

# **Incident Response Report – SOC Task2**

FutureInterns

- **Name :** Aman mali
- **Tool Used:** Splunk SIEM
- **Dataset:** SOC\_Task2\_Sample\_Logs
- **Date of Analysis:** November 10 2025
- **Objective:** To monitor, detect, and analyze suspicious security events within a simulated enterprise environment and prepare an incident response summary

## **2. Key Findings**

During the log analysis using Splunk, several suspicious patterns were detected:

- **Malware Activity:** Trojan malware detected on host system **172.16.0.3 (user=bob)**, indicating a possible infection or compromise.
- **Unauthorized Login Attempts:** Multiple failed login attempts recorded, suggesting possible brute-force or credential theft attempts.
- **Unusual Network Connections:** Outbound connections from internal systems to unknown external IP addresses, which could be linked to command-and-control (C2) activity or data exfiltration attempts.

These findings highlight a mix of high and medium-risk events that required containment and further analysis.

## **3. Severity Classification**

Based on the analysis of the simulated security logs, the detected threats were classified according to their potential impact and risk level:

- Trojan Malware Detection (High Severity):  
Confirmed malicious activity was observed on the host system 172.16.0.3 associated with user=bob. This indicates a successful infection by a Trojan, which could lead to data theft, unauthorized access, or further lateral movement across the network.
- Multiple Failed Logins (Medium Severity):  
Repeated failed authentication attempts were detected across user accounts. This pattern suggests a possible brute-force or password spraying attack, where an attacker systematically tries multiple password combinations to gain unauthorized access.
- Suspicious Network Connections (Medium Severity):  
Unusual outbound connection attempts were identified from internal systems to unknown or unauthorized IP addresses. Such activity often points to command-and-control (C2) communications or initial reconnaissance by a compromised endpoint.

## \*Testing & Validation:

The screenshot shows a Splunk search interface with the following details:

- URL:** 127.0.0.1:8000/en-US/app/search/search?q=search%20source%3DSOC\_Task2\_Sample\_Logs.txt%20host%3DLAPTOP-L6PF48S6%20sourceType%3Dtask%202&earliest=0&latest=&sid...
- Fields:**
  - SELECTED FIELDS: host 1, source 1, sourcetype 1
  - INTERESTING FIELDS: action 4, date\_hour 6, date\_mday 1, date\_minute 33, date\_month 1, date\_second 1, date\_wday 1, date\_year 1, date\_zone 1, index 1, ip 5, linecount 1, punct 3, splunk\_server 1, threat 5, timeendpos 1, timestamppos 1, user 5
- Results:** The main pane displays a list of log events. A sample of the data is shown below:
 

```

      i Event
      > 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
      > 2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
      > 2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
      > 2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
      > 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
      > 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
      > 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
      > 2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
      > 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
      > 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
      > 2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
      > 2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
      > 2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
      > 2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
      > 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
      > 2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
      > 2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
    
```

Fig 1.1 Dashboard\_raw data

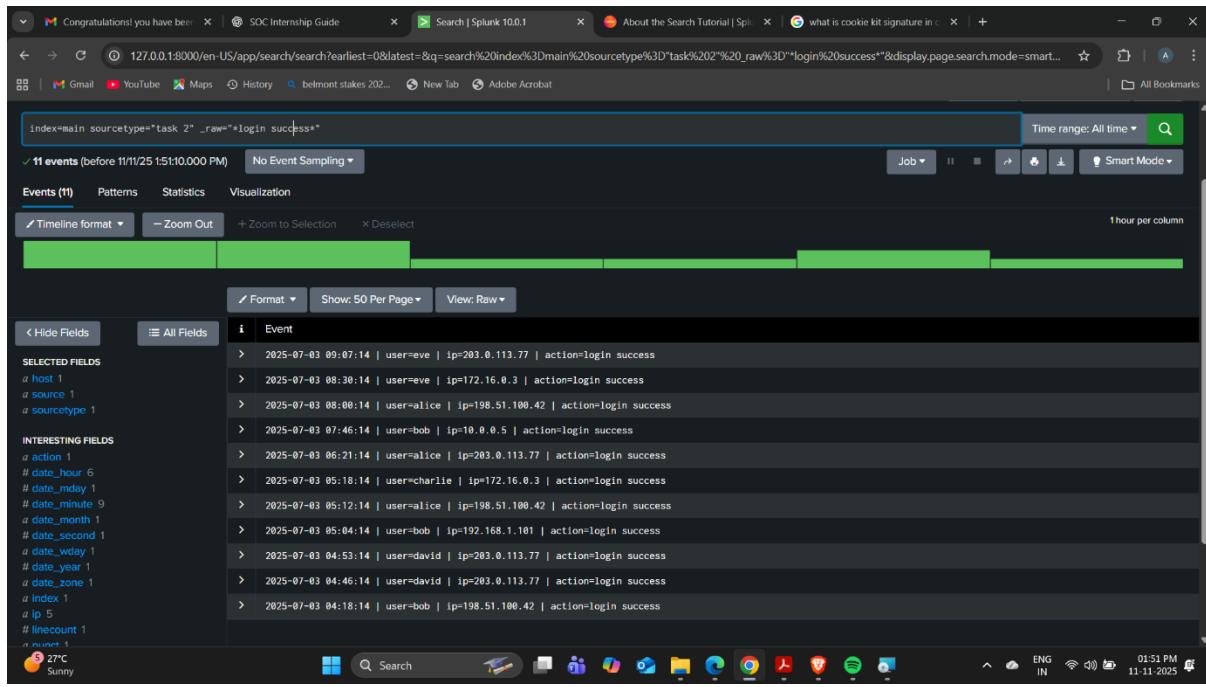


Fig 1.2 login\_success

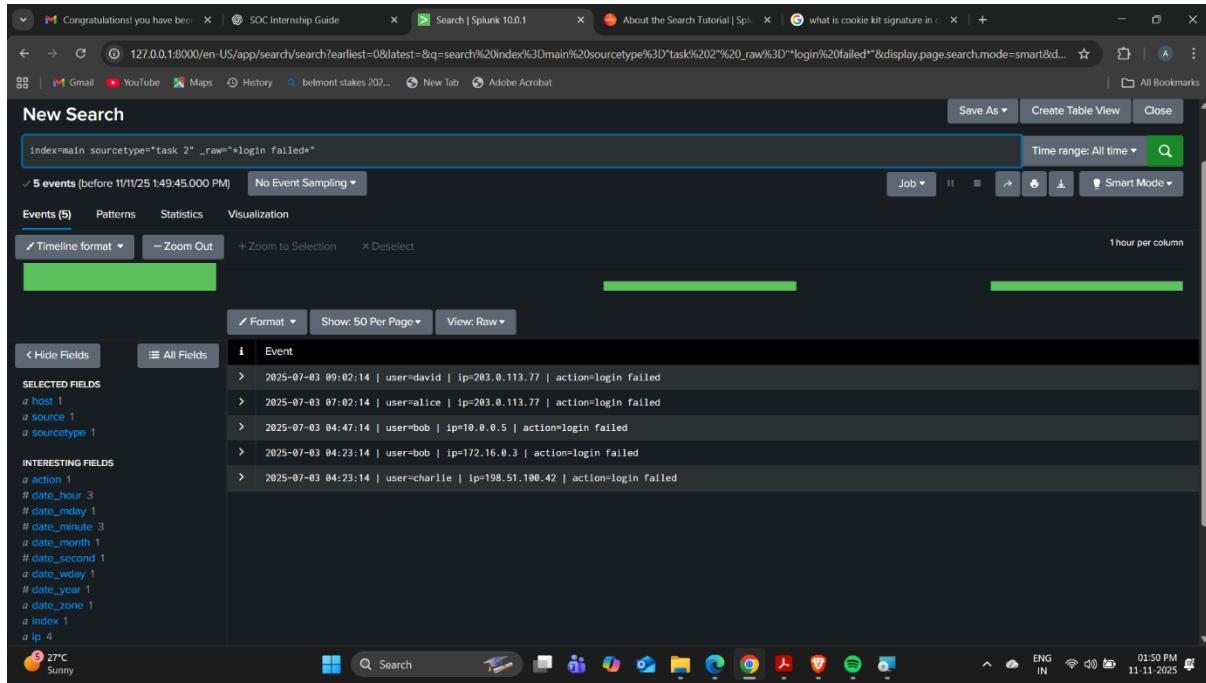


Fig 1.3 login\_fail

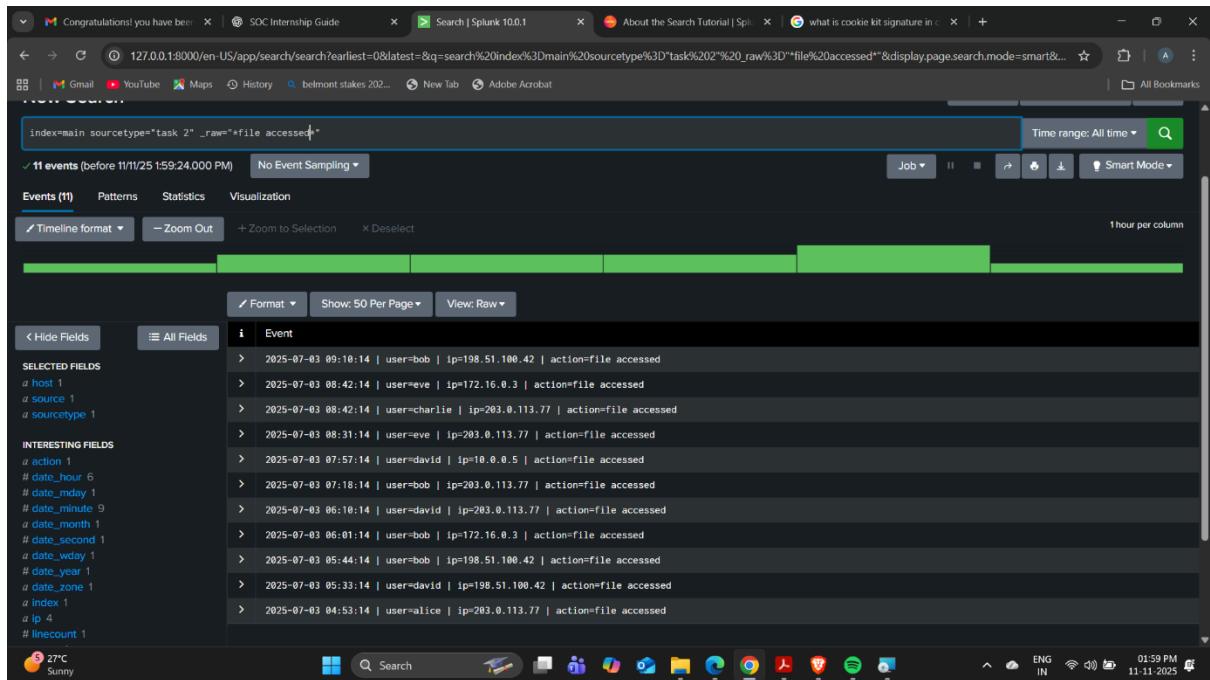


Fig 1.4 File\_accessed

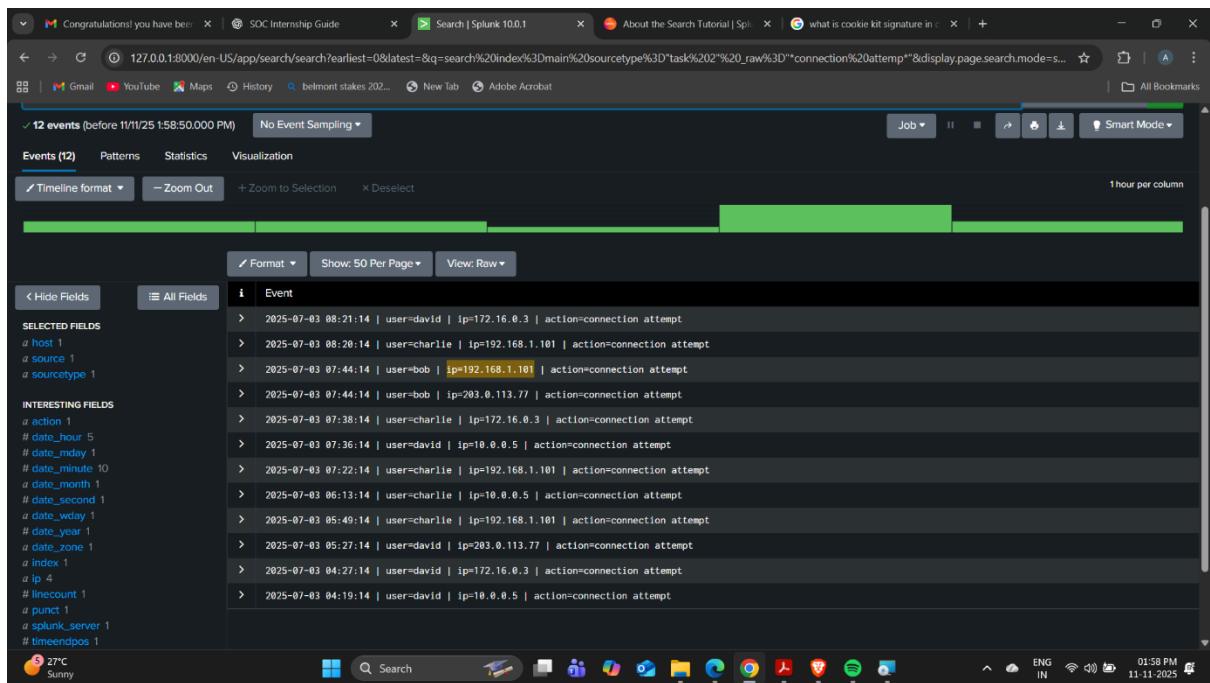


Fig 1.5 Connection\_attempts

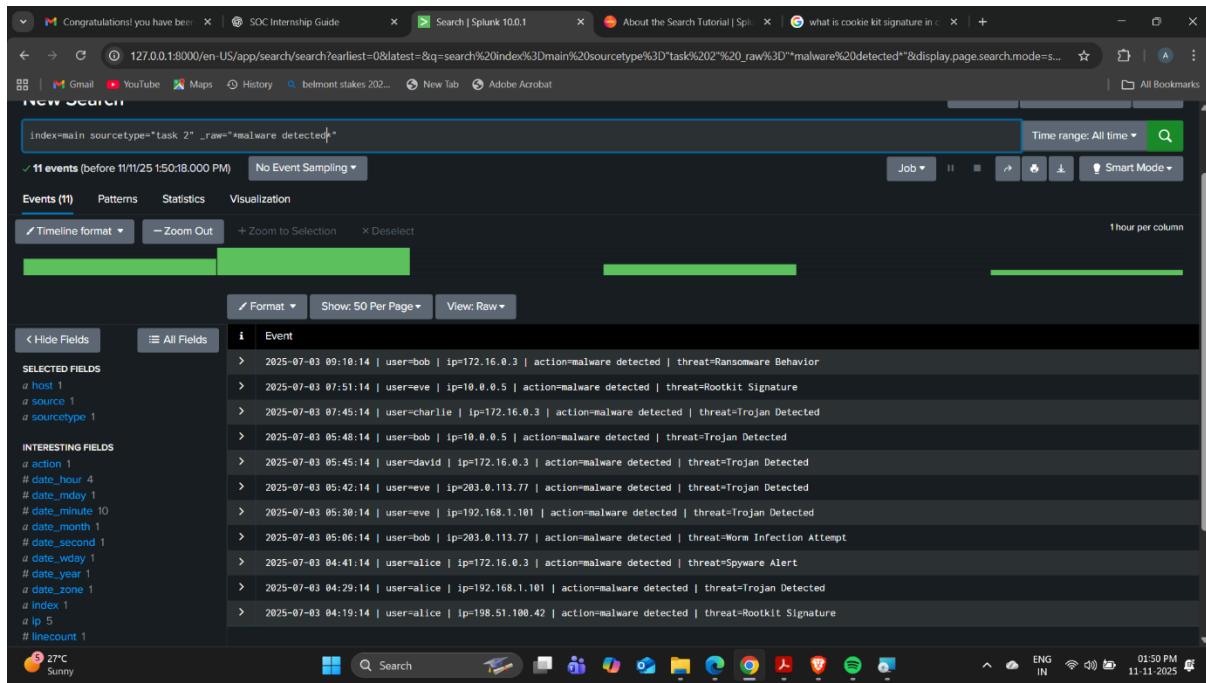


Fig 1.6 Malware\_detection

## 4. Impact Assessment

If left unmitigated, the threats identified could result in:

- **Data Breaches:** Exposure or theft of confidential organizational information.
- **Ransomware Attack:** Encryption of files or system lockdown by malicious software.
- **System Downtime:** Potential DDoS or performance degradation from compromised assets.
- **Credential Compromise:** Unauthorized access to sensitive user accounts or systems.

These risks underline the need for proactive detection and continuous monitoring.

## 5. Incident Response Actions

The following containment and mitigation steps were taken during analysis:

1. **Isolation:** The affected system (user=bob, IP 172.16.0.3) was identified and isolated from the network.
2. **Threat Containment:** Malware indicators were documented, and connection attempts from suspicious IPs were blocked.
3. **Account Protection:** Password reset procedures were initiated for impacted user accounts.
4. **System Review:** Security configurations and recent logins were examined to ensure no additional compromise.
5. **Recovery Measures:** Cleanup and validation were simulated as part of response testing.

## 6. Recommendations & Preventive Measures

To strengthen the organization's security posture:

- **Implement Multi-Factor Authentication (MFA):** Prevent unauthorized access through stolen credentials.
- **Synchronize Logs Using NTP:** Maintain consistent timestamps for accurate incident correlation.
- **Enhance Firewall Rules:** Restrict external IP communication and enforce stricter outbound policies.
- **Conduct Regular Security Scans:** Update antivirus definitions and run scheduled vulnerability scans.
- **Establish Account Lockout Policy:** Automatically disable accounts after multiple failed login attempts.
- **Increase SOC Monitoring:** Create automated alerts in Splunk for repeated login failures and malware detections.

## 7. Summary & Conclusion

The analysis successfully simulated a real-world Security Operations Center (SOC) workflow — from log ingestion to threat detection and response.

The **Trojan malware** detection was identified as the most critical threat, followed by repeated **unauthorized login attempts** and **connection anomalies**.

Through Splunk's SIEM capabilities, all alerts were efficiently correlated, categorized, and assessed based on severity.

The incident was contained within the simulation scope, and preventive recommendations such as **MFA implementation**, **NTP synchronization**, and **enhanced monitoring** were proposed to reduce future risks.