



## **INCIDENT RESPONSE REPORT**

**NAME: SMRIDHI GERA**

**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
- URL:** 127.0.0.1:8000/en-US/app/search/search?\_q=search%20index%3Dmain%20\*login%20failed\*&earliest=-8latest=&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=...
- Events (10):** Shows 10 events found before 11/2/25 7:33:09.000 PM.
- Time Range:** All time.
- Event Log:** Displays 10 log entries, each showing a failed login attempt from IP 203.0.113.77 to various users (david, alice, bob, charlie) via host smrdk\_geme on SOC\_Task2\_Sample\_Logs.txt.
- Fields:** Shows selected fields like host, source, and action, and interesting fields like date\_hour, date\_minute, date\_second, date\_usec, index, and user.

## 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
- URL:** 127.0.0.1:8000/en-US/app/search/search?&q=search%20index%3Dmain%20detected%20&earliest=-8&latest=&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_...
- Header:** Search, Analytics, Datasets, Reports, Alerts, Dashboards, Save As, Create Table View, Close.
- Section:** New Search
- Search Query:** indexname = "malware detected"
- Event Count:** 22 events (before 11/25/25 7:34:25.000 PM)
- Sampling:** No Event Sampling
- Time Range:** All time
- Job Status:** Job
- Visualizations:** Timeline format, Zoom Out, + Zoom to Selection, X Deselect, 1 hour per column.
- Event List:** The list shows 22 events from various hosts and sources, mostly from SOC\_Task2\_Sample\_Log.txt, detailing malware detections and threat types like Ransomware, Rootkit, and Trojan.

### 3. Suspicious External IP Activity (203.0.113.77)

Splunk logs indicated **30 events** involving **external IP 203.0.113.77**, 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

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

- Search Bar:** index=main 203.0.113.77
- Results Summary:** 30 events (before 11/2/25 7:35:40.000 PM)
- Event List:** The list displays 30 events across various time points on July 25, 2025. Some key entries include:
  - 2025-07-25 07:14:00 AM | user=eve | ip=203.0.113.77 | action=login success
  - 2025-07-25 07:14:00 AM | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 07:14:00 AM | user=david | ip=203.0.113.77 | action=login success
  - 2025-07-25 07:14:00 AM | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
  - 2025-07-25 09:02:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
  - 2025-07-25 09:02:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
  - 2025-07-25 08:42:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
  - 2025-07-25 08:42:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
  - 2025-07-25 08:42:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
  - 2025-07-25 08:31:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
  - 2025-07-25 08:31:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
  - 2025-07-25 07:44:14 | host=smbd\_gen | source=SO\_C\_Tek2\_Sample\_Log.txt | sourcetype=soc\_task2
  - 2025-07-25 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
- Fields Panel:** Shows selected fields like host, user, source, and sourcetype, along with a list of interesting fields including action, date, and file.
- Bottom Status:** 24°C, Clear, ENG IN, 19:35, 02-11-2025

## 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

Search | Splunk 10.0.1

127.0.0.1:8000/en-US/app/search/search?\_q=search%20index%3Dmain%20%user%3Dbob&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=&si=

Analytics Datasets Reports Alerts Dashboards

New Search

Save As Create Table View Close

Time range: All time

[index=main \*user=bob]

28 events (before 11/2/25 7:36:10,000 PM) No Event Sampling

Events (28) Patterns Statistics Visualization

Timeline format    Job

1 hour per column

Format Show 20 Per Page View List

Time Event

	Time	Event
SELECTED FIELDS	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# host 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# source 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# sourcetype 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
INTERESTING FIELDS	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# action 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# date_hour 5	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# date_mday 10	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# date_month 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# date_second 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# date_time 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# date_zone 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# index 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# ip 5	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# location 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# punct 3	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# sparkle_server 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# threat 3	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# timestamp 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# timespan 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# user 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
# user_ip 1	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[128.51.100.42]   action=file accessed host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2
+ Extract New Fields	> 7/3/25 9:10:44 AM	2025-07-03 09:10:14   user=bob   ip[172.16.0.3]   action=malware detected   threat=Ransomware Behavior host = smrdr_gene source = SOC_Task2_Sample_Log.txt sourcetype = soc_task2

24°C Clear

ENG IN 02 11:25

## 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
<b>Ransomware</b>	Bob	172.16.0.3	<b>High</b>	Could encrypt data, leading to loss of critical information.
<b>Rootkit</b>	Alice, Eve	198.51.100.42, 10.0.0.5	<b>High</b>	Enables persistence and privilege escalation.

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

## **RECOMMENDED ACTIONS**

- Block and isolate affected systems.**
- Reset credentials** for compromised and at-risk user accounts.
- Enable Multi-Factor Authentication (MFA)** and **account lockout policies**.
- Conduct a full forensic analysis** to identify infection sources.
- 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**

**To:** SOC Manager

**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.

**Regards,**

**Smridhi Gera**

SOC Analyst – Future Interns Cybersecurity