that offers the choice and flexibility on how you want to collect and analyze each data type, delivering a pricing approach with a high return on investment.
- Provides real-time visibility into your data usage so you know where you stand at all times and don't experience surprise overages and invoices.
- Flexible, data tiered pricing approach that enables you to ingest all of your data and decide how you want to align its analytics value with options for continuous, frequent, and infrequent analytics.

Conclusion

There's one thing organizations can count on: cybercriminals will continue to innovate and evolve their attack techniques. Your SIEM solution must provide the essential capabilities to support your investigations at speed and at scale.

The ideal solution should be built on a cloud-native architecture to support the scalability required for data analysis. It should also be easy for your existing SOC team to manage, and it should alleviate many of the investigation burdens organizations face today, including scalability and alert fatigue.

A solution that automates your alert analysis will provide your team with the most important, high fidelity insights that require your team's attention. And, to ensure your chosen solution has the best information to analyze, your SIEM should provide coverage for all your data sources, regardless of location, and it should provide out-of-the box content and ongoing content development.

When you apply the SIEM requirements from this guide, you'll be well on your way to selecting a solution that provides the best support to automate your SOC, accelerate your investigations, and, ultimately, empower your team to protect the organization.

About Sumo Logic

Sumo Logic Inc., (NSDQ: SUMO) is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy.

To learn how SumoLogic's cloud-native SIEM can modernize your SOC, visit:

https://www.sumologic.com/solutions/cloud-siem-enterprise/

---

[i] CrowdStrike. 2020 CrowdStrike Global Threat Report. 2020
[ii] Ponemon Institute. Cost of a Data Breach Report. 2020.
[iii] Ponemon Institute. Cyber Resilient Organization Report. 2020.
[iv] Forbes. 32% Of IT Budgets Will Be Dedicated To The Cloud By 2021. August 2020.
[v] Sumo Logic. 2020 State of SecOps and Automation. June 2020.
[vi] Ibid
[vii] Ibid
[viii] Ponemon Institute. Cyber Resilient Organization Report. 2020.

Learn more

To learn how Sumo Logic's cloud-native SIEM can modernize your SOC, visit:

https://www.sumologic.com/solutions/cloud-siem-enterprise/

sumo logic

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

Updated 02/2021