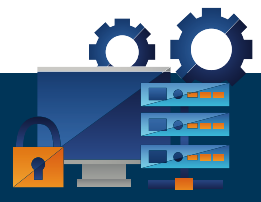
WHY DO I NEED A SECURITY INFORMATION AND EVENT MANAGEMENT?

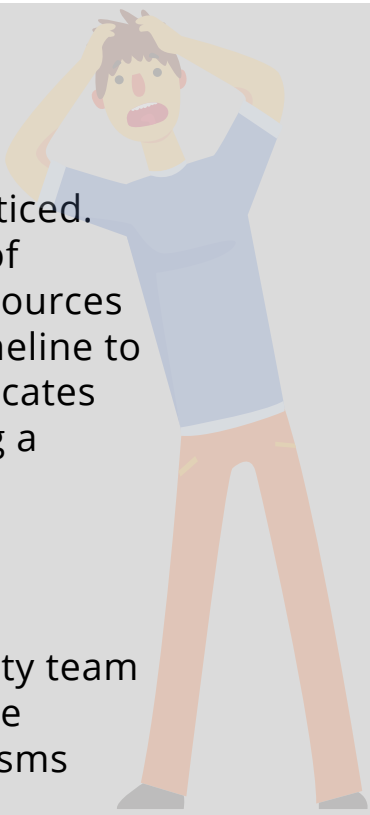
Security Information and Event Management (SIEM) is security platform that gathers log security data from diverse sources, categorizing and analysing security alerts in near-real time. SIEM combines security information management –meaning long term storage, analysis and reports on log data –with security event management, which monitors the system in real-time, correlating events and generating alerts.

SIEM platforms use correlation rules and statistical algorithms to extract actionable information from events and log entries. Key features of a SIEM security solution include:



- Visibility in Near-real Time: Uses visual consoles as dashboards to provide an overall view of the security system.
- Data Consolidation: Manages log events of data streaming from various sources.
- Correlation of Events: Uses Boolean logic rules to add context and intelligence to raw data.
- Automated Security Event Alerts: Analyses indicators of compromise and sends alerts, notifying issues in real time.

THE FOLLOWING ARE THE MAIN REASONS THAT ORGANIZATIONS NEED A SIEM SOLUTION:



Detecting Incidents

A SIEM solution detects incidents that otherwise can go unnoticed. This technology analyses the log entries to detect indicators of malicious activity. Moreover, since it gathers events from all sources across the network, the system can reconstruct the attack timeline to help determine its nature and impact. The platform communicates recommendations to security controls –for example, directing a firewall to block the malicious content.

Incident Management

A SIEM improves incident management by allowing the security team to identify an attack's route across the network, identifying the compromised sources and providing the automated mechanisms to stop the attacks in progress.

Davichi