SOC Incident Response Report

Executive Summary

This condensed SOC report summarizes key suspicious alerts detected in SIEM (Splunk). High■severity malware events, failed logins, and unusual file access indicate attempted compromise and potential lateral movement.

Top Suspicious Alerts

- **Ransomware Behavior (High)** – Bob, IP 172.16.0.3
- **Rootkit Detection (High)** – Alice, IP 198.51.100.42
- **Trojan Detection (High)** – Bob, IP 10.0.0.5
- **Failed Login Attempts (Medium)** – IP 203.0.113.77
- **Suspicious File Access (High)** – Charlie after malware alerts

Incident Timeline

- **04:19** – Rootkit detected on Alice
- **05:48** – Trojan detected on Bob
- **07:02** – Failed logins from 203.0.113.77
- **08:42** – Suspicious file access by Charlie
- **09:10** – Ransomware detected on Bob

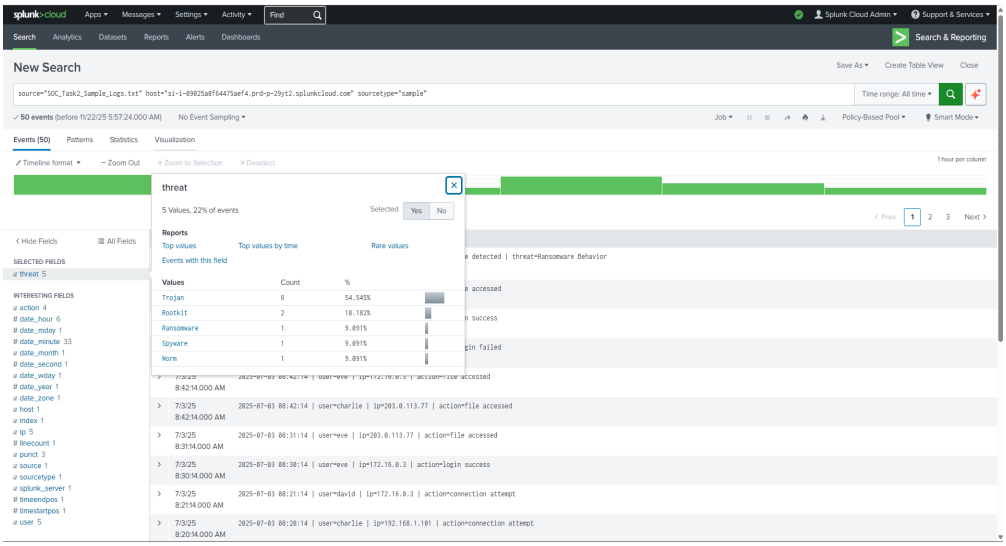
Impact & Risk

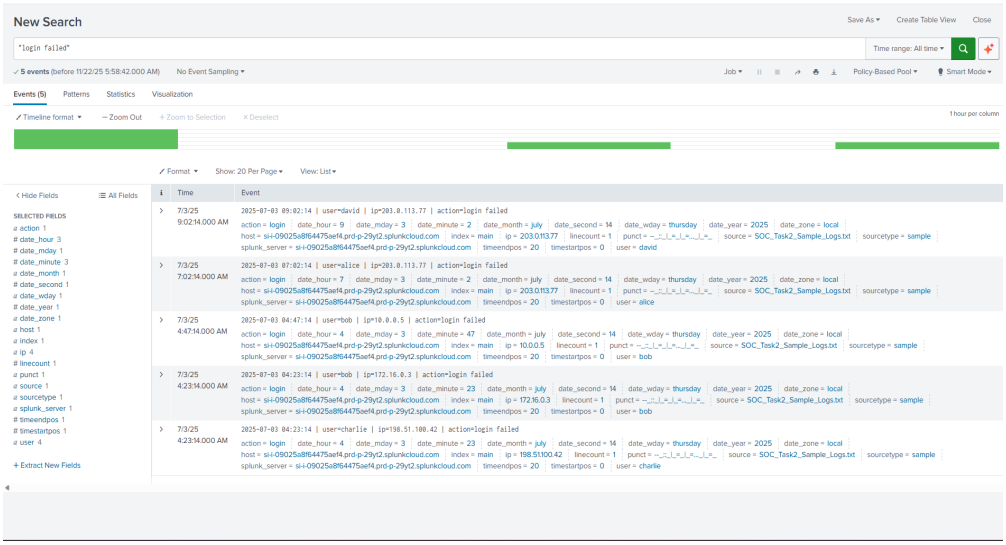
Multiple high■risk malware detections indicate deep compromise. Brute-force attempts and unusual file access suggest credential theft and lateral movement.

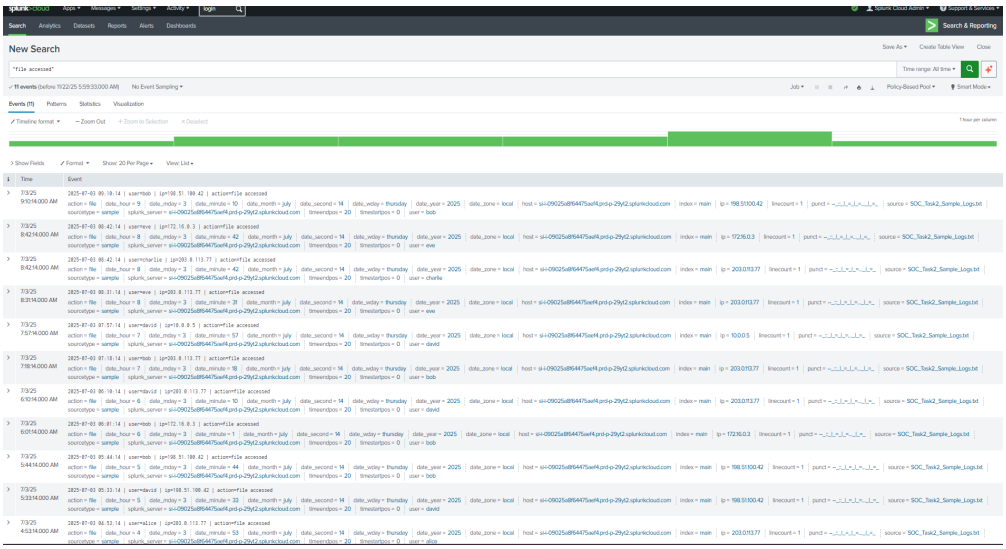
Recommended Actions

Immediate: Isolate infected hosts, block malicious IPs, reset user credentials.
Short■Term: Review past 7■day logs, patch endpoints, run full malware scans.
Long■Term: Implement SIEM alert rules, deploy EDR, enforce stronger hardening.

SIEM Dashboard Screenshots


splunk>cloud
New Search
source="SOC_Task2_Sample_Logs.txt" host="si-i-09025a8f64475aef4.prd-p-29yt2.splunkcloud.com" sourcetype="sample"
50 events (before 11/22/25 5:57:24.000 AM)
Events (50)
Patterns
Statistics
Visualization
threat
5 Values, 22% of events
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
Trojan
6
54.545%
Rootkit
2
18.182%
Ransomware
1
9.091%
Spyware
1
9.091%
Worm
1
9.091%


New Search
"login failed"
5 events (before 11/22/25 5:58:42.000 AM)
Events (5)
Patterns
Statistics
Visualization
Time
Event
7/3/25 9:02:14.000 AM
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
7/3/25 7:02:14.000 AM
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
7/3/25 4:47:14.000 AM
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
7/3/25 4:23:14.000 AM
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
7/3/25 4:23:14.000 AM
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed


New Search
"file accessed"