

[Download this free guide](#)

Go Now: Malware Protection Best Practices

Should security teams clean up the malware and move on or format the hard drives to start over with a clean system? In this expert guide, security pros weigh in on how antimalware protects the enterprise.

[Start Download](#)

The underlying principle of a SIEM system is that relevant data about an enterprise's security is produced in multiple locations and being able to look at all the data from a single point of view makes it easier to spot trends and see patterns that are out of the ordinary. SIEM combines [SIM](#) (security information management) and SEM (security event management) functions into one security management system.

A SEM system centralizes the storage and interpretation of logs and allows near real-time analysis which enables security personnel to take defensive actions more quickly. A SIM system collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm they are fulfilling an organization's legal compliance requirements.

A SIEM system collects logs and other security-related documentation for analysis. Most SIEM systems work by deploying multiple collection [agents](#) in a [hierarchical](#) manner to gather security-related events from [end-user](#) devices, [servers](#), network equipment -- and even specialized security equipment like [firewalls](#), [antivirus](#) or [intrusion prevention](#) systems. The collectors forward events to a centralized management console, which performs inspections and flags anomalies. To allow the system to identify anomalous events, it's important that the SIEM administrator first creates a profile of the system under normal event conditions.

PRO+ Content

**E-Handbook**[Managing access to keep privileged users' credentials secure](#)**E-Zine**[Cybersecurity careers soar with security leadership skills](#)**E-Zine**[Is your IAM policy a roadmap to security or leading you off a cliff?](#)

At the most basic level, a SIEM system can be rules-based or employ a statistical [correlation engine](#) to establish relationships between [event log](#) entries. In some systems, pre-processing may happen at edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced. The danger of this approach, however, is that relevant events may be filtered out too soon.

SIEM systems are typically expensive to deploy and complex to operate and manage. While Payment Card Industry Data Security Standard ([PCI DSS](#)) compliance has traditionally driven SIEM adoption in large enterprises, concerns over advanced persistent threats ([APTs](#)) have led smaller organizations to look at the benefits a SIEM managed security service provider ([MSSP](#)) can offer.

This was last updated in [December 2014](#)

Next Steps

Karen Scarfone explains the [basics of SIEM products](#) in the enterprise.

What are the [enterprise benefits of SIEM systems](#)?

Learn how to [evaluate SIEM products to determine which are the best for your organization](#).

Find out why network intrusion prevention systems compliment SIEM systems in this Buyer's Guide series that covers the [basics of network IPS systems](#), lays out the [enterprise benefits of network IPSes](#), and explains [how intrusion prevention systems use data from SIEM systems](#).

Continue Reading About security information and event management (SIEM)

- [Plan ahead to avoid SIEM deployment pitfalls](#)
- [Finding an enterprise SIEM: What problems are you trying to solve?](#)
- [The past, present and future of SIEM technology](#)

Related Terms

PCI assessment

A PCI assessment is an audit of the 12 credit card transaction compliance requirements required by the Payment Card Industry Data... [See complete definition](#) ⓘ

PCI QSA

Payment Card Industry Qualified Security Assessor (PCI QSA) is a designation conferred by the PCI Security Standards Council to ... [See complete definition](#) ⓘ

security awareness training

Security awareness training is a formal process for educating employees about corporate policies and procedures for working with ... [See complete definition](#) ⓘ

Join the conversation


2 comments

Share your comment


☒ Send me notifications when other members comment.

Add My Comment

Oldest ▼

[] [rajiv2177](#)
- 7 May 2014 8:22 AM
Can go for EventLog Analyzer

Reply

[] [bartour](#)
- 21 Oct 2016 11:04 AM

You said, "The acronym is pronounced "sim" with a silent e." However as you also stated, there exists a Security Information Management (SIM) and Security Event Management (SEM), so the SIEM has been pronounced like "SEEM" to distinguish it between the others ("sim" and "sem").

Reply

[CLOUD SECURITY](#) [NETWORKING](#) [CIO](#) [CONSUMERIZATION](#) [ENTERPRISE DESKTOP](#) [CLOUD COMPUTING](#) [COMPUTER WEEKLY](#)



SearchCloudSecurity

Four common cloud attacks and how to prepare for them

Cloud attacks are increasingly targeting service providers. Expert Frank Siemons looks at the different types of attacks from ...

How DevOps tools can be used to integrate cloud automation

DevOps tools can be used to deploy secure cloud automation. Expert Dave Shackelford looks at how this works and which tools are ...

[About Us](#) [Meet The Editors](#) [Contact Us](#) [Privacy Policy](#) [Videos](#) [Photo Stories](#)

[Guides](#) [Advertisers](#) [Business Partners](#) [Media Kit](#) [Corporate Site](#) [Contributors](#)

[CPE and CISSP Training](#) [Reprints](#) [Archive](#) [Site Map](#) [Events](#) [E-Products](#)

All Rights Reserved,
Copyright 2000 - 2017, TechTarget

