What is SIEM try hackme

sec. Info & Event. Management system → bu sayut bi kavram konsept gibi

collects data from various endpoints/network devices across the network, stores them at a centralized place, and performs correlation on them

each network component can have log sources (one or more) generating diff. logs.

Sysmon (System Monitor → windows system service and device driver devd. by Microsoft designed to monitor and log various event happening within a windows sys)

2 logical parts of log sources

① Host-centric log sources → releted to host → user accessing file

② Network-centric log sources → hosts w each other or access internet

Having SIEM sol. It only takes logs from various sources in real-time but also provides the ability to correlate betwn events.

SIEM → ① Collects data from sources → ② Aggregate data (toplamak, birlemek) → ③ Discover and detect threats → ④ Identify breaches and investig. alerts.

Windows → Event Viewer

Linux → var/log/httpd
var/log/...
httpd → response errors HTTP request
cron → releted to cron jobs
auth. log, secure → authent. related logs
kern → kernel related

WEB SERVER

keep an eye on request for any potential web attack

Linux → var/log/apache or var/log/httpd

Log Ingestion

Each SIEM solution has its own way of ingesting (ele almak) logs

common methods used by SIEM solution

① Agent/forwarder → catches imp. logs sent it to SIEM server Splunk

② Syslog → widely used protocol to collect data

③ Manual upload allow user to ingest offline data for quick analysis Splunk ELK

④ Port forwarding

- Why SIEM -

used to provide correlation on the collected data to detect threats once a threat is detected or a certain threshhold is crossed an alert is raised

major SOC component → starts collecting logs and examines

some capabilities of SIEM

- Correlation btwn events from diff log sources
- provide visibility on both centrics.
- allow anlyst to do investigation on latest threats and timely responses
- Hunts for threats that are not detected by the rules in place

Dashboard

Correlation rules & use cases?
↓
5 hatalı password 10dk bekleme
analyst to have action time

d
vardiye
notiona
yazdım

104 → event ID when ~~st~~ OS removed
↓
eventlogs

4688 → process exec activity