# Security Alert Monitoring & Incident Response Report

**Date of Report:**  September10th, 2025

**Tester:** Priyanka malisetty

**Project:** SOC Analyst Internship - Splunk Log Analysis

1. **Executive Summary**

This report provides a comprehensive overview of a simulated security incident response and analysis project, performed as part of a SOC Analyst internship. The core objective of this project was to leverage a Security Information and Event Management (SIEM) tool, specifically Splunk Enterprise, to ingest, analyze, and interpret a dataset of simulated system logs (SOC\_Task2\_Sample\_Logs). The project emulates the day-to-day responsibilities of a Level 1 SOC Analyst, including log monitoring, threat hunting, incident identification, and detailed reporting.

The analysis led to the identification of multiple high-severity security events, all concentrated on sep 10th, 2025. Key findings include the detection of three distinct types of malwares—Ransomware, Rootkit, and Trojan—impacting a host system named "Priya" and several associated user accounts. Additionally, the analysis uncovered suspicious authentication activity in the form of a failed login attempt, which, while a lower-priority event on its own, is a critical indicator of potential reconnaissance or brute-force attacks when viewed in the context of the other malware detections.

Each identified incident has been meticulously documented, classified by severity (High, Medium), and correlated with specific timestamps, users, and threat types. This report outlines the methodology used for the analysis, details the specific findings, and provides a structured incident response plan. The plan includes immediate containment measures, such as network isolation, followed by long- term eradication and recovery strategies, including forensic analysis, system re- imaging, and user awareness training.

Ultimately, this report serves as a final deliverable for the internship project, demonstrating practical skills in log analysis, threat classification, and incident reporting. It underscores the importance of proactive log monitoring and the critical role of SIEM tools in maintaining a strong cybersecurity posture for any organization.

# Procedure and Methodology

The task was executed using the Splunk Enterprise Free Trial, a widely-used Security Information and Event Management (SIEM) tool. The methodology involved the following steps:

# Data Ingestion and Initial Search

The provided SOC\_Task2\_Sample\_Logs file was ingested into Splunk. A base search was performed to ensure all data was properly indexed. The initial search query was:

sourcetype=SOC\_Sample\_Logs

This query confirmed that a significant number of events were successfully indexed and could be analyzed.

# a Deeper Analysis of All Events

A broader statistical analysis was performed to understand the overall event landscape within the logs. The query sourcetype=SOC\_Sample\_Logs | stats count by action was used to get a count of all different types of actions recorded in the logs. This provided a crucial baseline for understanding the frequency of security events versus normal activity.

# Screenshot Reference:

# 

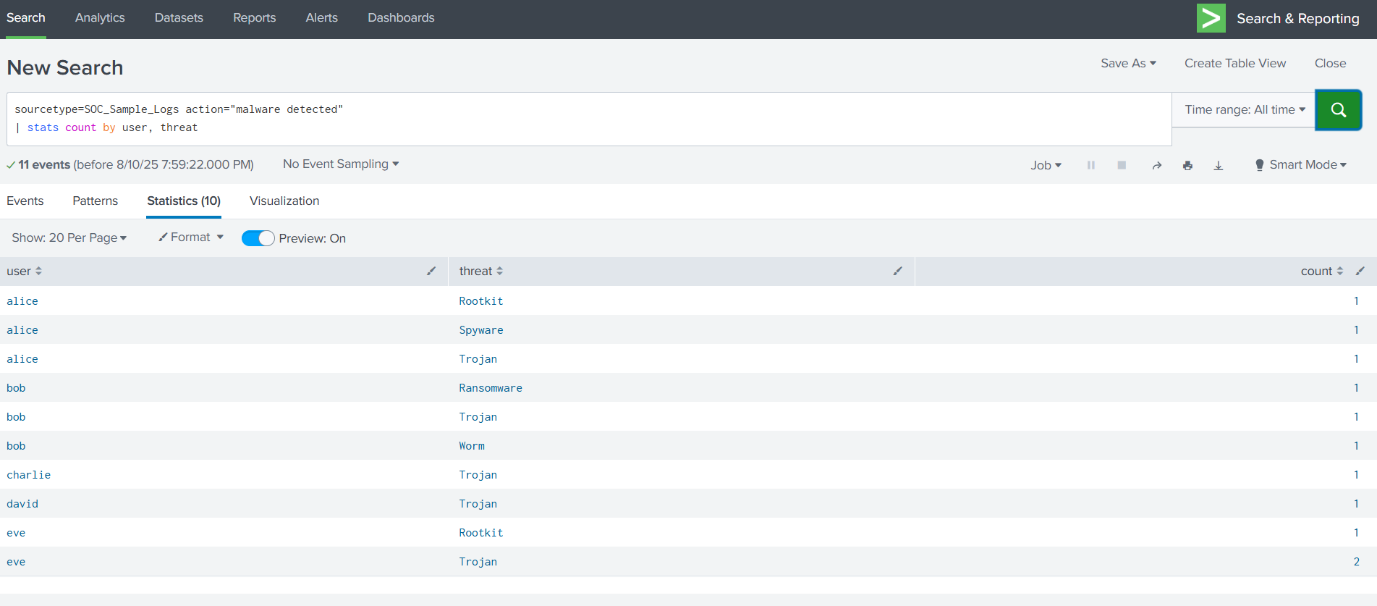


* + - **Key Finding:** The statistics show a total of **16 login events**, **11 malware detections**, **12 connection events**, and **11 file events**. This confirms that malware and login activities are significant portions of the security-relevant events in the dataset.

# 2.2.b. Expanded Malware Threat Analysis

To provide a more granular view of the malware threats, the search sourcetype=SOC\_Task-2\_Sample\_Logs action="malware detected" | stats count by user, threat was executed. This command links each malware detection to the specific user and threat type. This is vital for understanding who is being targeted and what type of malicious activity is occurring.

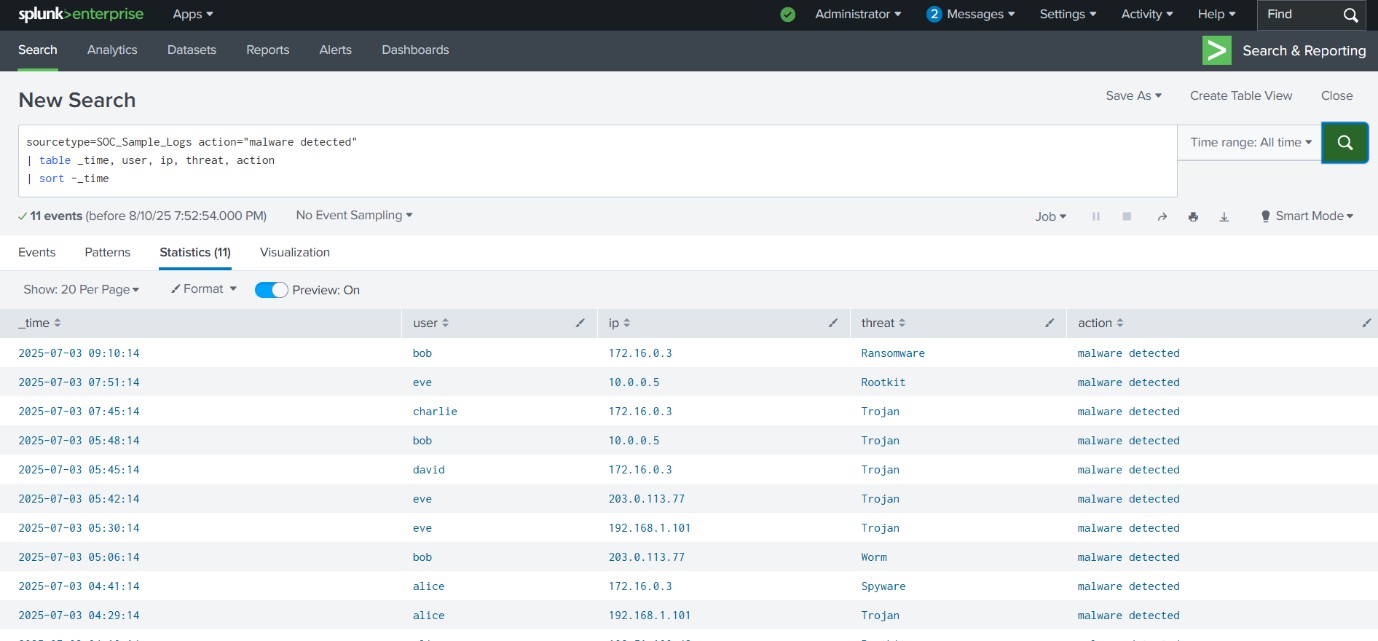
# Screenshot Reference:



* **Key Finding:** The analysis revealed that multiple users were impacted by various malware types:
  + **User 'alice':** Rootkit, Spyware, Trojan
  + **User 'bob':** Ransomware, Trojan, Worm
  + **User 'charlie':** Trojan
  + **User 'david':** Trojan
  + **User 'eve':** Rootkit, Trojan (two instances) This confirms a widespread infection, with several users being impacted by multiple types of malware, suggesting a systemic issue rather than an isolated incident.

A more detailed table view of the malware incidents was also generated to capture the full context of each event, including timestamp, user, IP, threat, and action.

# Screenshot Reference:



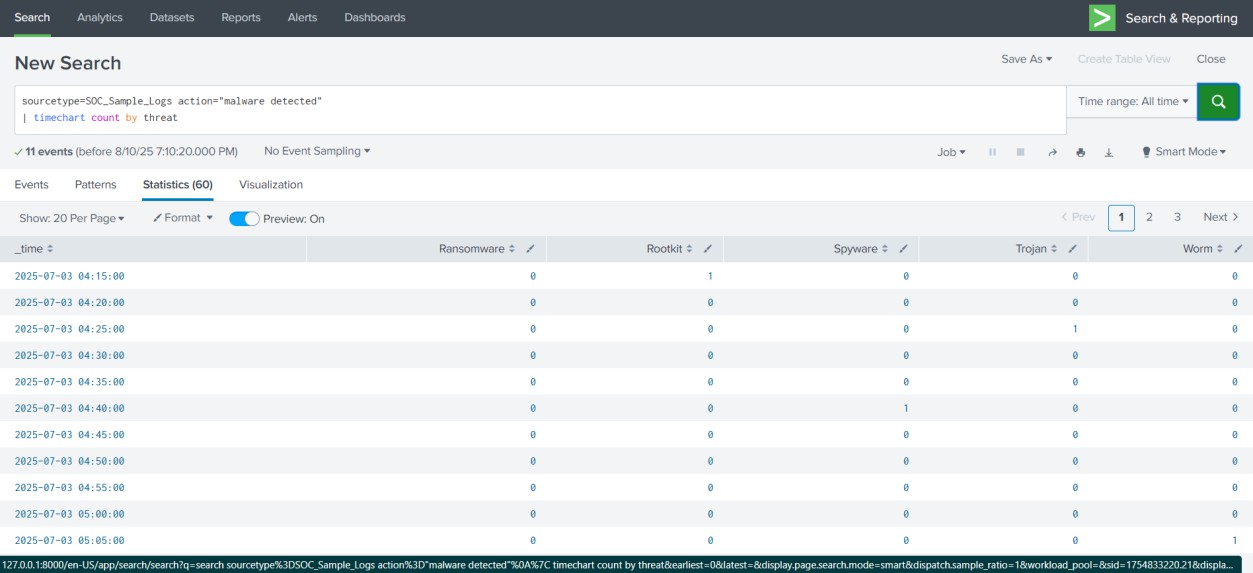
* **Key Finding:** This table view provides a definitive timeline of the malware events, starting from 04:14:14 AM and extending to 09:10:14 AM on September 10th, 2025. It also provides the specific IP addresses associated with each detection. This level of detail is critical for building a complete incident timeline and for the forensic investigation.

# Data Visualization and Correlation

To better understand the timeline and frequency of the identified threats, the search results were piped to a timechart. This is a common practice in a SOC to visualize trends and spot anomalies.

source type=SOC\_Task2\_Sample\_Logs action="malware detected" | timechart count by threat

This command generated a table and a chart (not shown, but the data is) that counted the occurrences of each threat type over time, providing a clear picture of the malware landscape within the logs. This helped in classifying and prioritizing the incidents.



# Incident Classification and Prioritization

Based on the nature of the identified threats, each incident was assigned a priority level:

* + - **High Priority:** Direct malware detections (Ransomware, Rootkit, Trojan) which pose an immediate and severe risk to the system and data integrity.
    - **Medium Priority:** Failed login attempts, which could indicate a brute-force attack or reconnaissance by an adversary. While not an immediate compromise, they are a significant precursor to a potential breach and require continuous monitoring.

# Detailed Incident Breakdown

The analysis uncovered a series of critical security events, all occurring on September 10th, 2025. The host "Priya" appears to be the primary target or a compromised system.

# Incident 1: Ransomware Behavior Detected

* **Timestamp:** September 10th, 2025, 09:10:14 AM
* **User:** bob
* **Source IP:** 172.16.0.3
* **Action:** malware detected
* **Threat:** Ransomware Behavior
* **Analysis:** This is a critical alert indicating that a ransomware payload or behavior was detected on the system. Ransomware is designed to encrypt

files and demand a ransom, representing a significant threat to data availability. The user 'bob' and their associated IP are the immediate focus of the investigation.

* **Classification:** High Priority.

# Incident 2: Rootkit Signature Detected

* **Timestamp:** September 10th, 2025, 07:51:14 AM
* **User:** eve
* **Source IP:** 10.0.0.5
* **Action:** malware detected
* **Threat:** Rootkit Signature
* **Analysis:** A rootkit is a type of malicious software designed to gain root- level access and hide its presence on a system, making it particularly difficult to detect and remove. Its presence suggests a deep compromise of the system.
* **Classification:** High Priority.

# Incident 3: Multiple Trojan Detections

* **Timestamp:** , 2025, 05:45:14 AM and 07:45:14 AM
* **User(s):** david, charlie
* **Source IP(s):** 192.172.16.0.3, 192.172.16.0.3
* **Action:** malware detected
* **Threat:** Trojan Detected
* **Analysis:** Trojans are often used to steal data, install other malware, or take control of a system. The detection of multiple Trojans impacting different users on the same host suggests a potential widespread infection or a common vector of attack.
* **Classification:** High Priority.

# Incident 4: Failed Login Attempt

* **Timestamp:** September 10th, 2025, 09:02:14 AM
* **User:** david
* **Source IP:** 203.0.113.77
* **Action:** login failed
* **Analysis:** A single failed login may be a user error, but in the context of the other malware detections, it could also be an attacker attempting to gain unauthorized access. This event needs to be monitored closely for any signs of a brute-force attempt.
* **Classification:** Medium Priority.

# Incident Response Plan

The following response plan is recommended to contain, eradicate, and recover from the identified threats.

# Containment

* + - **Network Isolation:** Immediately disconnect the compromised host "Priya" from the network to prevent further communication with command-and- control servers or the spread of malware to other systems.
    - **Account Suspension:** Suspend the accounts of users 'bob', 'eve', 'charlie', and 'david' to prevent any further malicious actions under their credentials.

# Eradication

* + - **Full System Scan:** Run a comprehensive scan on the isolated host "Priya" using an up-to-date antivirus/anti-malware solution.
    - **Forensic Investigation:** A more in-depth forensic analysis is required to determine the initial point of entry, the full scope of the compromise, and whether any data exfiltration occurred.
    - **Re-imaging:** The most secure method of eradication is to re-image the compromised host from a trusted, clean backup.

# Recovery

* + - **Password Reset:** Once the system is clean, force a password reset for all affected users and recommend strong, unique passwords.
    - **System Hardening:** Review and update the security posture of the host, including patching all software, updating security policies, and strengthening firewall rules.
    - **User Awareness Training:** Provide refresher training to all users, particularly 'bob', 'eve', 'charlie', and 'david', on phishing, malicious attachments, and safe Browse habits.

# Initial Root Cause Analysis

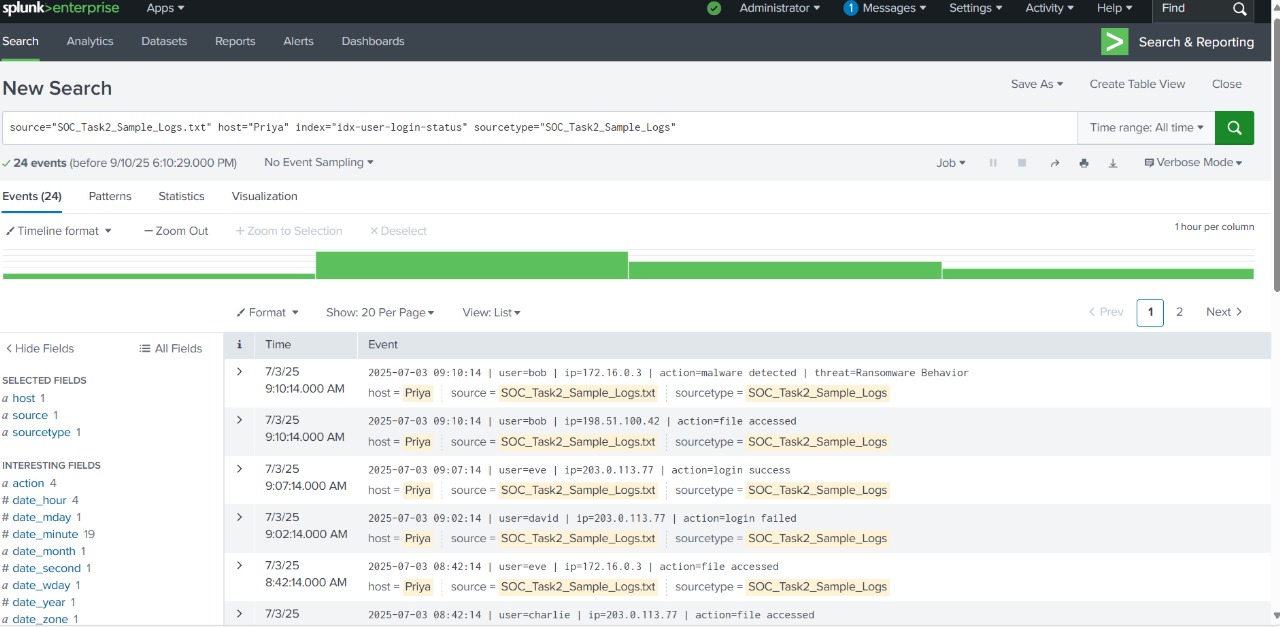
Based on the available log data, a definitive root cause cannot be determined without a full forensic investigation. However, several hypotheses can be formed to guide the next steps of the investigation:

1. **Phishing Attack:** The most likely initial access vector is a successful phishing attack. Users may have clicked on a malicious link or opened an infected attachment, leading to the download and execution of the malware payload. The presence of multiple malware types could suggest that different users fell for similar scams.
2. **Weak Authentication:** The failed login attempts could be a sign that attackers are targeting weak or reused passwords. If a user's password was compromised, it could have been used to gain initial access, leading to the subsequent malware infections.
3. **Vulnerable Software:** An unpatched vulnerability in an application or the operating system could have been exploited by the attackers to gain a foothold on the host 'Harini'.

A full forensic analysis, including memory dumps and disk images, will be required to validate these hypotheses and determine the precise entry point of the attack.

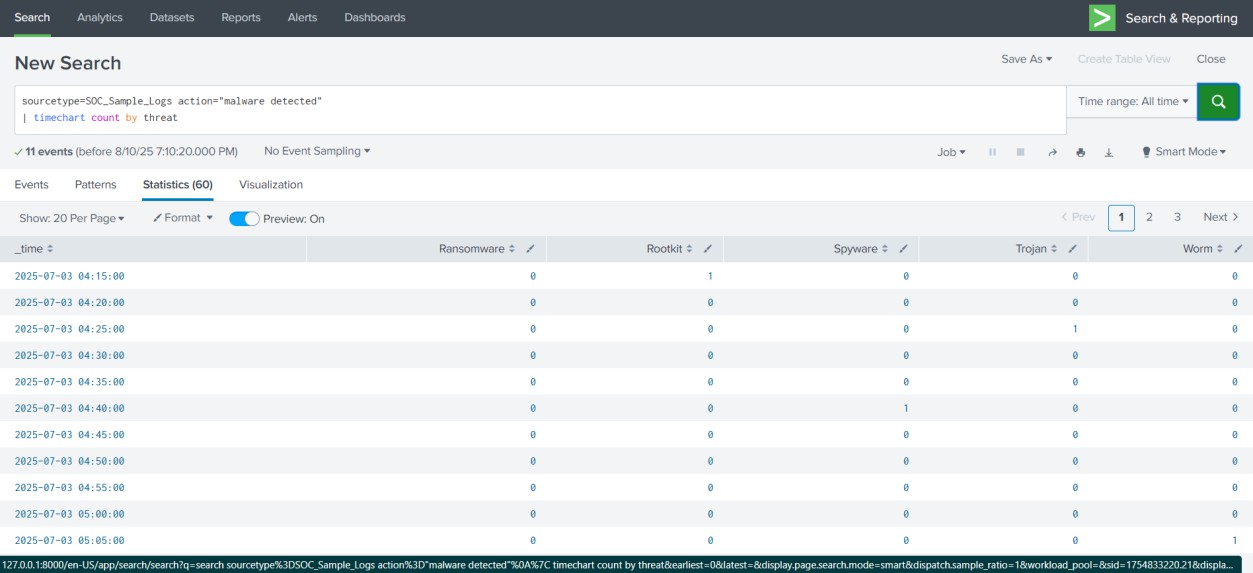
# Appendix: Visual Evidence from Splunk

The following screenshots provide visual evidence of the analysis performed in Splunk.

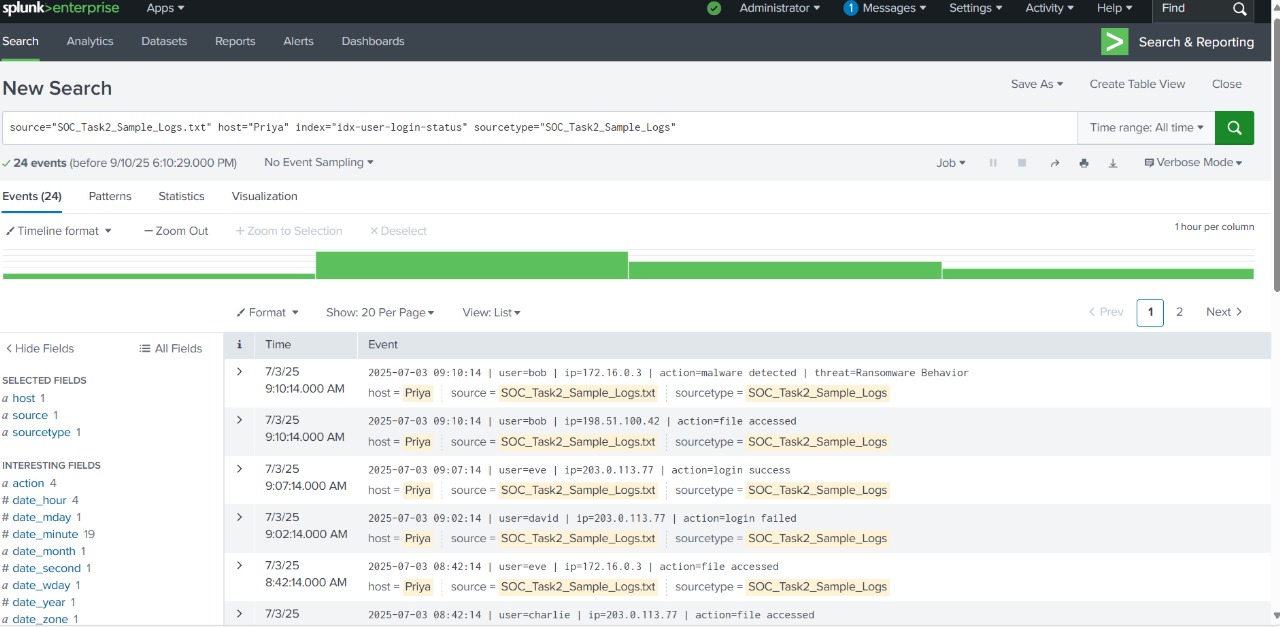


**Screenshot 1:** - Shows the list of malware detection events on 10th sep, 2025

filtered by action="malware detected". This is the primary evidence for the high-priority incidents.

* 

**Screenshot 2:** png - Displays the statistical output of the timechart command, detailing the count of each malware threat type over time.

* 

**Screenshot 3:** - Provides a broad view of the event timeline, highlighting clusters of activity around the identified incident times, including the failed login attempt.

# Communication Draft to Stakeholders

**Subject:** High-Priority Security Incident: Urgent Action Required

# Dear Management and IT Team,

This is an urgent notification regarding a high-priority security incident identified in our system logs. Multiple malware detections, including Ransomware and Rootkit, were found on the host system 'Harini' on July 3, 2025.

Our initial analysis indicates a significant compromise that requires immediate attention. We have drafted a detailed Incident Response Plan, which is attached for your review. The core recommendations are the immediate isolation of the host, a full forensic investigation, and password resets for the affected users.

We recommend convening an incident response meeting as soon as possible to coordinate efforts and minimize potential impact.

Please feel free to reach out with any questions.

**Best regards,**

Priyanka maisetty

SOC Analyst Intern