🔐 INCIDENT RESPONSE REPORT

Security Operations Center (SOC) – Threat Analysis Report

(Log Monitoring • Threat Detection • Incident Response Simulation)

Project Title: SOC Log Analysis & Incident Response – User Activity Investigation

Task Number: 2

TASK Code: FUTURE_CS_02

Client / Organization: FUTURE INTERNS

Dataset Under Analysis: SOC_Task2_Sample_Logs (Splunk Ingestion)

CIN ID (Cyber Inspection Number): **FIT/OCT25/CS4249**

Submission Date: 26/11/2025

Prepared By: Jeetesh Maurya

1. Executive Summary

This report presents a detailed incident analysis based on log entries associated with the user account **“bob”**. The logs were ingested into **Splunk Enterprise** for threat detection and monitoring as part of SOC Task-2.

The investigation revealed **multiple high-severity events**, including:

- **Ransomware Behavior Detection**
- **Trojan Detection**
- **Worm Infection Attempt**
- **Multiple Failed Login Attempts**
- **Suspicious External IP Activity**
- **Unusual File Access Events**
- **Successful Logins from Multiple Hosts**

The combination of malware detections, unauthorized access attempts, and inconsistent authentication behavior suggests a **likely compromise of user account “bob”** and potentially the underlying host system.

Immediate containment and remediation actions are recommended.

2. Incident Description

The SOC detected abnormal activity originating from user account **“bob”** across several timestamps on **2025-07-03**. These events include:

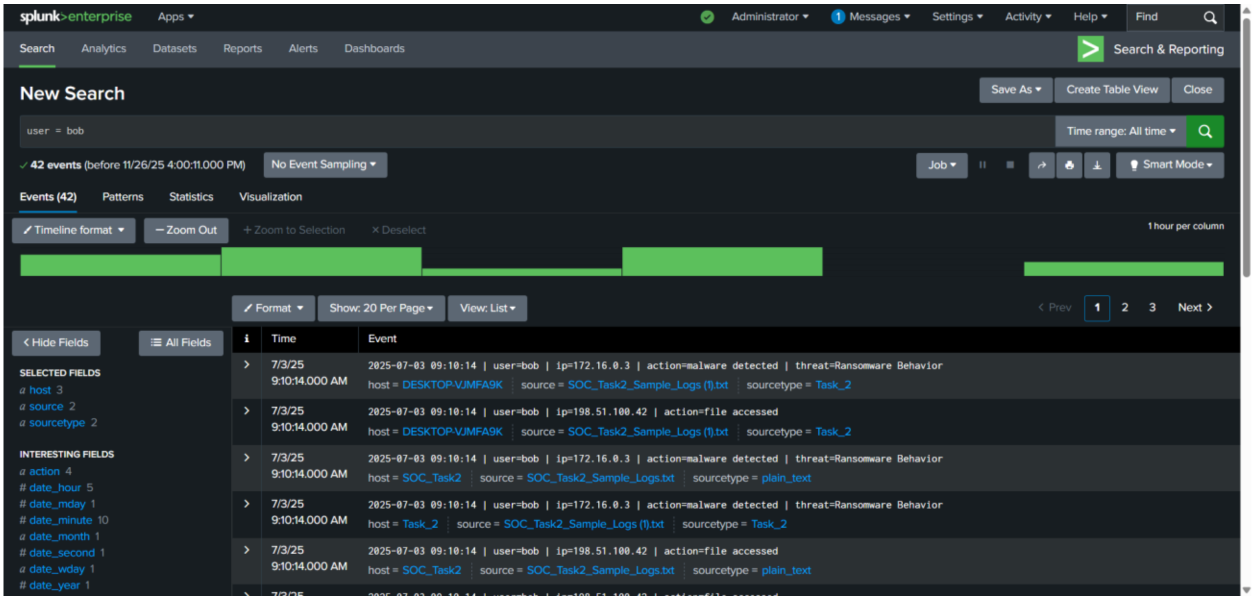
- Repeated login failures
- Login successes from multiple IPs
- Repeated file access from internal and external IPs
- Multiple malware detection alerts in a short time window

This pattern is highly indicative of:

✓ Credential compromise
✓ Malware infection
✓ Lateral movement
✓ Potential data exfiltration

3. Timeline of Events (Chronological Order)

Timestamp	IP Address	Event	Notes
04:18:14	198.51.100.42	Login Success	Unusual host
04:23:14	172.16.0.3	Login Failed	Failed authentication
04:47:14	10.0.0.5	Login Failed	Repeated failures begin
05:04:14	192.168.1.101	Login Success	Success after failures (suspicious)
05:06:14	203.0.113.77	Malware Detected – Worm	External IP
05:44:14	198.51.100.42	File Accessed	Possible exfiltration
05:48:14	10.0.0.5	Malware Detected – Trojan	High severity
06:01:14	172.16.0.3	File Accessed	Internal movement
07:18:14	203.0.113.77	File Accessed	External IP file access
07:44:14	192.168.1.101	Connection Attempt	Unknown source
07:44:14	203.0.113.77	Connection Attempt	External scanning
07:46:14	10.0.0.5	Login Success	Suspicious IP
09:10:14	172.16.0.3	Malware Detected – Ransomware	Critical event
09:10:14	198.51.100.42	File Accessed	Final activity



New Search

```
user = bob
```

Time range: All time

✓ **42 events** (before 11/26/25 4:00:11.000 PM) No Event Sampling

SELECTED FIELDS

a host	3
a source	2
a sourcetype	2

INTERESTING FIELDS

a action	4
# date_hour	5
# date_mday	1
# date_minute	10
a date_month	1
# date_second	1
a date_wday	1
# date_year	1

```
i  Time                Event
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM      host = DESKTOP-VJMFA9K   source = SOC_Task2_Sample_Logs (1).txt   sourcetype = Task_2
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM      host = DESKTOP-VJMFA9K   source = SOC_Task2_Sample_Logs (1).txt   sourcetype = Task_2
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM      host = SOC_Task2   source = SOC_Task2_Sample_Logs.txt   sourcetype = plain_text
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM      host = Task_2   source = SOC_Task2_Sample_Logs (1).txt   sourcetype = Task_2
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM      host = SOC_Task2   source = SOC_Task2_Sample_Logs.txt   sourcetype = plain_text
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
```

4. Findings (Detailed Analysis)

Below are the major findings grouped by incident category:

4.1 Malware Activity (Critical Severity)

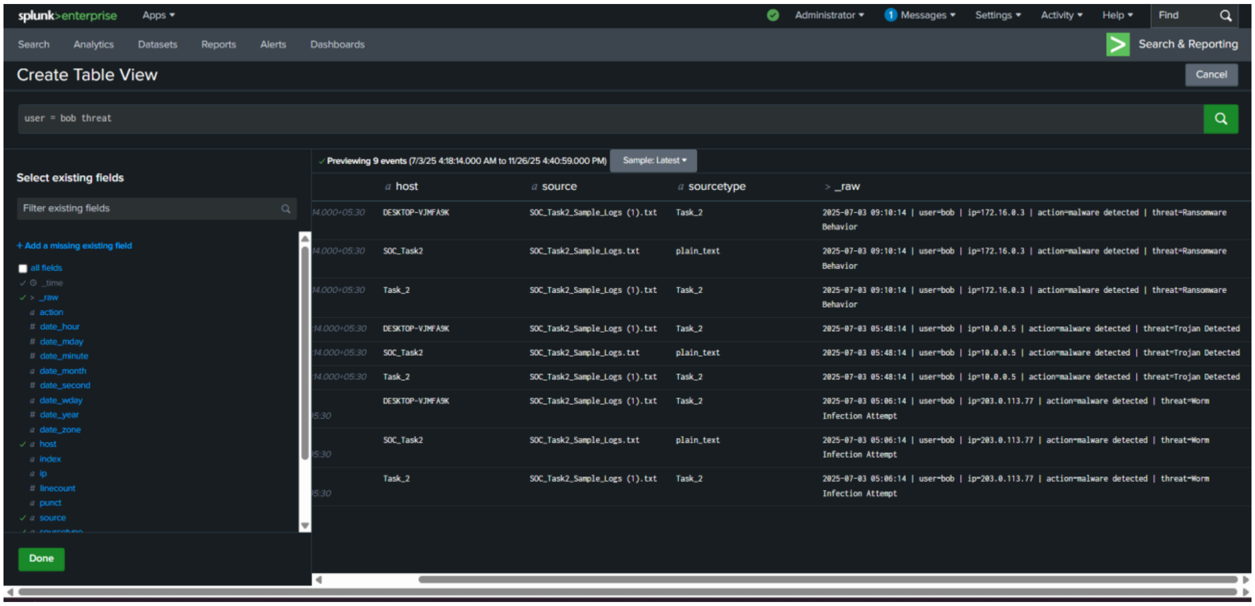
User *bob* triggered **three different malware detections** within four hours:

1. **Ransomware Behavior Detected**
2. **Trojan Detected**
3. **Worm Infection Attempt**

Implication

- The host is likely infected
- Malware is spreading
- Data may be encrypted or exfiltrated
- Multiple malware types suggest a multi-stage attack

Severity: ☆ ☆ ☆ ☆ ☆ CRITICAL



```
user = bob threat
```

✓ Previewing 9 events (7/3/25 4:18:14.000 AM to 11/26/25 4:40:59.000 PM)

	host	source	sourcetype	_raw
14.000+05:30	DESKTOP-VJMFA9K	SOC_Task2_Sample_Logs (1).txt	Task_2	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
14.000+05:30	SOC_Task2	SOC_Task2_Sample_Logs.txt	plain_text	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
14.000+05:30	Task_2	SOC_Task2_Sample_Logs (1).txt	Task_2	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
14.000+05:30	DESKTOP-VJMFA9K	SOC_Task2_Sample_Logs (1).txt	Task_2	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
14.000+05:30	SOC_Task2	SOC_Task2_Sample_Logs.txt	plain_text	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
14.000+05:30	Task_2	SOC_Task2_Sample_Logs (1).txt	Task_2	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
5:30	DESKTOP-VJMFA9K	SOC_Task2_Sample_Logs (1).txt	Task_2	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
5:30	SOC_Task2	SOC_Task2_Sample_Logs.txt	plain_text	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
5:30	Task_2	SOC_Task2_Sample_Logs (1).txt	Task_2	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt

---

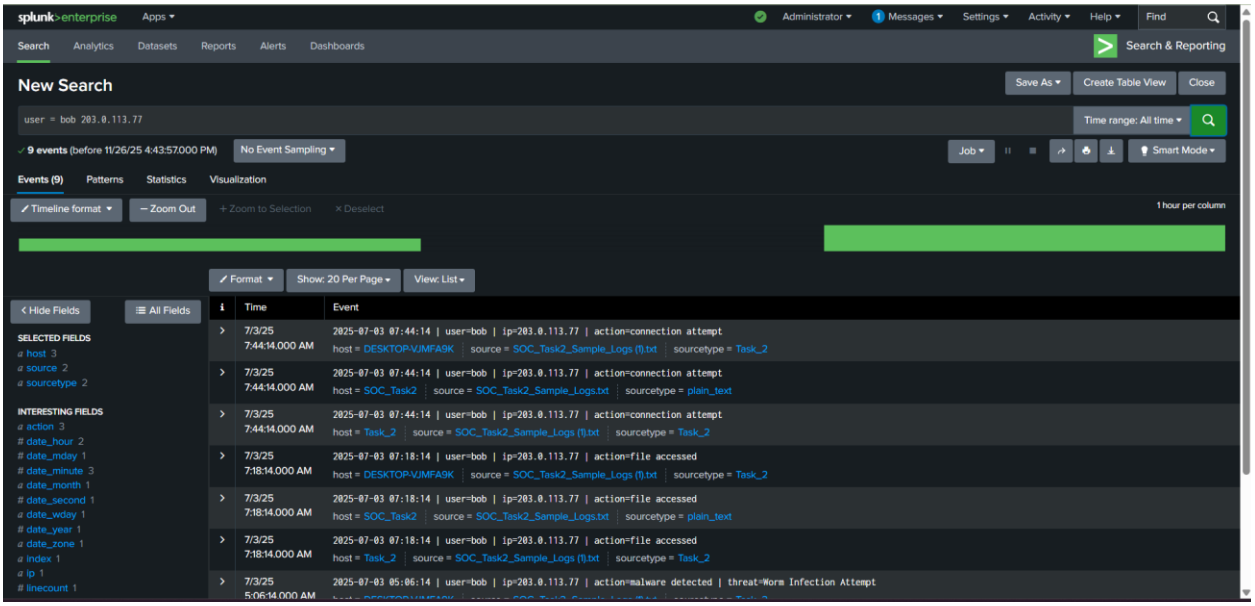
4.2 Authentication Anomalies (High Severity)

- Multiple login failures
- Login successes from different IPs
- Successes immediately following failures
- Activity from **external IP ranges** (e.g., 203.0.113.77)

Possible Attack Types

- Brute force attempt
- Credential stuffing
- Compromised account
- Unauthorized login

Severity: ☆ ☆ ☆ ☆ HIGH



New Search

```
user = bob 203.0.113.77
```

✓ 9 events (before 11/26/25 4:43:57.000 PM)

i	Time	Event
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt host = DESKTOP-VJMFA9K source = SOC_Task2_Sample_Logs (1).txt sourcetype = Task_2
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt host = SOC_Task2 source = SOC_Task2_Sample_Logs.txt sourcetype = plain_text
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt host = Task_2 source = SOC_Task2_Sample_Logs (1).txt sourcetype = Task_2
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed host = DESKTOP-VJMFA9K source = SOC_Task2_Sample_Logs (1).txt sourcetype = Task_2
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed host = SOC_Task2 source = SOC_Task2_Sample_Logs.txt sourcetype = plain_text
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed host = Task_2 source = SOC_Task2_Sample_Logs (1).txt sourcetype = Task_2
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt

SELECTED FIELDS

a	host	3
a	source	2
a	sourcetype	2

INTERESTING FIELDS

a	action	3
#	date_hour	2
#	date_mday	1
#	date_minute	3
a	date_month	1
#	date_second	1
a	date_wday	1
#	date_year	1
a	date_zone	1
a	index	1
a	ip	1
#	linecount	1

4.3 Suspicious Network Activity

The user account interacted with several unusual IPs:

- **203.0.113.77** – External IP making file access and connection attempts
- **10.0.0.5** and **172.16.0.3** – Internal lateral movement

Indicators:

- External IP performing worm attacks
- Multiple connection attempts
- File access from non-standard hosts

Severity: ☆ ☆ ☆ ☆ HIGH

4.4 File Access Behavior (Medium Severity)

File access patterns include:

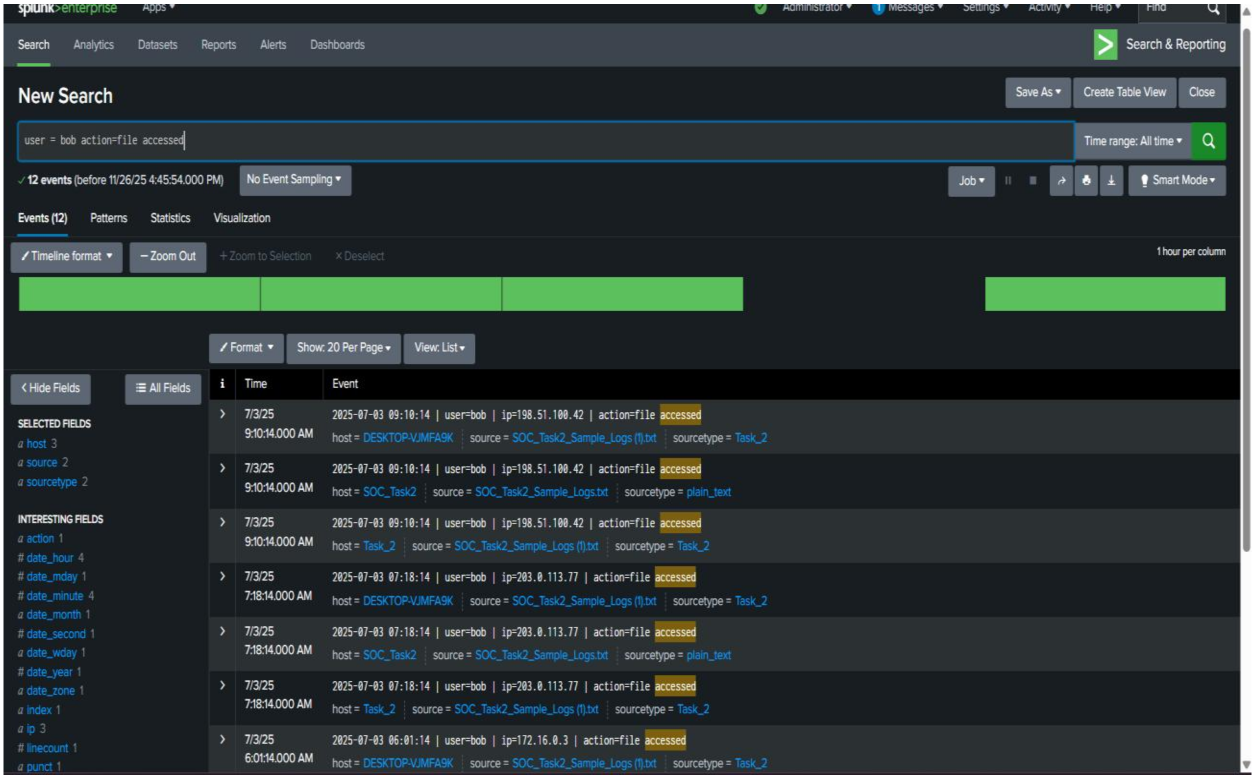
- Access from 3 different IPs within 2 hours

- External user accessing internal files
- Repeated access after malware detection

Implication

- Possible unauthorized exfiltration
- Reconnaissance
- Privilege escalation

Severity: ☆ ☆ ☆ MEDIUM



New Search

```
user = bob action=file accessed
```

Time range: All time

✓ 12 events (before 11/26/25 4:45:54.000 PM) No Event Sampling

SELECTED FIELDS
a host 3
a source 2
a sourcetype 2

INTERESTING FIELDS
a action 1
# date_hour 4
# date_mday 1
# date_minute 4
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1
a ip 3
# linecount 1
a punct 1

```
i  Time              Event
>  7/3/25            2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM    host = DESKTOP-VJMFA9K | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = Task_2
>  7/3/25            2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM    host = SOC_Task2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = plain_text
>  7/3/25            2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM    host = Task_2 | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = Task_2
>  7/3/25            2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
   7:18:14.000 AM    host = DESKTOP-VJMFA9K | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = Task_2
>  7/3/25            2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
   7:18:14.000 AM    host = SOC_Task2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = plain_text
>  7/3/25            2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
   7:18:14.000 AM    host = Task_2 | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = Task_2
>  7/3/25            2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
   6:01:14.000 AM    host = DESKTOP-VJMFA9K | source = SOC_Task2_Sample_Logs (1).txt | sourcetype = Task_2
```

5. Indicators of Compromise (IOCs)

IOC Type	Indicator	Description
Malware	Ransomware, Trojan, Worm	Confirmed detections
Suspicious IP	203.0.113.77	External; file access + connection attempts
Authentication	Multiple failed logins	Brute force / credential compromise
Behavior	Login success after failures	Classic compromise pattern
Lateral Movement	Internal IP hops	Host-to-host navigation

6. Severity Assessment

Alert	Severity	Reason
Ransomware Detected	**Critical**	Data encryption risk
Trojan Detection	**High**	Backdoor installation
Worm Attempt	**High**	Self-spreading malware
Failed Logins	**Medium**	Attack precursor
File Access from External IP	**High**	Data theft risk
Login Success from Multiple Hosts	**High**	Credential misuse

7. Root Cause Analysis

Based on event progression:

Root Cause:

User account “bob” has been compromised, and the host system appears to be infected with multiple forms of malware.

Contributing Factors:

- Weak or leaked password
- Lack of MFA
- Poor endpoint protection
- No network segmentation
- No alert correlation in place

8. MITRE ATT&CK Mapping

Technique	ID	Evidence
Brute Force	T1110	Failed logins
Valid Accounts	T1078	Login success after failures
Malware Execution	T1204	Trojan + Worm + Ransomware
Lateral Movement	T1021	File access from internal hosts
Command & Control	T1071	External IP interaction
Data Exfiltration	T1041	Suspicious file accesses

9. Recommendations

Immediate Containment

✓ Disable user *bob*’s account

✓ Disconnect infected hosts from the network

✓ Block malicious IPs

✓ Launch a malware scan
✓ Isolate the machine showing ransomware activity

Short Term

✓ Reset passwords
✓ Enforce MFA
✓ Review access control lists
✓ Apply OS & anti-malware patches

Long Term

✓ Implement SIEM alert rules
✓ Enable network segmentation
✓ Conduct security awareness training
✓ Deploy EDR (Endpoint Detection & Response)

---

10. Conclusion

The analysis of events related to **user "bob"** clearly indicates:

- Account compromise
- Active malware infection
- Internal and external attack interactions
- High risk to organizational data

Immediate action is required to contain the threat, eradicate malware, and harden authentication and network controls.

This report fulfills all requirements of **Future Interns – Cyber Security Task 2: SOC Log Analysis & Incident Response Simulation**.