Introduction to SIEM Systems

Reading

45m

Status | Incomplete

Introduction

This reading introduces you to security information and event management (SIEM) systems and how they form an integral part of threat detection engineering. You will learn about the features and capabilities of SIEM technology and how it is used to gather security insights for an organization.

Reading

The intricacy and level of complexity of today's threat landscapes are always growing rapidly and getting more advanced. It's almost impossible for a security team to predict what they will encounter next. The attack surface area is developing as a result of an increase in the number of endpoint devices and an increase in the dependence on cloud-based services. When all of these elements are taken into consideration, it becomes difficult for the SOC members to monitor activities that are occurring throughout a business network.

It is a well-known truth that businesses put in place several security measures, both hardware- and software-based, in order to detect suspicious activity and determine the nature of a security breach. However, because each of these sensors and pieces of software operate independently, their overall effectiveness is limited when it comes to identifying more sophisticated attacks. Attackers, undoubtedly, make use of a wide variety of tools, technologies, and methods in order to plan and carry out their operations and use sophisticated strategies to remain undetected by the security system of an organization. Attackers do not just concentrate their efforts on a single piece of software or system; rather, they conduct spread attacks across a number of platforms, which makes it impossible for the in-place security mechanisms to identify anomalous behavior.

This is where SIEM technology becomes extremely handy as it collects event log data from a range of sources, identifies activities that deviate from the norm, with real-time analysis, and takes appropriate action.

> ⚠ Read the following article to get an in-depth understanding of SIEMs: What is Security Information And Event Management (SIEM)?.

As you read the article, focus on the following:

- How is SIEM defined
- How a SIEM works
- SIEM features and capabilities
- Benefits and limitations of using SIEM
- Examples of SIEM tools

SIM vs. SEM vs. SIEM

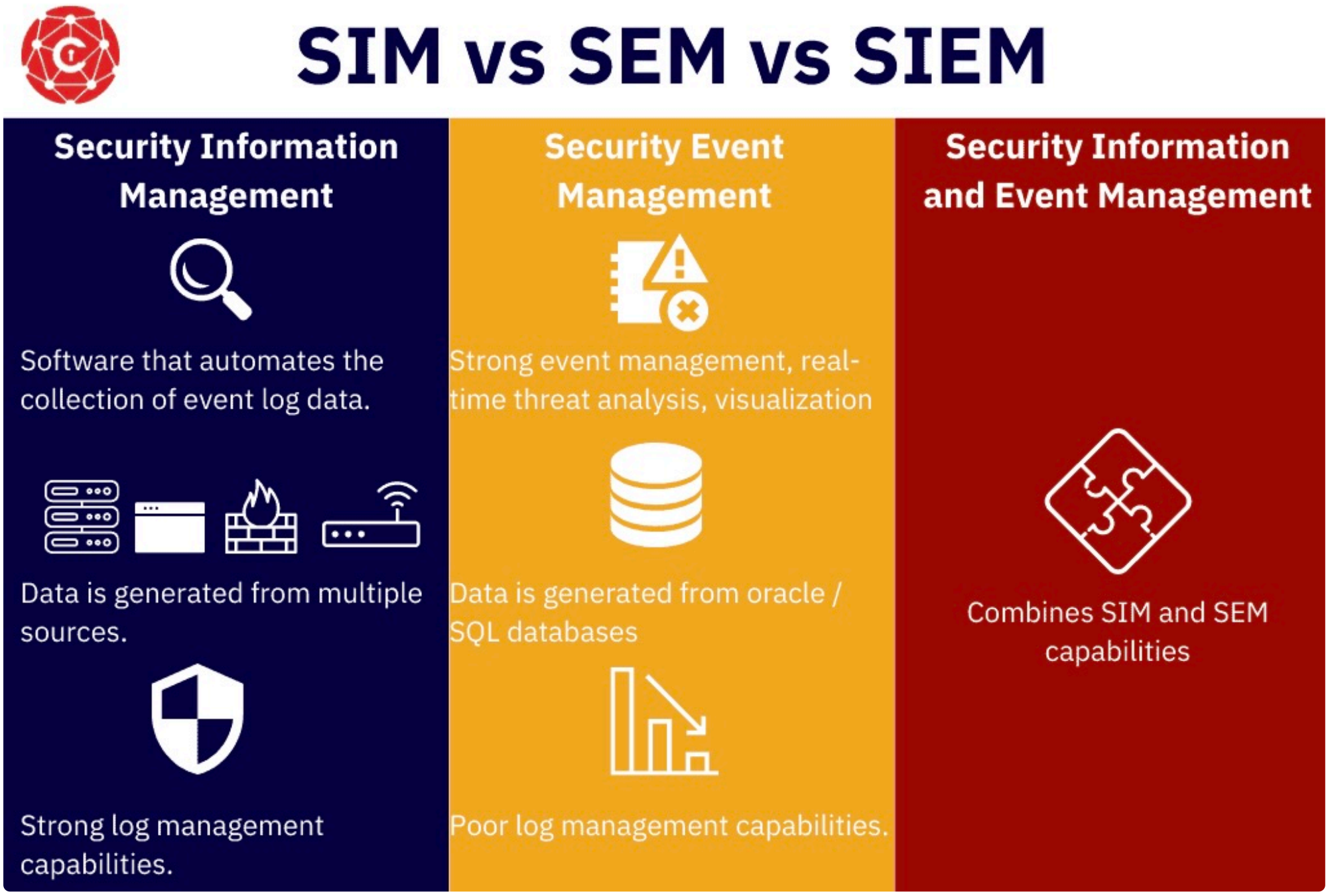

Figure 1: Comparison of SIM, SEM, and SIEM

> Now that you know the fundamentals of SIEM, it's important that you also understand how it compares with security information management (SIM) and security event management (SEM); go through the information given below to learn more.

SIM is an enhanced version of a log collection and management platform. It has strong log management capabilities, such as log retention, analysis, reporting, and correlation with threat intelligence sources. On the other hand, SEM allows Blue Team members to perform advanced operations like event aggregation, correlation, and notification triggering for endpoint and network devices like Firewalls, Linux, and Windows servers, etc. Finally, SIEM allows you to have benefits of both SIM and SEM through a single pane of glass.

> Crowdstrike appropriately defines SIEM in terms of SIM and SEM as given below:

"Security information and event management (SIEM) is a set of tools and services that combine security event management (SEM) and security information management (SIM) capabilities that helps organizations recognize potential security threats and vulnerabilities before business disruptions occur. SIM focuses on collecting and managing logs and other security data while SEM involves real-time analysis and reporting."

Conclusion

Now that you understand the basics of SIEM, it's time to jump to the next reading to learn about SIEM architecture and learn how SIEM systems are built to give security insights about an organization.

Further Reading

You may read the following TechTarget article to deepen your understanding of SIEM features and capabilities: Security Information and Event Management (SIEM).

✓ Mark Completed

Previous
Top Five Hunt Hypothesis

Next
SIEM Architecture & Implementation

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W08D2

Tue Aug 13

W08D2 Schedule »