Prompt 1

List the roles and responsibilities of four key team members in the incident response team. Use the following format to submit your answer:

Incident Response Team Leader: This experienced member of the team will oversee the incident response process, helping the team complete their task efficiently. It is important to have someone experienced to be able to make the final decision, and be in charge of reporting to management.

Legal and Compliance officer: This officer will help make sure that the security standards follow all legal and compliance standards needed for whatever asset is being held and the location it is being held. This could also help during a breach such as reporting the breach to the correct regulatory sources, and having standard compliances will increase the overall security of the system.

Security Operations Center (SOC) Analyst: This member of the team will continually monitor the network and use security tools to detect incidents in real-time, analyzing any threats and escalating them as needed. This will help with protecting against phishing attempts and prompt reporting of suspicious activity.

Malware Analyst: This member will investigate the software used in the attack. Considering the recent issues of phishing attacks we should have a dedicated member for malware as malicious attachments are commonly included with phishing emails.

Prompt 2

List the four methods or tasks you would use to monitor this company's internal systems for unusual activity.

Real-Time Intrusion Detection Systems (IDS): This continuously monitors the network traffic to identify malicious traffic over a network. When malicious traffic is detected, an alert is sent to the IT for further investigation, (you could also use IPS for a system that will block malicious traffic detected instead of just making an alert, though it may block false positives.).

Endpoint Security Tools: These tools such as antivirus, would be installed on endpoint devices to help identify any malware or potential threats. This should also include Endpoint monitoring such as collecting log data.

User Access Reviews: It is important to have general reviews of user access controls. Users should only have access to whatever is needed for their daily work.

File System Monitoring: It is important to monitor critical files for any potential unwanted changes such as file modifications or deletions.

Prompt 3

Using what you know about the NIST framework and this company, list four details to include when documenting detected incidents.

Incident Identification: Clearly label the incident (malware, phishing, DDoS) ext.) to ensure proper categorization. This will help with choosing the appropriate response measures.

Attack vector: Provide details on how the incident occurred as a specific vulnerability, human error, misconfiguration, or malicious actor.

Risk and Impact assessment: The overall impact of the attack should be recorded such as if it affected one system or multiple systems. This would also include the financial and reputational damages of the incident.

Response Plan: Record immediate actions taken in response to this incident such as containing the affected asset. This can also include plans for further responses.

Prompt 4

List at least two containment strategies and explain how these strategies will help the company with containment.

Isolating the Affected Systems: It is important to isolate any infected system as soon as possible. It is possible that the infection can spread to connected systems when investigated.

Deactivate Compromised Accounts: Any accounts that are known to be compromised should be deactivated immediately, to help prevent attackers from using any further access points.

Prompt 5

List the four steps the company would use to conduct post-incident reviews based on the NIST framework.

Step 1, **Preparation**: Establish and maintain an incident response capability to ensure readiness for incidents. This includes conducting risk assessments, audits, and training incident response teams.

Step 2, **Detection and Analysis**: Identify and confirm incidents through carful and thorough monitoring of assets. This can be done with various SIEM tools.

Step 3, **Containment, Eradication, and Recovery** : Implement plans to contain any infected asset, limit the impact of the incident, and restore any affected asset to operational efficiency.

Step 4, **Post-Incident Activity** : Analyze and record incident response process for future incident recovery. This can include updating incident manuals or writing new ones.

Prompt 6

Using the NIST framework, write a checklist of three tasks an organization can use to structure an approach for updating the response plan based on findings.

Task 1 **Post-Incident Review**: Hold a meeting to discuss the process of recovery, any gaps seen throughout the recovery, what was learned, and how recovery could be improved.

Task 2 **Update procedures and tools**: Update incident response procedures, security tools, or acquire new security tools depending on findings from the post-incident review.

Task 3 **Malware Samples**: A copy of the malware can be kept to understand the attacks behavior.

Prompt 7

Based on the case study and the NIST framework, identify four sources of digital evidence necessary for incident investigation.

Source 1 **Email Logs**: Used to identify potential phishing attempts.

Source 2 **Network Traffic Logs**: Used to identify any unusual data communication or exfiltration from untrusted servers.

Source 3 **System Logs**: Used to identify compromised systems, unauthorized login attempts, and potential malware activity.

Source 4 **Endpoint Data**: Information from employee devices such as laptops or phones. These devices could be infected by malware to potentially affect the organization's network.

Prompt 8

List the three steps required to assess the collected digital evidence and verify its integrity.

Step 1: **Ensure Proper Chain of Custody -** Document each step of the evidence handling process to ensure it hasn’t been tampered with and can be legally admissible.

Step 2: **Perform Hashing -** Use cryptographic hashes (e.g., SHA-256) to verify the integrity of the evidence by comparing the current hash value with the original one.

Step 3: **Cross-Validate Evidence -** Compare evidence from multiple sources (e.g., logs, malware samples, network traffic) to confirm the consistency and reliability of the collected data.

Prompt 9

Evidence Type 1: Network Traffic Logs

Network traffic logs can help identify unauthorized communications, such as data exfiltration. This could help reveal the method of the breach and the origin of the attack.

Evidence Type 2: Authentication Logs

Authentication logs contain records of login attempts, including successful and failed logins. These logs are crucial for identifying unauthorized access attempts, unusual login locations, or patterns that could reveal how the attackers gained entry.

Evidence Type 3: Malware Artifacts (Executables/Scripts)

Malware artifacts such as malicious executables, scripts, or dropped files can provide a large amount of information about the attacks. Analyzing these artifacts helps to understand the attack methods, whether the malware exploited a specific vulnerability, and how it spreads.

Prompt 10

Network Traffic Analysis: Continuously monitor inbound and outbound network traffic using tools like intrusion detection systems (IDS) to detect irregular patterns, such as unauthorized access or data exfiltration attempts.

Endpoint Monitoring: Deploy endpoint detection and response (EDR) tools to monitor all connected devices for suspicious behavior, such as unusual software installations or malware activities on employee devices.

File Integrity Monitoring: Implement systems that track changes to critical system files, applications, and configurations to detect unauthorized alterations or tampering, which could be indicative of a security breach.

User Access Auditing: Monitor user login activities, including failed login attempts, logins during off-hours, and access to sensitive data, to identify potential unauthorized access or compromised accounts.