Logsign

Security Information and Event Management (SIEM) Buyer's Guide

An Unbiased SIEM Guide: How to Choose the Right SIEM Solution.

Contents

1. Introduction

1.1 What is SIEM?

Modern-day threats are constantly evolving in complexity and sophistication. The security team does not know what they will face next. With an increasing number of endpoint devices and growing reliance on cloud-based services, the potential attack surface area is expanding. All these factors combined make it more difficult for security teams to keep
track of events happening across the enterprise network.

Organisations install multiple security devices and software to detect unusual behaviour and identify security incidents. However, these work in isolation making them inefficient when it comes to detecting advanced threats. Attackers use an arsenal of tools to plan and execute an attack as well as advanced techniques to evade detection and there is a growing tendency for attackers to launch distributed attacks on multiple systems rather than focusing on a specific system.

This is where a Security Information and Event Management (SIEM) system comes in as it helps provide the security team with real- time collection and analysis of log data. Gartner provides a widely accepted definition of SIEM as a "technology that supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources."*

1.2 How does a SIEM work?

A SIEM solution collects log and event data from various components on the enterprise network. After normalising the data, it uses threat intelligence, inbuilt rules, and advanced analytical functions to detect security incidents in real-time. In other words, SIEM offers a single-pane holistic view of an organisation's information security. Depending on its architecture, it arranges alerts into various categories such as malware, failed logins, successful logins, other potentially harmful activity.

It combines two technologies: Security Information Management (SIM) and Security Event Management (SEM). In modern SIEM solutions, it is difficult to separate the two components. SIM primarily looks after data collection from log sources and generates the desired reports while SEM performs real-time monitoring of enterprise systems for threat detection and event correlation.

When a SIEM solution identifies a potential threat, it generates alerts to notify the security team. Based on pre-defined rules, the priority of an alert can be low, medium, or high. For example, if the user account of user X generates ten login attempts in five minutes, that can be considered as suspicious activity. The most likely explanation, however, is that user X has forgotten their password and is unable to login. Suppose the same user account experiences 200 login attempts in the same duration. In that case, the SIEM solution will tag this activity as a high severity incident since it is most likely to be a brute-force attack.

1.3 Why do you need SIEM?

Modern SIEM solutions provide a robust method for threat detection, report generation, and long-term analysis of security logs. Scalable SIEM solutions grow with the organisation's business requirements and yield a maximum possible return on investment (ROI).
A SIEM solution supports a security team in responding to potential security incidents faster. It automates the tedious task of manually analysing log data from different sources. As a result, the security team can focus on alerts with high risk and significant impact. For example, a single alert generated by an anti-virus solution may not garner sufficient attention. However, if an organisation's firewall detects unusual traffic at the same time as the anti-virus alert, this could be indicative of an ongoing security incident. This correlation is what SIEM makes possible.
Some of the benefits of SIEM solutions include:

- Increased security team efficiency and utilisation of time
- Prevents potential security threats from becoming large-scale security incidents
- Reduces overall security expenditure
- Provides a better system for reporting, log analysis, and data retention
- Minimises the impact of security breaches

* https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

1.4 Migrating a legacy SIEM to next-gen SIEM

SIEM solutions came to market around the turn of the century and these initial SIEM solutions were complicated and hard to configure and were challenging to scale. These issues accelerated the development of SIEM solutions that are flexible, advanced, analysis-driven, and scalable. For modern SIEM solutions, collecting log data from a variety of sources is now a simple operation and the organisation has numerous options in terms of how they wish to store this data. The battle is turning this data into actionable intelligence.

Organisations that rely on legacy SIEM solutions often find that their SIEM is static in nature. It lacks sufficient correlation features and is relatively complicated making it struggle to support time-sensitive investigations. With the advent of cloud computing technology and the SaaS delivery model, next-gen SIEM solutions have emerged that are now capable of covering the full scope of potential threats. Some of the commonly observed issues in legacy SIEMs are:

- Limited detection, investigation, and incident response capabilities due to limited data ingestion
- Ingestion of data is a long winded process
- Fairly complex to operate and require skilled employees
- Generate a large number of false positive and false negative alerts
- Static and restrictive in nature with limited capabilities
- Incapable of detecting sophisticated threats leading to increased risk
- Lack of scalability and adaptability to business needs
- Numerous incidents of outages
- Lack of features to integrate with other security tools
- Often available in on-premises deployment model only

Next-gen SIEM solutions are analysis-driven and enable organisations to monitor and respond to threats in real-time. Such SIEM solutions rely on threat intelligence (TI) to understand the risks an organisation faces. Modern SIEMs do away with the limitation of deploying SIEM solutions on- premise. Instead, they can be deployed on cloud infrastructure or in a hybrid environment. Next-gen SIEM solutions also go beyond simple data correlation and now include specialised tools that are capable of dealing with threats through the platform itself.

2. SIEM Use Cases

Security Information and Event Management (SIEM) solutions aggregate event and log data from the entire enterprise network. They help the security team detect and respond to security events, along with generating reportsto demonstrate compliance, making a SIEM solution a vital component of an enterprise security strategy.

The following sub-sections discuss common SIEM use cases, from traditional to advanced capabilities. dern-day threats are continuously evolving in complexity and sophistication. A security team does not know what they will face next. With the increasing number of endpoint devices and growing reliance on cloud-based services, potential attack surface area is expanding. Considering all these factors, it becomes difficult for security teams to keep track of events happening across an enterprise network.

2.1 Data Exfiltration

Data exfiltration refers to the unauthorised transfer of data, either manually by a user or attacker or automatically using malware. It is manual transfer when a user transfers organisational data to a physical device or over the Internet. In contrast, it is automatic when malware has infected a computer system. Irrespective of an organization's size, data exfiltration is a severe problem.

A SIEM solution detects data exfiltration events by closely monitoring network traffic to identify data transfer in large volumes and can and monitor email server logs to identify emails sent to untrusted receivers. It may generate an alert when the recipient appears to be malicious or unknown. As SIEM solutions perform data correlation from multiple systems, they can also detect lateral movement and privilege escalation.

2.2 Zero-day Attacks

While vendors regularly release patches and updates for their products and services, there are often vulnerabilities that are not publicly known. When attackers exploit this particular subset of vulnerabilities, it is called as a zero-day attack. Traditional security tools such as IDS/IPS device or anti-virus/anti-malware software typically fail to detect such attacks as their attack as the signatures have yet to be recorded. Using real-time monitoring of an organisation's IT infrastructure, a SIEM solution can alert the security team as soon as it detects abnormal behaviour. A zero-day attack can target virtually any data source but SIEM solutions feature advanced investigation capabilities

enabling the security team to search for specific data points or to use data analytics to identify the patterns of a zero-day attack.

2.3 Remote Access from Suspicious Location

Remote access has become crucial for organisations during and following the pandemic. The organisation's business units and employee locations in specific countries should correspond with VPN logins but attackers from other regions may well try to log-n from other remote locations.

SIEM solutions come with inbuilt correlation rules for detecting anomalies concerning remote access. By using a database of IP address associated with geographic locations, a SIEM solution provides contextual location information up to the city level. Further, by monitoring login data for the enterprise network, it quickly generates an alert for the security team when it detects remote access from a suspicious location or concurrent VPN logins. Certain SIEM solutions may allow a white list or black list of countries to be maintained for determining access to the corporate network.

2.4 Privilege Escalation

When attackers break into the corporate network, they attempt to perform privilege escalation to increase the level of privileges associated with the compromised account. The ideal goal is to conduct vertical privilege escalation for gaining administrator-level system privileges. (Horizontal privilege escalation only allows attackers to gain access to other user accounts on the same access level.) Modern SIEM solutions use user and entity behaviour analytics (UEBA) to determine a baseline of normal behaviour so that the SIEM solution can easily detect such abnormal behaviour.

2.5 Brute Force Attacks

Brute force attacks have been around since the turn of the century and use a simple trial and error method to crack passwords. An attacker uses a combination of alphabets, numbers, and special characters to successfully guess the password and can also utilise dictionary words and commonly used words to increase the success rate. A successful brute force attack results in an attacker getting access to user credentials which they can use to steal sensitive information such as intellectual property, trade secrets, and personally identifiable information. Many SIEM solutions come with in-built rules that create alerts for suspicious source IP addresses that exceed the threshold of rejected/invalid login attempts
in the given time. Advanced SIEM rules may include the identification of failed login attempts over a given period of time and the blocking of compromised accounts.

2.6 PowerShell Attacks

Traditional malware attacks involve the execution of malicious code on a target system but file- less malware attacks utilise inbuilt Windows tools such as PowerShell. Since the attack involves legitimate programs, it can be challenging to detect and disabling PowerShell is not an option. For organisations, the situation has further worsened due to the large-scale distribution of exploit kits.

A SIEM solution can analyse incoming event logs to detect malicious activity and for PowerShell attacks, the platform looks for specific event IDs and their characteristics in event logs coming from Windows systems. For example, if detecting lateral movement, the SIEM solution will look for Windows Remote Management (WinRM) along with PowerShell command Enter-PSSession.

2.7 Lateral Movement

After an attacker has gained initial access to the enterprise network, they will seek to move deeper within to access sensitive data and critical assets. The initial breach may have been the result of a malware infection or phishing attack following which the attacker may impersonate a genuine user to avoid being detected. Lateral movement is generally observed in advanced cyber attacks where the attacker's aim is to inflict the maximum possible damage. Stealing credentials, privilege escalation, and gaining access to sensitive information are all indicators of lateral movement.

Unlike traditional point solutions that work in isolation, SIEM solutions have a comprehensive view of events happening across the enterprise network. With logs coming in from multiple systems and devices, it can easily detect the techniques used in lateral movement by using real-time monitoring and behavioural analysis to provide contextual evidence.

2.8 Insider Threats

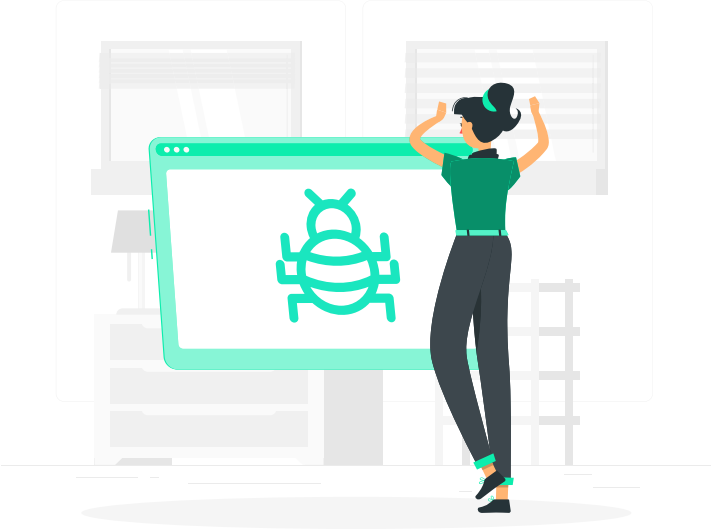
Insider threats are one of the top causes of security breaches as they tend to go unnoticed. Insider threats are not limited to an employee stealing data from the enterprise network; it can also happen unintentionally such as the loss of a laptop or storage drive or the sending of an email to an incorrect mail address.

SIEM solutions have multiple mechanisms to detect insider threats. A SIEM solution detects abnormal user behaviour by analysing login time, frequency of login, and commonly used resources and utlises threat intelligence (TI) feeds in correlation with network traffic to identify where a command and control center is being used. Other signs that trigger alerts include the unexpected encryption of data, movement of large amounts of data from one resource to another, and lateral movement.

2.9 Malware Detection

Malware refers to any malicious program that intends to cause damage to a system or gain unauthorised access so is something of a catch-all term that includes virus, trojan horses, worm, spyware, ransomware, and adware. Over the years, many prominent malware families and their variants have caused substantial damages to enterprises across the globe, with Stuxnet and WannaCry two notable examples.

Malware is generally delivered through drive-by downloads, email attachments, and freeware websites. Modern-day SIEM solutions perform continuous monitoring of enterprise systems to detect malicious files with known hashes. They rely on historical data, and threat intelligence feeds to detect malware. Next-gen SIEM solutions use signature-based techniques and attack patterns and also form hypotheses based on behaviour analyses for investigation.



2.10 Unauthorised Access to the Shared Folders

In a traditional setup, a shared file system creates a storage area network that allows multiple computer systems to gain access to storage. An organisation's access level system may guide the extent of access granted to individuals. These days, cloud-based services are increasingly being used to share storage space.

SIEM solutions aggregate authentication records from multiple systems and services to detect account takeover incidents. Next-gen SIEM solutions go one step further, using correlation rules and behaviour analytics to identify anomalous activities and detect unauthorised access to shared folders.

2.11 Excessive Web Activities

A plethora of requests and responses are sent over the network every day – database connection requests, website access, file downloads, video conferencing data, etc. As the size of the network increases, so too do the number of requests and responses.

A SIEM solution reduces the burden on the security team by filtering through unnecessary network events. Utilising inbuilt correlation rules and threat intelligence, a next-gen SIEM generates alerts for indicators such as excessive database connections, firewall connections from a single source, and excessive outbound connections. Alerts are accompanied by contextual information, allowing the security team to swiftly make decisions and take action.

3. Evaluation Criteria

3.1 Scalability and Big Data Infrastructure

As the organisation grows, so too does its log data. While many organisations plan for infrastructure expansion well ahead of their requirements, they cannot predict the amount of log data their enterprise network will generate in the future. A modern SIEM solution built upon big data infrastructure can scale with the organisation in every possible way, by number of devices, log sources, size of data, processing power, and efficiency, helping to futureproof the business.

3.2 Data Aggregation

Your SIEM solution should be able to process log data from all enterprise systems, including security devices, firewalls, VPNs, IPS/IDS, email servers, FTP servers, gateways, and anti-virus/anti-malware products. If a SIEM tool is not compatible with your existing infrastructure setup, it should not be a part of your security strategy.
The native support should cover operating system logs, database connection log, system logs, and cloud-based service logs at a minimum. Some next-gen SIEM solutions may allow security teams to develop manual code for processing log data from a particular source.

3.3 Correlation and Alerts

Legacy SIEM solutions identify most security events from different devices, but they have minimal or negligible power to establish a correlation between them. Modern SIEMs use correlation to provide a broader context and help the security team focus on high risk alerts that can have a significant impact. These SIEM solutions come with inbuilt correlation rules to identify a threat, vulnerability, or an ongoing security incident and each correlation rules that specify a sequence of events that indicate an anomaly or deviation from expected network behaviours. A prospective SIEM buyer should look for a SIEM vendor whose team consists of security experts with extensive domain knowledge and experience.

3.4 Security Analytics

Security analytics help security teams perform proactive advanced investigations, instead of limiting themselves to the waiting for for correlation rules to trigger an alert. Manually-defined correlation rules require a dedicated team to carry out continuous modification and upgrades which isn't viable given the rapid evolution of threats. Security analytics utilises machine learning algorithms to help the SIEM solution in identifying attack patterns and threats with no prior signatures, rules, or patterns. For machine learning techniques to perform efficiency, they need a vast amount of test data for analysis in a time-bound manner, so a big data architecture is necessary on the backend to aid processing and expedite insights and actions to the security team.

3.5 User and Network Behaviour Analytics

A SIEM solution provides the security team with a comprehensive view of user activity along with contextual data and creates alerts for known threats and behavioural changes. Next-gen SIEM solutions also provide insights into user and network-based threats that would often go unnoticed. Behavioural analytics is supported by artificial intelligence (AI) and machine learning (ML) technologies to shorten mean time to detection (MTTD) and mean time to response (MTTR).

3.6 Advanced Threat Detection

A modern SIEM solution should be capable of adapting to the continuously evolving threat environment. This capability is achieved through the combination of behaviour analysis, network monitoring, endpoint detection, and threat intelligence feeds. But advanced threat detection is not only about detecting a threat, it should also provide information such as the scope of a threat, movement across the network, and possible solutions to the threat.

Legacy SIEMs come with in-built static search queries that result in high false positives. As a result, security teams often fail to detect threats. In contrast, next-gen SIEM solutions allow the security team to run their own search queries for detecting threats and indicators of compromise (IOCs) and to customise alerts specific to business requirements.

3.7 Threat Intelligence

Many threat intelligence services provide information about tactics, techniques, and procedures (TTPs), indicators of compromise IOCs, and other contextual information about threats and security incidents and now next-gen SIEM also utilises this information to improve detection.

For example, if a computer system is communicating with an external IP address, the next-gen SIEM solution can quickly identify whether the destination IP address is a previously known C&C server used for malicious activity. A modern SIEM gathers the relevant incident data from various sources to help the security team analyse the impact of a security incident, and by combining incoming log data with threat intelligence can shorten detection time.

3.8 Search and Forensic Investigation

Traditional SIEM solutions only collect limited log data and have restricted search capabilities that then constrain the security team. Modern SIEM solutions allow the team to create their own search queries and enable a security team to explore log data to discover additional details related to the security incident.

Certain SIEM solutions may help a security team by presenting an incident-specific visual timeline of how the situation unfolded.

3.9 Compliance

SIEM solutions are very proficient at fulfilling compliance obligations and next-gen SIEM solutions take this a step further by offering highly customisable reports. These can be classified using various categories specific to industry regulations and standards.

This ensures that if the SIEM solution does not come with inbuilt reports for a given regulation or standard. these can be accommodated using customisable reporting.

3.10 SOC Automation

The SIEM solution becomes the foundation for the Security Operation Centre (SOC). Next-gen SIEM solutions automate SOC processes, enabling the security team to focus on critical and high-risk alerts. Generating alerts and creating tickets, gathering contextual data for an alert, providing information for mitigation, and creating reports on mitigation actions are some of the processes that a modern SIEM should automate. Moreover, for low-risk alerts, the security team should be able to define rules for mitigation so that containment actions are performed automatically.

3.11 Dashboards & Reports

SIEM dashboards help visualise the security posture of the organisation. A SIEM solution may come with a variety of dashboards for different purposes which should be customisable. When it comes to reporting, having a set of inbuilt reports helps with the initial setup and running of the SIEM solution but as business operations expand and security requirements change, the organisation should be able to customise these too. Before selecting a SIEM solution, the organisation must explore the customisation options on offer as these can help to significantly streamline day-to-day operations.

3.12 Automated Response

Manually responding to low-risk alerts can be time intensive and increases the chances of fatigue and frustration as a result of which the security team might miss a critical alert. Next-gen SIEM solutions allow security teams to define automated responses for commonly detected alerts. For example, if a user was unable to sign-in after 10 attempts carried out within 10 minutes an automated action could see the user account blocked and an alert issued to the security team who would then make a judgement call on whether the block should continue.

3.13 Retention

Next-gen SIEM solutions require vast data resources to feed the underlying machine learning algorithm. A SIEM solution should be capable of storing historical data over time without this affecting its integrity or processing capabilities. Historical data helps SIEM platforms make the correct predictions, minimises the number of false positive alerts and helps, security teams to trace the source of breaches more quickly and effectively. Certain jurisdictions may also require the organisation to store their security-related information for a specified duration.

3.14 Fault Tolerant

Fault tolerance refers to the ability of a system to continue its operations even when one or more of its substituent components fail. Modern SIEMs must be fault tolerant to ensure that there is no single point of failure (SPOF) in the entire backend architecture and to ensure business continuity and high availability.

Before selecting a SIEM solution the security team should seek to understand the underlying architecture of the SIEM vendor.

Logsign Security Information and Event Management

Big data infrastructure with infinite scalability	Limitless log collection and storage	Detection of complex threats	Fast and effective data protection
Rapid deployment & easy configuration in every environment	Collects every log from every environment with multiple, flexible pricing options	Comprehensive correlation of all data	Mitigation & eradication of threats
Unlimited log collection & storage	Advanced parsing and indexing techniques	Accelerated, detailed incident investigation	Automated incident notification, response, and remediation
Massively parallelised, fault tolerant system	Easy-to-work with normalised, classified, and enriched data	Early detection of cybersecurity threats	Minimised response times reducing alert fatigue
Long-term data retention		Uncovers anomalies and IOCs	Early prevention of phishing through detection of suspicious network traffic

Why Logsign SIEM?

360-Degree Visualisation

Visualisation with hundreds of built-in security analytics-driven dashboards and reports

Smartly Designed UI

Easy-to-use platform and built-in modules, with the flexibility to create new ones

Affordable Data Security

Calculating cost is simple with Logsign's multiple, flexible pricing options

Features of Logsign SIEM

Smartly Designed Big Data Environment

- Big data infrastructure based on Hadoop & NoSQL
- Unlimited scalability for petabyte-level experience
- Fast and easy deployment
- Massively parallelised system with flexibility to add any number of users, notes, or sources
- Continuously active with zero performance loss
- Unlimited log storage
- Long-term data retention

Finds hidden threats

- Search functionality with Logsign's drill-down, full-text search
- Accelerated incident investigation
- Uncovers threats, anomalies and IOCs using the MITRE ATT&CK framework

Heightens Visualisation

- 200+ built-in alerts, dashboards, and reports with easy customization
- Easy-to-use wizards
- Role-based access ensuring visibility and responsibility

Create Your Own Data Lake

- 400+ built-in integrations and vendor-agnostic integration capabilities
- Unstructured data parsing with free plugin service
- Limitless data collection from any source and any environment
- Real-time data enrichment with real-time threat intelligence
- Flexible data policy manager

Detect Complicated Threats

- Comprehensive correlation of data
- Risk-score based incident triage
- Advanced detection with minimum noise

Safeguard Your Data

- Automated incident response
- On-time incident notification
- Automated remediation actions for threats and vulnerabilities
- Easy-to-use platform and built-in modules, with the flexibility to create new ones
- Calculating cost is simple with Logsign's multiple, flexible pricing options