

## 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

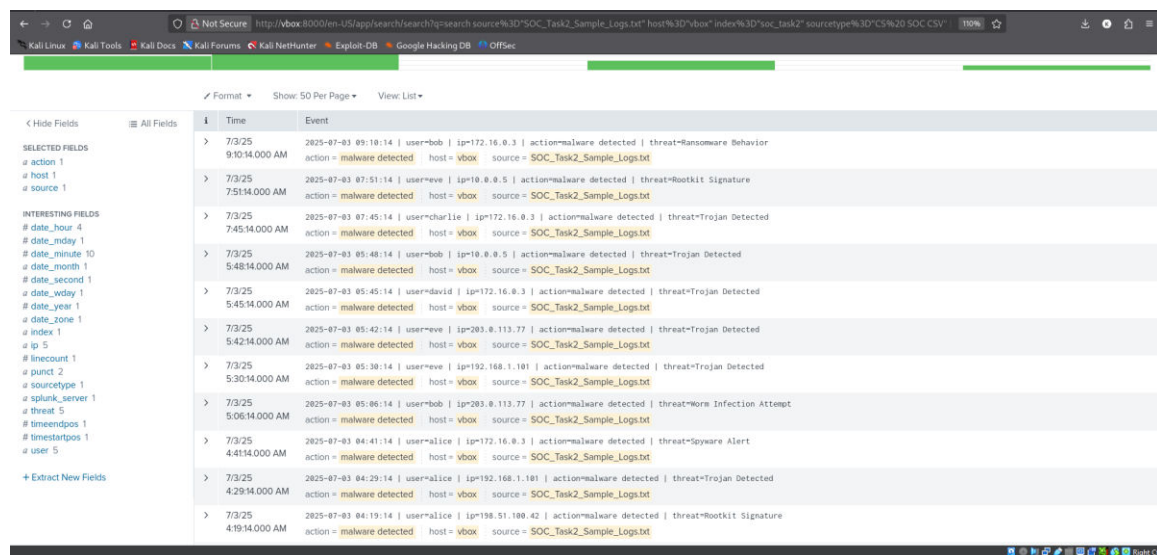
Ransomware Behavior

Rootkit Signature

Spyware Alert

Worm Infection Attempt

Failed Login Attempts



	Time	Event
	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=veve   ip=10.8.0.5   action=malware detected   threat=Rootkit Signature action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14   user=bob   ip=10.8.0.5   action=malware detected   threat=Trojan Detected action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14   user=dauid   ip=172.16.0.3   action=malware detected   threat=Trojan Detected action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14   user=veve   ip=203.8.113.77   action=malware detected   threat=Trojan Detected action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14   user=veve   ip=192.168.1.101   action=malware detected   threat=Trojan Detected action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14   user=bob   ip=203.8.113.77   action=malware detected   threat=Worm Infection Attempt action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14   user=alice   ip=172.16.0.3   action=malware detected   threat=Spyware Alert action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 4:29:14.000 AM	2025-07-03 04:29:14   user=alice   ip=192.168.1.101   action=malware detected   threat=Trojan Detected action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt
	7/3/25 4:19:14.000 AM	2025-07-03 04:19:14   user=alice   ip=198.51.100.42   action=malware detected   threat=Rootkit Signature action = malware detected host = vbox source = SOC_Task2_Sample_Logs.txt



The screenshot shows a Splunk search interface with the following query: `source="SOC_Task2_Sample_Logs.txt" host="vbox" index="soc_task2" sourcetype="CS SOC CSV" action="login"`. The results are displayed in a table with 16 events. The table has columns for user, ip, and count.

user	ip	count
eve	172.16.0.3	1
eve	203.0.113.77	1
david	203.0.113.77	3
charlie	172.16.0.3	1
charlie	198.51.100.42	1
bob	10.0.0.5	2
bob	172.16.0.3	1
bob	192.168.1.101	1
bob	198.51.100.42	1
alice	198.51.100.42	2
alice	203.0.113.77	2

## 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)***