ControlScan

SIEM: A Guide to Security Information & Event Management

WHAT IS A SIEM?

A SIEM (Security Information & Event Management) is a platform for managing security incidents. It allows the collection of system logs and machine data from across your IT environment to help identify unusual or suspicious activity — and then reports an alert in real time if it finds anything suspicious. You can think of a SIEM as a tool that provides a comprehensive view of an organization's IT security.

A SIEM essentially takes inputs from many different sources of information within a customer's IT environment, and allows correlation of that information to determine whether a security incident has occurred. In its most basic form, it ingests log files from devices on a customer's network, as well as threat intelligence data in the marketplace. A SIEM aggregates this endless stream of data to help make sense of what's happening within your environment.

Who uses a SIEM?

Historically, a SIEM was especially helpful for larger companies, as they tend to employ many more devices and people. That can mean logging thousands or even millions of events every day. But a SIEM can be useful for organizations of all sizes, especially when implemented as a service, or in a managed fashion. For example, a mid-sized company with a small, busy IT department might benefit most from a SIEM solution that includes resources to efficiently configure and manage the platform. Or consider a smaller organization where one person holds nearly all administrative privileges. It would be in their best interest to bring in a trusted partner to look out for abnormal usage from users with elevated permissions.

What is the ultimate value of a SIEM?

Security Information & Event Management is about awareness. SIEM solutions, when used properly, help identify and manage security events on a customer's network that would otherwise go undetected, and they allow for a quick response when there is an issue. It can also be about action; while a SIEM keeps digital record of network activity in case an organization should need to build a case against an attacker after the fact, a SIEM solution can also help you stop a breach before it causes damage.

A DAY IN THE LIFE OF A SIEM SYSTEM

Whether working for a small business or an international corporation, a SIEM platform is always busy. Here are just a few things that your SIEM could be doing for you every day:

Collecting and storing logs.

A SIEM aggregates records that detail what's happening within specific applications in a given environment, like desktop devices, servers, routers and more. It watches what's happening, makes record of that and then organizes it. It takes in this data not only for its own monitoring, but so you can find that information should you ever need it — for example, these records may be required to fulfill an organization's compliance standards.

Creating a story of events.

A SIEM not only collects raw data but seeks to understand it. It learns what is normal behavior (an employee logs into their workstation, opens a file-sharing system and downloads a local copy of a word document) and what isn't (someone at an unknown IP tries and fails to log in to the system a few dozen times outside of regular business hours).

Reporting and responding to potential incidents.

A SIEM recognizes that something about this suspicious user (the unknown IP mentioned above) isn't right, because their behavior falls outside the pre-defined definition of normal activity on this network. Maybe it sends an email to the IT department, or maybe it sends a message directly to the cell phone of the system administrator. A SIEM tool lets you react in real time to threats. The right tool can even take automatic action under predefined conditions, like disabling network adapters of potentially compromised hosts, or updating a user's access permissions.

TYPES OF SIEM SOLUTIONS

If you're looking for the right SIEM implementation for your organization, you have a few options from which you can choose. Each, of course, comes with its own pros and cons.

The Do-it-Yourself Approach

In-House SIEM

With an in-house SIEM solution, an organization would purchase the software and hardware and then manage it themselves, on premise.

+ Pros: In-house SIEM gives you ultimate control over your system. You can customize it to meet your organization's specific security needs and fine tune or update the system whenever you'd like. You wouldn't leverage a third party for any of it — you just log in and make your changes in real time. Additionally, all of your data stays "in-house"…a requirement for some businesses.
+ Cons: With a self-managed SIEM, you're totally responsible for it. That means integrating it into your existing systems, monitoring logs, customizing alerts, and training and/or employing special staff to handle it — not to mention paying for the large initial investment. You also have to maintain the infrastructure, perform your own system patching, and manage the implementation in its entirety.

Cloud-based SIEM

With cloud-based SIEM, customers subscribe to SIEM as a service.

+ Pros: The subscription SIEM platform is constantly updated. There's typically little to no SIEM hardware to maintain, and licensing is typically purchased as a monthly subscription based on capacity, versus purchasing up front. Customers control how they implement the SIEM system at their organization. They don't have to rely on a third party to manage the implementation.
+ Cons: Customers still must retain the expertise to leverage the SIEM functionality effectively. Some people may not be comfortable with their data residing anywhere other than their own data center. Additionally, many customers may choose to use subscription SIEM for a certain set of its capabilities; consequently, they may not realize its full benefits or potential.

Managed SIEM

Just like the do-it-yourself approach, Managed SIEM can leverage either an on-premise implementation, or a cloud-based implementation. Managed SIEM can come with all of the technology features of a do-it-yourself implementation, AND includes the expertise necessary to fully implement the technology in the best possible way to meet security objectives.

+ Pros: The subscription SIEM platform is constantly updated. There's typically little to no SIEM hardware to maintain, and licensing is typically purchased as a monthly subscription based on capacity, versus purchasing up front. Customers control how they implement the SIEM system at their organization. They don't have to rely on a third party to manage the implementation.
+ Cons: Customers still must retain the expertise to leverage the SIEM functionality effectively. Some people may not be comfortable with their data residing anywhere other than their own data center. Additionally, many customers may choose to use subscription SIEM for a certain set of its capabilities; consequently, they may not realize its full benefits or potential.

SIEM FEATURES AND CAPABILITIES

No matter what SIEM solution you choose, your platform should come with some basic capabilities.

Log management

The collection, standardization and ongoing monitoring of log files for behavioral anomalies.

Event correlation

The ability of a SIEM system to recognize that one threat may exist in various pieces on a network. A SIEM can match up suspicious activities of a given user across the network, and recognize that they're related.

Threat identification

With a SIEM platform, you would continually build your triggers for different alerts. And a SIEM platform managed by a skilled user improves your ability to identify threats and respond to them efficiently.

Reporting

This is a huge benefit of having a SIEM in place. You can create custom reporting so the right person or group of people always know when something isn't right.

Incident response

A SIEM allows you to aggregate information related to a potential incident. If something suspicious happens, you'll be able to open to the case and track related items to help resolve the problem.

Threat intelligence

A strong SIEM platform includes an integrated ability to access data about threats happening **around the globe**, and the ability to understand their possible relation to events happening on your network.

EVALUATING THE NEED FOR SIEM

If you are researching SIEM, then you already recognize that you may not be effectively handling all of the security information generated by your IT environment. If your business handles sensitive information (where if lost or compromised, would significantly impact your business) you are likely a perfect candidate for implementing a SIEM.

To be blunt, it is highly likely that most organizations would benefit from a SIEM. Historically, though, the cost of implementing a SIEM has rendered an implementation prohibitive. With the varied products on the market today, and the explosive growth in managed security services, SIEM is becoming more and more within reach for businesses of all size.

HOW DOES SIEM PRICING WORK?

On-premise SIEM implementations are priced by appliance, or by hardware and software. Prices vary wildly based on how capable your SIEM platform actually is, out of the box. Typical pricing for a modestly capable solution starts in the tens of thousands of dollars range, and scales up from there.

Cloud-based SIEM pricing is typically based on the amount of data the SIEM platform processes, and is presented as a monthly subscription on an annual contract. You might pay a threshold fee/rate for the capacity of log files being processed by the SIEM per day, or per second. You may also have a pricing variable based on how long you want the log data retained for audit purposes (typically driven by compliance requirements).

Managed SIEM, in either on-premise, or as a service configuration, will include in the price the availability of expert security operations staff members to assist in the setup, configuration, optimization and ongoing management of your SIEM implementation.

TOTAL COST OF OWNERSHIP

Your organization could always choose to take SIEM implementation and management all in-house. However, there are quite a few things you should keep in mind while considering this option. The value of your SIEM depends on how efficiently you are able to use it, whether that means recognizing security threats, prioritizing events, or even creating meaningful reports. This also refers to your team's ability to constantly improve threat intelligence, and to keep up with the speed at which digital threats are expanding and evolving.

All-in, implementing and managing a SIEM yourself effectively can cost you anywhere in the six-figure range...in its first year. This cost includes not only the actual technology and its installation, but the staff you'd need to hire and train to maintain it (and the space you'd need to house all of the aforementioned elements). And of course, as mentioned above, your SIEM is only as strong as the professionals who implement and maintain it. A managed SIEM implementation can start in the four figure range for the first year, and scale upwards depending on how large your environment is.

SIEM & COMPLIANCE

Your organization may need to keep up with a variety of compliance requirements. A SIEM can help you meet these. The most common include:

HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule covers the security of individuals' electronic protected health information (or ePHI). A SIEM provides you with actionable reports and empowers forensic investigations. With this tool in place, you will be able to get immediate notification and analysis of conditions impacting the integrity of your organization's ePHI data.

PCI DSS: The Payment Card Industry (PCI) Data Security Standards (DSS) cover data security for credit cardholders. It's also helped ensure the implementation of consistent security measures across the globe. A SIEM can help you meet PCI DSS compliance and simplify your investigations with alarms and reports that are automatically associated with the correct PCI DSS asset categories.

NIST: The National Institute of Standards and Technology (NIST) establishes standards and guidelines for data security and critical infrastructure. The collection, management, and analysis of log data is integral to meeting many NIST-CSF requirements. Implementing a SIEM can satisfy many of these requirements, as well as decrease the cost of complying with others.

Additionally, a properly managed SIEM can play an important role in your organization's ability to address a variety of other compliance frameworks:

+ SOX
+ FISMA
+ GPG 13
+ ISO 27001
+ NERC CIP
+ GLBA
+ 201 CMR 17.00
+ DoDi 8500.2
+ NRC RG 5.71
+ NEI 08-09 Rev 6

For more information on SIEM, contact us at 1-800-825-3301 x 2
or visit https://www.controlscan.com/log-monitoring/.

About ControlScan

ControlScan is the Managed Security Service Provider with a difference: We take a proactive approach to protecting businesses from cyber threats while helping ensure their compliance with security and privacy standards like PCI DSS and HIPAA/HITECH. Our unified security and compliance services deliver confidence to millions of businesses as well as the IT professionals who serve them. Merchant service providers and web hosting companies also partner with us to reduce cybercrime-related business risk. Based in Atlanta, ControlScan is venture backed and supported by a worldwide base of customers, partners and strategic alliances.