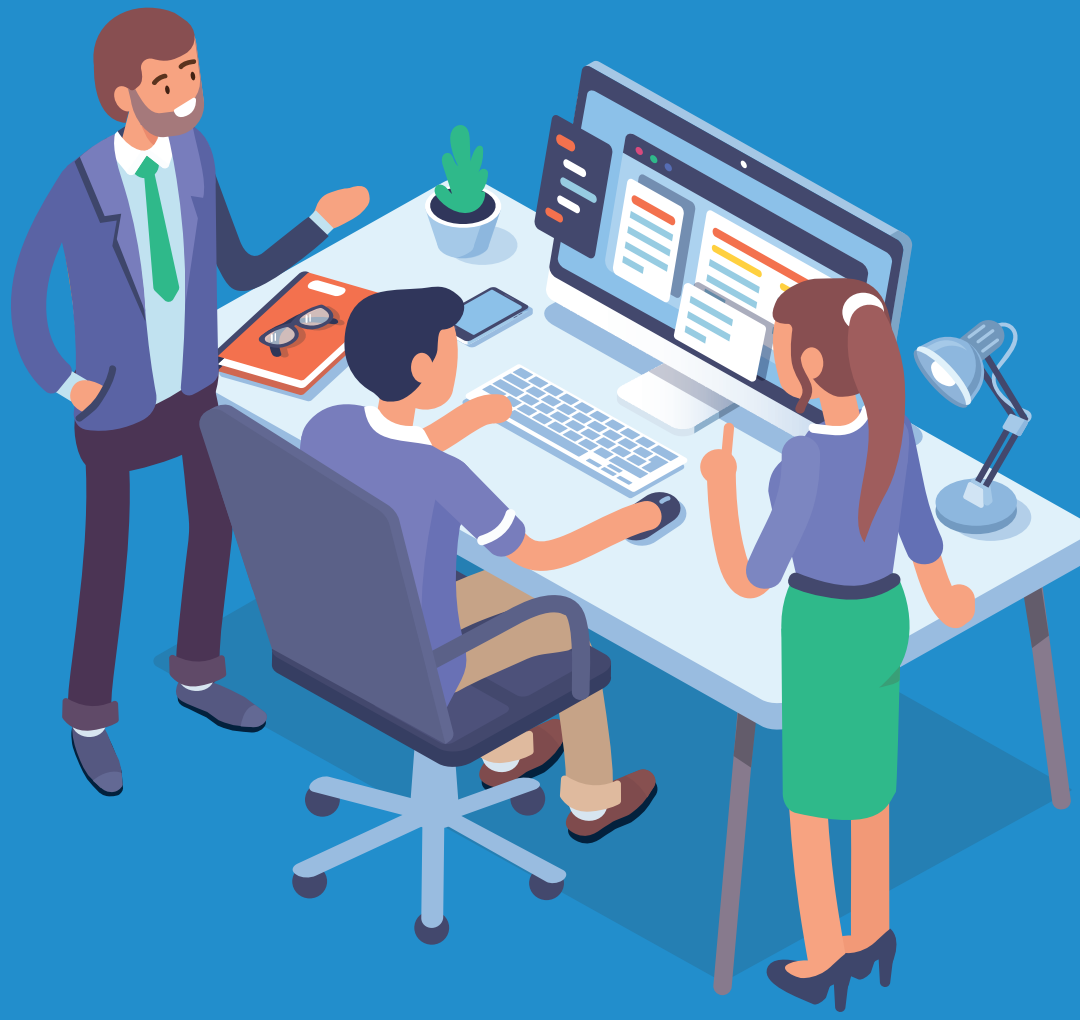
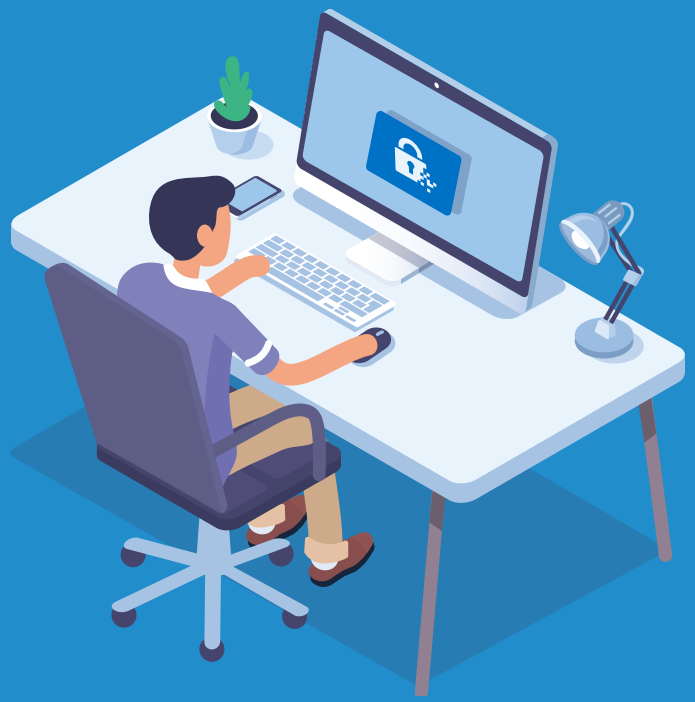
coresecurity
by HelpSystems

SIEM Buyer's Guide





SIEM Buyer's Guide

The Security Challenge Today

It's no secret that security threats are increasing, and they can come from both internal and external sources. In addition to ongoing threats from hackers looking to breach the security protocols guarding your sensitive information, another rapidly rising concern is that of employees who accidentally misconfigure security settings in a way that essentially opens the door to attack. To address these issues, IT organizations have put various systems in place to protect against intrusion and a host of different risks.

The downside of these safeguards is they generate so much monitoring data that IT teams are then faced with the problem of interpreting it all to pinpoint actual problems. In fact, the volume of security data flowing to understaffed IT security groups is largely useless unless it can be quickly analyzed and filtered into actionable alerts. Given the reams of data in question, it's no longer possible for organizations to use manual analysis to handle this job.

This is where SIEM software steps in.

Intro to SIEM

SIEM—or security information and event management—is a type of software that aims to give organizations helpful insights into potential security threats across critical business networks. This is possible via centralized collection and analysis of normalized security data pulled from a variety of systems, including anti-virus applications, firewalls, and intrusion prevention solutions.

Gartner coined the term 'SIEM' (pronounced "sim") in a 2005 report called "Improve IT Security With Vulnerability Management." The term brings together the concepts of security event management (SEM) with security information management (SIM) to achieve the best of both worlds. SEM covers the monitoring and correlating of events in real time as well as alerting the configuration and console views related to these activities. SIM takes this data to the next phase, which includes storage, analysis, and reporting of the findings.

Why Is SIEM Important to Companies Today?

With SIEM, you have an effective method of automating processes and centralizing security management in a way that helps you simplify the difficult task of protecting sensitive data. SIEM gives you a leg up in understanding the difference between a low-risk threat and one that could be detrimental to your business.

SIEM software relays actionable intelligence that enables you to manage potential vulnerabilities proactively based on real-time information, protecting your business and your customers from devastating data breaches. With the ever-increasing incidence of these attacks, this technology is more important than ever.

Sharpen Your View

SIEM is an essential part of your security and IT toolkit today. Think of it as a lens that sharpens your view across the big picture to help you focus your team's efforts on where they can have the most impact. This is particularly important in situations involving emerging threats, when the ability to collect and analyze incoming data aids in how quickly analysts can investigate and resolve issues.

Summary of Key SIEM Capabilities

- ✓ Centralize your view of potential threats
- ✓ Determine which threats require remediation, and which events are simply noise
- ✓ Escalate issues to the appropriate security analysts who can take fast action
- ✓ Include context for security events to enable well-informed fixes
- ✓ Document detected events and how they were remedied in an audit trail
- ✓ Show compliance with key industry regulations in an easy reporting format

How Has SIEM Advanced Over the Years?

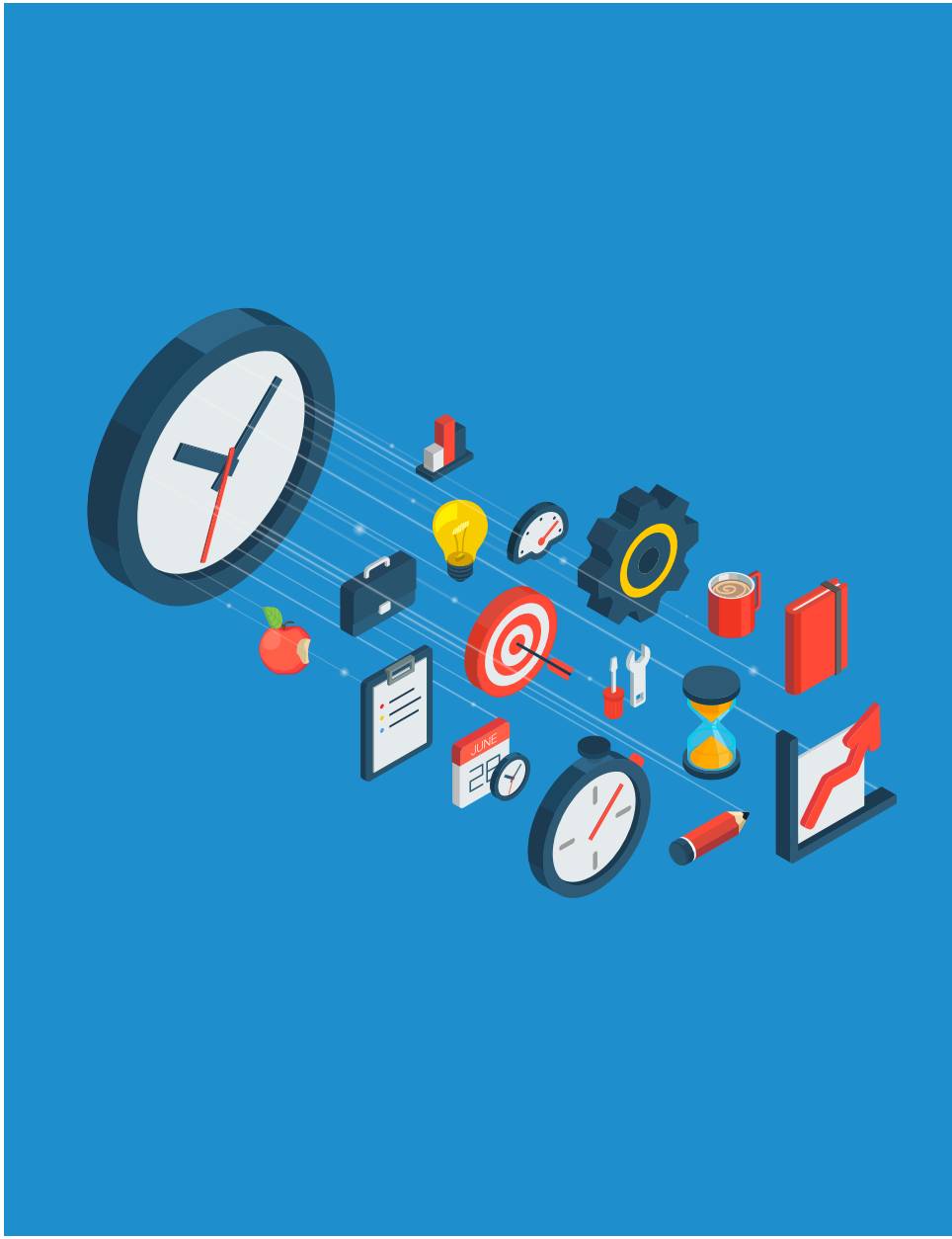
- **Integration with other security tools:** SIEM pulls in data from anti-virus applications, login data, and more to give you a holistic picture of your environment. This helps you assess potential impacts to the security of information stored on-premises, in the cloud, or in a hybrid configuration.

- **Forensic data:** SIEM gives you the ability to drill into the details of a security incident to determine exactly what happened and what equipment may have been affected.

- **Audit trial:** Meeting compliance requirements requires the ability to generate a detailed audit trail of your security practices and events, and SIEM enables this with detailed reporting.

- **Normalized data:** Having security data flowing into a centralized view of your infrastructure is effective only when that data can be normalized. This means that despite thousands or millions of inputs coming from different systems and sources, everything can be put into a common format ready for the SIEM solution to conduct its analysis and correlation. This takes the workload off your team and enables them to leverage a streamlined view of activity and potential concerns.

- **Correlation:** Oftentimes, correlating individual records or events (e.g., a login that was just created and then used to access sensitive information) enables you to clarify the bigger picture and identify malicious activities as they happen.



Key Features in an Effective SIEM Solution

Given the number of SIEM solutions on the market today and the capabilities described previously, it's helpful to understand the features you need to support your efforts. Consider these areas as you evaluate your options.

Security Event Prioritization

It is impossible to stay ahead of the curve if your security team is buried investigating meaningless security events. You need to determine which events are most critical and which are lower priority. Look for a solution that makes the prioritization process easy with out-of-the-box controls that can be adjusted as you see fit.

Normalization of Disparate Data Sources

Organizations rely on multiple technologies to run their business. This makes it difficult for security teams to understand the data coming in from these disparate sources. SIEM turns this data into actionable intelligence by normalizing it into a common format and giving it meaning. With a robust solution, analysts won't need to understand the nuances of different operating systems, applications, databases, firewalls, or network appliances to know what the data means and what to do with it.

Data Enrichment

Look for the ability to get additional context behind security events for quick and thorough response. Data enrichment puts all the necessary event details and forensic analysis at your fingertips. For example, if a new user is created and then that user immediately connects to a critical system, SIEM can recognize that this is not normal behavior and escalate the incident for investigation.

Real-Time Threat Detection

In order to minimize the impact of a breach, you have to detect threats quickly. This means having the ability to log, correlate, and prioritize events in real time to give your team a head start on resolving and mitigating threats before they result in a devastating breach.

Streamlined Incident Response

Automatically escalate events to the right person and manage any cases that require further investigation to make your team more efficient.

Out-of-the-Box Security

As you connect new data sources, like Windows® servers or Oracle® databases, make sure you can automatically apply the appropriate security controls and escalation rules. Out-of-the-box security templates make it easy to get started quickly and can be configured as needed.

Security and Compliance Reporting

IT operations and security teams alike are required to provide reports to both auditors and executives on a regular basis. Most organizations also need to comply with multiple regulations, which adds to the complexity and reporting effort. Having a robust reporting engine in your SIEM provides for easy reporting of log data, events, and incident response activity. Compliance reports generated by a SIEM can even help show you how your security posture is improving over time.

The Bottom Line on Features

Invest in a solution that has the right level of features to meet your needs—but isn't so complex your team won't be able to use it easily on a daily basis. You don't want to get stuck with a tool that's complicated or expensive because it will likely prevent you from implementing other critical controls in your organization.

Additional Areas to Evaluate

Aside from functionality considerations, there are other elements of your SIEM solution that will determine its long-term success and usability for your organization.

Enterprise Solutions vs. Open Source

Some SIEM solutions fall into the enterprise category, meaning they have a dedicated development team focused on product enhancements as well as customer support. Other options are built on the open source model and rely on a large community of developers for support and bug fixes. Open source SIEM solutions provide basic functionality that can be great for smaller organizations that are just beginning to log and analyze their security event data. But over time, many IT professionals find that open source SIEM software is too labor-intensive to be a viable option as the organization grows. In addition, some companies have policies that discourage the implementation of open source solutions, so make sure you know the pros and cons of each approach and what's allowable at your organization.

Automation

Some parts of the SIEM process can be automated to save time and speed information sharing among your team. Notifications can also be routed to the right person depending on the event/data source. For example, a virus detection event coming from your Linux environment can be directly routed to your Linux admin, who will know best how to quickly isolate the system and remediate the infection before it spreads across the environment.

Implementation and Training

Every software vendor has a different process when it comes to how their solutions are implemented and the ways your team can participate in training. Understanding your options for these services is key to getting a handle on how long it will take to get up and running on the software and when you can realistically start seeing the benefits. Intuitive solutions require a minimal amount of upfront training to start seeing results that will benefit your organization. More complicated solutions require your team to invest a substantial amount of time in training and regular system tuning activities.

Professional services usually provide integration, development, and consulting. If you don't have the resources needed to implement the solution, or you'd like to have the vendor help with the migration to the new solution, be sure to ask whether these services are available.

Training should give you in-depth knowledge of the solution. When you request details on the training, consider asking the vendor the following questions:

- Are the training costs the same regardless of how many people attend the session?
- Is the training interactive or demonstrated by the trainer?
- Are there course outlines you can review before purchasing the sessions?
- Can you customize what will be covered in training?

Support

Evaluate the vendor's customer support options. Are they offered 24/7? Can you communicate issues via web, phone, and chat? Is support outsourced or handled locally? All of these considerations are important to think through to protect the long-term health and relevance of your SIEM application.

Other Cost Considerations

Licensing and Deployment Methods

Some SIEM software vendors charge by the amount of data generated or by how many systems the solution is managing, and others simply have a flat-rate approach. Likewise, deployment models can be on-premises or in the cloud, and some solutions use agents while others don't. An agent is code that has to be placed between endpoints/systems to enable the sending of information from the system being monitored to the SIEM solution for normalization and evaluation. Agentless applications connect automatically to the systems they monitor to simplify administration. Find out how differences in the offerings you evaluate may affect your overall total cost of ownership.

ROI

Being able to detect threats and shut them down will have significant ROI for your business, but it could be hard to quantify. Focus on the efficiency the SIEM solution is bringing to your IT organization and the time it's saving as an aggregator of multiple sources of security information. You can evaluate how the SIEM solution helps you:

- Centralize your view of potential threats
- Determine which threats require remediation, and which events are simply noise
- Escalate issues to the appropriate security analysts who can take fast action
- Include context for security events to enable well-informed fixes
- Document detected events and how they were remedied in an audit trail
- Show compliance with key industry regulations in an easy reporting format

Impact on Headcount

Some solutions require dedicated staff to run the software and manage the interface of events. Others are a little more lightweight and can likely be managed by your existing staff. Determine whether the new SIEM application will require additional headcount for day-to-day management, and whether this cost is in your existing budget.

SIEM's Role in Regulatory Compliance

SIEM gained popularity with large businesses working to comply with the Payment Card Industry Data Security Standard (PCI DSS). In addition, it has highly useful applications in helping you meet regulations for the EU's General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX), and others. These laws require organizations to have mechanisms in place to detect threats and resolve them quickly. This means you have to know what's happening in a wide-reaching IT infrastructure that could span on-premises, cloud, and hybrid environments.

A SIEM solution is key to getting the right kind of insight in place to monitor data and act quickly for threats determined to be cause for alarm. When all this activity is captured in a detailed audit rail, auditors can see your organization is taking the necessary steps to protect its data.

Requirements Checklist

After you've thought through the features and other options you'll need in your SIEM solution, it's helpful to develop a requirements checklist to evaluate the various offerings on the market and how they line up with what you need.

Below is an example checklist to help you get started.

Requirement	Vendor 1	Vendor 2	Vendor 3
The solution has role-based access controls for separation of duties			
The security regulations I need, such as ____ (e.g., PCI DSS, HIPAA, SOX, BCRA, FISMA), are supported by the solution.			
The solution collects logs and events from multiple sources and system types I require, such as _____ (e.g., Linux, AIX, Windows, IBM i, VMware, network appliances, databases).			
The solution correlates security events in real time.			
The solution stores historical data over the long term to support compliance mandates.			
The solution works for multiple use cases, including non-security projects such as IT operations.			
It's easy to operate and doesn't require complex programming or specially skilled staff.			
The solution is scalable with predictable pricing.			
The solution is backed by a proven company with a history of providing robust software and making further investments and improvements.			
The solution isn't limited to being installed only on-premise; security practitioners must support hybrid and cloud-first models.			
There's an open ecosystem that enables user configurations to support their unique use cases.			
The dashboard supports data sorting and filtering with a few simple mouse clicks.			
There's built-in reporting with configurable report templates.			
The solution features a full audit trail of security analyst activities.			
The solution monitors user activity to pinpoint breach attempts and uncover misuse.			
The solution automatically prioritizes threat events and assigns them to analysts.			
The solution supports the ingestion of application logs and events via simple menu interfaces.			
The solution can identify notable events, indicate their severity, and display their status.			
The solution can perform ad-hoc searches of event and log data.			
The solution translates data from multiple sources into a common format for easy analysis.			

You Have Your Short List of Vendors—Now What?

Determine Your Budget

When determining how much you want to spend on a SIEM solution, consider what is—and isn't—included in the price. Questions to ask the vendor's sale team include:

- Can I license specific modules?
- Can I lease the software?
- Do you offer user- or vendor-based licensing, or are users and vendors unlimited?

Beyond initial software licenses, most buyers purchase a support package and annual maintenance, so they can upgrade to the latest product version as soon as it's available. Also consider any optional investments you'd like to put into the product, such as professional services (e.g., migration and implementation assistance, software training) or add-on modules that expand what you can do with your SIEM solution.

Study Vendor Resources

Take some time to explore each vendor's SIEM resources. Good resources, like online documentation and educational videos, tell you that a vendor is not only dedicated to developing powerful software, but that they're also dedicated to helping you understand everything the product can do for your organization.

Request a Demo

After you've whittled down the options to two or three that look like they will fit your organization's needs, invite stakeholders who are part of the purchase decision to live, one-on-one demos. These typically last an hour and are run by each vendor's SIEM product experts.

Come prepared and ask the questions that will help you fully evaluate each solution and address any concerns you have. During each demo, remember you're evaluating not only the software, but also the vendor's representatives and their professionalism. As they'll be your partner for SIEM functionality for years to come, you need to feel confident in their capabilities.

Trial the Solution

For the solution that truly piques your interest, determine whether you want to ask the vendor about doing a trial of the software. This means having it installed on your network for a real-world view of how it would perform. Trials typically last 14 to 30 days and let you test out scenarios with all your parameters in place.

coresecurity
by HelpSystems

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.

cs-gd-0621-79d