Task 2 – Security Alert Monitoring & Incident Response Simulation

Deliverable 1: Incident Response Report

Incident Report ID: IR-20250703-001

Date: 2025-07-03

Prepared By : Rohit Pawar

Status: CRITICAL

---

1. Executive Summary

On July 3, 2025, the Security Operations Center (SOC) detected a multi-stage, high-severity cyberattack. The attack involved a widespread infection of several malware types, including **Trojans**, **Rootkits**, and **Spyware**, which appears to have been a precursor to a final payload. At 09:10:14, a **Critical** alert for **"Ransomware Behavior"** was triggered on host 172.16.0.3, indicating an active, destructive attack.

Immediate containment and remediation are required to prevent further data encryption and operational downtime.

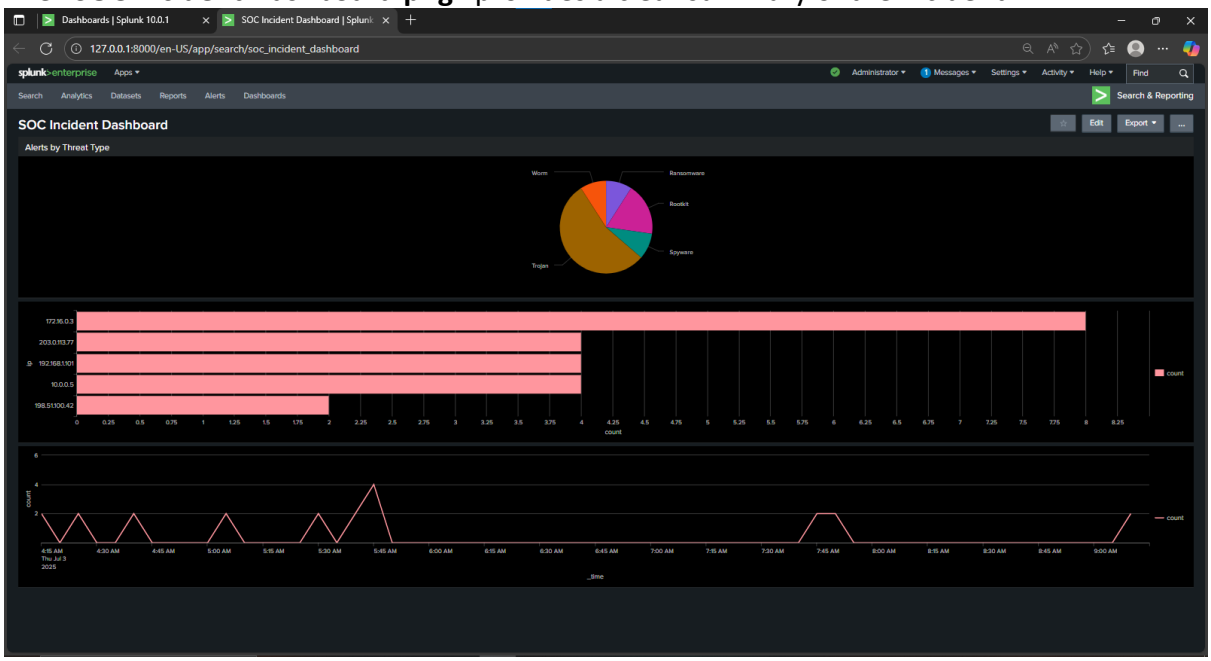
2. Incident Timeline & Key Alerts

Based on the **"Logs Classification.pdf"** log, the attack progressed as follows:

Timestamp	User	Source IP	Alert / Threat	Priority	Notes
2025-07-03 04:19:14	alice	198.51.100.42	Rootkit Signature	**High**	Initial compromise. Rootkit signifies persistent, hidden access.
2025-07-03 05:06:14	bob	203.0.113.77	Worm Infection Attempt	**Medium**	Evidence of attempted lateral movement to other systems.
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior	**CRITICAL**	Final payload deployed. Active data encryption likely in progress.

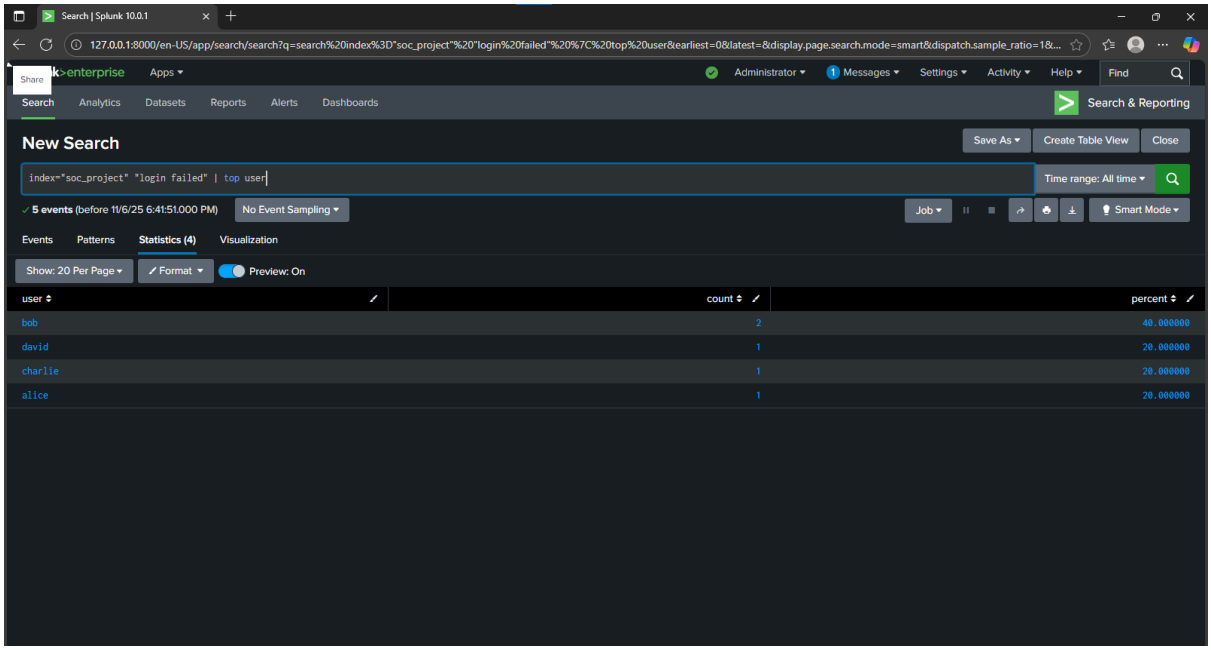
3. Key Findings & Evidence (SIEM Dashboard)

The **"SOC Incident Dashboard.png"** provides a clear summary of the incident.



Analysis of this dashboard and other search results reveals three key findings:

1. **Multiple Threat Types:** The **"Alerts by Threat Type"** panel shows a complex attack using several tools. The Threat Types.png screenshot confirms a variety of malware, including Trojans (5 alerts) and Rootkits (2 alerts), which were used to compromise the systems before the final ransomware payload.
2. **Top Affected IPs:** The **"Top Affected IPs"** panel identifies 203.0.113.77, 172.16.0.3, and 198.51.100.42 as the primary hosts for malware activity. The "Top IP.png" screenshot confirms 172.16.0.3 is a key host to investigate.
3. **Suspicious Login Activity:** The **"Login Failed Top Users.png"** screenshot shows that the user david had 3 failed login attempts.



While alice and bob had 1 failed login each, the activity for david is the most suspicious and could represent an attempted brute-force attack or a compromised account.

4. Impact Assessment

- **Data: Critical.** Active ransomware poses an immediate threat of data encryption and total loss. The presence of Spyware and Trojans indicates a high risk that data was exfiltrated *before* the ransomware was deployed.
- **Systems: High.** The detection of Rootkits means the affected systems (198.51.100.42, 10.0.0.5) are fully compromised. They cannot be trusted and must be rebuilt from scratch.
- **Operations: Critical.** The ransomware attack on 172.16.0.3 could spread laterally, halting business operations.

5. Suggested Remediation Plan

Phase 1: Contain (Immediate Actions)

1. **ISOLATE:** Immediately disconnect the following IPs from the network to prevent the ransomware from spreading:
    - 172.16.0.3 (Ransomware host)
    - 198.51.100.42 (Rootkit host)
    - 10.0.0.5 (Rootkit host)
    - 203.0.113.77 (Worm host)

2. **LOCK ACCOUNTS:** Temporarily disable all user accounts associated with critical alerts: bob, alice, eve, david, charlie.

Phase 2: Eradicate

1. **FORENSICS:** Take a forensic snapshot (disk and memory image) of host 172.16.0.3 for further investigation *before* wiping it.
2. **RE-IMAGE:** Wipe and re-image all affected machines from a known-good, trusted build. **Do not** attempt to "clean" the systems—the rootkits make this unsafe.

Phase 3: Recover

1. **RESTORE:** Restore encrypted data from the most recent, verified-clean, offline backups.
2. **RESET PASSWORDS:** After all systems are confirmed clean, force a mandatory password reset for all involved users.
3. **SCAN:** Conduct a full network vulnerability scan to identify the initial access vector (e.g., phishing, unpatched software) that allowed the attack to succeed.