

Incident Response Report

1. Executive Summary

This report summarizes the analysis of three types of simulated security logs ingested into Splunk Enterprise: Failed login attempts, Web access logs, and Malware detection alerts. The goal was to detect, categorize, and prioritize potential threats, then recommend remediation steps.

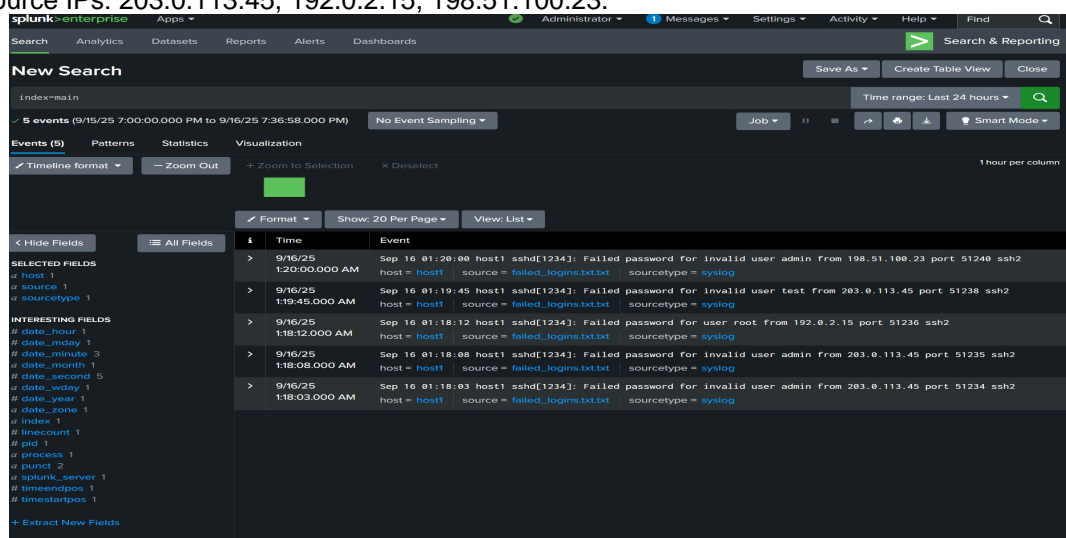
2. Data Sources & Methods

Failed Logins (failed_logins.txt) → Syslog events showing SSH login attempts. **Web Access Logs** (web_access.log.txt) → Syslog events showing HTTP GET/POST requests. **Malware Alerts** (malware_alerts.log) → Antivirus detections of different malware types. All logs were uploaded into Splunk (index = main, sourcetype = syslog). Queries were used to search, filter, and analyze events.

3. Findings

3.1 Failed Logins

- Multiple failed password attempts observed.
- Attackers tried different usernames (admin, root, test).
- Source IPs: 203.0.113.45, 192.0.2.15, 198.51.100.23.



The screenshot shows the Splunk Enterprise interface with a search for failed login attempts. The search results table is as follows:

Time	Event
9/16/25 1:20:00.000 AM	Sep 16 01:20:00 host1 sshd[1234]: Failed password for invalid user admin from 198.51.100.23 port 51240 ssh2 host = host1 source = failed_logins.txt.txt sourcetype = syslog
9/16/25 1:19:45.000 AM	Sep 16 01:19:45 host1 sshd[1234]: Failed password for invalid user test from 203.0.113.45 port 51238 ssh2 host = host1 source = failed_logins.txt.txt sourcetype = syslog
9/16/25 1:18:12.000 AM	Sep 16 01:18:12 host1 sshd[1234]: Failed password for user root from 192.0.2.15 port 51236 ssh2 host = host1 source = failed_logins.txt.txt sourcetype = syslog
9/16/25 1:18:08.000 AM	Sep 16 01:18:08 host1 sshd[1234]: Failed password for invalid user admin from 203.0.113.45 port 51235 ssh2 host = host1 source = failed_logins.txt.txt sourcetype = syslog
9/16/25 1:18:03.000 AM	Sep 16 01:18:03 host1 sshd[1234]: Failed password for invalid user admin from 203.0.113.45 port 51234 ssh2 host = host1 source = failed_logins.txt.txt sourcetype = syslog

3.2 Web Access Logs

- Detected repeated access attempts to login and admin endpoints.
- Suspicious User-Agent strings suggest possible automated tools (curl, scripts).
- Key IPs: 198.51.100.23, 192.0.2.99.

New Search

Save As Create Table View Close

Index=main

Time range: Last 24 hours

10 events (9/15/25 7:00:00.000 PM to 9/16/25 7:38:50.000 PM)

No Event Sampling

Job

Smart Mode

Events (10) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect 1 hour per column

Format Show: 20 Per Page View: List

Hide Fields All Fields

SELECTED FIELDS

host 2

source 2

sourcetype 1

INTERESTING FIELDS

date_hour 1

date_mday 1

date_minute 3

date_month 1

date_second 5

date_wday 1

date_year 1

date_zone 1

i	Time	Event
>	9/16/25 7:38:31.000 PM	198.51.100.23 - - [16/Sep/2025:02:05:00 +0000] "GET /wp-login.php HTTP/1.1" 200 234 "-" "Mozilla/5.0" host = soye_btc source = web_access.log.txt sourcetype = syslog
>	9/16/25 7:38:31.000 PM	192.0.2.99 - - [16/Sep/2025:02:00:00 +0000] "GET / HTTP/1.1" 200 1024 "-" "Mozilla/5.0" host = soye_btc source = web_access.log.txt sourcetype = syslog
>	9/16/25 7:38:31.000 PM	203.0.113.45 - - [16/Sep/2025:01:25:50 +0000] "POST /login HTTP/1.1" 401 120 "-" "Mozilla/5.0" host = soye_btc source = web_access.log.txt sourcetype = syslog
>	9/16/25 7:38:31.000 PM	198.51.100.23 - - [16/Sep/2025:01:25:40 +0000] "GET /admin HTTP/1.1" 404 209 "-" "curl/7.68.0" host = soye_btc source = web_access.log.txt sourcetype = syslog
>	9/16/25 7:38:31.000 PM	203.0.113.45 - - [16/Sep/2025:01:25:30 +0000] "GET /login HTTP/1.1" 200 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)" host = soye_btc source = web_access.log.txt sourcetype = syslog

3.3 Malware Alerts

- Multiple malware detections logged by antivirus.
- Malware types: Trojan, Ransomware, Worm, Spyware, Adware.
- Hosts affected: PC-01, PC-02, PC-03, PC-04.

a index 1

linecount 1

a malware 5

pid 1

a process 2

a punct 10

a splunk_server 1

timeendpos 1

a timestamp 1

timestartpos 1

+ Extract New Fields

>	9/16/25 10:22:55.000 AM	Sep 16 10:22:55 hostD antivirus: MALWARE DETECTED adware.exe on C:\Program Files\app\ad.exe host=PC-04 malware=Adware host = hostD source = malware_alerts.txt sourcetype = syslog
>	9/16/25 10:18:22.000 AM	Sep 16 10:18:22 hostA antivirus: MALWARE DETECTED spyware.exe on C:\Users\alice\AppData\Local\spy.dll host=PC-01 malware=Spyware host = hostA source = malware_alerts.txt sourcetype = syslog
>	9/16/25 10:15:10.000 AM	Sep 16 10:15:10 hostC antivirus: MALWARE DETECTED worm.exe on C:\Windows\Temp\update.tmp host=PC-03 malware=Worm host = hostC source = malware_alerts.txt sourcetype = syslog
>	9/16/25 10:12:45.000 AM	Sep 16 10:12:45 hostB antivirus: MALWARE DETECTED ransomware.exe on C:\Users\bob\Documents\finance.docx host=PC-02 malware=Ransomware host = hostB source = malware_alerts.txt sourcetype = syslog
>	9/16/25 10:10:02.000 AM	Sep 16 10:10:02 hostA antivirus: MALWARE DETECTED trojan.exe on C:\Users\alice\Downloads\invoice.exe host=PC-01 malware=Trojan host = hostA source = malware_alerts.txt sourcetype = syslog

4. Recommendations

1. Failed Logins

- Block repeated failed IPs at firewall.
- Enforce strong password + multi-factor authentication.
- Enable account lockout after failed attempts.

2. Web Access Logs

- Apply WAF (Web Application Firewall) rules.
- Patch vulnerable web applications.
- Monitor suspicious user agents.

3. Malware Alerts

- Isolate infected hosts.
- Perform malware removal and forensic investigation.
- Update antivirus signatures and EDR policies.

5. Conclusion

Splunk successfully detected brute-force login attempts, suspicious web requests, and malware infections. These findings demonstrate the importance of SIEM monitoring in identifying and prioritizing threats before they escalate.