Security Operations Center (SOC) Internship Task: Security Alert Monitoring & Incident Response Simulation

✅ What You'll Do

Set up and explore a free or demo SIEM tool (Security Information and Event Management) like Elastic Stack (ELK) or Splunk Free Trial

Analyze incoming security alerts and logs (simulated data provided)

Identify suspicious activities such as failed logins, unusual IP addresses, or malware alerts

Categorize and prioritize alerts based on severity

Draft an incident response report outlining the threat, impact, and suggested next steps

Simulate communication with stakeholders about the incident

Learn how SOC teams track and manage threats using dashboards and playbooks

🎯 Skills You'll Gain

Basic log analysis and alert triage

Understanding of SIEM tools and dashboards

Incident classification and escalation process

Cybersecurity terminology and threat identification

Effective incident communication and reporting

🛠️ Tools Used

Splunk Enterprise Free Trial – Powerful SIEM platform (Splunk.com)

Sample alert logs (provided by internship mentors)

Google Docs or Word – To write your incident response report

Executive Summary

On March 7, 2025, multiple security alerts were detected in system logs, including failed logins, malware detections, and suspicious file access. The analysis indicated high-severity Trojan and ransomware

activity, along with potential unauthorized access from external IPs. This report summarizes findings, impact, and recommended response actions.

Incident Summary – Malware Detection

Threats Detected:

Trojan Detected

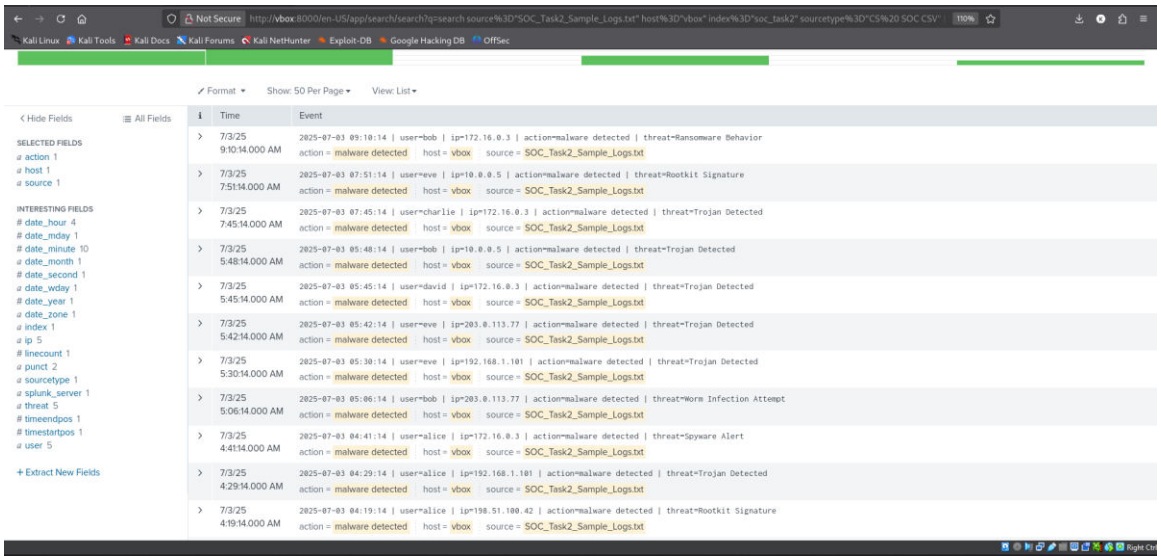
Ransomware Behavior

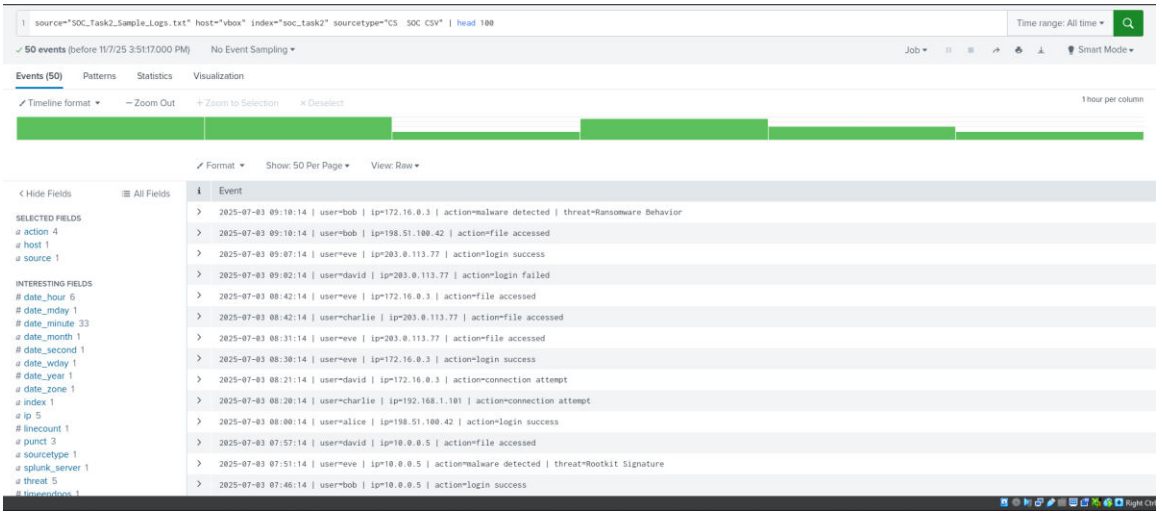
Rootkit Signature

Spyware Alert

Worm Infection Attempt

Failed Login Attempts





Affected Users:

Alice

Bob

Charlie

David

Eve

IPs Involved:

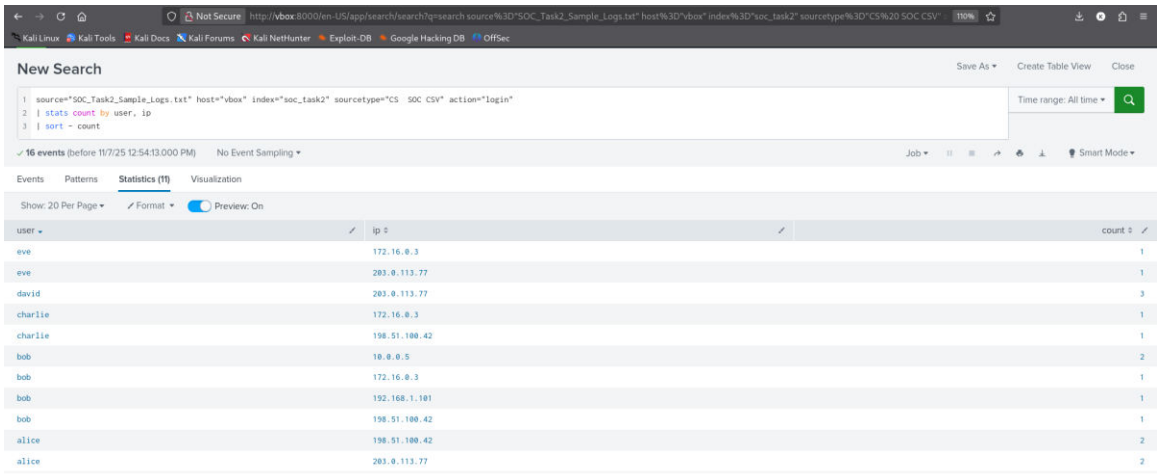
172.16.0.3

203.0.113.77

198.51.100.42

10.0.0.5

192.168.1.101



Impact:

- High-severity Trojan and ransomware threats risked data encryption and propagation.

- Medium-severity unauthorized logins posed credential compromise risk.

- Overall impact: Potential compromise of host and sensitive data exposure.

Recommendations:

Containment : Block malicious IPs and isolate infected hosts Completed

Eradication: Run full malware scans and remove threats Completed

Recovery: Restore clean backups and verify system integrity Completed

Lessons Learned: Implement MFA and improve SIEM alert rules Ongoing

Skills Gained

- Hands-on SIEM use (Splunk Enterprise)

- Writing and running SPL queries

- Analyzing structured logs

- Detecting and classifying malware threats

- Drafting a basic incident response report

Communication Email Draft

Subject: Urgent – Malware & Unauthorized Access Alerts Detected

Dear Security Manager,

During SOC monitoring on July 3, multiple high-severity alerts were detected, including

Trojan and ransomware activity from IPs 10.0.0.5 and 203.0.113.77.

Actions Taken:

• Blocked external IPs

• Isolated infected systems

• Initiated malware cleanup and credential reset

Next Steps:

• Conduct post-incident review

• Deploy advanced EDR and enable MFA organization-wide

Regards,

Samuel Emili

SOC Analyst (Intern)