



INCIDENT RESPONSE REPORT

NAME: PAWAN BHARAMBE

**TASK 2: SOC ALERT MONITERING & INCIDENT
RESPONSE**

**PROGRAM: FUTURE INTERNS- CYBERSECURITY
INTERNSHIP**

DATE: OCTOBER 2025

TARGET:SPLUNK SIEM

TASK SUMMARY

This task focused on **monitoring and analyzing system logs using Splunk SIEM** to identify suspicious activities such as failed login attempts, unusual IP addresses, and malware detection alerts. The objective was to simulate real-world **SOC (Security Operations Center) analyst responsibilities** — including monitoring security alerts, analyzing potential threats, and simulating incident response procedures.

TOOLS USED

- **Splunk SIEM (Free Trial)** – For log ingestion, correlation, and analysis.
- **Sample Log File (SOC_Task2_Sample_Logs.txt)** – Dataset containing simulated network events.
- **Manual Filtering and Search Queries** – To identify anomalies and correlate suspicious activities.

MY FINDINGS FROM THE SYSTEM LOGS

1. Failed Login Attempts

Splunk search queries detected **10 failed login attempts** between **7:33 PM and 9:00 PM before 11/2/25**, involving users **Bob, Alice, David, and Charlie**.

Multiple failed attempts originated from **IP 203.0.113.77**, indicating a possible **brute-force attack** targeting user accounts.

Key Observations:

Repeated login failures within a short time frame.

Common source IP (203.0.113.77).

Targeted accounts: Bob, Alice, David, Charlie.

Evidence: Alert1_FailedLogin.png

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

- Search Bar:** Search | Splunk 10.0.1
- Search Query:** index=main "login failed"
- Results:** 10 events (before 11/2/25 7:33:09.000 PM)
- Event List:** The table lists 10 log entries, each containing a timestamp, user ID, IP address, and source information. All entries show a failed login attempt from the IP 203.0.113.77, with the user ID being either bob, alice, david, or charlie.

Time	User	IP Address	Action
2025-07-01 07:33:09.000 AM	user=david	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=david	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=david	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=alice	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=alice	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=bob	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=bob	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=charlie	203.0.113.77	action=login failed
2025-07-01 07:33:09.000 AM	user=charlie	203.0.113.77	action=login failed

- Bottom Status Bar:** 24°C Clear, Search, Home, Taskbar icons, Network status (ENG IN), Battery level (93%), Date (02-11-2025), Time (19:33).

2. Malware Detection Events

Splunk SIEM analysis revealed **22 malware-related alerts** before 11/2/25.

Detected threats included **Ransomware, Rootkit, Trojan, Worm, and Spyware**, affecting multiple user accounts.

Affected Users: Bob, Eve, Charlie, David, Alice

Involved IPs: 172.16.0.3, 10.0.0.5, 192.168.1.101, 203.0.113.77, 198.51.100.42

Notably, **user Bob** was associated with both **Ransomware and Worm infections**, suggesting a **compromised system actively spreading malware**.

Evidence: Alert2_MalwareDetected.png

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

- Search Bar:** "Search | Splunk 10.0.1" and "127.0.0.1:8000/en-US/app/search/search?&q=search%20index%3Dmain%20*malware%20detected%20earliest=0&latest=8&display=page&search.mode=smart&dispatch.sample_ratio=1&worldload...".
- Event List:** 22 events (before 11/2/25 7:34:25.000 PM). The list includes:

 - 7/3/25 9:10:14 AM: user=Bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
 - 7/3/25 9:10:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 9:10:14 AM: user=Bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
 - 7/3/25 9:10:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:59:00 AM: user=alice | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
 - 7/3/25 7:59:00 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:59:14 AM: user=rene | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
 - 7/3/25 7:59:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2
 - 7/3/25 7:45:14 AM: user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
 - 7/3/25 7:45:14 AM: host=somehost_gems | source=SOCK_Tek2_Sample_Log.txt | sourcetype=soc_log2

- Time Range:** All time.
- Visualizations:** Timeline format, Zoom In, Zoom Out, View Selection.
- Bottom Status:** 24°C, ENG IN, 02-11-2025, 19:35.

3. Suspicious External IP Activity (203.0.113.77)

Splunk logs indicated **30 events** involving **externalIP203.0.113.77**, including login attempts, malware detections, and file access activities.

Key Findings:

Login Failures: Users Alice, David

Login Successes: Users Eve, Alice, David

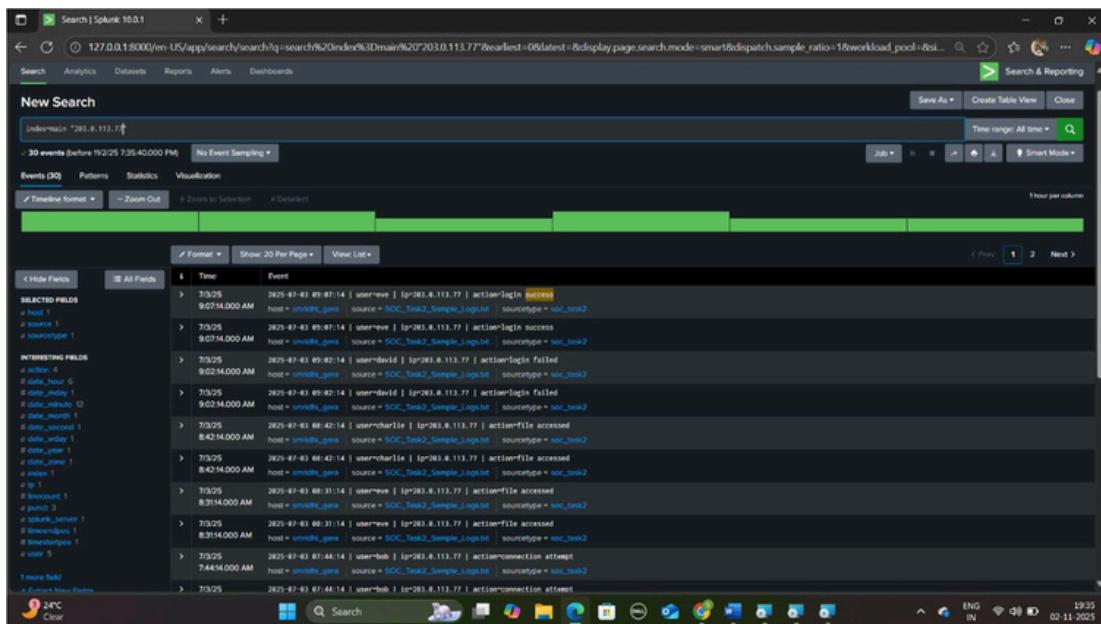
Malware Detected: Trojan and Worm infections (Bob, Eve)

File Access: Bob, Charlie, Eve, David

The simultaneous presence of failed and successful logins strongly suggests that multiple user accounts were compromised.

The IP **203.0.113.77** is considered a **high-risk external threat source** involved in multiple attack vectors.

Evidence: Alert3_SuspiciousIP.png



4. Compromised User Account – (Bob)

Splunk analysis revealed **28 security events** involving **user Bob**, confirming account compromise and active exploitation.

Key Findings:

Ransomware Attack from IP 172.16.0.3

Trojan Infection from IP 10.0.0.5

Worm Activity from IP 203.0.113.77

Failed Logins: From IPs 10.0.0.5, 172.16.0.3

Successful Logins: From IPs 10.0.0.5, 192.168.1.101, 198.51.100.42

Unauthorized File Access: From IPs 198.51.100.42, 203.0.113.77, 172.16.0.3

These combined events confirm that **Bob's account was actively targeted, infected, and exploited** for lateral movement within the network.

Evidence: Alert4_UserBobCompromised.png

INCIDENT SUMMARY

During the log analysis using Splunk SIEM, multiple **coordinated cyber threats** were identified across the monitored network.

Key Incidents Identified:

- Repeated **failed login attempts** targeting multiple user accounts.
- **Malware infections** (Ransomware, Trojan, Rootkit, Worm, Spyware).
- **Suspicious external IP (203.0.113.77)** involved in login and malware events.
- **Compromised account (Bob)** involved in unauthorized access and malware propagation.
-

These patterns indicate a **targeted cyber campaign** involving brute-force attacks, credential compromise, and malware deployment.

IMPACT & RISK ASSESSMENT

Threat	Impacted User(s)	IP(s) Involved	Risk Level	Description
Ransomware	Bob	172.16.0.3	High	Could encrypt data, leading to loss of critical information.
Rootkit	Alice, Eve	198.51.100.42, 10.0.0.5	High	Enables persistence and privilege escalation.

Threat	Impacted User(s)	IP(s) Involved	Risk Level	Description
Failed Logins	Bob, Alice, David, Charlie	203.0.113.77	Medium	Indicates possible brute-force attack.
Suspicious IP	Multiple Users	203.0.113.77	High	Involved in multiple malicious events.
Compromised Account (Bob)	Bob	Multiple IPs	Critical	Account compromised and used for spreading malware.

RECOMMENDED ACTIONS

- 1. Block and isolate affected systems.**
- 2. Reset credentials** for compromised and at-risk user accounts.
- 3. Enable Multi-Factor Authentication (MFA) and account lockout policies.**
- 4. Conduct a full forensic analysis** to identify infection sources.
- 5. Continuously monitor** for suspicious IP activity and failed logins.

Immediate containment and recovery measures are essential to **prevent further damage and data breaches**.

**SIMULATED COMMUNICATION EMAIL TO
STAKEHOLDERS**

SOCManager

To:

Subject: Security Incident Summary – Task 2

Dear Team,

During our routine log analysis using **Splunk SIEM**, several high-risk security alerts were detected, including **failed login attempts, malware infections, and suspicious external IP activity**. User **Bob's account appears to be compromised**, showing evidence of **ransomware infection and unauthorized access**.

Recommended immediate actions:

- Block malicious IP **203.0.113.77**
- Isolate affected endpoints
- Reset credentials for impacted users

Please review the attached report for details and initiate remediation steps accordingly.

SOCAnalyst—Future Interns Cybersecurity