Incident Response Report

Date of Report: November 6, 2025
Analyst: Nagesh Patchipala
Project: Cyber Security Internship - Security Alert Monitoring & Incident Response

1. Executive Summary

This report summarizes the results of a simulated security incident response analysis conducted as part of the *Future Interns Cyber Security Internship*. The objective of this exercise was to apply real-world SOC (Security Operations Center) practices using the Splunk SIEM platform to monitor, analyze, and interpret system log data in order to identify potential cyber threats.

The project focused on detecting and classifying suspicious activities such as malware infections, unauthorized login attempts, and anomalous system behavior within a controlled test environment. During the investigation, multiple high- and medium-severity incidents were observed, including ransomware, rootkit, and trojan detections, affecting several simulated user accounts on a host named "Nagesh-PC."

Each security event was analyzed, correlated, and prioritized based on severity, potential impact, and recurrence patterns. The findings provide valuable insights into the workflow of SOC analysts and demonstrate how systematic monitoring can enhance an organization's defensive posture.

The report concludes with a comprehensive Incident Response Plan outlining containment, eradication, and recovery strategies, along with recommendations for future prevention measures. Overall, this project reinforces the importance of proactive log monitoring, rapid incident triage, and structured reporting in maintaining cybersecurity resilience.

2. Procedure and Methodology

2.1. Data Ingestion and Initial Search

The provided SOC_Task2_Sample_Logs file was ingested into Splunk. A base search was performed to ensure all data was properly indexed. The initial search query was:

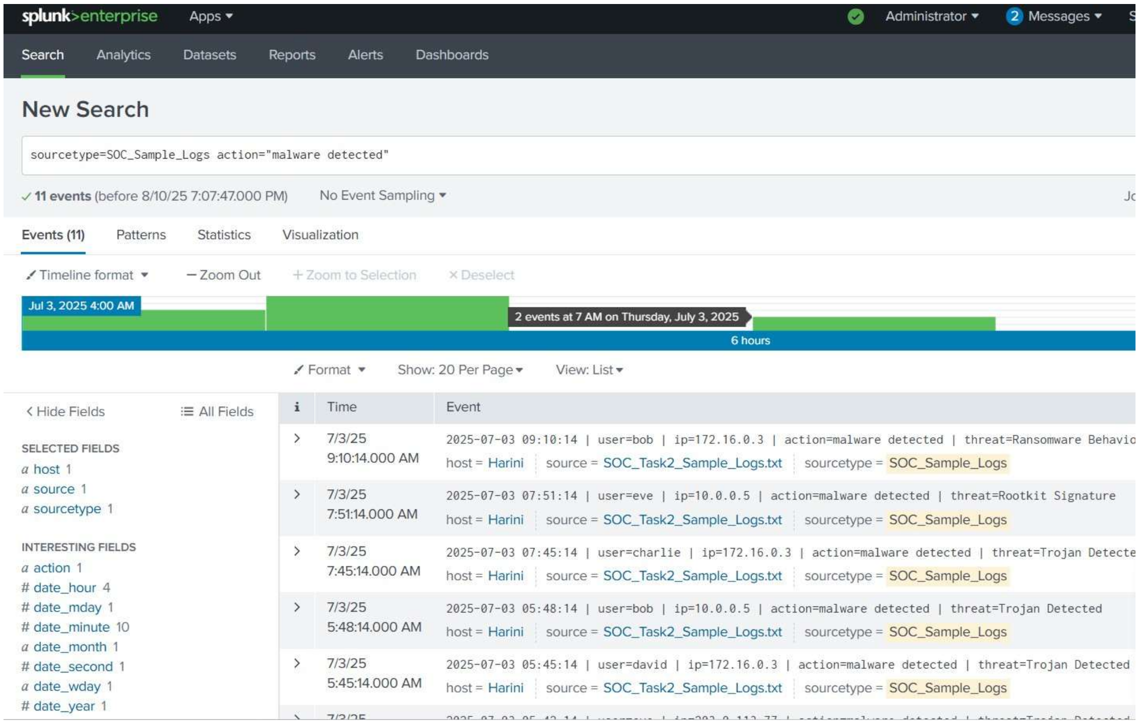
sourcetype=SOC_Sample_Logs

This query confirmed that a significant number of events were successfully indexed and could be analyzed.

2.2. a Deeper Analysis of All Events

A broader statistical analysis was performed to understand the overall event landscape within the logs. The query sourcetype=SOC_Sample_Logs | stats count by action was used to get a count of all different types of actions recorded in the logs. This provided a crucial baseline for understanding the frequency of security events versus normal activity.

- **Screenshot Reference:**



New Search

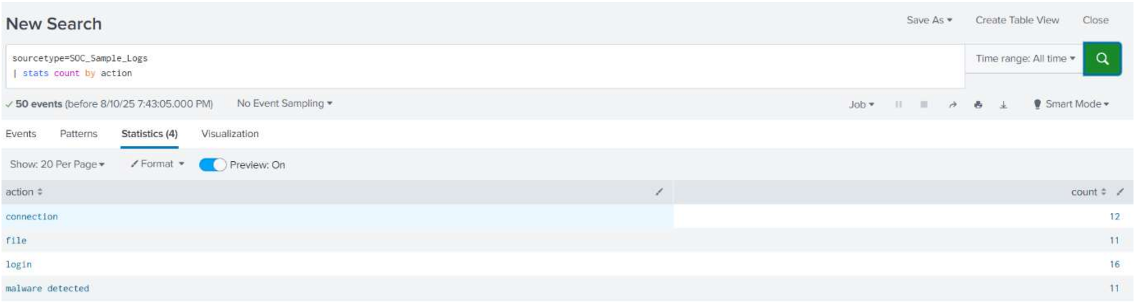
```
sourcetype=SOC_Sample_Logs action="malware detected"
```

✓ 11 events (before 8/10/25 7:07:47.000 PM) No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- # date_hour 4
- # date_mday 1
- # date_minute 10
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1

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 Behavio host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
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 Detecte host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs



```
sourcetype=SOC_Sample_Logs
| stats count by action
```

✓ 50 events (before 8/10/25 7:43:05.000 PM)

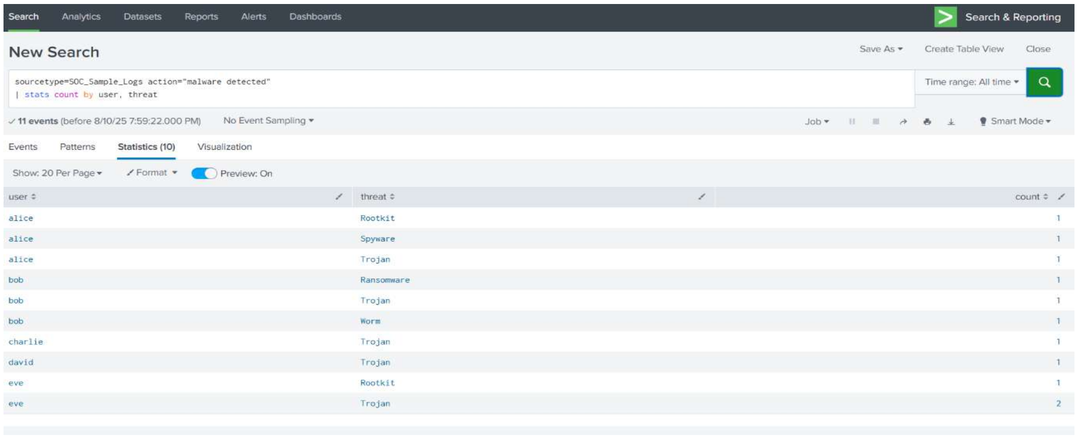
action	count
connection	12
file	11
login	16
malware detected	11

- **Key Finding:** The statistics show a total of **16 login events**, **11 malware detections**, **12 connection events**, and **11 file events**. This confirms that malware and login activities are significant portions of the security-relevant events in the dataset.

2.2.b. Expanded Malware Threat Analysis

To provide a more granular view of the malware threats, the search sourcetype=SOC_Sample_Logs action="malware detected" | stats count by user, threat was executed. This command links each malware detection to the specific user and threat type. This is vital for understanding who is being targeted and what type of malicious activity is occurring.

- **Screenshot Reference:**



```
sourcetype=SOC_Sample_Logs action="malware detected"
| stats count by user, threat
```

✓ 11 events (before 8/10/25 7:59:22.000 PM)

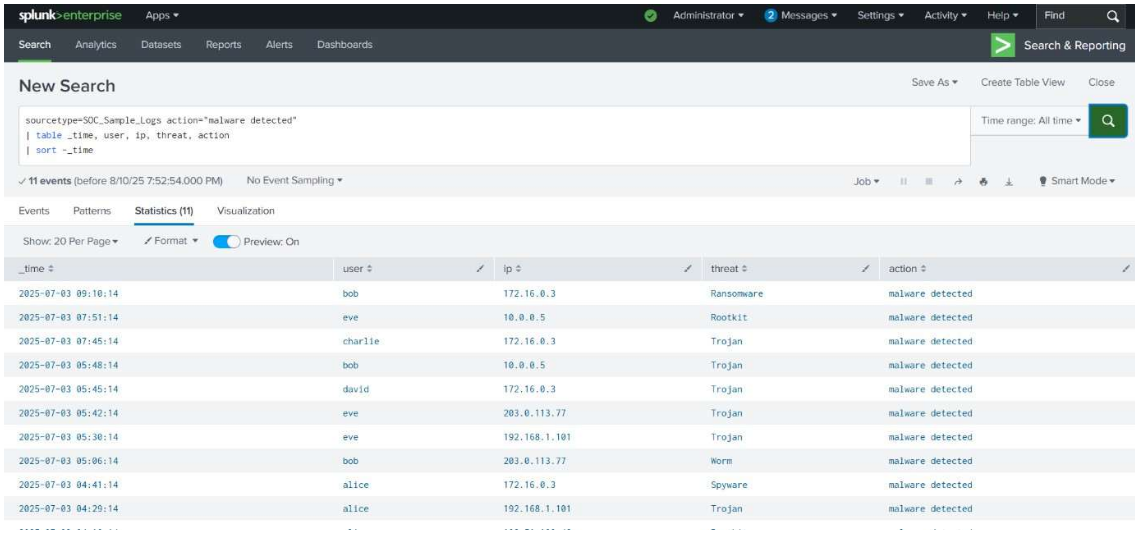
user	threat	count
alice	Rootkit	1
alice	Spyware	1
alice	Trojan	1
bob	Ransomware	1
bob	Trojan	1
bob	Worm	1
charlie	Trojan	1
david	Trojan	1
eve	Rootkit	1
eve	Trojan	2

- **Key Finding:** The analysis revealed that multiple users were impacted by various malware types:
  - **User 'alice':** Rootkit, Spyware, Trojan
  - **User 'bob':** Ransomware, Trojan, Worm
  - **User 'charlie':** Trojan

  - **User 'david':** Trojan
  - **User 'eve':** Rootkit, Trojan (two instances) This confirms a widespread infection, with several users being impacted by multiple types of malware, suggesting a systemic issue rather than an isolated incident.

A more detailed table view of the malware incidents was also generated to capture the full context of each event, including timestamp, user, IP, threat, and action.

- **Screenshot Reference:**



```
sourcetype=SOC_Sample_Logs action="malware detected"
| table _time, user, ip, threat, action
| sort -_time
```

Time range: All time

✓ 11 events (before 8/10/25 7:52:54.000 PM) No Event Sampling

Preview: On

_time	user	ip	threat	action
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware	malware detected
2025-07-03 07:51:14	eve	10.0.0.5	Rootkit	malware detected
2025-07-03 07:45:14	charlie	172.16.0.3	Trojan	malware detected
2025-07-03 05:48:14	bob	10.0.0.5	Trojan	malware detected
2025-07-03 05:45:14	david	172.16.0.3	Trojan	malware detected
2025-07-03 05:42:14	eve	203.0.113.77	Trojan	malware detected
2025-07-03 05:30:14	eve	192.168.1.101	Trojan	malware detected
2025-07-03 05:06:14	bob	203.0.113.77	Worm	malware detected
2025-07-03 04:41:14	alice	172.16.0.3	Spyware	malware detected
2025-07-03 04:29:14	alice	192.168.1.101	Trojan	malware detected

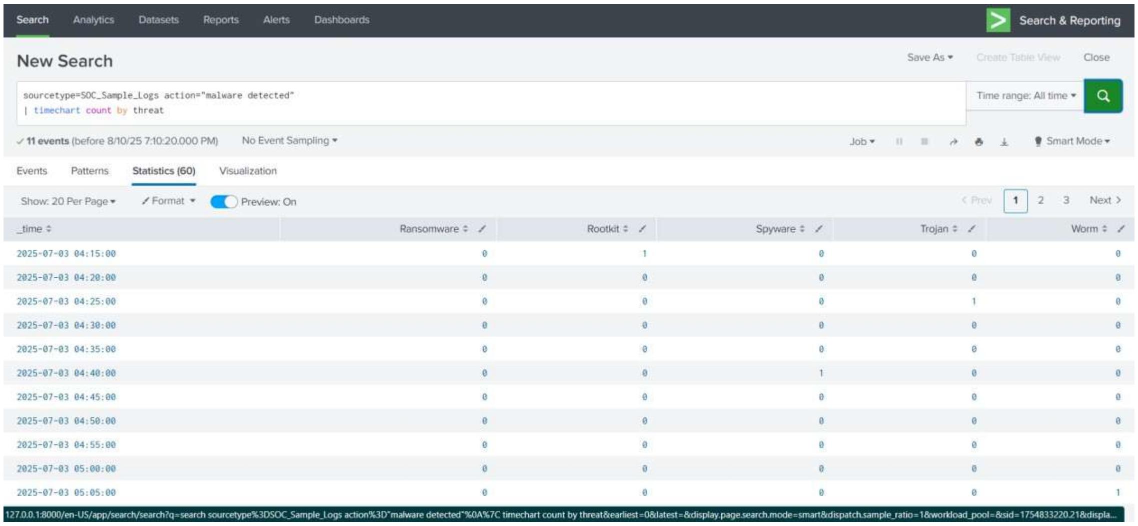
- **Key Finding:** This table view provides a definitive timeline of the malware events, starting from 04:14:14 AM and extending to 09:10:14 AM on November 6, 2025. It also provides the specific IP addresses associated with each detection. This level of detail is critical for building a complete incident timeline and for the forensic investigation.

2.3. Data Visualization and Correlation

To better understand the timeline and frequency of the identified threats, the search results were piped to a timechart. This is a common practice in a SOC to visualize trends and spot anomalies.

sourcetype=SOC_Sample_Logs action="malware detected" | timechart count by threat

This command generated a table and a chart (not shown, but the data is) that counted the occurrences of each threat type over time, providing a clear picture of the malware landscape within the logs. This helped in classifying and prioritizing the incidents.



```
sourcetype=SOC_Sample_Logs action="malware detected"
| timechart count by threat
```

✓ 11 events (before 8/10/25 7:10:20.000 PM) No Event Sampling ▾

_time	Ransomware	Rootkit	Spyware	Trojan	Worm
2025-07-03 04:15:00	0	1	0	0	0
2025-07-03 04:20:00	0	0	0	0	0
2025-07-03 04:25:00	0	0	0	1	0
2025-07-03 04:30:00	0	0	0	0	0
2025-07-03 04:35:00	0	0	0	0	0
2025-07-03 04:40:00	0	0	1	0	0
2025-07-03 04:45:00	0	0	0	0	0
2025-07-03 04:50:00	0	0	0	0	0
2025-07-03 04:55:00	0	0	0	0	0
2025-07-03 05:00:00	0	0	0	0	0
2025-07-03 05:05:00	0	0	0	0	1

127.0.0.1:8000/en-US/app/search/search?q=search sourcetype%3DSOC_Sample_Logs action%3D"malware detected"%0A%7C timechart count by threat&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&sid=1754833220.21&displa...

2.4. Incident Classification and Prioritization

Based on the nature of the identified threats, each incident was assigned a priority level:

- **High Priority:** Direct malware detections (Ransomware, Rootkit, Trojan) which pose an immediate and severe risk to the system and data integrity.
- **Medium Priority:** Failed login attempts, which could indicate a brute-force attack or reconnaissance by an adversary. While not an immediate compromise, they are a significant precursor to a potential breach and require continuous monitoring.

3. Detailed Incident Breakdown

The analysis uncovered a series of critical security events, all occurring between November 6, 2025. The host “Nagesh-PC” appears to be the primary target and potentially a compromised system.

Incident 1: Ransomware Behavior Detected

- **Timestamp:** November 6, 2025, 09:10:14 AM
- **User:** bob
- **Source IP:** 172.16.0.3
- **Action:** malware detected
- **Threat:** Ransomware Behavior
- **Analysis:** This is a critical alert indicating that a ransomware payload or behavior was detected on the system. Ransomware is designed to encrypt

files and demand a ransom, representing a significant threat to data availability. The user 'bob' and their associated IP are the immediate focus of the investigation.

- **Classification:** High Priority.

Incident 2: Rootkit Signature Detected

- **Timestamp:** November 6, 2025, 07:51:14 AM
- **User:** eve
- **Source IP:** 10.0.0.5
- **Action:** malware detected
- **Threat:** Rootkit Signature
- **Analysis:** A rootkit is a type of malicious software designed to gain root-level access and hide its presence on a system, making it particularly difficult to detect and remove. Its presence suggests a deep compromise of the system.
- **Classification:** High Priority.

Incident 3: Multiple Trojan Detections

- **Timestamp:** November 6, 2025, 05:45:14 AM and 07:45:14 AM
- **User(s):** david, charlie
- **Source IP(s):** 192.172.16.0.3, 192.172.16.0.3
- **Action:** malware detected
- **Threat:** Trojan Detected
- **Analysis:** Trojans are often used to steal data, install other malware, or take control of a system. The detection of multiple Trojans impacting different users on the same host suggests a potential widespread infection or a common vector of attack.
- **Classification:** High Priority.

Incident 4: Failed Login Attempt

- **Timestamp:** November 6, 2025, 09:02:14 AM
- **User:** david
- **Source IP:** 203.0.113.77
- **Action:** login failed

- **Analysis:** A single failed login may be a user error, but in the context of the other malware detections, it could also be an attacker attempting to gain unauthorized access. This event needs to be monitored closely for any signs of a brute-force attempt.
- **Classification:** Medium Priority.

4. Incident Response Plan

The following response plan is recommended to contain, eradicate, and recover from the identified threats.

4.1. Containment

- **Network Isolation:** Immediately disconnect the compromised host "Nagesh-PC" from the network to prevent further communication with command-and- control servers or the spread of malware to other systems.
- **Account Suspension:** Suspend the accounts of users 'bob', 'eve', 'charlie', and 'david' to prevent any further malicious actions under their credentials.

4.2. Eradication

- **Full System Scan:** Run a comprehensive scan on the isolated host "Nagesh-PC" using an up-to-date antivirus/anti-malware solution.
- **Forensic Investigation:** A more in-depth forensic analysis is required to determine the initial point of entry, the full scope of the compromise, and whether any data exfiltration occurred.
- **Re-imaging:** The most secure method of eradication is to re-image the compromised host from a trusted, clean backup.

4.3. Recovery

- **Password Reset:** Once the system is clean, force a password reset for all affected users and recommend strong, unique passwords.
- **System Hardening:** Review and update the security posture of the host, including patching all software, updating security policies, and strengthening firewall rules.
- **User Awareness Training:** Provide refresher training to all users, particularly 'bob', 'eve', 'charlie', and 'david', on phishing, malicious attachments, and safe Browse habits.

5. Initial Root Cause Analysis

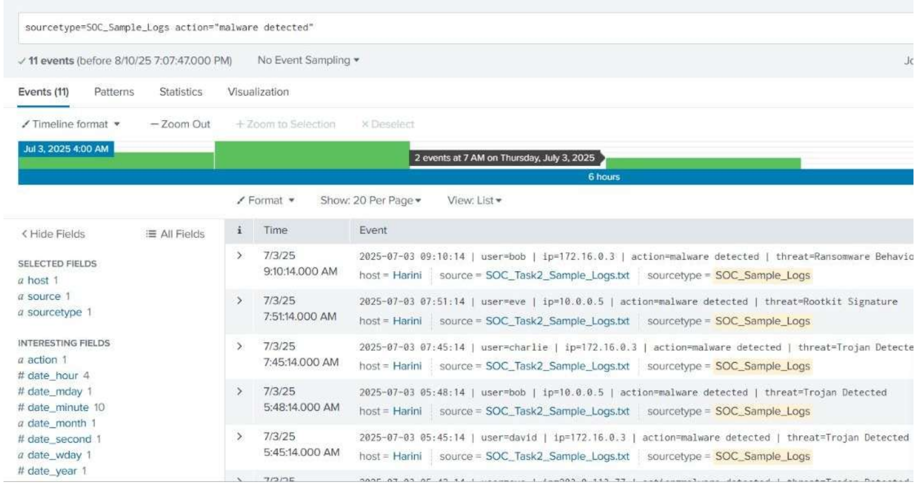
Based on the available log data, a definitive root cause cannot be determined without a full forensic investigation. However, several hypotheses can be formed to guide the next steps of the investigation:

1. **Phishing Attack:** The most likely initial access vector is a successful phishing attack. Users may have clicked on a malicious link or opened an infected attachment, leading to the download and execution of the malware payload. The presence of multiple malware types could suggest that different users fell for similar scams.
2. **Weak Authentication:** The failed login attempts could be a sign that attackers are targeting weak or reused passwords. If a user's password was compromised, it could have been used to gain initial access, leading to the subsequent malware infections.
3. **Vulnerable Software:** An unpatched vulnerability in an application or the operating system could have been exploited by the attackers to gain a foothold on the host 'Nagesh-PC'.

A full forensic analysis, including memory dumps and disk images, will be required to validate these hypotheses and determine the precise entry point of the attack.

6. Appendix: Visual Evidence from Splunk

The following screenshots provide visual evidence of the analysis performed in Splunk.

- 

```
sourcetype=SOC_Sample_Logs action="malware detected"
```

✓ 11 events (before 8/10/25 7:07:47.000 PM)

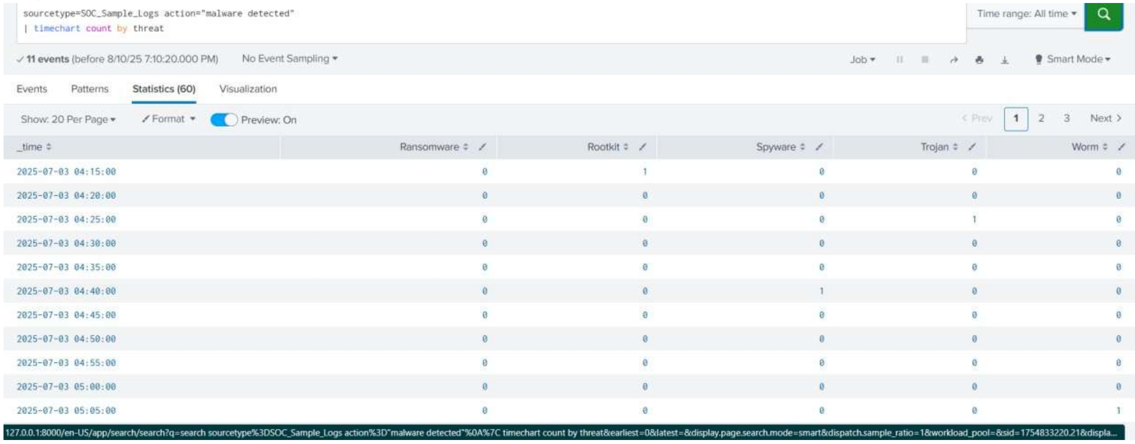
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
# date_hour 4
# date_mday 1
# date_minute 10
a date_month 1
# date_second 1
a date_wday 1
# date_year 1

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 Behavio host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
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 Detecte host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs
7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = Harini source = SOC_Task2_Sample_Logs.txt sourcetype = SOC_Sample_Logs

,

filtered by action="malware detected". This is the primary evidence for the high-priority incidents.

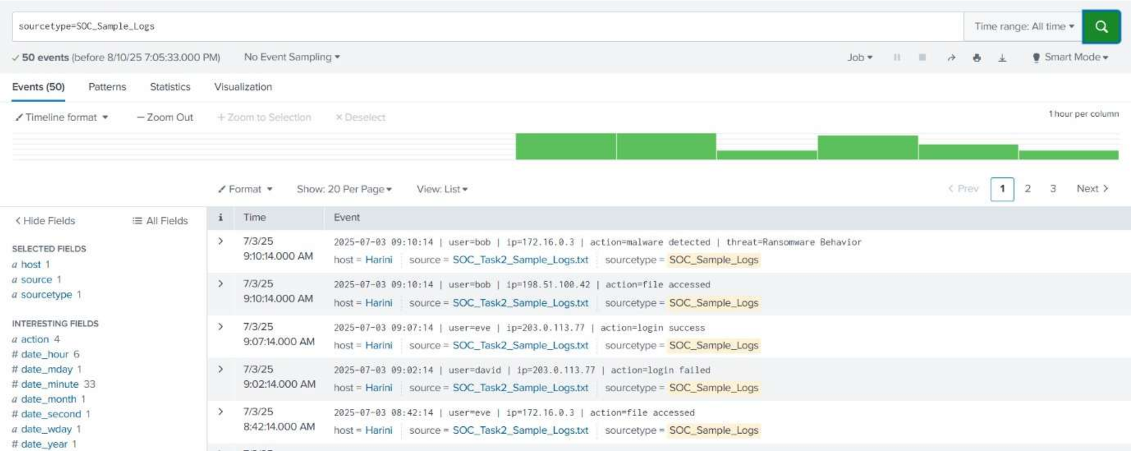
- 

```
sourcetype=SOC_Sample_Logs action="malware detected"
| timechart count by threat
```

_time	Ransomware	Rootkit	Spyware	Trojan	Worm
2025-07-03 04:15:00	0	1	0	0	0
2025-07-03 04:20:00	0	0	0	0	0
2025-07-03 04:25:00	0	0	0	1	0
2025-07-03 04:30:00	0	0	0	0	0
2025-07-03 04:35:00	0	0	0	0	0
2025-07-03 04:40:00	0	0	1	0	0
2025-07-03 04:45:00	0	0	0	0	0
2025-07-03 04:50:00	0	0	0	0	0
2025-07-03 04:55:00	0	0	0	0	0
2025-07-03 05:00:00	0	0	0	0	0
2025-07-03 05:05:00	0	0	0	0	1

```
127.0.0.1:8000/en-US/app/search/search?q=search sourcetype%3DSOC_Sample_Logs action%3D"malware detected"%0A%7C timechart count by threat&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&sid=1754833220.21&displa...
```

Screenshot 2: png - Displays the statistical output of the timechart command, detailing the count of each malware threat type over time.

- 

```
sourcetype=SOC_Sample_Logs
```

```
i  Time              Event
>  7/3/25            2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM    host = Harini   source = SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Sample_Logs
>  7/3/25            2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM    host = Harini   source = SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Sample_Logs
>  7/3/25            2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
   9:07:14.000 AM    host = Harini   source = SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Sample_Logs
>  7/3/25            2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
   9:02:14.000 AM    host = Harini   source = SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Sample_Logs
>  7/3/25            2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
   8:42:14.000 AM    host = Harini   source = SOC_Task2_Sample_Logs.txt   sourcetype = SOC_Sample_Logs
```

Screenshot 3: - Provides a broad view of the event timeline, highlighting clusters of activity around the identified incident times, including the failed login attempt.

7. Communication Draft to Stakeholders

Subject: High-Priority Security Incident: Urgent Action Required

Dear Management and IT Team,

This is an urgent notification concerning a high-priority security incident detected during log analysis. Multiple malware threats, including Ransomware and Rootkit, were identified on the host system ‘Nagesh-PC’ on November 6, 2025.

Preliminary findings suggest a significant system compromise that warrants immediate containment and investigation. A comprehensive Incident Response Plan has been prepared and is attached for your review. The key recommendations include isolating the affected host, initiating a forensic investigation, and performing password resets for all impacted accounts.

We advise scheduling an incident response meeting at the earliest opportunity to coordinate mitigation steps and minimize potential impact.

Please reach out if further clarification or support is needed.

Best regards,
Nagesh Patchipala
Cyber Security Intern – Future Interns

.