What is SIEM? A complete guide to Security Information and Event Management

SIEM definition – what is SIEM?

Security Information and Event Management (SIEM) is a solution that provides monitoring, detection, and alerting of security events or incidents within an IT environment. It provides a comprehensive and centralized view of the security posture of an IT infrastructure. It gives cyber security professionals insights into the activities within their IT environment.

How does SIEM work?

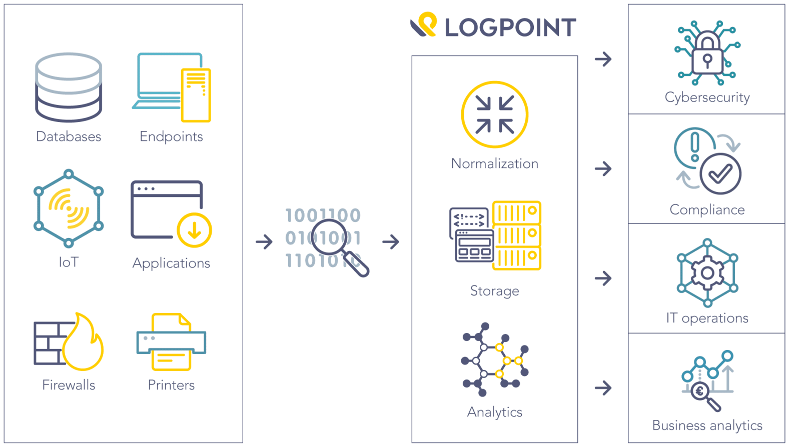
SIEM software collects and aggregates log data generated throughout the organization’s entire IT infrastructure. From cloud systems and applications, to network and security devices, such as firewalls and antivirus. The software then identifies, categorizes and analyzes incidents and events. SIEM analytics delivers real-time alerts, dashboards, and reports to several critical business and management units. Modern SIEMs also apply unsupervised machine learning to enable anomaly detection (User and Entity Behavior Analytics) to the collected log data.

Why choose LogPoint
Why companies choose LogPoint

Top 10 use cases to implement
Explore possibilities within LogPoint

Solutions for your industry
How LogPoint can benefit you

SIEM at a glance



What is a SIEM tool utilized for?

In the digital economy, enterprises must monitor and guard their data to protect themselves from increasingly advanced cyber threats. Chances are, your company has more data to collect and analyze than ever before. With exploding data volumes and increasing complexity, as IT infrastructures converge towards hybrid deployments between cloud and on-prem, it is increasingly important to have a central security solution to track behavior and critical events.

Additionally, the industry's lack of skilled resources means that security events can overburden analysts and Security Operation Centers (SOCs). The results are alert fatigue and the need to prioritize where to focus the company's security resources.

SIEM solutions enable companies to respond quickly and precisely to security incidents. A SIEM solution provides centralized collection, classification, detection, correlation, and analysis capabilities. This makes it easier for teams to

Without a SIEM solution, security analysts must go through millions of non-comparable and siloed data for each application and security source. In short, SIEM solutions can accelerate detection and response to cyber threats – making security analysts more efficient and accurate in their investigations.

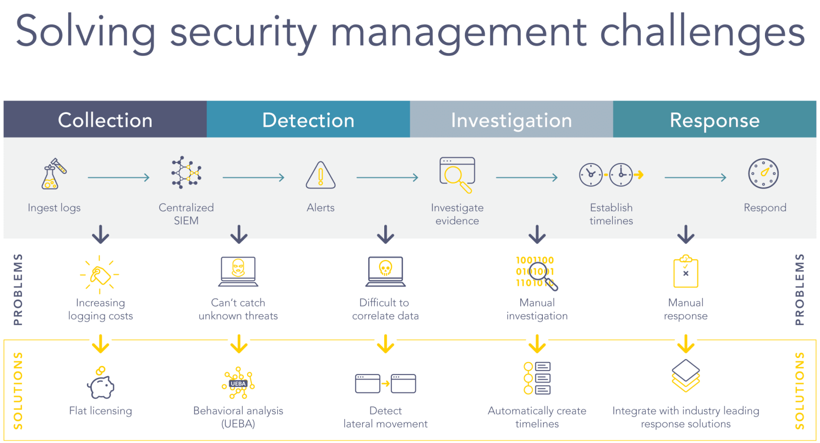
Limitations of traditional SIEM tools and solutions

SIEM tools have been around since 2005, but the SIEM definition and the answer to “what is SIEM?” has evolved considerably since then. Changes in the threat landscape have created a need to identify a wider variety of threats faster. For years, SIEM solutions were implemented to help security and IT teams analyze security alerts in real-time. But many traditional SIEM solutions cannot gather and analyze large amounts of data from a wider variety of sources – including IoT and proprietary applications.

Due to the exponentially growing amount of data, many organizations are facing limited value at increasing costs. Organizations that have a SIEM where the licensing model is based on data volume have to be selective of which data to ingest from which applications to not vastly exceed their budget. This can potentially mean missing out on data you need in the case of breaches or can leave your organization completely blind to anomalous behavior in critical systems

At the same time, there is a shortage of security analysts available in the labor market. Security operations teams struggle to keep up with the deluge of security alerts from a growing arsenal of threat detection technologies while relying on rule-based manual procedures for operations.

tools combined with developments in machine learning create new efficiencies in SIEM solutions that help remedy the cybersecurity skills gap.



Benefits of a modern SIEM solution

To establish a capable cybersecurity team, SIEM solutions are a must-have for businesses in any industry. Today's enterprises need a solution that can centralize, simplify, and automate security workflows to enable better analytics and incident response procedures.

The seven key benefits of a Modern SIEM are:

1. It collects and analyzes data from all sources in real-time

Organizations are generating more data than ever before. To keep up with the increase of data, SIEM tools must ingest data from all sources – including cloud and on-premise log data – to effectively monitor, detect, and respond to potential threats. Modern SIEM solutions can't just ingest and analyze more data. They thrive on it.

more visibility analysts will have into the activities. The more effective they will be in detecting and responding to threats.

2. It utilizes machine learning to add context and situational awareness to increase efficiency

Today's attacks are becoming more sophisticated, meaning organizations need equally advanced tools. Attackers often rely on compromised credentials or coercing users into performing actions that damage their organization. To identify these threats more quickly, SIEM tools should be equipped with machine learning capabilities like UEBA. This enables the monitoring of suspicious user behavior from internal as well as external threats.

With UEBA, organizations will see a dramatic increase in their SIEMs' ability to track and identify threats. UEBA limits false positives, so analysts have better situational awareness before, during, and after a threat – increasing efficiency and enable spending their limited time on real threats.

3. It's flexible and scalable architecture improves time to value

The amount of data produced by organizations has skyrocketed over the past few years, resulting in organizations needing big data architectures that are flexible and scalable. That way they can adapt and grow as the business changes over time. Modern SIEM solutions can deploy in virtual environments, on-premise, or in the cloud with the ability to handle complex implementations. Some SIEMs provide a short implementation time and low maintenance resource requirements, resulting in the SIEM providing value within a matter of days.

response tools

Modern SIEM solutions go beyond essential security monitoring and reporting. They provide analysts with the clarity they need to improve decision-making and response time. With innovative data visualization and intelligent business context to help analysts better interpret and respond to what the data is telling them, the incident response becomes more sophisticated. Better analytics means teams can efficiently manage incidents and improve their forensic investigations – all within a single interface.

5. It makes security analysts more productive from day 1

Once logs are collected, a SIEM system must provide use cases to help the security team detect and respond to threats immediately. For example, providing various correlation rules, complying with compliance standards, and detecting insider threats should be use cases that the SIEM security solution provides readily available across all applications immediately from implementation.

6. It reduces cybersecurity staff requirements

Today’s security teams are increasingly time-constrained, so enhanced automation frees analysts from manual tasks. It enables them to orchestrate responses to threats better. The best Modern SIEM solutions utilize unsupervised machine learning to help ease the burden of overworked security analysts. This is done by automating threat detection, providing enhanced context and situational awareness (such as threat intelligence), and utilizing user behavior to gain better insights.

volumes are continually increasing, and organizations shouldn't be punished for that. Modern SIEM pricing models should instead be based on the number of devices sending logs, meaning organizations won't have to worry that their data usage affects the cost, allowing them to focus on scaling for future business needs. Make sure you analyze the total cost of ownership, also for when the SIEM security needs to scale. Some vendors have added cost when increasing hardware capabilities or the number of employees that need access to the SIEM software.

LogPoint Roadmap

How to choose a SIEM solution?

internally or alongside a SIEM partner, to define and agree on the project scope and timeline. To determine the deployment's scope and timeline, you must identify, and more importantly prioritize, an initial list of use cases to dictate what the necessary log sources may be. It is also essential to agree upon a timeline for deployment to ensure the SIEM security aligns with the business's goals.

The four key questions to consider in the process of choosing a SIEM solution are;

1. **WHAT** applications to focus on?
2. **HOW** to respond when threats are detected?
3. **WHERE** are the most critical threats to your environment?
4. **WHY** are these the most critical threats, and what is the impact of a breach?

The three main steps in planning your SIEM project

1. ***Determine your business-critical data sources***

   Once you have a handle of the ideal project scope, you can then identify log sources within the scope to determine how to obtain the relevant data needed. For example, firewalls, intrusion detection systems, and antivirus software serve as prime data sources for SIEM security use cases. But there are many more, including routers, web filters, domain controllers, application servers, databases, and other digitally connected assets. It is crucial that you prioritize the sources included to ensure the SIEM provides the desired data to support the selected use cases.

2. ***Identify the high priority events and alerts***

   When it comes to protecting an organization against insider and external threats, security teams face an ever-growing list of security events that need to be analyzed and acted upon. To break through the noise, SIEM software can be used to make events and data more insightful. Still, businesses must first determine their high priority events and how to derive them from applications and devices within the infrastructure. This way, security teams can use the SIEM to spend more time on incidents and alerts that may be more critical to the business and its data.

3. ***Pinpoint your key success metrics***

must be determined before deployment to ensure maximum ROI. For example, reducing data theft or improving how businesses detect potential breaches or insider threats may be metrics to establish. But there are many others. Companies must determine what success means for them and how SIEM security use cases can be used to achieve it.

Businesses collaborating with LogPoint for a Modern SIEM solution can expect:

Fewer staff

Less spend

and response

A Modern SIEM solution provides real-time data analysis, early detection of data breaches, data collection, secure data storage and accurate data reporting to improve threat detection and response times.

frees security analysts from time-consuming manual tasks and enables them to better orchestrate a response to threats. The best Modern SIEM solutions utilize machine learning and user and entity behavior analytics (UEBA) to help ease the burden of overworked security analysts.

with a simple and predictable licensing model enables businesses to spend less to keep their data secure, regardless of the amount of data they have and the number of sources from which data is logged.

LogPoint's value proposition

We have a history of success in IT security and safeguarding businesses from risk and mitigating reputational and financial damage. By providing a simplified overview of your IT infrastructure you can make impactful business decisions.

By using, our advanced UEBA technology solution, based on machine learning, we give your security team and edge. We ensure less business downtime by enabling your team to respond and detect threats faster and efficiently.

The SIEM solution integrates easily with all devices in your network, giving a holistic and correlated overview of events in your IT infrastructure.

LogPoint's Modern SIEM solution translates all data into one common language, making it possible to compare events easy and efficient to search, analyze and report on the data. This helps accelerates the team's detection and response rate to threats reducing workload.

For compliance initiatives, LogPoint enables automatic monitoring of relevant compliance parameters and alerts you to relevant risks as they happen. Our Modern SIEM solution is easy to use with a low learning curve for busy professionals. We also drive operational efficiencies by supporting a proactive approach to understanding your network, by providing actionable, real-time insight into your IT infrastructure to drive business value.

Learn more

Learn more…

PLACEHOLDER PLACEHOLDER PLACEHOLDER