Choosing the Right Managed SIEM

compuquip

Table Of Contents

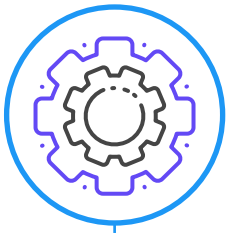
What is a SIEM? & How Does SIEM Work?

SIEM is an acronym for Security Information and Event Management.

This term refers to a variety of data logging tools that can be used to collect information about activity on a network and generate reports about that activity.

> *The underlying technology of a SIEM tool will vary between vendors. However, the fundamental concept of a SIEM platform is to collect and enrich data from a myriad of sources. Sources such as host, network, and application data can present an unified view into your infrastructure.*

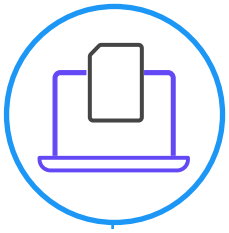
Why should you consider a SIEM?



Meeting Cybersecurity Compliance Standards

Many companies need to meet strict guidelines for storing and processing data. For example, PCI DSS (payment card industry data security standard), which applies to all companies that process payment card information, has a requirement for companies to “track and monitor all access to network resources and cardholder data.”

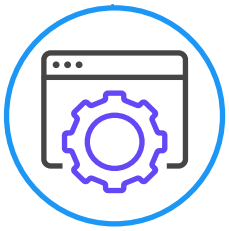
Using a SIEM tool to log all of the activity on the network allows businesses to easily meet this particular cybersecurity compliance requirement—as well as similar requirements in other compliance standards.



Detecting Security Events

As mentioned previously, SIEM solutions excel at collecting and correlating that can be used for analysis and alerting security events. This data can be used to discover malicious activity or misconfigurations within a company’s network before the impact is too costly.

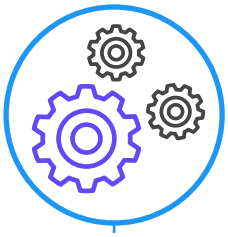
This security event data can also be used to showcase how well the company was adhering to critical cybersecurity standards—and whether the attack was reasonably preventable. This can be useful for avoiding liability purposes.



Improving User Login Verification

With the right SIEM tool, companies can improve visibility on user behavior and account login verification. A SIEM provides additional context for account logins such as, number of failed login attempts, login IP addresses, and login times. In addition, leveraging user behavioral analytics it is possible to identify unusual patterns that could indicate a compromise.

When Should You Consider a SIEM?



Countering Advanced Persistent Threats(APT's)

Targeted cyberattacks attempt to compromise systems to steal sensitive data without alerting the victim to the breach. These attacks frequently involve the use of malware that sits on a system for a long period of time—and may even involve the migration of data from a secure database to a less secure server so it is easier to retrieve for attackers.

A SIEM, can help companies spot APTs by watching for abnormal information access requests and data migration. Such activity, when detected, can be a major warning sign of an APT attack in progress.

This forensic data can also be used to showcase how well the company was adhering to critical cybersecurity standards—and whether the attack was reasonably preventable. This can be useful for avoiding liability issues.

Notifying Customers About Data Breaches

With the event logs from a SIEM tool, it's possible for an organization to identify the specific databases, apps, and other network systems that have been compromised by an attack. This information is priceless in ensuring the security team is aware of:

1. What information was compromised;
2. How severe the compromise is; and
3. What are the steps to remediate and protect customers

Managing SIEM Data Feed's

Security information and event management solutions parse a lot of information each day. For example, say that a business has just 20 employees who use the company's network and applications regularly. If each employee has 15 interactions each hour for an eight-hour shift, that's 2,400 total interactions each day. If the company has customer-facing apps, the sheer amount of traffic quickly becomes impossible to manage manually.

Managing a SIEM tool is, in some ways, similar to managing other "Big Data" systems. Big data tools sift through amounts of data that would be impossible to manage manually— so it's important to consider their configuration for reports to ensure that only the most relevant data is being presented for the person (or team) managing the tool. The exact process for managing an SIEM solution may vary depending on how the solution's dashboard is set up (or if it supports custom dashboards).

For effective SIEM solution management, organizations should have at least one person dedicated to the task. This solution expert should be familiar with the tool the organization is using—or become familiar with it through training provided by the solution maker (if available) or from someone else experienced in using the SIEM solution.

Popular SIEM Tools

There are numerous different SIEM solutions on the market today that have varying built-in functionalities. Knowing some of the top SIEM tools and their capabilities can be useful for creating a bencmark to compare other solutions to in the future.

Here's a short list of some of the top solutions on the market:

If you're unfamiliar with Rapid7, they're a cybersecurity solution provider that helps other organizations increase their security by using a combination of visibility, analytics, and automation solutions. Gartner recognized Rapid7 as a "visionary" company in their Magic Quadrant report for 2018—taking particular notice of Rapid7's "User Context and Monitoring, as well as Deployment, Operations, and Support."

The reason we're a Rapid7 partner is that they have incredibly powerful solutions for helping organizations assess their risks and manage their vulnerabilities.Their cloud-based InsightVM solution helps improve vulnerability management by providing detailed data for study from your entire cloud ecosystem as well as analyzing real-world attack information. This data helps our cybersecurity team prioritize customer vulnerabilities and remediate active threats more efficiently.

Furthermore, their dynamic application security helps our team improve its managed application security services by crawling and assessing web applications for vulnerabilities.

Popular SIEM Tools

LogRhythm

LogRythm's next-gen SIEM platform incorporates a variety of threat detection capabilities in a single solution. Some of its capabilities include network detection and response (NDR), security orchestration, automation, and response (SOAR), user and entity behavior analytics (UEBA), and machine-based analytics.

While many of these tools have some overlap, they all help to improve various aspects of threat detection and response—as well as threat investigation. One particularly valuable tool included in the LogRythm kit is their geolocation-based threat detection. This helps to identify where threats are coming from so companies can better understand who's targeting them and why.

splunk>

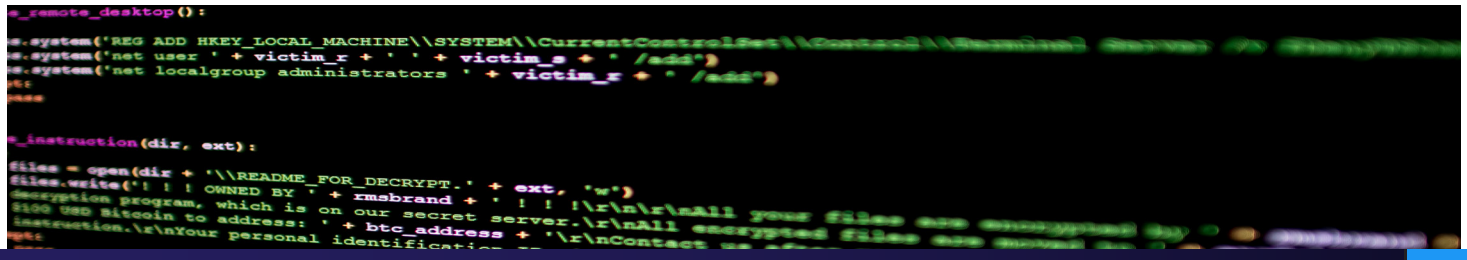
Splunk offers many data-related solutions for enterprises—and is one of the leading companies in the field. Their SIEM tool leverages the company's extensive experience in data analytics to create a solution that is both flexible and robust. It also integrates with other tools to help make customizing the solution simpler for users.

Splunk's behavioral analysis helps companies simplify their security operations by more accurately detecting anomalies in network use patterns. The solution also helps companies prioritize their most critical security issues so the issues with the biggest impact on security can be fixed first.

IBM QRadar

IBM is one of the more well-known names in the technology industry. Their QRadarSIEM solution is designed to "Detect known and unknown threats, go beyond individual alerts to identify and prioritize potential incidents, and apply AI to accelerate investigation processes by 50 percent."

QRadar's robust AI helps companies detect and counter insider threats, "zero day" attacks, and APTs more quickly. This, in turn, helps to minimize the impact of such attacks.



Managing SIEM Solutions

Security information and event management tools, or SIEM tools, are a crucial part of modern network security architectures. However, unlike many other cybersecurity tools, SIEM solutions don't directly work to stop cyberattacks. Instead, SIEM solutions collect information about security events on the network to generate alerts or instruct other security controls to take a pre-set action. In this way, security information and event management solutions can be invaluable for automating security incident response.

The challenge is in managing SIEM tools to eliminate false positives and sort through the massive amount of data they supply quickly and efficiently. Many organizations adopt an SIEM tool without the appropriate resources on hand to manage them—which leads to suboptimal incident response as they struggle to keep up with the ocean of data an SIEM solution can generate.

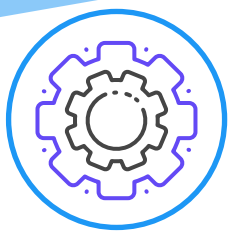
So, how can organizations manage an SIEM solution to achieve better cybersecurity without drowning in an ocean of noise?

Discovering the Right SIEM Solution

Not all SIEM solutions are the same, so it's important to do some research before choosing one.

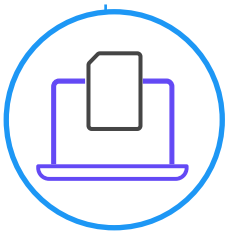
Some things to look for in an SIEM Include:

Managing SIEM Solutions



Deployment Method for the SIEM Product:

The deployment method for an SIEM solution can affect its management and cost. As noted by TechTarget, “Most SIEMs require the purchase of hardware or software, while usage fees determine the costs of cloud-based SIEM services.” Hardware-based SIEM solutions that are installed locally might have a higher upfront cost for installation and hardware, while cloud-based solutions will have an ongoing subscription fee.

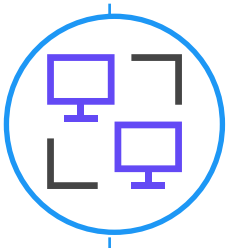


Post-Incident Reports & Forensics:

What reports does the SIEM tool generate following suspected security events? What information does it capture about these events to empower thorough investigations and allow cybersecurity experts to prevent future incidents? A security information and event management tool should make it easy to investigate the methodology behind an attack so future attacks may be prevented.

Use of Machine Learning:

Can the SIEM learn from the data it collects to eliminate false positives and reliably discover unusual traffic or activity that indicates an active security breach? SIEM tools with machine learning capabilities help to minimize the “noise” of irrelevant data by learning to differentiate normal traffic from suspicious activity.



Integration with Other Security Solutions.

Does the SIEM solution have the capability to trigger responses from other security tools to automate cyber threat response? If an SIEM tool can send commands to other security solutions based on observed traffic, it may be able to contain an attack before the attacker has time to break out into other assets on the network.

Threat Intelligence Feeds.

What threat intelligence tools does the SIEM solution integrate with to “learn” about new cyber threats? Can it work with the organization’s existing threat feeds, or can it only use a few proprietary ones? Being able to work with the threat intelligence tools that are most relevant to the threats faced by the organization is crucial for ensuring long-term SIEM effectiveness.

SIEM Co-Management & Why Should My Company Use It?

As mentioned earlier, SIEM co-management involves using an MSSP's services to help manage and control a SIEM solution. However, it differs from fully-managed SIEM in that the MSSP works with the company's IT/security team to ensure that the customer is kept abreast of any cybersecurity issues.

There are several key advantages of using co-managed SIEM services from an MSSP:

Instant Access to SIEM Experts

Because they have a larger team of dedicated experts, MSSPs are often able to provide expert advice on numerous SIEM tools. They can provide advice on which SIEM tools best fit a company's needs as well as training, so the internal IT team can eventually manage the solution on their own.

Being Able to Stay Informed

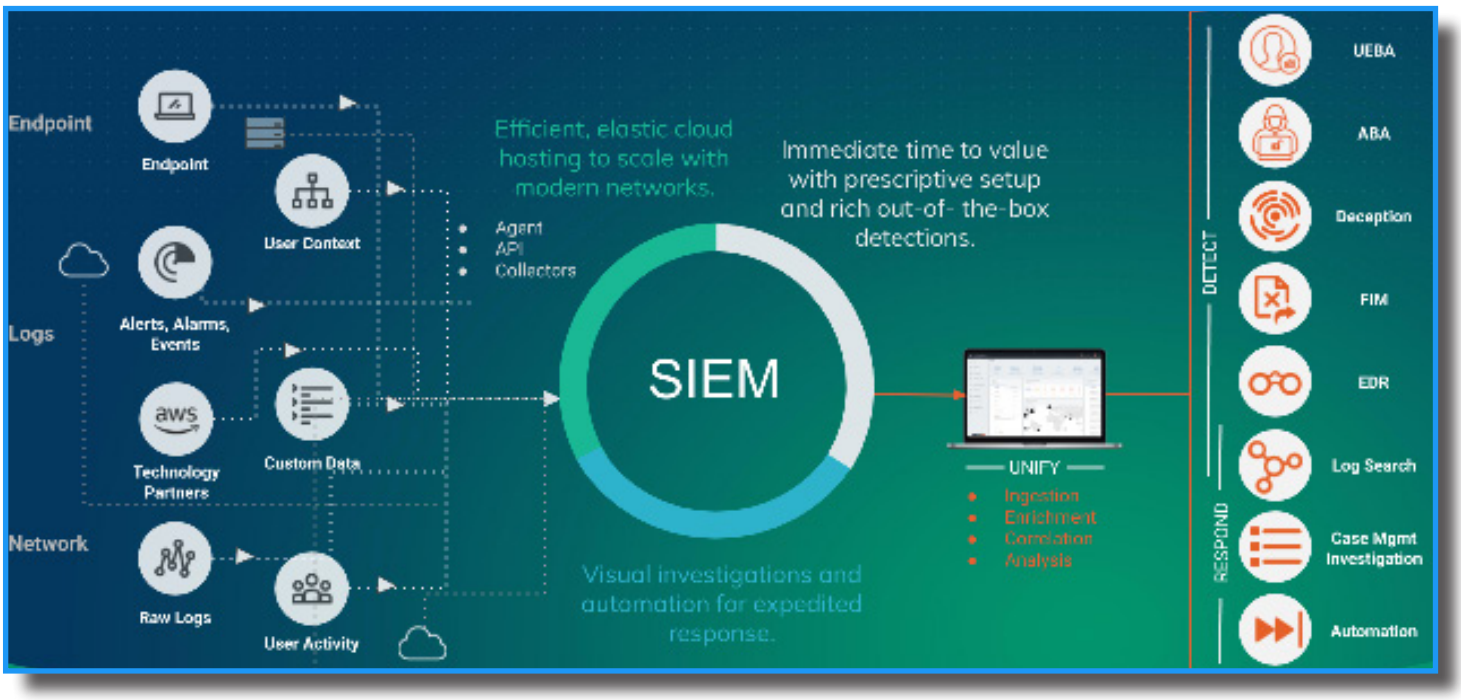
With a co-managed solution, organizations are explicitly kept well informed regarding any developments with the SIEM solution—and what it detects. This helps the internal cybersecurity team stay informed of and involved with security incidents.

SIEM Co-Management & Why Should My Company

Reducing IT Workloads

Bringing on a team of dedicated experts helps to alleviate some of the burden on an organization's IT department. This allows IT staff to focus on their company's core business rather than having to worry about cybersecurity—and at a fraction of the cost of hiring more internal security staff.

SIEM for the Modern Enviroment



Advantages of Co-Managed SIEM

Organizations of all sizes have faced constraints within their IT-budgets for some time now. As the threat landscape continues to grow daily and IT-budgets remain constant, this has left our SIEM tools dormant. Many organizations are mandated with a slew of cybersecurity policies, similar to those on Forbes, Global 2000, and remain with low budgets for IT teams.

SIEM tools, in general, are a more substantial capital improvement to an organization. Here at Compuquip, we understand the rules and regulations and the already-tight budgets in IT, so we tailor each managed SIEM solution to fit your organization's needs,

Our Co-Managed SIEM services but is not limited

System Integrations (SIEM, EDR, SOC)

Amplifying Operational Effectiveness

Detect Threats in Your Network

Advantages of Co-Managed SIEM

Compliance Reporting

Proactive Threat Hunting Capabilities

Investigation or Incident Management

Compuquip's Co-Managed SIEM will work with you and your teams 24/7 to ensure that the benefits listed above are met and exceeded. We specialize in detecting system vulnerabilities through automation and machine learning. Our proven track record shows how quickly and responsive we are towards threats and ensuring your organization's business continuity.

As your managed SIEM provider, one of our goals is to make sure your team will have more time to tackle larger projects while our team is in the background making sure that your daily operations remain stable.

Conclusion

Instead of dedicating a single internal employee to manage their SIEM tools, some organizations use a managed SIEM service from a managed security service provider (MSSP). With a managed SIEM service, the MSSP provides the labor for directly managing the SIEM solution—including reviewing activity logs, configuring alert settings, and checking the SIEM software's integrations with other network security measures.

Is your organization in need of help with its SIEM solutions? Whether you need help picking a tool, configuring it to your needs, or sifting through all of the data it provides, Compuquip Cybersecurity is here to help

Contact Us Today

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530
Coral Gables, FL 33134

Follow us on: