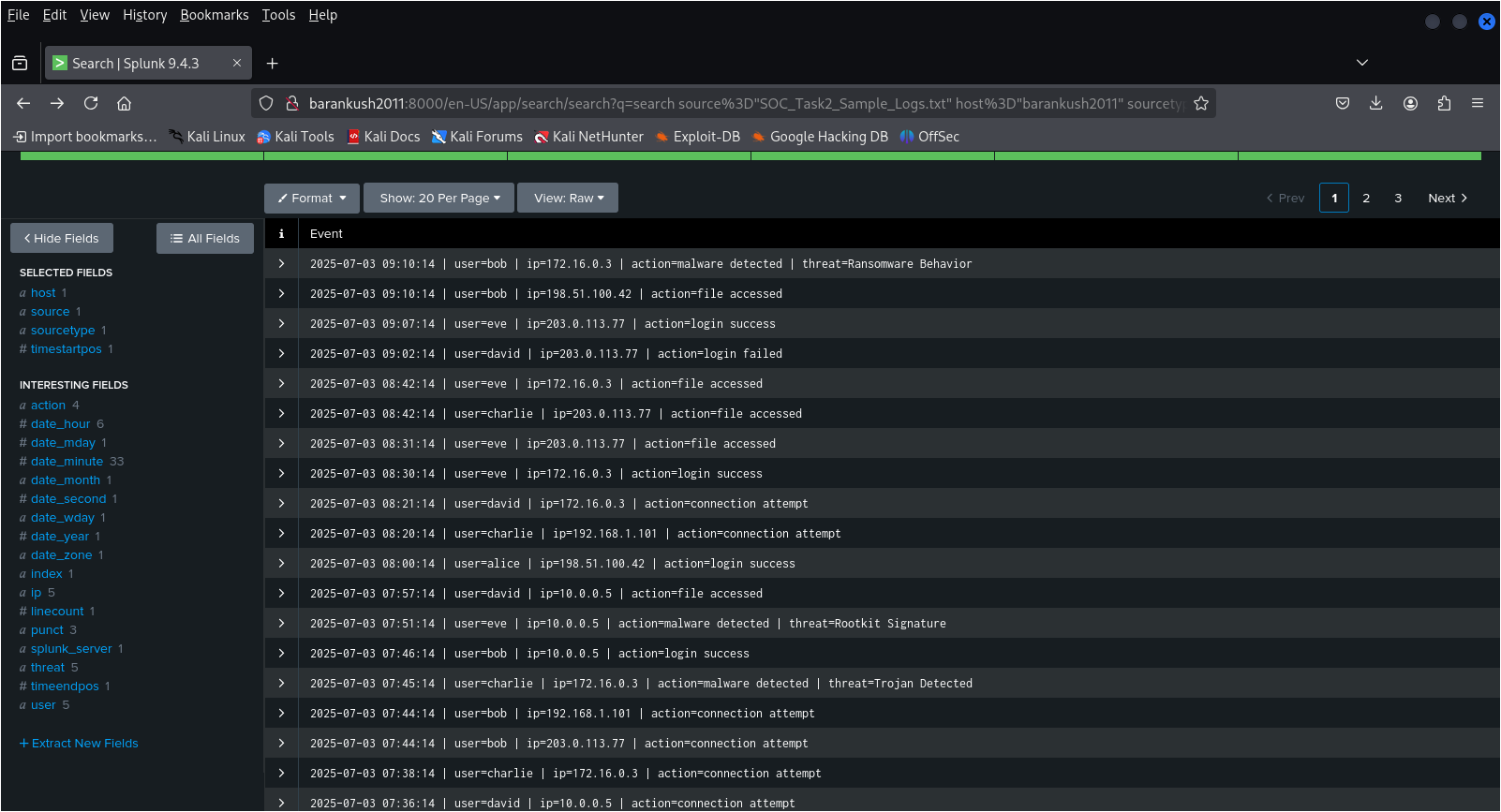
**SECURITY INCIDENT ANALYSIS AND RESPONSE REPORT**

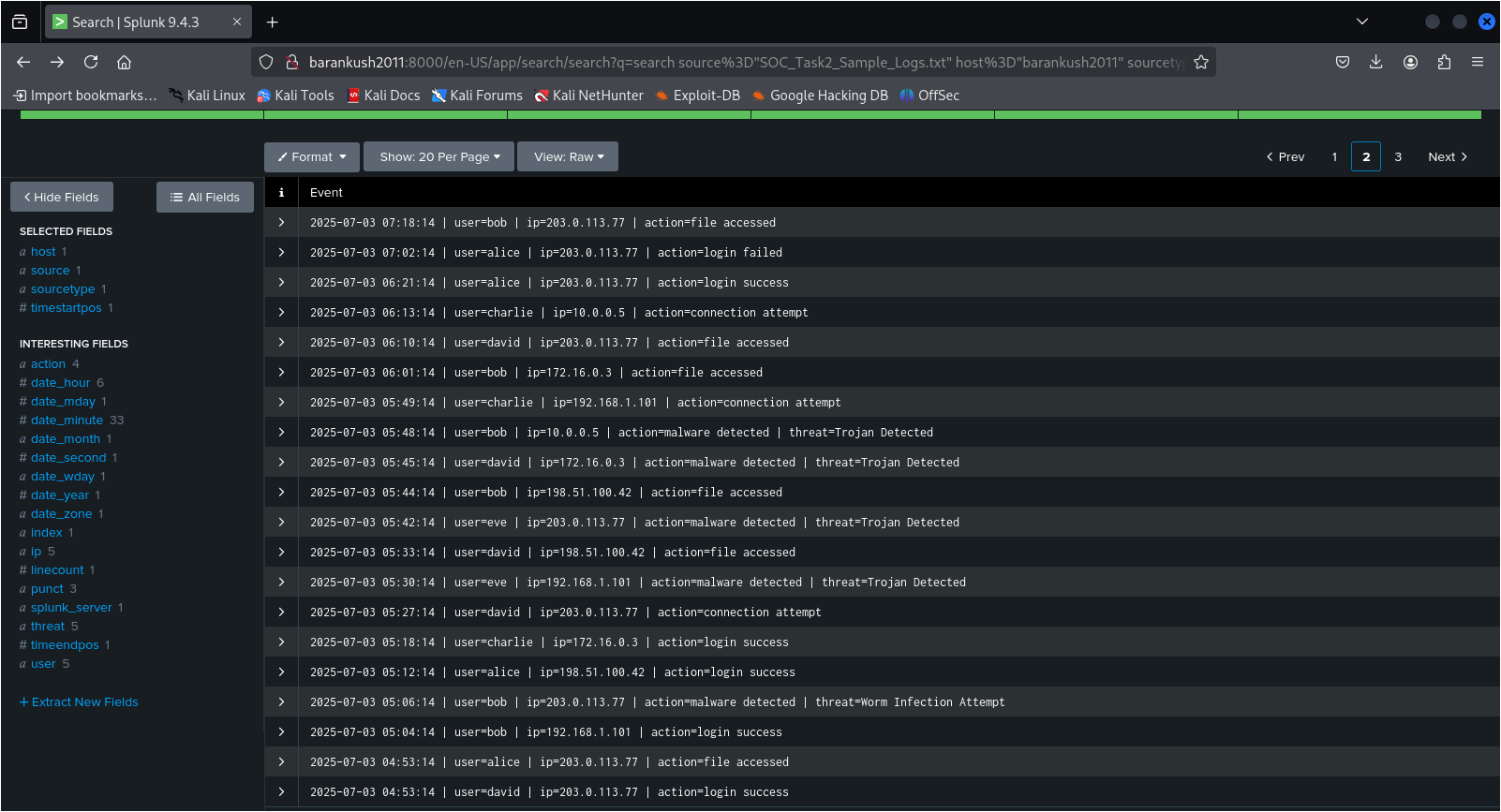
By: Lendani Canvil Kwati

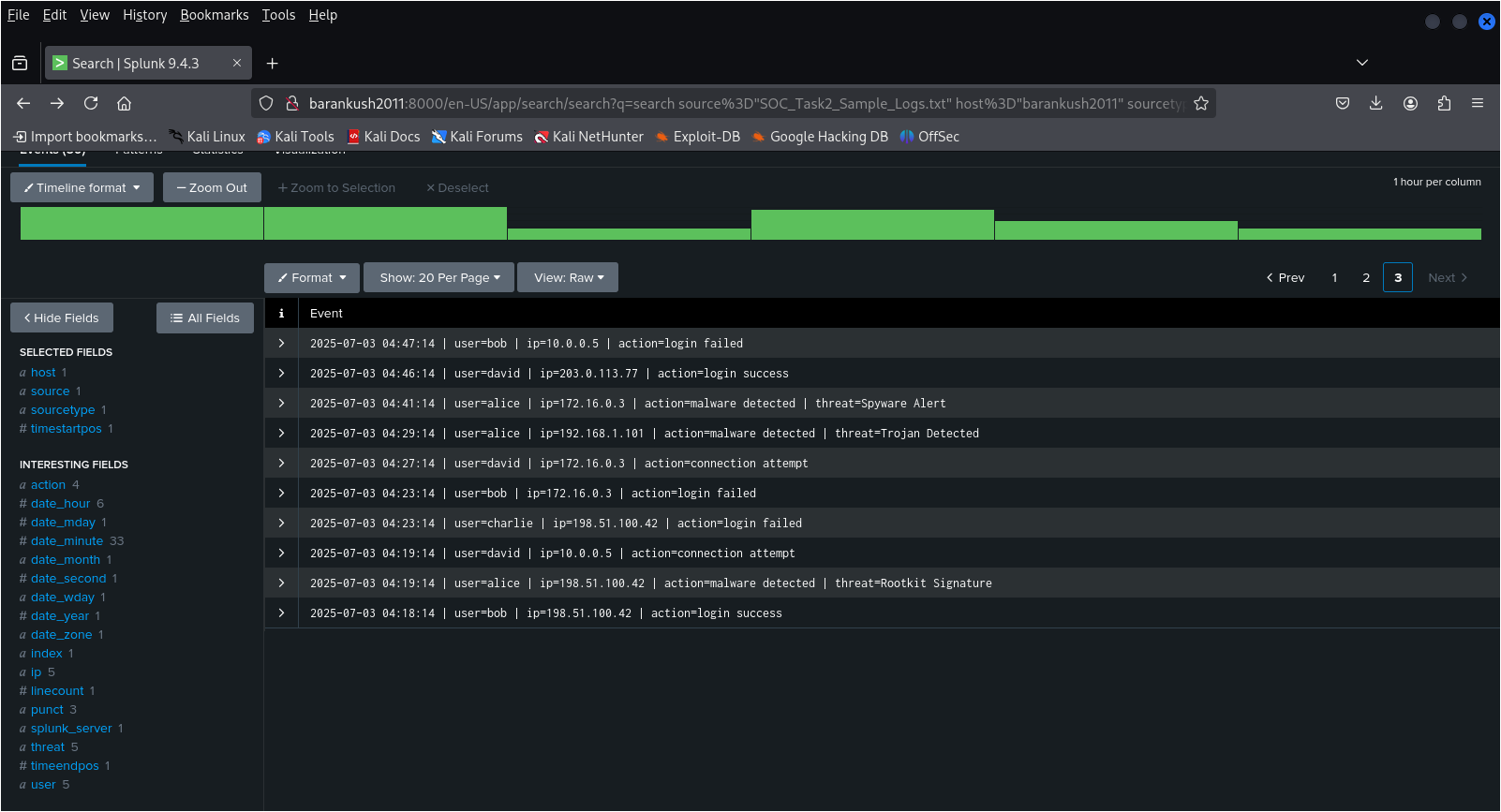
Using: Splunk Enterprise

Date of Activity: July 3, 2025

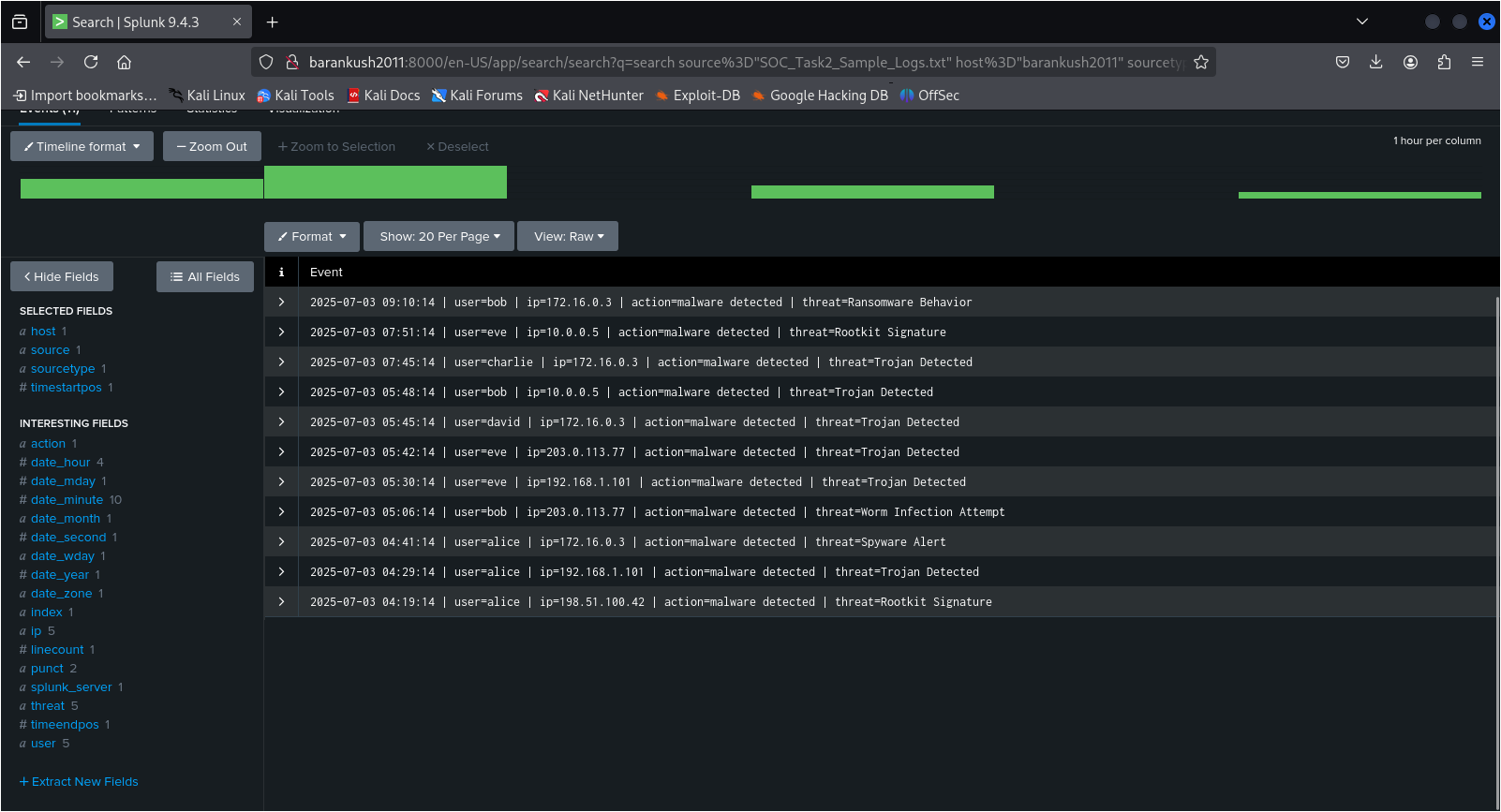
Time Range Analyzed: 04:18 – 09:11 hrs







## Suspicious Alerts Identified



* Malware Detection - Rootkit Signature

Time: 04:19:14

User: alice

IP Address: 198.51.100.42

Threat: Rootkit Signature

Classification: High

* Unauthorized Connection Attempt

Time: 04:19:14

User: david

IP Address: 10.0.0.5

**Classification:** Medium

* Multiple Malware Alerts (Trojan, Spyware, Ransomware, Worms), (Users Impacted: alice, bob, charlie, david, eve), Multiple Timestamps

04:41:14 (Spyware - alice)

05:06:14 (Worm - bob)

05:45:14 (Trojan - david)

07:45:14 (Trojan - charlie)

07:51:14 (Rootkit - eve)

09:10:14 (Ransomware - bob)

**Classification:** High

* Repeated Failed Logins & Connection Attempts (Users Involved: bob, charlie, david)

IPs: Various including 10.0.0.5, 172.16.0.3, 198.51.100.42

**Classification:** Low–Medium

* Suspicious File Access Following Malware Alerts

e.g. 09:10:14 — bob accesses a file from IP 198.51.100.42 right after ransomware detection from IP 172.16.0.3

**Classification:** High

## Incident Classification by Priority

|  |  |  |
| --- | --- | --- |
| **Priority** | **Description** | **Examples (Time/User/IP)** |
| High | Rootkit, Ransomware, and multiple malware detections | 04:19:14 (alice), 09:10:14 (bob), 07:51:14 (eve) |
| Medium | Repeated failed logins, suspicious connection attempts | 04:23:14 (charlie - login fail), 04:19:14 (david - conn attempt) |
| Low | Isolated events with limited context/ not directly linked to other alerts | 07:44:14 (bob - conn attempt), 08:20:14 (charlie - conn attempt) |

## Incident Response Report

Timeline of Events:

|  |  |
| --- | --- |
| **Time** | **Event** |
| 04:19:14 | Rootkit detected on alice’s system (IP: 198.51.100.42); david attempts connection from 10.0.0.5 at the same time. |
| 04:29–04:41 | More malware alerts on alice's account (Trojan, Spyware). |
| 04:47 | bob login fails from same IP as david’s earlier connection. |
| 05:06 | bob’s device shows Worm infection attempt. |
| 05:45–05:51 | charlie and eve also experience Trojan and Rootkit alerts. |
| 09:10 | bob is involved in both ransomware detection and file access from suspicious IPs. |

## Impact

* Multiple users across internal and external IPs were targeted or infected.
* Critical systems likely compromised due to presence of Rootkit, Trojan, and Ransomware behaviors.
* Unauthorized access and file exfiltration possible due to failed and successful login attempts around malware detections.

## Root Causes

* Unpatched systems and lack of endpoint protection.
* Potential lateral movement within network (multiple IPs accessing similar systems).
* Social engineering or credential theft.

## Recommendations & Remediation Steps

* Isolate Affected Systems

Immediately disconnect devices with confirmed malware infections (IPs: 198.51.100.42, 10.0.0.5, 172.16.0.3).

Conduct Full AV/Malware Scan

Especially on systems associated with alice, bob, and eve.

* Reset All User Passwords

Enforce MFA for users, particularly those with repeated failed logins and successful access from suspicious IPs.

* Audit Access Logs & File Transfers

Investigate all file accesses between 04:18–09:11 for potential data exfiltration.

* SIEM Alert Tuning

Improve detection rules to prioritize simultaneous malware alerts and connection attempts.

* Patch & Update

Apply latest security patches and OS updates to all devices.

## Key metrics:

* 7 Critical Alerts (Malware-related)
* 6 Unauthorized Access Attempts
* 3 Rootkit Detections
* 1 Ransomware Activity Detected