



# **SOC Incident Investigation Report**

**Intern :**

**ABAKTA Haana Camille**

**Organization :**

**Future Interns**

**Assignment :**

**Task 2 - Security Alert Monitoring & Incident Response Simulation**

**Date :**

**January 09, 2026**

## SUMMARY

<b>1. Executive Summary .....</b>	<b>3</b>
<b>2. Environment &amp; Methodology .....</b>	<b>3</b>
<b>3. Identified Threats &amp; Incident Analysis.....</b>	<b>3</b>
<b>3.1. Critical Incident: Ransomware Activity .....</b>	<b>3</b>
<b>3.2. High-Severity Incident: Rootkit Detection (Persistence) .....</b>	<b>4</b>
<b>3.3. External Threat: Worm &amp; Trojan Campaign .....</b>	<b>4</b>
<b>4. Visual Evidence (Screenshots) .....</b>	<b>4</b>
<b>5. Remediation &amp; Recommendations.....</b>	<b>5</b>
<b>6. Conclusion.....</b>	<b>6</b>

## 1. Executive Summary

This report details the security analysis of system logs dated July 3, 2025. The investigation was performed using Splunk to identify anomalies, unauthorized access, and malware activities. Multiple high-severity threats were detected, including Ransomware behavior, Rootkit signatures, and Worm infection attempts, indicating a major security breach affecting several users and workstations.

## 2. Environment & Methodology

- **Platform:** Kali Linux
- **SIEM:** Splunk Enterprise 10.0.2
- **Log Source:** SOC\_Task2\_Sample\_Logs.txt
- **Methodology:**
  1. Data ingestion and field extraction.
  2. Statistical analysis of event actions (Success vs. Failure).
  3. Threat hunting using SPL (Splunk Processing Language) to isolate "malware detected" actions.

## 3. Identified Threats & Incident Analysis

### 3.1. Critical Incident: Ransomware Activity

- **Timestamp:** 2025-07-03 09:10:14
- **User:** bob
- **Source IP:** 172.16.0.3
- **Threat Type:** Ransomware Behavior
- **Analysis:** This is the most critical alert. The system detected behavior consistent with ransomware encryption on Bob's machine. Immediate isolation is required to prevent data loss.

### 3.2. High-Severity Incident: Rootkit Detection (Persistence)

- **Users involved:** alice (04:19:14) and eve (07:51:14)
- **IPs:** 198.51.100.42 and 10.0.0.5
- **Analysis:** Rootkits allow attackers to maintain hidden, persistent access to the operating system. The presence of rootkits on two different machines suggests a potential lateral movement within the network.

### 3.3. External Threat: Worm & Trojan Campaign

- **Attacking IP:** 203.0.113.77
- **Analysis:** This IP address is associated with multiple "Worm Infection" and "Trojan" alerts. It appears to be a primary source of infection attempting to spread malware to Bob and Eve.

## 4. Visual Evidence (Screenshots)

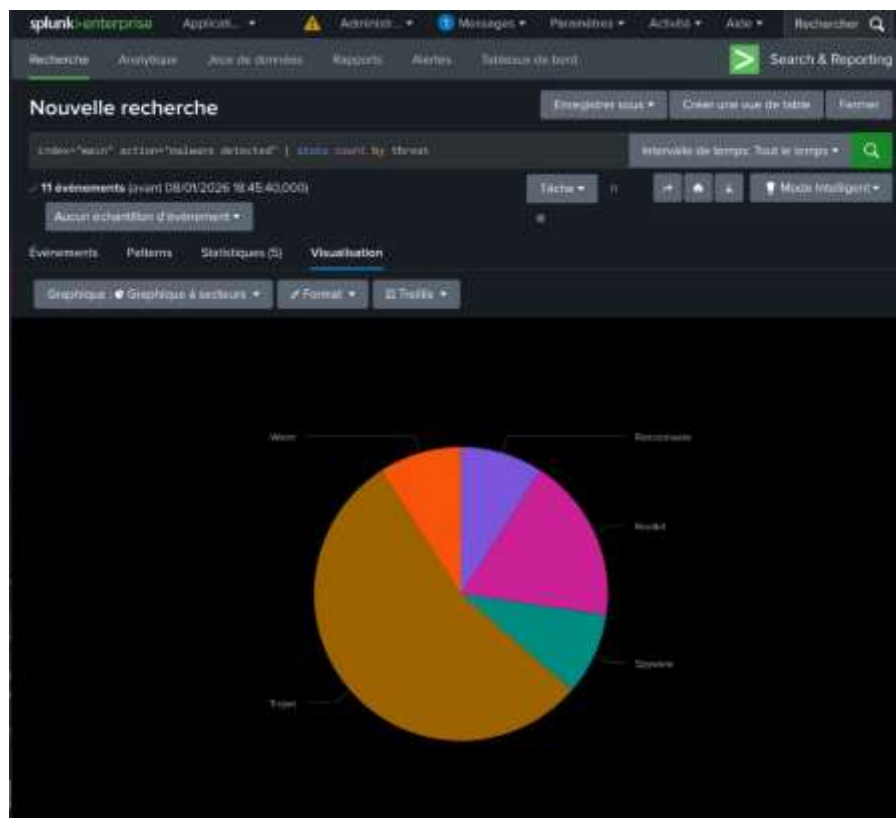


Figure 1: Threat Distribution Overview

**Description:** A Pie Chart showing the breakdown of detected malwares (Trojans, Ransomware, Rootkits).

**Nouvelle recherche**

index="main" action="malware detected" | table \_time, user, ip, threat | sort - \_time

11 événements (avant 08/01/2026 16:47:31.000)

Aucun échantillon d'événement

Événements Patterns **Statistiques (11)** Visualisation

Afficher: 20 per page Format Aperçu: activé

_time	user	ip	threat
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware
2025-07-03 09:01:14	eve	10.0.0.5	Rookit
2025-07-03 09:05:14	charlie	172.16.0.3	Trojan
2025-07-03 09:08:14	bob	10.0.0.5	Trojan
2025-07-03 09:05:14	David	172.16.0.3	Trojan
2025-07-03 09:42:14	eve	203.0.113.77	Trojan
2025-07-03 09:39:14	eve	192.168.1.101	Trojan
2025-07-03 09:08:14	bob	203.0.113.77	Worm
2025-07-03 04:41:14	alice	172.16.0.3	Spyware
2025-07-03 04:29:14	alice	192.168.1.101	Trojan
2025-07-03 04:19:14	alice	198.51.100.42	Rookit

Figure 2: Security Events Table

**Description:** A detailed view of the Splunk investigation table showing timestamps, users, IPs, and specific threats.

## 5. Remediation & Recommendations

Based on the findings, the following actions are highly recommended:

1. **Immediate Isolation:** Disconnect workstation 172.16.0.3 (Bob) and 198.51.100.42 (Alice) from the network to prevent further malware spread or data encryption.
2. **IP Blocking:** Blacklist the malicious external IP 203.0.113.77 on the corporate firewall and proxy.
3. **Password Reset Policy:** Force a global password reset for all affected accounts (Bob, Alice, Eve, David) as their credentials may have been compromised.

4. **Forensic Analysis:** Conduct a deep forensic scan on infected hosts to identify the "Patient Zero" and remove persistent Rootkits.
5. **EDR Deployment:** Ensure Endpoint Detection and Response (EDR) tools are active and updated to block known Ransomware signatures.

## **6. Conclusion**

The analysis confirms a sophisticated multi-stage attack involving various malware families. The timely detection through Splunk allowed us to identify the critical ransomware threat before total system failure. Swift execution of the remediation steps is mandatory to restore environment integrity.