

LO#03: Use Network Security Solutions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Incident and Event Management (SIEM)



- SIEM performs **real-time SOC** (Security Operations Center) functions like identifying, monitoring, recording, auditing, and analyzing security incidents
- It provides security by **tracking suspicious end-user behavior** activities within a real-time IT environment
- It provides security management services combining **Security Information Management (SIM)**, and **Security Event Management (SEM)**
 - SIM supports permanent storage, analysis and reporting of log data
 - SEM deals with real-time monitoring, correlation of events, notifications, and console views
- SIEM protects an organization's IT assets from **data breaches** due to internal and external threats

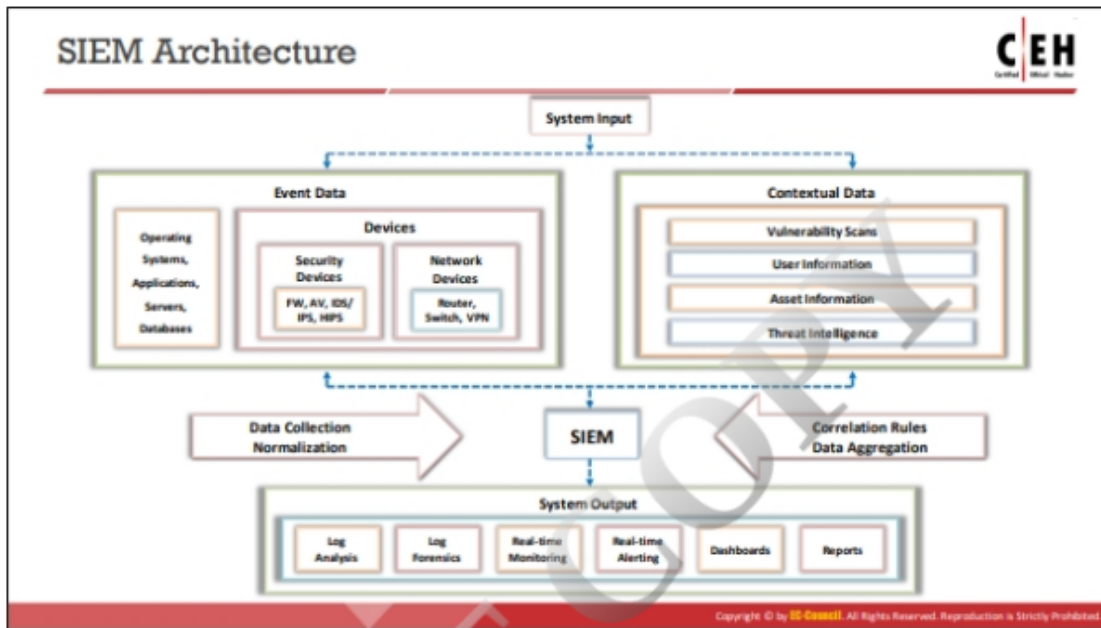
SIEM Functions

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance and Reporting
- Application Log Monitoring
- Object Access Auditing
- Data Aggregation
- Real-time Alerting
- User Activity Monitoring
- Dashboards
- File Integrity Monitoring
- System and Device Log Monitoring
- Log Retention



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____




User Behavior Analytics (UBA)

- UBA is the process of **tracking user behavior** to detect malicious attacks, potential threats, and financial fraud
- It provides **advanced threat detection** in an organization to monitor specific behavioral characteristics of employees
- UBA technologies are designed to **identify variations in traffic patterns** caused by user behaviors which can be either disgruntled employees or malicious attackers

Why User Behavior Analytics is Effective?

- Analyzes different patterns of human behavior and large volumes of user data
- Monitors geolocation for each login attempt
- Detects malicious behavior and reduces risk
- Monitors privileged accounts and gives real time alerts for suspicious behavior
- Provides insights to security teams
- Produces results soon after deployment



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Notes: _____
