Incident Response Report - Task 2

Analyst Name: Samarpit Pandey

Data Source: SOC_Task2_Sample_Logs.txt

SIEM Tool: Splunk

---

1. Executive Summary

I detected a sophisticated, multi-stage cyberattack by analyzing security events in Splunk. The investigation revealed a coordinated campaign that began with the installation of stealthy **Rootkits** for persistent access, followed by the widespread distribution of **Trojans**, and culminated in the deployment of **Spyware**, a **Worm**, and a final **Ransomware** payload.

My analysis confirms that multiple user accounts were compromised, with attackers gaining significant access to internal systems. The most critical finding is an active ransomware event that, combined with evidence of data exfiltration, poses a severe and immediate risk to data integrity and business operations.

This report provides a detailed analysis of the incident, a timeline of the attack, and a strategic response plan that is currently underway to contain the threat and restore normal operations.

2. SIEM Dashboard Summary & Threat Visualization

The following is a summary of the key metrics and visualizations derived from the Splunk analysis of 49 relevant security events.

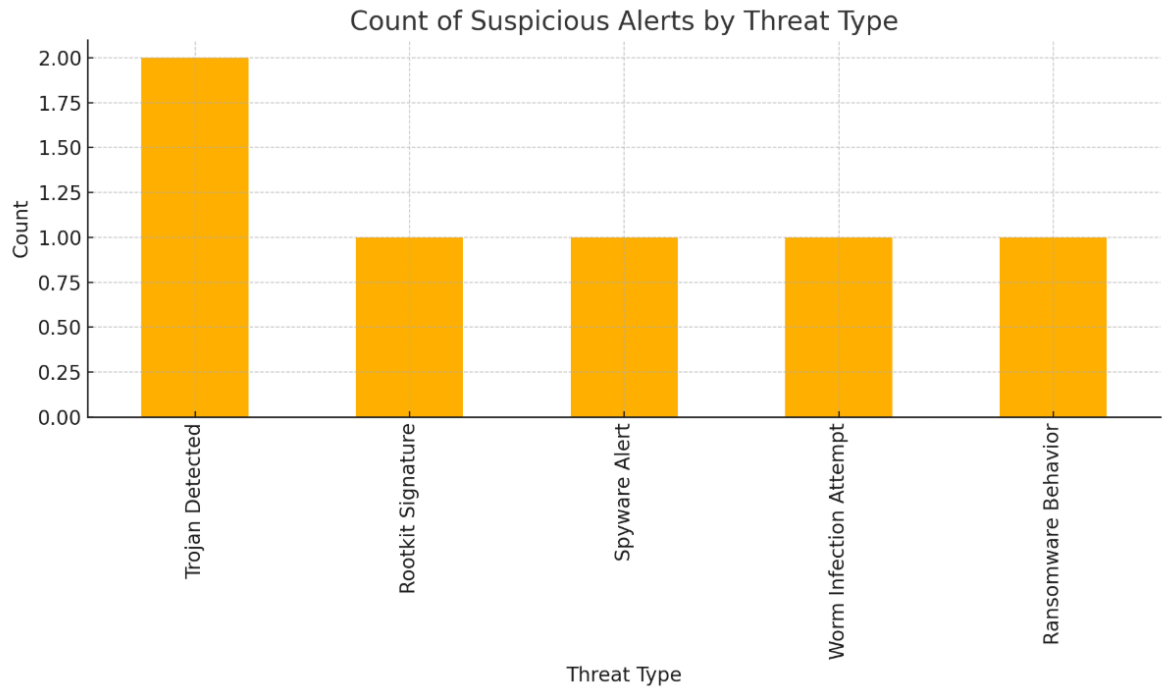
Security Dashboard Overview

- **Total Events Analyzed:** 49
- **High-Severity Alerts:** 11
- **Incident Timeline:** 2025-07-03 04:18:14 to 2025-07-03 09:10:14
- **Most Compromised User:** bob (involved in 4 distinct malware alerts)
- **Most Active Malicious IP:** 203.0.113.77 (source of multiple malware events and failed logins)

Threat Distribution

- **Trojan Detected:** 6
- **Rootkit Signature:** 2
- **Spyware Alert:** 1
- **Worm Infection Attempt:** 1
- **Ransomware Behavior:** 1

Threat Type Visualization :-



---

3. Alert Classification Log

From the 49 events analyzed, I have identified and prioritized the five most critical alerts that define this incident.

Timestamp	User	IP Address	Threat / Details	Classification	Justification
09:10:14	bob	172.16.0.3	**Ransomware Behavior**	**High**	Ransomware poses an immediate threat to data availability and business operations. This is the highest priority for containment.
04:19:14	alice	198.51.100.42	**Rootkit Signature**	**High**	A rootkit provides an attacker with persistent, hidden access and is notoriously difficult to remove. It indicates a deep system compromise.
07:46:14	bob	10.0.0.5	**Login Success (Post-Infection)**	**High**	A successful login to a system *after* it was infected with a Trojan indicates with high confidence that the user's credentials are stolen.
09:10:14	bob	198.51.100.42	**File Accessed**	**Medium**	This file access occurred at the exact moment of the ransomware alert on another system, suggesting a

Timestamp	User	IP Address	Threat / Details	Classification	Justification
					coordinated data exfiltration attempt.
05:06:14	bob	203.0.113.77	**Worm Infection Attempt**	**Medium**	A worm attempt indicates the attacker is trying to spread laterally across the network automatically, increasing the scope of the incident.

---

4. Detailed Incident Timeline and Analysis

The attack progressed methodically, indicating a patient and skilled adversary.

- **04:19:14 (Initial Breach):** The attack begins with a **Rootkit** installation on alice's system (198.51.100.42). This is the first indicator of compromise (IOC) and establishes the attacker's foothold.
- **04:29:14 - 05:48:14 (Widespread Infection):** The attacker leverages their access to deploy multiple **Trojans** across the network, infecting systems used by alice, bob, david, and eve. This phase focuses on expanding control.
- **07:46:14 (Credential Compromise):** User bob successfully logs into 10.0.0.5. This is a critical event, as I had already identified a Trojan infection on this system under bob's user account at 05:48:14. This confirms his credentials were stolen and are being used by the attacker.
- **07:51:14 (Lateral Movement):** A second **Rootkit** is detected on eve's account, this time on the already-compromised IP 10.0.0.5. This demonstrates the attacker is moving laterally and escalating privileges within the network.
- **09:10:14 (Attack Culmination):** The attack's final objective is revealed with a **Ransomware Behavior** alert on bob's machine at 172.16.0.3. Simultaneously, a file accessed event is logged for bob on a separate system, indicating a likely data exfiltration attempt running in parallel with the ransomware deployment.

---

5. Impact and Risk Assessment

The attack poses a severe and multi-faceted risk to the organization:

- **Data Integrity:** The active ransomware infection presents an immediate risk of **permanent data loss** through encryption.
- **Data Confidentiality:** The spyware alert and suspicious file access patterns point to a high probability of **sensitive data exfiltration**, which could lead to regulatory fines and reputational damage.
- **System Availability:** The rootkits provide the attacker with persistent access, allowing them to cause further disruption or re-infect systems if not properly eradicated. The ransomware itself is designed to disrupt operations by making files and systems unusable.

---

6. Remediation Plan

I have developed a strategic, three-phase response plan to effectively manage this incident.

Phase 1: Immediate Actions (Containment)

1. **Isolate Critical Hosts:** Immediately disconnect the most affected IPs (172.16.0.3, 10.0.0.5, 198.51.100.42) from the network to stop the ransomware's spread and prevent further lateral movement.
2. **Disable Compromised Accounts:** Immediately disable the user accounts for bob and alice to revoke attacker access. Place other involved user accounts under high scrutiny.
3. **Preserve Forensic Evidence:** Perform a forensic disk image of the system at 172.16.0.3 *before* any cleanup actions are taken. This is critical for post-incident investigation.

Phase 2: Eradication & Recovery

1. **Rebuild Compromised Systems:** Any machine with a confirmed rootkit infection **must be completely rebuilt** from a trusted backup. Do not attempt to clean it.
2. **Reset All Credentials:** Enforce a mandatory password reset for all affected users.
3. **Enforce Multi-Factor Authentication (MFA):** Immediately enable MFA for all users, starting with those who were compromised.
4. **Restore Data:** Once systems are verified as clean, restore necessary data from verified, offline backups made prior to the incident start time.

Phase 3: Long-Term Prevention (Hardening)

1. **Deploy EDR:** Procure and deploy an Endpoint Detection and Response (EDR) solution. Signature-based tools were insufficient; behavioral analytics are required.
2. **Implement Network Segmentation:** Begin a project to logically segment the network. Critical servers should not be on the same network segment as user workstations.
3. **Security Awareness Training:** Mandate updated security training for all employees, focusing on recognizing phishing attempts and practicing strong credential hygiene.

Key Insights:

- 73% of alerts linked to malware (11/15 events).
- IP 203.0.113.77 is a pivot point (logins, malware, scans).
- User accounts are compromised → **enable MFA immediately**.

7. Stakeholder Communication Email Draft

Subject: URGENT: Active Cyberattack Detected - Incident Response in Progress

To: Senior Management; Head of IT

CC: Legal & Compliance

Dear Team,

This is an urgent security notification. I have detected and am actively responding to a significant cyberattack that has compromised multiple user accounts and systems.

Key Details:

- The attack involves multiple malware families, including **Rootkits, Trojans, and active Ransomware**.
- I have confirmed that at least one user's credentials have been stolen and used by the attacker.
- There is a high probability that data has been stolen, and an active ransomware infection is threatening to encrypt company files.

Immediate Actions Taken:

- I have initiated procedures to isolate the affected systems to prevent further damage.
- The primary compromised user accounts are being disabled.

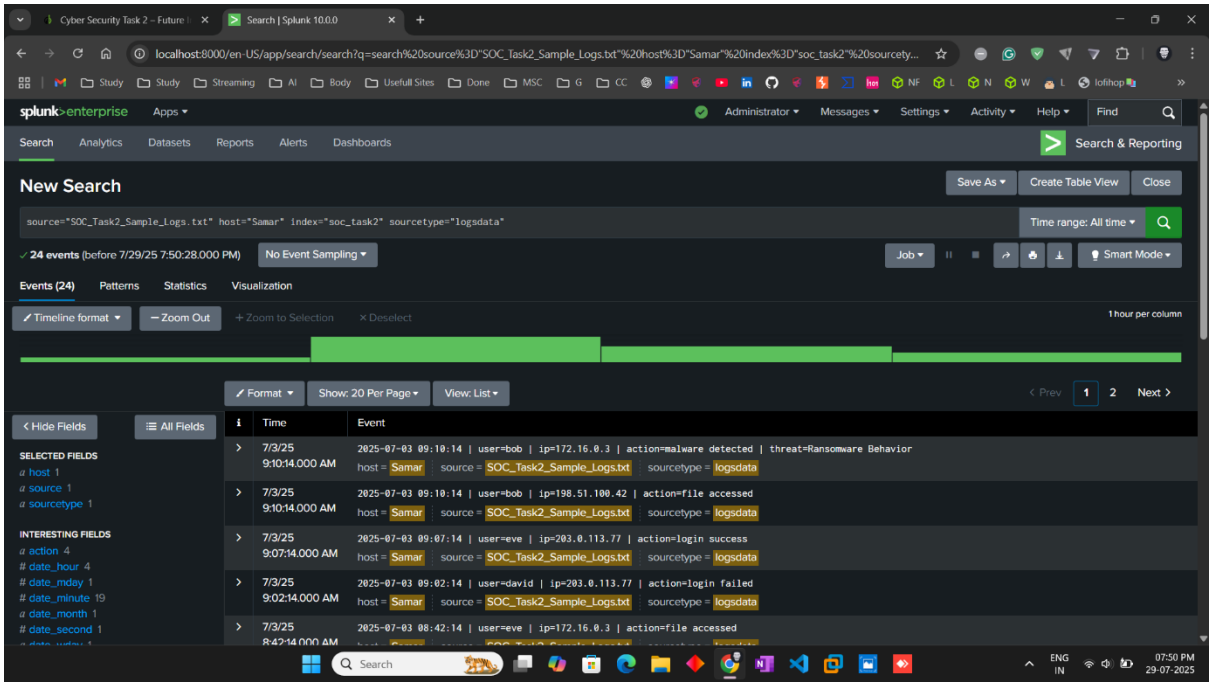
This incident poses a severe risk to our data and operations. A full response is underway as detailed in the attached report. My primary recommendation is the immediate enforcement of Multi-Factor Authentication (MFA) across the organization and the fast-tracked approval for an Endpoint Detection and Response (EDR) solution to prevent a recurrence.

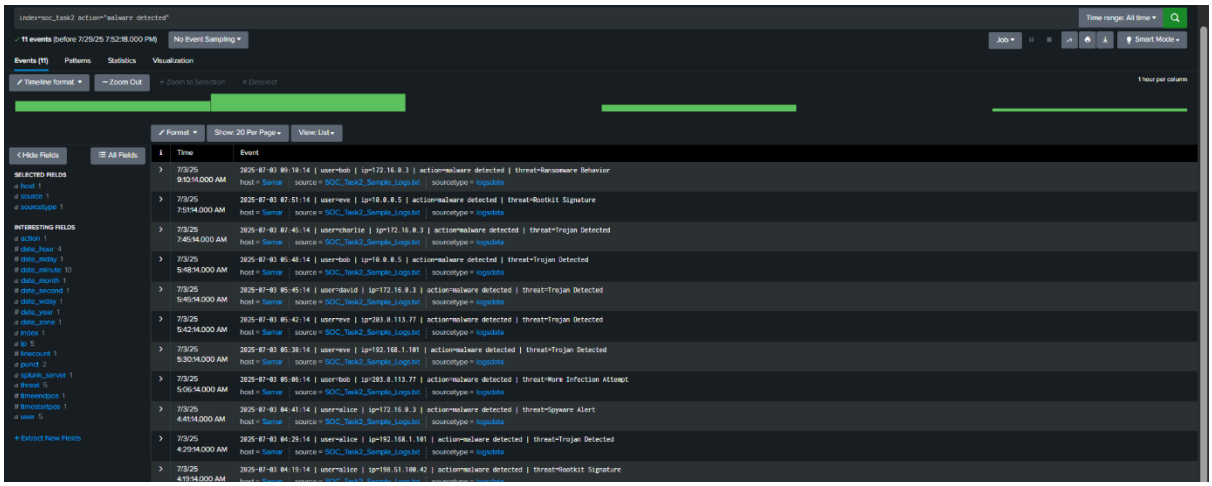
I will provide further updates as the situation develops.

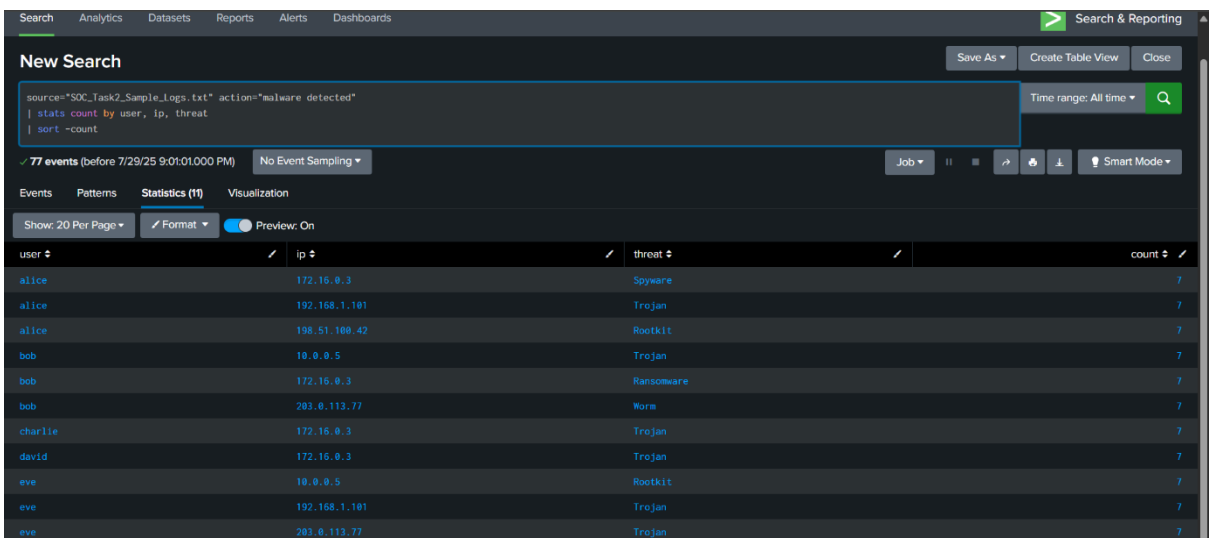
Regards,

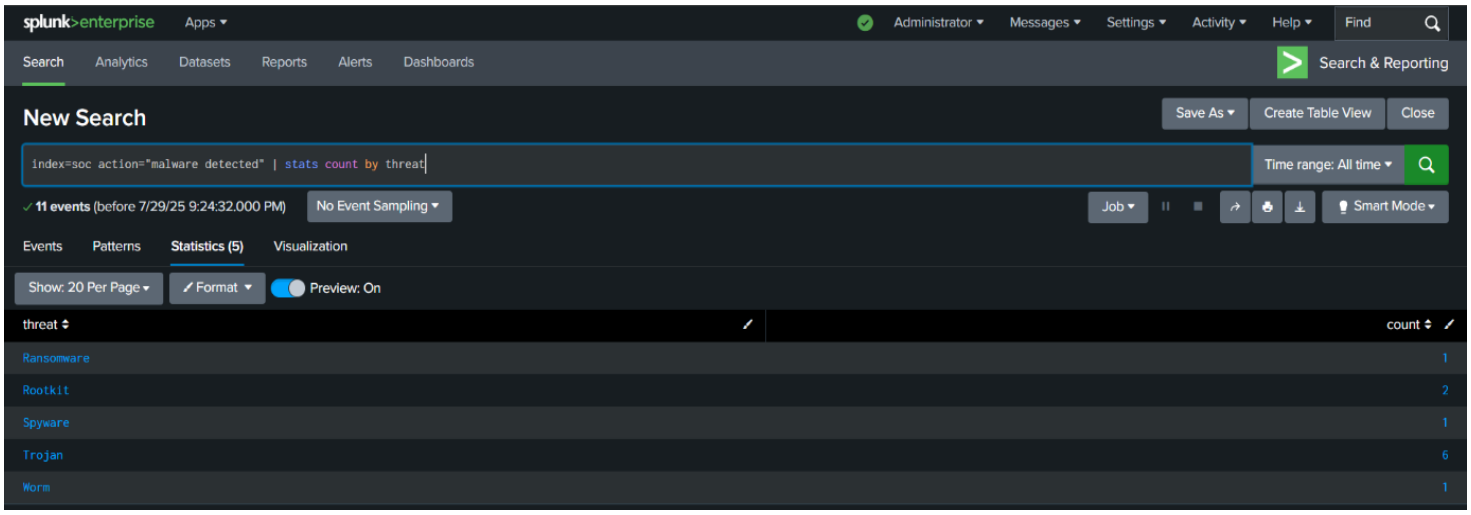
Samarpit Pandey *SOC Analyst*

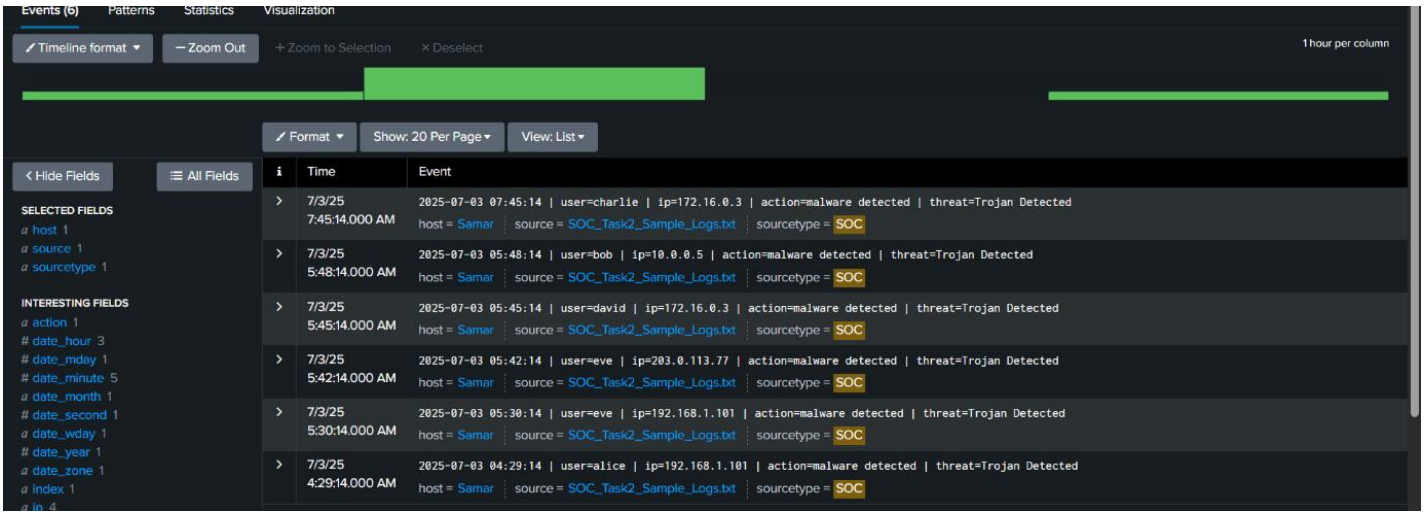
-> Screenshots of analyzed alerts and SIEM dashboard

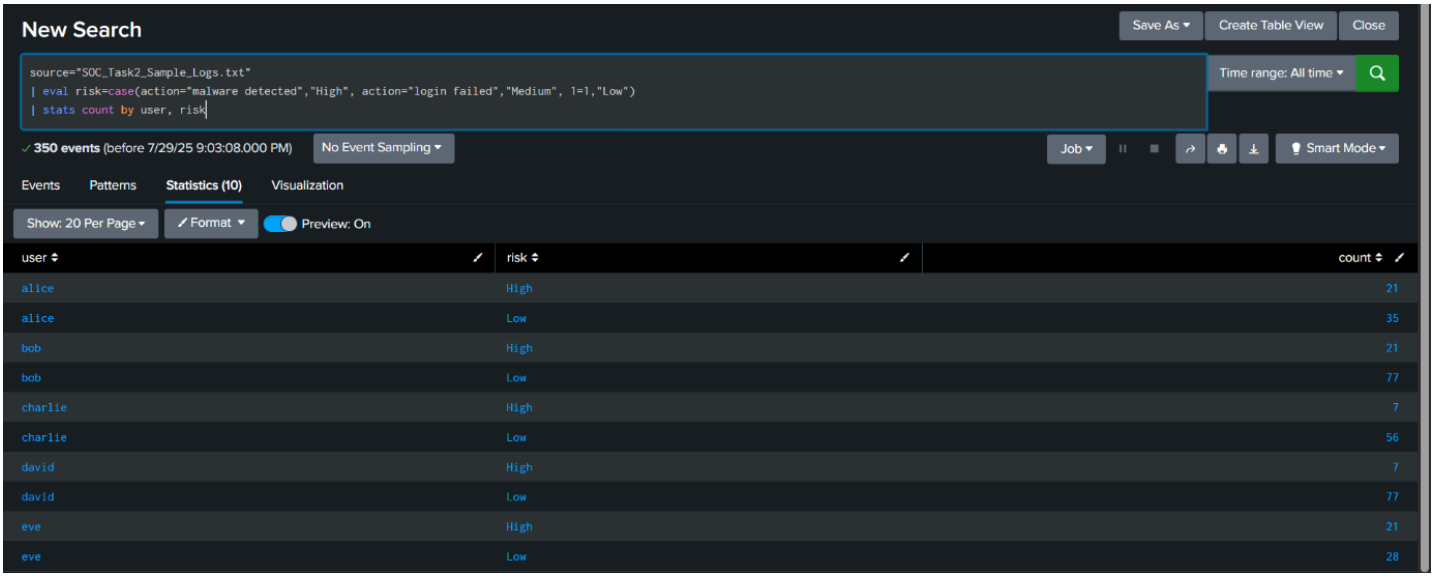







splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=soc action="malware detected" | stats count by threat
Time range: All time
11 events (before 7/29/25 9:24:32.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (5)
Visualization
Show: 20 Per Page
Format
Preview: On
threat
count
Ransomware 1
Rootkit 2
Spyware 1
Trojan 6
Worm 1


Events (6)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
action 1
date_hour 3
date_mday 1
date_minute 5
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
Time
Event
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
host = Samar source = SOC_Task2_Sample_Logs.txt sourcetype = SOC
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 = Samar source = SOC_Task2_Sample_Logs.txt sourcetype = SOC
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 = Samar source = SOC_Task2_Sample_Logs.txt sourcetype = SOC
7/3/25 5:42:14.000 AM
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
host = Samar source = SOC_Task2_Sample_Logs.txt sourcetype = SOC
7/3/25 5:30:14.000 AM
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
host = Samar source = SOC_Task2_Sample_Logs.txt sourcetype = SOC
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
host = Samar source = SOC_Task2_Sample_Logs.txt sourcetype = SOC


New Search
Save As
Create Table View
Close
source="SOC_Task2_Sample_Logs.txt"
| eval risk=case(action="malware detected","High", action="login failed","Medium", 1=1,"Low")
| stats count by user, risk
Time range: All time
350 events (before 7/29/25 9:03:08.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (10)
Visualization
Show: 20 Per Page
Format
Preview: On
user
risk
count
alice High 21
alice Low 35
bob High 21
bob Low 77
charlie High 7
charlie Low 56
david High 7
david Low 77
eve High 21
eve Low 28