

Incident Response Report

Internship Report Submission – Future Interns

Prepared by: M Fathima Jemina

Date: August 2025

Table of Contents

| S.NO | TITLE | PAGE NO |
|------|------------------------------|---------|
| 1. | Executive Summary | 1 |
| 2. | Objective | 1 |
| 3. | Scope | 2 |
| 4. | Target Details | 2 |
| 5. | Tools Used | 2 |
| 6. | SIEM Setup | 3 |
| 6.1 | Download and Install | 3 |
| 6.2 | Access Splunk Web Interface | 4 |
| 6.3 | Import Data | 4 |
| 6.4 | Create Field Extractions | 7 |
| 7. | Incident Overview and Alerts | 8 |
| 7.1 | After Hour Login | 8 |
| 7.2 | Connection Attempt | 12 |
| 7.3 | Ransomware Alert | 15 |
| 7.4 | Rootkit Alert | 17 |
| 7.5 | Spyware Alerts | 19 |
| 7.6 | Trojan Alert | 21 |
| 7.7 | Worm Infection Alert | 23 |
| 8. | Detection Logic | 25 |
| 8.1 | After Hour Login | 25 |
| 8.2 | Internal Connection Attempt | 26 |
| 8.3 | External Connection Attempt | 26 |
| 8.4 | Ransomware Detection | 27 |
| 8.5 | Rootkit Detection | 27 |
| 8.6 | Spyware Detection | 27 |
| 8.7 | Trojan Detection | 28 |
| 8.8 | Worm Infection Detection | 28 |

| | |
|---|----|
| 9. Incident Classification and Severity | 29 |
| 10. Timeline of Events | 30 |
| 11. Impact Assessment | 33 |
| 12. Remediation & Containment Actions | 34 |
| 13. Result and Conclusion | 36 |

1. Executive Summary

This incident response report presents the results of a simulated Security Operations Center (SOC) exercise designed to assess the organization's ability to detect, analyze, and respond to cyber threats in real time. The engagement involved monitoring simulated security events using Splunk Enterprise, focusing on authentication activity, network connection attempts, and malware detections. The analysis adhered to industry best practices for SOC operations, leveraging structured alert triage, severity classification, and incident documentation.

Using a combination of custom SPL queries and dashboard visualizations, multiple high-severity threats were identified, including ransomware, trojan, rootkit, spyware, and worm infections. Additional findings included after-hours logins from suspicious IP addresses and anomalous connection attempts from both internal and external sources. If these events had occurred in a production environment, they could have resulted in data compromise, unauthorized system access, and operational disruption.

The findings underscore the importance of proactive monitoring, timely detection, and structured incident response procedures. This report provides actionable recommendations for containment, eradication, and prevention, aimed at enhancing the organization's security posture, reducing risk exposure, and ensuring resilience against evolving cyber threats. The ultimate goal is to strengthen defenses and ensure critical assets remain protected against potential exploitation.

2. Objective

- Detect and analyze simulated security incidents in real time.
- Test the effectiveness of Splunk SIEM for log ingestion, alerting, and threat detection.
- Classify and prioritize security events based on severity and potential impact.
- Provide remediation recommendations aligned with SOC best practices.
- Strengthen incident response capabilities and overall organizational security posture.

3. Scope

- Monitoring of simulated security events from authentication logs, network connection attempts, and malware alerts.
- Analysis of after-hours login activity and connections from both internal and external IP ranges.
- Detection of malware activity, including ransomware, trojan, rootkit, spyware, and worm infections.
- Classification of incidents based on severity, aligned with SOC triage standards.
- Focused use of Splunk SIEM for log ingestion, search, alerting, and dashboard-based monitoring.

4. Target Details

The analysis was performed on simulated SOC event data provided as `SOC_Task2_Sample_Logs.csv`.

The dataset contained:

- Authentication Events – Successful and failed login attempts, including after-hours activity.
- Network Connection Attempts – Both internal (private IP) and external (public IP) sources.
- Malware Alerts – Ransomware, trojan, rootkit, spyware, and worm detections.
- File Access Events – Suspicious file read/write activity.
- These logs were ingested into Splunk Enterprise for processing, field extraction, and security alert simulation. The simulated environment replicates a typical enterprise SOC data feed, enabling realistic detection and analysis workflows.

5. Tools Used

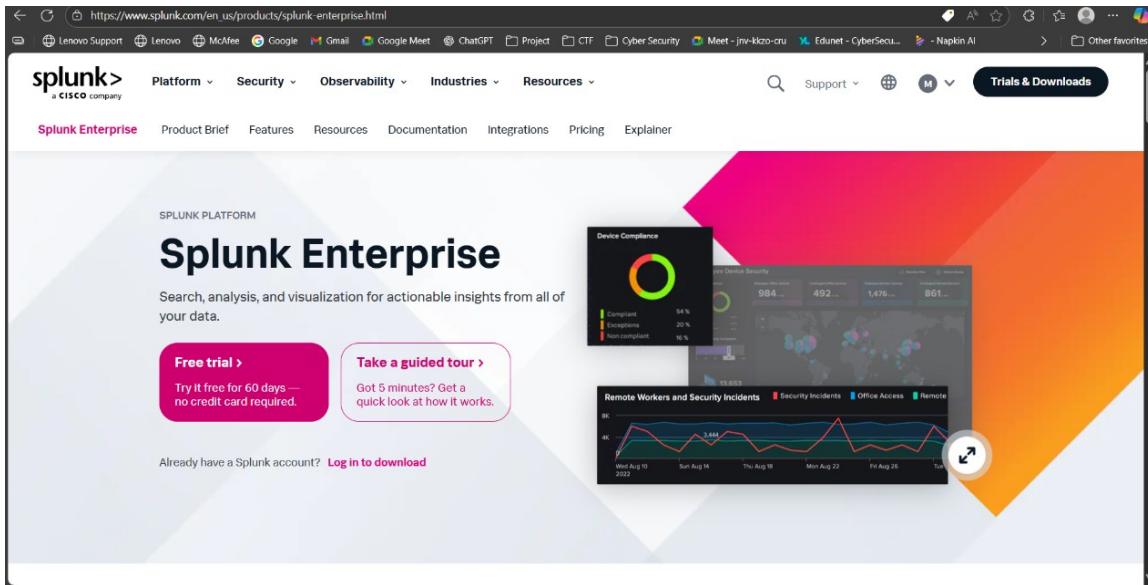
- Splunk Enterprise (Free Trial) – SIEM platform for log ingestion, search, and dashboarding.
- Google Docs / Microsoft Word – For report preparation.

6. SIEM Setup

Splunk Enterprise (Free Trial) was installed, configured, and used to ingest the provided SOC log dataset. Custom field extractions and SPL queries were created to detect, classify, and visualize security events.

6.1 Download and Install

1. Visit <https://www.splunk.com>



2. Navigate to Products → Splunk Enterprise
3. Click Free Trial and choose your OS (Windows, Linux, or macOS)
4. Create a free Splunk account (if not already registered)
5. Download the installer

6. Install using the default options (you may change the install directory if needed)
7. During installation, set an **admin username and password**

6.2 Access Splunk Web Interface

Open your browser and go to: <http://localhost:8000>

- Log in with the **admin credentials** you created during installation.
- You should now see the **Splunk Home Dashboard**.

6.3 Import Data

1. From the Splunk Home page, click Settings → Add Data

The screenshot shows the Splunk Enterprise homepage. On the left, there's a sidebar titled 'Apps' with various categories like 'Search & Reporting', 'Audit Trail', 'Data Management', etc. The main area is titled 'Hello, Administrator' and contains sections for 'Bookmarks', 'Dashboard', 'Search history', 'Recently viewed', 'Created by you', and 'Shared with you'. Below these are sections for 'Shared by me', 'Shared by other administrators', and 'Splunk recommended (13)'. At the bottom, there are 'Common tasks' such as 'Add data', 'Search your data', 'Visualize your data', 'Manage alerts', 'Add team members', and 'Manage permissions'.

2. Choose Upload

FOLLOW GUIDES FOR ONBOARDING POPULAR DATA SOURCES

This section displays four categories for uploading data sources:

- Cloud computing**: Get your cloud computing data in to the Splunk platform. (10 data sources)
- Networking**: Get your networking data in to the Splunk platform. (2 data sources)
- Operating System**: Get your operating system data in to the Splunk platform. (1 data source)
- Security**: Get your security data in to the Splunk platform. (3 data sources)

4 data sources in total

Or get data in with the following methods

This section shows three methods for getting data into Splunk:

- Upload**: files from my computer. (Local log files, Local structured files (e.g. CSV), Tutorial for adding data)
- Monitor**: files and ports on this Splunk platform instance. (Files - HTTP - WMI - TCP/UDP - Scripts, Modular inputs for external data sources)
- Forward**: data from a Splunk forwarder. (Files - TCP/UDP - Scripts)

3. Browse and select SOC_Task2_Sample_Logs.csv

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: SOC_Task2_Sample_Logs.csv

Select File

Drop your data file here
The maximum file upload size is 500 Mb

✓ File Successfully Uploaded

FAQ

- What kinds of files can the Splunk platform index?
- What is a source?
- How do I get remote data onto my Splunk platform instance?

- Click Next and Set Source type as csv, set delimiter according to the csv file, in this case it is pipe (|) operator.

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: SOC_Task2_Sample_Logs.csv

Source type: csv ▾

Save As

Timestamp

Delimited settings

Define how the Splunk platform extracts fields from structured data.

Field delimiter: (pipe) |

Quote character: (double quote) *

File preamble:

A regular expression that instructs Splunk to ignore these preamble lines within the file.

Field names: All... Lin... Cust... Rege...

| | _time | 2025_07_03_06_13_14 | action_connection attempt | EXTRA_FIELD_5 | ip_10_0_0_5 | user_charlie |
|---|--------------------------|---------------------|---------------------------|------------------------|------------------|--------------|
| 1 | 7/3/25 8:20:14.000 AM | 2025-07-03 08:20:14 | action=connection attempt | | ip=192.168.1.101 | user=charlie |
| 2 | 7/3/25 5:04:14.000 AM | 2025-07-03 05:04:14 | action=login success | | ip=192.168.1.101 | user=bob |
| 3 | 7/3/25 6:01:14.000 AM | 2025-07-03 06:01:14 | action=file accessed | | ip=172.16.0.3 | user=bob |
| 4 | 7/3/25 5:18:14.000 AM | 2025-07-03 05:18:14 | action=login success | | ip=172.16.0.3 | user=charlie |
| 5 | 7/3/25 4:27:14.000 AM | 2025-07-03 04:27:14 | action=connection attempt | | ip=172.16.0.3 | user=david |
| 6 | 7/3/25 5:48:14.000 AM | 2025-07-03 05:48:14 | action=malware detected | threat=Trojan Detected | ip=10.0.0.5 | user=bob |
| 7 | 7/3/25 8:30:14.000 AM | 2025-07-03 08:30:14 | action=login success | | ip=172.16.0.3 | user=eve |

View Event Summary

- Click Review → Submit to finish import

Review

Input Type Uploaded File
File Name SOC_Task2_Sample_Logs.csv
Source Type csv
Host JEMINA-PC
Index Default

Submit

6.4 Create Field Extractions

Once the data is imported, run the following SPL in **Search & Reporting** to extract key fields:

* - It is used to return all the data from all available logs

The screenshot shows the Splunk interface with a search bar containing a single asterisk (*). Below the search bar, it says "98 events (before 8/12/25 7:13:25.000 PM) No Event Sampling". The main area displays a table of search results with columns for Time and Event. The table includes several rows of log entries. At the bottom left, there are buttons for "Hide Fields" and "All Fields". On the right, there are buttons for "Format", "Show: 20 Per Page", and "View: List". The bottom right corner shows page navigation buttons (1, 2, 3, 4, 5, Next).

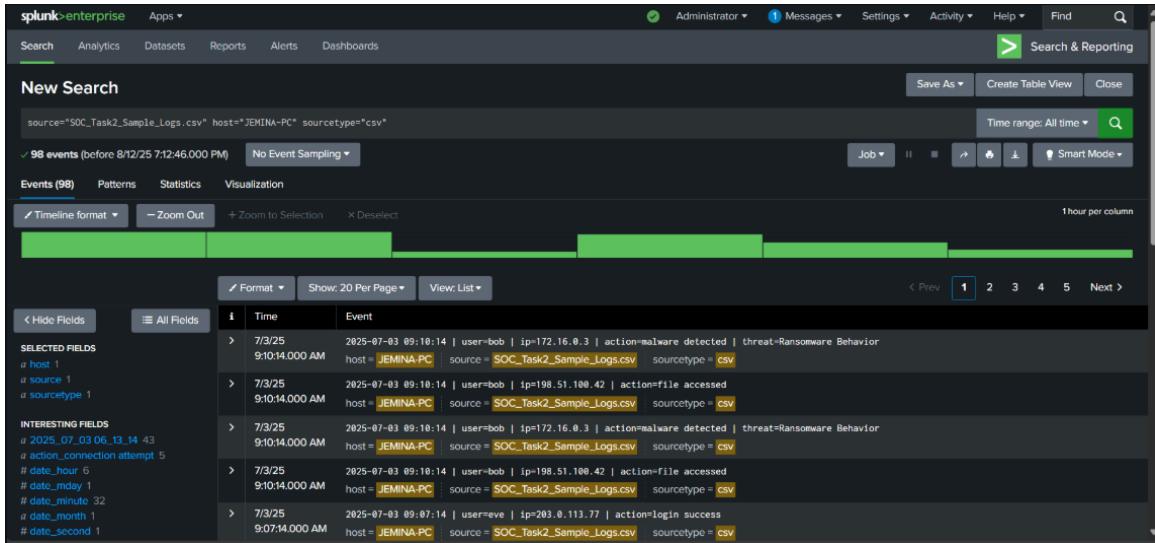
| Time | Event |
|-----------------------|--|
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=eve ip=203.0.113.77 action=login success host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |

To add a particular id or variable to filter search, right click on it and click add to search and enter to find the filtered results

The screenshot shows the Splunk interface with a search bar containing a single asterisk (*). Below the search bar, it says "98 events (before 8/12/25 7:14:30.000 PM) No Event Sampling". The main area displays a table of search results. A context menu is open over a specific log entry, showing options: "Add to search", "Exclude from search", and "New search". The bottom right corner shows page navigation buttons (1, 2, 3, 4, 5, Next).

| Time | Event |
|-----------------------|--|
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |
| 7/3/25 9:10:14.000 AM | 2025-07-03 09:10:14 user=eve ip=203.0.113.77 action=login success host = JEMINA-PC source = SOC_Task2_Sample_Logs.csv sourcetype = csv |

By default it will show the results of uploaded file or system logs:



7. Incident Overview and Alerts

Analysis of the ingested SOC logs revealed multiple security events, including after-hours logins, suspicious connection attempts, and high-severity malware detections, all categorized by severity for incident response.

The Splunk searches revealed multiple suspicious events:

- After-hours successful logins from public IP addresses.
- Internal and external connection attempts.
- Multiple malware detections (Trojan, Rootkit, Spyware, Ransomware, Worm).

7.1 After Hour Login

This detection identifies successful logins that occur outside the standard business hours of **09:00–19:00**. Such activity may indicate **compromised credentials**, **insider threats**, or unauthorized access attempts. While some after-hours activity may be legitimate (e.g., maintenance work), it should always be verified.

Why It Matters

- Threat actors often exploit off-hours when security staff presence is minimal.
- After-hours logins from unusual IPs can be an early indicator of account compromise.
- If combined with other suspicious actions (e.g., data exfiltration, malware execution), the severity increases significantly.

Severity

- **Medium** – For isolated after-hours logins.
- **High** – If linked with malicious activity such as file access anomalies or malware alerts.

Detection of After Hour Login in Splunk:

```

source="SOUC_Task2_Sample_Logs.csv"
| rex field=_raw "user=<user>\$+"
| rex field=_raw "ip=(?:ip\$\w*)"
| rex field=_raw "action=(?>action=\")+\"
| eval hour= strftime(_time, \"%I\")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time

```

56 events (before 8/13/25 12:15:05.000 PM) No Event Sampling ▾

| _time | user | ip | action | hour |
|---------------------|---------|---------------|---------------|------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.8.3 | login failed | 04 |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.8.3 | login failed | 04 |

Setting Alerts for After Hour Login:

To set alert for the following event, click on the “Save as” drop down, select “Alert”. It will open the Alert window, fill in the details and click save. Future events which have unusual logins will be viewed in the “Triggered Alerts” as you have saved it.

Save As Alert

| | | |
|---|---|---------------|
| Description | Montiors login success or failures outside working hours | |
| Permissions | Private | Shared in App |
| Alert type | Scheduled | Real-time |
| Expires | 10 | day(s) ▾ |
| Trigger Conditions | | |
| Trigger alert when | Per-Result ▾ | |
| Throttle ? | <input type="checkbox"/> | |
| Trigger Actions | | |
| + Add Actions ▾ | | |
| When triggered | <input checked="" type="checkbox"/> Add to Triggered Alerts | Remove |
| Severity Medium ▾ | | |
| <input type="button" value="Cancel"/> <input type="button" value="Save"/> | | |

Viewing Alerts in Splunk

1. Navigate to Activity (top right corner) → Triggered Alerts.

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user:(?<user>\$*)"
| rex field=_raw "ip:(?<ip>\$*)"
| rex field=_raw "action:(?<action>[^|]+)" 
| eval hour=strftime(_time,"%H")
| search action="Login success" OR action="Login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time
    
```

14 events (7/3/25 5:30:00.000 AM to 7/3/25 12:45:00.668 PM)

| _time | user | ip | action | hour |
|-------------------------------------|---------|---------------|---------------|------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | Login success | 04 |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | Login failed | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | Login failed | 04 |
| 2025-07-03 04:40:14 | david | 283.0.113.77 | Login success | 04 |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | Login failed | 04 |
| 2025-07-03 04:51:14 | david | 283.0.113.77 | Login success | 04 |
| 127.0.0.1 @8000 en-US/alerts/search | bob | 192.168.1.101 | Login success | 05 |

2. Click After-Hour Login → View Results to analyze details.

Triggered Alerts

Filter Show: 20 per ... of 2 pages

| App | Search & Report... | Owner | All owners | Severity | All severity | Alert name | All alerts | | |
|---|--------------------|-------|------------|-----------------------------|--------------|------------|------------|------------|---|
| Time | | | | Alert name | App | Type | Severity | Mode | Actions |
| 2025-08-13 13:22:27 India Standard Time | | | | Connection Attempt | search | Real-time | Low | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | Worm Infection Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | External Connection Attempt | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | Rootkit Alert | search | Real-time | Critical | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | Ransomware Detected | search | Real-time | High | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | Trojan Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | AfterHour_Login | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:26 India Standard Time | | | | Spyware Detected | search | Real-time | Low | Per Result | View Results Edit Search Delete |
| 2025-08-13 13:22:21 India Standard Time | | | | Connection Attempt | search | Real-time | Low | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | Worm Infection Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | External Connection Attempt | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | Rootkit Alert | search | Real-time | Critical | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | Ransomware Detected | search | Real-time | High | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | Trojan Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | AfterHour_Login | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| 2025-08-13 12:45:00 India Standard Time | | | | Spyware Detected | search | Real-time | Low | Per Result | View Results Edit Search Delete |

source="SOC_Task2_Sample.Logs.csv"
| rex field=_raw "user(?<user>\+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action(?<action>\[\"|\"])"
| eval hours= strftime(_time, "%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time

Time range: Before date time ▾ Q

14 events (W/70 5:30:00.000 AM to 8/13/25 12:26.951 PM) No Event Sampling ▾

Events Patterns Statistics (M) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | hour |
|---------------------|---------|---------------|---------------|------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | 04 |
| 2025-07-03 04:46:14 | david | 263.0.113.77 | login success | 04 |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | 04 |
| 2025-07-03 04:53:14 | david | 263.0.113.77 | login success | 04 |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | 05 |
| 2025-07-03 05:12:14 | alice | 198.51.100.42 | login success | 05 |
| 2025-07-03 05:18:14 | charlie | 172.16.0.3 | login success | 05 |
| 2025-07-03 06:21:14 | alice | 263.0.113.77 | login success | 06 |
| 2025-07-03 07:02:14 | alice | 263.0.113.77 | login failed | 07 |

3. Switch to the **Visualization** tab for charts and timelines.



Recommended Response

- Validate with the user if the login was intentional.
 - Check the source IP and geolocation.
 - Look for correlated suspicious activity in the same session.

- If confirmed malicious, **disable the account immediately** and initiate incident response.

7.2 Connection Attempt

This detection identifies network connection attempts made by hosts in the monitored environment. It differentiates between **internal** connections (originating from private IP ranges) and **external** connections (originating from public IP addresses). While internal connection attempts can indicate normal operations, they may also signal **lateral movement** if initiated by compromised devices. External connection attempts are more suspicious, as they may represent **probing, reconnaissance, or intrusion attempts** from outside the organization.

Why It Matters

- **Internal Connection Attempts** – May reveal lateral movement or unauthorized access to internal systems.
- **External Connection Attempts** – Could indicate targeted attacks, brute force attempts, or scanning from unknown entities.

Severity

- **Low** – Internal connection attempts from private IP ranges (10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x).
- **Medium** – External connection attempts from public IP addresses.

Detection of event in Splunk:

Internal Connection Attempt:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?>user>\$+)"
| rex field=_raw "ip=(?>ip>\$+)"
| rex field=_raw "action=(?>action>\$+)"
| search action="connection attempt"
| eval severity=case(
    match(ip, "^10\.\w{2}\.\w{2}\.\w{2}"), "Low",
    match(ip, "^192\.(168\.\w{1}){2}\w{1}\.\w{1}"), "Low",
    match(ip, "^172\.(16\.\w{1}|17\.\w{1}|19\.\w{1})\.\w{1}\.\w{1}"), "Low",
    true(), "Medium"
) | search severity="Low"
| table _time user ip action severity
| sort _time

```

| _time | user | ip | action | severity |
|---------------------|-------|----------|--------------------|----------|
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | Low |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | Low |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | Low |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | Low |

External Connection Attempt:

The screenshot shows a Splunk search interface. The search bar contains the following command:

```
source="SOC_Task2_Sample_logs.csv"
| rex field=_raw "user(?<user>$)"
| rex field=_raw "ip(?<ip>$)"
| rex field=_raw "action(?>action[*])"
| search action="connection attempt"
| eval severity=case(
    match(ip, '^10\.\d{2}\.\d{1,2}\.\d{1,2}$', "Low",
    match(ip, '^192\.\d{1,2}\.\d{1,2}\.\d{1,2}$', "Low",
    match(ip, '^172\.(1[6-9]|2[0-9]|3[0-1])\.\d{1,2}$', "Low",
    true), "Medium"
) | search severity="Medium"
| table _time user ip action severity
| sort _time
```

The results table shows 8 events from 2025-07-03 at 05:27:14 to 07:44:14. The columns are: _time, user, ip, action, and severity. All actions are "connection attempt" and severity is "Medium".

| _time | user | ip | action | severity |
|---------------------|-------|--------------|--------------------|----------|
| 2025-07-03 05:27:14 | david | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 05:27:14 | david | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 05:27:14 | david | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 05:27:14 | david | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 07:44:14 | bob | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 07:44:14 | bob | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 07:44:14 | bob | 203.0.113.77 | connection attempt | Medium |
| 2025-07-03 07:44:14 | bob | 203.0.113.77 | connection attempt | Medium |

Set Alert to Monitor Connection Attempt:

To set alert for the following event, click on the “Save as” drop down, select “Alert”. It will open the Alert window, fill in the details and click save. Future events which have unusual logins will be viewed in the “Triggered Alerts” as you have saved it.

For Internal Connection Attempt set Severity to low, and External set to High.

The dialog box is titled "Save As Alert". It has the following settings:

- Permissions: Private
- Alert type: Scheduled
- Expires: 10 day(s)
- Trigger Conditions:
 - Trigger alert when: Per-Result
 - Throttle:
- Trigger Actions:
 - + Add Actions ▾
 - When triggered:
 - Add to Triggered Alerts
 - Severity: Medium
- Buttons: Cancel, Save

Viewing Alerts in Splunk

1. Navigate to Activity (top right corner) → Triggered Alerts.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. On the far right of the header, there are buttons for Jobs, Triggered Alerts, and other system settings. Below the header is a search bar and a table titled "New Search". The search query is:

```
source="SOC_Task2_Sample_logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[\S]+)"
| eval hour=strftime(_time,"%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time
```

The table displays 14 events from July 3, 2025, between 04:18:14 and 04:51:14. The columns are: _time, user, ip, action, and hour. The data includes various logins (success and failed) for users like bob, charlie, and david across different IP addresses and hours.

2. Click Connection Attempt → View Results to analyze details.

The screenshot shows the "Triggered Alerts" page. At the top, there are filters for App, Owner, Severity, Alert name, and All alerts. The main area shows a table of 24 results, with the first few rows listed below:

| | Time | Alert name | App | Type | Severity | Mode | Actions |
|--------------------------|---|-----------------------------|--------|-----------|----------|------------|---|
| <input type="checkbox"/> | 2025-08-13 13:22:27 India Standard Time | Connection Attempt | search | Real-time | Low | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Worm Infection Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | External Connection Attempt | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Rootkit Alert | search | Real-time | Critical | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Ransomware Detected | search | Real-time | High | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Trojan Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | AfterHour_Login | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Spyware Detected | search | Real-time | Low | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:21 India Standard Time | Connection Attempt | search | Real-time | Low | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Worm Infection Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | External Connection Attempt | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Rootkit Alert | search | Real-time | Critical | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Ransomware Detected | search | Real-time | High | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Trojan Alert | search | Real-time | High | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | AfterHour_Login | search | Real-time | Medium | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Spyware Detected | search | Real-time | Low | Per Result | View Results Edit Search Delete |

3. Using Statistics, we can see the number of occurrences of each event

New Search

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user:(?<user>\\$+)"
| rex field=_raw "ip:(?<ip>\\$+)"
| rex field=_raw "action:(?>action>[!\\])"
| search action="connection attempt"
| eval severity=case(
 match(ip, "*10.", "Low",
 match(ip, "*192.168.", "Low",
 match(ip, "*172.([6-9]|2[0-9]|3[0-1]).", "Low",
 true), "Medium"
) | search severity="Medium"
| table _time user ip action severity
| sort _time

Time range: Before date time ▾ 🔍

2 events (IV70 5:30:00.000 AM to 8/13/25 12:45:00.655 PM) No Event Sampling ▾

Events Patterns Statistics (2) Visualization Job ▾ || ↶ ↷ ↓ ⚡ Fast Mode ▾

Show: 20 Per Page Format ▾ Preview: On

| _time | user | ip | action | severity |
|---------------------|-------|--------------|--------------------|----------|
| 2025-07-03 05:27:14 | david | 283.0.113.77 | connection attempt | Medium |
| 2025-07-03 07:44:14 | bob | 283.0.113.77 | connection attempt | Medium |

Recommended Response

- **For Internal (Low Severity):**
 - Verify if the source host is performing legitimate network operations.
 - Review system logs for signs of lateral movement.
 - **For External (Medium Severity):**
 - Check IP reputation using threat intelligence sources.
 - Block or restrict communication from suspicious IPs.
 - Investigate for potential intrusion attempts.

7.3 Ransomware Alert

This detection identifies events in which the threat field contains indicators of **Ransomware activity**. Ransomware is a type of malicious software that encrypts files on a victim's system and demands payment (usually in cryptocurrency) for the decryption key. Early detection is critical to prevent widespread damage and data loss.

Why It Matters

- Ransomware attacks can lead to **complete data unavailability, business downtime, and financial loss**.
 - Quick containment is necessary to prevent the spread to other systems within the network.
 - In many cases, ransomware detection may indicate an **ongoing compromise** that requires immediate incident response.

Severity

High – Any ransomware detection should be treated as a critical incident.

Detecting in Splunk Search:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>[^>]+)"
| rex field=_raw "ip=(?<ip>[^>]+)"
| rex field=_raw "action(?<action>[^>]+)"
| rex field=_raw "threat(?<threat>[^>]+)"
| eval malware_type=case(
    match(threat, '(?i)Trojan'), 'Trojan',
    match(threat, '(?i)Rootkit'), 'Rootkit',
    match(threat, '(?i)Spyware'), 'Spyware',
    match(threat, '(?i)Ransomware'), 'Ransomware',
    match(threat, '(?i)Worm'), 'Worm Infection',
    true(), 'Other'
)
| search malware_type="Ransomware"
| table _time user ip action threat malware_type

```

6 events (before 8/13/25 5:36:30.000 PM) No Event Sampling

Events Patterns Statistics (6) Visualization Job ▾ II ⌂ 🔍 Smart Mode ▾

Show: 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | threat | malware_type |
|---------------------|------|------------|------------------|---------------------|--------------|
| 2025-07-03 09:18:14 | bob | 172.16.0.3 | malware detected | Ransomware Behavior | Ransomware |
| 2025-07-03 09:18:14 | bob | 172.16.0.3 | malware detected | Ransomware Behavior | Ransomware |
| 2025-07-03 09:18:14 | bob | 172.16.0.3 | malware detected | Ransomware Behavior | Ransomware |

Viewing Alerts in Splunk

1. Navigate to Activity (top right corner) → Triggered Alerts.

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>[^>]+)"
| rex field=_raw "ip=(?<ip>[^>]+)"
| rex field=_raw "action(?<action>[^>]+)"
| eval hour=strftime(_time,"%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time

```

14 events (7/7/25 5:30:00.000 AM to 8/13/25 12:45:00.668 PM) No Event Sampling

Events Patterns Statistics (14) Visualization Job ▾ II ⌂ 🔍 Fast Mode ▾

Show: 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | hour |
|----------------------------------|---------|---------------|---------------|------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | 04 |
| 2025-07-03 04:40:14 | david | 203.0.113.77 | login success | 04 |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | 04 |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | 04 |
| 12.0.0.18000/en-US/alerts/search | bob | 192.168.1.191 | login success | 05 |

2. Click Ransomware Detected → View Results to analyze details.

Triggered Alerts

Filter Show: 1 - 20 of 24 results

| App | Search & Report... | Owner | Severity | Alert name | All alerts | Actions | | |
|--------------------------|---|-------|----------|-----------------------------|------------|-----------|------------|---|
| <input type="checkbox"/> | Time | | Low | Connection Attempt | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:27 India Standard Time | | High | Worm Infection Alert | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Medium | External Connection Attempt | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Critical | Rootkit Alert | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | High | Ransomware Detected | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | High | Trojan Alert | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Medium | AfterHour_Login | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Low | Spyware Detected | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 13:22:21 India Standard Time | | Low | Connection Attempt | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | High | Worm Infection Alert | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Medium | External Connection Attempt | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Critical | Rootkit Alert | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | High | Ransomware Detected | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | High | Trojan Alert | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Medium | AfterHour_Login | search | Real-time | Per Result | View Results Edit Search Delete |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Low | Spyware Detected | search | Real-time | Per Result | View Results Edit Search Delete |

3. Using Statistics, we can see the number of occurrences of each event

The screenshot shows the Splunk interface with a search bar at the top containing a complex regex-based search command. Below the search bar is a table titled 'Statistics' with one row of data. The table columns are: _time, user, ip, action, threat, and malware_type. The data row is: 2025-07-03 09:18:14, bob, 172.16.8.3, malware_detected, Ransomware Behavior, Ransomware. At the bottom of the interface, there are various navigation and configuration buttons.

Recommended Response

- Immediately **isolate affected systems** from the network.
- Identify and secure backups before ransomware can encrypt them.
- Begin incident response procedures, including malware removal and forensic investigation.
- Notify relevant stakeholders and, if required, legal and compliance teams.

7.4 Rootkit Alert

This detection identifies events in which the threat field contains indicators of **Rootkit activity**. Rootkits are malicious tools designed to gain privileged access to a computer system while actively hiding their presence. They often modify the operating system's core components to conceal files, processes, and network connections, making them extremely difficult to detect and remove.

Why It Matters

- Rootkits enable **persistent and stealthy access** to compromised systems.
- They can disable security tools, making further compromise easier.
- Often used as part of **Advanced Persistent Threat (APT)** campaigns.

Severity

- **Critical** – Any rootkit detection should be treated as a critical security incident.

Detecting in Splunk Search:

The screenshot shows a Splunk search interface. The search bar contains the following command:

```
source="SOC_Task2_Sample_logs.csv"
| rex field=_raw "user=(?<user>\$)"
| rex field=_raw "ip=(?<ip>\$4)"
| rex field=_raw "action=(?>action>[\"])"
| rex field=_raw "threat=(?>threat>.+)"
| eval malware_typecase(
    match(threat, "(?1)Trojan"), "Trojan",
    match(threat, "(?1)Rootkit"), "Rootkit",
    match(threat, "(?1)Spyware"), "Spyware",
    match(threat, "(?1)Ransomware"), "Ransomware",
    match(threat, "(?1)Worm"), "Worm Infection",
    true(), "Other"
)
| search malware_type="Rootkit"
| table _time user ip action threat malware_type
```

The search results pane shows 6 events from July 3, 2025, between 4:18:14 AM and 8:13:25 PM. The results are as follows:

| _time | user | ip | action | threat | malware_type |
|---------------------|-------|---------------|------------------|-------------------|--------------|
| 2025-07-03 07:51:14 | eve | 10.0.0.5 | malware detected | Rootkit Signature | Rootkit |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | Rootkit |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | Rootkit |
| 2025-07-03 07:51:14 | eve | 10.0.0.5 | malware detected | Rootkit Signature | Rootkit |
| 2025-07-03 07:51:14 | eve | 10.0.0.5 | malware detected | Rootkit Signature | Rootkit |

Viewing Alerts in Splunk

1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk enterprise' logo, 'Apps', 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the top bar are links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a magnifying glass icon for search. Below the top bar is a secondary navigation bar with 'Jobs' (selected), 'Triggered Alerts', 'Save As...', 'Create Table View', and 'Close'. A green banner at the top says 'New Search'. The main area shows a search command in the text input field:

```
source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>>S)"
| rex field=_raw "ip=(?<ip>>S)"
| rex field=_raw "action=(?<action>[! ]+)"
| eval hour=strftime(_time,"%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time
```

Below the command, it says 'Time range: Before date time' with a green search button. Underneath the command is a summary: '✓ 14 events (7/7/20 5:30:00.000 AM to 8/3/25 12:45:00.668 PM) No Event Sampling'. To the right are buttons for 'Job', 'Fast Mode', and other controls. The bottom section is a table with columns: '_time', 'user', 'ip', 'action', and 'hour'. The table contains 14 rows of log data. At the very bottom left is the URL '127.0.0.1:8000/app/US/alerts/search'.

2. Click **Rootkit Detected** → **View Results** to analyze details.

| Triggered Alerts | | | | | | |
|--------------------------|---|------------------------------|-----------------------------|------------|------------|------------|
| Filter | | Showing 1 - 20 of 24 results | | | | |
| | | Owner | Severity | Alert name | All alerts | 1 per page |
| <input type="checkbox"/> | Time | | Alert name | App | Type | Severity |
| <input type="checkbox"/> | 2025-08-13 13:22:27 India Standard Time | | Connection Attempt | search | Real-time | Low |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Worm Infection Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | External Connection Attempt | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Rootkit Alert | search | Real-time | Critical |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Ransomware Detected | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Trojan Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | AfterHour_Login | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | Spyware Detected | search | Real-time | Low |
| <input type="checkbox"/> | 2025-08-13 13:22:21 India Standard Time | | Connection Attempt | search | Real-time | Low |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Worm Infection Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | External Connection Attempt | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Rootkit Alert | search | Real-time | Critical |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Ransomware Detected | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Trojan Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | AfterHour_Login | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | Spyware Detected | search | Real-time | Low |

3. Using Statistics, we can see the number of occurrences of each event

New Search

```
source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\$+)"
| rex field=_raw "ip=(?<ip>\$+)"
| rex field=_raw "action=(?<action>\$+)"
| rex field=_raw "threat=(?<threat>\$+)"
| eval malware_type=case(
    match(threat, "(?!)Trojan"), "Trojan",
    match(threat, "(?!)Rootkit"), "Rootkit",
    match(threat, "(?!)Spyware"), "Spyware",
    match(threat, "(?!)Ransomware"), "Ransomware",
    match(threat, "(?!)Worm"), "Worm Infection",
    true), "Other"
)
| search malware_type="Rootkit"
| table _time user ip action threat malware_type
```

2 events (IV/70 5:30:00.000 AM to 8/13/25 1:22:26.952 PM) No Event Sampling

Events Patterns Statistics (2) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | threat | malware_type |
|---------------------|-------|---------------|------------------|-------------------|--------------|
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | Rootkit |
| 2025-07-03 07:51:14 | eve | 18.0.0.5 | malware detected | Rootkit Signature | Rootkit |

Recommended Response

- Immediately **quarantine affected systems** from the network.
- Use trusted offline tools to scan and attempt rootkit removal.
- Perform **memory forensics** to uncover hidden processes.
- Consider **reinstalling the OS** if removal cannot be guaranteed.
- Review system logs and access history for possible data exfiltration.

7.5 Spyware Alerts

This detection identifies events in which the threat field contains indicators of **Spyware activity**. Spyware is malicious software designed to secretly monitor user activity, collect

sensitive information (such as credentials, browsing history, or keystrokes), and send it to an attacker without the user's consent.

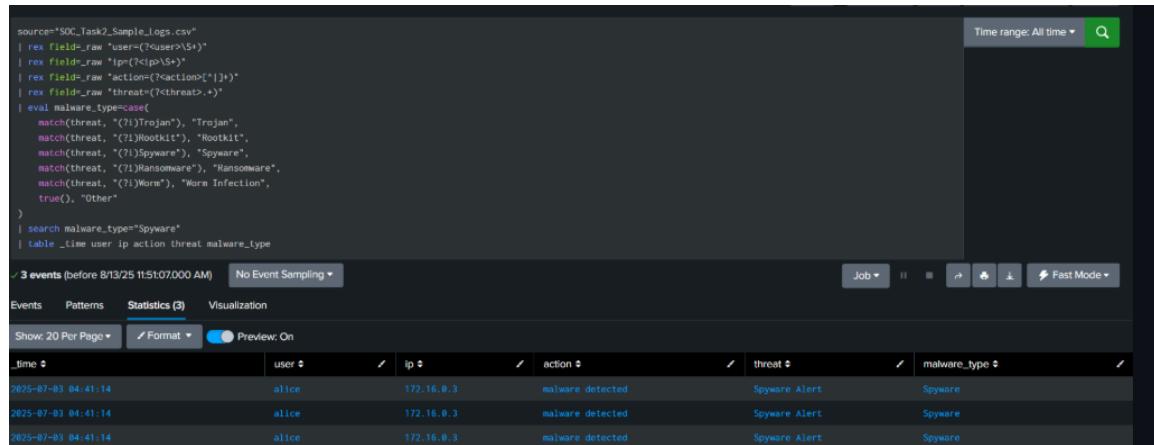
Why It Matters

- Can lead to **credential theft** and **identity compromise**.
- Often operates silently, making detection difficult until damage is done.
- Frequently used as part of **espionage campaigns** to gather long-term intelligence.

Severity

- **High** – Any spyware detection should be treated as a critical incident due to its data theft potential.

Detecting in Splunk Search:



```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>[Ss])"
| rex field=_raw "ip=(?<ip>[Ss])"
| rex field=_raw "action=(?<action>[^|]+)"
| rex field=_raw "threat=(?<threat>[^|]+)"
| eval malware_type=case
    match(threat, "(?!)Trojan", "Trojan",
    match(threat, "(?!)Rootkit", "Rootkit",
    match(threat, "(?!)Spyware", "Spyware",
    match(threat, "(?!)Ransomware", "Ransomware",
    match(threat, "(?!)Worm", "Worm Infection",
    true(), "Other"
)
| search malware_type="Spyware"
| table _time user ip action threat malware_type

```

Time range: All time ▾ 🔍

3 events (before 8/13/25 11:51:07:000 AM) No Event Sampling

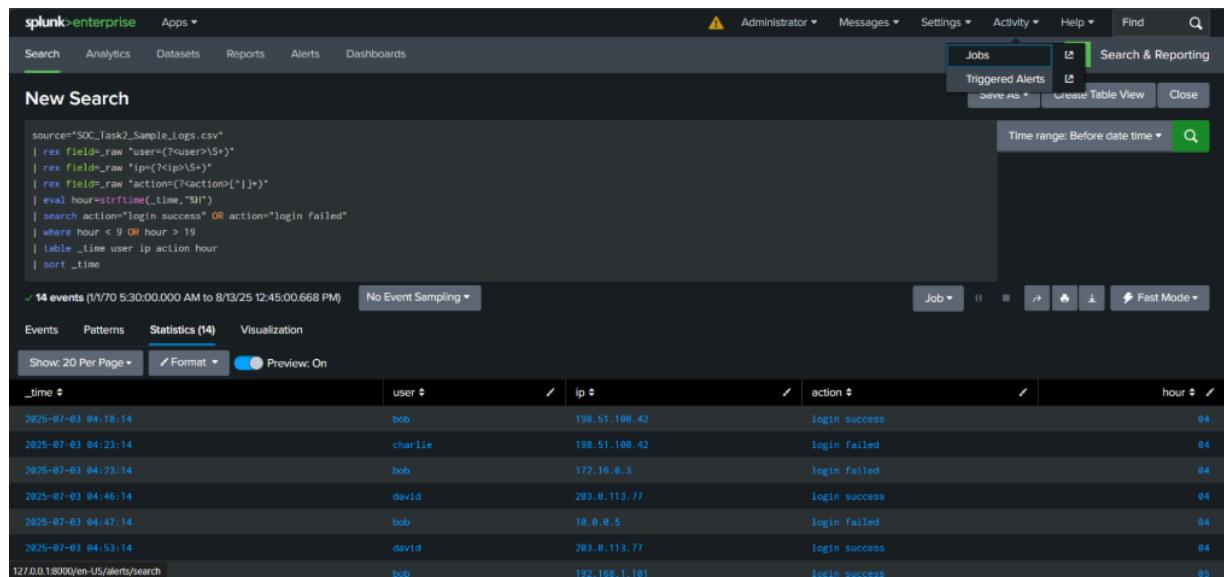
Events Patterns Statistics (3) Visualization

Show: 20 Per Page ▾ Format Preview: On

| _time | user | ip | action | threat | malware_type |
|---------------------|-------|------------|------------------|---------------|--------------|
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware |

Viewing Alerts in Splunk

1. Navigate to Activity (top right corner) → Triggered Alerts.



spunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Jobs Triggered Alerts Save As ▾ Create Table View Close

New Search

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>[Ss])"
| rex field=_raw "ip=(?<ip>[Ss])"
| rex field=_raw "action=(?<action>[^|]+)"
| eval hour=strftime(_time,"%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time

```

14 events (1/1/70 5:30:00.000 AM to 8/13/25 12:45:00.668 PM) No Event Sampling

Events Patterns Statistics (14) Visualization

Show: 20 Per Page ▾ Format Preview: On

| _time | user | ip | action | hour |
|------------------------------------|---------|---------------|---------------|------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | Login failed | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | Login failed | 04 |
| 2025-07-03 04:46:14 | david | 283.0.113.77 | login success | 04 |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | Login failed | 04 |
| 2025-07-03 04:53:14 | david | 283.0.113.77 | login success | 04 |
| 127.0.0.1:8000/en-US/alerts/search | bob | 192.168.1.101 | login success | 05 |

2. Click Spyware Detected → View Results to analyze details.

| Triggered Alerts | | | | | | | |
|--------------------------|---|-------|--|-----------------------------|--------------|------------|------------|
| Filter | | Owner | | Severity | All severity | Alert name | All alerts |
| <input type="checkbox"/> | Time | | | Alert name | App | Type | Severity |
| <input type="checkbox"/> | 2025-08-13 13:22:27 India Standard Time | | | Connection Attempt | search | Real-time | Low |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Worm Infection Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | External Connection Attempt | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Rootkit Alert | search | Real-time | Critical |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Ransomware Detected | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Trojan Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | AfterHour_Login | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Spyware Detected | search | Real-time | Low |
| <input type="checkbox"/> | 2025-08-13 13:22:21 India Standard Time | | | Connection Attempt | search | Real-time | Low |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Worm Infection Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | External Connection Attempt | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Rootkit Alert | search | Real-time | Critical |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Ransomware Detected | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Trojan Alert | search | Real-time | High |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | AfterHour_Login | search | Real-time | Medium |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Spyware Detected | search | Real-time | Low |

3. Using Statistics, we can see the number of occurrences of each event

New Search

```
source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user(<user>)$"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action(<action>[^|]+)"
| rex field=_raw "threat(<threat>.+)"
| eval malware_type=case(
    match(threat, "(?!Trojan)", "Trojan",
    match(threat, "(?!Rootkit)", "Rootkit",
    match(threat, "(?!Spyware)", "Spyware",
    match(threat, "(?!Ransomware)", "Ransomware",
    match(threat, "(?!Worm)", "Worm Infection",
    true(), "Other"
)
| search malware_type="Spyware"
| table _time user ip action threat malware_type
```

1 event (1/1/70 50:00:00 AM to 8/13/25 1:22:26.952 PM) No Event Sampling ▾ Job ▾

Events Patterns Statistics (1) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | threat | malware_type |
|---------------------|-------|------------|------------------|---------------|--------------|
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware_detected | Spyware Alert | Spyware |

Recommended Response

- Immediately **disconnect affected hosts** from the network.
- Identify and remove the spyware using trusted security tools.
- Rotate all potentially compromised credentials.
- Conduct a full **endpoint forensic investigation** to determine data loss.
- Increase monitoring for follow-up compromise attempts.

7.6 Trojan Alert

This detection identifies events where the threat field contains indicators of **Trojan activity**. A Trojan (or Trojan Horse) is a type of malicious software that disguises itself as

legitimate software to trick users into executing it. Once inside the system, it can create backdoors, steal sensitive information, or deploy additional malicious payloads.

Why It Matters

- Trojans can be the **entry point** for larger attacks such as ransomware or data exfiltration.
 - Often used by attackers to gain **persistent access** to compromised systems.
 - Can evade detection by masquerading as harmless files or applications.

Severity

- **High** – Trojans pose a significant risk to system integrity and data security.

Detecting in Splunk Search:

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\\$4)"
| rex field=_raw "ip=(?<ip>\\$5)"
| rex field=_raw "action=(?<action>[!\\n]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval malware_type=case(
 match(threat, "(?i)Trojan"), "Trojan",
 match(threat, "(?i)Rootkit"), "Rootkit",
 match(threat, "(?i)Spyware"), "Spyware",
 match(threat, "(?i)Ransomware"), "Ransomware",
 match(threat, "(?i)Worm"), "Worm Infection",
 true(), "Other"
)
| search malware_type="Spyware"
| table _time user ip action threat malware_type

3 events (before 8/13/25 11:51:07.000 AM) No Event Sampling ▾ Job ▾ II ■ ⚡ 🔍 Fast Mode ▾

Events Patterns Statistics (3) Visualization

Show 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | threat | malware_type |
|---------------------|-------|------------|------------------|---------------|--------------|
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware |

Viewing Alerts in Splunk

1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.

2. Click **Trojan Detected** → **View Results** to analyze details.

| Triggered Alerts | | | | | | |
|--------------------------|---|------------------------------|------------|-----------------------------|--------------|------------|
| Filter | | Showing 1 - 20 of 24 results | | | | |
| App | Search & Report... | Owner | All owners | Severity | All severity | Alert name |
| <input type="checkbox"/> | Time | | | Alert name | App | Type |
| <input type="checkbox"/> | 2025-08-13 13:22:27 India Standard Time | | | Connection Attempt | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Worm Infection Alert | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | External Connection Attempt | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Rootkit Alert | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Ransomware Detected | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Trojan Alert | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | AfterHour_Login | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | | | Spyware Detected | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 13:22:21 India Standard Time | | | Connection Attempt | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Worm Infection Alert | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | External Connection Attempt | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Rootkit Alert | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Ransomware Detected | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Trojan Alert | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | AfterHour_Login | search | Real-time |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | | | Spyware Detected | search | Real-time |

3. Using Statistics, we can see the number of occurrences of each event

| source=*SOC_Task2_Sample_Logs.csv* rex field=_raw "user=(?<user>[^\$])" rex field=_raw "ip=(?<ip>\S+)" rex field=_raw "action=(?<action>[^\]+)" rex field=_raw "threat=(?<threat>.+)" eval malware_type=case(match(threat, "(?i)Trojan"), "Trojan", match(threat, "(?i)Rootkit"), "Rootkit", match(threat, "(?i)Spyware"), "Spyware", match(threat, "(?i)Ransomware"), "Ransomware", match(threat, "(?i)Worm"), "Worm Infection", true), "Other") search malware_type="Trojan" table _time user ip action threat malware_type | | | | | | |
|--|---------|---------------|------------------|-----------------|--------------|--|
| Time range: Before date time ▾  | | | | | | |
|  Job ▾      | | | | | | |
|  Events  Patterns  Statistics (6)  | | | | | | |
|  Show 20 Per Page ▾  Format ▾  Preview: On | | | | | | |
| _time | user | ip | action | threat | malware_type | |
| 2025-07-03 05:48:14 | bob | 10.0.0.5 | malware detected | Trojan Detected | Trojan | |
| 2025-07-03 05:45:14 | david | 172.16.0.3 | malware detected | Trojan Detected | Trojan | |
| 2025-07-03 05:30:14 | eve | 192.168.1.101 | malware detected | Trojan Detected | Trojan | |
| 2025-07-03 05:42:14 | eve | 203.0.113.77 | malware detected | Trojan Detected | Trojan | |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan | |
| 2025-07-03 07:45:14 | charlie | 172.16.0.3 | malware detected | Trojan Detected | Trojan | |

Recommended Response

- Isolate affected machines** from the network immediately.
- Remove Trojan infection using reputable antivirus or malware removal tools.
- Check for **backdoors or unauthorized accounts** created by the Trojan.
- Monitor for **secondary payloads** such as ransomware.
- Conduct full incident investigation and restore clean backups if necessary.

7.7 Worm Infection Alert

This detection identifies events where the threat field contains indicators of **Worm infection**. Worms are self-replicating malware that spread across networks without user

intervention, often exploiting vulnerabilities or weak security configurations. They can cause network congestion, system crashes, and act as carriers for additional malware.

Why It Matters

- Worms can **spread rapidly** within internal and external networks.
- Often used to deploy **payloads such as ransomware or Trojans**.
- Can lead to **widespread operational disruption** in minutes if unchecked.

Severity

- **High** – Immediate containment is required due to rapid infection potential.

Detecting in Splunk Search:

The screenshot shows a Splunk search interface with the following search command:

```
source="SOC_Task2_Sample.Logs.csv"
| rex fields=_raw "user=(?<user>>+)"
| rex fields=_raw "ip=(?<ip>\$)"
| rex fields=_raw "action=(?<action>[\"1\"])"
| rex fields=_raw "threat=(?<threat>+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",
    match(threat, "(?i)Ransomware"), "Ransomware",
    match(threat, "(?i)Worm"), "Worm Infection",
    true(), "Other"
)
| search malware_type="Worm Infection"
| table _time user ip action threat malware_type
```

The results table shows three events:

| _time | user | ip | action | threat | malware_type |
|---------------------|------|--------------|------------------|------------------------|----------------|
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection |

Viewing Alerts in Splunk

1. Navigate to Activity (top right corner) → Triggered Alerts.

The screenshot shows a Splunk search interface with the following search command:

```
source="SOC_Task2_Sample.Logs.csv"
| rex fields=_raw "user=(?<user>>+)"
| rex fields=_raw "ip=(?<ip>\$)"
| rex fields=_raw "action=(?<action>[\"1\"])"
| eval hour=strftime(_time, "%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time
```

The results table shows 14 events:

| _time | user | ip | action | hour |
|------------------------------------|---------|---------------|---------------|------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | 04 |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | 04 |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | 04 |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | 04 |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | 04 |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | 04 |
| 127.0.0.1:8000/en-US/alerts/search | bob | 192.168.1.101 | login success | 05 |

2. Click Trojan Detected → View Results to analyze details.

| Triggered Alerts | | | | | | |
|--------------------------|---|-----------------------------|--------|-----------|------------|------------|
| Filter | | Search & Report... | | Owner | All owners | Severity |
| | Time | Alert name | App | Type | Severity | Mode |
| <input type="checkbox"/> | 2025-08-13 13:22:27 India Standard Time | Connection Attempt | search | Real-time | Low | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Worm Infection Alert | search | Real-time | High | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | External Connection Attempt | search | Real-time | Medium | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Rootkit Alert | search | Real-time | Critical | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Ransomware Detected | search | Real-time | High | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Trojan Alert | search | Real-time | High | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | AfterHour_Login | search | Real-time | Medium | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:26 India Standard Time | Spyware Detected | search | Real-time | Low | Per Result |
| <input type="checkbox"/> | 2025-08-13 13:22:21 India Standard Time | Connection Attempt | search | Real-time | Low | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Worm Infection Alert | search | Real-time | High | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | External Connection Attempt | search | Real-time | Medium | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Rootkit Alert | search | Real-time | Critical | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Ransomware Detected | search | Real-time | High | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Trojan Alert | search | Real-time | High | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | AfterHour_Login | search | Real-time | Medium | Per Result |
| <input type="checkbox"/> | 2025-08-13 12:45:00 India Standard Time | Spyware Detected | search | Real-time | Low | Per Result |

3. Using Statistics, we can see the number of occurrences of each event

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^]+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",
    match(threat, "(?i)Ransomware"), "Ransomware",
    match(threat, "(?i)Worm"), "Worm Infection",
    true(), "Other"
)
| search malware_type="Worm Infection"
| table _time user ip action threat malware_type

```

1 event (1/170 5:30:00.000 AM to 8/13/25 12:45:00.674 PM) No Event Sampling

Events Patterns Statistics (1) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

| _time | user | ip | action | threat | malware_type |
|---------------------|------|--------------|------------------|------------------------|----------------|
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware_detected | Worm Infection Attempt | Worm Infection |

8. Detection Logic

Detection was based on SPL queries to extract relevant fields, identify patterns, and classify events.

8.1 After Hour Login

Detects successful logins outside of standard business hours (09:00–19:00).

Severity: Medium (unless combined with malware indicators).

SPL Query:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^]+)"

```

```

| eval hour=strftime(_time,"%H")
| search action="login success" OR action="login failed"
| where hour < 9 OR hour > 19
| table _time user ip action hour
| sort _time

```

8.2 Internal Connection Attempt

Detects connection attempt events from private IP ranges.

Severity: Low.

SPL Query:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| search action="connection attempt"
| eval severity=case(
    match(ip, "^10\."), "Low",
    match(ip, "^192\.168\."), "Low",
    match(ip, "^172\.(1[6-9]|2[0-9]|3[0-1])\."), "Low",
    true(), "Medium"
)
| search severity="Low"
| table _time user ip action severity
| sort _time

```

8.3 External Connection Attempt

Detects connection attempt events from public IP addresses.

Severity: Medium.

SPL Query:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| search action="connection attempt"
| eval severity=case(
    match(ip, "^10\."), "Low",
    match(ip, "^192\.168\."), "Low",
    match(ip, "^172\.(1[6-9]|2[0-9]|3[0-1])\."), "Low",
    true(), "Medium"
)
| search severity="Medium"
| table _time user ip action severity
| sort _time

```

8.4 Ransomware Detection

Detects threats with “Ransomware” in the threat field.

Severity: High.

SPL Query:

```
source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",
    match(threat, "(?i)Ransomware"), "Ransomware",
    match(threat, "(?i)Worm"), "Worm Infection", true(), "Other" )
| search malware_type="Ransomware"
| table _time user ip action threat malware_type
```

8.5 Rootkit Detection

Detects threats with “Rootkit” signatures.

Severity: High.

SPL Query:

```
source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",
    match(threat, "(?i)Ransomware"), "Ransomware",
    match(threat, "(?i)Worm"), "Worm Infection", true(), "Other" )
| search malware_type="Rootkit"
| table _time user ip action threat malware_type
```

8.6 Spyware Detection

Detects threats with “Spyware” in the threat field.

Severity: High.

SPL Query:

```
source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
```

```

| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",
    match(threat, "(?i)Ransomware"), "Ransomware",
    match(threat, "(?i)Worm"), "Worm Infection", true(), "Other" )
| search malware_type="Spyware"
| table _time user ip action threat malware_type

```

8.7 Trojan Detection

Detects threats with “Trojan” in the threat field.

Severity: High.

SPL Query:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",
    match(threat, "(?i)Ransomware"), "Ransomware",
    match(threat, "(?i)Worm"), "Worm Infection", true(), "Other" )
| search malware_type="Trojan"
| table _time user ip action threat malware_type

```

8.8 Worm Infection Detection

Detects threats with “Worm” in the threat field.

Severity: High.

SPL Query:

```

source="SOC_Task2_Sample_Logs.csv"
| rex field=_raw "user=(?<user>\S+)"
| rex field=_raw "ip=(?<ip>\S+)"
| rex field=_raw "action=(?<action>[^|]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval malware_type=case(
    match(threat, "(?i)Trojan"), "Trojan",
    match(threat, "(?i)Rootkit"), "Rootkit",
    match(threat, "(?i)Spyware"), "Spyware",

```

```
match(threat, "(?i)Ransomware"), "Ransomware",
match(threat, "(?i)Worm"), "Worm Infection", true(), "Other" )
| search malware_type="Worm Infection"
| table _time user ip action threat malware_type
```

9. Incident Classification and Severity

All detected security events were assigned a **severity rating** based on potential business impact, urgency for response, and likelihood of compromise. The classification follows a SOC-inspired triage model:

- **High Severity –**
 1. Incidents that indicate confirmed or highly probable **malware compromise**.
 2. This includes: **Trojan**, **Rootkit**, **Spyware**, **Ransomware**, and **Worm Infection** detections.
 3. These threats can cause severe operational disruption, data exfiltration, or complete system compromise.
 4. **Immediate response** and containment actions are required to prevent further spread or damage.
- **Medium Severity –**
 1. Incidents that present **elevated risk** but are not yet confirmed as active compromise.
 2. Examples include **after-hours successful logins from public IPs** and **external connection attempts** from unrecognized sources.
 3. These activities may indicate **account compromise** or **reconnaissance attempts** and require prompt investigation to determine legitimacy.
- **Low Severity –**
 1. Incidents that typically occur within **normal network boundaries** but may still warrant monitoring for anomalous patterns.
 2. For example, **internal connection attempts** from private IP address ranges (10.x.x.x, 172.16–31.x.x, 192.168.x.x).
 3. While these may be routine, they should be reviewed to ensure they align with expected network behaviour.

Incident Classification SPL in Splunk:

```

source="SOC_Task2_Sample_Logs.csv" | rex field=_raw "user=(?<user>\$+)"
| rex field=_raw "ip=(?<ip>\$+)"
| rex field=_raw "action=(?<action>[!]+)"
| rex field=_raw "threat=(?<threat>.+)"
| eval hour=strftime(_time,"%H")
| eval priority=case(
    match(threat, "(?)Trojan|Rootkit|Worm|Ransomware"), "High",
    (action=="login success" AND match(ip, "(198\.[203\.]*)") AND (hour<9 OR hour>19)), "Medium",
    (action=="login failed" AND match(ip, "(198\.[203\.]*)")), "Medium",
    (action=="file accessed" AND match(ip, "(198\.[203\.]*)")), "Medium",
    (action=="connection attempt" AND match(ip, "(10\.|172\.)")), "Low",
    (action=="login failed"), "Low",
    i==1, "Low"
)
| table _time user ip action threat hour priority
| sort _time

```

98 events (before 8/12/25 7:57:31000 PM) No Event Sampling ▾ Job ▾ II ■ ▾ Smart Mode ▾

| _time | user | ip | action | threat | hour | priority |
|---------------------|---------|---------------|--------------------|-------------------|------|----------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | 04 | Medium |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | 04 | Medium |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | 04 | Low |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | 04 | High |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | 04 | High |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | 04 | Low |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | 04 | Low |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | 04 | Medium |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | 04 | Low |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | 04 | Medium |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | 04 | Low |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | 04 | Low |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | 04 | High |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | 04 | High |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | 04 | Low |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | 04 | Low |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | 04 | Medium |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | 04 | Medium |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | 04 | Low |

10. Timeline of Events

A consolidated incident timeline was created in Splunk to visualize all security events in chronological order, providing clarity on the sequence of malicious activities. This unified view allows analysts to track how each incident unfolded, identify related events, and understand escalation patterns.

The SPL query aggregated logs based on `_time`, `user`, `ip`, `action`, `threat`, and `event_type`, ensuring that every detection type — from malware infections (Trojan, Rootkit, Spyware, Ransomware, Worm) to suspicious logins and connection attempts — is captured in the correct order.

The timeline is especially useful for:

- **Correlating multiple alerts** affecting the same user or system.
- **Identifying the first point of compromise** and subsequent attacker actions.

- Determining dwell time between detection and response.
- Linking related internal and external threats to build an attack narrative.

Below are the visual timelines generated for each major incident type:

1. Spyware Alert Timeline

| _time | user | ip | action | threat | event_type |
|---------------------|-------|---------------|------------------|-----------------|-------------------|
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan Detected |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | alice | 172.16.0.3 | malware detected | Spyware Alert | Spyware Detected |
| 2025-07-03 04:41:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:46:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | login failed | | After-Hours Login |

2. Trojan Alert Timeline

| _time | user | ip | action | threat | event_type |
|---------------------|---------|---------------|--------------------|-----------------|-----------------------------|
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:27:14 | david | 172.16.0.3 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan Detected |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan Detected |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan Detected |
| 2025-07-03 04:29:14 | alice | 192.168.1.101 | malware detected | Trojan Detected | Trojan Detected |

3. Rootkit Alert Timeline

| _time | user | ip | action | threat | event_type |
|---------------------|---------|---------------|--------------------|-------------------|-----------------------------|
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | bob | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 04:18:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | malware detected | Rootkit Signature | RootKit Detected |
| 2025-07-03 04:19:14 | david | 10.0.0.5 | connection attempt | | Internal Connection Attempt |
| 2025-07-03 04:23:14 | bob | 172.16.0.3 | login failed | | After-Hours Login |
| 2025-07-03 04:23:14 | charlie | 198.51.100.42 | login failed | | After-Hours Login |

4. Worm Infection Timeline

| _time | user | ip | action | threat | event_type |
|---------------------|-------|---------------|------------------|------------------------|-------------------------|
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 04:53:14 | david | 203.0.113.77 | login success | | After-Hours Login |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | | After-Hours Login |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | | After-Hours Login |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | | After-Hours Login |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | | After-Hours Login |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | | After-Hours Login |
| 2025-07-03 05:04:14 | bob | 192.168.1.101 | login success | | After-Hours Login |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection Detected |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection Detected |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection Detected |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection Detected |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection Detected |
| 2025-07-03 05:06:14 | bob | 203.0.113.77 | malware detected | Worm Infection Attempt | Worm Infection Detected |
| 2025-07-03 05:12:14 | alice | 198.51.100.42 | login success | | After-Hours Login |
| 2025-07-03 05:12:14 | alice | 198.51.100.42 | login success | | After-Hours Login |

5. Ransomware Timeline

11. Impact Assessment

This section evaluates the potential business, operational, and security consequences of each detected alert type. The assessment considers the scope of compromise, data sensitivity, possible persistence mechanisms, and potential for lateral movement or further exploitation.

1. After-Hours Login

Impact:

- Increased risk of compromised credentials being used when monitoring is minimal.
- Potential entry point for lateral movement and privilege escalation.
- May indicate insider threat or unauthorized external access.

2. Internal & External Connection Attempts

Impact:

- **External Attempts:** Could be reconnaissance or brute-force attacks from threat actors attempting to breach the network perimeter.
- **Internal Attempts:** May indicate unauthorized pivoting between internal systems, possibly post-compromise.
- Could enable attackers to locate sensitive resources or spread malware.

3. Ransomware Behavior

Impact:

- High risk of data encryption and operational disruption.
- Potential permanent loss of critical business data if backups are not available.
- Can trigger regulatory reporting obligations (e.g., GDPR, HIPAA) due to data unavailability and confidentiality breaches.

4. Rootkit Detected

Impact:

- Persistent and stealthy compromise allowing attackers to maintain long-term access.
- Ability to hide malicious processes, making detection and eradication difficult.

- Can disable security tools and log collection, impacting incident response capabilities.

5. Trojan Detected

Impact:

- May provide remote control to attackers for data theft, credential harvesting, or launching additional malware.
- Can act as a dropper for more dangerous payloads such as ransomware or spyware.
- May compromise multiple systems in a short time if undetected.

6. Spyware Alert

Impact:

- High risk of confidential data exfiltration, including credentials, emails, and business-sensitive documents.
- Long-term surveillance may lead to strategic data loss and business intelligence leakage.
- Could facilitate future targeted attacks.

7. Worm Infection Detected

Impact:

- Self-propagating malware can rapidly spread across the network, disrupting operations.
- Can consume bandwidth and system resources, leading to service degradation.
- May be used as a vector to deliver other malware such as ransomware or Trojans.

12. Remediation & Containment Actions

This section outlines the immediate containment measures and long-term remediation strategies for each detected threat, aimed at preventing further damage and reducing the likelihood of recurrence.

1. After-Hours Login

Containment:

- Immediately validate the legitimacy of the login with the associated user.

- Temporarily disable suspicious accounts until confirmed safe.

Remediation:

- Enforce MFA for all remote and high-privilege accounts.
- Implement geolocation and time-based access restrictions.

2. Internal & External Connection Attempts

Containment:

- Block identified malicious IPs at the firewall and intrusion prevention systems.
- Isolate affected internal systems from the network.

Remediation:

- Review and tighten internal segmentation policies.
- Deploy network anomaly detection to flag abnormal traffic patterns.

3. Ransomware Behavior

Containment:

- Immediately isolate infected systems from the network.
- Disable shared drives and halt automated backup processes to prevent encryption of backups.

Remediation:

- Restore from clean, offline backups after eradication.
- Conduct organization-wide patching and ransomware awareness training.

4. Rootkit Detected

Containment:

- Quarantine and remove the infected system from the production environment.
- Switch to trusted boot media for forensic analysis.

Remediation:

- Reinstall OS from trusted sources, as rootkits are difficult to remove completely.
- Implement kernel-level monitoring solutions.

5. Trojan Detected

Containment:

- Block C2 (Command & Control) communications via firewall/IDS rules.

- Revoke potentially compromised credentials.

Remediation:

- Perform a full malware scan and remove associated artifacts.
- Patch vulnerabilities exploited for Trojan delivery.

6. Spyware Alert

Containment:

- Terminate suspicious processes and disconnect the system from the internet.
- Identify and revoke any stolen credentials.

Remediation:

- Conduct a full scan for persistence mechanisms.
- Implement Data Loss Prevention (DLP) controls.

7. Worm Infection Detected

Containment:

- Isolate all affected systems immediately.
- Temporarily disable network shares and removable media usage.

Remediation:

- Patch vulnerabilities that enabled the worm's spread.
- Deploy endpoint protection with behavior-based detection.

13. Result and Conclusion

The incident investigation successfully identified and categorized multiple security threats within the monitored environment, including malware infections (Trojan, Rootkit, Spyware, Worm), ransomware behavior, unauthorized after-hours logins, and suspicious internal/external connection attempts.

Through SIEM analysis in Splunk, each alert was correlated with associated user activity, IP addresses, and timestamps, producing a detailed timeline of events for forensic review. The classification into **High, Medium, and Low severity** allowed for prioritizing remediation efforts effectively.

Containment measures were executed promptly, including system isolation, account suspension, and network blocking, to prevent further compromise. Long-term remediation

strategies such as enforcing multi-factor authentication, network segmentation, and endpoint hardening have been recommended to improve resilience.

Overall, the incident response process demonstrated that proactive monitoring and rapid containment significantly reduced potential damage. Continuous improvements in detection rules, user awareness training, and security policy enforcement will further strengthen the organization's defense against future threats.