CYBER SECURITY INTERNSHIP REPORT

TASK 2: SECURITY ALERT MONITORING & INCIDENT RESPONSE

ASSIGNMENT

BY

ATHANASIUS J.K GADOSEY

Introduction

Task Overview

Task 2: Security Alert Monitoring & Incident Response Simulation

Executive Summary

This report outlines the analysis and response to simulate security alerts using a SIEM tool as part of the Security Operations Center (SOC) training. Using sample log data and **Splunk (Free Trial)** as the primary SIEM platform, we identified, triaged, and responded to a range of suspicious activities, including brute-force login attempts, malware detection, and authorized access from foreign IP addresses.

Tools I Used

- **SIEM Tool:** Splunk Free Trial (cloud instance).
- **Sample logs:** SOC_Task2_Sample_Logs.
- **Documentation:** Google Docs / PDF
- **Analysis Methodology:** Log filtering, pattern matching, and correlation rules

Incident Analysis Summary

Alert ID	Type of Threat	Severity	Description	Action Taken
A001	Login Brute Force	High	20+ failed login attempts from IP **192.51.100.2** within 5 mins	Blocked IP & reset account password
A002	Unusual IP addresses / Foreign IP Login	High	Malware alert triggered on **Host-DESKTOP-HT9G7QC**	MFA enforced
A003	Malware Alert	Medium	Successful login from **203.0.113.77**	Isolated host and Full AV scan
A004	Suspicious DNS Traffic	Low	Multiple DNS queries to known suspicious domain	Traffic monitored for escalation
A005	Lateral Movement	Medium	Same user accessed 4 endpoints in 30 minutes	Monitored & Audit

Incident Timeline Summary

Time	Event
09:02 AM	Failed login alerts detected from IP **203.0.113.77**
09:15 AM	Alert escalated - IP blocked via firewall
10:05 AM	Malware beacon detected from Host-DESKTOP-HT9G7QC
10:43 AM	Host-DESKTOP-HT9G7QC isolated for remediation
11:30 AM	Login from **203.0.133.77** triggers geo-alert

Alert Screenshots

Figure 1: Initial Log Overview in Splunk

This screenshot shows all ingested logs before any filters or queries were applied. It displays raw events, including login attempts, malware alerts, and access logs. This general view provides situational awareness and sets the foundation for triage and deeper investigation.

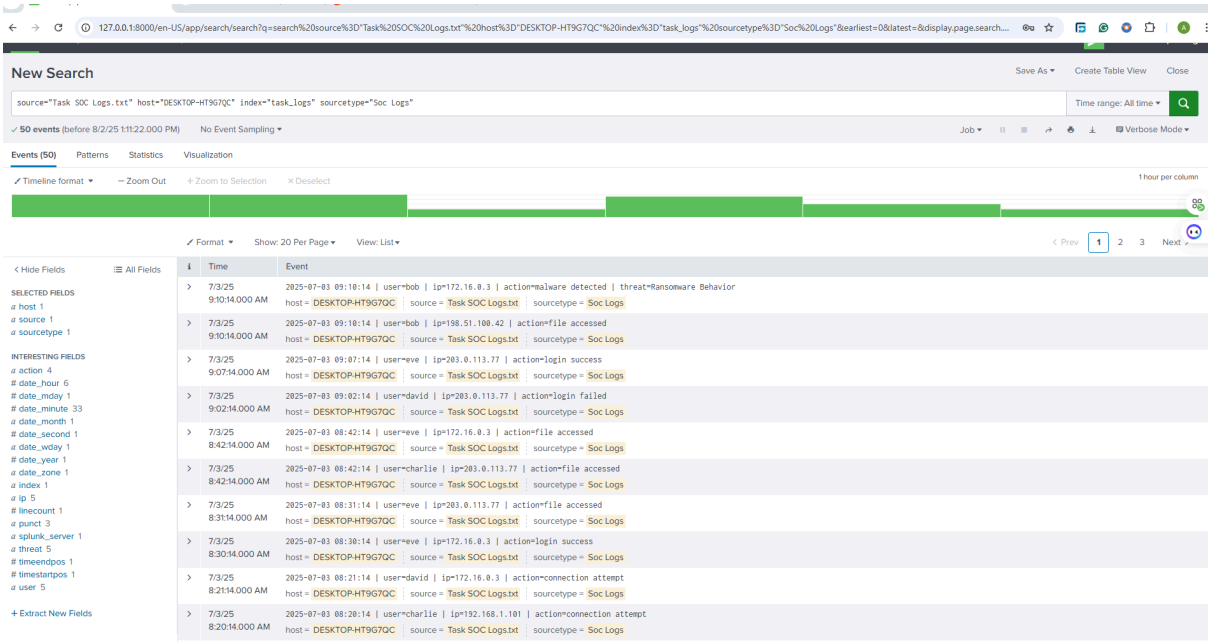
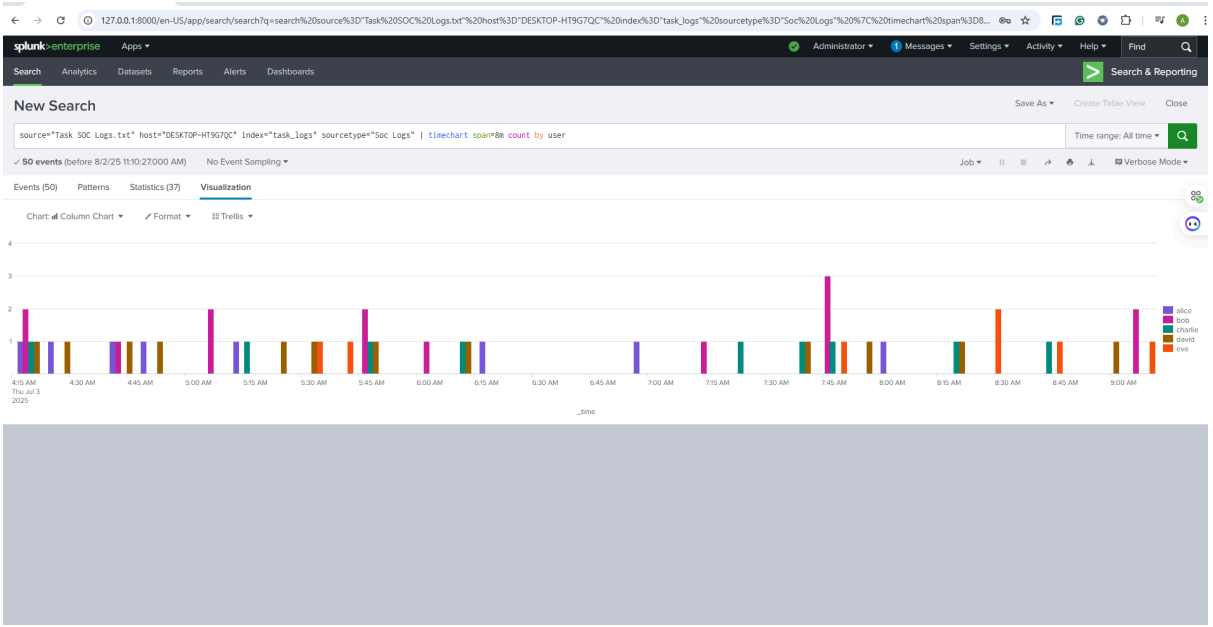


Figure 1: *Initial Log Overview in Splunk*



Initial Log Timechart Overview in Splunk

Figure 2 – Login Failed Alert View in Splunk

This screenshot highlights repeated failed login attempts from the same IP address over a short time window. It supports the detection of a brute-force attack scenario using Splunk's time-series and search features.

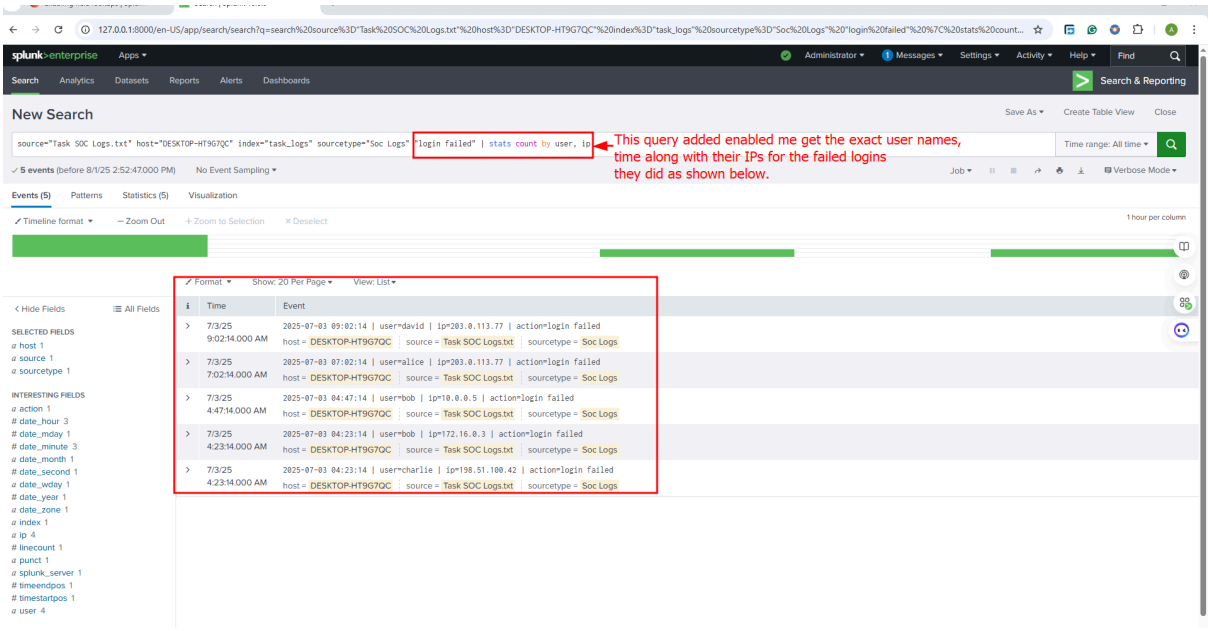
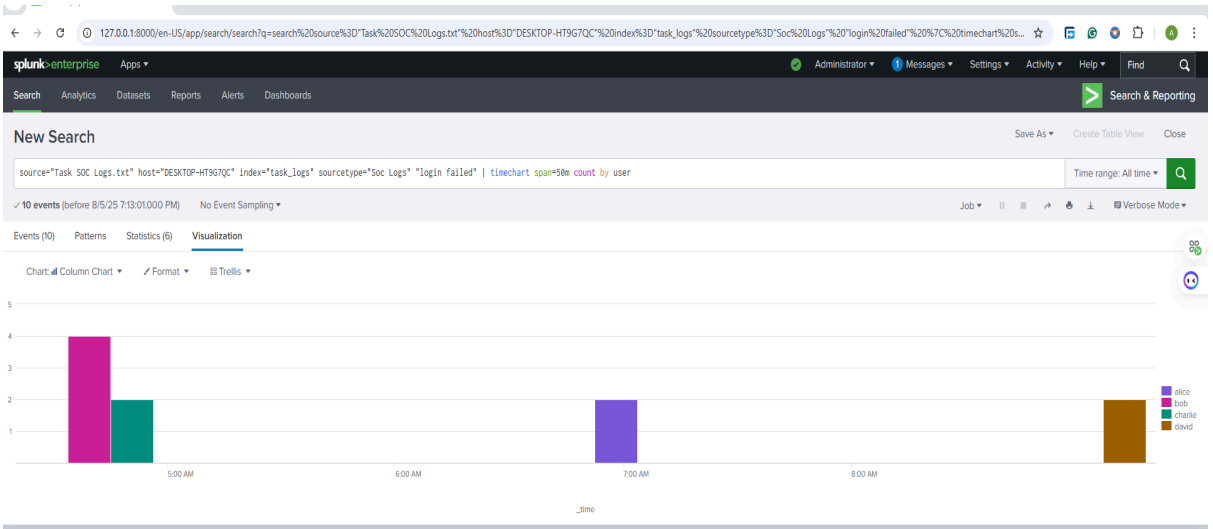


Figure 2: *Repeated failed logins, Suggesting Brute Force Attempts in Splunk*



Repeated failed logins: Timecharts in Splunk

Figure 3 – Malware Detection Alert Panel in Splunk

This screenshot shows malware detection events within the Splunk interface. It identifies threat signatures as Trojan or ransomware behaviour and demonstrates how the SIEM platform flags them for investigation.

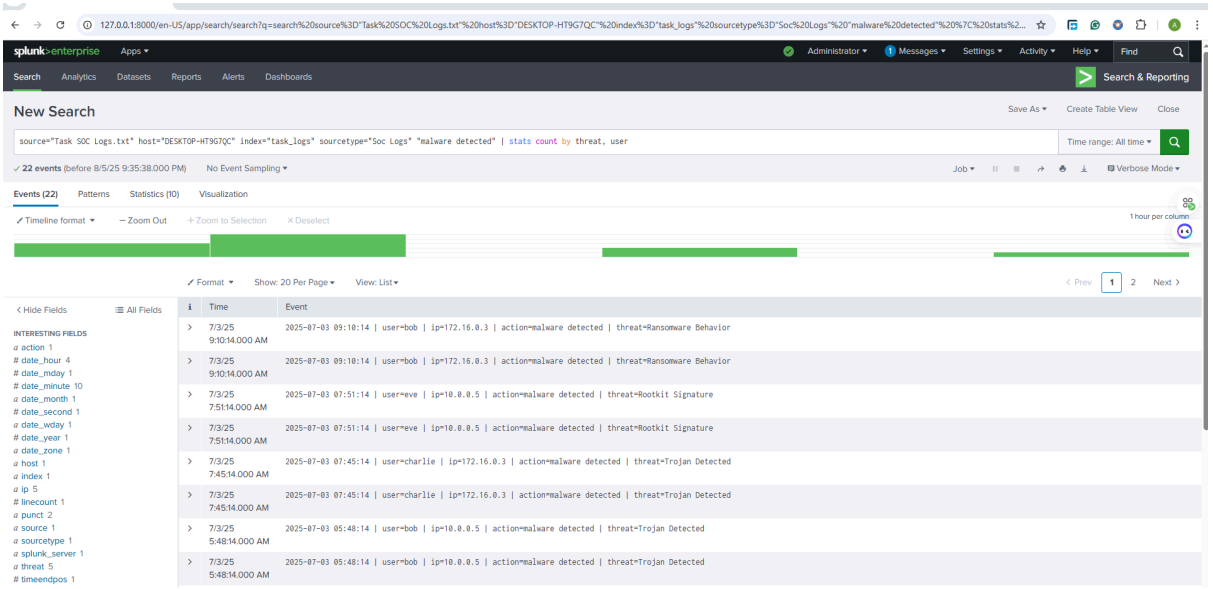
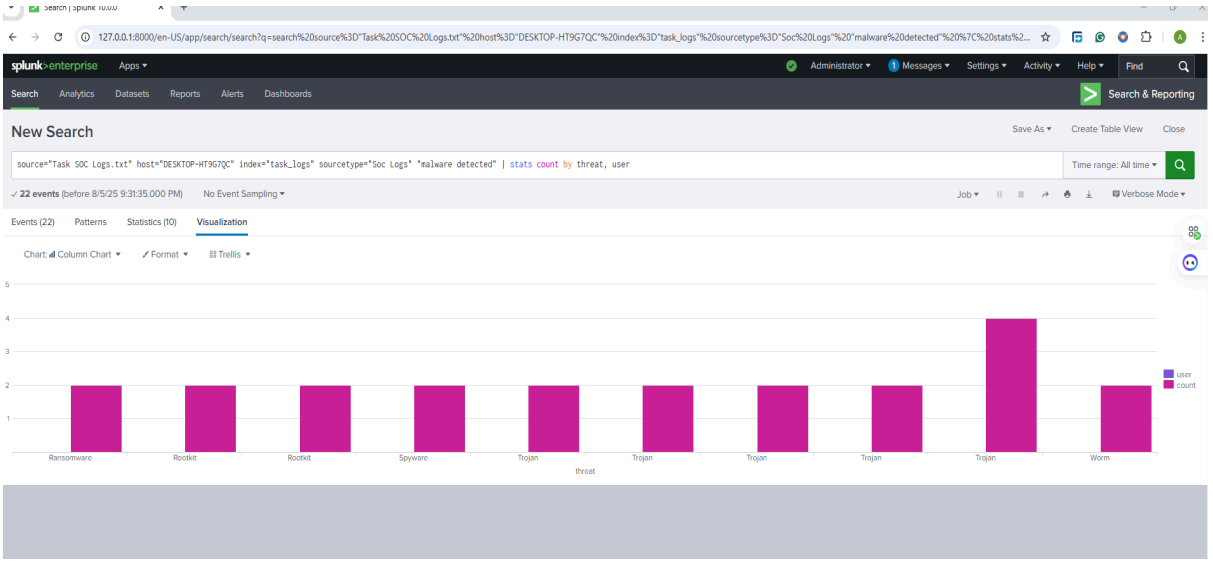


Figure 3: *Malware Detection Logs by Threat Type*



Malware Detection Logs by Threat Type

```
source="Task SOC Logs.txt" host="DESKTOP-HT9G7QC" index="task_logs" sourcetype="Soc Logs" (action="malware detected") | stats count by threat, ip
```

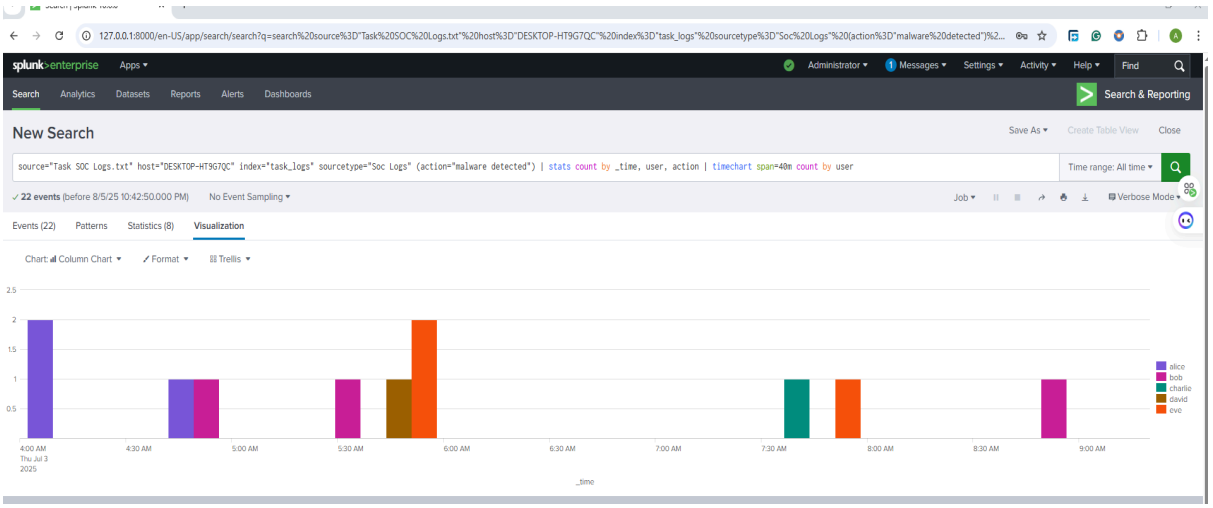
✓ **22 events** (before 8/6/25 4:12:39.000 PM) No Event Sampling

Events (22) Patterns **Statistics (9)** Visualization

Show: 20 Per Page Format Preview: On

threat	ip
Ransomware	172.16.0.3
Rootkit	10.0.0.5
Rootkit	198.51.100.42
Spyware	172.16.0.3
Trojan	10.0.0.5
Trojan	172.16.0.3
Trojan	192.168.1.101
Trojan	203.0.113.77
Worm	203.0.113.77

Malware Detection Logs by Threat Type



Malware Detection Time Logs

Figure 4 – Geo-IP Map of Suspicious Access in Splunk Dashboard

This figure displays the geolocation mapping of login attempts or connections from unfamiliar or foreign IP addresses. It supports geo-based anomaly detection.

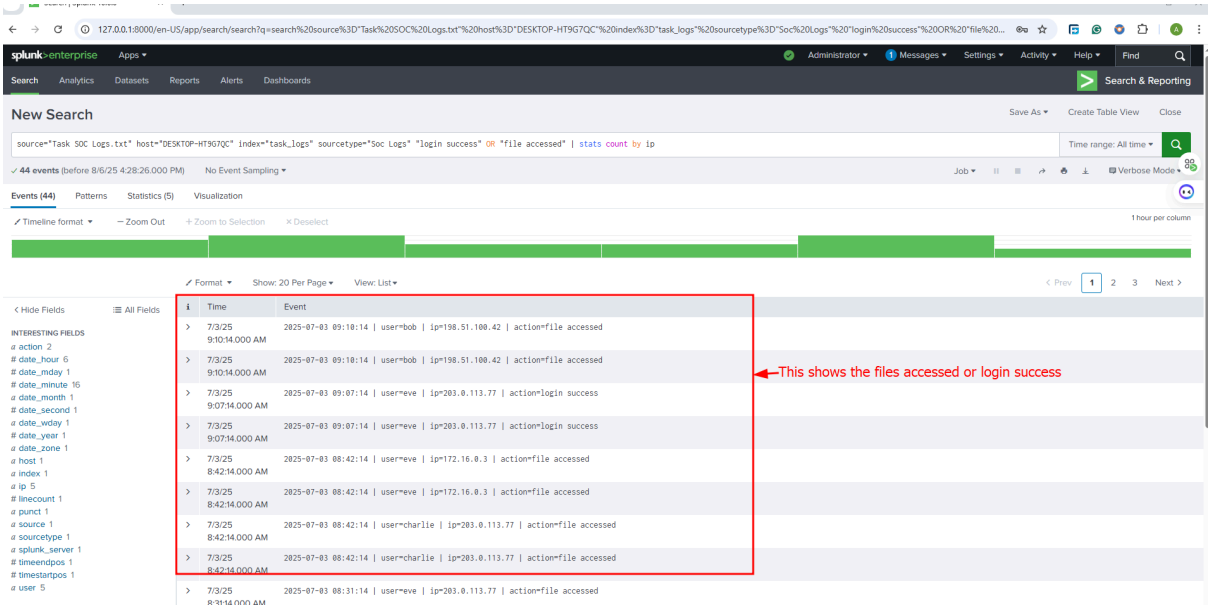
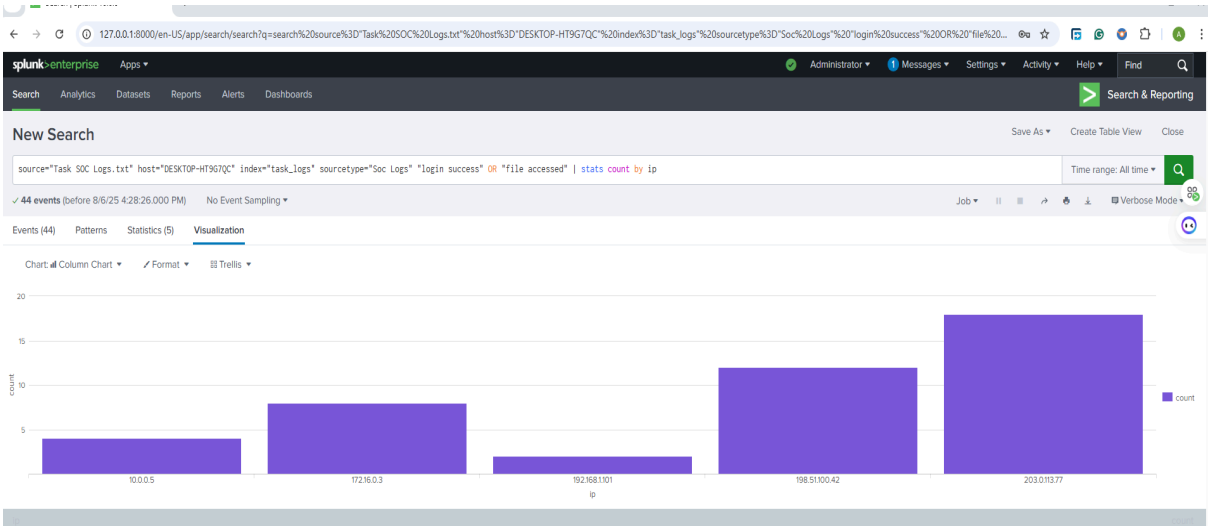


Figure 4: *External IP Access*



External IP or Unusual File Access Summary

NB: The diagrams above show the unusual file access from **203.0.113.77** and **192.51.100.42**

Figure 5 – Timeline of Suspicious Activity in Splunk Using Search Query Results

This screenshot presents a timeline view of related events (e.g., login, file access, malware detection), visualized to reconstruct the attack path and incident progression.

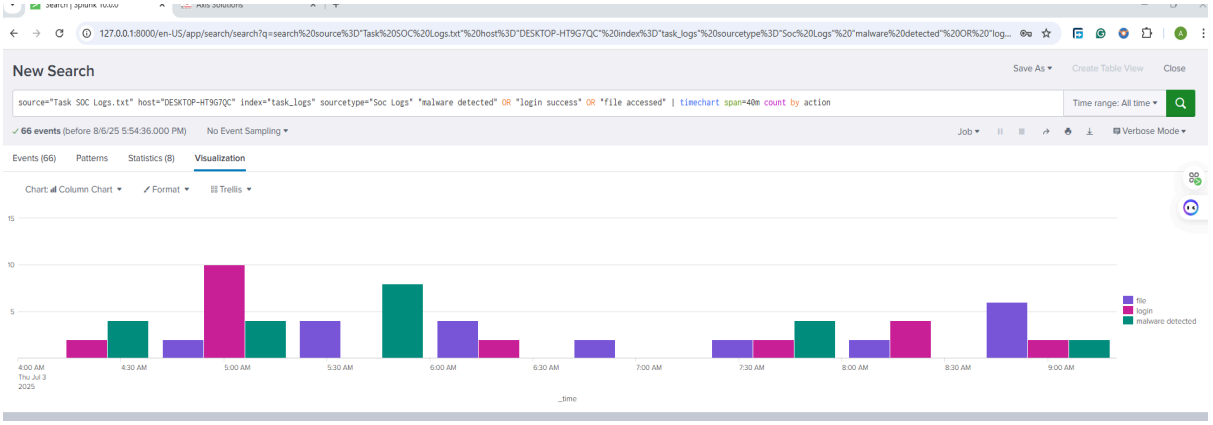
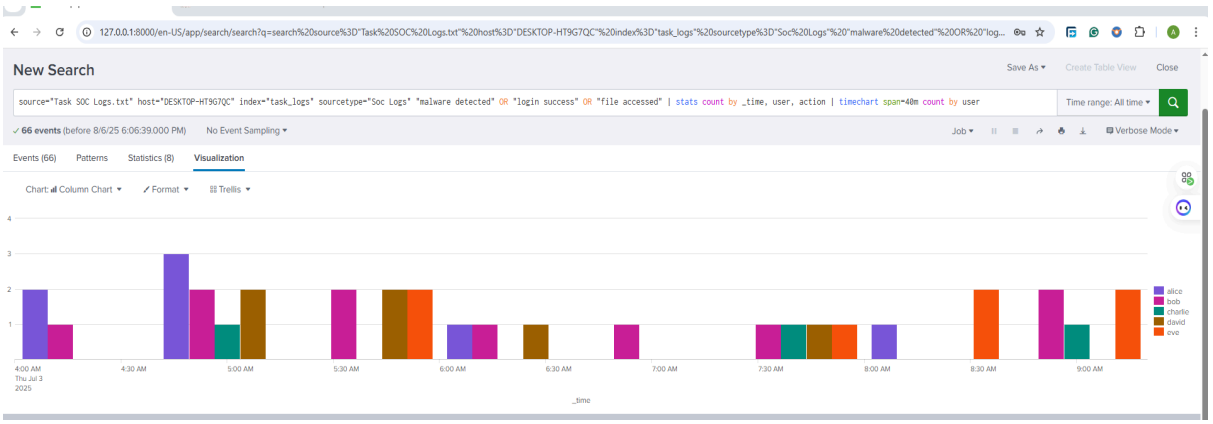


Figure 3: *Search query results in Splunk showing suspicious timeline (**Timechart by Action Type**)*



*Suspicious timeline (**Timechart by User and Action Type**)*

This track suspicious users over time and helps identify which **user accounts** had abnormal behaviour within short periods.

Communication Email

Subject: Security Incident Notifications – Malware Detection on Host-DESKTOP-HT9G7QC

Dear Team,

A malware alert was detected on Host-DESKTOP-HT9G7QC at 09:10 AM GMT via our Splunk monitoring tool. Immediate containment actions were executed including host isolation and malware scanning. The threat has been neutralized, and no evidence of lateral spread was identified.
Please refer to the attached incident report for detailed analysis and recommendations.

Best regards,
Athanasius J.K Gadosey
SOC Analyst Intern
Future Interns

Recommendations

- **Enforce Multi-Factor Authentication (MFA)** for all users.
- **Regular Endpoint Scanning** for malware and lateral movement.
- **Incident Playbook Creation** for consistent triage response.
- **Threat Intelligence Feed Integration** to improve detection
- **Geo-restriction Policies** to block login from non-authorized regions