Improve Cyber Security with SIEM as Part of an Overall Security Solution

Cyber-attacks have become a fact of business life, with hackers often lurking in the network for months without detection. But savvy organizations know to take a proactive approach to information security. Augmenting cyber security with SIEM can mean the difference between catastrophe and business as usual.

By collecting and analyzing log and event data from across the system in real time, SIEM (Security Incident Event Monitoring) allows organizations to detect and mitigate security threats early. Artificial intelligence and machine learning enhance the process, bringing SIEM far beyond mere log management.

In addition to managing threats, SIEM plays a key role in regulatory compliance. And when combined with preventative measures and threat response, it forms a critical component of a comprehensive cyber security strategy.

How SIEM Works

SIEM programs operate by continuously collecting logs from devices and applications throughout an organization's entire network. This includes software applications, servers, cloud environments, firewalls, and other security devices. The program then normalizes the data, organizing it so that event logs from various systems can be examined together.

Next, the system analyzes the collected data, looking for patterns that may signal a breach. SIEM sorts events into categories that can include failed login attempts, malware activity and other potential problems and uses predefined policies to determine next steps. It then alerts security personnel of potential significant events.

For example, predefined policies may trigger an alert when logs indicate a huge number of files sent to an external location. Additionally, these rules will recognize that hundreds of failed login attempts in a few minutes likely indicate a hacker. On the other hand, a half a dozen failed attempts probably mean a user simply forgot their password.

Because modern SIEM programs use automation and machine learning, they can perform these functions very quickly. This means security teams receive early alerts and can respond quickly to potential security incidents, saving valuable time and protecting critical assets.

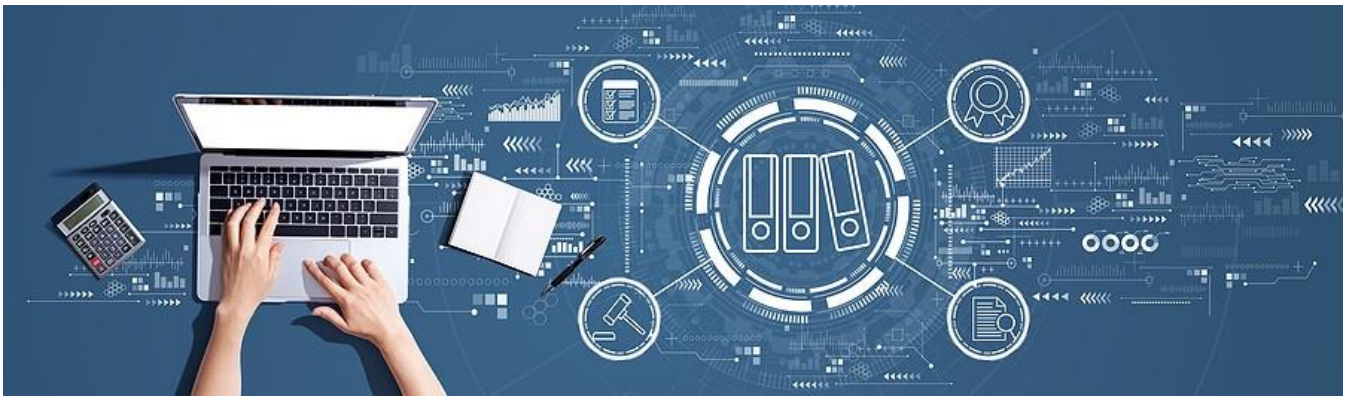
Benefits of Cyber Security with SIEM

While this early warning system represents one of the key benefits of SIEM, other benefits also contribute to a substantial return on investment. For instance, not only do timely alerts improve incident response times, but the SIEM also provides a valuable tool for forensics investigators to re-create and analyze an incident.

Additionally, SIEM plays an important role in demonstrating regulatory compliance. With automated data collection and detailed analysis, SIEM programs produce the reports required to show that the organization has implemented required security controls. These reports also indicate whether security incidents have occurred and the nature of the events.

SIEM Limitations

While SIEM programs deliver significant benefits, they do not deliver a magic bullet to solve all cyber security problems. They may require a substantial investment and can prove complex to implement. Organizations also need the assistance of experts to define correlation rules and configure reports, as misconfigurations can result in missed alerts.



SIEM an Essential Part of Security Strategy

Consequently, organizations should include SIEM as one element in an overall security operations center (SOC). By partnering with a reputable managed services provider (MSP), even mid-size and smaller organizations can access enterprise-class security monitoring.

For instance, with eMazzanti's eCare SOC, organizations gain SIEM as part of comprehensive SOC-as-a-service. The service includes real-time, automated monitoring of the entire network, with 24/7/365 support from human cyber security experts. Monitoring covers both on-premises and cloud environments and supports hundreds of security products.

By partnering with security experts, organizations gain access to cutting edge SIEM technology and industry best practices for threat detection and remediation. Combined with preventative measures and robust data backups, these form the basis of a solid security strategy.