SoC Analyst

- SIM stands for security information management
- SEM stands for security event management
- SIM + SIEM stands for security information event management

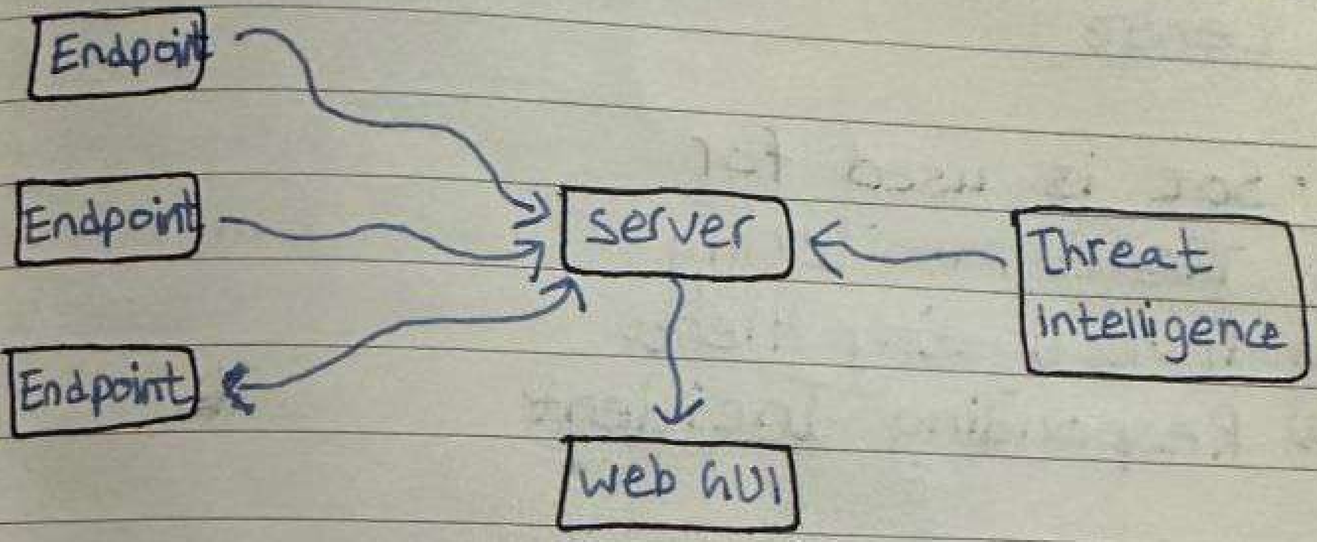
- Siem is used for

1) Log collection
2) Log Aggregation
3) Rule based alert
4) Artifical intelligence
5) Response
6) Parsing
7) Normalization
8) categorization
9) Enrichment
10) Indexing
11) storage

- EDR stands for Endpoint detection and response

EDR collets only single sourcse Logs unlike (siem which collects from multiple sources.

EDR Architecture



- EDR is used for

1) Real-time continious monitering (online/off-Line)
2) Endpoint data collection
3) Signature-less detection
4) Rules based Automated Response (Real-time)

- EDR is collecting

1) Network connections
2) Process execution
3) Registry modification
4) currently running process
5) cross Process Events

- Soc stands for security operation centre

- Soc is used for

1) Threat Monitoring
2) Investigating Alerts
3) Responding Incident

- Technology used in Soc

1) SIEM
2) EDR - End point detection and response
3) TIP - Threat Intelligence Platform
4) SOAR (security orchestration automated res
5) Tickting system - service Now / jira
6) MDR (managed detection and response

- Task of L1 Soc Analyst

1) Alert Triage
2) Ist Line of Defense
3) Identifying anomalies
4) Raising request for whitelists
5) Perfoming Investigation

- Task of L2 soc Analyst

1) Monitoring Alerts
2) Threat Hunting
3) Resource Mentoring
4) creating and approving whitelists
5) Handling Escalated investigations

- Task of L3 soc Analyst

1) client Onboarding
2) Incident Management
3) Report and Documentation
4) stakeholders Communication (Technical)

SOAR

- Security technologies used in soar

1) Ticking
2) DLP
3) SIEM
4) EDR
5) CTI(TIP)
6) Email and web gateways
7) Network security
8) Vulnerablity Management
9) cloud Tools
10) IAM / PAM

- Automation to protect envoirment.

1) Triage
2) Enrichment
3) TI Gathering
4) Validation across detection tools
5) Close False positives
6) Email users
7) Block IOCs
8) Alert Administrators

- NIST Incident response Framework

1) Prepration
2) Detection and Analysis
3) containment, Eradication and Recovery
4) Post Incident Activity

- SANS incident response Framework

1) Prepration
2) Identification
3) containment
4) Eradication
5) Recovery

- Eradication is used for

1) Removing Artifacts
2) Identify ALL Hosts
3) updating configuration
4) Patches
5) Documentation

- Recovery

1) Restoration
2) Normal operations
3) Activities
4) Monitoring
5) Documaentation
6) Prevent reinfection

- Lesson learned

1) Meeting
2) 5W1H
3) way forward
4) Documentation

- Website to practise free blue team Labs

1) cyber defenders
2) Blue team Level 1
3) Let defend

* Cyber defenders

- For Network security we can use

1) webstrike
2) HawkEye
3 Nuke Browser

- For Malware Analysis

1) GetPDF
2) MalDoc101
3) obfuscated

* Blue team cyber range

- For Network Analysis

1) webshell
2) Ransomware
3) Malware compromise

- For End point

1) sysmon
2) Brute Force
3) compromised wordpress

- For Malware

1) Ransomware script
2) Melissa
3) ILoveYou

- For Phishing Analysis

1) Phishing Analysis 1 and 2

* Lets Defend

- For Malware

1) Powershell script
2) Pdf Analysis

- For Phishing

1) Phishing Email
2) Email Analysis

- For Endpoint

1) Investigate Web Attack
2) conti Ransomware

- For Network

1) Port scan Activity
2) Infection with cobalt strike