SOC Operations Documentation

1. Detection Scenarios

Scenario 1: Phishing Attempt via Email Attachment

- Detection Method: Email gateway and SIEM correlation rule
- Indicators:
  - Executable attachment (.exe) scanned by VirusTotal (10/72 vendors flagged it malicious)
  - MD5/SHA256 hash match to known malware
  - Unusual subject line and external domain
- Alert Trigger: SIEM rule matching high-risk file hash + external domain email

Scenario 2: Lateral Movement via Pass-the-Hash Attack

- Detection Method: Log correlation from Windows Event Logs & endpoint monitoring
- Indicators:
  - Multiple failed logins followed by success from a new host
  - Kerberos authentication anomalies
  - PowerShell script execution detected
- Alert Trigger: Rule matching unusual authentication pattern with high-privilege account

Scenario 3: Malicious Web Payload via HTA Attack

- Detection Method: Web proxy logs + endpoint security agent
- Indicators:
  - User access to suspicious shortened URL
  - Downloaded HTA file execution from cloned website
  - PowerShell obfuscation signature
- Alert Trigger: Rule identifying HTA delivery combined with encoded PowerShell

2. Threat Indicator Categories & Use in Monitoring

- File Hashes: Unique fingerprints of files (MD5, SHA1, SHA256). Example: Malware hash match.

- IP Addresses: Known bad IPs or geolocation anomalies.
- Domain Names: Malicious or typo-squatting domains used in phishing.
- File Names/Types: Suspicious extensions such as .exe, .hta.
- User Behavior: Unusual logon times, unexpected access patterns.

3. Structured Threat Analysis Methodology

1. Detection - Alert triggered in SIEM
2. Triage - Classify severity based on asset, user, and threat type
3. Investigation - Gather logs (auth, DNS, proxy, endpoint) and correlate
4. Containment - Isolate system or block IOC (hash/IP/domain)
5. Eradication - Remove malware and clean registry or tasks
6. Recovery - Restore systems, reset credentials
7. Post-Mortem - Lessons learned, IOC feed updates, rule tuning

4. Alert Investigation Exercise

Scenario Used: Executable flagged in VirusTotal

Alert Details:

- Alert Name: "Malicious File Detected via Email"
- Asset: Marketing workstation
- Initial Indicator: Executable attachment emailed and downloaded

Investigation Steps:

1. File hash lookup on VirusTotal - 10/72 engines flagged it.
2. User Email Analysis - External domain, attachment file .exe
3. Endpoint Log Review - Executable launched -> outbound C2 attempt detected
4. Web Proxy Logs - DNS query to suspicious domain resolved
5. Action Taken:
   - Isolated host
   - Notified affected user

- Submitted hash to endpoint blocklist
- Added detection rule for file name and hash

5. Understanding Detection Fundamentals

- Correlation Rules: Combine multiple indicators/events for precise detection.
- Threat Intelligence: Enhances context to alerts (reputation-based).
- Behavioral Analysis: Looks for deviations rather than specific signatures.
- False Positive Reduction: Focus on asset context to minimize noise.
- Automated Response: Integrates SOAR for faster containment.