ManageEngine
Log360

SIEM Evaluator's Guide

www.manageengine.com/log-management

Introduction

> *According to the recent Verizon Data Breach Report, "Sixty-eight percent of breaches took months or longer to discover, even though eighty-seven percent of the breaches examined had data compromised within minutes or less of the attack taking place."*

Security threats are on the rise and hackers' attack methods are becoming more sophisticated each day.

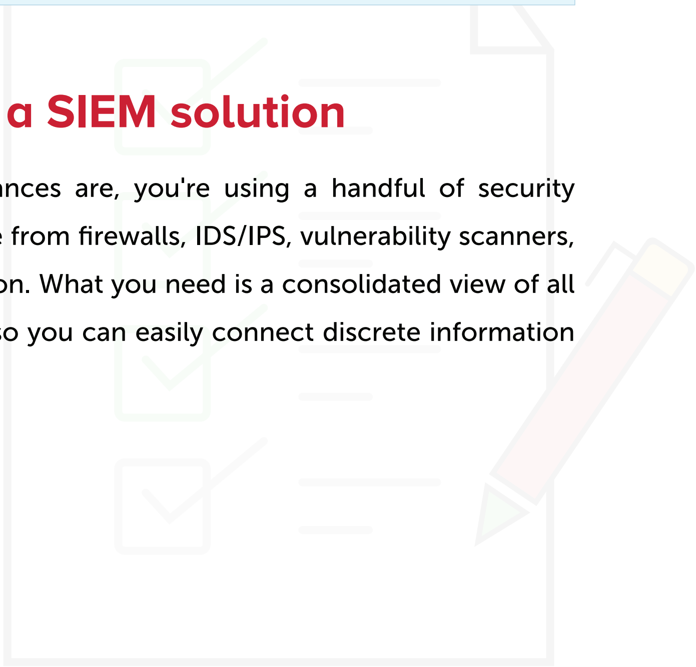
This means attackers are using techniques that go unnoticed by security operations centers (SOCs). In many cases, data breaches are detected by a third party who notifies the business; the business then commissions a forensic investigation. Though a considerable number of attacks take very little time to steal targeted data, the intrusion method, the lateral movements within the network, and the route through which data is stolen are dug out only months later. By this time, the data is long gone.

These attacks leave traces, even if the SOC fails to connect the dots. With the advent of stringent compliance mandates such as the General Data Protection Regulation (GDPR) and Protection of Personal Information Act (POPIA) coming into effect, the IT security landscape is changing. Organizations are looking for solutions that detect and address incidents before they become critical, and security information and event management (SIEM) solutions are the best way to do it.

> *Gartner's Magic Quadrant for SIEM elaborates on the capabilities required for a SIEM solution. Read the report.*

Three reasons why you need a SIEM solution

- **In-depth visibility into network incidents:** Chances are, you're using a handful of security solutions in your network. These solutions range from firewalls, IDS/IPS, vulnerability scanners, antivirus and anti-malware applications, and so on. What you need is a consolidated view of all the security events happening in your network so you can easily connect discrete information that indicates a possible attack.



A SIEM solution collects log data from across the network, extracts meaningful information from those logs, correlates different events to detect attack patterns, and helps you search log data for root cause analysis, providing in-depth visibility into what's happening in your network. This helps in preventing or containing security attacks as quickly as possible.

- **Continuous auditing is key:** When it comes to detecting and containing security attacks, you should never set it and forget it . Though you set critical security policies such as firewall rules, access control lists, group membership permissions, and so on, you need to constantly watch for any changes to these configurations. A SIEM solution offers regular reports that help you continuously audit events to validate policy enforcement and detect critical configuration changes or unusual user behaviors to keep threats in check.
- **Security orchestration:** Organizations use various solutions to ease their IT operations. For instance, help desk software is used to handle IT requests and network operations. A SIEM solution should integrate with such solutions to make security operations as efficient as possible. Integrating with help desk solutions will increase the speed of incident resolution and ensure accountability.

Read this year's Gartner's Magic Quadrant for SIEM to learn more and compare the capabilities of different players in the market.

What you should consider while choosing a SIEM solution

We'll now be demystifying the critical capabilities of SIEM tools and show you what to consider when picking a solution.

Budget plays a crucial role

When purchasing a SIEM solution, budget plays an important role. Some SIEM vendors license their solution based on the volume of log data that is being processed, meaning the product's price tends to fluctuate. On the other hand, when licensing is based on the number of log sources being added for monitoring—with no limit on the volume of log data being processed—then your spending tends to remain constant. These source-dependent pricing models also help you accommodate your SIEM solution better during network expansions.

Apart from budget constraints, the SIEM solution you choose must provide certain capabilities.

The seven capabilities you must consider while choosing a SIEM solution

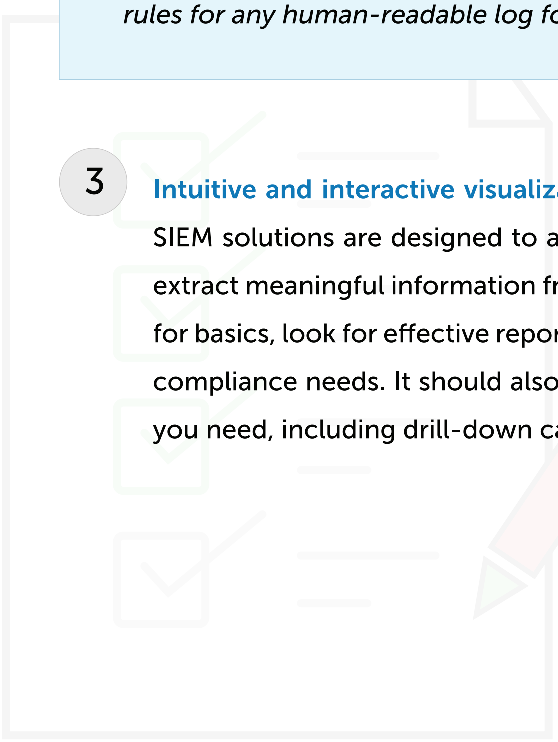
1 **Scalability:** Whatever the license model, the SIEM solution that you choose must be able to scale both horizontally and vertically. When your organization grows, your SIEM solution should grow too. Find out how many log sources a single instance of the solution can handle and check whether that falls within your network size. Also, make sure to check the SIEM solution's peak event handling capacity, which should fall within your log generation limits.

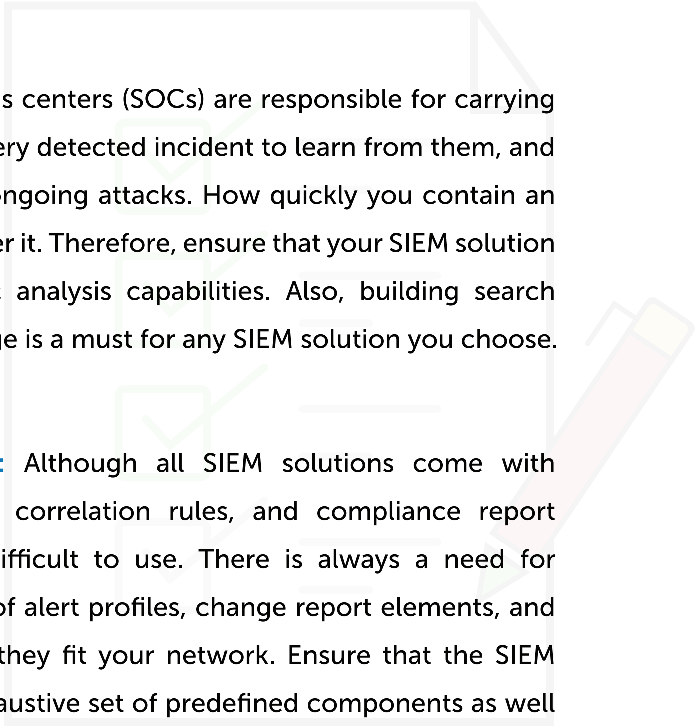
Did you know that Log360, our comprehensive SIEM solution, can handle 25,000 logs/second? Check out what else this solution has to offer.

2 **Log data compatibility:** Your network probably has a wide range of devices, each with its own log type. You might have a mix of network perimeter devices—such as routers, switches, firewalls, and IDS/IPS—as well as applications, servers, workstations, and even entire cloud environments. The SIEM solution you choose should be able to assimilate log data from all these platforms, right out of the box. It should only take minimal effort to configure log collection and analysis from the devices in your network.

Just saying, Log360 can automatically parse and analyze log data from more than 750 log sources. Furthermore, the solution's custom log parser can automatically create parser rules for any human-readable log format.

3 **Intuitive and interactive visualization:** Analytics is the key feature of every SIEM solution. SIEM solutions are designed to automate the log management process and specifically to extract meaningful information from these logs and present them as actionable insights. So, for basics, look for effective reporting capabilities that help meet your security, auditing, and compliance needs. It should also have an interactive dashboard that presents exactly what you need, including drill-down capabilities.





4. **Effective forensic analysis:** Security operations centers (SOCs) are responsible for carrying out rapid and accurate forensic analysis of every detected incident to learn from them, and ultimately prevent new threats and contain ongoing attacks. How quickly you contain an attack depends on how long it takes to discover it. Therefore, ensure that your SIEM solution possesses high-speed and efficient forensic analysis capabilities. Also, building search queries without having to use a query language is a must for any SIEM solution you choose.

5. **Ready-made and tailor-made components:** Although all SIEM solutions come with prebundled auditing reports, alert profiles, correlation rules, and compliance report templates, you might find these features difficult to use. There is always a need for customization to fine-tune threshold values of alert profiles, change report elements, and modify criteria for correlation rules so that they fit your network. Ensure that the SIEM solution you choose comes with both an exhaustive set of predefined components as well as the ability to customize them with minimal effort.

6. **Security orchestration:** Your SIEM tool should work in harmony with other IT management solutions in your network. Your network might contain solutions that ease your IT operations, such as a monitoring tool that watches the performance and health of devices and servers, or help desk solutions that assist in resolving IT-related queries. The SIEM solution that you choose should be able to effectively get input from and feed data to your other IT management solutions. For instance, your SIEM solution should be able to receive server downtime alerts from your monitoring solution and validate whether these alerts signal a DDoS attack. When your SIEM tool identifies an attack, it should be able to raise this incident as a ticket in your help desk and assign that ticket to a security administrator for effective incident resolution.

7. **Predictive intelligence:** Predictive intelligence makes SIEM solutions stand out from other network security solutions. The SIEM solution that you choose should be able to add business context to events occurring on your network, plot user and entity behavior trends, identify variations from typical trends, and provide real-time notifications about deviations. Your SIEM tool must come with rules and algorithms based on machine learning that can identify suspicious behavior in your network.

About Log360, ManageEngine's comprehensive SIEM solution

Log360 is a comprehensive SIEM solution that helps security professionals meet their heavy auditing, security, and compliance needs. With over 1,200 predefined reports, 900 alert profiles, and over 70 correlation actions and rules, this solution can detect and mitigate both internal and external threats. Log360's in-depth Active Directory auditing capability helps administrators closely monitor privileged user activity and other user behaviors to instantly detect anomalies. Log360 also supports more than 700 log sources, including routers, switches, firewalls, IDS/IPS, servers, databases, and web servers. It collects, analyzes, correlates, and archives log data from these sources and ensures data security 24/7.

Explore Log360 for free

Online demo

Learn more

Log360 is a champion in Software Reviews' Customer Experience Diamond for SIEM 2019

The Customer Experience Diamond, which assesses solutions based on feature satisfaction and vendor experience, ranks Log360 ahead of all other solutions in the SIEM market.

Get the full report