The future of SIEM tools
Previously, you were introduced to security information and event management (SIEM) tools, along with a few examples of SIEM tools. In this reading, you will learn more about how SIEM tools are used to protect organizational operations. You will also gain insight into how and why SIEM tools are changing to help protect organizations and the people they serve from evolving threat actor tactics and techniques.

Current SIEM solutions

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

The future of SIEM tools

As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments. Cloud-hosted SIEM tools are operated by vendors who are responsible for maintaining and managing the infrastructure required to use the tools. Cloud-hosted tools are simply accessed through the internet and are an ideal solution for organizations that don't want to invest in creating and maintaining their own infrastructure.

Similar to cloud-hosted SIEM tools, cloud-native SIEM tools are also fully maintained and managed by vendors and accessed through the internet. However, cloud-native tools are designed to take full advantage of cloud computing capabilities, such as availability, flexibility, and scalability.

Yet, the evolution of SIEM tools is expected to continue in order to accommodate the changing nature of technology, as well as new threat actor tactics and techniques. For example, consider the current development of interconnected devices with access to the internet, known as the Internet of Things (IoT). The more interconnected devices there are, the larger the cybersecurity attack surface and the amount of data that

threat actors can exploit. The diversity of attacks and data that require special attention is expected to grow significantly. Additionally, as artificial intelligence (AI) and machine learning (ML) technology continues to progress, SIEM capabilities will be enhanced to better identify threat-related terminology, dashboard visualization, and data storage functionality.

The implementation of automation will also help security teams respond faster to possible incidents, performing many actions without waiting for a human response. **Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can't be automated with a SOAR. Nevertheless, the expectation is for cybersecurity-related platforms to communicate and interact with one another. Although the technology allowing interconnected systems and devices to communicate with each other exists, it is still a work in progress.

Key takeaways

SIEM tools play a major role in monitoring an organization's data. As an entry-level security analyst, you might monitor SIEM dashboards as part of your daily tasks. Regularly researching new developments in SIEM technology will help you grow and adapt to the changes in the cybersecurity field. Cloud computing, SIEM-application integration, and automation are only some of the advancements security professionals can expect in the future evolution of SIEM tools.