

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

New Search

source="SOC_Task2_Sample_Logs.txt" host="si-i-09825abf64473af4.prd-p-29y2.splunkcloud.com" sourcetype="sample"

50 events (before 11/22/25 5:57:24 AM) No Event Sampling ▾

Events (50) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

threat

5 Values, 22% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values Count %

Trojan 6 54.54% action=accessed

Rootkit 2 18.18% threat=threat

Ransomware 1 9.09% threat=Ransomware Behavior

Spyware 1 9.09% threat=malware

None 1 9.09% threat=none

action=success

action=failed

1 hour per column

◀ Hide Fields ▶ All Fields

SELECTED FIELDS

threat: 5

INTERESTING FIELDS

action 4 # date_hour 5 # date_minute 5 # date_month 33 # date_minute 1 # date_second 1 # date_wday 1 # date_year 1 # date_zone 1 # host 1 # index 1 # ip 3 # location 1 # punct 3 # source 1 # sourcetype 1 # splunk_server 1 # timestamp 1 # timestampos 1 # user 9

Events (50)

source="SOC_Task2_Sample_Logs.txt" host="si-i-09825abf64473af4.prd-p-29y2.splunkcloud.com" sourcetype="sample"

50 events (before 11/22/25 5:57:24 AM) No Event Sampling ▾

Events (5) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

login failed

5 events (before 11/22/25 5:58:42 AM) No Event Sampling ▾

Events (5) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

Format Show 20 Per Page ▾ View: List ▾

◀ Hide Fields ▶ All Fields

SELECTED FIELDS

action 1 # date_hour 3 # date_minute 1 # date_month 1 # date_second 1 # date_wday 1 # date_year 1 # date_zone 1 # host 1 # index 1 # ip 4 # location 1 # punct 1 # source 1 # sourcetype 1 # splunk_server 1 # timestamp 1 # timestampos 1 # user 4

+ Create New Fields

Events (5)

source="SOC_Task2_Sample_Logs.txt" host="si-i-09825abf64473af4.prd-p-29y2.splunkcloud.com" sourcetype="sample"

5 events (before 11/22/25 5:58:42 AM) No Event Sampling ▾

Events (5) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

login failed

5 events (before 11/22/25 5:59:33 AM) No Event Sampling ▾

Events (5) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

Time range: All time ▾

Save As ▾ Create Table View Close

Search & Reporting

Splunk Cloud Admin Support & Services