SOAR PLAYBOOK FOR AUTOMATED INCIDENT RESPONSE WITH EXAMPLES

BY IZZMIER IZZUDDIN

SOAR INCIDENT RESPONSE PLAYBOOK

MALWARE

Objective: Automatically detect malware infections, analyse the threat, isolate infected systems, and remove the malware while blocking communication with any command and control (C2) servers.

Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **EDR (Endpoint Detection and Response):** (e.g., CrowdStrike, Carbon Black)
- **Firewall:** (e.g., Palo Alto, Fortinet)
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Threat Intelligence Platforms:** (e.g., VirusTotal, ThreatConnect)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM for any alerts related to known malware indicators (e.g., unusual process activity, suspicious file behaviour, network communication with known malicious domains).
- **Automation Task:** Use predefined correlation rules within the SIEM to detect malware activity. For example, if the SIEM detects unusual process execution, such as C:\Windows\Temp\malicious.exe, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once malware is detected, automatically extract Indicators of Compromise (IOCs) such as file hashes, malicious domains, and IPs.
- **Automation Task:**
    - **Enrichment:** The SOAR platform automatically enriches the IOCs with threat intelligence from external sources (e.g., VirusTotal, ThreatConnect) to gather information about the malware variant and associated threats.
    - **Analysis:** The platform assesses the severity of the malware based on its behaviour, the affected system, and the enriched threat intelligence data.

Step 3: Containment

- **Trigger:** After confirming the malware, initiate automated containment actions.
- **Automation Task:**
    - **Isolate Infected Systems:** Command the EDR tool to disconnect the infected endpoints from the network to prevent further spread of the malware.

    - **Block Communication Channels:** Update firewall rules to block outbound traffic to known malicious IP addresses or domains associated with the malware's C2 infrastructure.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.
- **Automation Task:**
    - **Malware Removal:** Automatically remove the malicious files using the EDR's remediation capabilities.
    - **System Rollback:** If necessary, roll back the affected system to a known good state using snapshots or backup data.

Step 5: Recovery

- **Trigger:** Post-eradication, prepare the system for recovery.
- **Automation Task:** Validate that the malware has been completely removed and restore any affected data from clean backups. Ensure that the system is patched to prevent reinfection.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a comprehensive report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis to review the incident response process.
- **Automation Task:** Update the playbook with any lessons learned, ensuring it is optimised for future malware incidents.

Example

Scenario: A malware strain is detected running on a company's HR server, showing suspicious file execution patterns and communication with a known malicious domain. The SIEM logs reveal unusual process activity, triggering the malware incident response playbook.

Step-by-Step:

1. **SIEM Alert:**
    - **Trigger:** The SIEM detects unusual process execution, C:\Windows\Temp\malicious.exe, which matches known malware behaviour patterns.

    - **Example:** The SIEM logs show a process attempting to connect to malicious-domain.com, a known C2 server.
2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the SIEM alert and begins the enrichment process.
    - **Enrichment:** The platform queries VirusTotal and finds that the file hash abc123... is associated with the "Emotet" malware variant.
3. **Containment Actions:**
    - **EDR:** The SOAR platform commands the EDR tool to isolate the HR server from the network to prevent further spread of the malware.
    - **Firewall:** The platform updates the firewall rules to block outbound connections to malicious-domain.com.
4. **Eradication:**
    - **Malware Removal:** The EDR tool automatically removes the detected malware file from the HR server.
    - **System Rollback:** The server is restored to a snapshot taken before the infection occurred.
5. **Recovery:**
    - **Data Restoration:** Any data affected by the malware is restored from clean backups.
    - **System Patching:** The server is patched with the latest security updates to prevent reinfection.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The platform generates a detailed incident report summarising the malware infection, actions taken, and final outcome.
    - **SOC Review:** The SOC team reviews the report and updates the playbook with any improvements identified during the incident.

CRYPTOJACKING

Objective: Automatically detect cryptojacking activity, isolate infected systems, and block cryptojacking domains.

Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **EDR (Endpoint Detection and Response) Tools**
- **Firewall**
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Threat Intelligence Platforms:** (e.g., VirusTotal, DomainTools)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM and EDR tools for alerts related to cryptojacking indicators (e.g., abnormal CPU usage, unauthorised mining software, outbound connections to known mining pools).
- **Automation Task:** Use predefined correlation rules to detect cryptojacking activity. For example, if the SIEM detects consistent high CPU usage from a specific endpoint along with outbound connections to a mining pool, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once cryptojacking is detected, automatically extract Indicators of Compromise (IOCs) such as malicious file hashes, domains, and IPs related to cryptojacking.
- **Automation Task:** The SOAR platform automatically enriches the IOCs with threat intelligence from external sources (e.g., VirusTotal, DomainTools) to confirm the cryptojacking activity.

Step 3: Containment

- **Trigger:** After confirming cryptojacking, initiate automated containment actions.
- **Automation Task:**
    - **Isolate Infected Systems:** Command the EDR tool to disconnect the infected endpoints from the network to prevent further cryptojacking activity.
    - **Block Domains:** Update firewall rules to block outbound traffic to known cryptojacking domains and mining pools.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.

- **Automation Task:** Automatically remove unauthorised cryptojacking software from the infected systems using EDR remediation tools or manual intervention as needed.

Step 5: Recovery

- **Trigger:** Post-eradication, ensure the system is fully restored and secured.
- **Automation Task:** Validate that the cryptojacking activity has ceased, and restore any system settings or files that were altered due to the cryptojacking activity.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis.
- **Automation Task:** Update the playbook with any lessons learned, ensuring it is optimised for future cryptojacking incidents.

Example

Scenario: A cryptojacking attack is detected on multiple employee workstations. The SIEM logs show abnormal CPU usage and outbound connections to a known mining pool.

Step-by-Step:

1. **SIEM Alert:**
    - **Trigger:** SIEM detects abnormal CPU usage and outbound connections from multiple endpoints to a known mining pool domain.
    - **Example:** CPU usage spikes to 100% on workstation01, workstation02, etc., with connections to miningpool.com.
2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the SIEM alert and begins the enrichment process.
    - **Enrichment Task:** Extracts IOCs such as the file hash of the mining software and the domain miningpool.com.
    - **IOCs Extracted:** File Hash: abcd1234..., Domain: miningpool.com.
3. **Containment Actions:**
    - **Isolate:** The EDR tool automatically isolates the infected workstations from the network.
    - **Blocking:** Firewall rules are updated to block traffic to miningpool.com and other associated domains.
4. **Eradication:**

    - **Removal:** Unauthorised mining software is removed from all infected workstations.
    - **System Restoration:** Systems are scanned for any remaining traces of the cryptojacking software, and any altered configurations are restored.
5. **Recovery:**
    - **Validation:** CPU usage and network traffic are monitored to ensure the cryptojacking activity has ceased.
    - **System Hardening:** Additional security measures are implemented to prevent future cryptojacking attempts.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The SOAR platform generates a detailed report summarising the cryptojacking incident, including detected indicators, actions taken, and recommendations for prevention.
    - **SOC Review:** The report is reviewed by the SOC team, who then update the playbook based on lessons learned.

PHISHING EMAIL

Objective: Automatically detect phishing emails, analyse email content for suspicious patterns, and quarantine affected emails.

Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **Email Security Gateway:** (e.g., Proofpoint, Mimecast)
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Threat Intelligence Platforms:** (e.g., VirusTotal, DomainTools)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM and Email Security Gateway for alerts related to known phishing indicators (e.g., suspicious URLs, attachments, or sender domains).
- **Automation Task:** Use predefined correlation rules to detect potential phishing emails. For example, if the SIEM detects an email from a known malicious domain or with a suspicious attachment, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once a potential phishing email is detected, automatically extract Indicators of Compromise (IOCs) such as suspicious URLs, domains, and email content patterns.
- **Automation Task:** The SOAR platform enriches the IOCs with threat intelligence from external sources (e.g., VirusTotal, DomainTools) to determine if the email is part of a phishing campaign.

Step 3: Containment

- **Trigger:** After confirming the email is phishing, initiate automated containment actions.
- **Automation Task:**
    - **Quarantine Emails:** Command the email security gateway to quarantine the suspected phishing email across all user mailboxes.
    - **Block Domains:** Update email filtering rules to block the sender's domain or any identified malicious URLs.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.
- **Automation Task:** Automatically delete all instances of the phishing email from user mailboxes and update the email gateway's blocklists to prevent future delivery of similar emails.

Step 5: Recovery

- **Trigger:** Post-eradication, ensure that the threat has been neutralised.
- **Automation Task:** Notify affected users about the phishing attempt and advise them on any necessary actions (e.g., changing passwords if credentials were potentially compromised).

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis.
- **Automation Task:** Update the playbook with any lessons learned, ensuring it is optimised for future phishing incidents.

Example

Scenario: A phishing email is detected in the inbox of multiple employees, containing a malicious link designed to harvest credentials.

Step-by-Step Simulation:

1. **SIEM Alert:**
    - **Trigger:** SIEM and the email security gateway detect a suspicious email sent from an unknown domain with a subject line like "Urgent: Update Your Account Information."
    - **Example:** Email from phishing@maliciousdomain.com with a URL: http://maliciousdomain.com/login.
2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the SIEM alert and begins the enrichment process.
    - **Enrichment Task:** Extracts the URL and checks it against VirusTotal, which flags it as malicious.
    - **IOCs Extracted:** URL: http://maliciousdomain.com/login, Sender Domain: maliciousdomain.com.
3. **Containment Actions:**
    - **Quarantine:** The email security gateway automatically quarantines the email across all user mailboxes.
    - **Blocking:** The firewall and email filtering rules are updated to block traffic to maliciousdomain.com.
4. **Eradication:**
    - **Deletion:** All instances of the phishing email are removed from user mailboxes.

    - **Blocklist Update:** The sender's domain is added to the email gateway's blocklist to prevent future occurrences.
5. **Recovery:**
    - **User Notification:** Affected users are notified of the phishing attempt and instructed to reset their passwords if they clicked the link.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The SOAR platform generates a detailed report summarising the incident, including the detected phishing email, actions taken, and recommendations for prevention.
    - **SOC Review:** The report is reviewed by the SOC team, who then update the playbook based on lessons learned.

DENIAL OF SERVICE (DOS)

Objective: Automatically detect Denial of Service (DoS) attacks, analyse the threat, isolate affected systems, and mitigate the attack by blocking malicious traffic while maintaining legitimate services.

Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **Firewall:** (e.g., Palo Alto, Fortinet)
- **Intrusion Prevention System (IPS):** (e.g., Snort, Suricata)
- **Load Balancer:** (Optional, to distribute legitimate traffic)
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Threat Intelligence Platforms:** (e.g., VirusTotal, ThreatConnect)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM and IPS for any alerts related to DoS attack patterns (e.g., unusual traffic spikes, SYN floods, UDP floods, ICMP floods).
- **Automation Task:** Use predefined correlation rules within the SIEM to detect signs of a DoS attack. For example, if the SIEM detects a high volume of SYN packets from a single IP address, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once a DoS attack is detected, automatically extract Indicators of Compromise (IOCs) such as source IP addresses, affected services, and traffic patterns.
- **Automation Task:**
    - **Enrichment:** The SOAR platform automatically enriches the IOCs with threat intelligence from external sources to determine if the source IPs are part of known botnets or malicious networks.
    - **Analysis:** The platform assesses the severity of the attack based on traffic volume, affected services, and the potential impact on the organisation.

Step 3: Containment

- **Trigger:** After confirming the DoS attack, initiate automated containment actions.
- **Automation Task:**
    - **Block Malicious IPs:** Command the firewall to block inbound traffic from identified malicious IP addresses.
    - **Rate Limiting:** Apply rate limiting on the firewall or load balancer to restrict the number of requests from suspicious sources.

- **Redirect Traffic:** If applicable, redirect legitimate traffic to a backup server or a load balancer to minimise service disruption.

Step 4: Mitigation

- **Trigger:** Once containment is successful, the SOAR platform triggers the mitigation phase.
- **Automation Task:**
  - **Traffic Filtering:** The firewall or IPS is configured to filter out malicious traffic patterns while allowing legitimate traffic to pass through.
  - **DDoS Protection:** If applicable, engage DDoS protection services (e.g., Cloudflare, AWS Shield) to absorb and mitigate the attack.

Step 5: Recovery

- **Trigger:** Post-mitigation, prepare the systems for recovery.
- **Automation Task:** Validate that the DoS attack has been mitigated and services are restored to normal operation. Monitor traffic patterns to ensure no residual attack activity remains.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a comprehensive report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis to review the incident response process.
- **Automation Task:** Update the playbook with any lessons learned, ensuring it is optimised for future DoS incidents.

Example

Scenario: A DoS attack is detected targeting the company's web server, causing a significant increase in SYN requests, leading to service disruption. The SIEM logs show an abnormal traffic spike from multiple IP addresses, triggering the DoS incident response playbook.

Step-by-Step Simulation:

1. **SIEM Alert:**
   - **Trigger:** The SIEM detects an unusually high number of SYN requests coming from several IP addresses, indicative of a SYN flood attack.

    - **Example:** The SIEM logs show traffic spikes to the web server, with SYN packets originating from a range of IPs: 192.168.1.100, 192.168.1.101, etc.
2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the SIEM alert and begins the enrichment process.
    - **Enrichment:** The platform queries threat intelligence sources to determine if the IP addresses are associated with known malicious networks.
3. **Containment Actions:**
    - **Firewall:** The SOAR platform commands the firewall to block inbound traffic from the identified malicious IPs.
    - **Rate Limiting:** Rate limiting is applied to the firewall to limit the number of SYN requests per second from any given IP address, preventing the attack from overwhelming the server.
4. **Mitigation:**
    - **Traffic Filtering:** The IPS is configured to drop any further SYN packets that match the attack pattern, ensuring that only legitimate traffic reaches the server.
    - **DDoS Protection:** The SOAR platform engages a DDoS protection service to absorb any remaining attack traffic.
5. **Recovery:**
    - **Service Restoration:** Once the attack subsides, the web server traffic is monitored to ensure normal operation is restored, and no residual attack activity persists.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The platform generates a detailed incident report summarising the DoS attack, actions taken, and final outcome.
    - **SOC Review:** The SOC team reviews the report and updates the playbook with any improvements identified during the incident.

WEB DEFACEMENT

Objective: Automatically detect web defacement incidents, analyse the threat, restore the original content, and secure the compromised systems to prevent future attacks.

Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **Web Application Firewall (WAF):** (e.g., Imperva, AWS WAF)
- **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** (e.g., Snort, Suricata)
- **Version Control System (VCS):** (e.g., Git, SVN)
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Backup System:** (e.g., AWS S3, Google Cloud Storage)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM and IDS/IPS for any alerts related to unauthorised changes in web content or suspicious activity on web servers.
- **Automation Task:** Use predefined correlation rules within the SIEM to detect signs of web defacement. For example, if the SIEM detects changes in web files (e.g., HTML, JavaScript) that weren't part of an authorised update, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once web defacement is detected, automatically extract Indicators of Compromise (IOCs) such as modified files, IP addresses, and attack vectors.
- **Automation Task:**
    - **File Integrity Check:** The SOAR platform compares the current web files against the last known good version stored in the VCS.
    - **Threat Intelligence Enrichment:** Automatically enrich IOCs (e.g., attacker IPs, malicious scripts) using threat intelligence sources to assess the threat's severity.

Step 3: Containment

- **Trigger:** After confirming the web defacement, initiate automated containment actions.
- **Automation Task:**
    - **WAF Configuration:** Update the WAF rules to block further malicious requests from identified attacker IPs or to filter out suspicious content.
    - **Network Isolation:** Temporarily isolate the compromised web server from the network if needed to prevent further tampering.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.
- **Automation Task:**
    - **Remove Malicious Content:** Automatically restore the defaced web pages to their original state using the last known good version from the VCS.
    - **Patch Vulnerabilities:** Deploy patches or security updates to the web server to close any vulnerabilities exploited during the attack.

Step 5: Recovery

- **Trigger:** Post-eradication, prepare the system for recovery.
- **Automation Task:**
    - **Re-enable Services:** Once the web server is secured, reconnect it to the network.
    - **Backup Verification:** Ensure that backups are intact and that no unauthorised changes have been made to the backup files.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a comprehensive report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis to review the incident response process.
- **Automation Task:** Update the playbook with any lessons learned, ensuring it is optimised for future web defacement incidents.

Example

Scenario: An attacker defaces the company's website by altering the homepage content to display unauthorised messages. The SIEM logs show unauthorised file changes, triggering the web defacement incident response playbook.

Step-by-Step Simulation:

1. **SIEM Alert:**
    - **Trigger:** The SIEM detects unauthorised changes to the homepage file index.html.
    - **Example:** The SIEM logs show a modified file with unexpected content like "Hacked by XYZ".
2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the SIEM alert and begins the enrichment process.

    - **File Integrity Check:** The platform compares the current index.html file with the last known good version stored in the VCS.
3. **Containment Actions:**
    - **WAF Configuration:** The WAF is updated to block any further malicious requests targeting the vulnerable web application.
    - **Network Isolation:** If necessary, the web server is temporarily isolated to prevent further unauthorised changes.
4. **Eradication:**
    - **Restore Content:** The SOAR platform automatically restores the defaced index.html file from the VCS.
    - **Patch Deployment:** The web server is patched to close the vulnerability that allowed the defacement.
5. **Recovery:**
    - **Service Restoration:** The web server is reconnected to the network, and normal operations resume.
    - **Backup Verification:** The backup system is checked to ensure no unauthorised changes were made during the incident.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The platform generates a detailed incident report summarising the web defacement attack, actions taken, and final outcome.
    - **SOC Review:** The SOC team reviews the report and updates the playbook with any improvements identified during the incident.

BRUTE-FORCE

Objective: Automatically detect brute-force attacks, analyse the threat, block malicious IP addresses, and secure affected systems to prevent unauthorised access.

Tools Required:

- **SIEM:** (e.g., Splunk, QRadar)
- **Firewall:** (e.g., Palo Alto, Cisco ASA)
- **Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** (e.g., Snort, Suricata)
- **Endpoint Detection and Response (EDR):** (e.g., CrowdStrike, Carbon Black)
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM and IDS/IPS for any alerts related to failed login attempts across various systems that indicate a potential brute-force attack.
- **Automation Task:** Use predefined correlation rules within the SIEM to detect patterns of multiple failed login attempts from a single IP address or across multiple accounts. For example, if the SIEM detects more than a specific number of failed login attempts within a short period, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once a brute-force attack is detected, automatically extract Indicators of Compromise (IOCs) such as attacker IP addresses and targeted usernames.
- **Automation Task:**
    - **IOC Enrichment:** The SOAR platform automatically enriches the IOCs with threat intelligence from external sources (e.g., VirusTotal, ThreatConnect) to determine the reputation of the attacking IPs.
    - **Attack Severity Assessment:** Assess the severity of the brute-force attack based on the number of failed attempts, the targeted systems, and whether any accounts were compromised.

Step 3: Containment

- **Trigger:** After confirming the brute-force attack, initiate automated containment actions.
- **Automation Task:**
    - **Block Malicious IPs:** Automatically update firewall rules to block the attacking IP addresses identified during the analysis phase.
    - **Account Lockdown:** Temporarily lock accounts that were targeted during the brute-force attack to prevent unauthorised access.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.
- **Automation Task:**
    - **Password Reset:** Automatically trigger a forced password reset for affected accounts to eliminate the possibility of unauthorised access using compromised credentials.
    - **Malware Scan:** Initiate an EDR scan on systems targeted by the brute-force attack to ensure no malware or backdoors were installed during the attack.

Step 5: Recovery

- **Trigger:** Post-eradication, prepare the system for recovery.
- **Automation Task:**
    - **Account Restoration:** After password resets and ensuring the integrity of the system, restore access to the affected accounts.
    - **Network Reconfiguration:** Ensure firewall and IDS/IPS rules are optimised to prevent similar brute-force attacks in the future.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a comprehensive report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis to review the incident response process.
- **Automation Task:** Update the playbook with any lessons learned, including improved detection rules, enhanced containment strategies, and updates to user access policies.

Example

Scenario: An attacker attempts a brute-force attack against the company's VPN by repeatedly trying to guess user passwords. The SIEM logs show hundreds of failed login attempts from a single IP address, triggering the brute-force incident response playbook.

Step-by-Step Simulation:

1. **SIEM Alert:**
    - **Trigger:** The SIEM detects more than 100 failed login attempts from IP address 192.168.1.100 within a 5-minute window targeting multiple user accounts.
    - **Example:** Failed login attempts for usernames izzmier, iffah, and admin.

2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the SIEM alert and begins the IOC enrichment process.
    - **IOC Enrichment:** The IP address 192.168.1.100 is checked against threat intelligence sources and found to be associated with previous brute-force attacks.
3. **Containment Actions:**
    - **Block IP:** The SOAR platform updates the firewall to block all traffic from 192.168.1.100.
    - **Account Lockdown:** User accounts izzmier, iffah, and admin are temporarily locked to prevent unauthorised access.
4. **Eradication:**
    - **Password Reset:** The SOAR platform triggers a forced password reset for izzmier, iffah, and admin.
    - **Malware Scan:** An EDR scan is initiated on the VPN server and associated systems to ensure no malware was installed during the attack.
5. **Recovery:**
    - **Account Restoration:** Once new passwords are set, accounts izzmier, iffah, and admin are reactivated.
    - **Network Reconfiguration:** Firewall and IDS/IPS rules are reviewed and updated to prevent future brute-force attacks.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The platform generates a detailed incident report summarising the brute-force attack, actions taken, and final outcome.
    - **SOC Review:** The SOC team reviews the report and updates the playbook with improvements identified during the incident.

DATA LOSS PREVENTION (DLP)

Objective: Automatically detect data loss prevention (DLP) incidents, quarantine affected data, and initiate remediation workflows to prevent unauthorised data exfiltration.

Tools Required:

- **DLP Solution:** (e.g., Symantec DLP, McAfee Total Protection for Data Loss Prevention)
- **SIEM:** (e.g., Splunk, QRadar)
- **SOAR Platform:** (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)
- **Encryption and Data Management Tools:** (e.g., BitLocker, VeraCrypt)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the DLP solution for any alerts related to potential data exfiltration or unauthorised data access.
- **Automation Task:** Use predefined policies within the DLP solution to detect specific data types (e.g., personally identifiable information, financial records) being transferred or accessed inappropriately. For example, if the DLP detects sensitive files being transferred to an external USB drive, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once a DLP incident is detected, automatically gather details about the incident, including the type of data involved, the source, and the destination.
- **Automation Task:**
    - **Incident Enrichment:** The SOAR platform automatically enriches the incident details with contextual information, such as user details, device information, and location.
    - **Risk Assessment:** Assess the severity of the DLP incident based on the sensitivity of the data, the volume of data involved, and the potential impact on the organisation.

Step 3: Containment

- **Trigger:** After confirming a DLP incident, initiate automated containment actions to prevent further data exfiltration.
- **Automation Task:**
    - **Quarantine Data:** The DLP solution quarantines the affected files to prevent further access or transfer.
    - **Disconnect or Isolate Endpoint:** Automatically disconnect the endpoint involved in the data transfer from the network to prevent further data leakage.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.
- **Automation Task:**
    - **Secure Data:** Encrypt the quarantined data to prevent unauthorised access.
    - **Remediate Vulnerabilities:** Identify and fix any vulnerabilities that allowed the data loss, such as unpatched software, misconfigured security settings, or weak access controls.

Step 5: Recovery

- **Trigger:** Post-eradication, prepare the system for recovery.
- **Automation Task:**
    - **Restore Access:** Once the threat is neutralised, restore access to the affected systems and files under stricter security policies.
    - **Audit and Compliance Check:** Ensure that all remediation actions are documented and comply with relevant data protection regulations.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a comprehensive report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis to review the incident response process.
- **Automation Task:** Update the playbook with any lessons learned, including improved detection rules, enhanced containment strategies, and updates to data handling policies.

Example

Scenario: An employee attempts to transfer sensitive customer data to a personal USB drive. The DLP solution detects the unauthorised data transfer and triggers the DLP incident response playbook.

Step-by-Step Simulation:

1. **DLP Alert:**
    - **Trigger:** The DLP solution detects an attempt to copy files containing customer credit card information to a USB drive.
    - **Example:** File detected - CustomerData.xlsx containing credit card numbers.

2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the DLP alert and begins the incident enrichment process.
    - **Incident Enrichment:** The platform gathers additional details, such as the user involved (Izzmier), the device (CompanyLaptop123), and the location (Office HQ).
3. **Containment Actions:**
    - **Quarantine Data:** The DLP solution automatically quarantines the file CustomerData.xlsx.
    - **Disconnect Endpoint:** The SOAR platform instructs the DLP tool to disconnect CompanyLaptop123 from the network to prevent further data transfer.
4. **Eradication:**
    - **Secure Data:** The quarantined file CustomerData.xlsx is automatically encrypted.
    - **Remediate Vulnerabilities:** The SOAR platform identifies that the endpoint did not have USB data transfer restrictions and automatically applies the necessary policies.
5. **Recovery:**
    - **Restore Access:** After ensuring the data is secure, the laptop is reconnected to the network with USB data transfer restrictions in place.
    - **Audit and Compliance:** The SOAR platform checks that all actions comply with GDPR and other relevant data protection regulations.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The platform generates a detailed incident report summarising the DLP incident, actions taken, and final outcome.
    - **SOC Review:** The SOC team reviews the report and updates the playbook with any necessary improvements.

RANSOMWARE

Objective: Automatically detect ransomware infections, isolate infected systems, and block ransomware communication channels.

Tools Required:

- SIEM (e.g., Splunk, QRadar)
- EDR (Endpoint Detection and Response) tools
- Firewall
- SOAR platform (e.g., Palo Alto Cortex XSOAR, Splunk Phantom)

Steps to Implement the Automation:

Step 1: Detection

- **Trigger:** Monitor the SIEM for any alerts related to known ransomware indicators (e.g., file encryption patterns, unusual file system activity).
- **Automation Task:** Use predefined correlation rules to detect ransomware activity. For example, if the SIEM detects file encryption with a high entropy value, it triggers the playbook.

Step 2: Triage and Analysis

- **Trigger:** Once ransomware is detected, automatically extract indicators of compromise (IOCs) such as malicious file hashes, domains, and IPs.
- **Automation Task:** The SOAR platform automatically enriches the IOCs with threat intelligence from external sources (e.g., VirusTotal, ThreatConnect).

Step 3: Containment

- **Trigger:** After confirming the ransomware, initiate automated containment actions.
- **Automation Task:**
    1. **Isolate Infected Systems:** Command the EDR tool to disconnect the infected endpoints from the network.
    2. **Block Communication Channels:** Update firewall rules to block outbound traffic to known ransomware C2 (Command and Control) servers.

Step 4: Eradication

- **Trigger:** Once containment is successful, the SOAR platform triggers the eradication phase.
- **Automation Task:** Automatically remove the malicious files, either through EDR remediation actions or by rolling back the system to a clean state using snapshots or backups.

Step 5: Recovery

- **Trigger:** Post-eradication, prepare the system for recovery.
- **Automation Task:** Validate that the ransomware is eradicated and restore data from clean backups.

Step 6: Post-Incident Analysis

- **Trigger:** After recovery, generate an incident report.
- **Automation Task:** The SOAR platform compiles logs, actions taken, and final outcomes into a report, which is then sent to the SOC team for review.

Step 7: Playbook Refinement

- **Trigger:** Conduct a post-mortem analysis.
- **Automation Task:** Update the playbook with any lessons learned, ensuring it is optimised for future incidents.

Example

Scenario: A ransomware strain is detected encrypting files on an employee's workstation. The SIEM logs show abnormal file encryption activity, triggering the ransomware playbook.

Step-by-Step:

Scenario: An employee inadvertently downloads a malicious attachment, which triggers ransomware that begins encrypting files on their computer.

Step-by-Step Simulation:

1. **Ransomware Alert:**
    - **Trigger:** The EDR solution detects an attempt to encrypt multiple files on the employee's device.
    - **Example:** Ransomware detected - WannaCry variant attempting to encrypt files on DeviceXYZ.
2. **Automation Initiated:**
    - **SOAR Action:** The SOAR platform picks up the EDR alert and begins the incident enrichment process.
    - **Incident Enrichment:** The platform gathers additional details, such as the user involved (Izzmier), the device (DeviceXYZ), and the location (Remote Office).
3. **Containment Actions:**
    - **Isolate Infected System:** The SOAR platform instructs the EDR tool to isolate DeviceXYZ from the network to prevent further ransomware spread.
    - **Block C2 Communication:** The SIEM blocks the ransomware's communication with its command and control server.

4. **Eradication:**
    - **Remove Ransomware:** The EDR solution automatically removes the ransomware from DeviceXYZ.
    - **Remediate Vulnerabilities:** The SOAR platform identifies that the device lacked the latest security patches and automatically applies the necessary updates.
5. **Recovery:**
    - **Restore from Backup:** After ensuring the threat is neutralised, files on DeviceXYZ are restored from the latest backup.
    - **Audit and Compliance:** The SOAR platform checks that all actions comply with relevant data protection regulations.
6. **Post-Incident Reporting:**
    - **SOAR Report:** The platform generates a detailed incident report summarising the ransomware incident, actions taken, and final outcome.
    - **SOC Review:** The SOC team reviews the report and updates the playbook with any necessary improvements.