Incident Response Report

Internship Report Submission – Future Interns

Prepared by: M Fathima Jemina

Date: August 2025

Table of Contents

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

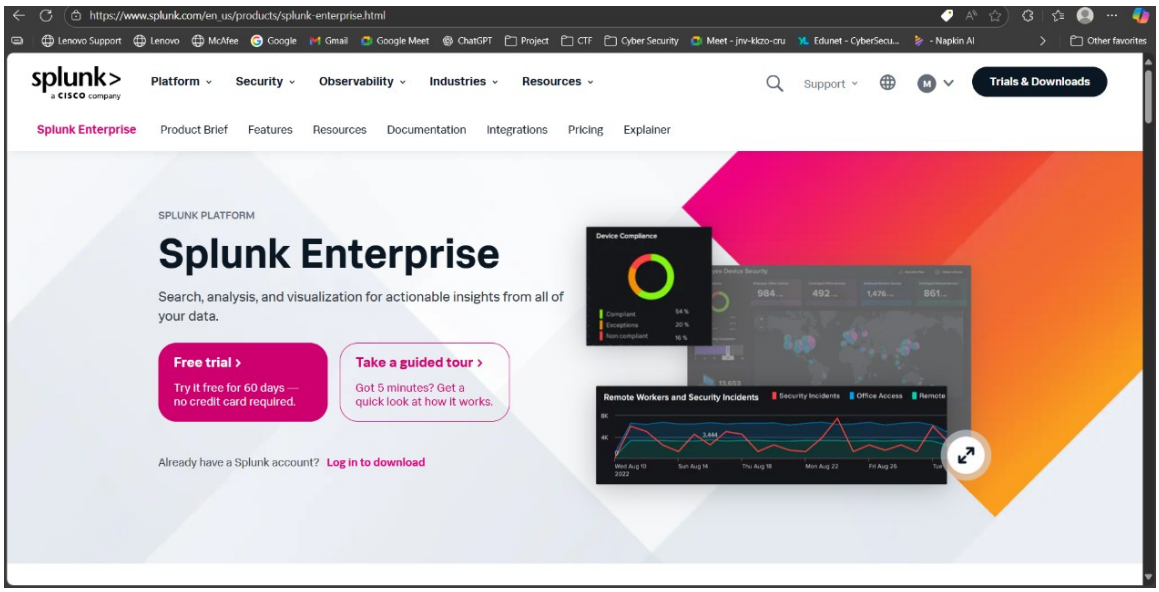
- Splunk Enterprise (Free Trial) – SIEM platform for log ingestion, search, and dashboarding.
- Google Docs / Microsoft Word – For report preparation.

6. SIEM Setup

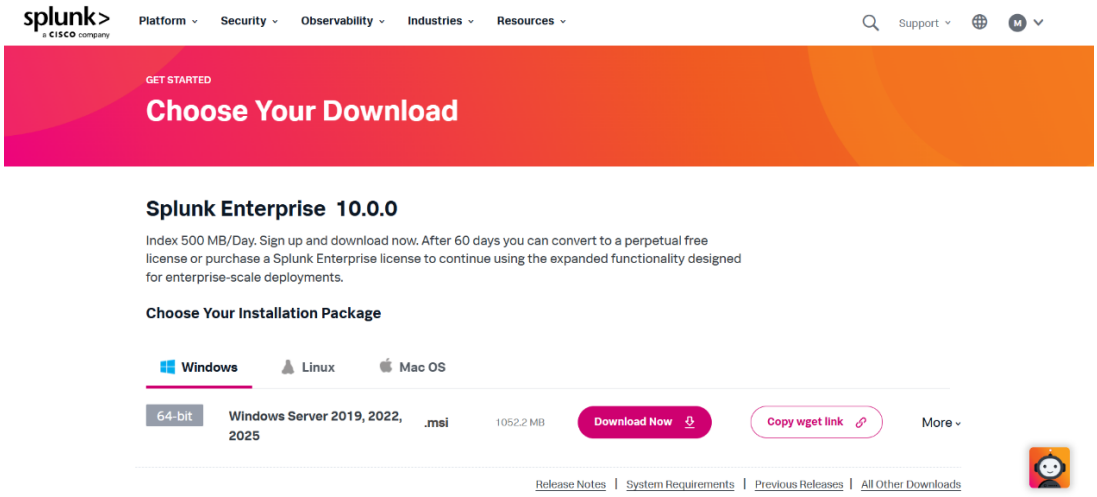
Splunk Enterprise (Free Trial) was installed, configured, and used to ingest the provided SOC log dataset. Custom field extractions and SPL queries were created to detect, classify, and visualize security events.

6.1 Download and Install

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



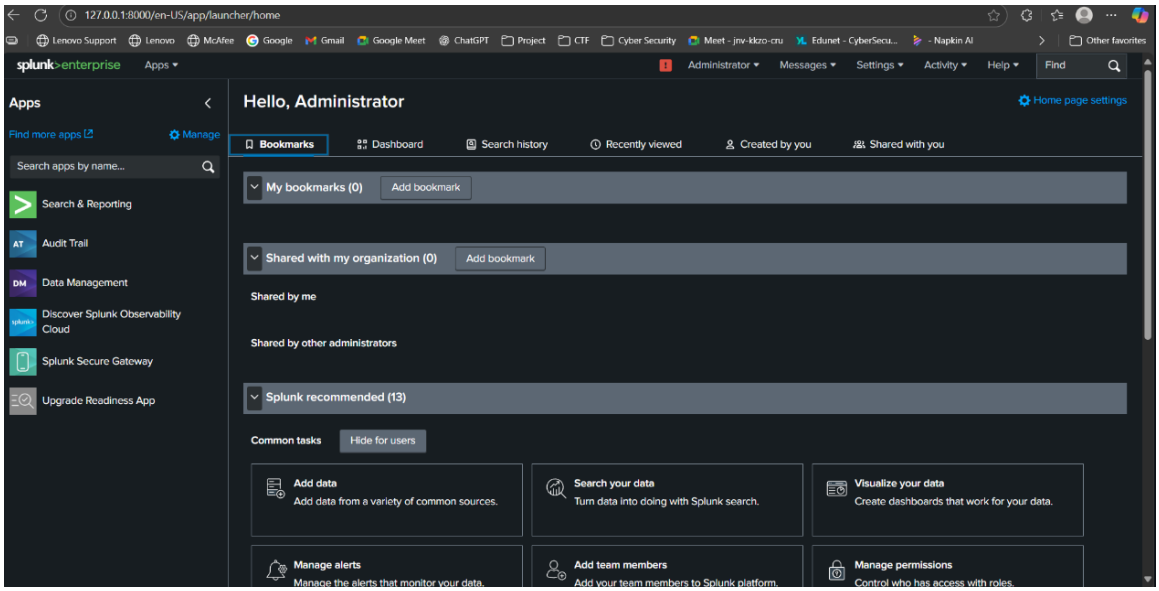
2. Navigate to **Products → Splunk Enterprise**
3. Click **Free Trial** and choose your OS (Windows, Linux, or macOS)
4. Create a free Splunk account (if not already registered)
5. Download the installer



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

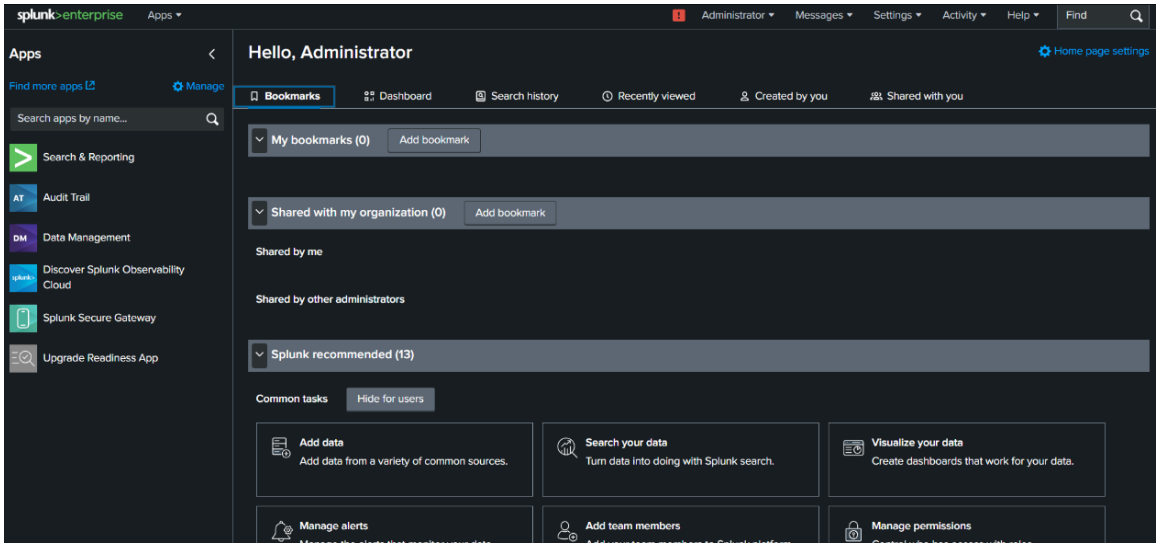
Open your browser and go to: http://localhost:8000



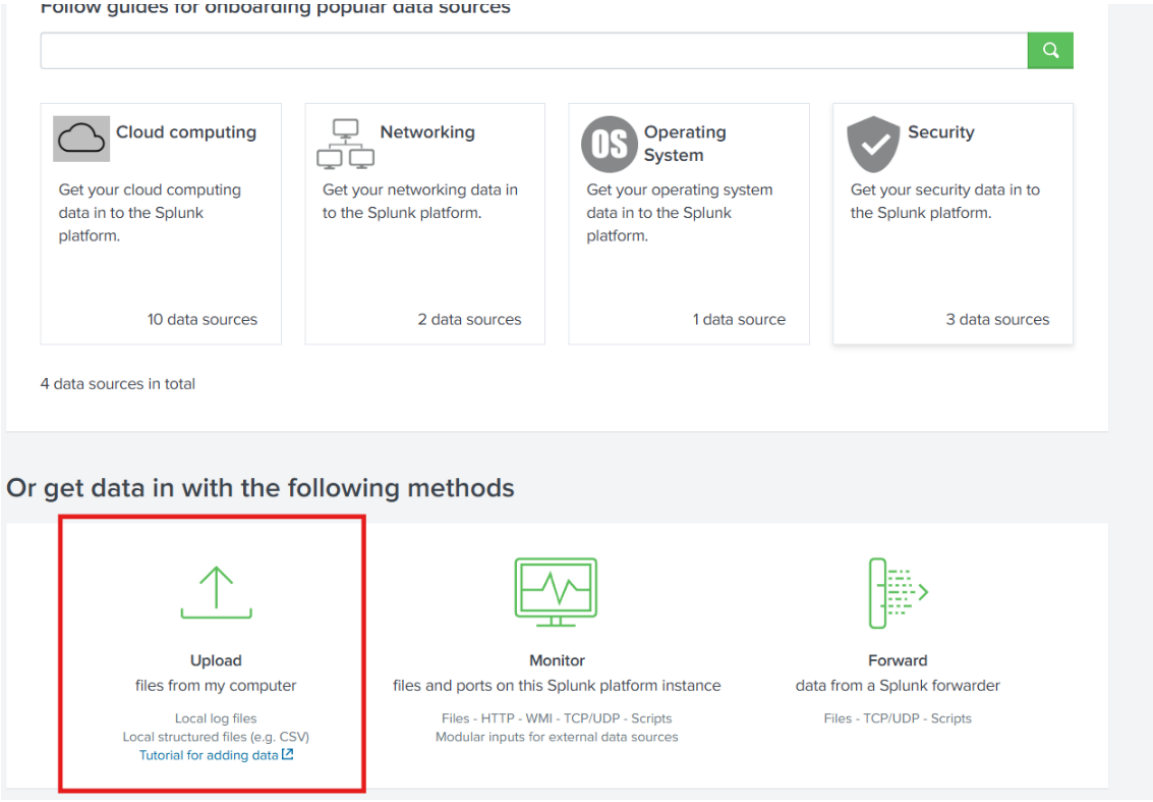
- Log in with the **admin credentials** you created during installation.
- You should now see the Splunk **Home Dashboard**.

6.3 Import Data

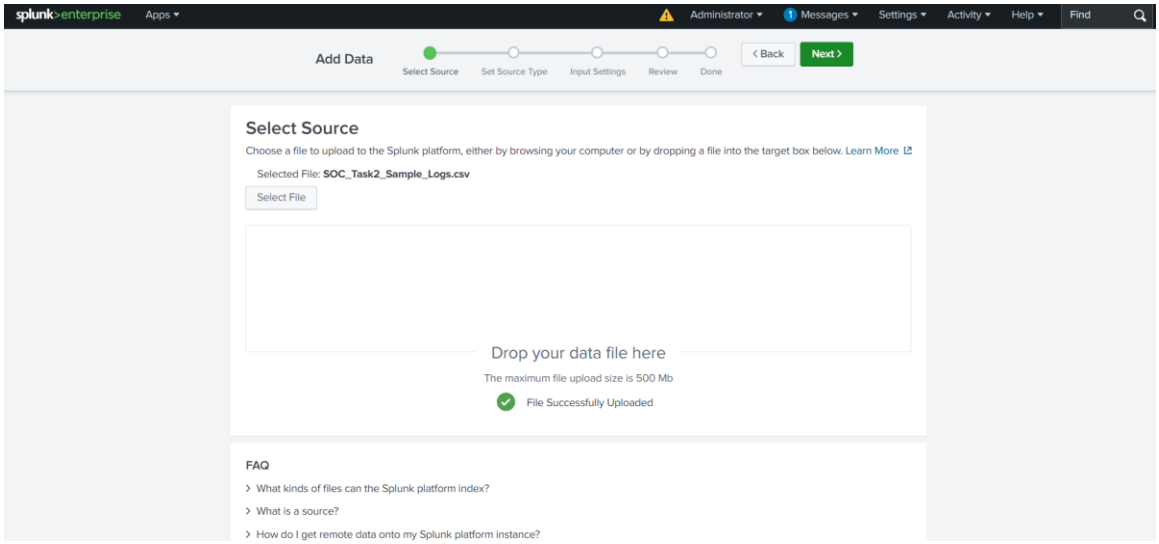
1. From the Splunk Home page, click Settings → Add Data



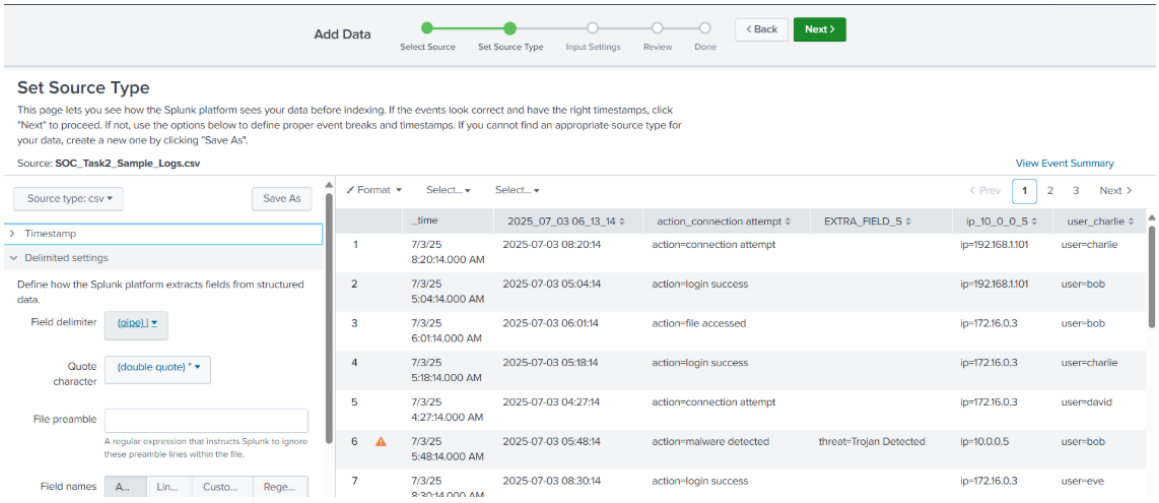
2. Choose **Upload**



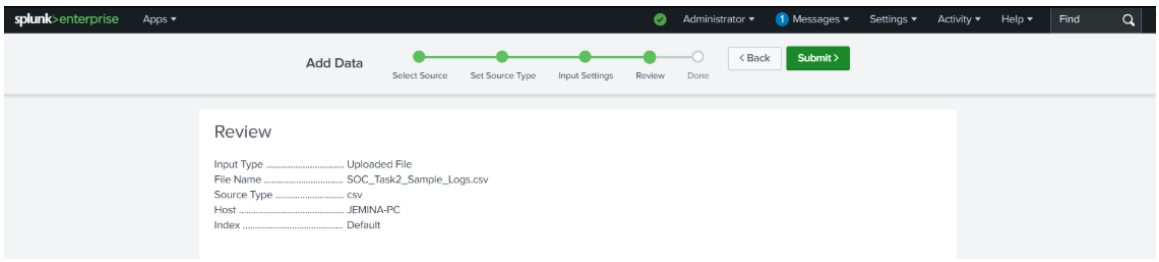
3. Browse and select SOC_Task2_Sample_Logs.csv



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



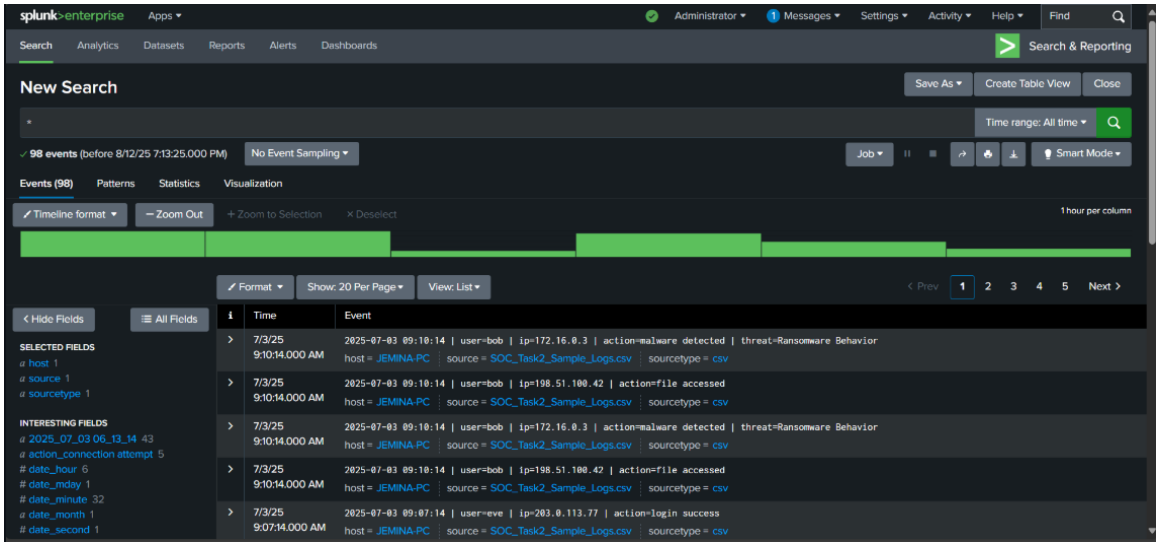
5. Click **Review → Submit** to finish import



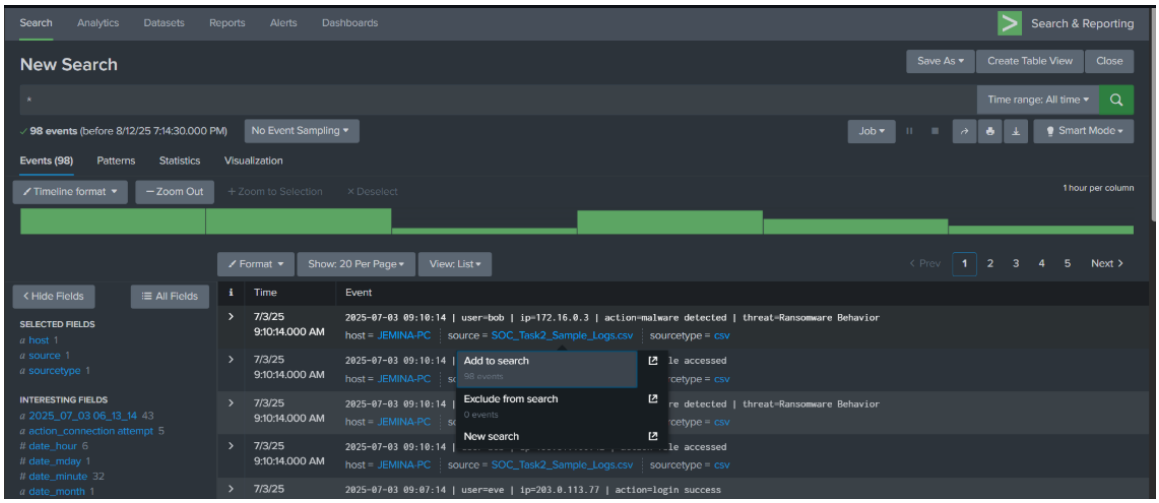
6.4 Create Field Extractions

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

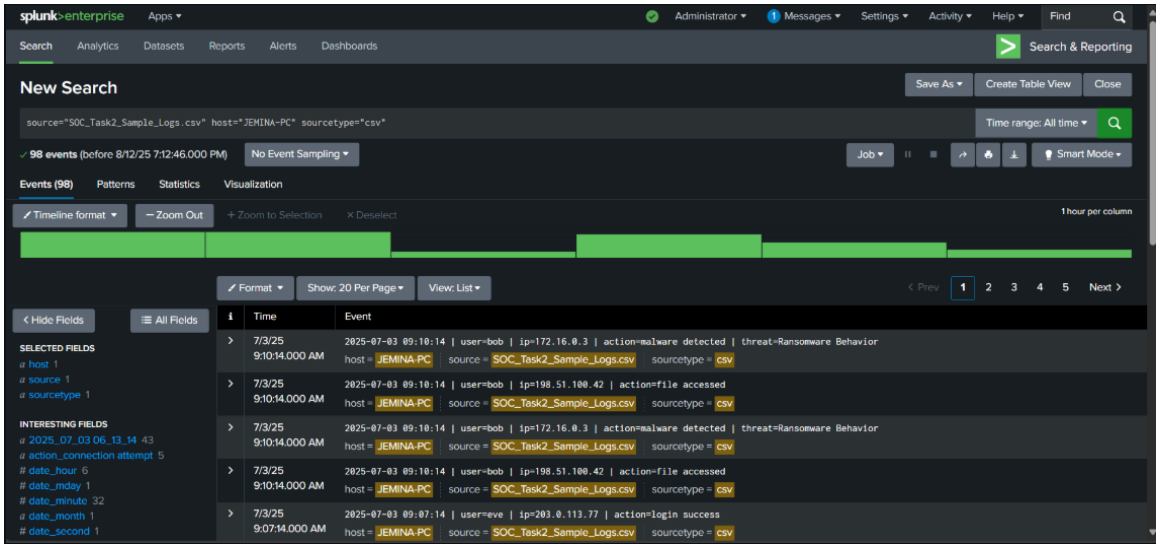
* - It is used to return all the data from all available logs



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



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.

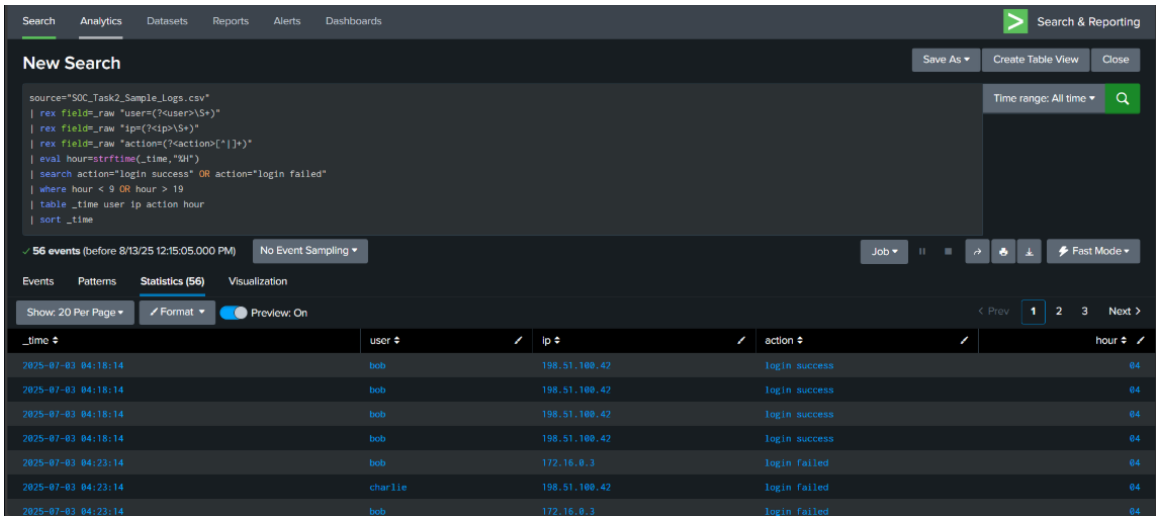
Why It Matters

- 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

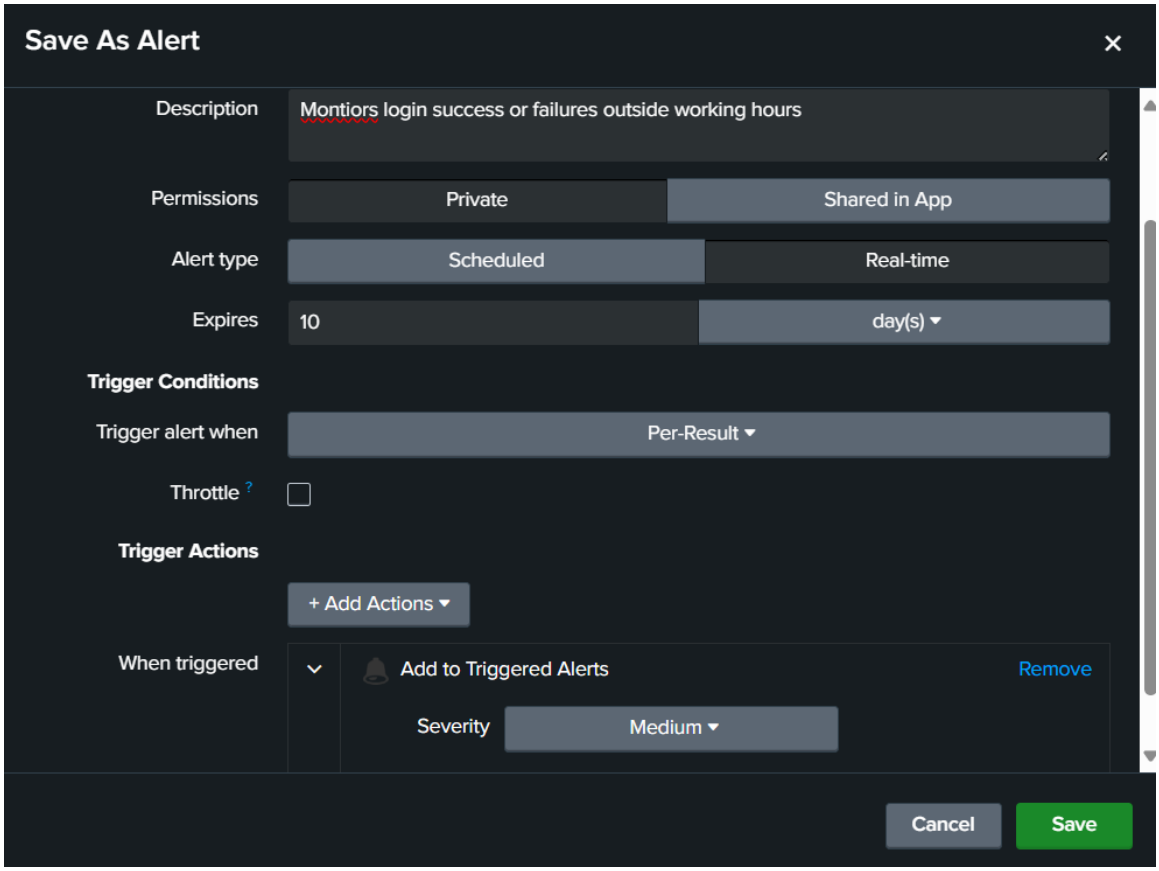
- **Medium** – For isolated after-hours logins.
- **High** – If linked with malicious activity such as file access anomalies or malware alerts.

Detection of After Hour Login in Splunk:



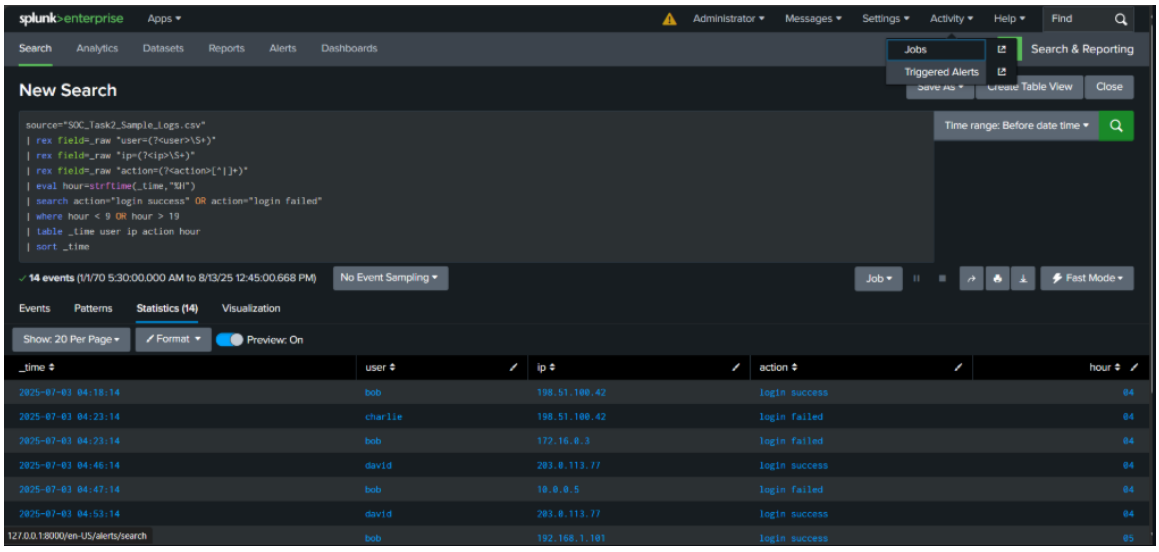
Setting Alerts for After Hour Login:

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.

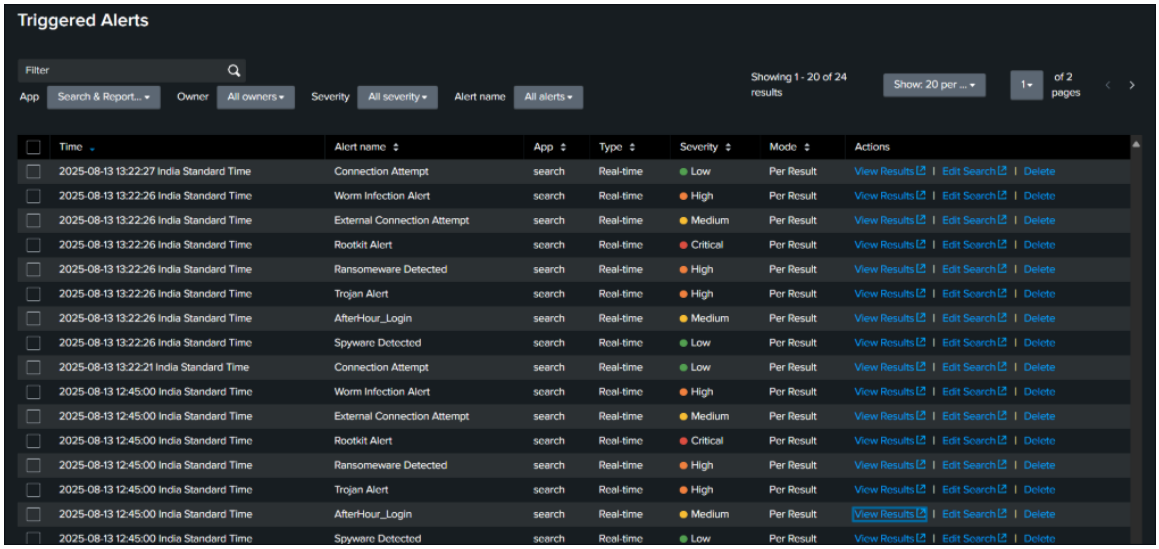


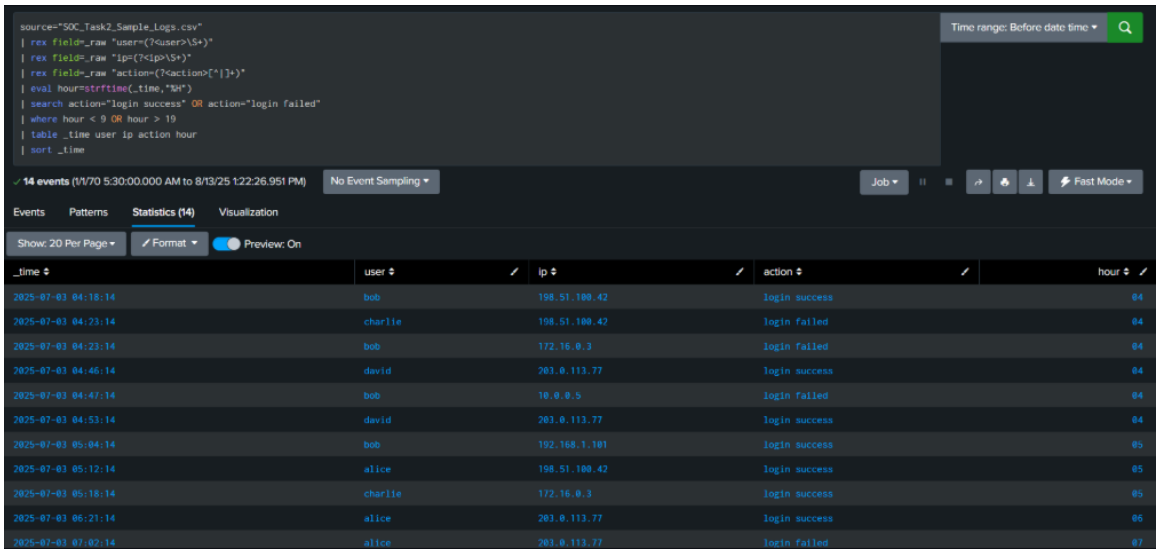
Viewing Alerts in Splunk

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



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





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

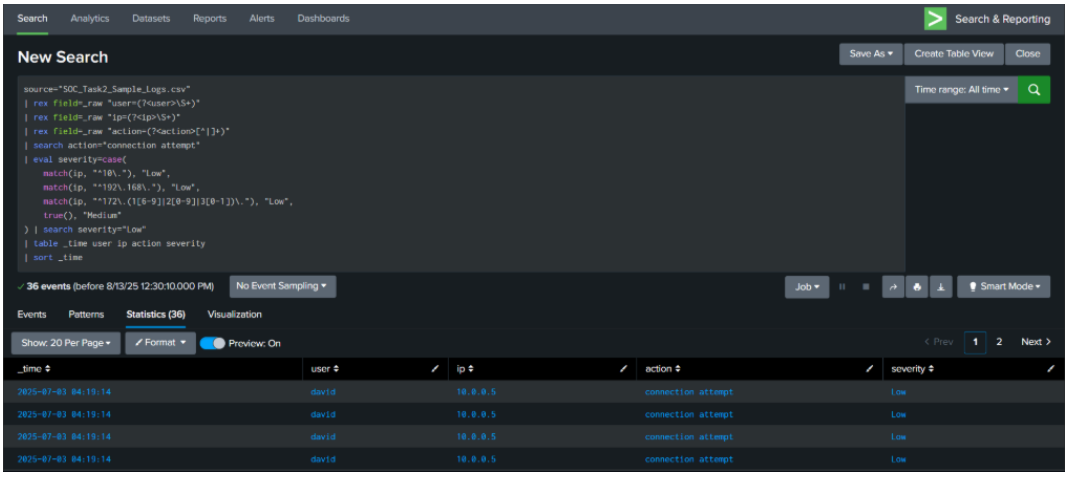
- **Internal Connection Attempts** – May reveal lateral movement or unauthorized access to internal systems.
- **External Connection Attempts** – Could indicate targeted attacks, brute force attempts, or scanning from unknown entities.

Severity

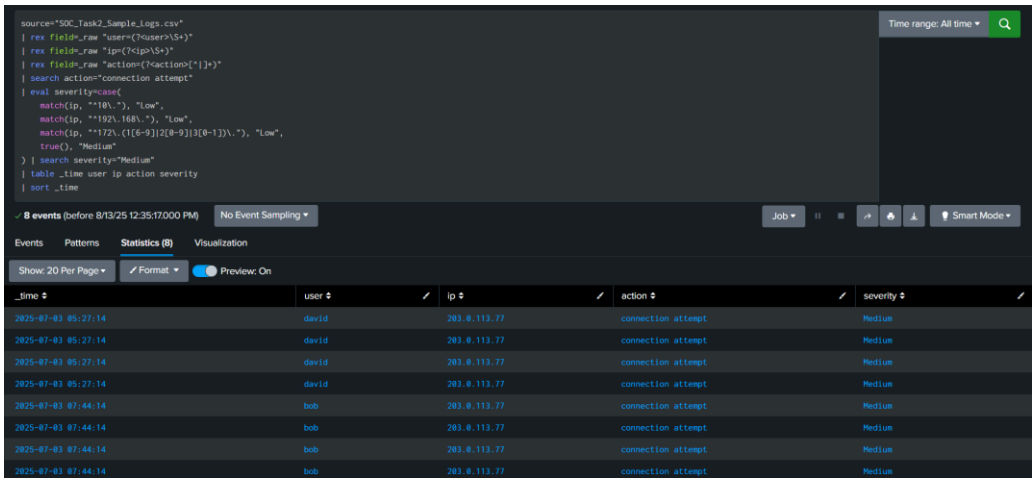
- **Low** – Internal connection attempts from private IP ranges (10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x).
- **Medium** – External connection attempts from public IP addresses.

Detection of event in Splunk:

Internal Connection Attempt:



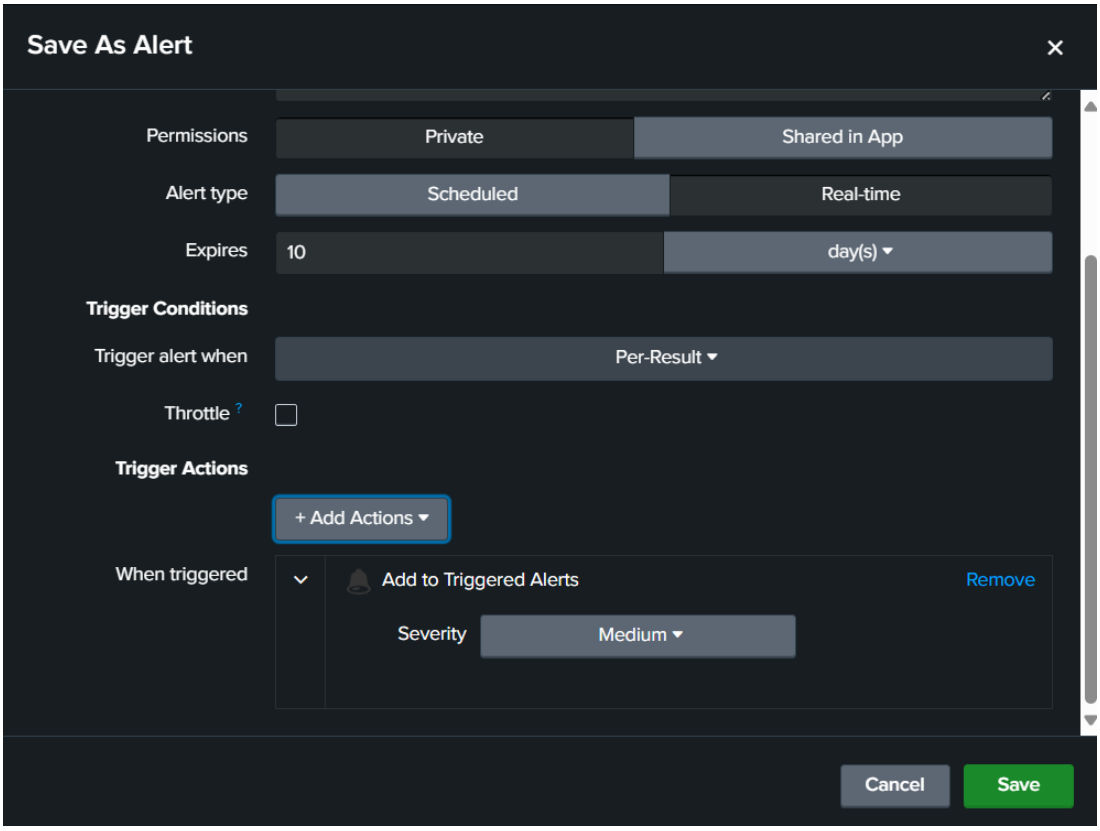
External Connection Attempt:



Set Alert to Monitor Connection Attempt:

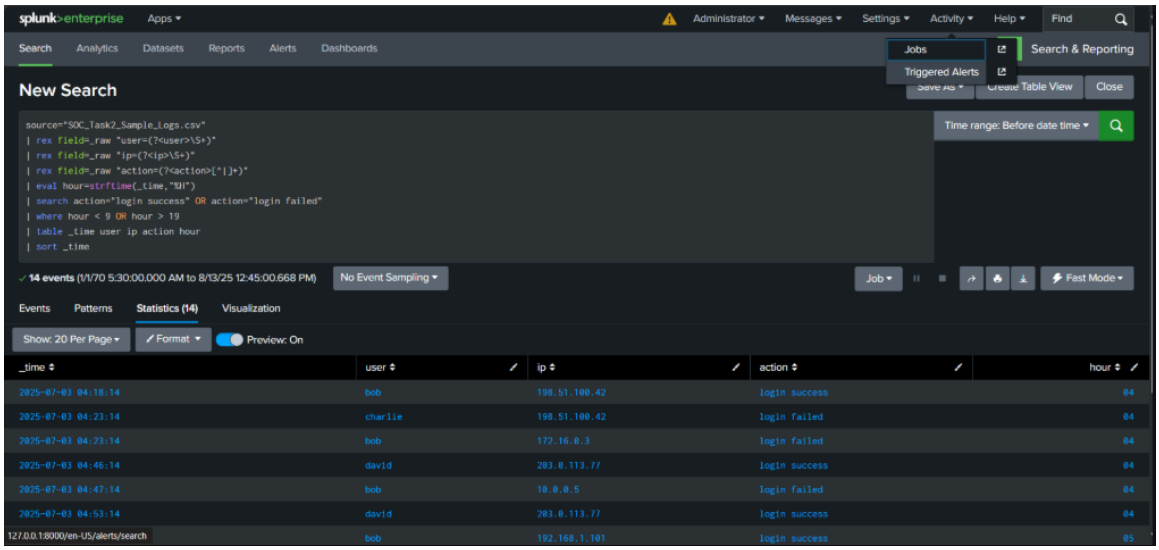
To set alert for the following event, click on the "Save as" drop down, select "Alert". It will open the Alert window, fill in the details and click save. Future events which have unusual logins will be viewed in the "Triggered Alerts" as you have saved it.

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

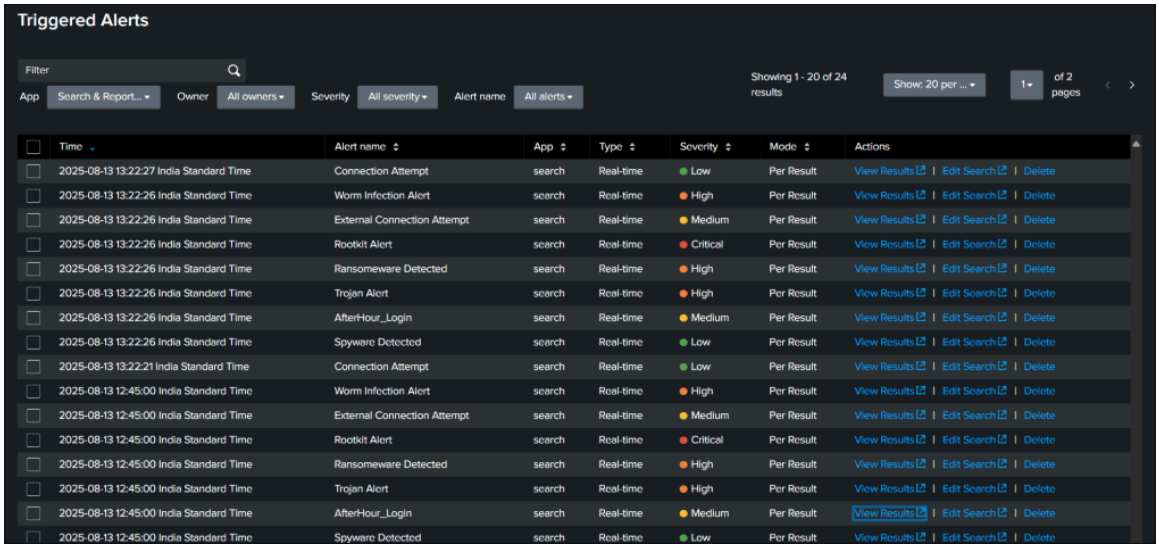


Viewing Alerts in Splunk

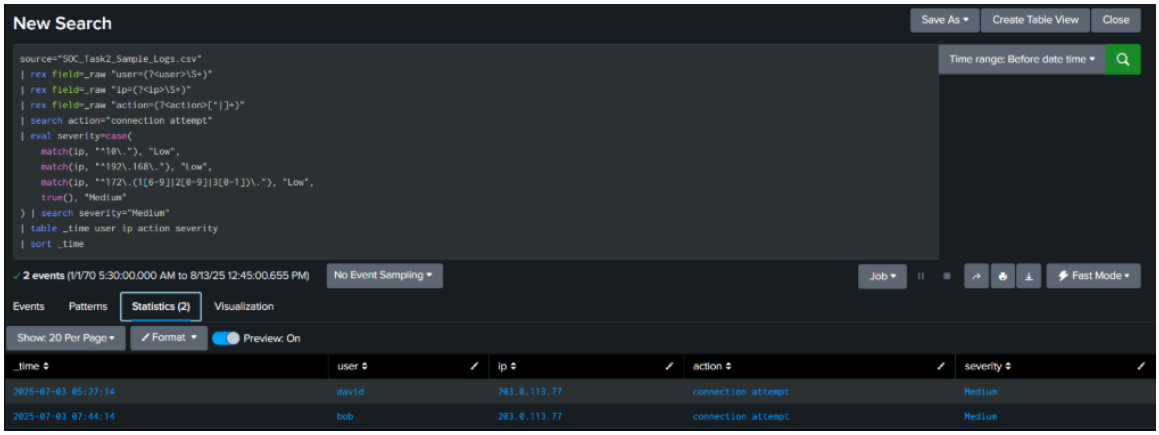
1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.



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



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



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.

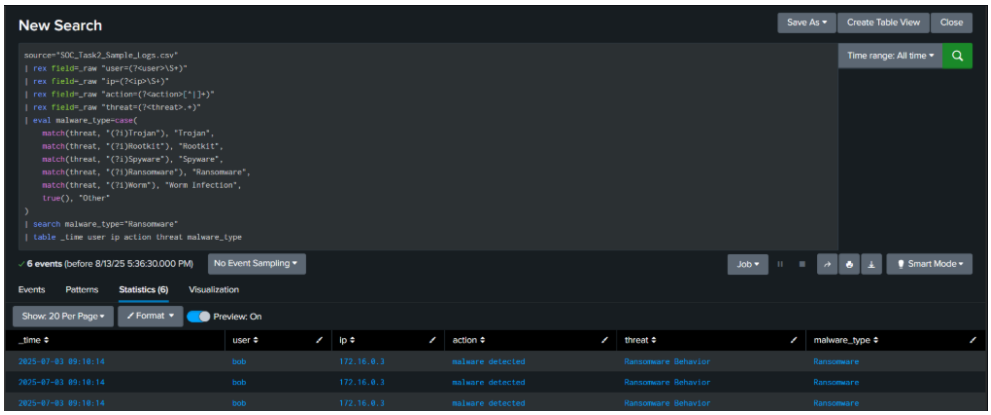
Why It Matters

- 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

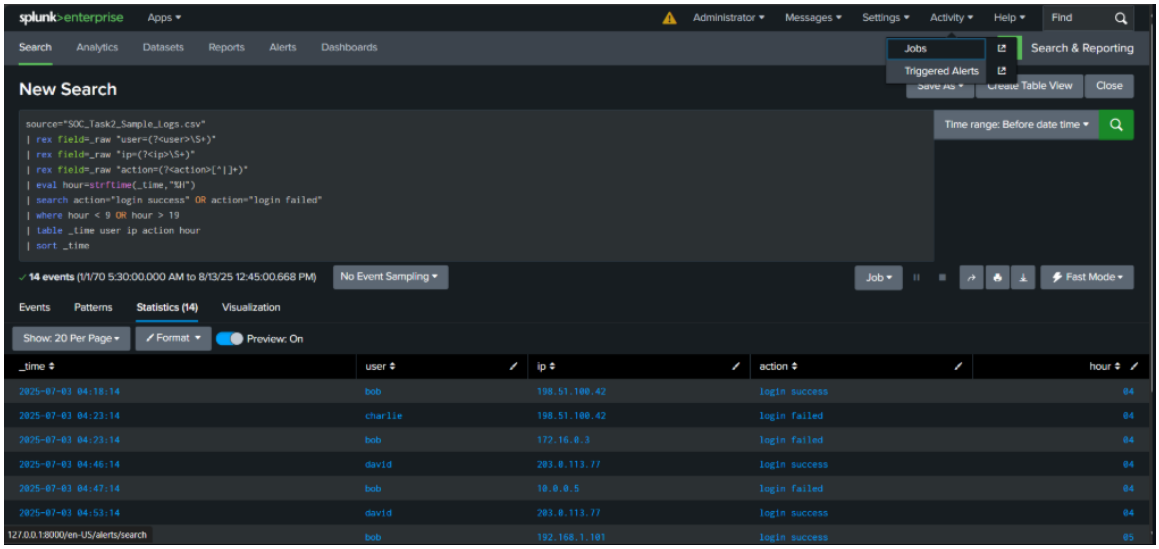
High – Any ransomware detection should be treated as a critical incident.

Detecting in Splunk Search:

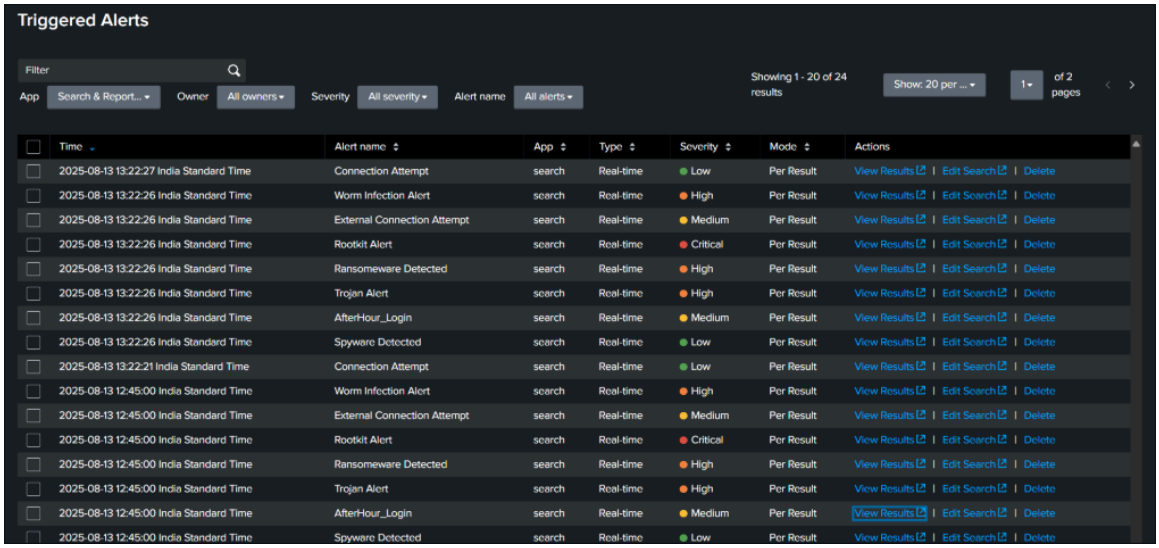


Viewing Alerts in Splunk

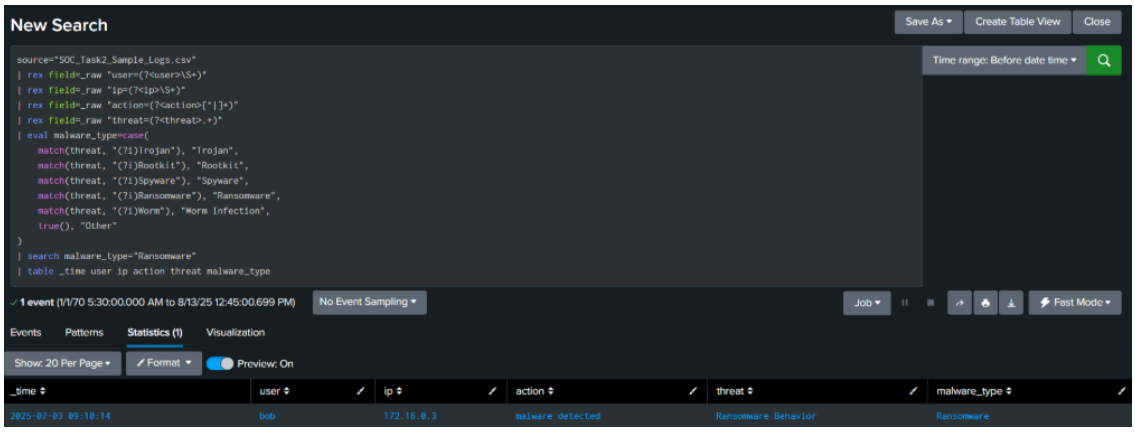
1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.



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



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



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.

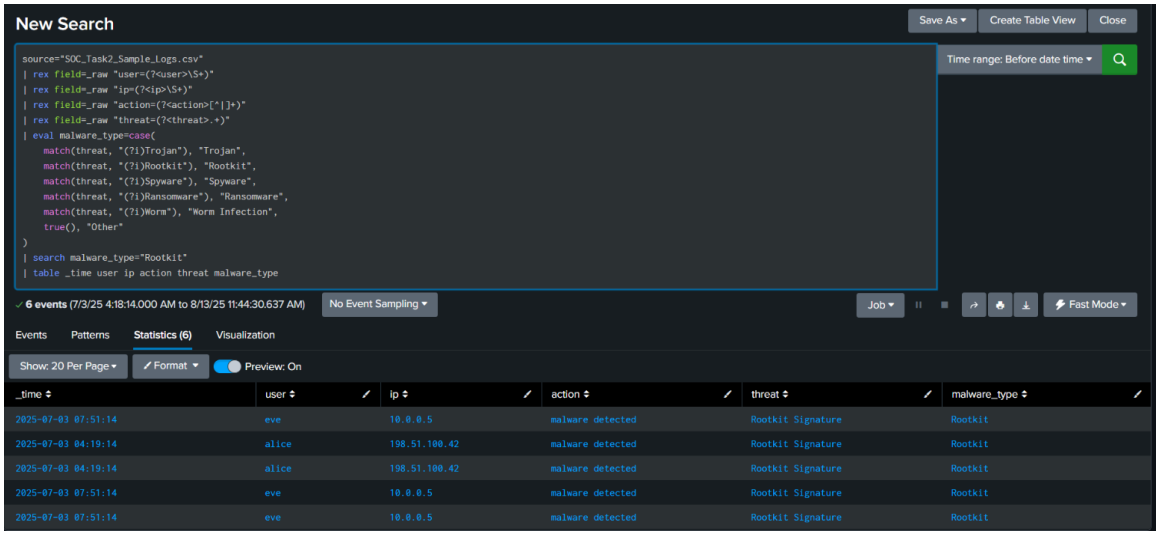
Why It Matters

- 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

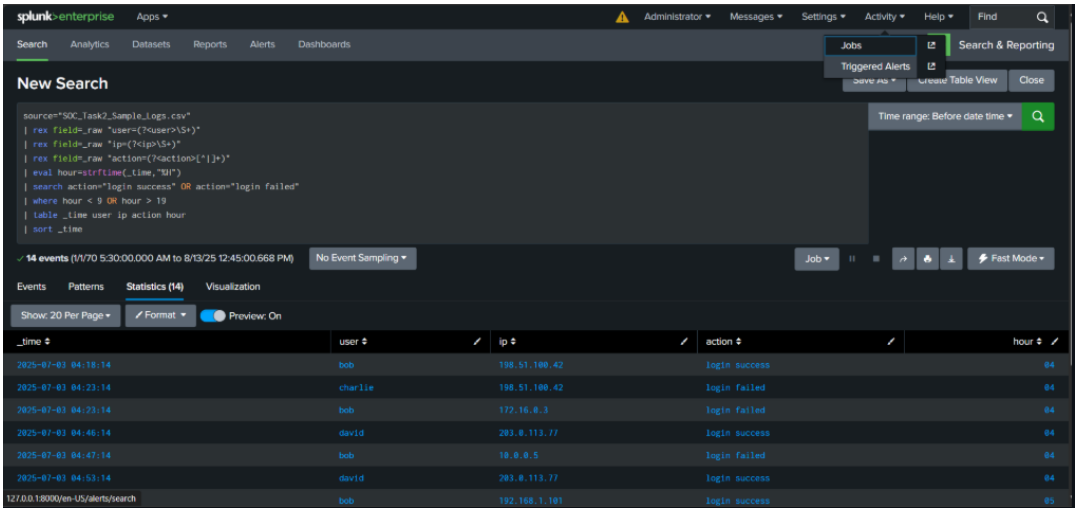
- **Critical** – Any rootkit detection should be treated as a critical security incident.

Detecting in Splunk Search:

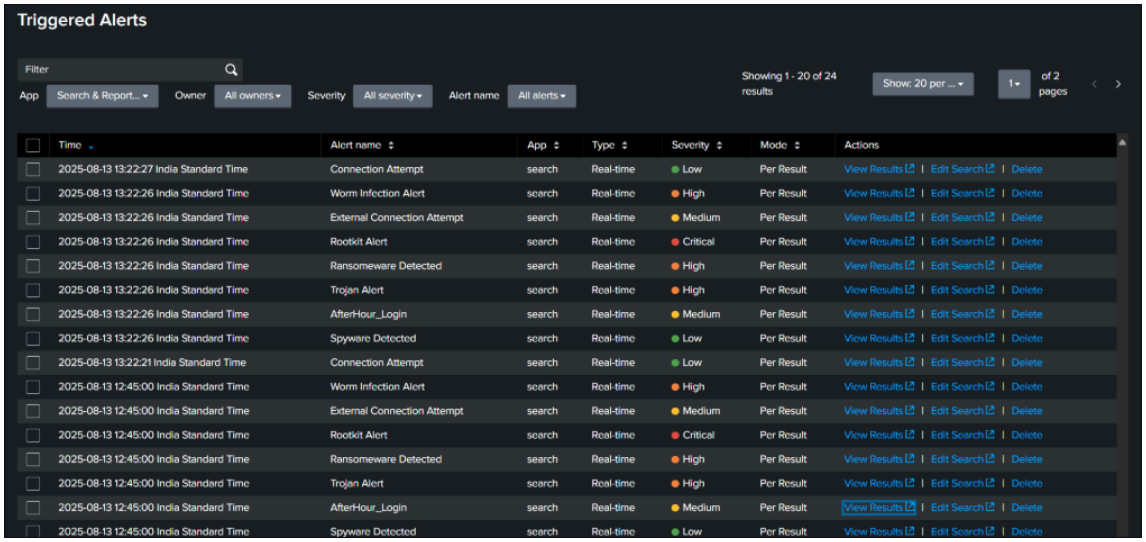


Viewing Alerts in Splunk

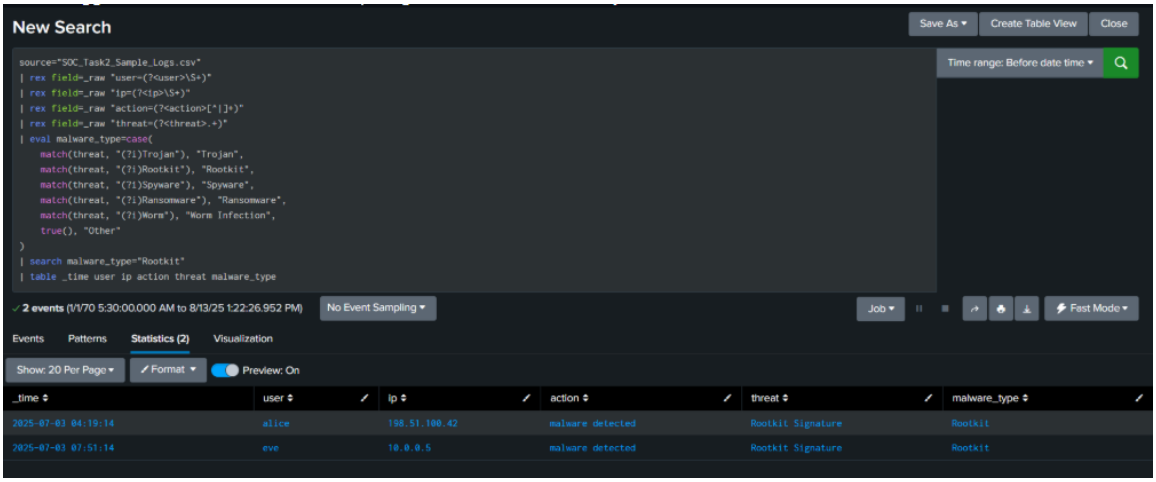
1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.



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



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



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.

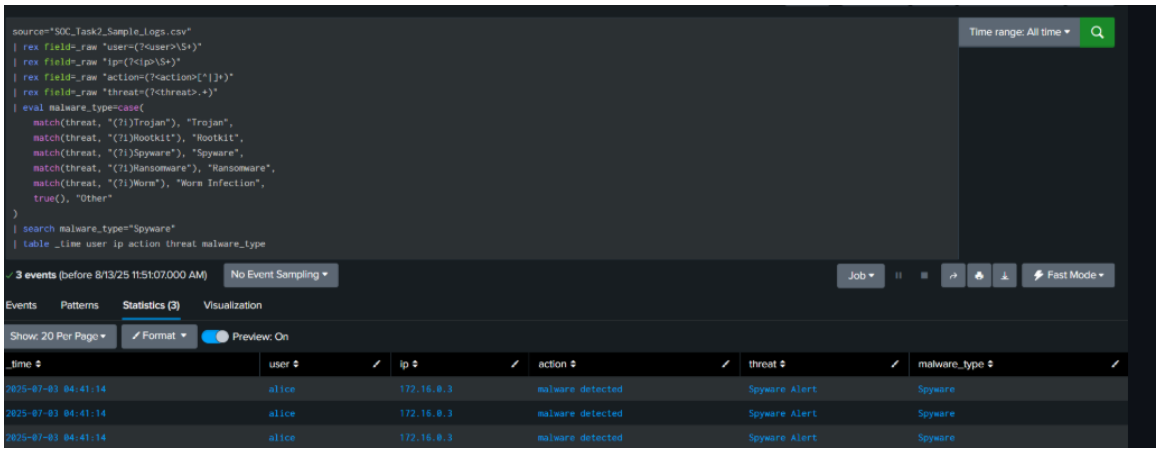
Why It Matters

- 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

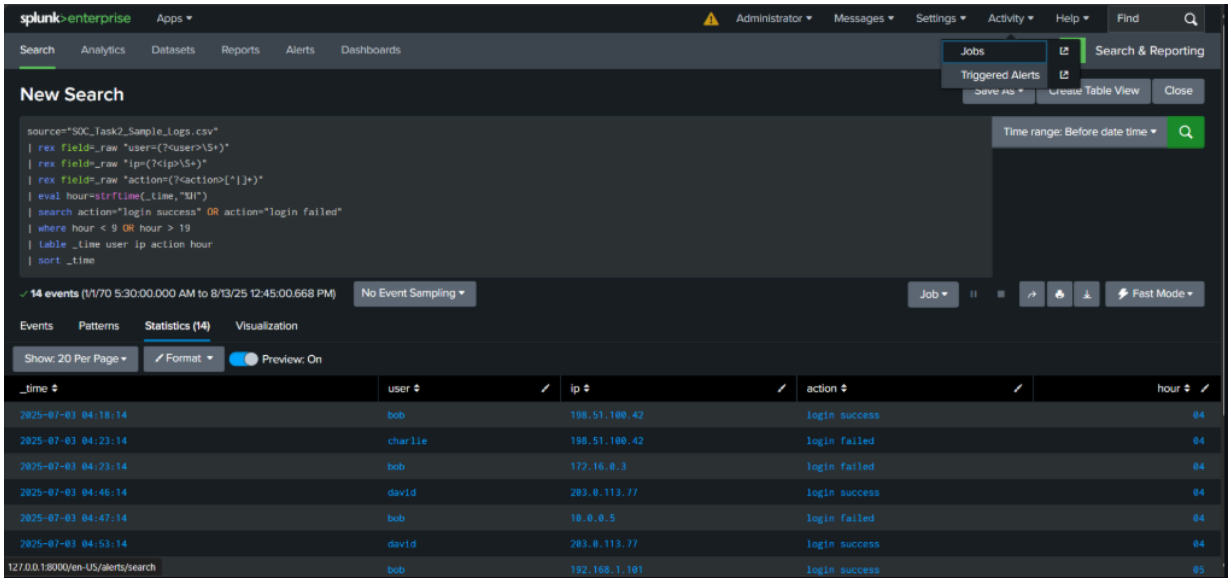
- **High** – Any spyware detection should be treated as a critical incident due to its data theft potential.

Detecting in Splunk Search:

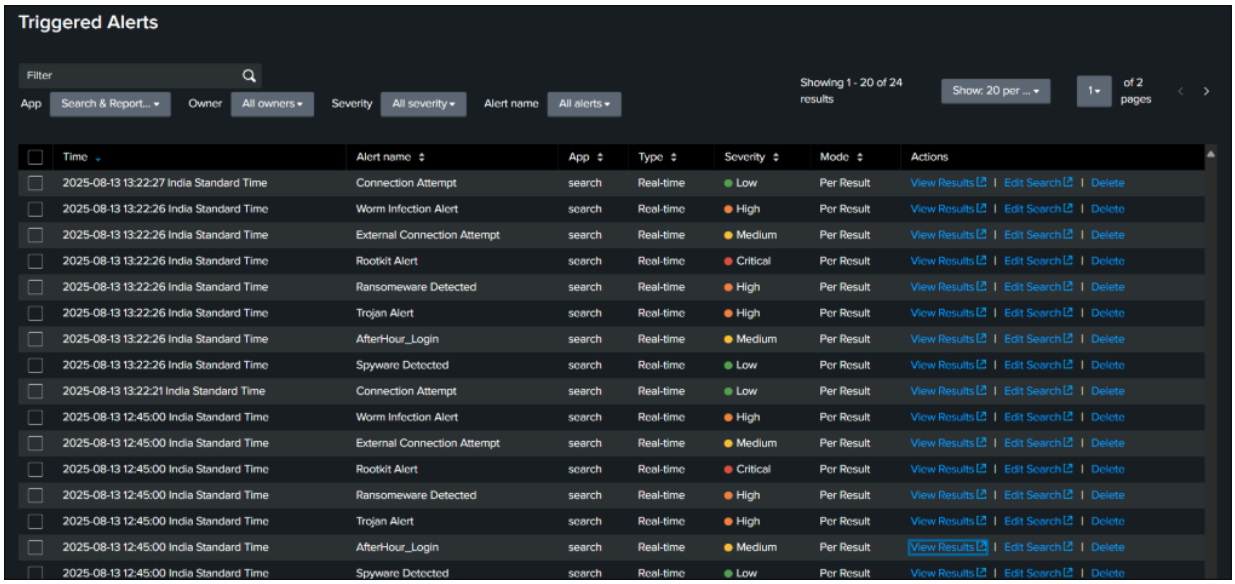


Viewing Alerts in Splunk

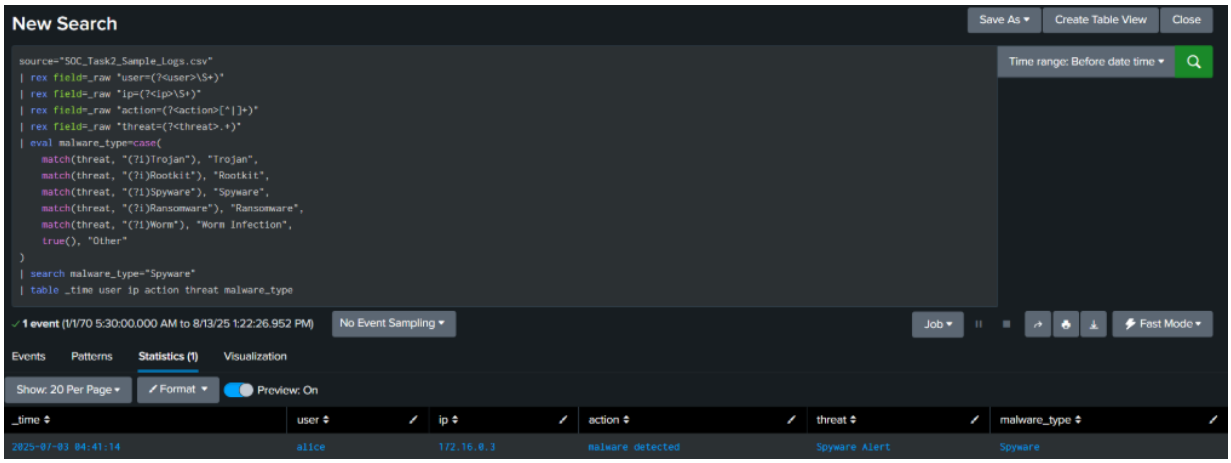
1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.



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



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



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.

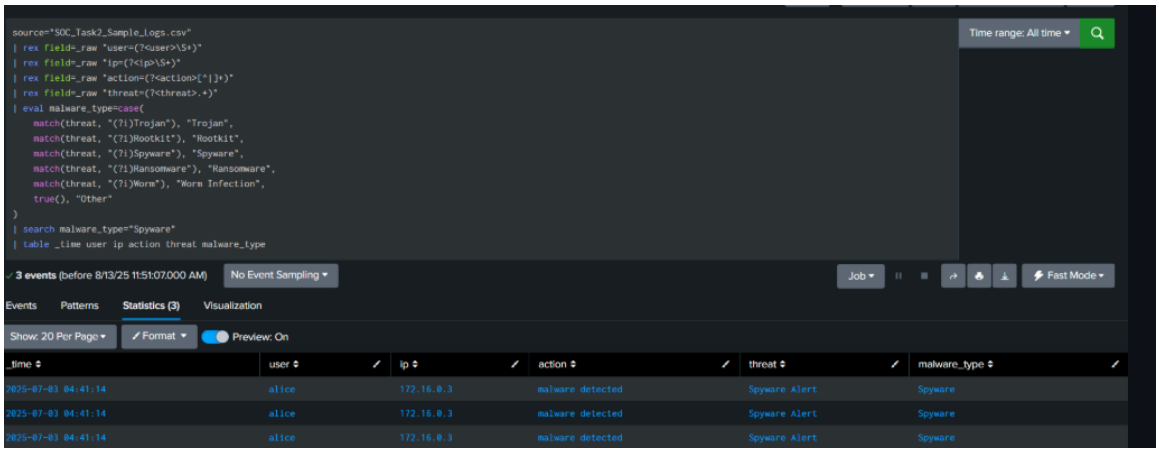
Why It Matters

- 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

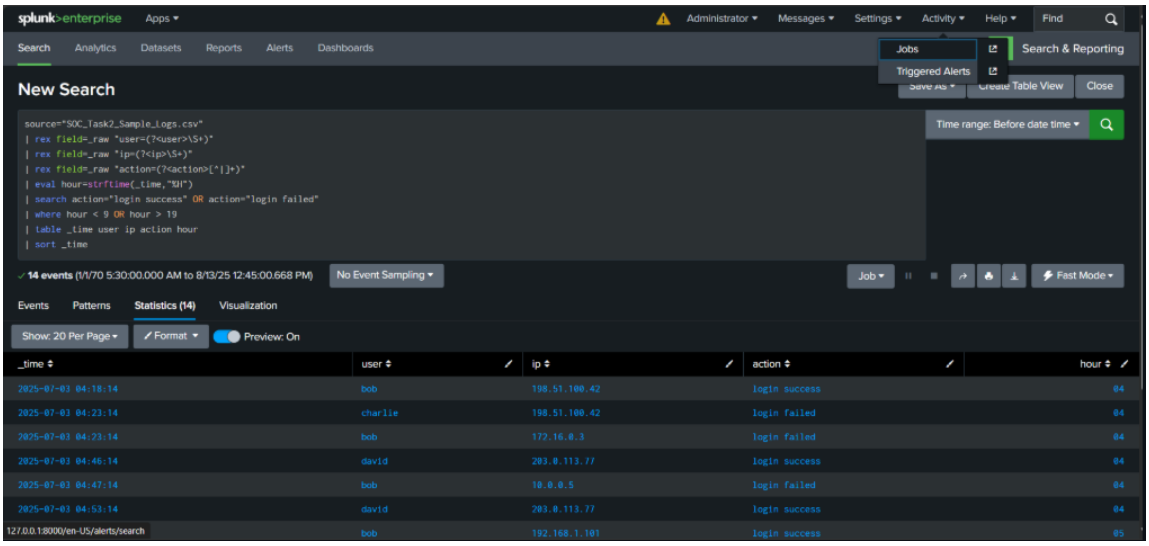
- **High** – Trojans pose a significant risk to system integrity and data security.

Detecting in Splunk Search:

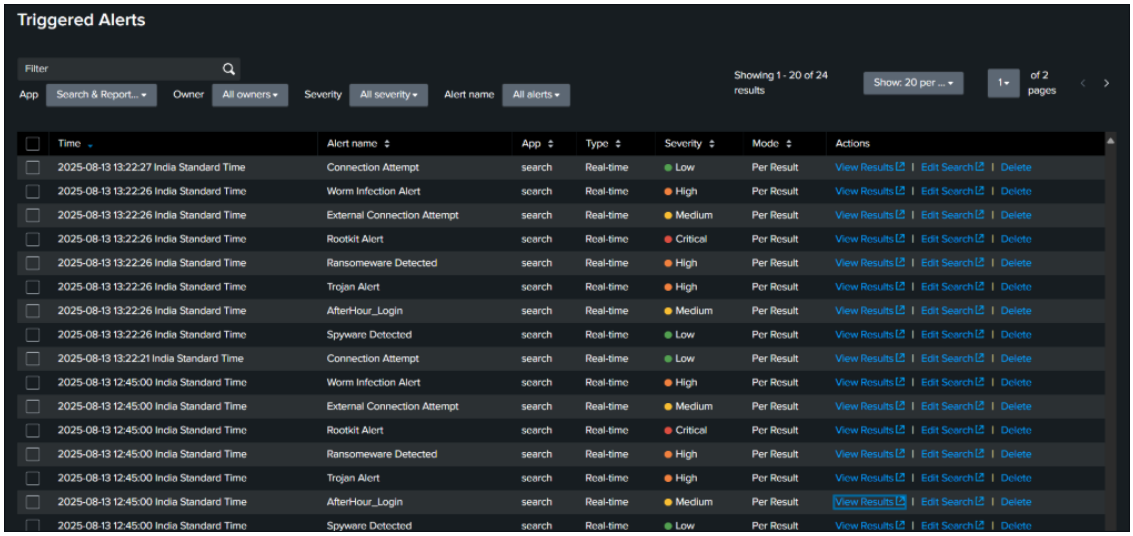


Viewing Alerts in Splunk

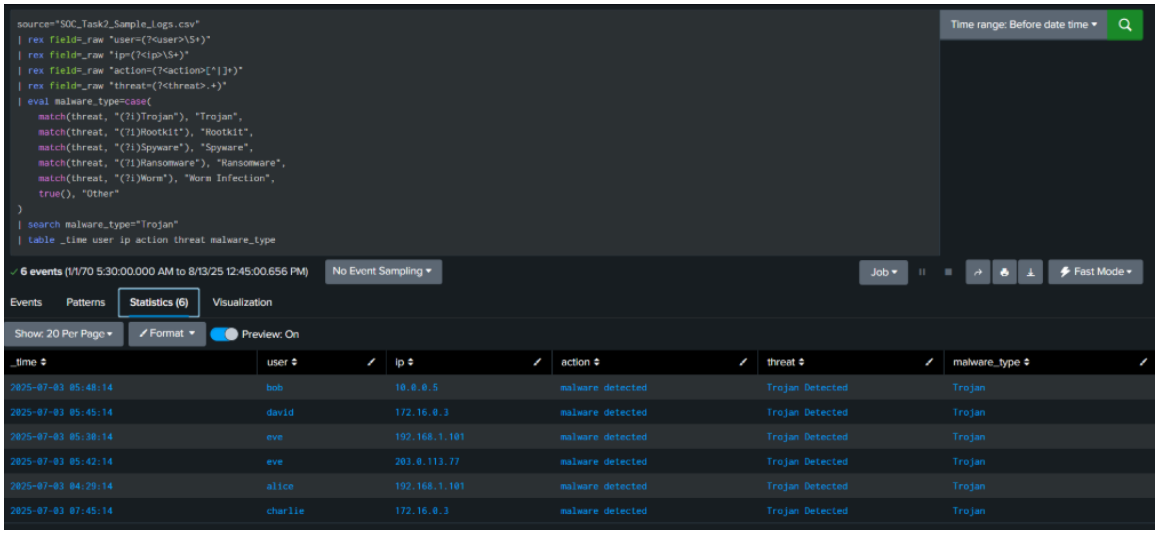
1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.



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



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



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.

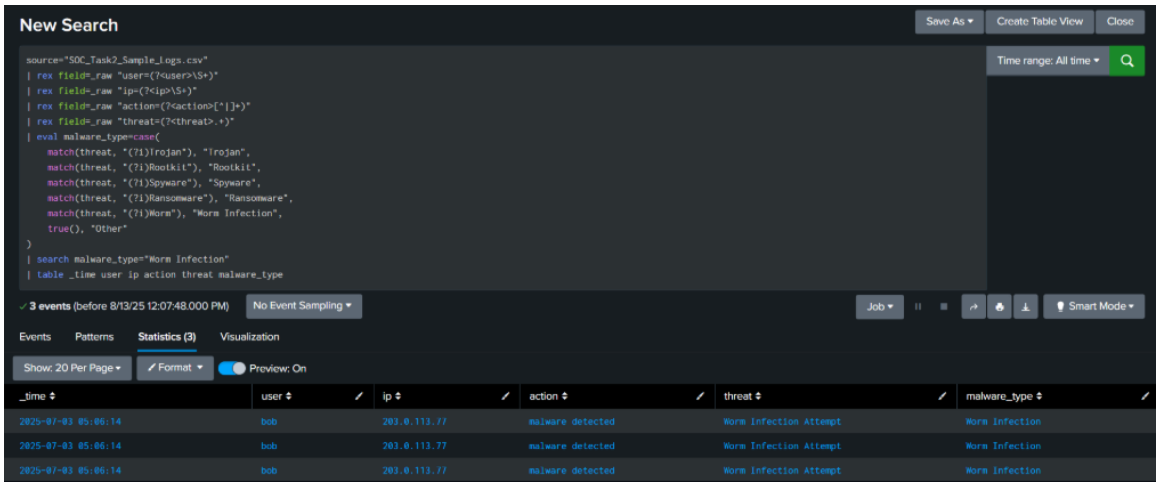
Why It Matters

- 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

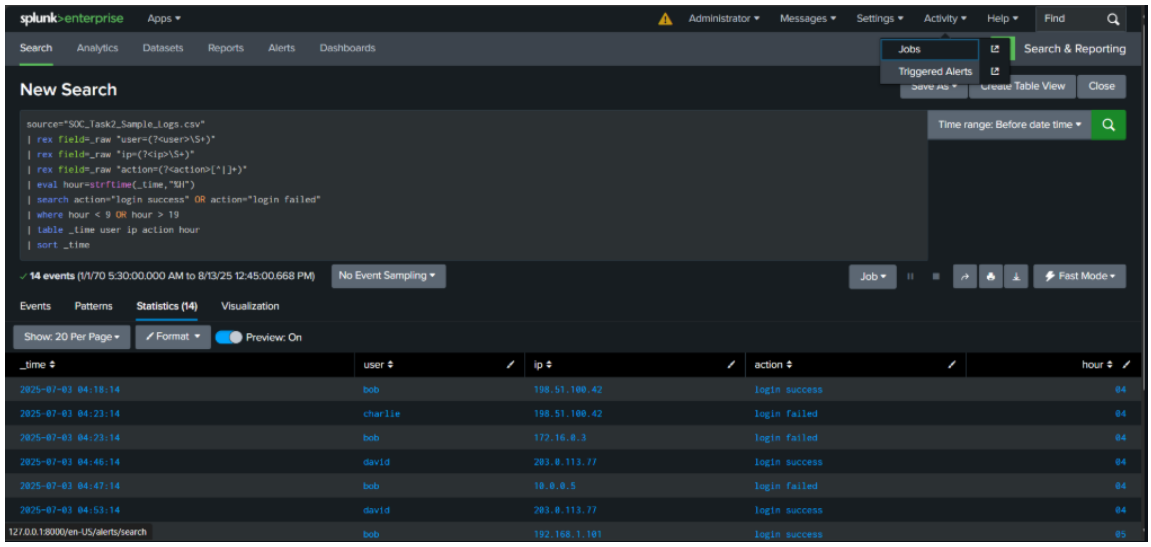
- **High** – Immediate containment is required due to rapid infection potential.

Detecting in Splunk Search:

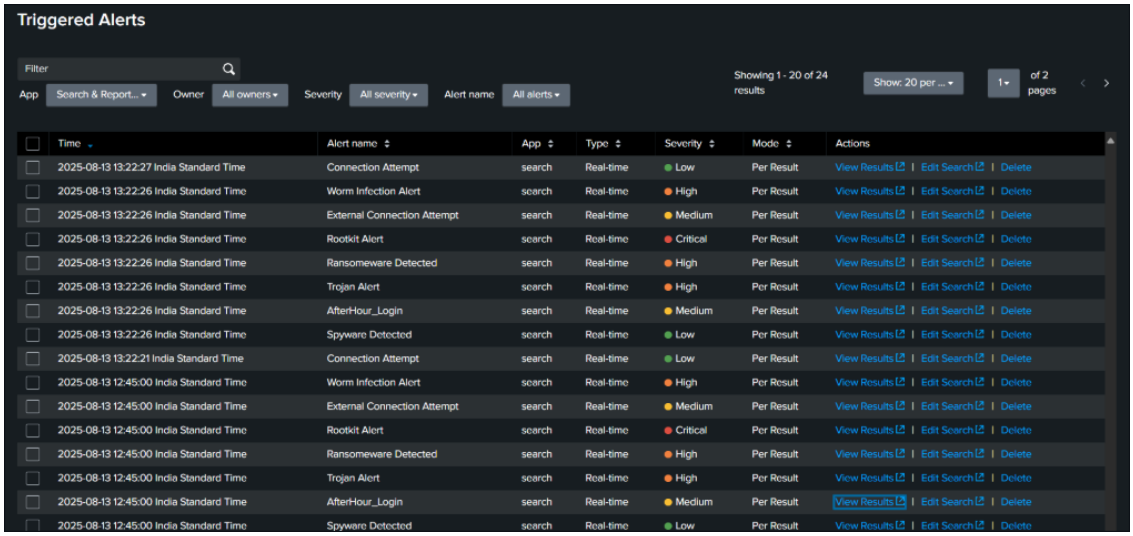


Viewing Alerts in Splunk

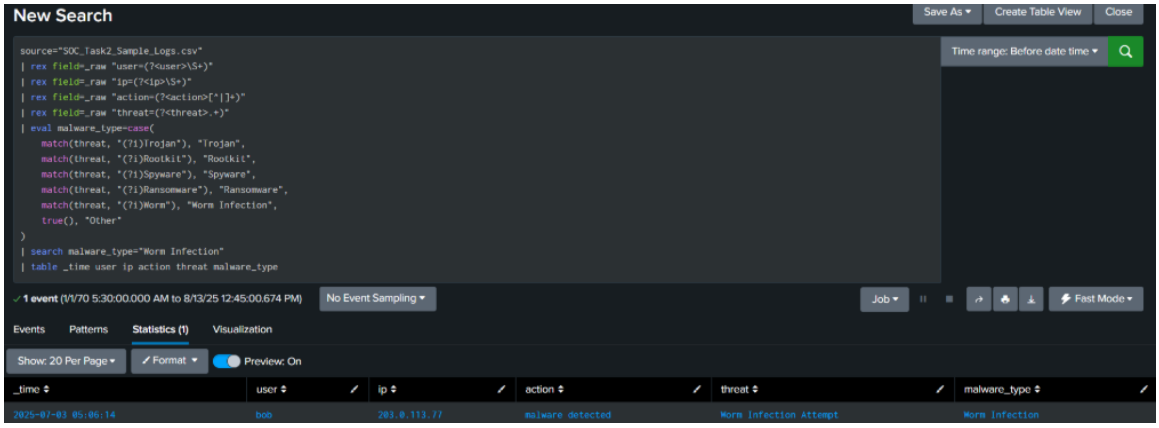
1. Navigate to **Activity** (top right corner) → **Triggered Alerts**.



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



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



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

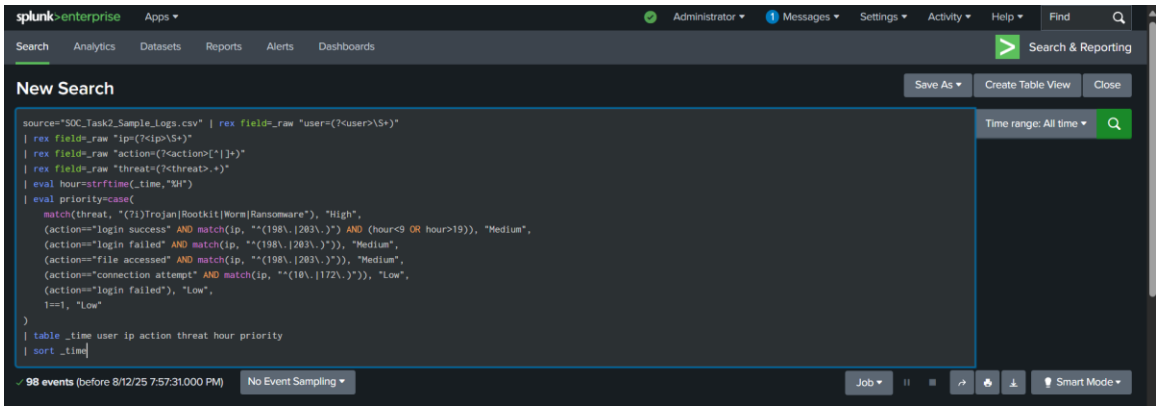
All detected security events were assigned a **severity rating** based on potential business impact, urgency for response, and likelihood of compromise. The classification follows a SOC-inspired triage model:

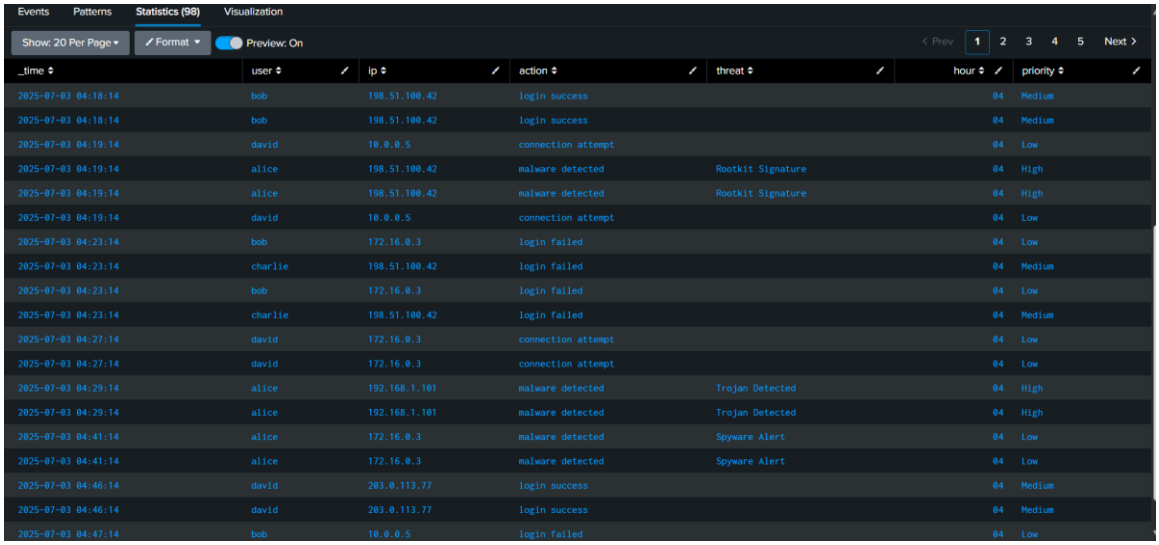
- **High Severity** –
  1. Incidents that indicate confirmed or highly probable **malware compromise**.
  2. This includes: **Trojan**, **Rootkit**, **Spyware**, **Ransomware**, and **Worm Infection** detections.
  3. These threats can cause severe operational disruption, data exfiltration, or complete 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:





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 04:46:14	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

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	bob	172.16.0.3	login failed		After-Hours Login
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 04:19:14	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	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 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

_time	user	ip	action	threat	event_type
2025-07-03 08:21:14	david	172.16.0.3	connection attempt		Internal Connection Attempt
2025-07-03 08:21:14	david	172.16.0.3	connection attempt		Internal Connection Attempt
2025-07-03 08:21:14	david	172.16.0.3	connection attempt		Internal Connection Attempt
2025-07-03 08:21:14	david	172.16.0.3	connection attempt		Internal Connection Attempt
2025-07-03 08:30:14	eve	172.16.0.3	login success		After-Hours Login
2025-07-03 08:30:14	eve	172.16.0.3	login success		After-Hours Login
2025-07-03 08:30:14	eve	172.16.0.3	login success		After-Hours Login
2025-07-03 08:30:14	eve	172.16.0.3	login success		After-Hours Login
2025-07-03 08:30:14	eve	172.16.0.3	login success		After-Hours Login
2025-07-03 08:30:14	eve	172.16.0.3	login success		After-Hours Login
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior	Ransomware Detected
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior	Ransomware Detected
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior	Ransomware Detected
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior	Ransomware Detected
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior	Ransomware Detected
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior	Ransomware Detected

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.