Insight

SIEM: A Key Component in Network Security

When an organization encounters a network security threat, the first response is usually to consult the logs in an effort to review as much information about the threat as possible. The problem is that a single log — independent of other security protocols and components of your network — lacks context.

Think about your existing security architecture and how many false positives you need to mitigate in a given week. Yes, intrusion detection can alert you to an attack, but hits in those logs could be any number of other non-malicious malfunctions. The same can be true for endpoint security, service logs, asset management or any other protocols you may have in place.

For the modern security analyst, there is a lot of information to comb through — in good times and bad. This can be a very complicated process. Add that to the fact that network threats often do not look like threats initially. If they did, it would be a lot easier to protect against them. That is why having all of your security apparatuses working together is key in network security.

And that is what SIEM provides.

What is SIEM?

SIEM is Security Information and Event Management. It brings together the existing concepts of Security Information Management (SIM) and Security Event Management (SEM). Information alone is only useful after an event and, if you are having an event, information can be used to inform decisions. SIEM is the marriage of the two, with some other capabilities:

- **Log management** for all of the data collected by your hardware, such as servers, databases, applications and security products
- **Alerting** for immediate issues
- **Dashboards** displaying all this data in a more palatable and actionable format
- Gathering of **compliance data** automatically
- **Retaining** data for long-term compliance and analysis
- **Searching** across logs based on granular criteria for forensic analysis and historical precedents

What are the benefits of SIEM?

The benefits of a SIEM system can perhaps best be discussed in relation to time: before, during and after a security event occurs.

SIEM systems can detect and alert for incidents that would have otherwise not been detected by siloed logs. The system can see the big picture and correlate events that perhaps would not have been seen as symptoms of a threat until it's too late. Over time, as this correlation occurs, more threats can be identified and isolated before they cause damage.

If an event is occurring, the SIEM system provides a centralized resource for all of your log data. Whatever incident protocols you enact are expedited because you and your staff do not have to chase down information from dozens of sources to isolate the threat. The machines that were attacked can be identified, and the threat can be mitigated without further damage.

Finally, many organizations have found the true benefit in SIEM to be its data handling capabilities, particularly those enterprises that need to follow compliance reporting mandates. Reports can easily be sourced or collected over a specified period. Log data is constantly archived in a centralized location. Common compliance reports can be automatically generated and distributed with little to no in-person management.

How does SIEM work?

To start, a SIEM system centralizes the storage of all the logs being collected on your network. All of the logs created by your network infrastructure, user machines, servers and software are gathered and stored in a centralized database. Specialized agents amass this collection, usually in a hierarchical manner based on the importance of the piece in question. That is how the database is organized.

A console, usually displayed as a dashboard, then inspects this data on a constant basis. When anomalies are found, they are flagged until a correlation can be made. The administrator can set rules in the system for alerts, or a statistical engine can be employed that provides more automation for the process.

As this goes on, all of the data is stored and organized based on the specifications of the user. This might be for compliance or simply to keep a record of previous events.

What is a sample SIEM scenario?

1. One of your employees unknowingly downloads some malware from a website.
2. The malware tries to propagate around your network, but is caught by your antivirus system.

How many separate logs are involved in that very common occurrence? There's your firewall, proxy server, outward-facing router, any logs that could be found on the employee's machine, any logs on the machines that the malware tried to infect on your system, various network infrastructure devices and your antivirus system. It would take forever to go through them all. You wouldn't even know of the threat before users encountered issues. But SIEM would see that chain of events, nearly instantaneously and alert you.

What is the optimal method of containing the threat in this scenario? You don't have to shut down anything that affects the whole network. Only the original employee's computer is infected. Instead, all you need to do is clean out that employee's computer and make sure the website from which he downloaded the malware is no longer accessible by anyone on your network. Because this is a common occurrence, your SIEM system can automatically implement those steps if you so choose.

Why is correlation important?

Think of your network as a city with you as its mayor. From personal experience, you might know everything there is to know about your neighborhood, but not much about the surrounding area. You rely on many sources for information about the other neighborhoods, including the news, your various other departments and word of mouth. Only with those other sources can you be an effective mayor. Think of SIEM as the executive assistant that organizes all of that information and has it ready for you when you arrive in the morning.

The primary capability SIEM provides is correlation. Logs, although necessary and valuable, are also disparate entries that only apply to their specific area in your network. In the modern network, those areas are interconnected now. Being able to match up data from various sources allows you to both study security events after the fact and set up alerts for events as they are happening.

Even in a smaller organization, there is simply too much information generated by logs for one person — or even a team of people — to comb through. But because your "executive assistant," the SIEM system, has already found the highlights for you by collecting all of the data and isolating the interesting parts, your job of finding and mitigating threats is greatly reduced.

The process can be as automated as you choose. Say the system notices that certain data entries on logs, when they occur in concert, signify a threat. It can tell you about that correlation, and then you can set an alert for every time that scenario occurs. Otherwise, it just keeps storing the data in its incredibly large database until a new trend comes along.

SIEM: What network security should be.

How Insight helps

From business and government organizations to healthcare and educational institutions, Insight empowers clients with Intelligent Technology Solutions™ to realize their goals. We provide the guidance and expertise needed to select, implement and manage complex technology solutions to drive business outcomes. Through our world-class people, partnerships, services and delivery solutions, we help businesses run smarter.

Learn more about how Insight's custom solutions and services meet your security needs and keep your critical assets protected.