By Mohammed AlSubayt

Cyber Threats - Playbooks for SOC Analysts

1. Phishing Emails Alert

Steps :
1. Initial Triage : Verify the alert and gather basic information (sender, recipient, timestamp, subject line).
2. Email Analysis : Examine email headers, body content, and attachments for signs of phishing.
3. URL Analysis : Check embedded links using URL reputation services.
4. Attachment Analysis : Analyze attachments in a sandbox environment.
5. User Interaction : Contact the recipient to determine if any action was taken.
6. Containment : Block sender's email address and domain, isolate affected systems.
7. Remediation : Educate the user on recognizing phishing attempts, update email filters.

Reputation Check :
- [VirusTotal](https://www.virustotal.com)
- [URLVoid](http://www.urlvoid.com/)

2. Malware Investigation

Steps :
1. Initial Triage : Confirm the alert and gather details (affected system, user, timestamp, type of malware).
2. System Isolation : Disconnect the affected system from the network.
3. Malware Analysis : Perform static and dynamic analysis on the malware sample.
4. IOC Identification : Extract IOCs from the malware.
5. IOC Deployment : Use IOCs to search for other infected systems and update detection tools.
6. Containment and Eradication : Remove malware from the infected system, restore from a clean backup.
7. Remediation : Apply security patches, update antivirus definitions, review firewall and IDS/IPS rules.

Reputation Check :

- [Hybrid Analysis](https://www.hybrid-analysis.com)
- [MalwareBazaar](https://bazaar.abuse.ch)

3. Brute Force Analysis

Steps :

1. Initial Triage : Validate the alert and collect information (source IP, target system, number of attempts).
2. Log Analysis : Review authentication logs for multiple failed login attempts.
3. Source IP Investigation : Check the reputation of the source IP.
4. Account Lockout : Temporarily lock the targeted accounts.
5. Containment : Block the source IP at the firewall or IDS/IPS.
6. Remediation : Educate users on creating strong passwords, implement MFA, review and update account lockout policies.

Reputation Check :

- [IPVoid](http://www.ipvoid.com)
- [AbuseIPDB](https://www.abuseipdb.com)

4. DoS/DDoS Attack Alert

Steps :

1. Initial Triage : Confirm the alert and gather information (target, attack duration, type of attack).
2. Traffic Analysis : Analyze network traffic patterns for signs of DoS/DDoS.
3. Source Identification : Identify the IP addresses or networks involved in the attack.
4. Containment : Apply rate limiting, block malicious IPs, use DDoS mitigation services.
5. Service Continuity : Redirect traffic to backup servers or increase bandwidth if necessary.
6. Post-Attack Analysis : Review logs and traffic patterns to understand the attack and improve defenses.

Reputation Check :

- [Cisco Talos Intelligence](https://talosintelligence.com)
- [Radware Threat Intelligence](https://www.radware.com)

5. Proxy Logs Investigation (Communication to bad IP/domain)

By Mohammed AlSubayt

Steps :

1. Initial Triage : Validate the alert and gather details (source IP, destination IP/domain, timestamp).
2. Log Analysis : Examine proxy logs to identify the nature of the communication.
3. Reputation Check : Use threat intelligence services to check the reputation of the destination IP/domain.
4. System Inspection : Investigate the source system for signs of compromise.
5. Containment : Block outbound communication to the suspicious IP/domain.
6. Remediation : Remove any malicious software, update antivirus definitions, review firewall/proxy rules.

Reputation Check :

- [IPVoid](http://www.ipvoid.com)
- [URLHaus](https://urlhaus.abuse.ch)

6. Windows Event Log Analysis (Login & Logout)

Steps :

1. Initial Triage : Confirm the alert and gather details (user, system, timestamps).
2. Event Log Review : Analyze Windows Event Logs for suspicious login/logout patterns.
3. Contextual Analysis : Compare the log events with normal user behavior and known good logins.
4. Source IP Investigation : Check the reputation of source IPs for remote logins.
5. Containment : Lock affected accounts and reset passwords if unauthorized access is confirmed.
6. Remediation : Implement MFA, review and update login policies, educate users on secure login practices.

Reputation Check :

- [AbuseIPDB](https://www.abuseipdb.com)

7. Unknown Process Installation Investigation

Steps :

1. Initial Triage : Verify the alert and gather information (affected system, user, timestamp).

2. Process Analysis : Identify and analyze the unknown process using process monitoring tools.
3. File Analysis : Examine associated files and directories for signs of malicious activity.
4. IOC Identification : Extract IOCs and search for their presence on other systems.
5. Containment : Terminate the unknown process and isolate the affected system if necessary.
6. Remediation : Remove any related malware, update antivirus definitions, review system and application logs for further signs of compromise.

Reputation Check :

- [VirusTotal](https://www.virustotal.com)
- [Hybrid Analysis](https://www.hybrid-analysis.com)

8. Insider Threats

Steps :

1. Initial Triage : Validate the alert and gather information (employee involved, affected systems, activities observed).
2. Behavioral Analysis : Review recent actions of the suspected insider (access logs, file transfers, communication patterns).
3. Access Review : Check for unauthorized access or unusual data access patterns.
4. Interview : Conduct interviews with the employee if appropriate, and with their colleagues or supervisors.
5. Containment : Restrict the insider's access to sensitive systems and data if necessary.
6. Remediation : Implement stricter access controls, conduct regular audits, and provide security awareness training.

Reputation Check :

- [MITRE ATT&CK - Insider Threat](https://attack.mitre.org/tactics/TA0005/)

9. Credential Theft

Steps :

1. Initial Triage : Confirm the alert and gather information (user account involved, source of alert, potential compromise method).
2. Log Analysis : Review login attempts and access patterns for anomalies.

3. User Verification : Contact the affected user to verify recent login activity.
4. Password Reset : Force a password reset for the affected user account.
5. Containment : Disable the compromised account temporarily if necessary.
6. Remediation : Educate the user on creating strong passwords, implementing MFA, reviewing and enhancing password policies.

Reputation Check :
- [Have I Been Pwned](https://haveibeenpwned.com)
- [DeHashed](https://www.dehashed.com)

10. Ransomware Attack

Steps :
1. Initial Triage : Verify the alert and gather information (affected systems, type of ransomware, infection vector).
2. System Isolation : Disconnect infected systems from the network.
3. Ransomware Analysis : Analyze the ransomware sample in a controlled environment to understand its behavior and decryption possibilities.
4. Backup Restoration : Identify unaffected backups and prepare for restoration.
5. Containment : Block communication with known ransomware command and control servers.
6. Remediation : Restore systems from backups, apply security patches, update antivirus definitions.

Reputation Check :
- [ID Ransomware](https://id-ransomware.malwarehunterteam.com)
- [No More Ransom](https://www.nomoreransom.org)

11. Data Exfiltration

Steps :
1. Initial Triage : Validate the alert and gather information (source, destination, type of data involved).
2. Traffic Analysis : Analyze network traffic to identify patterns and volumes of data transfer.
3. Endpoint Inspection : Check the affected endpoints for signs of compromise and tools used for data exfiltration.
4. Containment : Block the suspicious data transfers and isolate affected systems.

5. Remediation : Remove any malware or unauthorized software, update data loss prevention (DLP) policies, and enhance network monitoring.

Reputation Check :
- [AbuseIPDB](https://www.abuseipdb.com)
- [OTX AlienVault](https://otx.alienvault.com)

12. Exploited Vulnerability

Steps :
1. Initial Triage : Confirm the alert and gather details about the affected systems, the vulnerability exploited, and the attack vector.
2. Vulnerability Analysis : Identify the specific vulnerability and review available patches or mitigations.
3. System Inspection : Check the affected systems for signs of compromise and unauthorized access.
4. Containment : Apply immediate mitigations such as disabling vulnerable services or blocking exploit vectors.
5.

Remediation : Apply patches, update software versions, and review and enhance security configurations.

Reputation Check :
- [CVE Details](https://www.cvedetails.com)
- [NVD (National Vulnerability Database)](https://nvd.nist.gov)

13. Social Engineering

Steps :
1. Initial Triage : Validate the alert and gather information on the type of social engineering attempt (e.g., phishing, pretexting).
2. Communication Review : Analyze communication logs and patterns to identify the scope of the attack.
3. Employee Interaction : Interview the targeted employees to gather more details about the interaction and potential compromise.
4. Containment : Implement measures to prevent further social engineering attempts, such as email filtering or employee awareness.
5. Remediation : Conduct training sessions to educate employees about recognizing and responding to social engineering tactics.

Reputation Check :
- [SANS Security Awareness - Social Engineering](https://www.sans.org/security-awareness-training/simply-put/social-engineering)
- [KnowBe4](https://www.knowbe4.com)

14. Web Application Attack

Steps :
1. Initial Triage : Confirm the alert and gather information on the type of attack (e.g., SQL injection, XSS, CSRF).
2. Log Review : Analyze web server logs to identify malicious requests and patterns.
3. Vulnerability Analysis : Assess the web application for known vulnerabilities and potential misconfigurations.
4. Containment : Block malicious IP addresses and apply web application firewall (WAF) rules.
5. Remediation : Fix identified vulnerabilities, update application code, and enhance security configurations.

Reputation Check :
- [OWASP Vulnerabilities](https://owasp.org/www-project-top-ten/)
- [SANS Internet Storm Center](https://isc.sans.edu)

15. Rogue Device Detection

Steps :
1. Initial Triage : Confirm the alert and gather information on the rogue device (device type, MAC address, location).
2. Network Scan : Conduct a network scan to identify unauthorized devices.
3. Device Analysis : Analyze the rogue device's activity and network traffic.
4. Containment : Disconnect the rogue device from the network.
5. Remediation : Strengthen network access controls and review security policies.

Reputation Check :
- [MAC Address Lookup](https://maclookup.app)
- [Wireshark](https://www.wireshark.org)

16. Privilege Escalation

Steps :

1. Initial Triage : Validate the alert and gather information (affected system, user, type of privilege escalation).
2. Log Review : Analyze logs to identify how privileges were escalated.
3. User and System Analysis : Investigate the affected user and system for signs of compromise.
4. Containment : Revoke elevated privileges and reset affected accounts.
5. Remediation : Apply patches, review and update access controls, and educate users on privilege escalation risks.

Reputation Check :

- [Microsoft Security Updates](https://portal.msrc.microsoft.com/en-us/security-guidance)

17. DNS Tunneling

Steps :

1. Initial Triage : Confirm the alert and gather information (affected system, suspicious domain).
2. Traffic Analysis : Monitor DNS traffic for unusual patterns.
3. Domain Analysis : Check the reputation of the suspicious domain.
4. Containment : Block malicious DNS traffic and domains.
5. Remediation : Review and update DNS policies, and educate users on DNS tunneling risks.

Reputation Check :

18. Advanced Persistent Threat (APT)

Steps :

1. Initial Triage : Validate the alert and gather information (affected systems, type of APT activity).
2. Log and Traffic Analysis : Review logs and network traffic for signs of APT.
3. IOC Identification : Identify IOCs associated with the APT.
4. Containment : Isolate affected systems and block APT communication channels.
5. Remediation : Apply security patches, update detection tools, and enhance monitoring.

Reputation Check :
- [FireEye Threat Intelligence](https://www.fireeye.com)
- [MITRE ATT&CK](https://attack.mitre.org)

19. Dark Web Monitoring

Steps :
1. Initial Triage : Confirm the alert and gather information (type of data found, source).
2. Data Analysis : Verify the authenticity and relevance of the data.
3. Containment : Notify affected parties and take steps to mitigate any risks.
4. Remediation : Strengthen data protection measures and monitor for further leaks.

Reputation Check :
- [Have I Been Pwned](https://haveibeenpwned.com)
- [IntSights](https://intsights.com)

20. Zero-Day Exploit

Steps :
1. Initial Triage : Confirm the alert and gather information (affected systems, type of zero-day exploit).
2. Vulnerability Analysis : Identify the zero-day vulnerability and review available mitigations.
3. System Inspection : Check the affected systems for signs of exploitation.
4. Containment : Apply immediate mitigations to protect against the zero-day exploit.
5. Remediation : Apply patches or updates as they become available, and review security controls.

Reputation Check :
- [Zero Day Initiative](https://www.zerodayinitiative.com)
- [CVE Details](https://www.cvedetails.com)

Additional Resources for Threat Intelligence and Reputation Check

1. VirusTotal : https://www.virustotal.com
2. URLVoid : http://www.urlvoid.com

3. Hybrid Analysis : https://www.hybrid-analysis.com
4. IPVoid : http://www.ipvoid.com
5. AbuseIPDB : https://www.abuseipdb.com
6. OTX AlienVault : https://otx.alienvault.com
7. Cisco Talos Intelligence : https://talosintelligence.com
8. Radware Threat Intelligence : https://www.radware.com
9. ID Ransomware : https://id-ransomware.malwarehunterteam.com
10. No More Ransom : https://www.nomoreransom.org
11. CVE Details : https://www.cvedetails.com
12. NVD (National Vulnerability Database) : https://nvd.nist.gov