ManageEngine
Log360

The Absolute Guide to SIEM

www.manageengine.com/log-management

Table of Contents

The need for SIEM

> According to the recent Verizon Data Breach Report[1], "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."

No organization is immune to security attacks. Irrespective of their size, organizations are facing attack attempts every day. Although security devices such as firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) are capable of detecting anomalous events and isolated attacks, they're ill-equipped to deal with sophisticated attacks. Be it ransomware or exploiting a long-known vulnerability in the operating system, hackers are employing distributed, slow, and targeted attack methods that are difficult to detect with single-point security devices.

What enterprise security operation centers (SOCs) need is an intelligent platform that can tackle these types of attacks. This is where security information and event management (SIEM) solutions and services come in. Without the right SIEM solution, it's nearly impossible for organizations to keep track of security incidents.

Understanding SIEM

According to Gartner, "SIEM technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources."

The main purpose of SIEM is to detect and stop security attacks by gathering and correlating activities happening across the network. To do this, many SIEM solutions or services offer different capabilities such as:

- Log collection, processing, and archival.
- Searching and reporting.
- Real-time security monitoring.
- End-to-end incident management and automated workflows.
- Threat intelligence.
- User and entity behavior analytics.

Each of these components works independently from each other, and together provide visibility into network security. Let's take a closer look at these components.

1 https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

The six capabilities of a SIEM solution

1. Log collection, processing, and archival

Log data is fundamental for SIEM solutions. It is essential for a SIEM solution to both centrally and securely collect, process, and archive log data from all sources across the network. Log processing involves parsing and normalizing log data to gain meaningful insights out of it.

Your network generates different formats of log data. For instance, the log format of an SQL database is different from that of a Windows server. Similarly, these formats differ based on vendors; a Juniper firewall's log format is different from that of a Palo Alto firewall. A good SIEM solution should be able to ingest and process any log format.

Log archival is the process of compressing and securely storing massive amounts of log data for conducting forensic analysis. Your SIEM solution should come with built-in log archival capabilities. You should also make sure that the SIEM solution you choose comes with a decent compression ratio and adopts efficient encryption techniques to prevent tampering of log data.

2. Searching and reporting

It's impossible to completely eliminate the risk of a security attack. But with the right mix of proactive and reactive security strategies, SOCs can mitigate this threat. While advanced analytics and threat intelligence capabilities work as a proactive attack defense mechanism, searching and reporting capabilities help shape your organization's reactive defense system.

According to the Cyber Security Survey Report[2], it takes 175 days on average to detect an attack. This period is known as the attack dwell time. The shorter the dwell time, the better contained the attack usually is. To greatly reduce the dwell time, your SIEM solution should have a high-speed forensic analytical capability that swiftly searches your logs to detect the attack pattern and its impact.

Further, SOCs need to conduct investigations on anomalous or suspicious security events. Investigating these indicators of compromise (IoCs) should be quick and easy and shouldn't involve the expertise of building SQL queries. Your SIEM solution should provide detailed, intuitive reports with graphical dashboards to facilitate easy investigations. A prebuilt report console will not only speed up investigations, but will also help with meeting the heavy auditing and compliance needs of many enterprises.

Log360 offers high-speed log processing. It can process 25,000 logs/second on average with a peak log handling capacity of 30,000 logs/second.

Log360's exhaustive reporting console includes over 1,200 predefined reports that help enterprises meet their auditing, security, and compliance needs. The solution includes predefined compliance mandate report templates for IT regulations such as PCI DSS, HIPAA, FISMA, the GDPR, ISO 27001, and GPG13. Admins can also customize Log360's predefined templates to satisfy internal security policies.

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

3. Real-time security monitoring

Real-time security monitoring helps SOCs instantly detect the indicators of an attack so they can quickly analyze and respond to the attack or attack attempt. A good SIEM solution uses a combination of components to support real-time security monitoring, including:

- An event response system.
- An event correlation engine.
- Intuitive analytics.

Real-time event response system

SIEM solutions often come bundled with predefined alert profiles to detect known IoCs. When it comes to these alert profiles, your SIEM solution should offer customization capabilities to modify threshold limits as well as other criteria. For instance, to detect a confidential file tampering event with your SIEM solution, you need to:

1. Enable the alert profile that looks for the File modifications event in the log data.
2. Specify the file servers in which this criteria should be checked.
3. State the threshold values such as the number of occurrences for an event or the time interval within which the event has to occur. Specify these values based on business-contextual information.
4. Set up a workflow that will remediate the effects of the event that's occurred. In this case, you can set up a workflow to rollback the file to its previous version after your SIEM solution detects unwarranted tampering.

To optimize the use of a real-time alerting console and avoid false positives, you need to set threshold values and criteria based on your business' specific requirements.

While the alerting console helps with detecting the individual events that indicate network compromise, event correlation connects the dots between the discrete anomalies happening in the network to detect attack patterns, identify ongoing attacks, or even shut down an attack before it impacts your network.

> Log360's real-time event console includes over 800 predefined alert profiles that are carefully drafted based on known IoCs and meticulously categorized for easy access. The console also offers real-time notification and script-based workflow capabilities to send you an alert and mitigate any incidents automatically.

Real-time event correlation

Your SIEM solution should be able to automatically ingest business-contextual information about your network's resources such as devices, applications, and users. It should also use threat feeds and identity and access information (role of the user, permissions assigned to a specific user, and more) to detect threats. Once your SIEM solution detects indicators of attack (IoAs), the correlation engine flags these critical security events as an incident by validating them against contextual information about your business.

Log360's real-time correlation engine can detect data exfiltration as well as attacks on critical business applications such as databases and web servers. Log360 offers over 70 predefined correlation rules along with the ability to customize these rules at the field level to spot attacks precisely.

Log360's correlation and real-time event response systems also integrate with its incident management component. This integration allows SOCs to assign an incident to specific users based on rules, manage an incident at its various stages, and much more.

Correlation explained with a use case

An SQL database backup is not considered a threat until it's correlated with a series of incidents, starting with:

- Consecutive VPN logon failures on an internet-facing resource.
- A successful VPN logon on that same resource.
- A suspicious software installation on the resource.
- Continuous access attempts from the same resource to connect to a database server.
- An SQL backup initiation attempt.

Correlation engines look at these incidents as a whole, spot any related events (originating from the same vector), trigger an alert to respective security professionals, and initiate the workflow.

The difference between an event response system and a correlation engine

Event response system	Event correlation engine
Detects discrete events that indicate compromise of the network or data. **Example:** File deletion on a critical file server.	Detects attack patterns by correlating suspicious security events across the network. **Example:** Privilege escalation followed by backdoor account creation followed by firewall rule modification and malware download from a malicious source.
Determines whether the identified event is an IoC by comparing the log data from specific sources against the defined criteria and threshold. **Example:** A hundred consecutive logon failures happening on a critical database server.	Determines the attack pattern by matching up log data from different sources across the network, and pairing these findings with contextual information. **Example:** Consecutive logon failures from a malicious source (threat feed) followed by a successful logon during non-business hours (business-contextual information).
Needs manual forensic analysis to get more details on the incident and assess its impact.	Aggregates all the related incidents together making the analysis quick and easy.
High risk of false positives due to lack of contextual information.	Reduces false positives by fine-tuning the conditions that trigger an alert.

Intuitive analytics

The advanced analytics feature of your SIEM solution should include an intuitive and interactive user interface with dashboards, views, and reports. You should be able to drill down into dashboards and set up real-time alert notifications. Aggregating related incidents on a timeline helps facilitate effective analytics. The way security information is presented by the SIEM solution should speed up attack detection, facilitate quick remedial measures taken on detected threats, and more. There should also be an option to liberally customize analytical components.

> Drill down into the root cause of an incident with Log360's intuitive dashboard widgets and interactive reports dashboard to conduct effective security analysis.

4. End-to-end incident management and automated workflows

Security attack mitigation doesn't stop with incident detection—it's where it starts. The incident management process undergoes a few different stages, including:

- Critical event detection.
- Analysis of the detected event.
- Flagging it as a false positive or an incident.
- Assigning the incident to a security professional to ensure accountability in incident resolution.
- Taking remedial steps to resolve the incident.
- Implementing measures to avoid similar incidents in the future.

Your SIEM solution, with its end-to-end incident management capability, should provide you with the ability to manage incidents right through the last step. Refer to the table below to learn how SIEM solutions can help you carry out effective incident management.

Incident management process	The SIEM solution's capability
Incident detection	• Real-time event response system. • Real-time correlation engine.
Incident analysis	• Advanced analytics. • Incident aggregation. • Forensic analysis through log search.
Ensuring accountability in incident resolution	• Automatic alert assignment based on rules. • Ability to track open, closed, and on-hold incidents. • Notetaking to fill other security professionals in on the incident. • Incident management streamlined with other IT components, like the help desk.
Incident resolution	• Automated workflows.
Implementing measures to avoid similar incidents in the future	• Advanced analytics to identify loopholes. • Automated workflows/scripts to seal security loopholes.

Automated workflows

Workflows are remedial actions carried out to mitigate or contain an attack. For instance, if a user tries to log on to a server that holds confidential information from multiple sources, that user account would be automatically disabled using workflows. Many SIEM solutions come with prebuilt basic workflow actions. Some SIEM solutions also provide the option to customize workflows or re-use a built-in workflow for a different alert profile or correlation rule.

Log360's incident management system is tightly coupled with a real-time event response system and correlation engine. This component offers SOCs the ability to:

- Automatically assign incidents to security professionals based on rules.
- Monitor various stages of an incident using the incident management dashboard.
- Raise tickets for every alert that gets triggered in help desk solutions such as ServiceNow, ServiceDesk Plus, JIRA, and Zendesk. This helps streamline the incident management process with the rest of the IT components.

5. Threat intelligence

Even as you read this guide, there are millions of threats being identified around the world. A threat feed is a list of malicious sources (URLs, IP addresses, and domains) that are a hazard to your network's security. Threats can arise from within your network (internal threats) or from outside your organization's perimeter (external threats).

According to Gartner, threat intelligence is defined as "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

In simpler terms, threat intelligence aggregates bad vectors' information identified by reliable sources and looks for any activity by these actors in an organization's network. The threat intelligence framework of your SIEM solution helps identify these threats while its analytic techniques help your SOC effectively mitigate any risks to your network.

The threat intelligence component of your SIEM solution should:

- Aggregate threat feeds from trusted open-source or third-party providers.
- Look for suspicious incidents that are caused by the attack vectors identified in the threat feeds.
- Send alerts when an incident is detected as well as collate related incidents and present the information in the form of intuitive dashboards and reports.

Spotting bad actors using threat intelligence

SIEM solutions often collect threat feeds from as many reliable sources as possible and update these feeds frequently. Your SIEM solution should also provide the option to ingest custom or in-house threat information to to detect internal attacks. SIEM solutions come with prebuilt rules to detect the first level of IoCs in any attack. These include intrusion attempt events such as denied traffic connections, allowed traffic from malicious sources, and requested access to web or file servers. These rules will be automatically enabled in most SIEM solutions so the solution starts scanning the network to detect potential threats immediately after deployment.

Your SIEM solution's threat intelligence platform should always be streamlined with other components like a real-time correlation engine, intuitive analytics, an incident management module, and workflows. This way, when threats are reported you can carry out further analysis using the intuitive analytics feature and implement remediation using the workflow options.

Log360's advanced threat intelligence platform supports STIX/TAXII threat feeds, source feeds from AlienVault OTX, and other reliable sources.

A typical use case for Log360's threat intelligence platform:

Let's use an internal attack as an example. A disgruntled contract worker is trying to install a malicious program on an internet-facing machine. Their goal is to gain privileged access to the database where customers' personal data is stored and copy that data.

Log360's threat intelligence platform detects this activity and alerts you the moment the contract worker has downloaded and installed the malicious software. The threat intelligence system identifies that the source from which the software is installed is blacklisted. Further, it shuts down the malicious software and uninstalls it to prevent the data breach from occurring altogether.

6. User and entity behavior analytics

User and entity behavior analytics (UEBA) baselines the regular activities of users and resources in the network and spots deviations from the baseline activities, which could be a potential intrusion or malicious activity.

UEBA is a recent addition to the mandatory capabilities your SIEM solution should provide. It helps resolve advanced security use cases by predicting potential attacks to implement a proactive security approach. UEBA uses machine learning and artificial intelligence techniques to learn the regular activities of a user such

- The user's routine logon time.
- Where the user typically logs on from.
- The permissions the user possesses.

This baseline is formulated automatically by studying the behaviors of users over a period of time. In most SIEM solutions, UEBA is coupled with a user risk assessment system.

How user risk assessment and UEBA work

Every user gets a risk score depending on their activities in the network. If they perform their regular activities and nothing more, their risk score is usually low. If a user is suddenly trying to access a file server for which they don't have permission, this is spotted as an anomaly from the user's normal behavior. That user's risk score then gets increased, and the SOC gets an alert.

Not all anomalous activities present the same level of risk. For example, critical threats are far more serious than warning incidents like logon failures.

The five-point checklist for choosing the right SIEM solution

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

Budget plays a crucial role

When purchasing a SIEM solution, price is always important. Some SIEM vendors license their solution based on the volume of log data that's 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 rather than the volume of log data being processed, your spending tends to remain constant. These source-dependent pricing models also help you accommodate your SIEM solution better during network expansions.

Apart from fitting into your budget, the SIEM solution you choose should provide certain capabilities:

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 meet your log generation requirements.
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, IDSs, and IPSs—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 be easy to configure log collection and analysis from the devices in your network.

Ready-made and tailor-made components	Although all SIEM solutions come with pre-bundled auditing reports, alert profiles, correlation rules, and compliance report templates, you might find these features difficult to use. You need to be able to customize and 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.
Security orchestration	Your SIEM tool should work in harmony with other IT management solutions in your network. Your network might contain solutions to simplify 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. Your SIEM solution should be able to effectively receive 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.
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.

ManageEngine
Log360

About Log360, ManageEngine's comprehensive SIEM solution

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes,investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

Explore Log360 for free | Online demo | Learn more

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

About the author

Subhalakshmi Ganapathy currently works as a senior product marketing analyst for the IT security solutions team at ManageEngine. She has in-depth knowledge in information security and compliance management and she has provided strategic guidance for enterprises on security information and event management (SIEM) deployments, network security, and data privacy. Reach out to Subha at subhalakshmi.g@manageengine.com