Implement Security Monitoring and Incident Response

1. Security Monitoring Setup and Use Case

Security Monitoring Setup

Tool Used: Security Information and Event Management (SIEM) System (e.g., Splunk, Elastic SIEM, or Microsoft Sentinel)
Monitoring Target: Network activity for potential unauthorized access to critical servers.
Objective: Detect brute-force attacks targeting Remote Desktop Protocol (RDP) and alert on excessive failed login attempts.

Detection Rules:

- **Rule Name:** RDP Brute Force Detection
- **Conditions:**
    - Event Source: Windows Security Logs
    - Event ID: 4625 (Failed Login Attempt)
    - Threshold: >10 failed login attempts from a single IP address within 5 minutes
- **Action:** Generate a high-priority alert in the SIEM system.

Mock Data Example:

- *Event:*
    - **Source IP:** 192.168.1.15
    - **Destination:** RDP Server (10.0.0.5)
    - **Attempts:** 15 failed login attempts in 3 minutes
    - **Alert Triggered:** "Potential RDP Brute-Force Attack Detected"

Alert Prioritization Process:

- **High Priority:** When the source IP belongs to an external or suspicious domain.
- **Medium Priority:** When the source IP is internal but has unusual activity.
- **Low Priority:** Repeated failed logins due to user misconfiguration.

Response Procedures:

1. *Validate Alert:* Confirm the excessive login attempts using log correlation in the SIEM.
2. *Investigate:* Check the source IP in threat intelligence feeds.
3. *Contain:* Block the source IP at the firewall.
4. *Remediate:* Reset the credentials of targeted accounts.
5. *Report:* Document the incident for compliance and analysis.

---

2. Incident Response Scenario

Scenario Description:

Incident: Ransomware detected on a user workstation after a phishing email was opened.

Incident Classification:

- **Type:** Malware Attack (Ransomware)
- **Severity:** Critical
- **Impact:** Encrypted files on the local workstation and mapped network drives.

Response Steps Taken:

1. **Detection:**
    - The SIEM detected unusual file changes and flagged a ransomware behavior signature.
    - Alert: "Potential Ransomware Activity Detected – File Encryption in Progress."
2. **Containment:**
    - Disconnected the affected workstation from the network to prevent further spread.
    - Disabled the user account temporarily.
3. **Eradication:**
    - Ran an anti-malware tool in safe mode to remove the ransomware.
    - Identified the phishing email and quarantined it from other inboxes.
4. **Recovery:**
    - Restored encrypted files from the most recent backup.
    - Conducted full system scans on affected systems to ensure no remnants of ransomware.
5. **Communication:**
    - Notified the incident response team and IT leadership.
    - Provided users with phishing education training as a follow-up.