MANDATORY THEORY

QUESTION 1

QUESTION `1A

: Can you walk me through the steps you would take in responding to a security incident in a corporate environment?

ANSWER

The following are the required steps to take when responding to an incident in a corporate environment:

1. **Preparation :** various methods are put in place to prevent incidents from happening in the first place and they include; Incident Response Plan Development. This plan is essential in preparing for an incident as it shows incident response teams a blueprint of procedures and necessary roles to take when responding to various security incidents. Next up is to train the team, when you make certain that all relevant teams in the corporate environment are well trained and educated on their specific roles, incident response process will be in compliance. Lastly, ensure that all communication protocols between the employees and external partners are validated to promote smooth running and active response to any security incidence.

2. **Detection and Analysis** : This step simply involves identification by monitoring system logs and systems for unusual or malicious activity or potential threats. The incident response teams use necessary resources and tools needed to detect and analyze the threat scale and nature

. 3. **Containment** : Once an incident has been detected, it is crucial to stop it from affecting other systems. The threat is hereby contained and ceased from spreading, which can be implemented via either short-term or long term containment. Short-term containment involves enacting immediate measures to limit the spread of the incident while long-term containment involves deploying tactics to keep the incident contained while you work on eradication.

4. **Eradication** : Eradication simply means eliminating/removing threat. When a threat has been detected and contained, it is necessary to exterminate all traces of such threat, for instance, a virus from the system so it doesn't complicate other systems on the network

. 5. **Recovery** : After threat detection, containment, and eradication comes the recovery process. This involves bringing all impacted systems back online for system restoration in order to shun further issues. In the recovery process, it is important to validate proper system functioning by implementing necessary updates for accurate and secure running

. 6. **Post-Incident Activity** : Next step after recovery is the post-incident activity which involves the following;

Report/ Documentation : It is necessary to document all aspects and actions taken during the incident and further present comprehensive reports to relevant stakeholders and regulatory bodies if necessary.

Lessons Learned : Evaluate and dissect the incident for review, in order to understand what happened and how it was handled. Then your processes by updating your incident response plan and security measures taken based on the lessons learned.

QUESTION B

Follow-Up: What are the key stages of the incident response lifecycle, and how do you ensure that each stage is handled effectively

ANSWER

The key stages of incident response lifecycle are:

--Preparation

--Detection and Analysis

--Containment, Eradication, and Recovery

--Post-Incident Activity

To ensure each stages are handled effectively, it is important to :

--Develop an incident response plan

--Conduct regular training and awareness programs for the incident response team

--Deploy necessary tools for threat analysis and detection

--Monitor systems regularly using SIEM tools for anomalies detection

--Establish containment strategies and coordinate actions

--Identify the root cause and perform thorough analysis

--Restore systems and ensure proper communication with employees and stake holders

--Conduct post-incident review and make necessary policy updates to enhance future incident response efforts

QUESTION 2

QUESTION 2A

How would you configure and optimize a SIEM tool to ensure it effectively detects and alerts on security incidents

ANSWER

`-The first stage is to identify the features the SIEM should address which includes malware detection, unauthorized access attempts, data exfiltration, insider threat and compliance with regulating bodies`

`Ensure the SIEM collect logs from all relevant sources such as endpoint,network devices,servers, cloud services and applications`

`Use machine learning and behavioural analytics to detect anomalies that may not be caught by static rules`

`Assign severity levels to alerts based on potential impact and where possible integrate with SOAR (security orchestration automation and response), to respond to alerts such as isolation of a compromised endpoint.`

`Continuous monitoring and tuning is important while optimizing a SIEM tool to ensure it detects and alerts on security incidents`

QUESTION 2B

What are the key metrics and alerts you would configure in a SIEM, and how do you minimize false positives while ensuring coverage of real threats?

ANSWER

The key metrics and alerts that should be configured in a SIEM include:

Traffic(outgoing and ingoing) of the network and Anomalies

- **Metric**: Volume and patterns of network traffic, detection of known malicious traffic, unusual data exfiltration.
- **Purpose**: distribution denial of service.

- **Configuration**: baselines should be configured for normal network traffic and set up alerts for deviations such as large outbound data transfers or traffic to/from suspicious IP addresses.

Endpoint and Malware Activity

- **Metric**: Detection of malware, file integrity monitoring repudiation
- **Purpose**: Detect malware infections, unauthorized changes to files which affect integrity and potential compromises.
- **Configuration**: Integrate endpoint protection logs and set alerts for known malware signatures, unusual process executions, or file modifications on critical systems.

Privileged Account Monitoring

- **Metric**: Use of administrative privileges, changes to critical configurations, access to sensitive areas.
- **Purpose**: Detect misuse or compromise of privileged accounts , principle of least privilege
- **Configuration**: Monitor actions taken by privileged accounts and set alerts for unusual activities, such as privilege escalation or changes to security settings.

KEY ALERTS TO CONFIGURE

`Alerts that need to be configured include malware detection, brute force detection``,suspicious network activity ,data exfiltration and privilege account activity`

`HOW TO MINIMIZE FALSE POSITIVES WHILE ENSURING COVERAGE OF REAL THREATS`

`The first step is to have a baseline which will state what a normal activity in your enviroment is\`

`The second step is to gather events related events into a single alert to reduce false positives`

`The use of suppresion rules which will help to  suppress known benign alerts or group related alerts to avoid overwhelming the SOC (Security Operations Center) with noise.`

`Regular review of SIEM and tuning by conducting periodic reviews of false positives, adjusted thresholds, and updating  rule sets to improve` accuracy.

QUESTION 3

QUESTION 3A

What is threat hunting, and how would you approach a proactive threat hunting exercise in an enterprise network?

ANSWER

Threat hunting is a proactive practice where cyber security analyst search for hidden threats , malicious activities within an organization that is yet to be detected.

I will approach a proactive hunting exercise by

`Stating my objectives-this simply means knowing what i want to achieve from the threat hunt.`

`Gathering of intelligence which include collecting and reviewing threat intelligence, recent vulnerabilities, emerging attack techniquew  which are relevant`

`Understanding the network environment is important because i will make sure i am familiar with the architecture of the network, normal user behaviour as well as similar network patterns`

`I will formulate an hypthesis from the intelligence gathered.I will determine the data source which will be relevant to testing my hypothesis which includes network traffic data and log files`

`I will gather data from accross the enterpise which focus majoritily on my hypothesis which may include firewall AND proxy logs ,endpoint devices data`

`I will perform baseline analysis so as to know the normal behaviour of the network by analyzing hisotiral data. This baseline will help identify anomalies that might indicate a threat. I will also use my hypothesis to search for unusual or suspicious activities.`

`I will then investigate the anomalies detected and confirm if the anomalies are threat or benign(not harmful) anomalies.`

`After completing all of this,i will document my findings showing every step of how i carried out this and its impact on the organization.`

`If a threat is confirmed, i will seek the incident response team(IRT) to contain and eradicate the threat.`

`After seeking the help of the IRT, i wil conduct a review so as to understand how it was able to by pass the existing defense and seek for improvement`

QUESTION 3B

: Can you explain a scenario where threat hunting helped uncover an undetected threat? What tools and techniques did you use?

ANSWER

Earlier this year 2024,i worked for **TITI and SAM Company**(a financial institution) and we noticed an unusual traffic patterns of outbound traffic to an IP address in India

PROCESS

-My aim is to uncover an undetected threat

-my hypothesis is: an attacker has compromised one of the company system and has a backdoor to the system which is being used to exfiltrate data.

-I collected data from firewall and proxy logs so i could analyze the outbound traffic. I also collected endpoint devices, DNS and SIEM logs

-With the logs I collected, I was able to create a baseline for the normal outbound traffic and identify anomalies. I noticed that the laptop in the guest room is making steady connections to an IP address located in brazil where the financial institution has no business or customer.

-My Boss **Mr. Samuel** gave me access to use the EDR(endpoint detection and response) logs in which I noticed that the endpoint had an unusual file **AWOBODU.EXE** running as a legitimate service which was initiating the outbound service

-I sent the IP address from brazil to the the threat intelligence feed and uploaded on **any.run** and it shows that the IP address is associated with **KHOLI's hacker group** known for targeting financial institutions.

-I immediately isolated the affected system from the network and prevented further data exfiltration. I removed the backdoor and patched all that need to be patched to avoid any more vulnerabilities the hacker must have exploited.

-TOOLS USED INCLUDE SIEM , EDR , AND THREAT INTELLIGENCE FEEDS

QUESTION 4

: How do you approach log analysis for detecting security incidents? Can you give an example of how you would correlate logs from different sources to identify a potential security threat?

QUESTON 4A

SOLUTION

Approaching log analysis for detecting security incidents involves a structured process that combines technical skills with analytical thinking. Here's a step-by-step guide on how to effectively analyze logs:

<1..All logs should be collected and centralized--Logs should be collected from sources such as servers, firewalls , routers and a log collection for to consolidate log should be used such as splunk or ELK stack

< 2. - The network architecture should be studied and one needs to be familiar with the system and network topology.

<3 - IoC (indicator of compromise should be identified) which include known patterns or signatures from malware, unauthorized access, or suspicious network activity such unusual log entries, such as sudden spikes in traffic, access from uncommon locations, or failed login attempts.

<4- Analysis of Log patterns: Examine logs over time to identify patterns, especially during off-hours or outside regular usage periods.

<5. Specific criteria should be used to narrow down logs to relevant events such as IP address, user id's or error codes. Log analysis tools or leverage tools such as grep command and splunk should be used for filtering and searching

Other steps include investigation, documentation, reporting, remediation, prevention and continuous monitoring

QUESTION 4B

Follow-Up: What are the common challenges in log correlation, and how would you address them?

ANSWER

Log correlation, a crucial step in identifying and responding to security threats, often faces specific challenges. Here are common challenges and strategies to address them:

Challenges in Log Correlation:

1. *Volume and Complexity*: Dealing with a vast number of logs from diverse sources can overwhelm.
- *Addressing Strategy*: Implement centralized log management systems (e.g., ELK Stack, Splunk) to consolidate and filter logs efficiently. Use scalable log processing tools and automation for preliminary analysis.

2. *Timestamp Discrepancies*: Time differences in logs from various sources can hinder correlation.
- *Addressing Strategy*: Normalize timestamps to a single time zone (e.g., UTC) to ensure consistency. Use tools that handle time zone conversions automatically.

3. *Log Format Variability*: Different systems generate logs in various formats, making correlation difficult.
- *Addressing Strategy*: Standardize log formats where possible. Use parsers or log normalization tools (like Logstash) to convert logs into a consistent format.

4. *Data Quality Issues*: Incomplete or incorrect log data complicates analysis.
- *Addressing Strategy*: Implement robust logging mechanisms and validate logs during collection. Regularly audit logs for completeness and accuracy.

5. *False Positives*: High rates of false positives can dilute real threats.
- *Addressing Strategy*: Fine-tune detection rules and thresholds. Implement machine learning models or statistical analysis to reduce false positives, ensuring alerts are meaningful.

6. *Integration Challenges*: Integrating logs from different systems can be complicated.
- *Addressing Strategy*: Leverage APIs, agents, or standardized protocols (e.g., Syslog) for seamless integration. Use SIEM systems designed for log consolidation.

7. *Data Privacy and Compliance*: Handling sensitive data while maintaining compliance.
- *Addressing Strategy*: Implement privacy-preserving techniques and ensure compliance with regulations (e.g., GDPR, HIPAA) by anonymizing or encrypting sensitive data as needed.

8. *Alert Fatigue*: Overwhelming analysts with too many alerts.
- *Addressing Strategy*: Prioritize alerts based on severity and relevance. Implement tiered alert systems, with only critical alerts requiring immediate attention.

9. *Resource Constraints*: Limited resources (time, expertise) for thorough analysis.
- *Addressing Strategy*: Automate repetitive analysis tasks. Train and augment teams with security analysts skilled in log correlation. Use automated tools for initial filtering.

10. *Threat Evolution*: Keeping up with evolving threats.
- *Addressing Strategy*: Stay informed through threat intelligence feeds, security forums, and continuous training. Use anomaly detection to catch unknown threats.