Incident response report

Introduction

This report documents the analysis of simulated security logs to identify suspicious activities as part of a SOC internship task.

Tools & Data Used

- Splunk SIEM (for log ingestion and analysis)
- Simulated system and network logs (TXT format)

Incident Summary

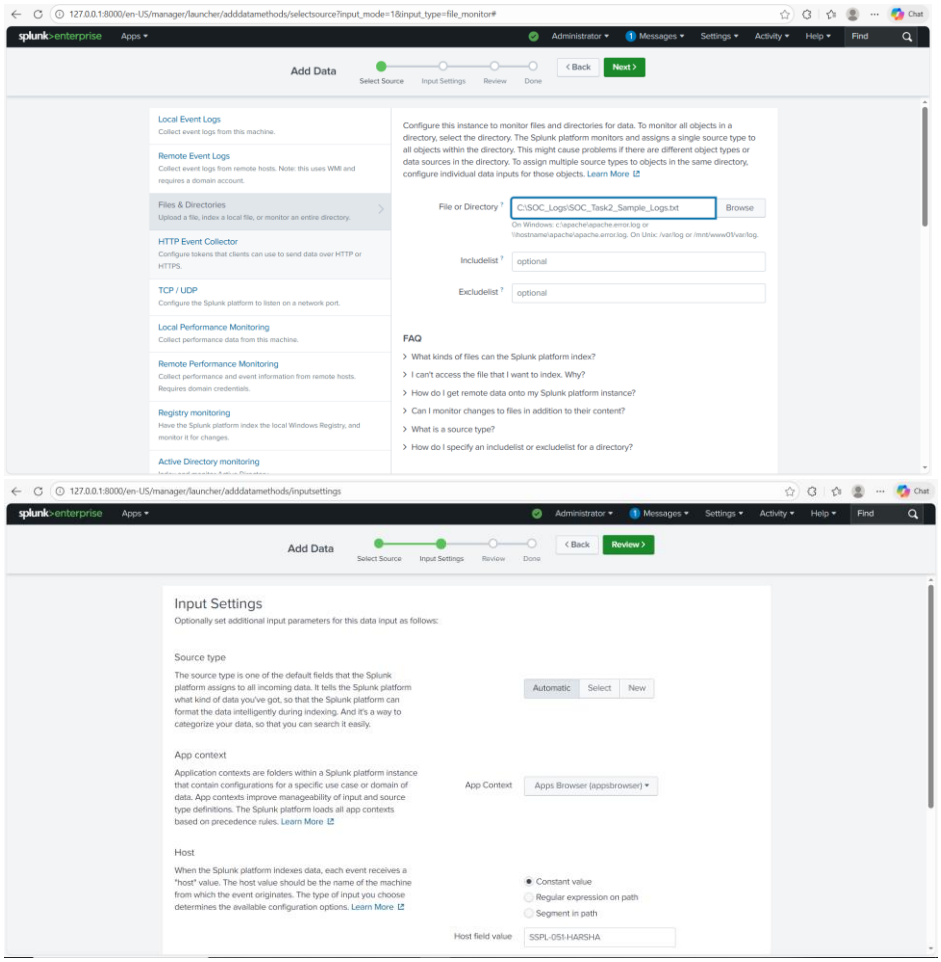
The analysis identified multiple high-risk security incidents, including malware infections, suspicious login behaviour, and repeated connection attempts.

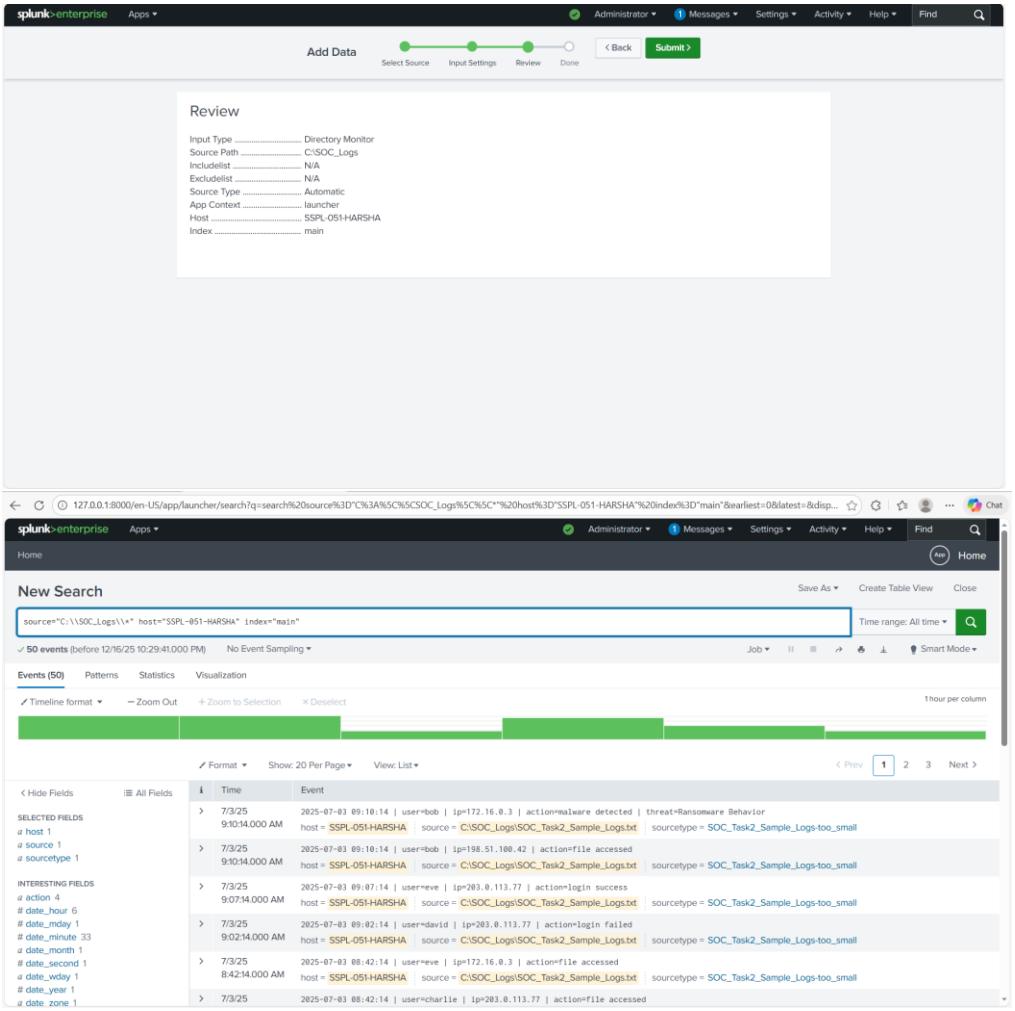
Alert classification logs

Alert ID	Date & Time	User	IP Address	Alert Type	Description	Severity	Action Taken
A1	2025-07-03 04:19	Alice	198.51.100.42	Malware Detection	Rootkit signature detected	High	System isolation recommended
A2	2025-07-03 05:06	Bob	203.0.113.77	Malware Detection	Worm infection attempt	High	Antivirus scan & password reset
A3	2025-07-03 05:48	Bob	10.0.0.5	Malware Detection	Trojan detected	High	Block IP and investigate
A4	2025-07-03 07:45	Charlie	172.16.0.3	Malware Detection	Trojan detected	High	Endpoint monitoring
A5	2025-07-03 09:10	Bob	172.16.0.3	Malware Detection	Ransomware behavior detected	High	Immediate incident escalation

Incident Analysis

Steps taken to upload and analyse the logs in Splunk:





Incident 1: Malware Infection

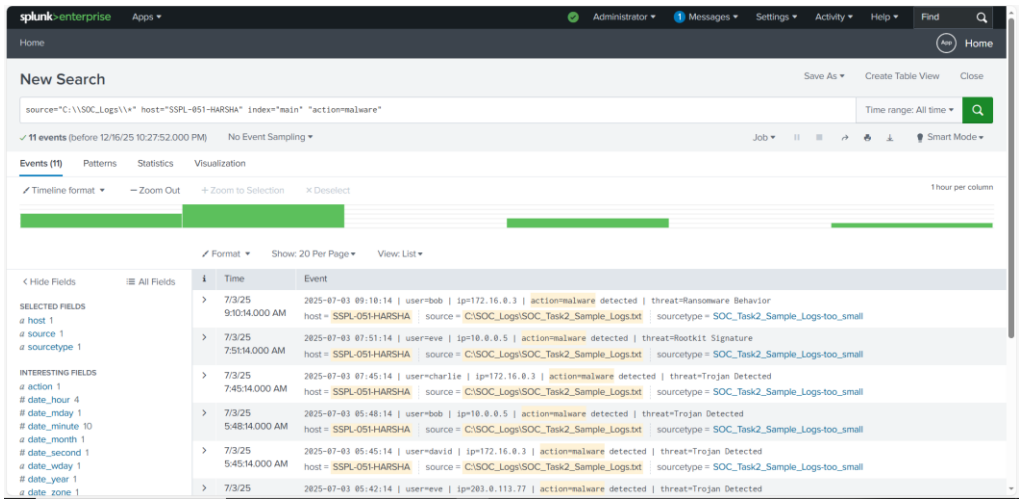


Figure 1: Splunk SIEM showing malware detection alerts

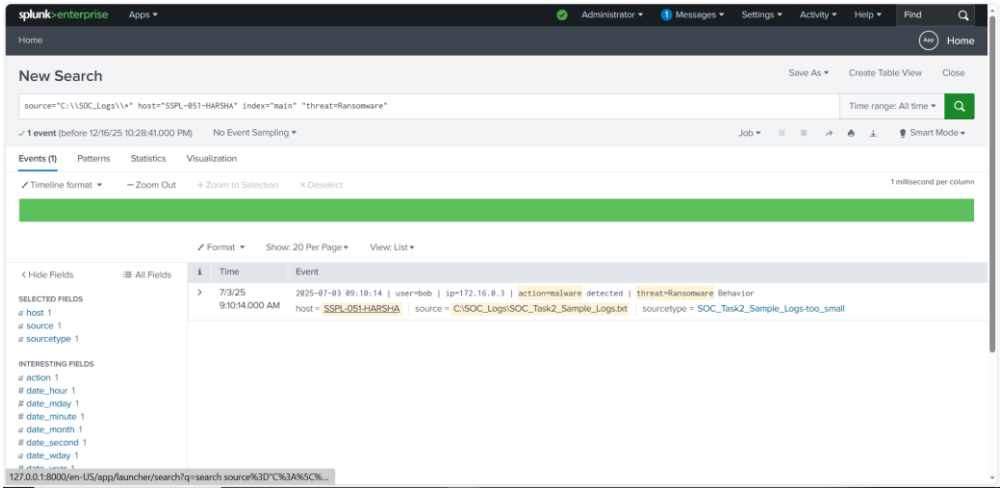


Figure 2: Splunk SIEM showing Ransomware detection alerts

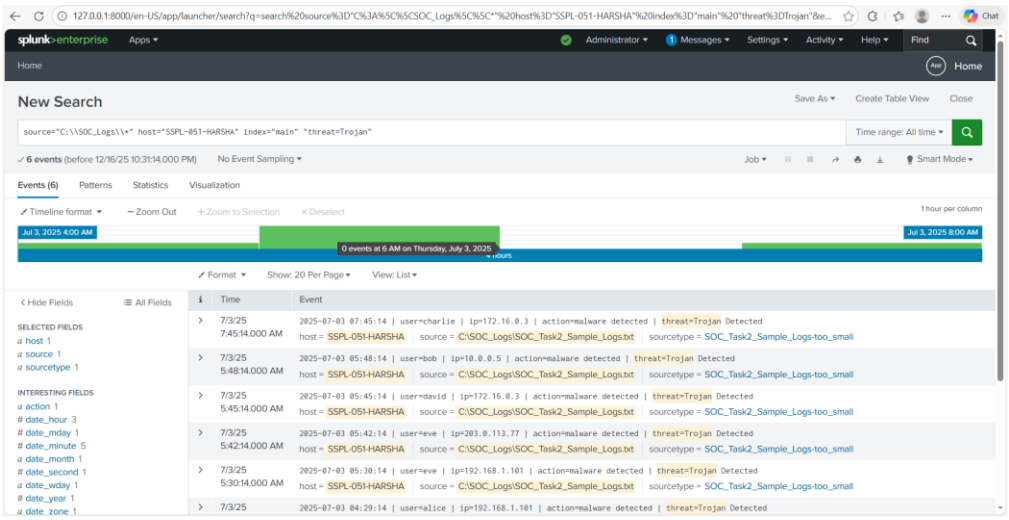


Figure 3: Splunk SIEM showing Trojan malware detection alerts

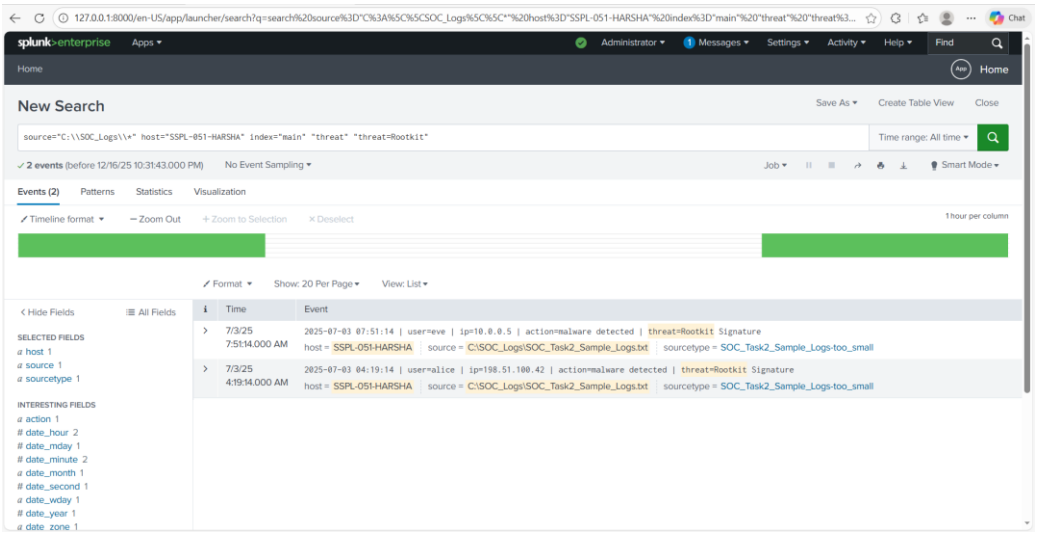


Figure 4: Splunk SIEM showing Rootkit signature alerts

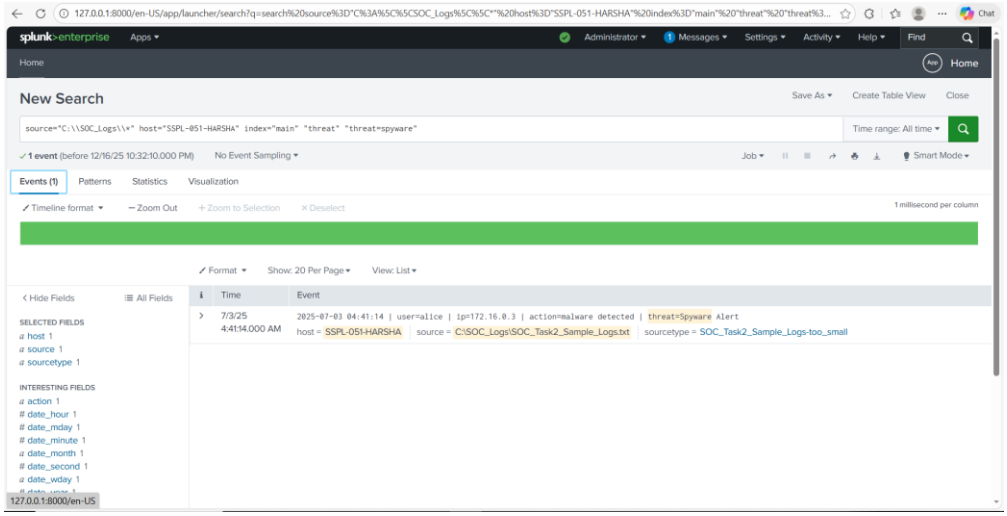


Figure 5: Splunk SIEM showing spyware detection alerts

- **Severity:** High
- **Impact:** Risk of system compromise, data loss, and ransomware spread.
- **Malware detected:** Ransomware, Trojan, Rootkit, Spyware, Worm.
- **Affected Users:** Bob, Alice, David
- **Recommended Action:** Isolate infected systems, run antivirus scans, reset credentials.

Incident 2: Unauthorised Access Risk

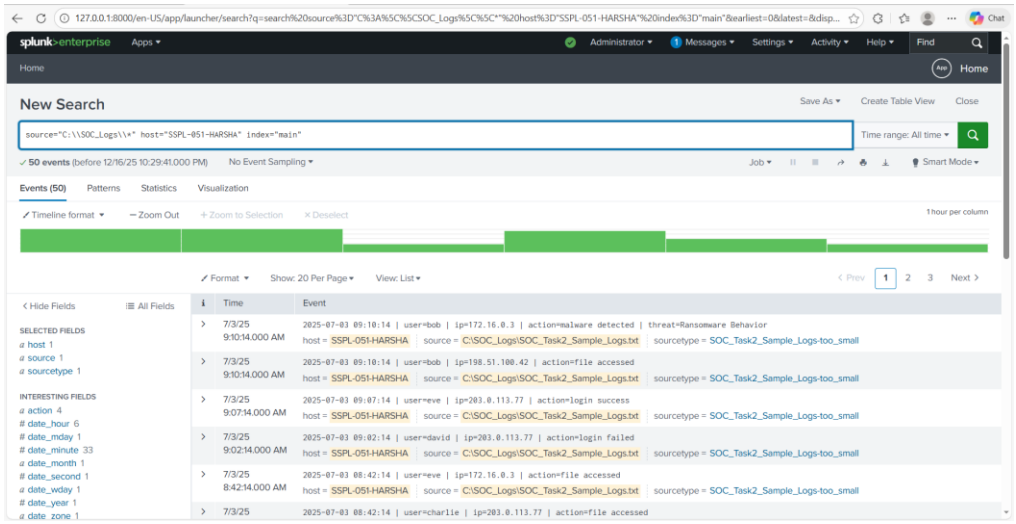


Figure 6: Splunk SIEM showing login after malware detected

- **Severity:** High
- **Description:** Login success detected after malware alerts.
- **Impact:** Potential account takeover.
- **Recommended Action:** Force password resets, enable MFA (Multifactor Authentication).

Incident 3: Suspicious Connection Attempts

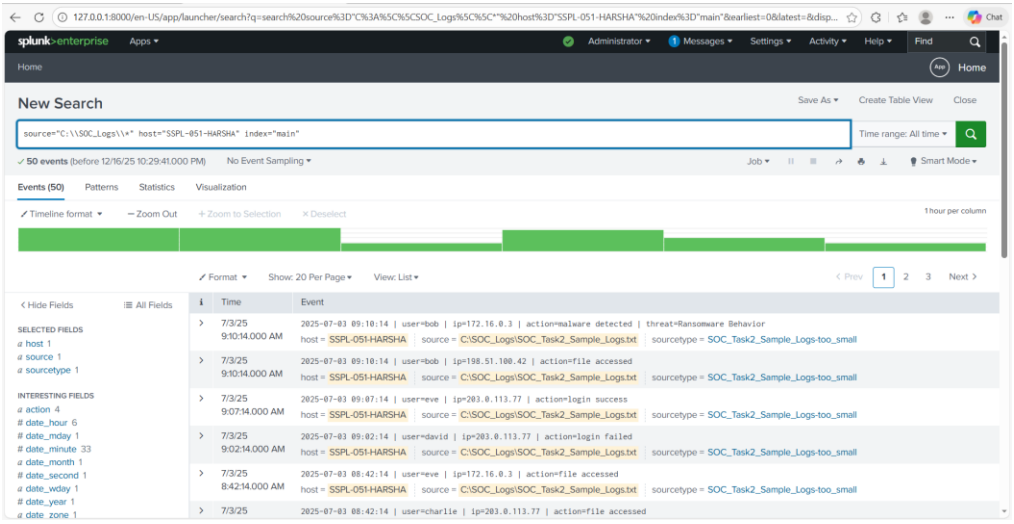


Figure 7: Splunk SIEM showing multiple connection attempts

- **Severity:** Medium
- **Description:** Repeated connection attempts by users.
- **Impact:** Possible reconnaissance activity.
- **Recommended Action:** Monitor IPs, apply firewall rules.

Incident 4: Multiple failed login attempts

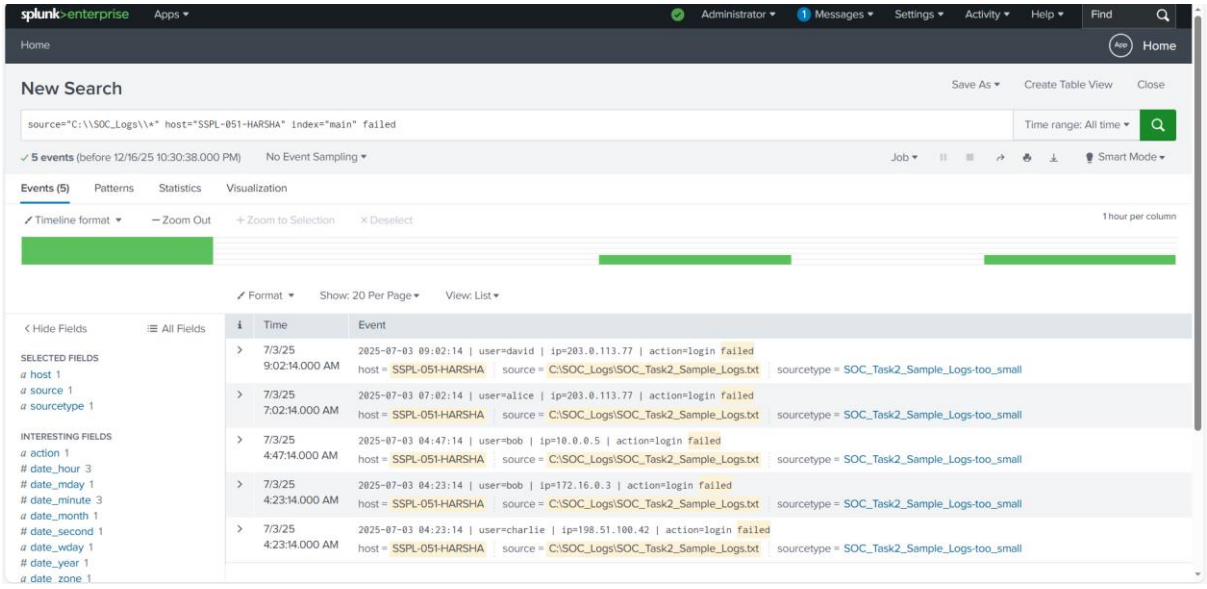


Figure 8: Splunk SIEM showing failed login attempts

- **Severity:** Low
- **Description:** Repeated failed connection attempts by users.
- **Impact:** Possible brute force or DoS attack.
- **Recommended Action:** Monitor Ips.

Splunk Dashboard

‹ Prev 1 2 3 4 5 Next ›

i	Time	Event
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
>	7/3/2025 9:07:14.000 AM	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
>	7/3/2025 9:02:14.000 AM	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
>	7/3/2025 8:42:14.000 AM	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
>	7/3/2025 8:42:14.000 AM	2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
>	7/3/2025 8:31:14.000 AM	2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
>	7/3/2025 8:30:14.000 AM	2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
>	7/3/2025 8:21:14.000 AM	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
>	7/3/2025 8:20:14.000 AM	2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt

Figure 9: Splunk SIEM dashboard

Timeline of Events

Time (2025-07-03)	Event Description
04:18	Login success detected for user *bob* from IP 198.51.100.42
04:19	Malware detected on *alice's* system (Rootkit Signature)
04:27	Repeated connection attempts observed from user *david*
05:06	Malware detected on *bob's* system (Worm Infection Attempt)
05:48	Trojan detected on *bob's* system from IP 10.0.0.5
07:45	Trojan detected on *charlie's* system
09:10	Ransomware behaviour detected on *bob's* system

Conclusion

The detected incidents indicate active security threats that require immediate containment, monitoring, and remediation.

Email to Management

Subject: SOC Alert – Multiple Malware & Suspicious Activities Detected

Dear Management Team,

During SOC monitoring, multiple malware infections and suspicious login activities were detected across systems.

Immediate containment and remediation actions are recommended to prevent further impact.

Regards,
SOC Analyst (Intern)