Introducing the SIEM:

A Proactive Security and Compliance Tool

As cyber security becomes more and more critical, organizations are increasingly looking at what's going on in their network. But how do you go about doing that?

When tools like firewalls, servers and mobile devices aren't able to "talk" to each other, it poses a challenge. Although a firewall may succeed in stopping traffic from getting through, it cannot tell the switch or computer that something is suspicious. In order to change this, a Security Information and Event Management (SIEM) system needs to be introduced properly.

Here's a primer on where SIEMs fit into the security landscape, including the four most common uses today.

Where Does a SIEM Fit In?

When talking about SIEMs, the simplest analogy comes from Robert De Niro's character in the film Casino. A SIEM is the "eye in the sky that watches us all." It tracks and records people as they come in through a door, sit down at the slots, go up to the hotel, move over to roulette, play blackjack and eat a meal before cashing out and going home.

While every organization has infrastructure, a SIEM can keep records (called logs) of what these same tools generate, and show how they are interacting with each other in real time. This allows you to investigate events, either as they happen or after the fact should you miss them. As more organizations take a proactive step toward improving their overall security posture, leveraging SIEMs will become even more important.

4 Top Use Cases for SIEMs to Improve Cyber Security

SIEM Use Case ①

Security

Security is one of the top reasons why companies choose to deploy a SIEM. Whether it's preventing an event from happening or figuring out how a breach took place, a SIEM is a critical tool, tracking events you might not see otherwise.

Proactive cyber security is about finding that malicious needle in your virtual haystack. As activity hits your network, individual interactions might be suspicious without rising to the level of flagging an alert. In a lot of cases, IT tools aren't designed for the purpose of investigating events in the first place. A SIEM, though, can look at the pattern of behavior across multiple devices and systems, and flag suspect events for your analysts to investigate further.

SIEM Use Case ②

Breach Investigation

A SIEM's abilities in the event of a breach are even more powerful. At your hypothetical hotel and casino, should George Clooney's Danny Ocean decide to pay you a visit — bringing 10 to 12 of his closest friends — you'll want to have the ability to figure out what those thieves took when they're gone. A SIEM can help answer questions like which pieces of code were malicious, how long they were on your machines, which hosts were impacted and where the code originated.

Interviewing security guards, pit bosses and other patrons is important. But it's far more useful to look at videos and see every interaction Danny Ocean had throughout his stay. After all, wouldn't you want a record of who he spoke with — both inside and outside of your hotel and casino?

SIEM Use Case ③

Compliance Management

A less sensational but equally useful purpose of a SIEM is managing compliance. A SIEM can take advantage of its ability to centralize logs in order to generate reports that demonstrate compliance. Depending on the product you use, some SIEMs come with built-in compliance tools for common certifications, like PIPEDA, SOC-2, PCI DSS or ISO 27001. This helps organizations demonstrate compliance more easily to auditors, saving you significant remediation work after the auditors leave and accelerating the attestation process.

SIEM Use Case ④

Reporting

The last common use of SIEMs is operationalizing security. SIEMs are designed with strong reporting tools that can be very specific and targeted, such as a list of servers that haven't been patched or a list of users that have an unusual number of failed logins. They can also be targeted at a higher level in order to look at areas relevant to business leaders.

In terms of what can be presented to you, the sky truly is the limit. This means that whatever the key performance indicators are, security and executive teams can be measured and reported on according to the schedule that best meets your needs.

Challenges

As with every other piece of technology, SIEMs also come with challenges, the biggest of which include the following.

Cost

Like any software application, there are licensing and maintenance costs associated with SIEMs. There are a couple of different models based on the specific application, but they all come down to how much you want to monitor. Simply put, the more your casino needs to be watched over, the more cameras you'll require and, the higher the cost. Also, because SIEMs are actively looking at your network, the requirement for hardware is on the higher side.

Scarce Expertise

Even though the deployment of SIEMs is more and more common, the expertise to configure them is still somewhat niche. This is part of a broader problem with IT Security: the massive shortage of trained experts. By 2030, the worldwide shortage of security experts is expected to be 3 million, with 500,000 in North America. A large number of IT teams, particularly in the small and medium business space, must make due with no cyber-threat experts on staff at all.

This impacts organizations aiming to deploy a SIEM on two fronts. First, setting up a system like this is based on how well you can tune it. IT environments tend to become "noisy" and it's a SIEM's job to follow events through that noise. You don't want the system flagging everything and generating excessive false positives, but under-tuning it creates the same problem because nothing is flagged at all.

In your casino, you want to make sure that your camera system is only catching people who are doing things that they shouldn't be doing, like counting cards or signaling. Over- or under-tuning the system will lead to trust problems.

24/7 Operation

SIEMs are not set-it-and-forget-it technology. IT environments are dynamic, and as you make changes, you'll want someone to ensure the SIEM is properly configured and up to date. More importantly, as the SIEM finds events, someone has to investigate what the system is flagging. After all, a camera system isn't all that useful if no one is paying close attention to the monitors.

Malicious actors don't sleep, which means systems like this need monitoring 24 hours a day, seven days a week. The minimum number of people needed to operate around the clock is six. You'll also want a senior security professional, typically with a designation like CISSP, to act on more serious events and decide what needs to be flagged for management.

One Solution to These Problems

So how do you enjoy the benefits of having a SIEM while addressing the challenges? One way is to hire a Managed Security Services Provider (MSSP). Usually companies that offer proactive management use a SIEM as one of the cornerstone pieces for their Security Operations Center (SOC). In almost every case for a small or medium business, the cost is significantly cheaper. Some estimates are as low as 10 percent of the cost of doing it yourself — with the same technology and people — on an ongoing basis.

Leveraging an MSSP allows your security and IT teams to instead focus on ensuring that your company's IT is working to meet your organization's objectives.

Final Thoughts

The SIEM market is expected to grow 12 percent a year going forward, outpacing the broader security market as companies look to take a more proactive approach to security and better manage their compliance. Despite the large number of breaches being reported and the changes in regulations being brought in by government — a story for another day — there's good reason to be optimistic about the cyber security future. Ultimately, having the right cyber security posture is critical to organizations. It helps foster trust, as IT is depended on more and more as part of your ongoing digital transformation.

To learn more about how SIEMs can improve your security landscape, visit simnet.ca or contact Simnet at 866-982-2854.

simnet.ca