

# **Incident Response Report**

**-By Using SIEM Tools**

## **Table Of Contents:**

- 1.Incident Summary
- 2.Detection Method(Includes Tools Used)
- 3.Procedure
4. Alert Summary Table
5. Incident Timeline
- 6.Affected Entities(Includes Screen Shots)
- 7.Impact Analysis
- 8.Recommendations
- 9.Conclusion

## Incident Title - Trojan Malware Detection

### 1. Incident Summary:-

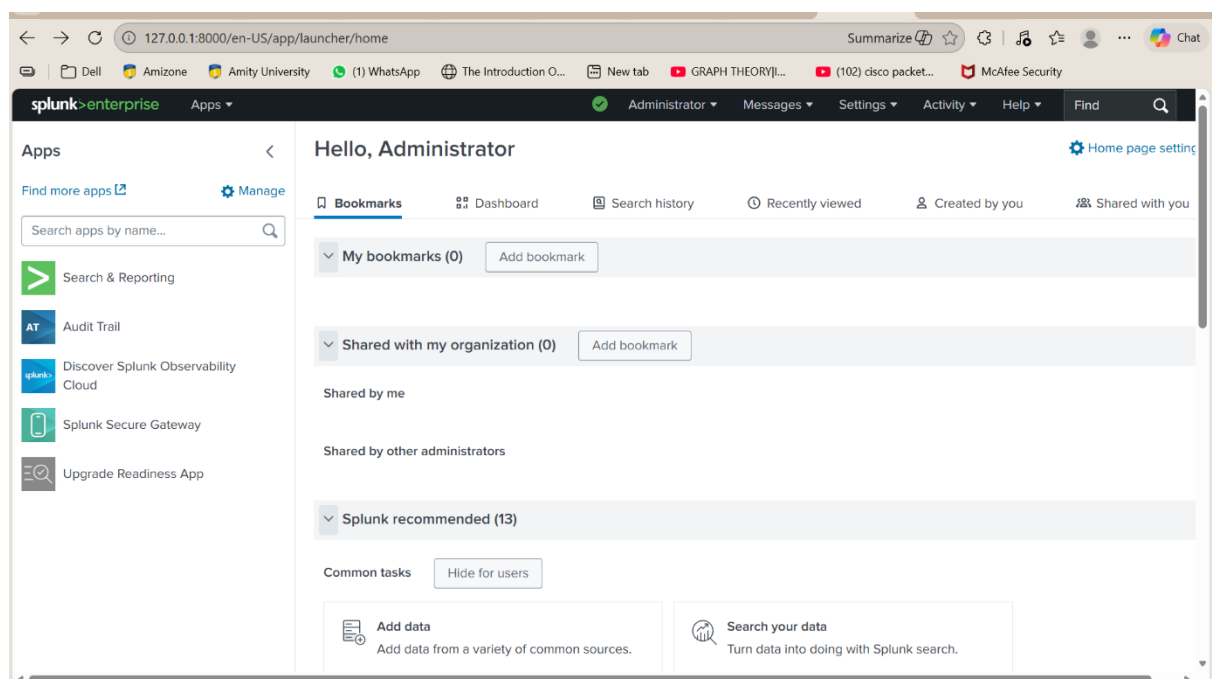
Multiple malware detection alerts indicating Trojan activity were observed in the system logs. These alerts were detected across different users and IP addresses, suggesting a potential malware infection within the environment.

### 2. Detection Method:-

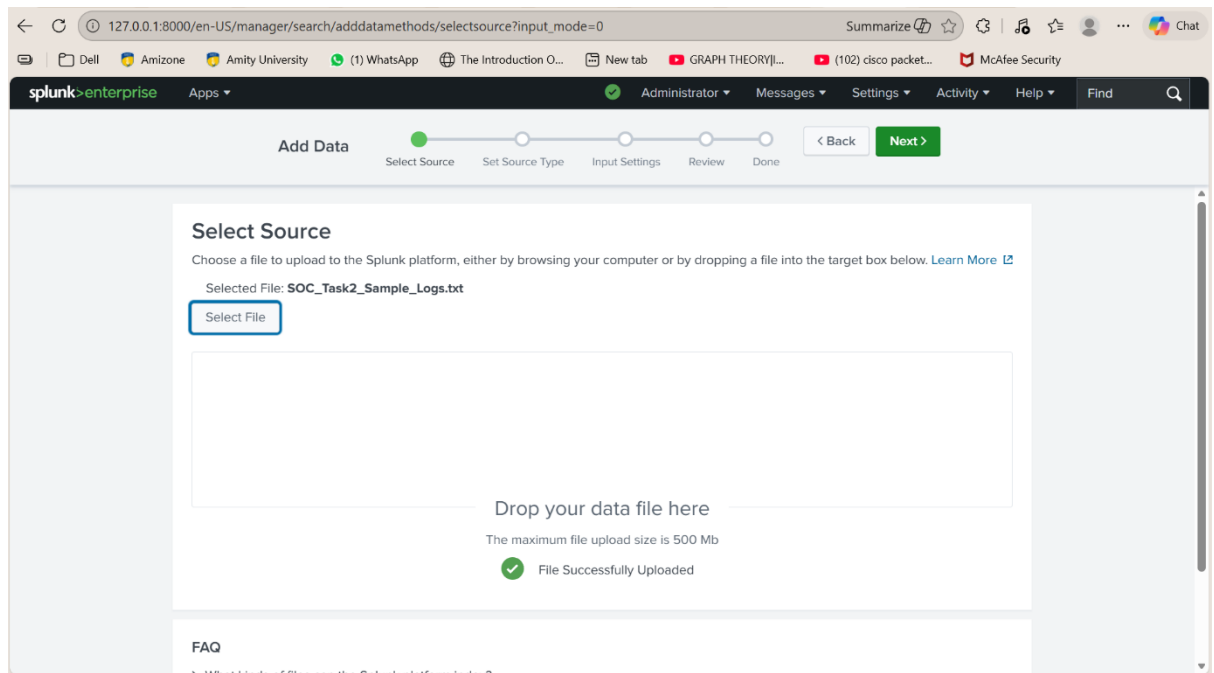
The incident was detected through SIEM log analysis using Splunk, by filtering events where the action field indicated malware detected and the threat type was Trojan Detected.

### 3. Procedure:-

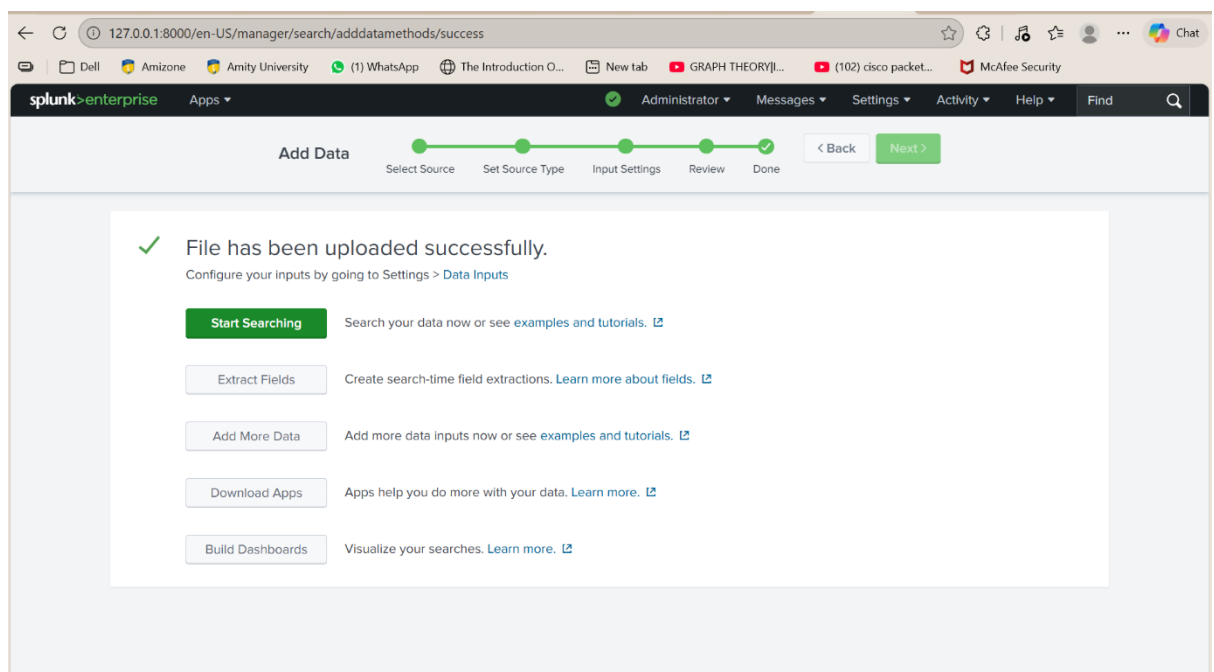
3.1. Splunk was set up as the SIEM tool for log analysis.



3.2. Sample log files were uploaded into Splunk and indexed successfully.

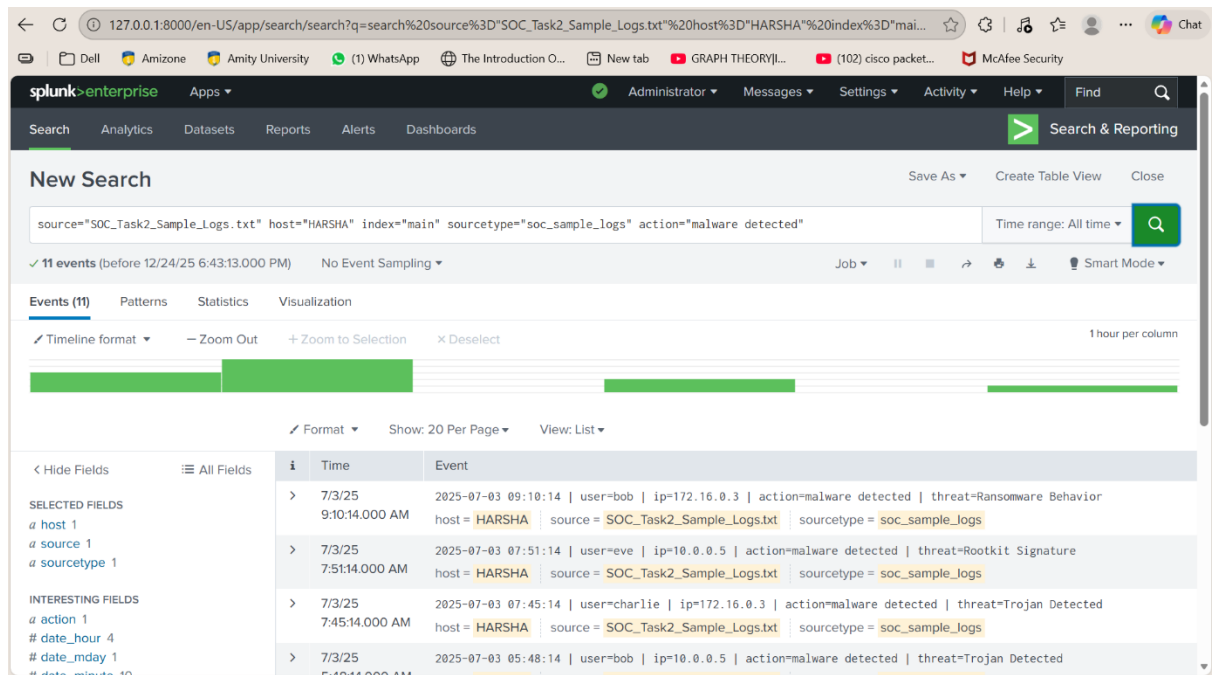


3.3. Log analysis was performed by defining source, index, and host parameters, making the data ready for security queries.



3.4. Malware Detection Query:

```
source="SOC_Task2_Sample_Logs.txt" host="HARSHA" index="main"
sourcetype="soc_sample_logs" action="malware detected"
```



#### 4. Alert Summary Table:-

Alert ID	Alert Type	Severity	Log Source
A-01	Trojan Malware Detected	High	Endpoint Logs
A-02	Multiple Login Failures	Medium	Authentication Logs
A-03	Unusual IP Activity	Medium	Network Logs

#### 5. Incident Timeline

Time (Approx.)	Activity
09:04	Malware detection alert triggered in SIEM
09:10	SOC analyst reviewed logs and identified Trojan activity
09:20	Incident classified as High severity
09:30	Recommended containment and remediation actions documented

#### 6. Affected Entities:-

- **Users:** bob, eve, charlie, alice
- **IP addresses:** 172.16.0.3, 203.0.113.77, 10.0.0.5, 192.168.1.101

Format Show: 20 Per Page View: List		
i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14   user=eve   ip=203.0.113.77   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14   user=eve   ip=192.168.1.101   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	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 host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14   user=alice   ip=172.16.0.3   action=malware detected   threat=Spyware Alert host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs

- **Severity Level:-High**

## 7. Impact Analysis:-

Trojan malware can allow unauthorized access, data theft, and further malware installation. If left unaddressed, this could lead to system compromise and data loss.

## 8. Recommended Actions

- Isolate affected systems from the network
- Perform malware scans and removal
- Reset compromised user credentials
- Monitor network traffic for suspicious activity
- Apply security patches and updates

## 9. Conclusion:-

The investigation confirmed multiple high-severity malware alerts indicating Trojan activity across several user accounts and IP addresses. The detected behaviour suggests a potential system compromise that could lead to unauthorized access, data theft, or further malware spread if left unmitigated. Based on the analysis, the incident was classified as High severity and requires immediate containment and remediation actions. Continuous monitoring and improved security controls are recommended to prevent similar incidents in the future.

