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.

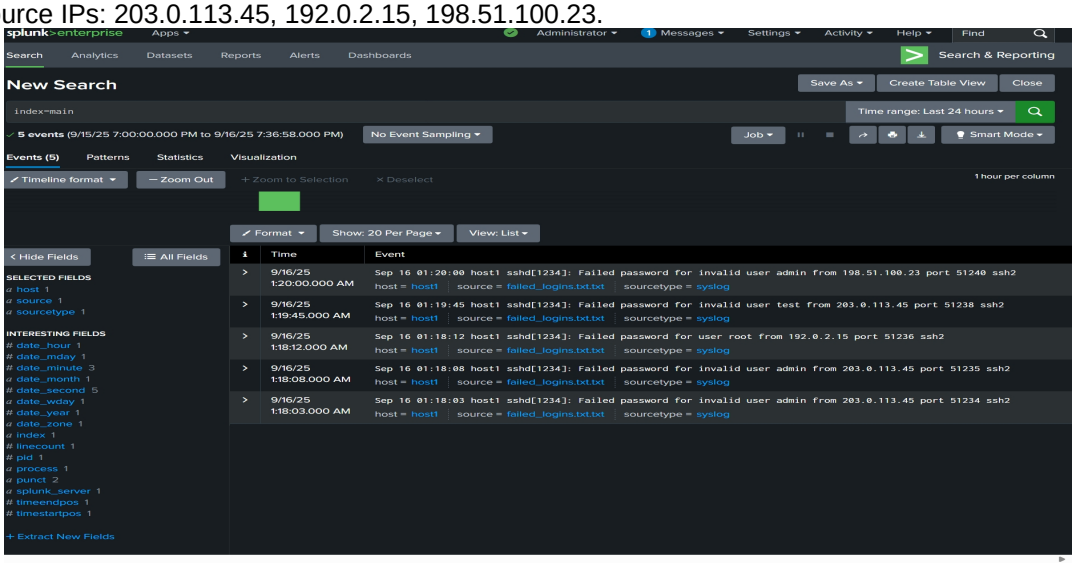
2. Data Sources & Methods

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

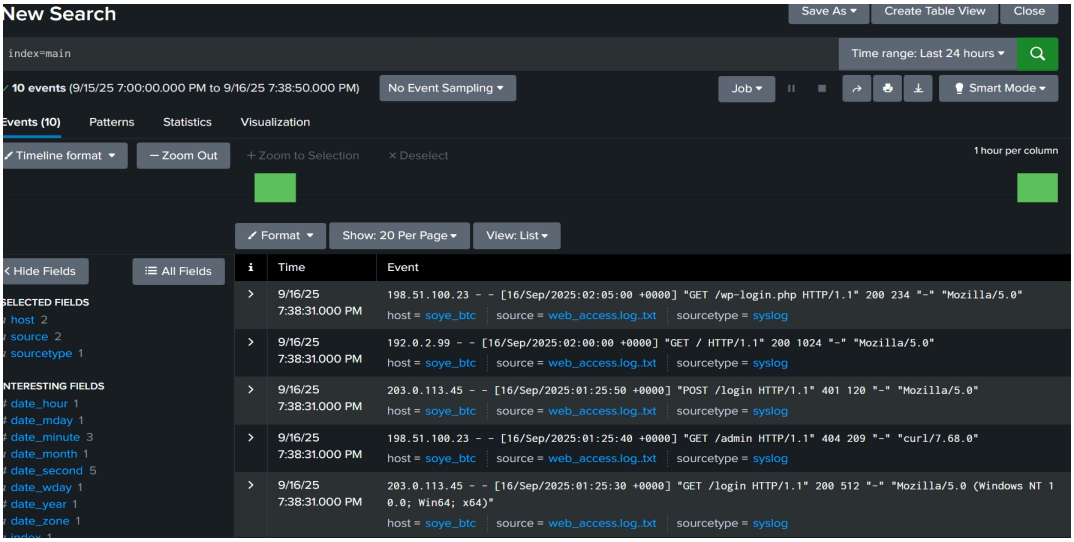
3.1 Failed Logins

• 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.



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.



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.

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.