SECURITY ALERT MONITORING AND INCIDENT RESPONSE

REPORT BY: AKSHITA SHARMA

INTRODUCTION

This report details the analysis of simulated security alerts and logs as part of the "Security Alert Monitoring & Incident Response" task for the Future Interns Cyber Security program. The objective of this task is to monitor security alerts, identify suspicious activities, classify incidents, and draft a comprehensive incident response report. The logs analyzed were sourced from

SOC_Task2_Sample_Logs.txt and Windows Event Logs on the host AKSHITASHA2006. The primary tools utilized for this analysis were Splunk (for log ingestion, search, and analysis) and the provided sample log files. This report outlines the identified security incidents, their classifications, and recommended remediation strategies. Multiple security incidents were identified, including malware infections (Trojan, Spyware, Ransomware Behaviour, Worm), suspicious file access attempts, and a successful login after a connection attempt. Immediate remediation actions are recommended to contain and eradicate these threats.

INCIDENTS

Incident 1: Trojan Malware Detected

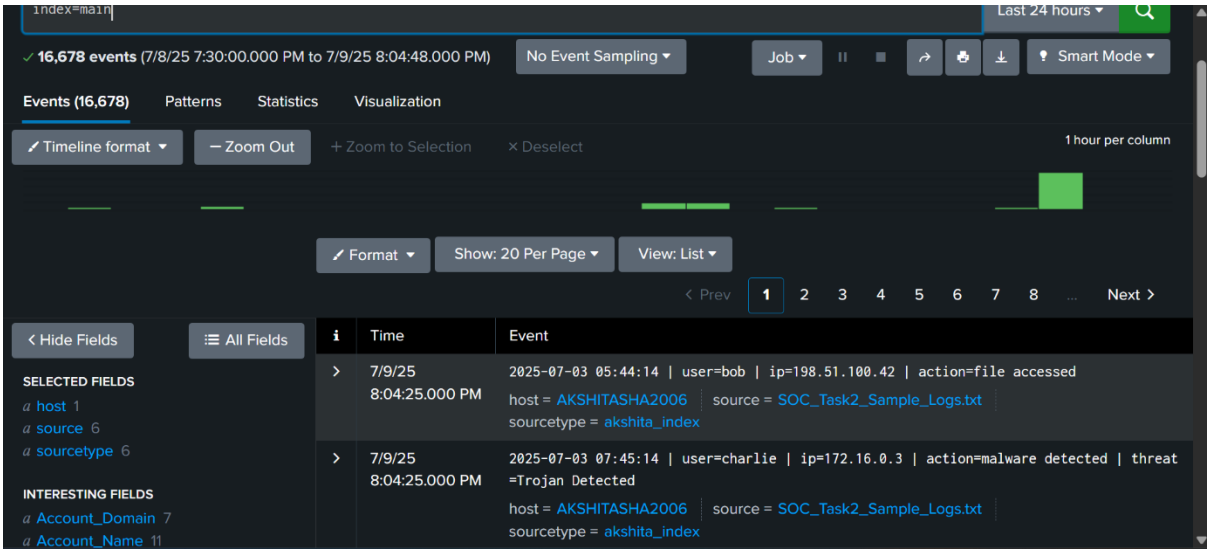
- **Incident Title:** Trojan Malware Detected on Host AKSHITASHA2006
- **Date and Time Detected:** 2025-07-03 07:45:14
- **Source(s) of Alert:** SOC_Task2_Sample_Logs.txt
- **Description of Activity:** An event was logged indicating that malware, specifically a "Trojan Detected", was found on host=AKSHITASHA2006. The alert is associated with

user=charlie from ip=172.16.0.3.

  - **Relevant Log Entry:** 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat =Trojan Detected host=AKSHITASHA2006 source=SOC_Task2_Sample_Logs.txt sourcetype=akshita_index

- **Affected Systems/Users:** Host: AKSHITASHA2006, User: charlie
- **Incident Classification:**
  - **Type:** Malware Infection
  - **Severity:** High (Direct threat to system integrity and data confidentiality)
- **Analysis:** The explicit "Trojan Detected" alert is a clear indication of a malicious executable or script attempting to or having already compromised the system. Trojans can lead to backdoor access, data theft, or further compromise of the system.
- **Remediation Recommendations:**
  1. **Containment:** Immediately isolate AKSHITASHA2006 from the network to prevent further spread or data exfiltration.
  2. **Eradication:** Perform a full antivirus/anti-malware scan on AKSHITASHA2006. Manually remove any identified malicious files. Consider reimaging the system if the compromise is deep.

3. **Investigation:** Investigate user=charlie's account for signs of compromise (e.g., weak password, suspicious activities).
4. **Prevention:** Update antivirus definitions, ensure all system patches are applied, and review endpoint detection and response (EDR) configurations. Educate users on safe Browse and email practices.

- 

Incident 2: Multiple Malware Infections (Spyware, Ransomware, Worm)

- **Incident Title:** Multiple Malware Detections on Host AKSHITASHA2006
- **Date and Time Detected:**

    - 2025-07-03 04:41:14 (Spyware)
    - 2025-07-03 09:10:14 (Ransomware Behaviour)
    - 2025-07-03 05:05:14 (Worm Infection Attempt)
- **Source(s) of Alert:** SOC_Task2_Sample_Logs.txt
- **Description of Activity:** Multiple distinct malware detection events were observed on host=AKSHITASHA2006:
    - A "Spyware Alert" associated with

user=alice from ip=172.16.0.3.

    - "Ransomware Behavior" detected, associated with

user=bob from ip=172.16.0.3.

    - A "Worm Infection Attempt" associated with

user=bob from ip=203.0.113.77.

    - **Relevant Log Entries:**

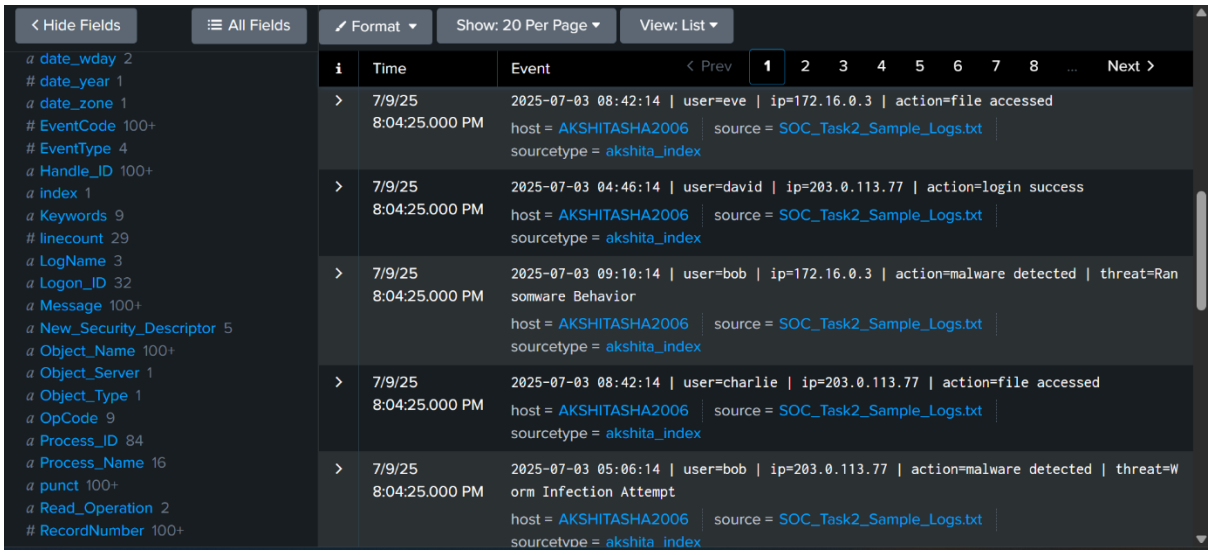
    - 2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert host=AKSHITASHA2006 source=SOC_Task2_Sample_Logs.txt sourcetype=akshita_index
    - 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior host=AKSHITASHA2006 source=SOC_Task2_Sample_Logs.txt sourcetype=akshita_index
    - 2025-07-03 05:05:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt host=AKSHITASHA2006 source=SOC_Task2_Sample_Logs.txt sourcetype=akshita_index
- **Affected Systems/Users:** Host: AKSHITASHA2006, Users: alice, bob
- **Incident Classification:**

    - **Type:** Multiple Malware Infections (Spyware, Ransomware, Worm)
    - **Severity:** Critical (Indicates a highly compromised system with various active and attempted malware types, posing severe risk to data integrity, confidentiality, and availability).
- **Analysis:** The detection of multiple types of malware (spyware, ransomware, and a worm) indicates a significant and widespread compromise on AKSHITASHA2006. This suggests either a highly persistent threat, multiple infection vectors, or a system that is severely outdated in terms of security. The presence of ransomware behavior is particularly concerning due to potential data loss.
- **Remediation Recommendations:**
    1. **Containment:** Immediately isolate AKSHITASHA2006 from the network.
    2. **Eradication:** The presence of multiple malware types strongly suggests a

complete system wipe and reinstallation is necessary. A full forensics analysis may be required if data breach is suspected.

3. **Investigation:** Investigate the initial infection vector. Check for other compromised systems on the network. Review alice and bob's activities and accounts for further compromise.

4. **Prevention:** Implement stringent email and web filtering. Deploy advanced endpoint protection solutions. Conduct regular vulnerability assessments and penetration testing. Strengthen user awareness training for phishing and suspicious links.

- 

Incident 3: Suspicious File Access

- **Incident Title:** Suspicious File Access on Host AKSHITASHA2006
- **Date and Time Detected:**
  - 2025-07-03 05:44:14
  - 2025-07-03 07:22:14
  - 2025-07-03 08:42:14
  - 2025-07-03 08:31:14
  - 2025-07-03 09:10:14
- **Source(s) of Alert:** SOC_Task2_Sample_Logs.txt
- **Description of Activity:** Multiple instances of action=file accessed were observed from different users and IP addresses on AKSHITASHA2006:
  - user=bob from ip=198.51.100.42 at 2025-07-03 05:44:14.
  - user=alice from ip=203.0.113.77 at 2025-07-03 07:22:14.

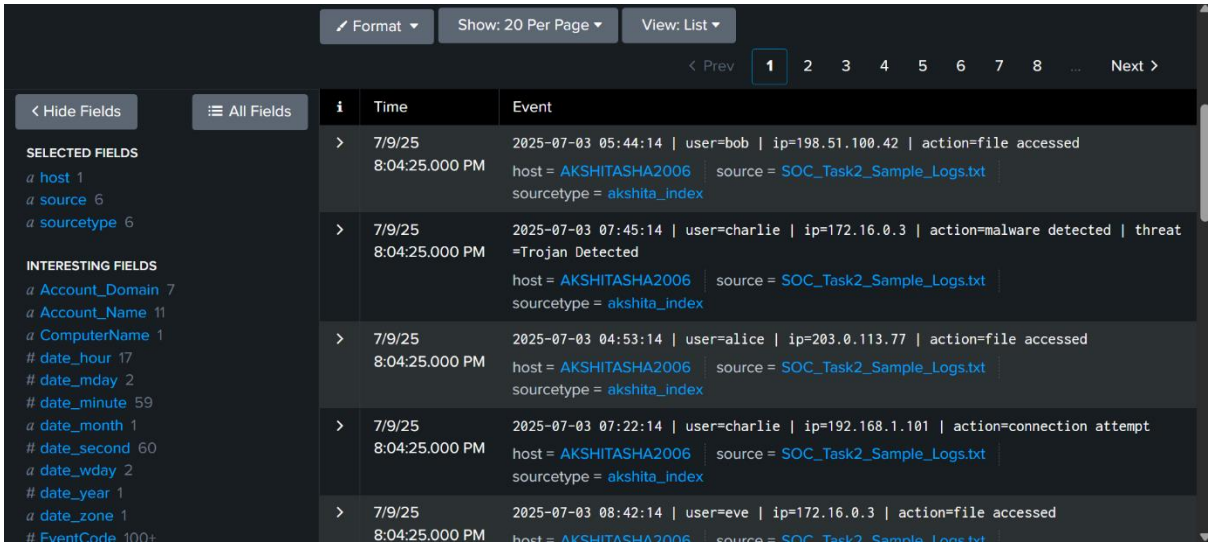
    - user=eve from ip=172.16.0.3 at 2025-07-03 08:42:14.
    - user=eve from ip=203.0.113.77 at 2025-07-03 08:31:14.
    - user=bob from ip=198.51.100.42 at 2025-07-03 09:10:14.
- **Affected Systems/Users:** Host: AKSHITASHA2006, Users: bob, alice, eve
- **Incident Classification:**
    - **Type:** Unauthorized Access / Data Access Anomaly
    - **Severity:** Medium (Requires further investigation to determine if access was legitimate or malicious, especially given other malware detections).
- **Analysis:** While "file accessed" events are common, their correlation with malware detections and multiple users/IPs warrants investigation. It's unclear what files were accessed, which is critical for determining the severity. The repeated access by

user=bob from ip=198.51.100.42 and user=eve from different IPs requires verification.

- **Remediation Recommendations:**
    1. **Investigation:**
        - Determine if the file accessed events were legitimate actions by the respective users (bob, alice, eve).
        - Identify the specific files or directories that were accessed.
        - Verify the source IP addresses. Are these internal IPs, or external/VPN connections?
        - Check for any other unusual activities by these users around the time of file access.
    2. **Access Control Review:** Review file system permissions and ensure they are appropriately configured (least privilege).
    3. **User Account Security:** If any user account is suspected of compromise, force

password resets and implement multi-factor authentication.

4. **Monitoring:** Enhance monitoring for unusual file access patterns, especially for sensitive data.

- 

Incident 4: Connection Attempt Followed by Login Success

- **Incident Title:** Suspicious Connection and Login on Host AKSHITASHA2006
- **Date and Time Detected:**
  - Connection Attempt: 2025-07-03 07:36:14
  - Login Success: 2025-07-03 07:46:14

- **Source(s) of Alert:** SOC_Task2_Sample_Logs.txt
- **Description of Activity:** A connection attempt was initiated by user=david from ip=10.0.0.5 at 2025-07-03 07:36:14. Approximately 10 minutes later, a

login success event was recorded for user=bob from the *same* ip=10.0.0.5 at 2025-07-03 07:46:14.

    - **Relevant Log Entries:**
        - 2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt host=AKSHITASHA2006 source=SOC_Task2_Sample_Logs.txt sourcetype=akshita_index
        - 2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success host=AKSHITASHA2006 source=SOC_Task2_Sample_Logs.txt sourcetype=akshita_index
- **Affected Systems/Users:** Host: AKSHITASHA2006, Users: david, bob
- **Incident Classification:**

    - **Type:** Potential Unauthorized Access / Account Compromise
    - **Severity:** Medium (Requires clarification; if david and bob are the same person or david is authorized to attempt connection and bob to log in from that IP, it might be benign. If not, it's highly suspicious.)
- **Analysis:** The sequential connection attempt by david and login success by bob from the same internal IP (10.0.0.5) within a short timeframe is suspicious. This could indicate an attempt to gain access to the system. It's unclear if

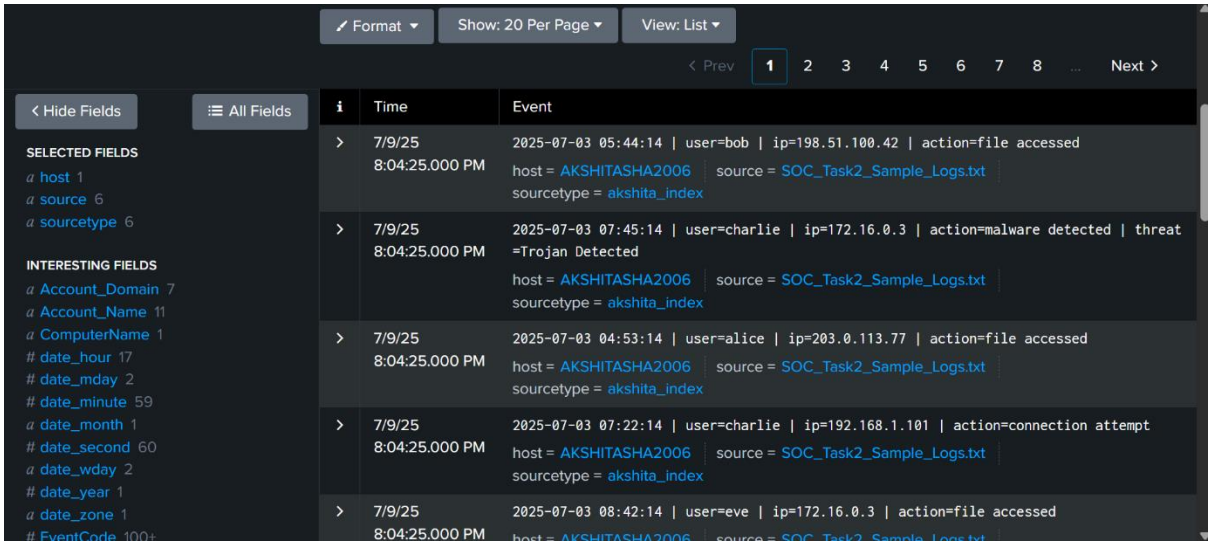
david and bob are related users or if david represents an initial probe that led to bob's successful login, possibly through credential stuffing or a different attack vector.

- **Remediation Recommendations:**

1. **Investigation:**
    - Verify the legitimacy of the connection attempt by user=david from 10.0.0.5.

- Confirm if user=bob's login from 10.0.0.5 at that specific time was legitimate and authorized.
- Check user=david's activity logs prior to the connection attempt.
- Review AKSHITASHA2006's authentication logs for any failed login attempts between the connection attempt and successful login.

2. **Account Review:** If suspicious, force password resets for both david and bob's accounts.
3. **Network Monitoring:** Enhance monitoring for unusual connection attempts and subsequent successful logins, especially from internal IPs.

- 

Tools Used:

- Splunk (for log ingestion, search, and analysis)
- Sample log files:

  SOC_Task2_Sample_Logs.txt

Conclusion:

The identified incidents highlight significant security vulnerabilities on AKSHITASHA2006. Prompt execution of the recommended remediation actions is essential for containing the threats, restoring system integrity, and strengthening defenses against future cyberattacks. This task

reinforced critical skills in security monitoring and incident response.