OVERVIEW OF THE THREAT HUNTING PROCESS WITH AN SCENARIO

VAISHALI SHISHODIA

Threat Hunting: A Cybersecurity Analyst's Guide to Investigating Alerts

Introduction:

Threat hunting is a proactive approach to identifying and mitigating potential security threats in a network or system before they can cause harm. Cybersecurity analysts must use a variety of tools, techniques, and methods to investigate alerts, identify threats, and ensure the security of the organization's infrastructure. This document outlines the steps that a cybersecurity analyst follows when investigating alerts and includes the tools and information they use at each step.

Step 1: Alert Triaging

Purpose: The first step in threat hunting is to assess the alerts to determine their severity and relevance. Analysts must review incoming alerts from various sources such as SIEMs, intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions.

Tools and Information Used:

- **SIEM (Security Information and Event Management):**
    - **Splunk**, **IBM QRadar**, **LogRhythm**, or **Elastic Stack**: Collect, aggregate, and analyze log data from various sources (e.g., firewalls, servers, endpoint devices).
    - Use **Correlations** to identify abnormal behavior that may indicate an attack.
- **Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS):**
    - **Snort**, **Suricata**, or **Zeek**: Monitor network traffic for suspicious activity.
- **Endpoint Detection and Response (EDR):**
    - **CrowdStrike Falcon**, **Carbon Black**, **Microsoft Defender for Endpoint**: Detect suspicious behaviors on individual endpoints.
- **Alerting Thresholds and Categories:**
    - **Alert severity level (High, Medium, Low)**.
    - **Type of alert**: Suspicious login, malware detection, abnormal network traffic, etc.

Step 2: Initial Investigation and Data Collection

Purpose: After triaging the alert, analysts need to gather more data to assess the scope of the potential threat.

Tools and Information Used:

- **Network Traffic Analysis Tools:**
    - **Wireshark**, **Tshark**, or **tcpdump**: Analyze raw network traffic to detect anomalies like data exfiltration, command-and-control traffic, etc.
- **Endpoint Analysis:**
    - **Sysinternals Suite**: Check running processes, network connections, and file activity.
    - **Volatility**: Perform memory forensics to analyze the system's memory dump.

- **File Analysis:**
    - **VirusTotal**: Analyze suspicious files or URLs for known signatures of malicious activity.
    - **Cuckoo Sandbox**: Perform dynamic analysis of suspicious files in a sandbox environment.
- **Threat Intelligence Platforms:**
    - **MISP (Malware Information Sharing Platform)**, **AlienVault OTX**, **Anomali**: Use threat intelligence feeds to correlate with existing attack patterns, IPs, domains, and hashes.
- **Web Shell and C2 Server Analysis:**
    - Investigate URLs, IP addresses, and domain names flagged in the alert using DNS lookup tools or WHOIS queries.

Step 3: Correlation and Contextualization

Purpose: Contextualize the threat by correlating the alert with historical data, threat intelligence, and other indicators to determine its legitimacy and scope.

Tools and Information Used:

- **Threat Intelligence Feeds:**
    - Use external threat intelligence sources like **Anomali**, **IBM X-Force**, or **Recorded Future** to correlate and check if the identified IPs, URLs, or hashes are associated with known attack groups.
- **SIEM Correlation Rules:**
    - Leverage preconfigured correlation rules in **Splunk**, **QRadar**, or **LogRhythm** to link related events and build a clearer picture of the attack.
- **Firewall Logs and Router Logs:**
    - **Firewall (Palo Alto, Fortinet)** logs to check whether traffic originated from suspicious sources.
    - **NetFlow**, **sFlow**: Check patterns in traffic flows to identify anomalous connections.
- **System Logs (Windows/Linux logs):**
    - **Windows Event Logs**, **Syslog**: Identify any unusual login times, privilege escalation, or abnormal application behavior.
- **User Behavior Analytics (UBA):**
    - **Exabeam**, **Sumo Logic**: Detect anomalous user behavior and correlate it with other alerts (e.g., multiple failed login attempts or unusual data access).

Step 4: Incident Analysis and Threat Identification

Purpose: Once the alert is analyzed and contextualized, analysts move to identify the specific threat (e.g., malware, insider threat, DDoS attack) and understand its tactics, techniques, and procedures (TTPs).

Tools and Information Used:

- **MITRE ATT&CK Framework:**
    - Use the **MITRE ATT&CK** knowledge base to map the behavior of the threat and understand the attack vectors, lateral movement, and methods used by the adversary.
- **Malware Analysis:**
    - **PEStudio**, **Cuckoo Sandbox**, **Ghidra**, or **IDA Pro**: Static and dynamic analysis of malware to understand its behavior and objectives.
- **Behavioral Analysis:**
    - **Elastic Security** (formerly **Endgame**): Use behavioral analytics to spot abnormal patterns, such as unexpected data exfiltration or privilege escalation.
- **OSINT (Open Source Intelligence):**
    - **Shodan**, **Censys**, **HaveIBeenPwned**: Search for exposed assets, breached credentials, or vulnerabilities tied to the attack.

Step 5: Containment and Mitigation

Purpose: Once the threat has been identified, the analyst must take steps to contain and mitigate it to prevent further damage.

Tools and Information Used:

- **EDR Tools (Containment):**
    - **CrowdStrike Falcon**, **Carbon Black**: Quarantine infected endpoints, block malicious processes, or isolate affected systems from the network.
- **Firewall Configuration:**
    - **Palo Alto**, **Fortinet**, **Cisco ASA**: Block malicious IP addresses or URLs associated with the threat.
- **Network Segmentation:**
    - **VMware NSX**, **Cisco ACI**: Use network segmentation to limit the lateral movement of the attacker.
- **Application Whitelisting:**
    - Use **AppLocker** (Windows) or **OSSEC** (Linux) to block unapproved applications from running.

- **Patch Management:**
    - **WSUS** (Windows Server Update Services), **Qualys**, or **Tenable**: Apply necessary security patches to affected systems and services.

Step 6: Eradication and Recovery

Purpose: After containing the threat, analysts work to remove the malware or threat actor's presence from the environment, followed by recovery actions.

Tools and Information Used:

- **Malware Removal Tools:**
    - **Malwarebytes**, **HitmanPro**: Clean affected endpoints by removing malicious files and registry entries.
- **System Reimaging:**
    - **Acronis** or **Veeam**: Reimage compromised systems from known good backups.
- **Restore from Backup:**
    - Ensure that clean, verified backups are used to restore any lost or corrupted data from trusted sources.

Step 7: Post-Incident Analysis and Reporting

Purpose: After handling the incident, cybersecurity analysts must document the incident and review what went wrong to improve the overall security posture.

Tools and Information Used:

- **Forensic Analysis Tools:**
    - **EnCase**, **FTK**: Investigate the incident in-depth and preserve evidence for future reference or legal action.
- **Incident Report Writing:**
    - Use a template or standard for incident reporting (such as **SANS** or **NIST** guidelines) to record findings, actions, and recommendations for future improvements.
- **Root Cause Analysis (RCA):**
    - Analyze the root cause of the attack, such as an unpatched vulnerability, human error, or inadequate monitoring. Tools like **OWASP ZAP** or **Qualys** may be used to identify systemic weaknesses.
- **Threat Hunting Improvement Plans:**
    - Use lessons learned to improve hunting techniques, modify detection rules, and enhance the organization's threat response strategy.

Step 8: Continuous Improvement

Purpose: Implement improvements to prevent similar attacks in the future.

Tools and Information Used:

- **Security Awareness Training:**
    - Regular employee training sessions to mitigate human error (e.g., phishing).
- **Red/Blue Team Exercises:**
    - Use **Cobalt Strike** (Red Team) and **Mandiant** (Blue Team) to simulate attacks and improve defenses.
- **Vulnerability Management Tools:**
    - **Tenable.io**, **Qualys**, **Rapid7**: Continuously scan for vulnerabilities and patch them before they are exploited.

Example of Threat Hunting: Investigating a Potential Malware Infection

Scenario: A cybersecurity analyst receives an alert from the SIEM system indicating unusual network traffic from a workstation in the organization's internal network. The alert shows outbound communication to an external IP address that is not part of the company's known traffic. The IP address is flagged for hosting malicious activity in threat intelligence sources. The analyst decides to initiate a threat hunt to investigate the possibility of a malware infection.

Step 1: Alert Triaging

Action: The analyst begins by reviewing the alert details and initial data provided by the SIEM system.

Tools and Information Used:

- **SIEM System**: The analyst accesses **Splunk** to review the network traffic logs. The alert shows that a workstation (IP: 192.168.1.101) sent a significant amount of data to an external IP address (IP: 198.51.100.55) on port 443, which is unusual for that machine.
- **Threat Intelligence Feeds**: The IP address 198.51.100.55 is flagged by **AlienVault OTX** and **MISP** as a known malicious command-and-control server (C2 server).

The analyst recognizes the external IP address as a potential threat and decides to investigate further.

Step 2: Initial Investigation and Data Collection

Action: The analyst gathers additional data to understand the scope of the issue. They need to verify whether the suspicious traffic is related to malware.

Tools and Information Used:

- **Network Traffic Analysis**: The analyst uses **Wireshark** to capture the traffic between the affected workstation and the suspicious IP address. They observe that the workstation is sending encrypted traffic over HTTPS to the external IP. The traffic pattern is unusual, and the analyst suspects data exfiltration.
- **Endpoint Analysis**: The analyst accesses the workstation using **Microsoft Defender for Endpoint (EDR)** to gather more context on the machine's state. The EDR shows an unusual process running called update.exe in the background, which isn't part of any authorized application list.
- **VirusTotal**: The analyst submits the suspicious update.exe file to **VirusTotal** for scanning. The file is flagged as containing a known piece of malware (Trojan.Agent) associated with data theft.

Step 3: Correlation and Contextualization

Action: To understand the attack's scope and gather more information, the analyst correlates the data with other security systems and threat intelligence.

Tools and Information Used:

- **MITRE ATT&CK Framework**: The analyst maps the behavior of the malware to the **MITRE ATT&CK** framework. They identify that the malware uses **T1071** (Application Layer Protocol) for communication and **T1083** (File and Directory Discovery), which aligns with the observed behavior in the logs.
- **SIEM Correlation**: The analyst runs a query in **Splunk** to correlate network activity from the affected workstation with other systems in the network. They find that the workstation also attempted to connect to several other IP addresses in different regions, suggesting possible lateral movement or scanning behavior.
- **Threat Intelligence Platforms**: The analyst checks additional threat intelligence sources like **Anomali** and **AlienVault OTX** to confirm the malware's tactics, techniques, and procedures (TTPs) and determine whether other systems have been targeted.

Step 4: Incident Analysis and Threat Identification

Action: After collecting sufficient information, the analyst identifies that the threat is indeed a malware infection, likely a Remote Access Trojan (RAT) designed to communicate with a C2 server for instructions and potentially exfiltrate data.

Tools and Information Used:

- **Malware Analysis**: The analyst uses **Cuckoo Sandbox** to perform a dynamic analysis of the suspicious file (update.exe). The analysis reveals that the file communicates with external IP addresses, downloads additional payloads, and attempts to steal sensitive data from the workstation.

- **User Behavior Analytics**: The analyst checks the behavior of the user associated with the infected workstation in **Exabeam** and notices that the user logged in at unusual hours and accessed a large amount of data, which aligns with typical exfiltration activities.

Step 5: Containment and Mitigation

Action: The analyst now moves to contain the malware infection to prevent further damage or data exfiltration.

Tools and Information Used:

- **EDR Tool**: Using **CrowdStrike Falcon**, the analyst isolates the affected workstation from the network to prevent further communication with the C2 server. The malware is also quarantined by the EDR tool to prevent it from executing.
- **Firewall Configuration**: The analyst updates the **Palo Alto** firewall to block outbound traffic to the IP address 198.51.100.55 and other suspicious IP addresses related to the malware's C2 infrastructure.
- **Endpoint Remediation**: The analyst uses **Microsoft Defender for Endpoint** to remove the malicious process (update.exe) and any associated registry keys or persistence mechanisms.

Step 6: Eradication and Recovery

Action: The analyst begins the process of eradicating the malware and restoring the workstation to a safe state.

Tools and Information Used:

- **Malware Removal**: The analyst uses **Malwarebytes** to perform a full scan on the affected workstation and ensures all traces of the malware are removed.
- **System Reimaging**: As an extra precaution, the analyst reimages the workstation using a clean system image and restores necessary files from known good backups.
- **Patch Management**: The analyst ensures that the latest security patches are applied to the workstation, as the malware exploited an unpatched vulnerability.

Step 7: Post-Incident Analysis and Reporting

Action: The analyst documents the findings of the investigation and provides a detailed report on the incident to the security team.

Tools and Information Used:

- **Forensic Tools**: The analyst uses **EnCase** to gather forensic evidence and preserves logs for potential legal or compliance needs.
- **Incident Reporting**: The analyst prepares an incident report using **SANS** guidelines, documenting the timeline of events, the threat identification process, actions taken, and recommendations for preventing future incidents.
- **Root Cause Analysis**: The analyst conducts a **root cause analysis** to determine that the malware was able to infiltrate the system through a phishing email, which led to the execution of the update.exe file. They recommend improved phishing awareness training and the implementation of stronger email filtering.

Step 8: Continuous Improvement

Action: Based on the lessons learned from the incident, the analyst recommends improvements to the organization's overall security posture.

Tools and Information Used:

- **Security Awareness Training**: The analyst recommends additional **phishing simulation exercises** for employees to reduce the risk of future social engineering attacks.
- **Red/Blue Team Exercises**: The analyst suggests running regular **Red Team** exercises using **Cobalt Strike** to simulate attacks and improve the organization's detection and response capabilities.
- **Vulnerability Management**: The analyst uses **Qualys** to ensure that the entire network is regularly scanned for vulnerabilities and that security patches are applied promptly.

Conclusion:

By following a structured threat hunting process, the cybersecurity analyst successfully identified, contained, and remediated a malware infection on a workstation. The proactive steps taken ensured that the attack was stopped before it could spread or cause significant damage. Additionally, the analyst's efforts to report and analyze the incident contributed to strengthening the organization's security posture, reducing the likelihood of similar attacks in the future.