CYBER SECURITY SUMMIT
Security solutions through collaboration™

www.cybersecuritysummit.org

Webinar Series — June 2021
Rapporteur Report

What is a SIEM and Why Do You Need One?

Cyber Security Summit Webinar Series
June 29, 2021

Speaker: Mary Frantz Chief Information Security Officer, Prescryptive Health, Inc; Founder, Enterprise Knowledge Partners, LLC

Moderator: Sean Costigan, Professor George C. Marshall European Center for Security Studies

Rapporteur: Simon Bracey-Lane, Ph.D. Candidate, University of Canberra

What is a Security Information and Event Management system?

A SIEM offers real-time monitoring and analysis of events, as well as tracking and logging of data from across an IT system.

SIEM was a term established in 2005. But the concept of using log management, packet capture, NetFlow, sys/event logs to track and manage everything from system latency to code bugging has been around for a long time. As these disparate systems grew, individual monitoring became increasingly cumbersome. SIEM systems have emerged as a tool able to effectively streamline the monitoring and archiving of logs. This capability has ensured that a correctly configured SIEM system that detects abnormal and suspicious attacker activity.

Ineffective logging, monitoring, and the inability to correlate event logs across a system lead to successful cyber attacks. The end goal of a SIEMs is complete visibility over the organizations' systems to detect threats investigate anomalies and alert.

Garbage in, garbage out.

SIEM is a reactive defense tool that alerts and informs. It must be configured to ensure it is collecting analyzing and flagging the right information. Incorrect data will waste time, resources and pose a security risk. To work best, a SIEMs must be correctly configured to gain as clear a picture of system normality as possible. If not, it won't be able to alert of potentially harmful activity, because it doesn't know it is happening. It cannot, for example, detect a zero-day if it hasn't developed a baseline around your environment to identify anomalies. Most modern, large-scale SIEMs use AI, but these systems only become automated when you automate them.

SIEM is one part of a security infrastructure. It is detective, not preventative. It is a reactive defensive tool that informs and alerts. It can't make you respond to an alert. A SIEMs is not natively secure. It must be adequately protected. Its role in collecting sensitive log data, and capacity to ensure an attacker remains undetected makes it is a valuable target within a compromised IT system. It's important to monitor access to the SIEM and protect access to log sources against non-repudiation and other factors.

One universal bad idea occasionally deployed by organizations is the implementation of multiple separate SIEMs in each department or division. What ends up happening is that these systems individual generate a lot of noise. Warnings are missed and things slip through the cracks. In three high-profile incidents where this form of SIEMs had been used, the attackers were really loud, but everyone missed it. Using many SIEMs can help threat actors get away with things because they have multiple areas to obfuscate their work that show up differently. Using one consolidated SIEMs avoids this issue.

What can a SIEM do: a tool, not a process.

Compliance, Log Archival, and Storage:

Provided you have parsed and created adequate rules, organizations can manage who has access to sensitive information. A SIEM can help an organization ensure adherence to compliance and data protection regulations through the acquisition and archiving of logs. It also helps by enabling you to closely supervise privilege access management, ensuring you can demonstrate that access to sensitive information is adequately monitored. Which is useful for satisfying many compliance regulations.

Correlation Analysis:

Different pieces of an IT ecosystem can be monitored from a central location. This is vital when you are trying to analyze activity. Without a SIEM you will have to dive into each area to get that information. A SIEM brings those pieces together.

Threat Intelligence:

Modern SIEMs pass that correlated information through a malware detection platform called the MISP. This a free, open-source threat intelligence platform for sharing, storing, and correlating Indicators of Compromise of targeted attacks. This threat intelligence service means you are alerted when certain things match certain patterns.

Behavior patterns:

A well-configured SIEM will learn your normal behavior. If a System Administrator has never logged in from Germany and all of a sudden does, even with the right credentials and passesMFA, your SIEM is going to know this is an anomaly and flag it because it's learned your normal behavior patterns.

Configuration Change Management:

You can ensure a SIEM alerts you if a rule change is made, or new software is deployed. As a SIEM is just one element of your security infrastructure, you can then check that alert against your change management rules to identify whether that was supposed to happen.

Incident Response:

A SIEM allows you to perform incident response much easier. As the logs are consolidated in one place and if you have the SIEM, not on a centralized system that may have been compromised you have a seeing eyeglass into your systems. You can see the threat actor's activities, you can trace their IOCs because the SIEM is passive. They're scraping the logs and putting agents on your system and gathering your logs in a holding pattern, but not interacting with your core systems. You can trace, search without leaving a footprint in your system. Performing threat hunting without triggering the threat actor and causing them to go into hiding.

Reducing False Positives/Negatives:
If you configure your SIEM to learn, you can determine false positives. That behavior pattern you're establishing in the SIEM will also help you avoid false negatives. False negatives are when something bad is happening, but you're not able to detect it. One of the primary reasons that preventing false negatives is constantly held in our minds when creating rules because they are the most dangerous. If you can eliminate false positives your time for operational stability following an attack is much shorter.

What to look for in a SIEM:

Scalability and Speed:
Logs increase over time, but it is important not to let this slow your processes down. If your SIEM is only grabbing logs, every hour or every 24 hours, if an attacker gets in there, they can do a tremendous amount of damage. You need to look for size capacity you will grow to and multiple that by the amount you want to conduct behavioral analyses with and the speed will need to access that data. Not all systems are going to be equal, you will pay more for scalability, speed, and storage.

Log Ingestion:
There are a lot of tools that will hook into your SIEMs, but it is worth being careful to check that they can positively interact with every element of your ecosystem. You may need to do some manual work to ensure that information is being captured. Not all SIEMS grab raw packets and allow you to analyze NetFlow. Some will retain your logs for 1 year, with a 30 day look back but to retain it for longer, it will cost you in storage per GB, TB, etc. All that adds to cost. You want to look at what the SIEM will ingest and what it will cost you to keep it.

Exit Strategy.
A company deploys a large, in-depth SIEM solution, but it isn't happy and wants to change vendors. When exploring options, they need to know if they get those raw packets, can those raw packets be ingested into a new system you might need an overlap where you pay for two vendors. Can you extract those raw logs and put them on hold in the case of a data breach or litigation? Especially in the way you know you need to. It's important to look at exit strategies and how they might impact your organization.

Frequency of Ingestion:
It is vital to keep in mind the timeliness of alerts and note how long it takes to parse and filter that information so that those logs turn into meaningful alerts. You must undertake a manual Are there any elements of your system that could inhibit the speed at which those logs can be registered as meaningful alerts.

Support and Training:
Are there user groups or slack channels available to learn what others are doing? It can be useful to access any provider-run training to ensure you're able to use the tool effectively and not expend

unnecessary resources constantly writing rules and configuring filters. If you get the best tool and configure it wrong, it can do you a great deal of harm.

The Future:

Many tools have used AI crossed over the threshold into becoming preventative tools. Increased the breadth of what we consider SIEM tools. We see this more in gov and advanced services and part of large companies that are part of critical infrastructure. Most tools will be offering that more broadly in the next four to five years.

Next-generation firewalls are looking for patterns of behavior and behaving reactively. Seeing suspicious traffic the firewall will automatically go and block it. Not waiting for a human to click, block, no/yes or take evasive action. Learning from your previous behaviors of where you think the thresholds are and behaving autonomously. But you can't entirely replace human intuition/brain patterns.