

Incident Response Report

Name: Mayur Sandipan Jadhav

Date: 16 August 2025

Incident Title: Multiple Security Alerts Detected Through Splunk SIEM Monitoring

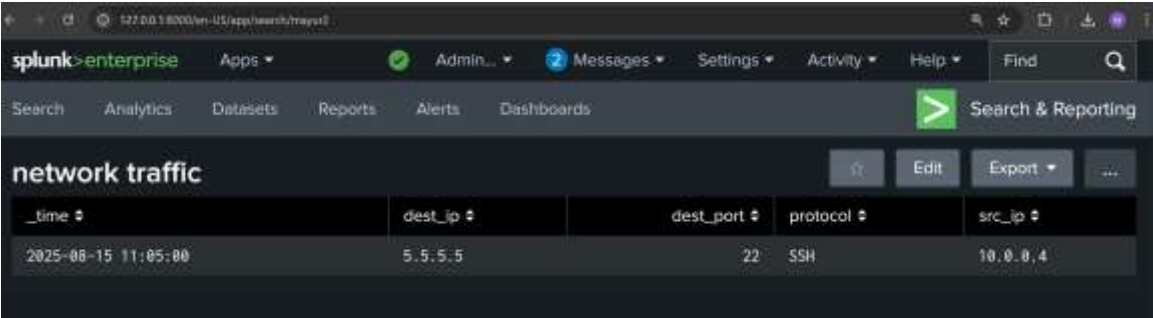
Summary:

During routine log monitoring using Splunk SIEM, multiple suspicious activities were detected across network traffic, firewall logs, and malware alerts.

Findings & Evidence:

- 1. Network Traffic Anomaly (SSH Attempt): src_ip 10.0.0.4, dest_ip 5.5.5.5, port 22 (SSH).

Screenshot:



The screenshot shows the Splunk SIEM interface with a search bar at the top. Below the search bar, there are tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search & Reporting' tab is active. The main content area displays a table titled 'network traffic'. The table has columns for _time, dest_ip, dest_port, protocol, and src_ip. The data row shows a timestamp of 2025-08-15 11:05:00, dest_ip 5.5.5.5, dest_port 22, protocol SSH, and src_ip 10.0.0.4.

| _time | dest_ip | dest_port | protocol | src_ip |
|---------------------|---------|-----------|----------|----------|
| 2025-08-15 11:05:00 | 5.5.5.5 | 22 | SSH | 10.0.0.4 |

- 2. Firewall Logs: 203.0.113.10 blocked on 3389, 198.51.100.5 blocked on 22.

Screenshot:



The screenshot shows the Splunk SIEM interface with a search bar at the top. Below the search bar, there are tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search & Reporting' tab is active. The main content area displays a table titled 'Firewall_logs'. The table has columns for _time, source, timestamp, src_ip, status, dest_ip, and dest_port. The data rows show two blocked connections: one from 203.0.113.10 to 10.0.0.10 on port 3389, and another from 198.51.100.5 to 10.0.0.11 on port 22.

| _time | source | timestamp | src_ip | status | dest_ip | dest_port |
|---------------------|-------------------|------------------|--------------|---------|-----------|-----------|
| 2025-08-15 13:00:00 | firewall_logs.csv | 2025-08-15 13:00 | 203.0.113.10 | blocked | 10.0.0.10 | 3389 |
| 2025-08-15 13:10:00 | firewall_logs.csv | 2025-08-15 13:10 | 198.51.100.5 | blocked | 10.0.0.11 | 22 |

- 3. Malware Alert: PC1 infected with Trojan.Generic (High severity).

Screenshot:

Malware_Alerts

Global Time Range: Last 24 hours

| _time | malware_name | severity | hostname |
|-------------------------------|----------------|----------|----------|
| 2025-08-15T12:00:00.000+05:30 | Trojan.Generic | High | PC1 |

4. Failed Login Attempts: User john had 2 failed attempts.

Screenshot:

Login_failed

| _time | host | action | src_ip | user |
|---------------------|-------|--------|-------------|-------|
| 2025-08-15 10:04:00 | Mayur | failed | 18.0.0.3 | admin |
| 2025-08-15 10:03:00 | Mayur | failed | 192.168.1.5 | john |
| 2025-08-15 10:01:00 | Mayur | failed | 192.168.1.5 | john |
| 2025-08-15 10:10:00 | Mayur | failed | 172.16.0.2 | guest |

Impact & Risk Assessment:

- Unauthorized SSH Attempt: Medium risk
- Firewall Blocked Traffic: High risk
- Malware Infection: High risk
- Failed Login Attempts: Low-Medium risk

Recommendations / Remediation:

- Block suspicious IPs
- Conduct malware removal on PC1
- Reset passwords, enforce MFA
- Monitor SSH/RDP ports
- Update antivirus and SIEM rules

Conclusion:

Splunk monitoring identified multiple security incidents requiring immediate mitigation steps.

Prepared by: Mayur Sandipan Jadhav