What is SIEM — tryhackme

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

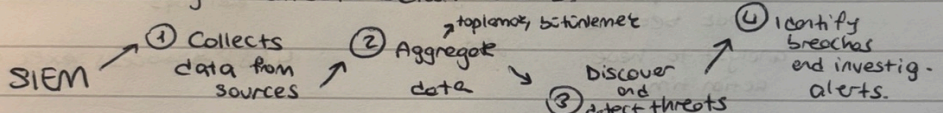
each network component can have log (one or more) sources generating diff. logs.

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

2 logical parts of log sources

1. Host-centric log sources → related to host → user accessing file
2. Network-centric log sources → hosts w each other or access internet

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



Windows → Event Viewer Linux → var/log/httpd

var/log/...

httpd → response errors HTTPrequest

cron → related 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

ele almak

Each SIEM solution has its own way of ingesting 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 & usecases?
↓
5 hatalı password 10dk sedeme analyst to have action time
d
vari diye notiona yetkim

104 → event ID when ~~~~ is removed
↓
eventlogs

4688 → process exec activity