Mod 3

Learn

- Logs
- SIEM Dashboards
- Common SIEM Tools

Logs

Intro : A record of events that occur within an organization's system and network

Common log Sources

- Firewall logs
- Network logs
- Server logs

Firewall log: is a record of attempted or established connection for incoming traffic from the internet It also includes outbound request to the internet from within the network

Network log: is a record of all computer and devices that enter and leave the network. It also record connection between devices and services on the network.

Server log: is a record of all events related to services, such as websites, emails or file shares. It include action such as login, password and username request

Security information and event management (SIEM)
An application that collects and analyze log data to monitor critical activities in an organization.

SIEM Dashboard

Metrics: Key technical attributes, such as response time availablity and failure rate which assess the performance of a software applicat

SIEM Tools

Types
- Self hosted
- Cloud hosted
- Hybrid hosted

Splunk Enterprise: A self hosted tool used to retain, analyze and search an organization's log data to provide security information and alerts in real time

Splunk Cloud: A cloud hosted tool used to collect, search and monitor log data

Chronicle: A cloud native tool designed to retain, analyze and search data