SOC INCIDENT RESPONSE REPORT

Prepared by: Murtaza Sukhsarwala

Cybersecurity Internship Project

Executive Summary

- This report summarizes key suspicious alerts detected using Splunk SIEM.
- High severity malware, failed logins, and unusual file access indicate attempted compromise.

Top Suspicious Alerts

- Ransomware Behavior – High
- Rootkit Detection – High
- Trojan Detection – High
- Failed Login Attempts – Medium
- Suspicious File Access – High

Incident Timeline

- 04:19 – Rootkit detected
- 05:48 – Trojan detected
- 07:02 – Failed logins
- 08:42 – Suspicious file access
- 09:10 – Ransomware detected

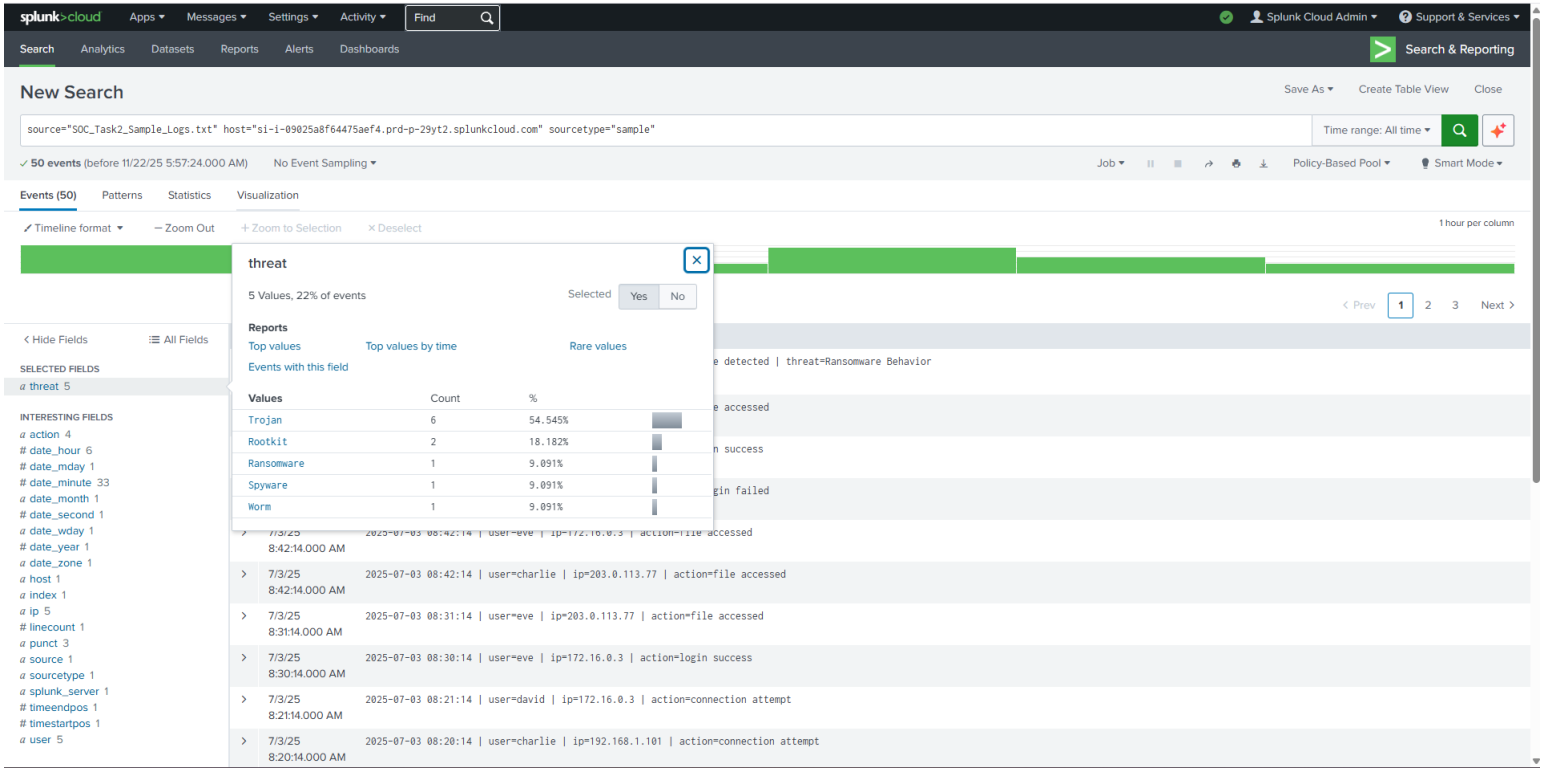
Impact & Risk

- • Multiple high-risk malware infections detected.
- • Signs of credential theft and brute-force attempts.
- • Possible lateral movement inside the network.

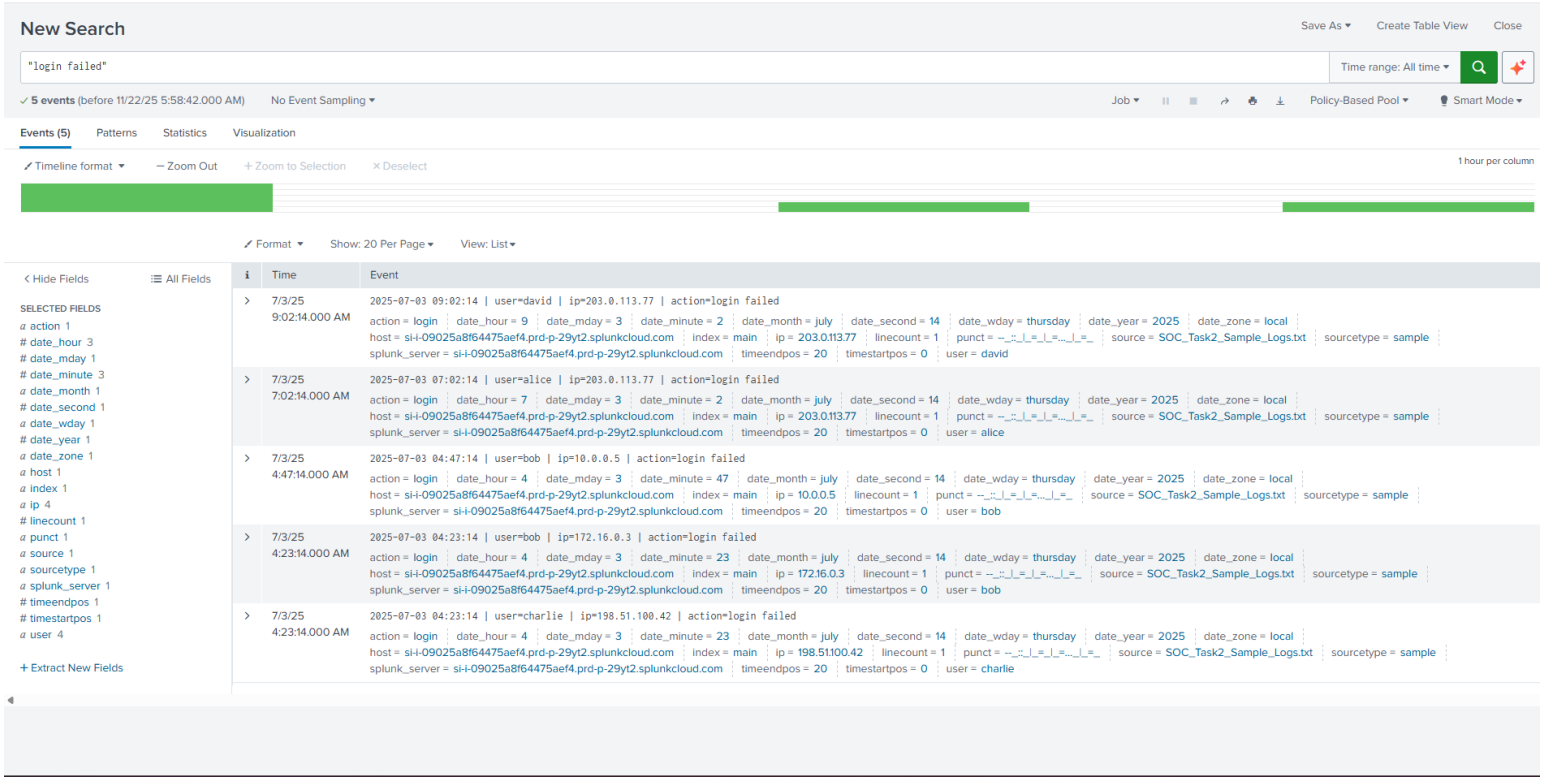
Recommended Actions

- Immediate: Isolate hosts, block malicious IPs.
- Short-Term: Reset passwords, analyze logs.
- Long-Term: Implement SIEM rules, deploy EDR.

SIEM Dashboard Screenshot



SIEM Dashboard Screenshot



SIEM Dashboard Screenshot