SIEM

شركة الإلكترونيات المتقدمة
Advanced Electronics Company
AEC

Security Information and Event Management

Security information and event management (SIEM) products combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications, servers and network devices

AEC SIEM has multiple capabilities including gathering, analyzing and presenting information from network and security devices, database and application logs, as well as providing sandboxing capabilities that is used to execute untested or untrusted programs, files, and URLs from unverified or untrusted third sources without exposing harm to the host machine

System Functionalities

Log Management

Collects and stores log files from multiple hosts and systems into a centralized single location instead of accessing them from each system individually

Sandbox

Executes files and URLs, inline or on-demand, in an isolated environment to protect users from zero-day. It examines the behavior of the files and URLs, and reports the result of the analysis

Network Forensics

Provides an after-the-fact investigative capability that other security tools cannot provide. Use cases include capturing malware samples, network exploits and determining if data exfiltration has occurred

Incident Response

Provide the functionality of generating tickets based on security alerts, by the system or customized use cases, in order to enable Incident Response team to investigate alerts and respond to verified breaches

Threat Intelligence

Enables the SIEM to recognize the emerging attack campaigns and new trends. The primary objective of threat Intel in to detect Advanced Persistent Threats (APT) and zero-days attack