

## What is SIEM try hackme

Sec. Info & Event. Management system → by sayut si kaaron concept giba

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

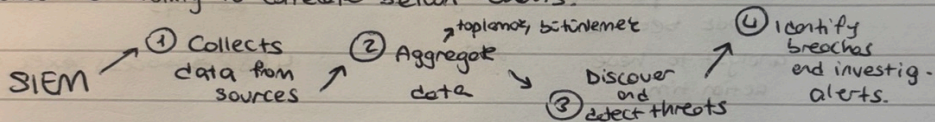
each network component can have log <sup>(one or more)</sup> sources generating diff. logs.

Sysmon (System Monitor → windows system service and device driver dev. 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 → related 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 between events.



Windows → Event Viewer      Linux → `var/log/httpd`  
`var/log/...`

### WEB SERVER

keep an eye on request for any potential web attack

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

`httpd` → response errors HTTP request

`cron` → related to cron jobs

auth. log } auth. related logs  
secure }

kern → kernel related

### Log Ingestion

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  
elephant

### Wing SIEM -

used to provide correlation on the collected data to detect threats  
once a threat is detected or a certain threshold is crossed an alert is raised  
major SOC component → stores collected logs and examines  
some capabilities of SIEM

- Correlation between events from diff log sources
- provide visibility on both contexts
- allow analyst to do investigation on lower threats and timely responses
- Hunts for threats that are not detected by the rules in place

### Dashboard

#### Correlation rules & usecases?

• match patterns and dig  
look between various  
analyst to have  
action time

104 → event 10 rules  
determined  
variables

4688 → process exec activity