🔐 Security Alert Monitoring & Incident Response Simulation Report

Project: Incident Response Simulation Report
Tools Used: Splunk (Free Trial), Sample SOC Logs, SPL Queries
Prepared by: *RAWLINGS ODIERO*
Date: August 2025
Task: 2

FutureInterns

1. Executive Summary

This report summarizes the analysis of simulated system, network, and authentication logs from the organization's SIEM platform. The investigation identified multiple failed login attempts, suggesting brute-force attacks, along with malware infections (Trojan, Rootkit, Spyware, Worm, Ransomware) across several hosts. Signs of potential privilege escalation and lateral movement were also detected. These findings indicate attempted account compromise and widespread malware activity. Immediate containment and remediation are recommended to reduce risk.

---

2. Purpose

The purpose of this exercise is to understand SOC processes by analyzing simulated security logs to identify potential threats, assess their impact, and recommend mitigation measures.

2.1 Scope

The analysis is limited to simulated system, network, and authentication logs. Physical security, cloud platform events, and live production systems are not included.

---

3. Objectives

- Analyze incoming security alerts and logs (simulated data provided).
- Identify suspicious activities such as failed logins, unusual IP addresses, or malware alerts.
- Categorize and prioritize alerts based on severity.
- Draft an incident response report outlining the threat, impact, and suggested next steps.
- Simulate communication with stakeholders about the incident.
- Learn how SOC teams track and manage threats using dashboards and playbooks.

---

4. Tools and Methodology

- **Splunk:** Used for log analysis, correlation, and dashboard visualization.
- **Custom Search Queries:** Developed two core Splunk queries:

1. **User Activity Summary** (failed logins, malware, file access per user)

```
source="soc_task2_sample_logs.txt" host="kali" sourcetype="Soc logs"
| eval login_success=if(action="login success",1,0),
      login_failed=if(action="login failed",1,0),
      connection_attempt=if(action="connection attempt",1,0),
      file_accessed=if(action="file accessed",1,0),
      malware_detected=if(action="malware detected",1,0)
| stats sum(login_success) AS "Login Success",
       sum(login_failed) AS "Login Failed",
       sum(connection_attempt) AS "Connection Attempts",
       sum(file_accessed) AS "Files Accessed",
       sum(malware_detected) AS "Malware Detected"
  BY user
| sort - "Malware Detected" "Login Failed"
```

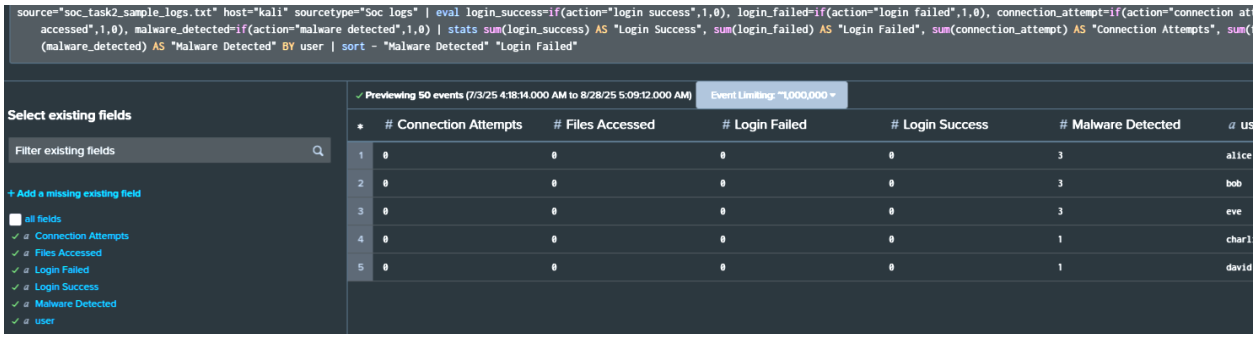
2. **User + IP Activity Summary** (to trace suspicious actions by source IP):

```
source="soc_task2_sample_logs.txt" host="kali" sourcetype="Soc logs"
| eval login_success=if(action="login success",1,0),
      login_failed=if(action="login failed",1,0),
      connection_attempt=if(action="connection attempt",1,0),
      file_accessed=if(action="file accessed",1,0),
      malware_detected=if(action="malware detected",1,0)
| stats sum(login_success) AS "Login Success",
       sum(login_failed) AS "Login Failed",
       sum(connection_attempt) AS "Connection Attempts",
       sum(file_accessed) AS "Files Accessed",
       sum(malware_detected) AS "Malware Detected"
  BY user ip
| sort user - "Malware Detected" - "Login Failed"
```

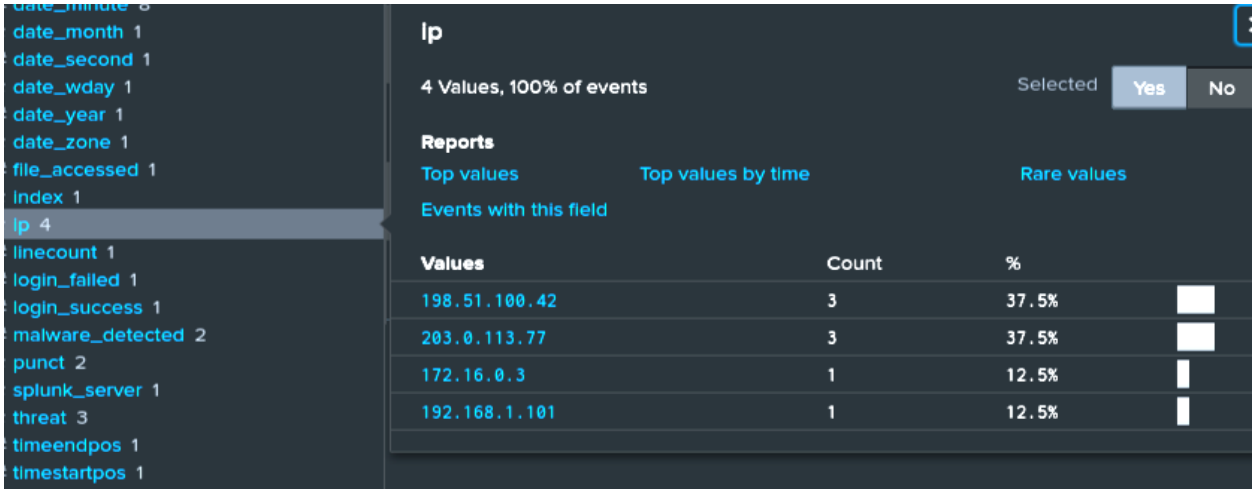
- **Incident Analysis:** Logs were reviewed to detect correlations between login failures, successful access, malware detections, and suspicious IPs.
- **Reporting:** Incidents were categorized by severity and outlined with recommended response actions.

🚨 Incident 1: Multiple Failed Logins

- **Date/Time:** 2025-07-03
- **Source IPs:** 203.0.113.77, 10.0.0.5, 172.16.0.3, 198.51.100.42
- **Users Affected:** Alice, David, Bob, Charlie
- **Severity:** Medium
- **Impact:** Possible brute-force/credential stuffing



ip	Login Failed	Login Success	Malware Detected	user
172.16.0.3	0	0	1	alice
192.168.1.101	0	0	1	alice
198.51.100.42	0	0	1	alice
203.0.113.77	0	0	0	alice
10.0.0.5	0	0	1	bob
172.16.0.3	0	0	1	bob
203.0.113.77	0	0	1	bob
192.168.1.101	0	0	0	bob
198.51.100.42	0	0	0	bob
172.16.0.3	0	0	1	charlie
10.0.0.5	0	0	0	charlie
192.168.1.101	0	0	0	charlie
198.51.100.42	0	0	0	charlie
203.0.113.77	0	0	0	charlie
172.16.0.3	0	0	1	david
10.0.0.5	0	0	0	david
198.51.100.42	0	0	0	david
203.0.113.77	0	0	0	david



Recommended Actions:

- Block suspicious IPs
- Monitor authentication attempts
- Enforce MFA

🚨 Incident 2: Malware Spread Detected

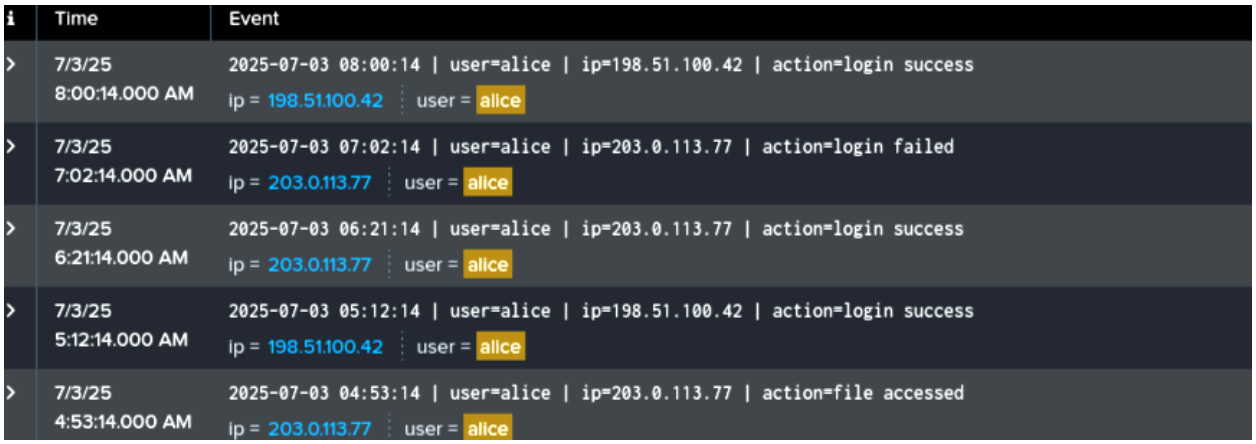
- **Date/Time:** 2025-07-03
- **Affected Hosts:** 10.0.0.5, 172.16.0.3, 198.51.100.42, 192.168.1.101, 203.0.113.77
- **Threats:** Trojan, Rootkit, Spyware, Worm, Ransomware
- **Severity:** High
- **Users Affected:** Alice, David, Charlie
- **Impact:** Multiple malware infections detected across systems

Recommended Actions:

- Isolate infected machines
- Run AV scans and remove threats
- Patch systems and check persistence

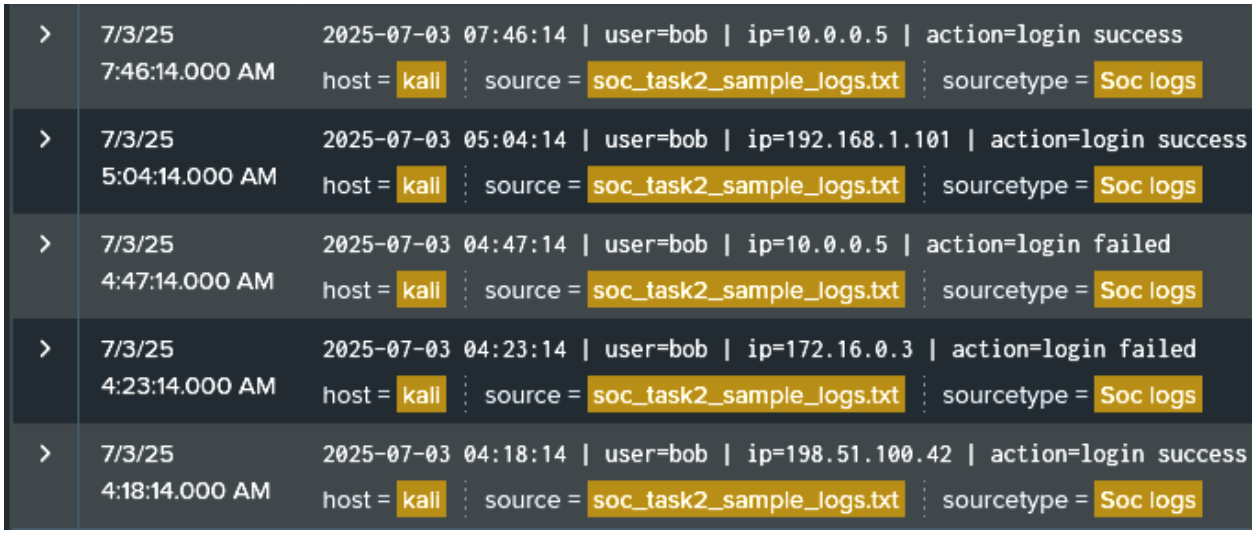
🚨 Incident 3: Potential Privilege Escalation

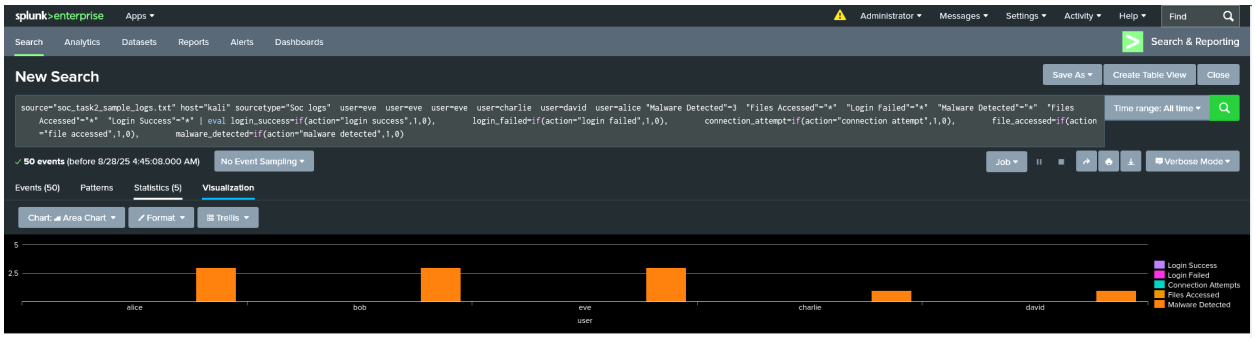
- **Date/Time:** 2025-07-03
- **Users Involved:** Alice, Bob
- **Source IP:** 203.0.113.77
- **Suspicious Activity:** Failed logins → successful login → sensitive file access → malware activity
- **Severity:** High
- **Impact:** Possible lateral movement / compromised accounts



Time	Event
7/3/25 8:00:14.000 AM	2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success ip = 198.51.100.42 user = alice
7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed ip = 203.0.113.77 user = alice
7/3/25 6:21:14.000 AM	2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success ip = 203.0.113.77 user = alice
7/3/25 5:12:14.000 AM	2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success ip = 198.51.100.42 user = alice
7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed ip = 203.0.113.77 user = alice

7/3/25 5:33:14.000 AM	2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed ip = 198.51.100.42 user = david
7/3/25 5:27:14.000 AM	2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt ip = 203.0.113.77 user = david
7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success ip = 203.0.113.77 user = david
7/3/25 4:46:14.000 AM	2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success





Recommended Actions:

- Reset credentials of affected users
- Review sudo/admin privileges
- Investigate files accessed

Incident Response Summary:

During monitoring of the simulated environment, three key categories of security incidents were detected and analyzed:

1. **Multiple Failed Login Attempts**
    - Several failed login events were recorded from IP **`203.0.113.77`** targeting users *Alice* and *David*, as well as from other IPs targeting *Bob* and *Charlie*.
    - This activity is consistent with brute-force or credential-stuffing attempts.
    - **Action Taken:** Correlated login events in Splunk, flagged IPs with repeated failures, recommended blocking offending IPs and enforcing multi-factor authentication.

2. **Malware Signatures Detected**
    - Multiple malware alerts were logged across different hosts (**`10.0.0.5`**, **`172.16.0.3`**, **`198.51.100.42`**, **`192.168.1.101`**, **and** **`203.0.113.77`**).
    - Threats included Trojan, Rootkit, Spyware, Worm, and Ransomware.
    - **Action Taken:** Infected hosts were identified and prioritized for isolation. Recommendations included system patching, malware scanning, and threat signature updates.

3. **Potential Privilege Escalation Attempts**
    - Suspicious behavior was observed where users (notably *Alice* and *Bob*) showed a sequence of failed logins followed by successful access and subsequent file activity, in some cases coinciding with malware detections.
    - This suggests possible lateral movement or escalation of privileges by compromised accounts.
    - **Action Taken:** User accounts flagged for review, credential resets recommended, and monitoring of file access logs advised.

Conclusion:

The analysis of the simulated SOC logs highlighted how common threats can be detected using SIEM tools like Splunk. Key findings demonstrated brute-force login attempts, widespread malware infections, and suspicious privilege escalation activity.

The incident response workflow provided practical exposure to:

- **Detection:** Using SPL queries to identify failed logins, malware detections, and abnormal user behavior.
- **Analysis:** Correlating events across multiple IPs, users, and actions to assess severity.
- **Response:** Drafting recommended remediation steps such as isolating infected hosts, enforcing stronger authentication, resetting credentials, and applying patches.
- **Communication:** Summarizing findings in a structured report suitable for SOC stakeholder briefings.

This exercise underscores the importance of continuous monitoring, proactive detection, and timely incident response in safeguarding organizational systems.
