****

**SUBMISSION OF TASK: FUTURE INTERNS TASK 2**

**NAME: ADEPOJU ESTHER ITUNUOLUWA**

**TASK: Security Alert Monitoring & Incident Response Simulation.**

**TOOLS USED: SIEM TOOL (SPLUNK FREE TRIAL, SAMPLE ALERT LOG, MS WORD (for reporting).**

DETAILS: In this task, I monitored and analyzed incoming security alerts and logs using the simulated data provided. I also identified suspicious activities like failed logins, unusual IP addresses, and malware detection.

This task helped me to simulate what the daily activities of a SOC analyst look like.

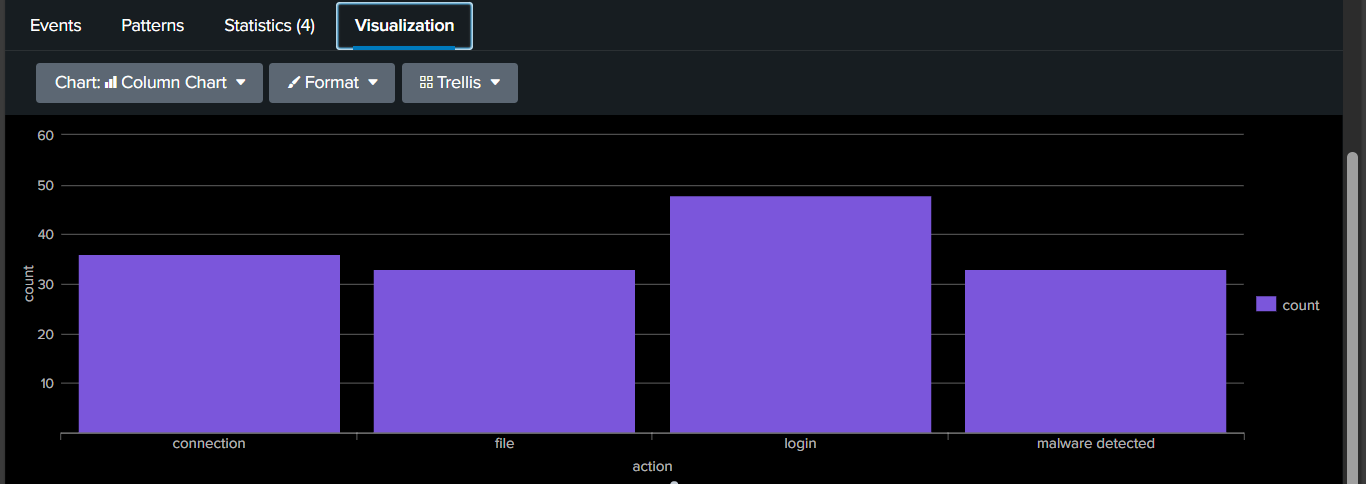


Fig 1: Image of the splunk dashboard result.

**My Findings**: During my routine SIEM monitoring using Splunk, multiple high-severity alerts were detected across several users. Further analysis revealed repeated failed login attempts, suspicious IP activities, and multiple malware detections (including Ransomware, Trojan, Rootkit, Worm, and Spyware).

These suggest a coordinated brute-force and malware propagation campaign that may have resulted in multiple system compromises.

**Malware Detected**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Type | Severity | Affected Users | IP addresses | Observation |
| Ransomware | High | Bob | 172.16.0.3 | File encryption |
| Rootkit | High | Eve & Alice | 10.0.0.5, 198.51.100.42 | Persistence on system startup. |
| Trojan | High | Bob, Alice, Charlie, David, Eve | 10.0.0.5, 172.16.0.3, 192.168.1.101 | Credential Theft, C2 communication |
| Worm Infection | Medium | Bob & Eve | 203.0.113.77, 192.168.1.101 | Network Propagation |
| Spyware | Medium | Alice | 172.16.0.3 | Data collection |

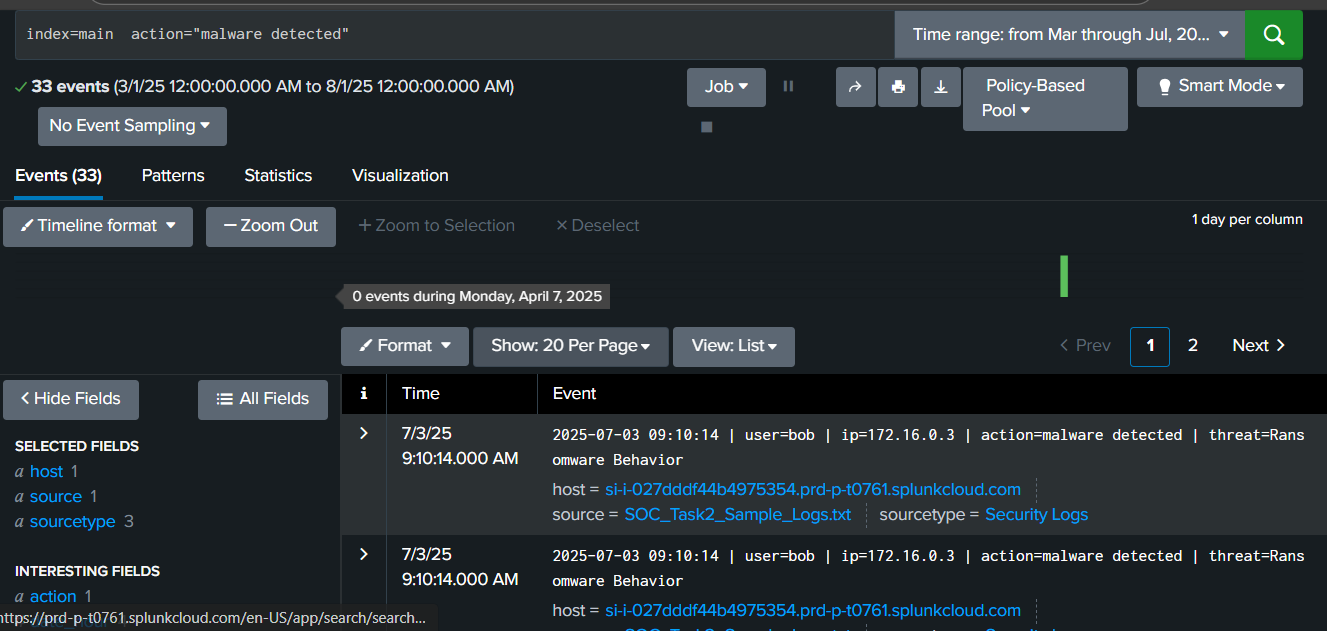


Fig 2: Image of malware alert detected

**Suspicious Activities Detected, such as Failed Login**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User | Time | Date | IP addresses | No of attempts | Observation |
| David | 9:02am | 7/3/2025 | 203.0.113.77 | 3 | Possible brute-force attempt |
| Alice | 7:02am | 7/3/2025 | 203.0.113.77 | 3 | Same external IP as David; correlation. This indicates threat actors’ reuse |
| Bob | 4:43-4:47am | 7/3/2025 | 10.0.0.5 & 172.16.0.3 | 6 | Multiple IPs, which could signify a likely credential compromise |
| Charlie | 4:23am | 7/3/2025 | 198.51.100.42 | 3 | Repeated attempts from an external IP |

This indicates that Bob’s account was compromised (two different IP addresses were used, and his account was accessed multiple times). His account was exploited.

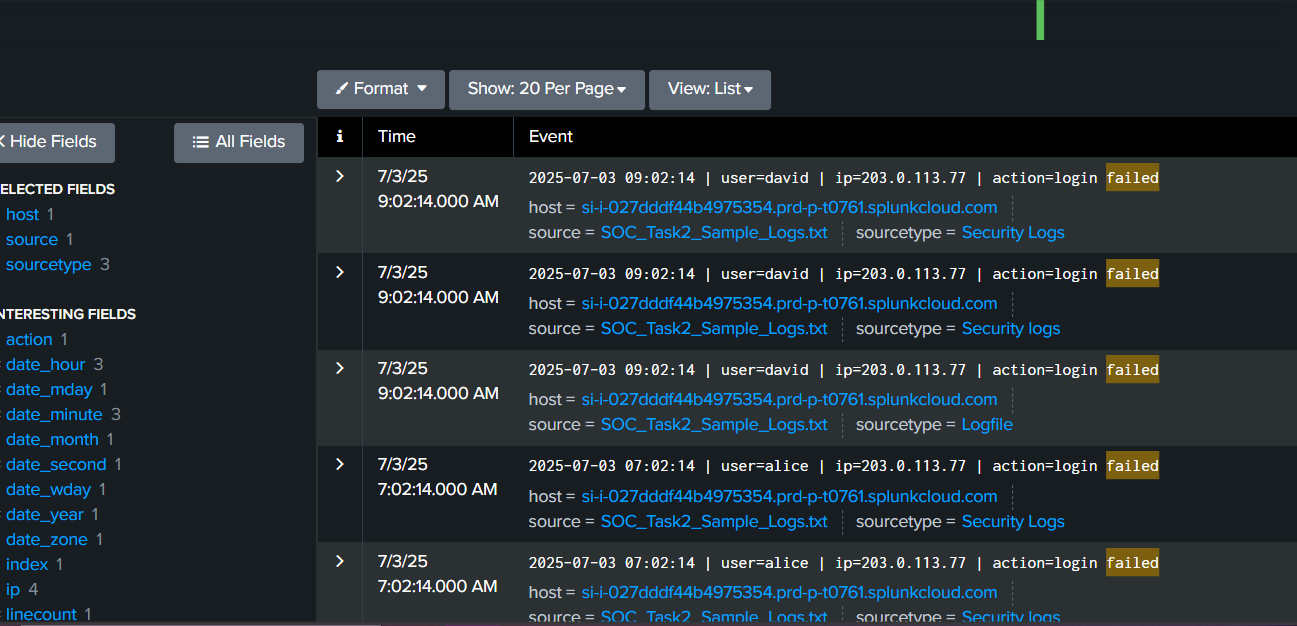


Fig 3: Image of failed logins

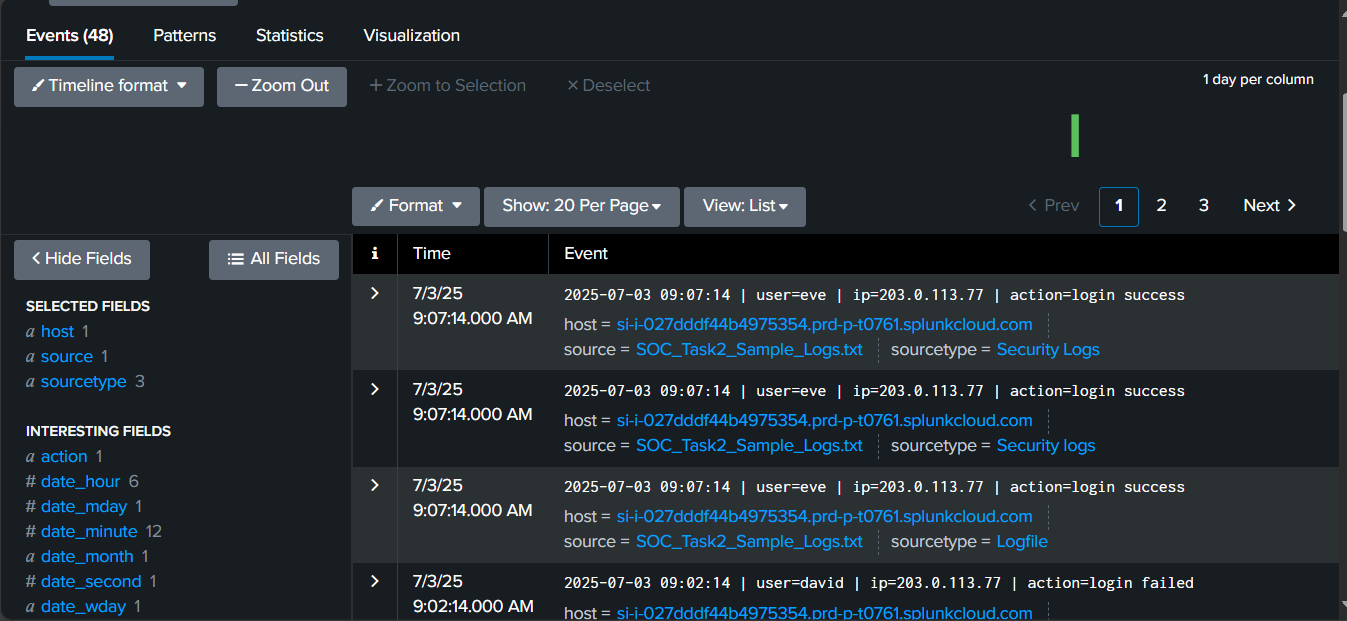


Fig 4: Image of successful logins

**Unusual IP addresses:**

**203.0.113.77 – Repeated login failures (David, Alice) and malware detections (Bob, Eve).**

This is likely an external threat actor IP that is used for command & control or data exfiltration. Suspicious IP address 203.0.113.77 logs 15 entries, which showed in Alice and David failed logins using the same IP address, and malware detection of Bob and Eve with the same suspicious IP address.

IP address 203.0.113.77 is linked to multiple attack vectors and could indicate exfiltration attempts.

**198.51.100.42 – Associated with Rootkit infection (Alice, Charlie):** Persistence-based threat source.

**Malware Activity Correlation:**

Bob’s device (IPs 10.0.0.5 and 172.16.0.3) shows multiple malware infections and Ransomware presence which indicates complete compromise.

Eve’s system exhibits multi-vector infection (Trojan, Rootkit, Worm) suggesting lateral movement.

**Alert Categorization & Prioritization:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert type** | **Severity level** | **Impact** | **Priority actions** |
| Ransomware, Rootkit and Trojan activity | High | System Compromise, Data loss. | Isolate immediately |
| Failed Logins, Worm infection | Medium | Credential theft | Contain network spread and password reset enforcement. |
| Single successful logins after failed ones | Low | Normal but needs monitoring | Log correlation and observation |

**Impact Assessment:**

Scope: 5 users affected (Alice, Bob, Charlie, David, Eve)

Assets Affected: 3-4 internal hosts.

Data at Risk: User credentials, sensitive documents, potential internal data exfiltration.

Operational Impact: Possible downtime due to ransomware encryption; reduced system integrity.

Severity: High (multi-endpoint compromise with external C2 link)

**Immediate response actions to be taken:**

1.Isolate Infected systems: Bob and Alice’s workstations should be disconnected immediately.

2.Block any suspicious IP addresses: Susoicious IP addreses such as 203.0.113.77, 198.51.100.42 should be blockd immediately.

3. Multi-factor Authentication Enforcement: Password reset for all affected users must be enforced immediately.

Enabled multi-factor authentication only for privileged accounts.

4. Malware Containment: A full system scan must be deployed and quarantined using updated antivirus definitions.

5. Forensic Analysis: A detailed memory and disk forensics on Bob and Eve’s systems must be conducted.

Network packets must be captured and analyzed for suspicious outbound traffic.

Patch & Update:

6. Ensure OS and security tools are fully patched and updated.

7. User Awareness Training: Educate users on phishing indicators and strong password practices.

8. Threat Hunting: Search for additional indicators tied to IP 203.0.113.77 in historical logs.

9. Backup & Recovery: Verify integrity of backups prior to restoring systems impacted by ransomware.

10. Continuous Monitoring: A SIEM rule must be put in place for

i. Multiple login failures per minute

ii. Cross-IP login attempts for the same user

iii. Malware signature detection correlation

**Letter to stakeholders about the Incidence:**

To: Security Team, IT Department, and Management

From: SOC Analyst (Adepoju Esther I.)

Subject: **High-Severity Security Incident Response Summary**

**Summary of incidence:**

The SIEM monitoring detected coordinated malicious activity targeting multiple employee accounts (Bob, Alice, Eve, Charlie, and David). Indicators include failed logins, multiple internal and external IPs used per account, and confirmed malware infections — including ransomware and rootkits. Immediate containment actions have been initiated to prevent further spread.

The Impact of these incidences are as follows:

i. High risk of data compromise.

ii. Two systems isolated for forensic analysis.

iii. Malicious IPs blocked at the firewall level.

**The following steps have been suggested:**

i. Complete endpoint reimaging for compromised devices.

ii. Perform threat intelligence correlation to identify the attacker infrastructure.

iii. Submit full report to management for compliance documentation.

From my findings, the detected incident reflects a coordinated multi-vector intrusion involving credential compromise, malware propagation, and possible data exfiltration. The prompt containment actions mitigated further spread, but ongoing monitoring and user re-education remain essential.

**SKILLS GAINED:**

1. Security Monitoring and log analysis
2. Threat Detection and classification
3. Incident response and containment; Incident classification and escalation process.
4. Network and endpoint security
5. Understanding of SIEM tools and dashboards
6. Effective incident communication and reporting