15th Dec '24

Mastering SOC – Week 3

SIEM – Security Information Event Management

Event: Real-time monitoring and alerts

"A SIEM centrally collects, normalises, and analyses log and event data from various sources in real-time and historically, to identify and alert on security incidents, facilitate compliance reporting, and aid in organisational troubleshooting."

Purpose:

1. Visibility - Collects and aggregates data across disparate environments to provide unified visibility
2. Threat Detection - Identify potential threats in live data to be investigated and responded to
3. Security Control Centre - Facilitate investigations, security decisions and response plans to keep businesses secure and compliant

Data ingestion – Ingestion of Data from different environments like endpoint, server, applications, etc.

- SIEM Data steps – Collect -> Normalise -> Analyse -> Investigate -> Store
- *{Collect -> Normalise} stage:*
- Collection -> Transport -> Format -> Parsing -> Normalisation
- Best metaphor is books collection from depot at Library. -> Arranging them and placing across appropriate sections of library.

Understanding **False Positives** – is not about reducing noise, it's about tuning into right signals

Incident/Alert Prioritisation –

- Each alert and incident has its own impact and urgency, that's why it's important to have strategic, informed decision-making rather than responding to every alert.
- So, you can assess the type of threats that comes in, the assets that could be under danger(could be compromised), any compliance requirements, and also have to be understanding company's broader operations to determine then if the alert then needs to become an incident.
- *Key strategies*: Assessment with precision, dynamic prioritisation, resource stewardship, client-specific communication, feedback loops for Strategy Refinement
- Why Prioritisation so important?
    - ↪ Securing and working according to MSSP, data sensitivity, operational framework, compliance requirements, etc. All this is done with the help of as many evidences that can be collected to effectively prioritise the actions, better decisions.
- Resource allocation – delicacy should be there! Senior analysts do that

- Any feedback from the alerts is to be discussed by other analysts.

Incident/Alert Prioritisation Criteria

- Analogous to hospital triage system
    - Who – helps identify the affected systems, departments or parties.
    - What – helps determine the type of incident, just like the kind of road block in the traffic management system.
    - Where – pin points the location of incident, within networks, cloud services or specific devices
    - When – establishes the timeline of the alert/incident. Using priority calculators to score incident severity, these tools consider factors like data sensitivity, scale, potential harm, and legal implications! This tool serves as a guide not a proper path.
- Learning form past tickets and mistakes.
- Incorporating customer preferences and feedback! Tailoring and prioritising, operational continuity, data privacy, data compliances, etc.

APT (Advanced Persistent Threats)

- Characterised by their stealthy, persistence, and sophisticated techniques. Mostly found under the topic “State Sponsored attacks”, to stay undetected.
- Cyber Kill Chain(very important to detect APTs at each stage) – Designed to protect companies from APTs.
    - Reconnaissance – Weaponisation/tools - Exploit – installation – command and control
- Detecting APT requires multi-layered security approach, described as Defence-in-depth. Eg. Using multiple advanced monitoring tools like Firewall, Network Intrusion Detection System, Anomaly detection, performing regular Network Audits, Vulnerability Assessments, etc. (Large companies are able to afford these multiple Defence-in-Depth techniques).
- Recognising subtle signs of a possible APT:
    - Unusual network traffic
    - Unexpected data flow
    - Unusual behaviour with a specific user
- Crowdstrike’s threat landscape page on the website shows, state sponsored groups locations and motive. (important in understanding real-time threats)
- APTs target large industries in general.
- Mitigating APTs:
    - Hold regular meetings and discussions with security researchers and industry experts from different companies and organisations
    - Using ML analyse vast amounts of data and predict the threat.

APT Attack Vectors: IoT Devices, Cloud Computing, PsyOps (Psychological Operations)

Characteristics of APTs

- Stealthy - Remain hidden for a prolonged period of time infiltrating the network, system, and services before the actual attack. Eg. Malware infiltrating the computer network, Stuxnet attack on Iran's nuclear facility, Target Data Breach, Solar Winds hack, Anthem Data Breach, DHC hack.
- Mitigation measures are similar to those explained in the prior segment. Multi-layered defence mechanisms, updating software and system regularly, educating staff about potential threats.

Web Application Attacks

Topics studied: Different attacks, and attack vectors

WebApp attacks – Prevalent threat in digital landscape that exploit vulnerabilities in web applications. Main purpose we learn about these different attacks is to protect the web applications and data of MSSP clients effectively.

OWASP Top 10 – valuable resource to understand and address one of the most critical risks facing to web applications.

HOME PROJECT

Nessus

Installed Nessus on Linux

Steps:

1. Register
2. Nessus Essentials
3. Get the activation code
4. Login
5. Click "New Scan" button on the top right corner to start the Vulnerability scan
6. Bunch of scans for Host Discovery, Vulnerabilities, and Compliance will be shown
7. Test different scans, starting with Host Discovery -> Click on it -> Add your network IP (find your
8. IP using ipconfig or ifconfig depending on what OS you're using Windows or Linux) -> Save the scan -> Click on "Launch"
9. After the scan is complete -> click on "Vulnerabilities" -> Can explore the details of vulnerabilities if any -> can easily look at the vulnerability scan results
10. The results were displayed based on vulnerabilities found, categorized by severity (e.g., Critical, High, Medium, Low).
11. On clicking on the vulnerabilities, details would come up, including affected services, description, CVSS score, and recommended remediation steps.
12. Experimenting with different scans, find vulnerabilities and provide solutions to those vulnerabilities was key part of learning in this project.

Nessus tool is essential in terms of automation, vulnerabilities, scans, reporting, etc.