What does a Security Information & Event Management (SIEM) do?

The SIEM is a technology solution that combines security information management (SIM) and security event management (SEM) functionalities to provide comprehensive security monitoring, threat detection, and incident response capability.

It accomplishes this by collecting a log of data and security events. SIEM systems can gather data from sources such as firewalls, intrusion detection/prevention systems, anti-virus software, and authentication systems.

What can a Security Information & Event Management (SIEM) do to benefit your organisation?

Log Collection

The SIEM collects log data from different sources, devices, and applications across the network. These logs contain valuable information about security events.

Event Correlation

The SIEM will analyse the log data to identify any patterns and security risks. Doing this via multiple sources allows the SIEM to provide a more broadened understanding to identify any potential threats.

Real-Time Monitoring

The SIEM systems provide real-time scanning of security risks, this gives the relevant departments the ability to actively observe and track any potential threats. Being able to monitor in real-time means that the SIEM can generate alerts or notifications when patterns or events meet predefined criteria or are highlighted as a match for known attack signatures.

Threat Detection

The SIEM embodies a range of detection capabilities, following things like algorithms, statistics, and using intelligence to identify security risks. It can detect indicators of compromise (IoCs), suspicious activities, and any failed/unauthorised access attempts into the system.

Incident Response

The SIEM responds to incidents promptly by detailing information regarding security events. It will also include features for things like case handling and work flow management.

Compliance Reporting

SIEM solutions will generate reports that aid in compliance audits and reporting obligations.

Why does your organisation need a Security Information & Event Management (SIEM)?

1. 24/7 Monitoring to identify any suspicious patterns and anomalies in the logs. This then provides an alert or triggers an automated response to security events, allowing for a faster and more effective incident response process.
2. Offers powerful analysis and search capabilities to examine logs and security threats in great detail. SIEM tools can aid in identifying the root cause of a security incident, as well as understand the full severity of the issue and gather evidence for further action or legal purposes.
3. It has the capabilities to streamline security operations by automating log collection, analysis, and reporting processes. This saves time and hassle by not having to manually review logs. Instead, security teams can focus their efforts on investigating and responding to any critical events that require full attention within the organisation.
4. Helps organisations to demonstrate adherence to security policies, identify vulnerabilities, and generate compliance reports.
5. Streamlines security operations by automating log collection, analysis, and reporting processes as opposed to having to manually review through the logs, allowing the security teams to focus on investigating and responding to more critical events.
6. Enhances the organisations security stance by providing detailed information on emerging threats, known attack patterns, and indicators of a data breach.