****

**SIEM – Security Information Event Management**

User Manual Document

By

Velox Solution Pvt. Ltd.

India | USA | Dubai | South Africa | Mexico | Sri Lanka Website: [www.velox.co.in](http://www.velox.co.in/)

# Table of Content

|  |  |  |
| --- | --- | --- |
| **SR. NO.** | **TITLE** | **PAGE NO.** |
| 01 | Declaration | 04 |
| 02 | Introduction | 05 |
| 03 | **LOGIN**   * Login Instructions: | 06 |
| 04 | **HOME**  **Analysis | Dashboard | SoC | All Event | Event Summary | MITRE | Alerts | Unparsed Messages | Report | Admin |Threat Intel | AI/ML | AI/ML Report | Playbook | Vulnerabilities | Cases |Logout** | 07 |
| 05 | **ANALYSIS**   * Custom Query Search: * Saved Queries: * Result of Query: * From Date – To Date: | 08 |
| 06 | **DASHBOARD**   * Total Events: * Distinct Risks: * Total Log Sources: * Top 10 Risks: * Top 10 log Source: * Threat Trends: * Top 10 Source IP: * Top 10 Destination IP: | 09 – 10 |
| 07 | **SoC**   * Total Alerts: * Open Alerts: * Closed Alerts: * New Alerts: * Incident by Solution: * Recent 100 Alerts: * Top 10 Alerts: * Top 10 Users: * Top 10 Endpoints: | 11 - 12 |

|  |  |  |
| --- | --- | --- |
| 08 | **ALL EVENT**   * Event counts by hour * Event Summary for All Device | 13 |
| 09 | **EVENT SUMMARY**   * Rules * Authentication Rules * Showing events of Rules | 14 |
| 10 | **MITRE**   * Top Reporting IP Addresses * Top Alert Distribution * Top Mitre Tactics * Events with More ATT@CK Refs. * Technique Names * Tactic Names | 15 - 16 |
| 11 | **ALERTS**   * Severity Level * Distinct Alerts by Name * Alert Listing | 17 |
| 12 | **UNPARSED MESSAGES** | 18 |
| 13 | **REPORT**   * Severity Report * Log Host Report * User Activity Report * Configuration Change Report * Incident Tracking Report * Source Attack Report * Access Control Report * Security Configuration Report * Compliance Logging Report | 19 - 23 |
| 14 | **ADMIN**   * User * Device * Rule | 24 - 26 |
| 15 | **Threat Intel**   * Top 10 Risk Users * Top 10 Risk Log Sources * Top 10 Risk Destination IP * Intel Sources * Distinct Alerts by Name * Alert Listing | 27 |
| 16 | **AI/ML**   * Anomalies * User   Entities | 28 - 32 |
| 17 | **AI/ML Report**   * Logins * System Activities | **33** |
| 18 | **Playbook**   * Playbook * Enabled * Disabled * Create Playbook | **34** |
| 19 | **Vulnerabilities**   * Severity * IP Addresses * Vulnerability Table * Assigned Ticket in ITSM | **35** |
| 20 | **Cases**   * Rule Name * Severity * Assign Playbook * Playbook | **36** |
| 21 | **LOGOUT** | 37 |

**DECLARATION**

The technical details outlined in this document are confidential and intended solely for the use of the designated client. The logos, document style, and content are protected by copyright under the laws of India and international best practices. Unauthorized duplication or misuse of this material for any personal or professional gain is strictly prohibited.

The content contained within this document constitutes the Intellectual Property (IP) of Velox Solution Pvt. Ltd. (VELOX) and may not be replicated in any form without the explicit written permission of Velox.

**© 2024 Velox Solution Pvt. Ltd.**

**All rights reserved.**

# INTRODUCTION

**Welcome to the SIEM - ScanPlus User Manual**

In today’s rapidly evolving digital landscape, maintaining robust security measures is more critical than ever. The ***SecureIT SIEM - ScanPlus*** is designed to be your comprehensive solution for managing and safeguarding your organization’s IT infrastructure. As a powerful Security Information and Event Management (SIEM) tool, SecureIT SIEM – ScanPlus tool enables you to efficiently collect, analyze, and respond to security events and incidents in real-time.

**What is SIEM?**

Security Information and Event Management (SIEM) is a technology that provides real-time analysis of security alerts generated by various hardware and software infrastructures in an organization. A SIEM tool aggregates and correlates log data from across your network, helping to identify and mitigate potential threats before they can impact your operations.

**Purpose of This Manual**

This user manual is designed to guide you through the functionalities and features of or SecureIT SIEM tool Whether you are a system administrator, security analyst, or IT professional, this document will provide you with the essential information needed to effectively deploy, configure, and utilize the tool.

**Getting Started**

This manual will take you through a step-by-step approach, starting from the initial setup and configuration to advanced features and troubleshooting. By the end of this guide, you will be equipped with the knowledge to leverage SecureIT SIEM to its full potential, enhancing your organization’s security posture and response capabilities.

Should you have any questions or require further assistance, please refer to the “[**support@velox.co.in**](mailto:support@velox.co.in)”

section at the end of this manual or visit our online support portal.

Welcome to a new level of security management with our SecureIT SIEM – ScanPlus Solution.

# SECURITY INFORMATION AND EVENT MANAGEMENT

 **LOGIN**

To access the ***SecureIT SIEM tool***, users need to enter the following URL into their web browser. This action will display the login screen, as illustrated in the Image below.

**URL:** <http://localhost:8080/ScanPlus-SIEM/>

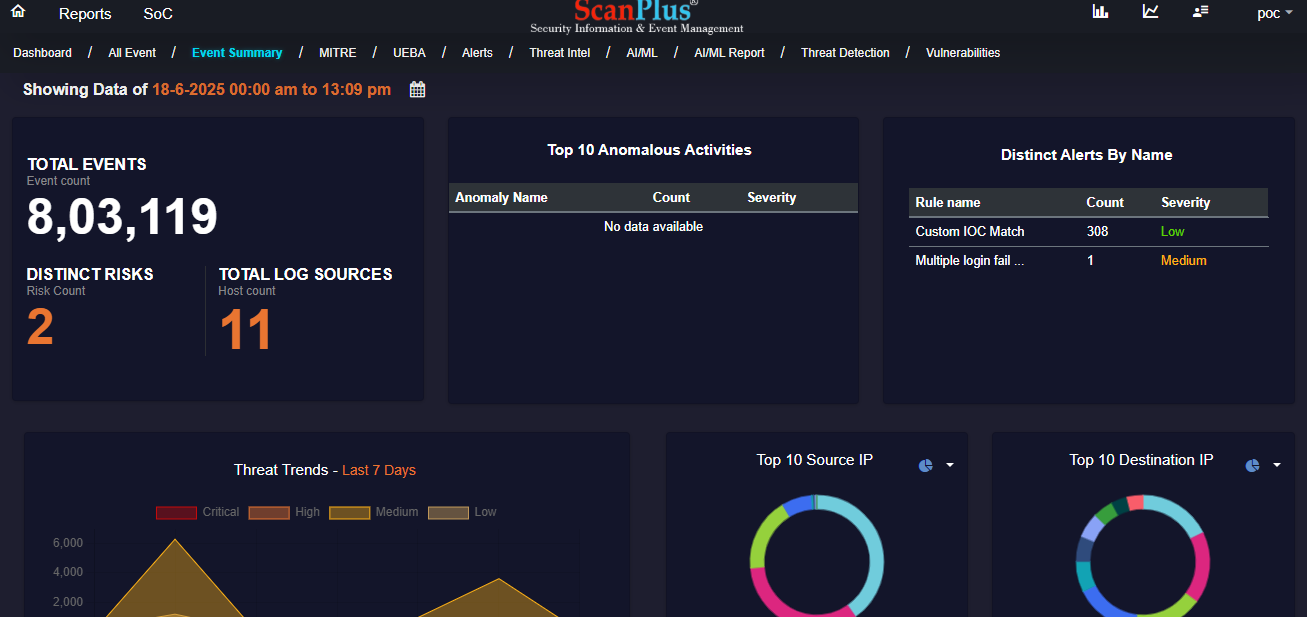


**Login Instructions:**

* Enter your **Username** and **Password** in the respective fields.
* Click on **LOGIN** Button.
* Upon clicking **LOGIN**, you will be redirected to the Dashboard page.
* If you want to remember login detail click on **Remember Me.**
* If you click on **CLEAR**, all entered data will be cleared.

# HOME

* The Welcome screen will display the Dashboard Screen.
* From here, you can navigate to the following sections:
  + **Report**
  + **SoC**
  + **Dashboard**
  + **All Event**
  + **Event Summary**
  + **MITRE**
  + **UEBA**
  + **Alerts**
  + **Unparsed Messages**
  + **Report**
  + **Admin**
  + **Threat Intel**
  + **AI/ML**
  + **AI/ML Report**
  + **Playbook**
  + **Vulnerabilities**
  + **Cases**
  + **Logout**

****

# Reports

* In Analysis User can Filter logs using **Custom Query** search bar and clicking on **Search** button.
* User can also write custom query according to requirement and save it using **Save** button and access it when required using **Saved Queries** option.

**Queries:**

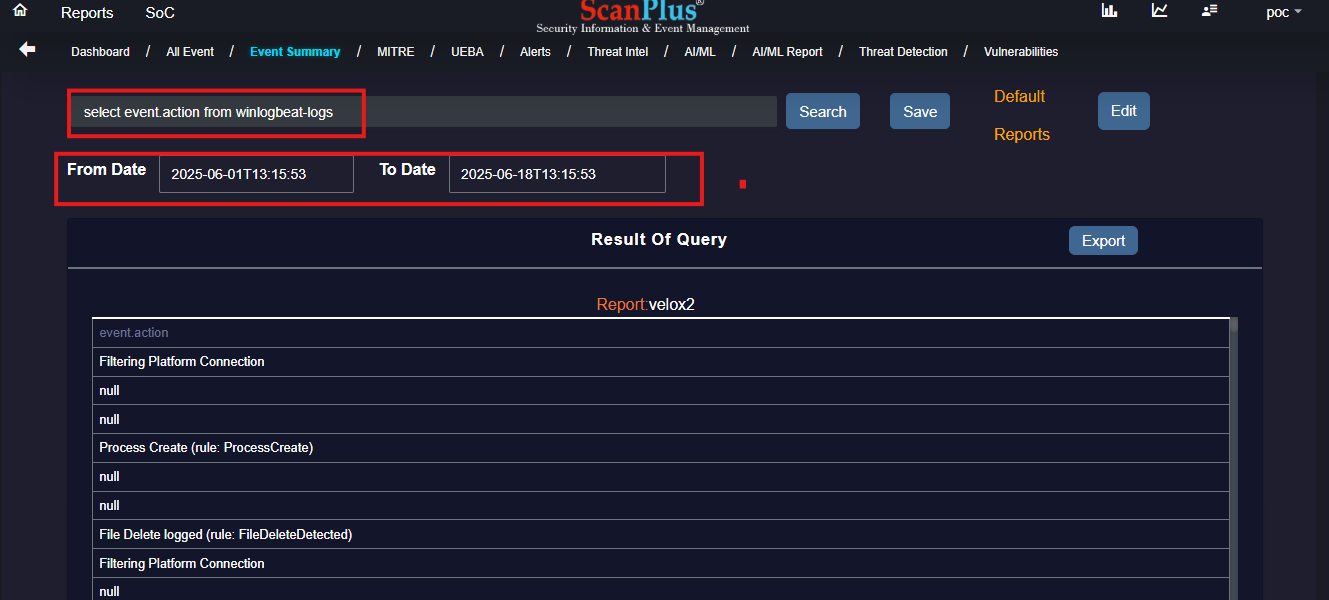
**Windows:**

select @timestamp, host.ip, event.action, source.ip, destination.ip, message from winlogbeat-logs;

**fortinet:**

select @timestamp, host.ip, event.action, source.ip, destination.ip, event.original from filebeat-fortinet;

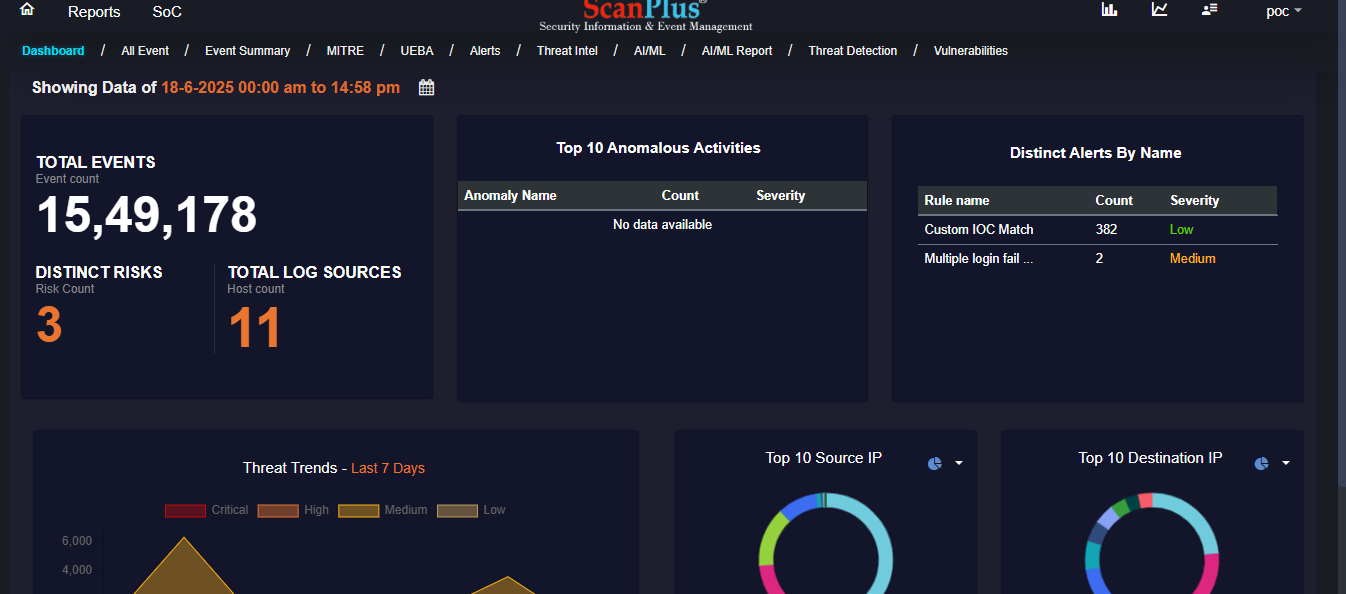
* Using above query for **Fortinet User** can search for *network device events*.
* Using above query for **Windows user** can search for *windows log events*.
* User can export **Result of Query** into excel file using **Export** button as shown below.



* Using **From Date – To Date** user can **Filter** *Result of Ǫuery.*

# DASHBOARD

* **Total Events (event count):** This shows the total number of logs that have been generated.
* **Distinct Risks (risk count):** This shows *Count of Distinct Alerts by name***,** which are already defined in Alerts Tab with proper Alert *Rule Name, Count and Severity.* (Severity means Strictness).



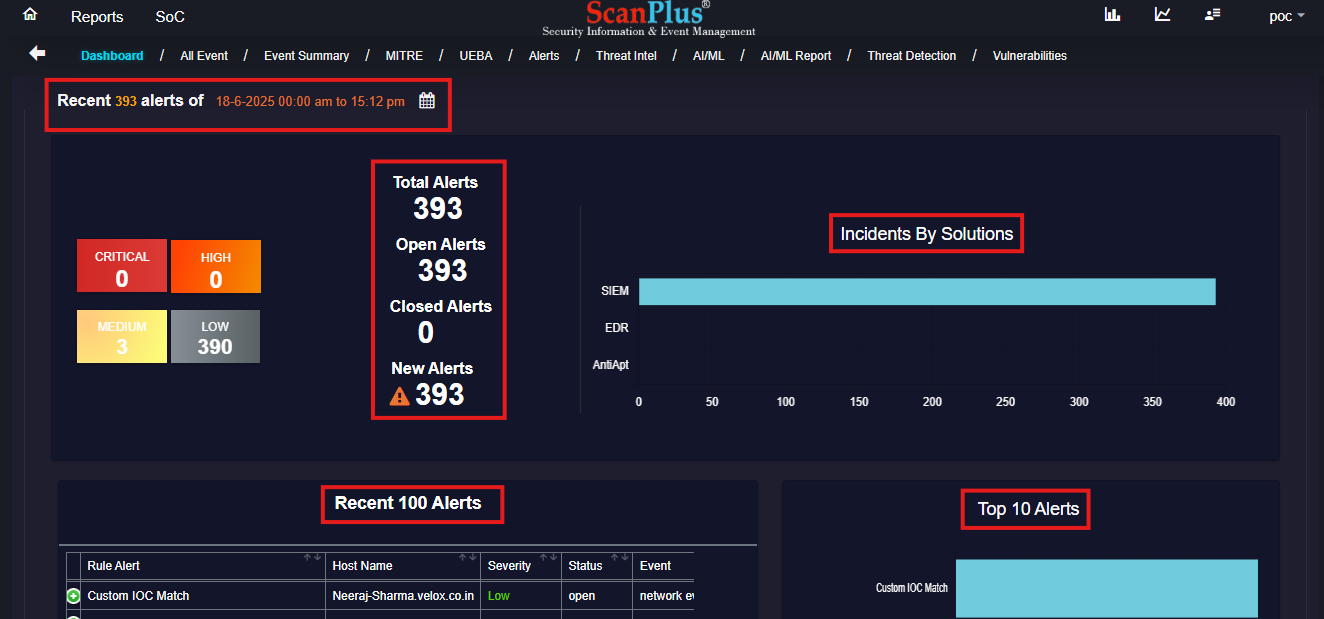
* **Total Log Sources (Host Count):** This shows the total number of devices from which logs are being generated.
* **Top 10 Risks:** This shows top 10 alerts according to *Rule Name* with their *Count*.
* **Top 10 log Source:** This will display top 10 devices that has been added along with their *Log Source* and *Events* count. *NOTE: It will display* ***todays*** *Log Source IP & Events Count.*
* **Top 10 Source IP:** This will display top 10 source IP.
* **Top 10 Destination IP:** This will display Top 10 Destination IP.
  + ***Source IP Address -*** This is where the log or events comes from, or the device that is generating the Data.
  + ***Destination IP Address*** - This is where the logs are being sent to as the main device, which collects the log from multiple Source IP addresses.

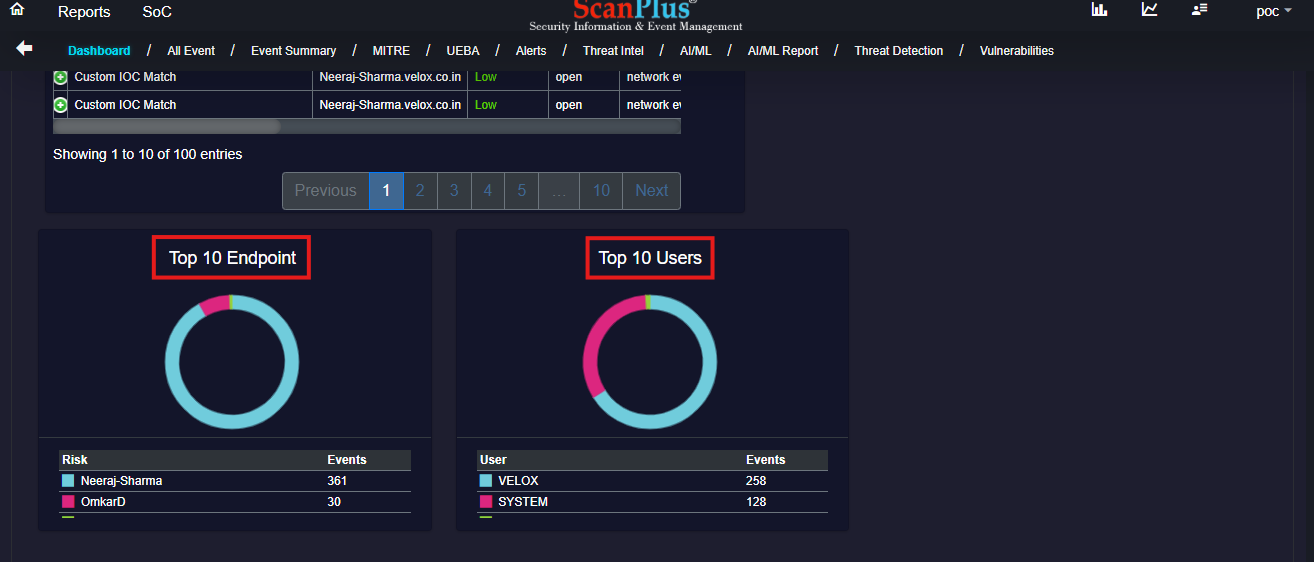
So, the *Source* IP shows where the log is coming from and the *Destination* IP is where the log is going to and being collected.

* **Threat Trends:** This is to display 7-day event logs using defined severity.

 **SoC**

* **Total Alerts:** This shows the total number of security alerts generated by the SIEM tool. Alerts are notifications about potential security issues that need attention, classified into Cri tical, High, Medium, Low.
* **Open Alerts:** Displays the number of alerts that are currently open and need attention.
* **Closed Alerts:** Indicates the number of alerts that have been resolved.
* **New Alerts:** This will display all the new alerts.
* **Incident by Solution:** This breaks down security incidents based on the solutions or methods used to address them. It helps in understanding which solutions are most frequently involved in handling incidents.
* **Recent 100 Alerts:** Displays the most recent 100 alerts, helping the SOC team quickly see the latest potential issues that need to be reviewed.





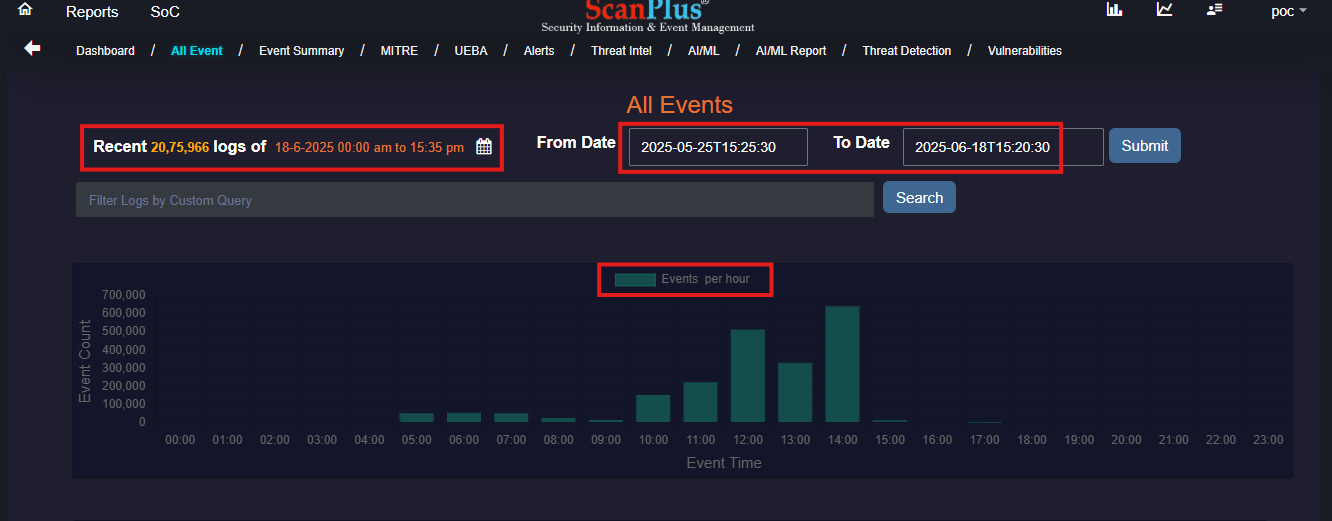
* **Top 10 Alerts:** Shows the top 10 types of alerts that have been triggered by the most events. This helps identify the most common types of alerts being generated.
* **Top 10 Users:** This section will display top 10 users that have generated recent alerts.
* **Top 10 Endpoints:** This section includes top 10 endpoints (devices or systems) generating the most alerts.
* **Top 10 locations:** Shows the top 10 physical or network locations that have generated the most alerts, which can help in pinpointing geographic or network hotspots of concern.

This interface helps security teams monitor and manage threats effectively by providing a comprehensive overview of security alerts and incidents.

# ALL EVENT

In `*All Events*` we are able to look at all the events, below are few actions that we are able to perform under All Events tab:

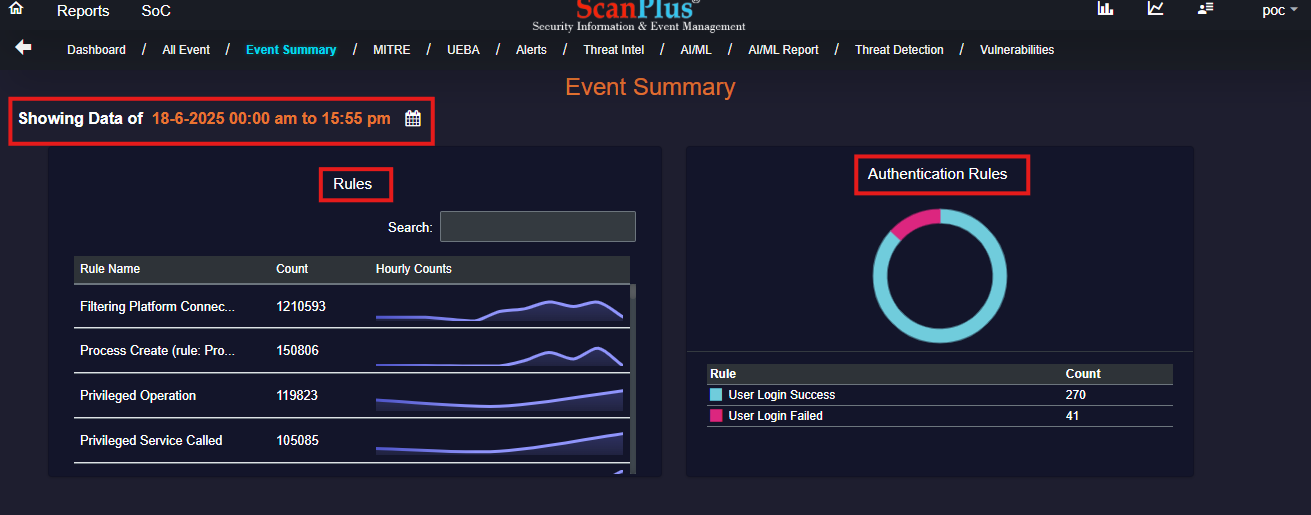
* *All Event* will display recent 500 logs.
* The Graph displays events count generated per hour.
* In the **search bar** we can search using keywords which will then filter below data and bar-chart accordingly.
* We can further filter data by selecting date in **From Date s To Date** datetime selection, this will filtrate data in bar-chart as well as below **Event Summary for All Device** table.
* There is **calendar** option which has predefined filters to filter below data.





* In Above image we are able to look at all the events log message with their source IP and date- time of the generated log. It also displays rule which has been triggered. This Data can be downloaded using above highlighted fields.
* The **Models** in above table contains information about the event that has been generated.
* **Custom Visibility** is used to select column which user wants to hide from table.

# EVENT SUMMARY

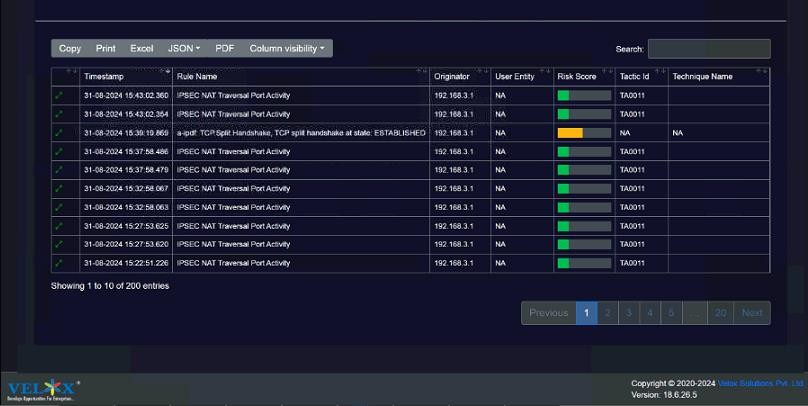
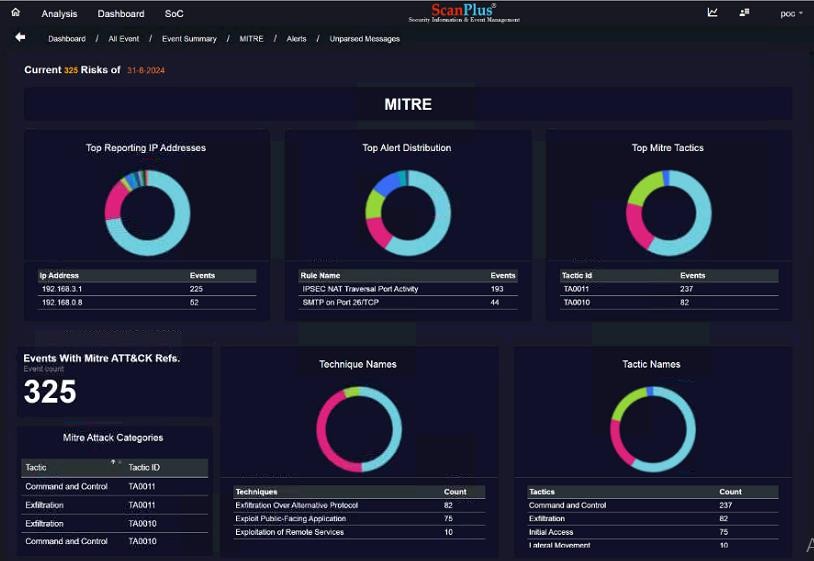
****

****

* In above picture of ***Event Summary***, there is again an option of *calendar* from which we could filter data as we have seen earlier.
* The ***Rules*** section is to demonstrate count of events group by rule name, the *hourly count* will display line graph.
* ***Authentication Rules*** are used to display if the auth was successful or failed.
* Above image is displaying all events of rules in summary, each header is similar to what we discussed in *`All Events`.*

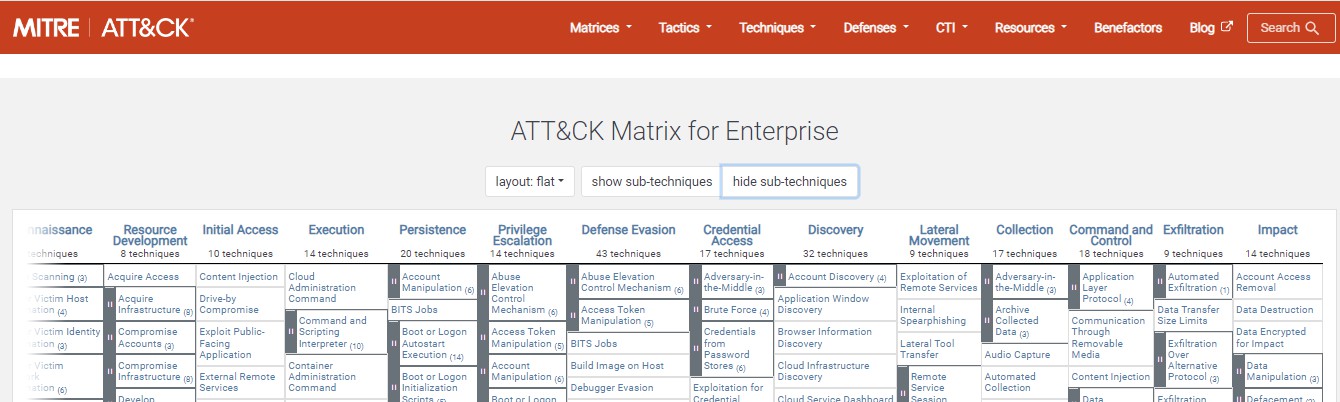
# MITRE

* **Top Reporting IP Addresses:** This section displays Top IP Address of Host and events generated count group by Host IP Address.
* **Top Alert Distribution:** It will group events by rule name and display top alerts generated.
* **Top Mitre Tactics:** This displays the tactic ID with the count of events that has been generated for particular IDs.
  + **Tactic ID:** The description for tactic ID is displayed in this link: <https://attack.mitre.org/tactics/>
  + **Events –** This shows the total `count` of top alert distribution.



Download

* **Events with Mitre ATTsCK Refs.:** This is total count of rule wise grouped events in **Top Alert Distribution**.
* **MITRE Attack Category:** This show category of tactic along with tactic ID. This IDs and Categories are listed from MITRE to categorize events and log that have been generated.
  + You can view category wise events rules here: <https://attack.mitre.org/>



* **Tactics:** It represents the *"why"* of an ATTCCK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access, so the count of **tactics** is displayed along with its category and total **count**.
* **Techniques:** It represents *'how'* an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access, so the count of **techniques** is displayed along with its category and total **count**.
* As we have seen earlier, we can **export** data using the **above highlighted fields.**

# UEBA

# **UEBA** stands for **User and Entity Behavior Analytics**. It is a cybersecurity process that uses machine learning, algorithms, and analytics to **detect abnormal behavior by users and entities.**

**Incident** Details-Help correlate behavioral anomalies like brute-force, insider threats, etc.

**Host** IP Info-Understand the context and location of impacted devices.

Source IP- Info Identify potential **threats**, especially from external or unusual IPs.

User- user account was involved in the detected activity. Could be used on multiple hosts or

during both **failed** and **successful** login attempts.

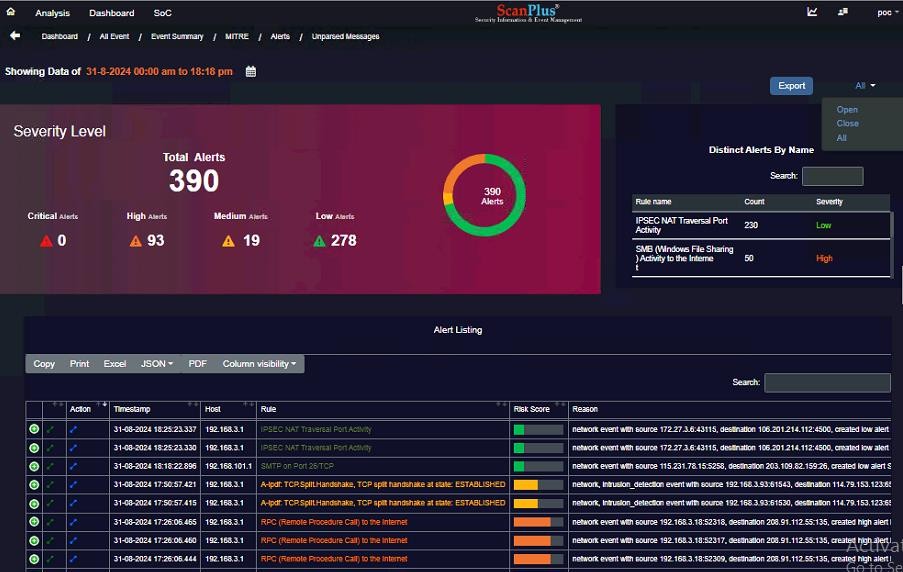
# 

# 

# ALERTS

In SIEM tool, the **Alerts** section is where we monitor and manage all security alerts. Here’s a

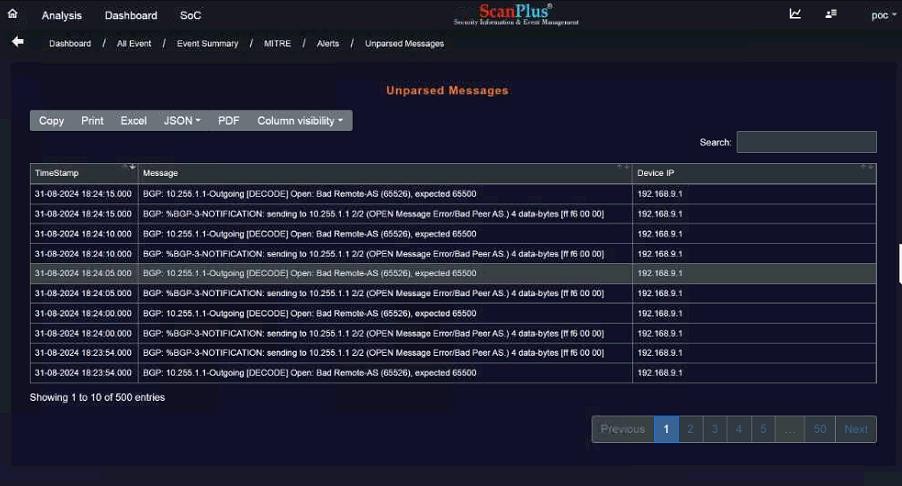
breakdown of what each part does and how I use it:



* **Severity Level** the donut chart displays the distribution of alerts based on their severity levels.
* **Distinct Alerts by Name** this section lists the different types of alerts by their rule names, along with the count and severity for each type. The count shows how many times the rule has been triggered.
* **Alert Listing Table** the “Alert Listing” table is used to track individual alerts and their details.
* The **export** options s used to create reports and perform detailed analysis of all the data into excel.

# UNPARSED MESSAGES

* The **Unparsed Messages** section in our SIEM tool helps me track and manage log messages that the system couldn’t interpret. By examining these messages and their timestamps, user can identify and address issues with log parsing to ensure all relevant data is processed and analyzed effectively.

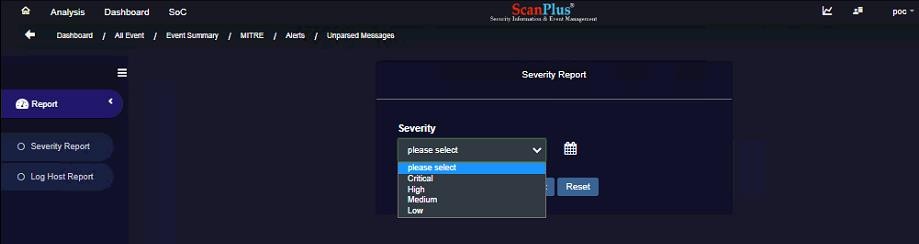


* Using above highlighted fields user can **export** report in different formats.
* **Custom Visibility** helps user to hide the columns that are not required.

# REPORT

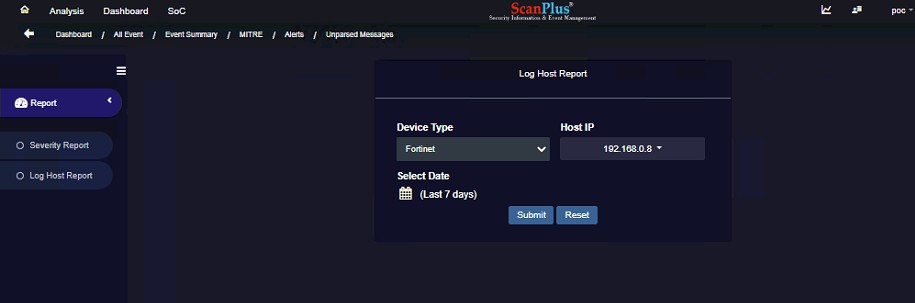
When clicked on Report there are 10 options.

* **Severity Report**
* In the **Severity Report** we get to select the statuses from the Drop down as shown below; after selecting status we need to select the days of which we need to find out the report and click on **submit**.
* This **Severity Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



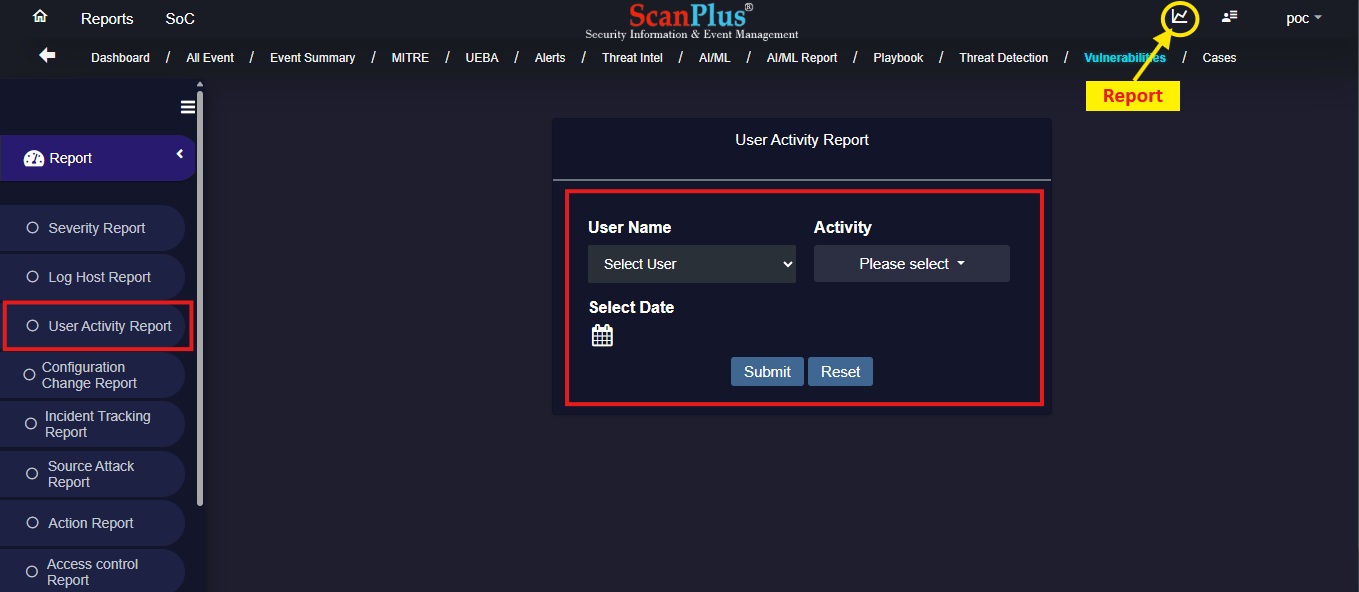
**Report**

* **Log Host Report**
* In the **Log Host Report** we get to select the Devices type from the Drop down; after selecting device type (Fortinet) we need to select the date and Host IP of which we need to find out the report and click on **submit**.
* This **Log Host Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.

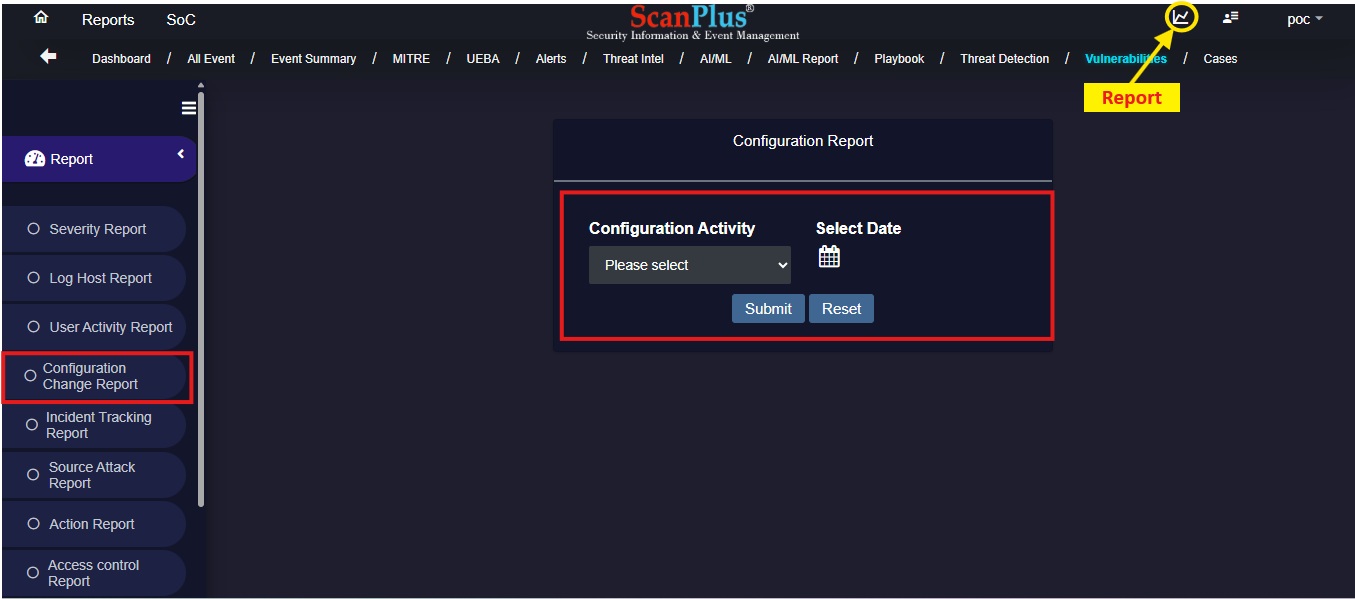


**Report**

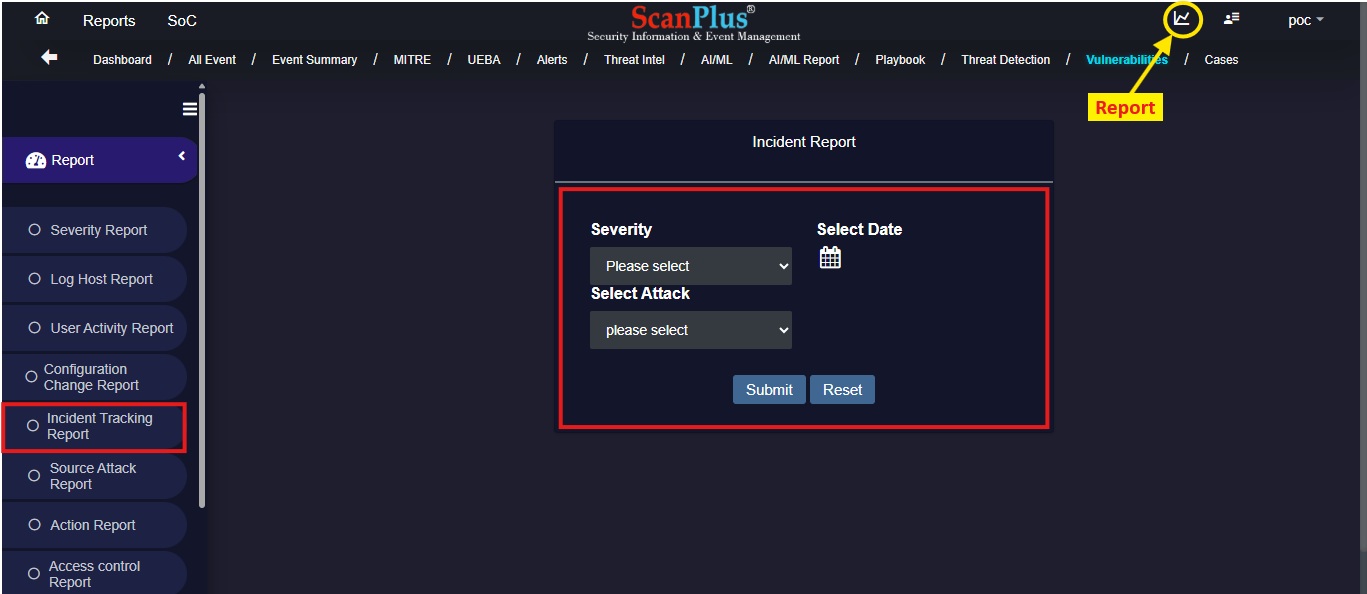
* **User Activity Report**
* In the **User Activity Report,** we get to select the User Name and Activity from the Drop down; after selecting User Name and Activity we need to select the date and click on **submit**.
* This **User Activity Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



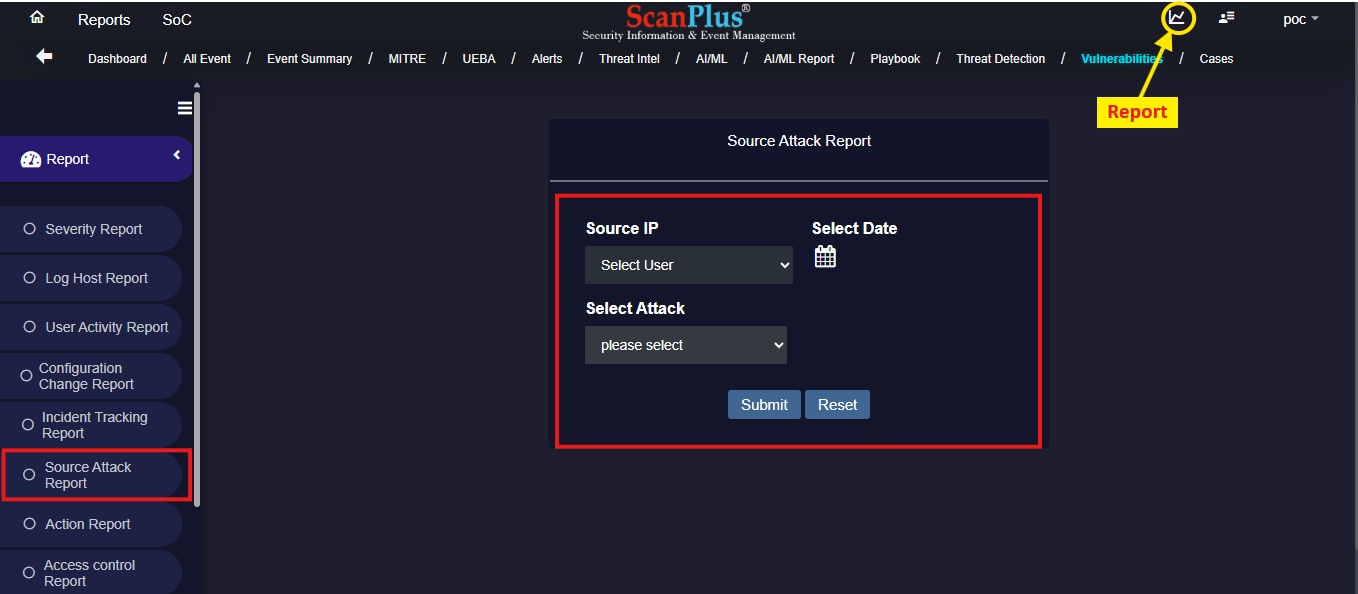
* **Configuration Change Report**
* In the **Configuration Change Report,** we get to select the Configuration Activity; after selecting Configuration Activity we need to select the date and click on **submit**.
* This **Configuration Change Activity Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



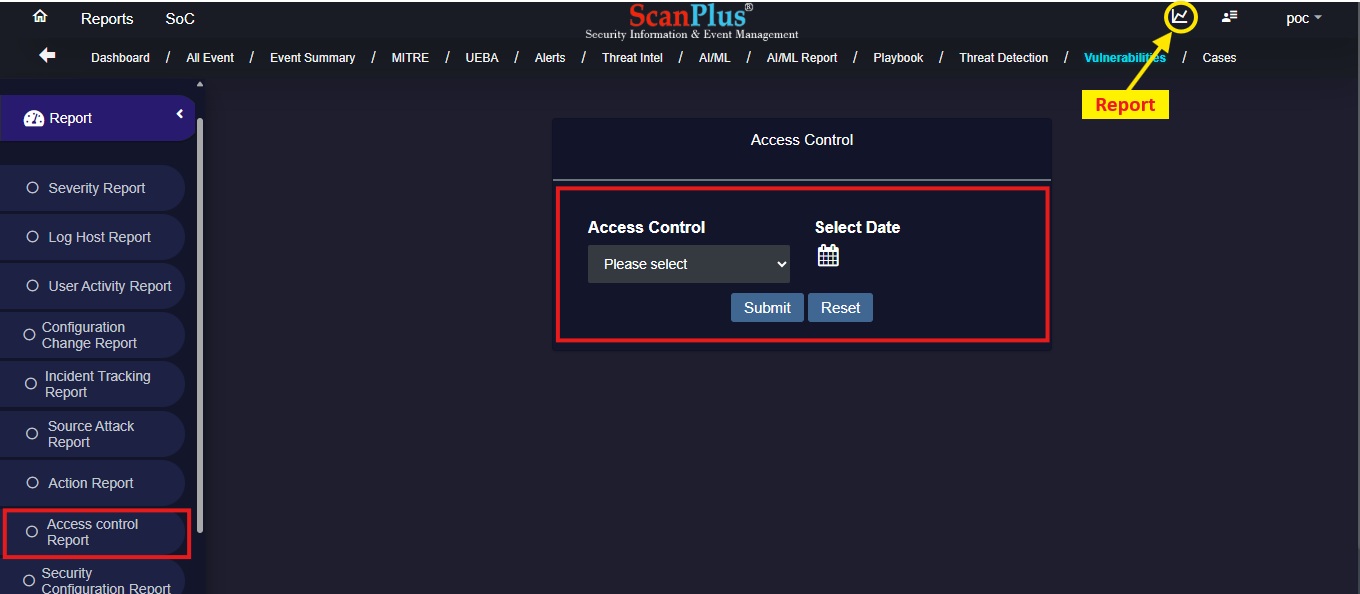
* **Incident Tracking Report**
* In the **Incident Tracking Report,** we get to select the Severity and Attack from the Drop down; after selecting Severity and Attack we need to select the date and click on **submit**.
* This **Incident Tracking Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



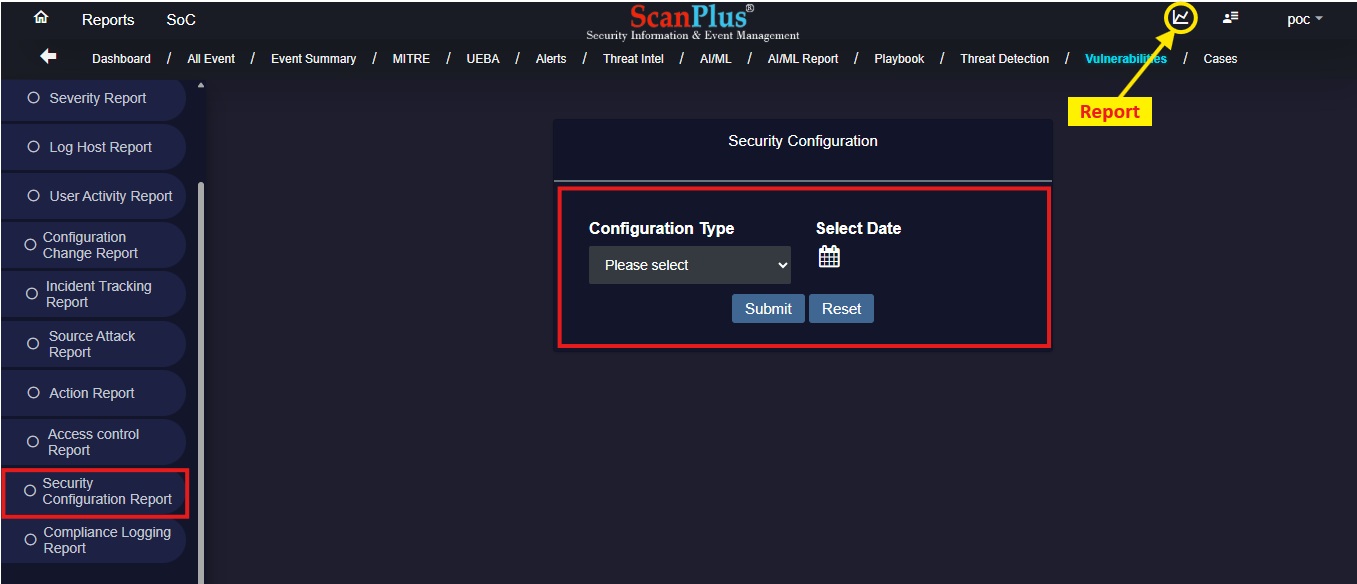
* **Source Attack Report**
* In the **Source Attack Report,** we get to select the Source IP and Attack from the Drop down; after selecting Source IP and Attack we need to select the date and click on **submit**.
* This **Source Attack Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



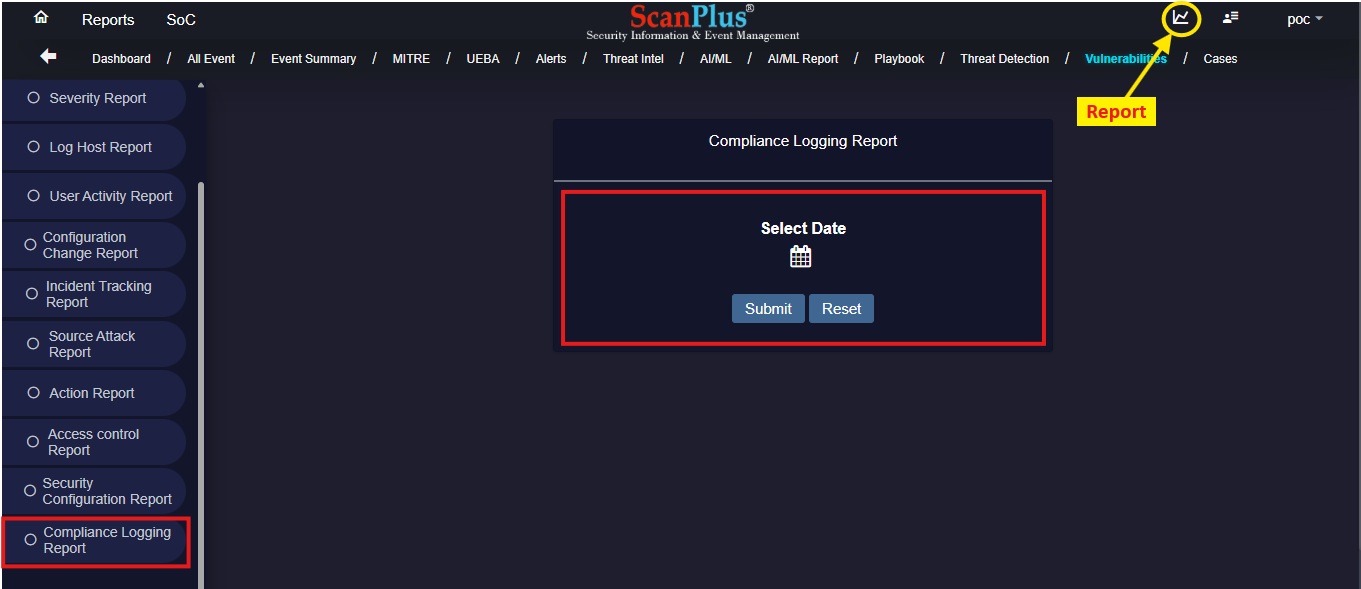
* **Access Control Report**
* In the **Access Control Report,** we get to select Access Control from the Drop down; after selecting Access Control we need to select the date and click on **submit**.
* This **Access Control Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



* **Security Configuration Report**
* In the **Security Configuration Report,** we get to select Configuration Type from the Drop down; after selecting Configuration Type we need to select the date and click on **submit**.
* This **Security Configuration Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.



* **Compliance Logging Report**
* In the **Compliance Logging Report,** we get to select the date and click on **submit**.
* This **Compliance Logging Report** will get downloaded into a folder name **log report** where the SIEM tool has been installed.

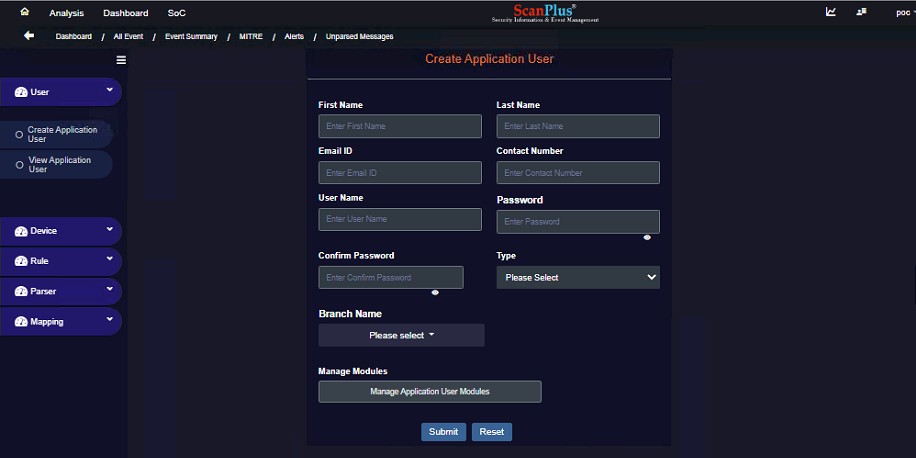


# ADMIN

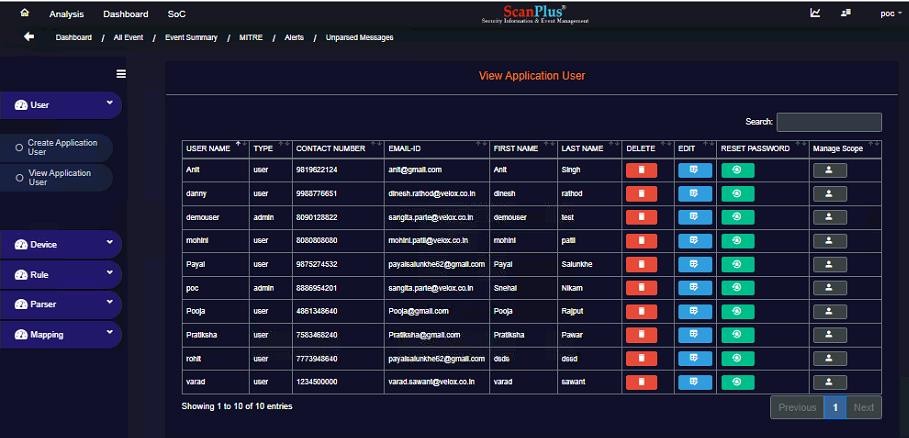
In **Admin** there are various options such as **User**, **Device**, **Rule**, **Parser**, **Mapping.**

## User

* **Create Application User :** In this admin can *Add New User* to give User Access to the application.



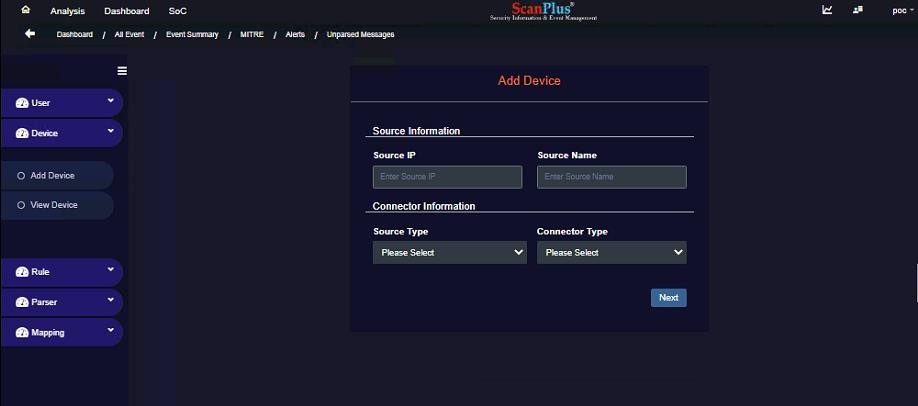
* **View Application User:** Admin can *View Added Users List*. Admin can also modify User Access, as shown below.



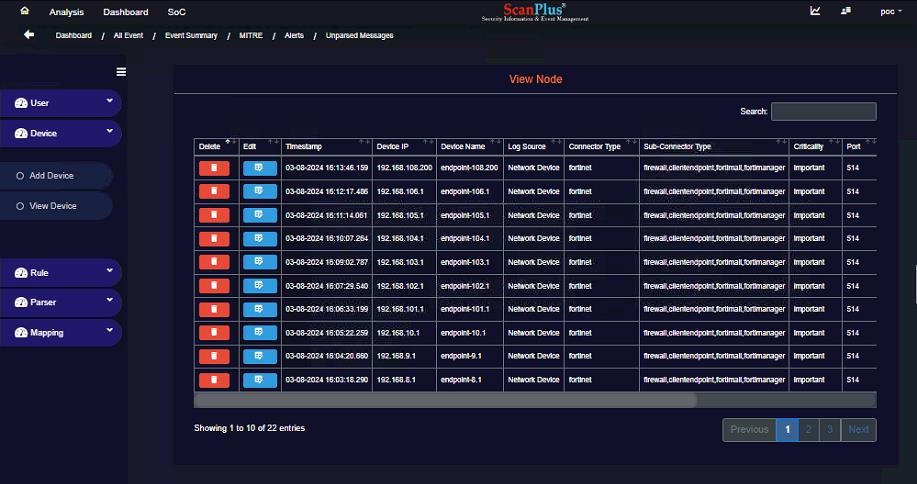
**Modify Users**

## Device

* **Add Device:** Using Add Device option admin can add new device of different types by entering appropriate information required.

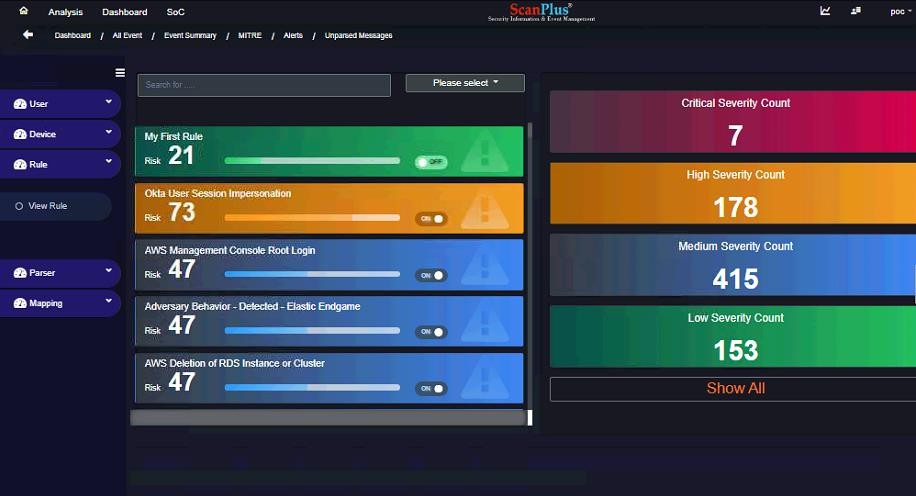


* **View Device:** Admin can *View Added Devices* over here, also can **edit** C **delete** according to their requirements.



## Rule

* **View Rule:** User can view added rules, turn on or off any rule which are not required.



## Parser

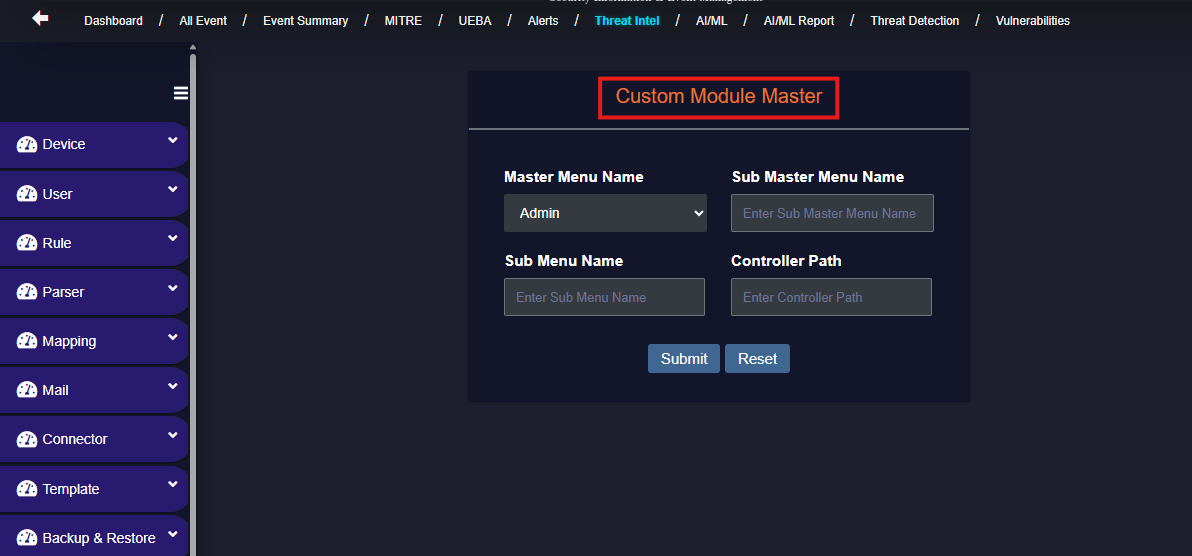
## View Parser: It is used for parsing different rules into SIEM.

## 

## Mapping:

## Here mapping is used for master access to add different U.I on page by selecting and entering

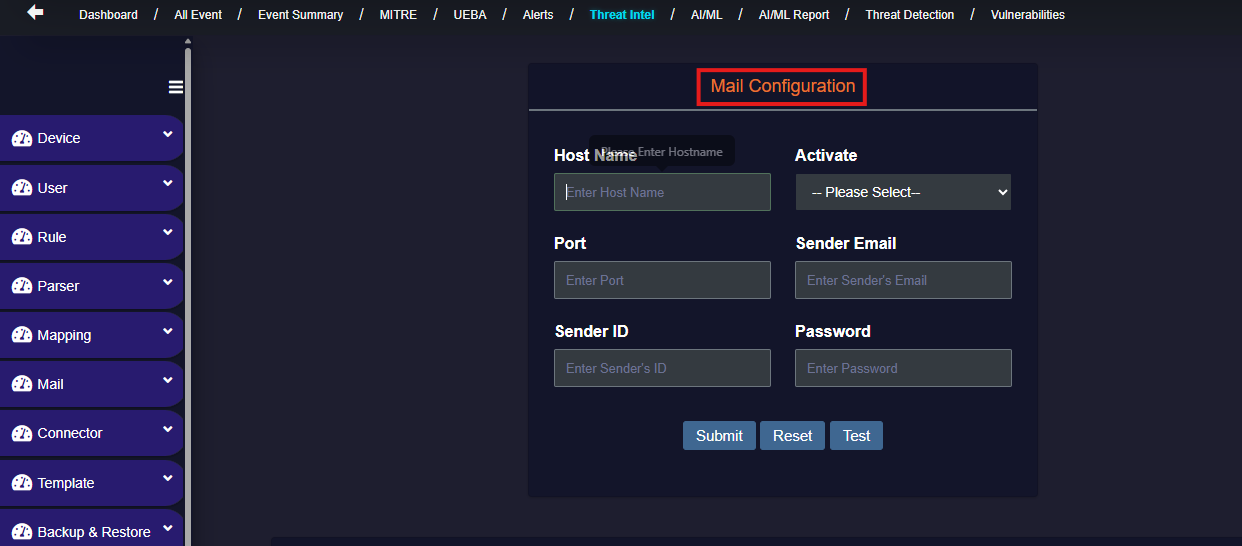
## the correct information.



## Mail:

* + Add mail:

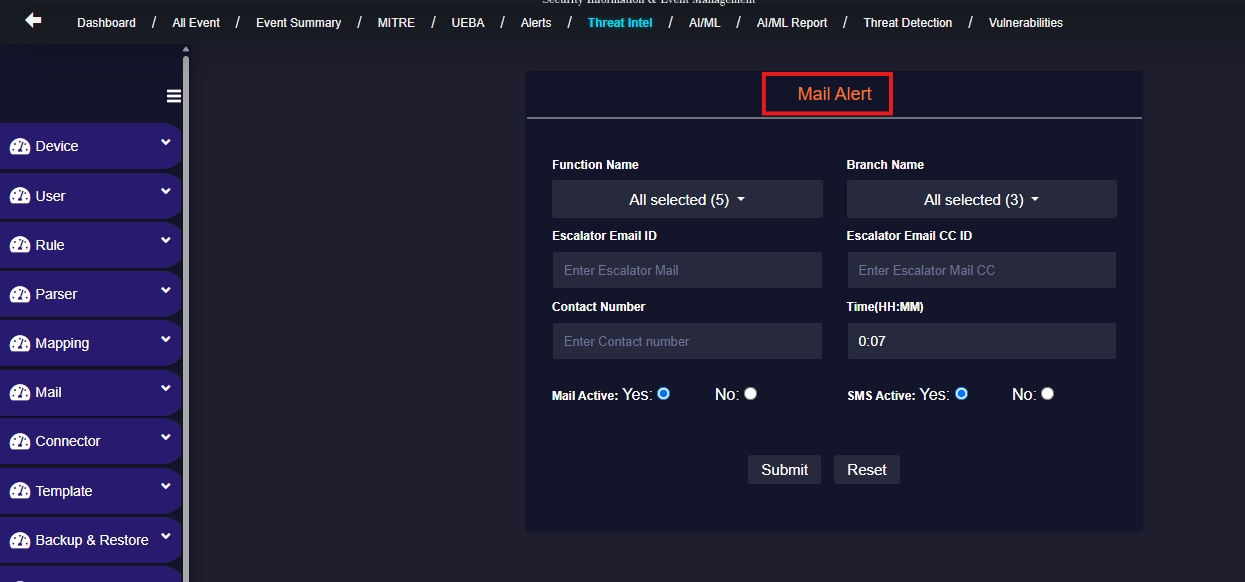
In add mail we can add new mails by selecting the proper details into given boxes.



* + Alert Configuration:

Here we can set the different alerts with its branch name by selecting the mail id,

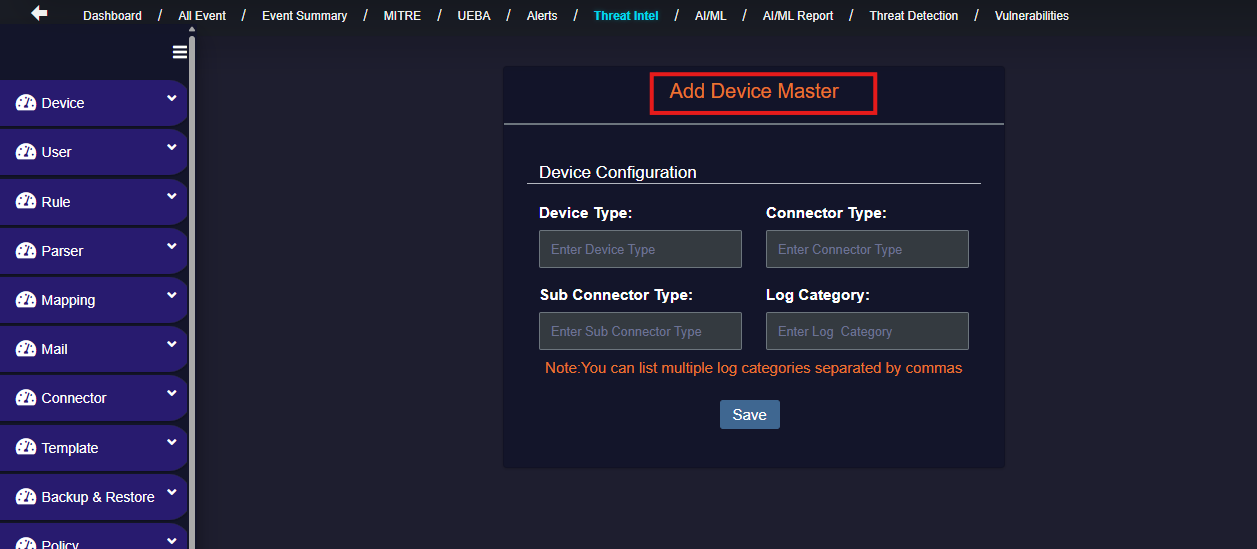
contact number & time.



## Connector:

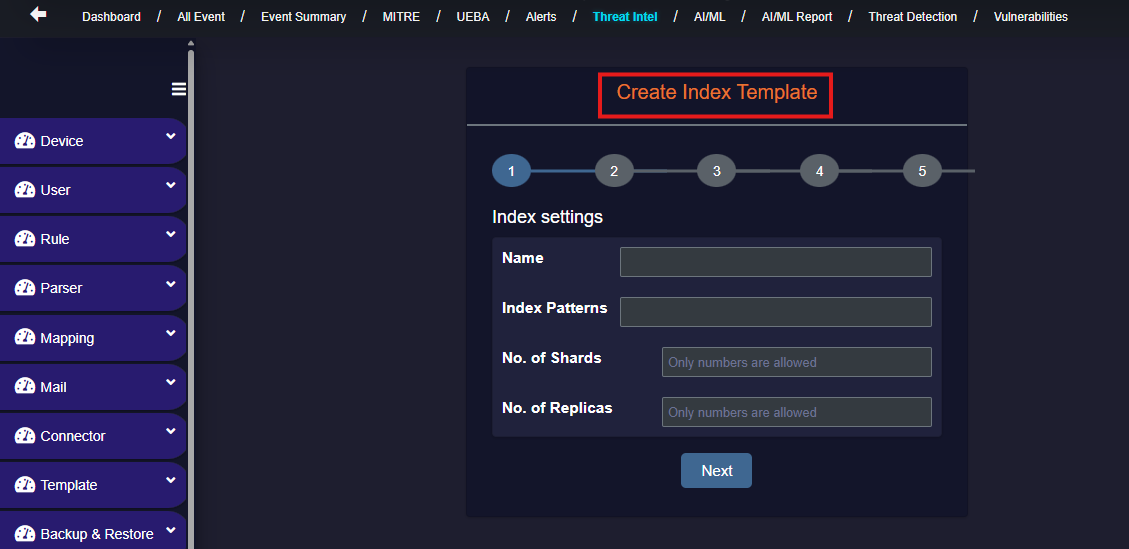
* + Add Connector:

Through using this connector option we can add different application here.

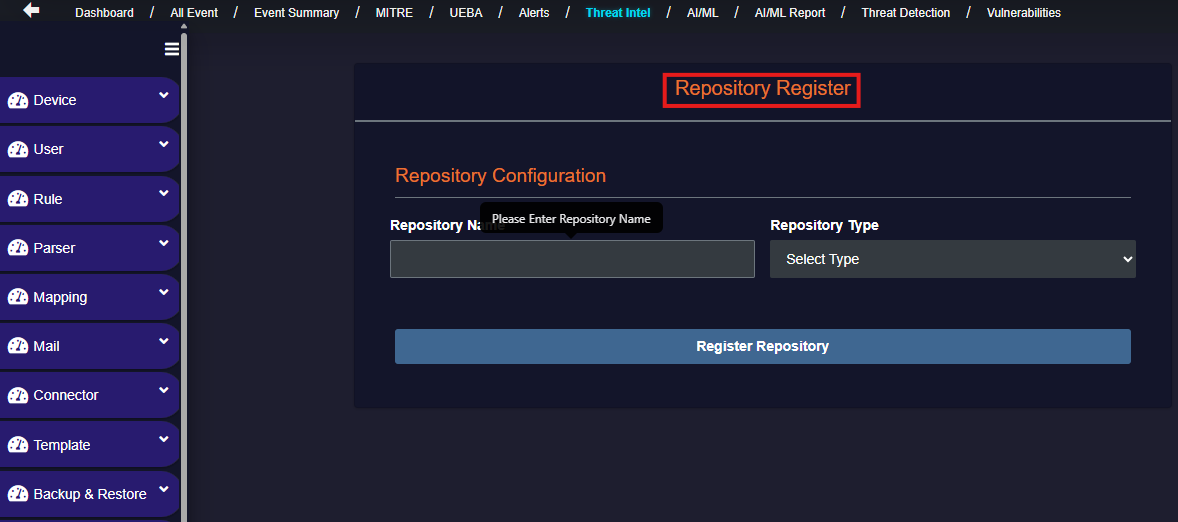


* **Template:**
  + Add Template:

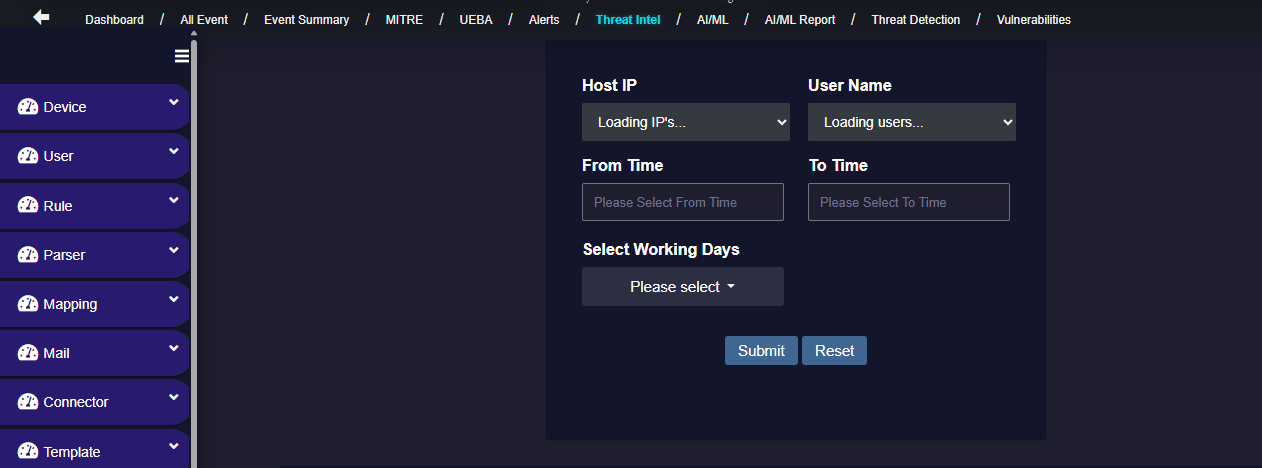
This is used for adding coding templates.

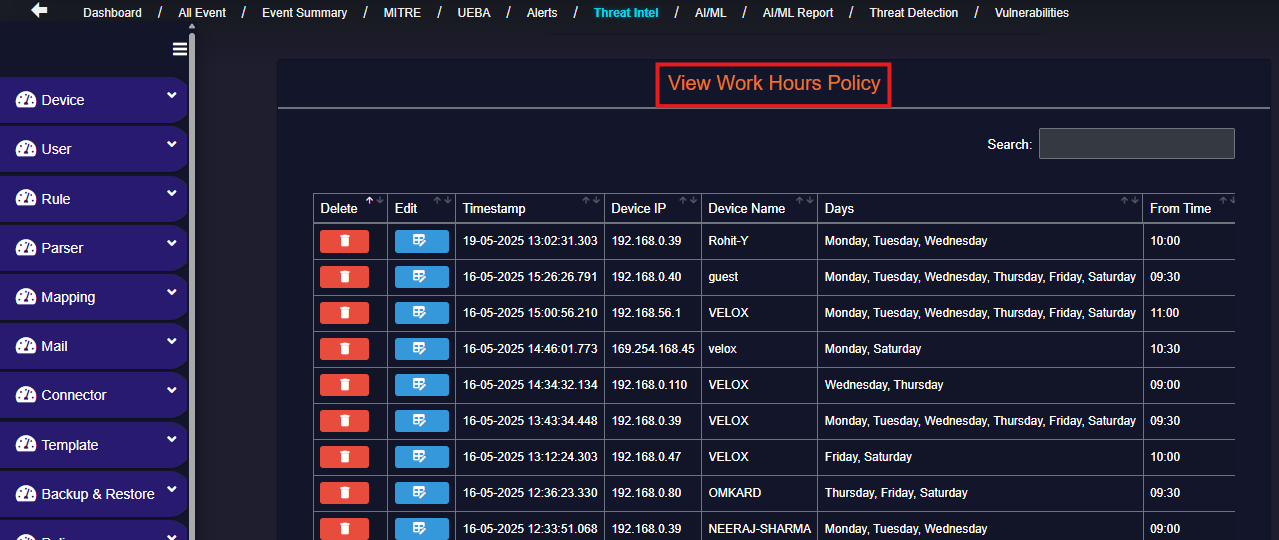


* Backup & Restore:



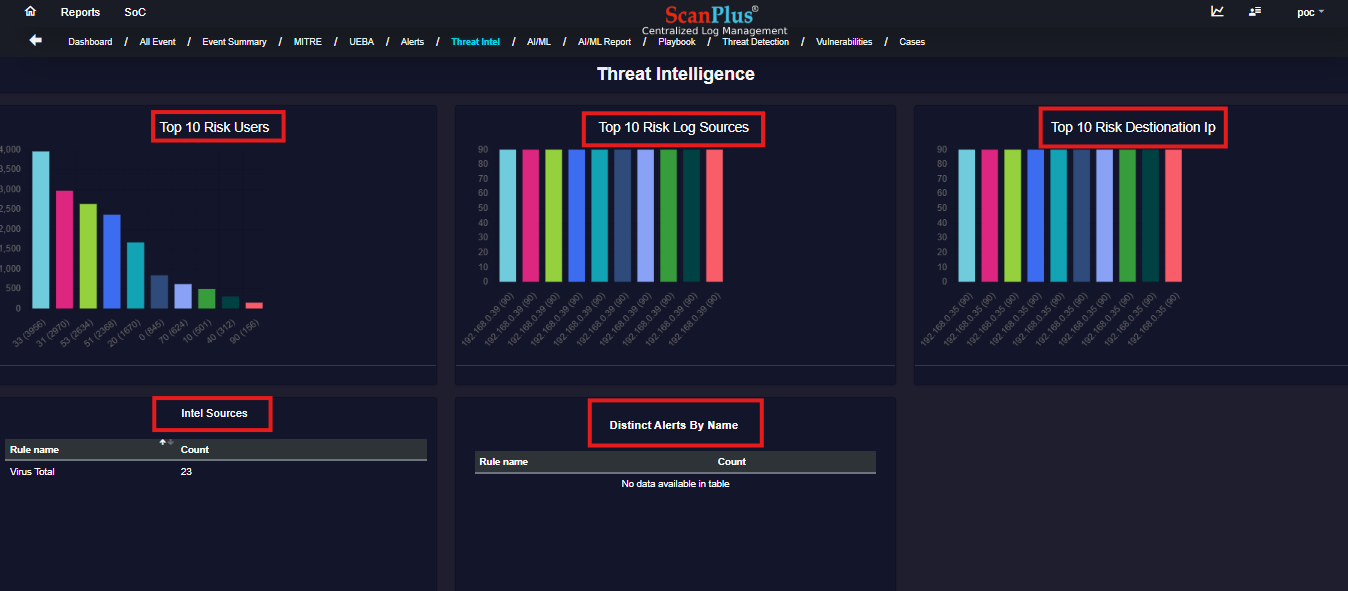
* **Policy:**



****

# Threat Intel

* **Top 10 Risk Users:** This bar chart identifies users who are most frequently associated with risks.
* **Top 10 Risk Log Sources:** This chart displays the log sources contributing most to detected threats.
* **Top 10 Risk Destination IP:** Shows the top IP addresses that are receiving potentially malicious traffic or data exfiltration attempts.
* **Intel Sources:** This section lists threat intelligence feeds used by the platform to detect known malicious indicators.
* **Distinct Alerts By Name:** Shows a list of unique alert rule names and their count.



* **Alert Listing:** The Alert Listing page provides a comprehensive view of all threat alerts detected.

# 

# AI/ML

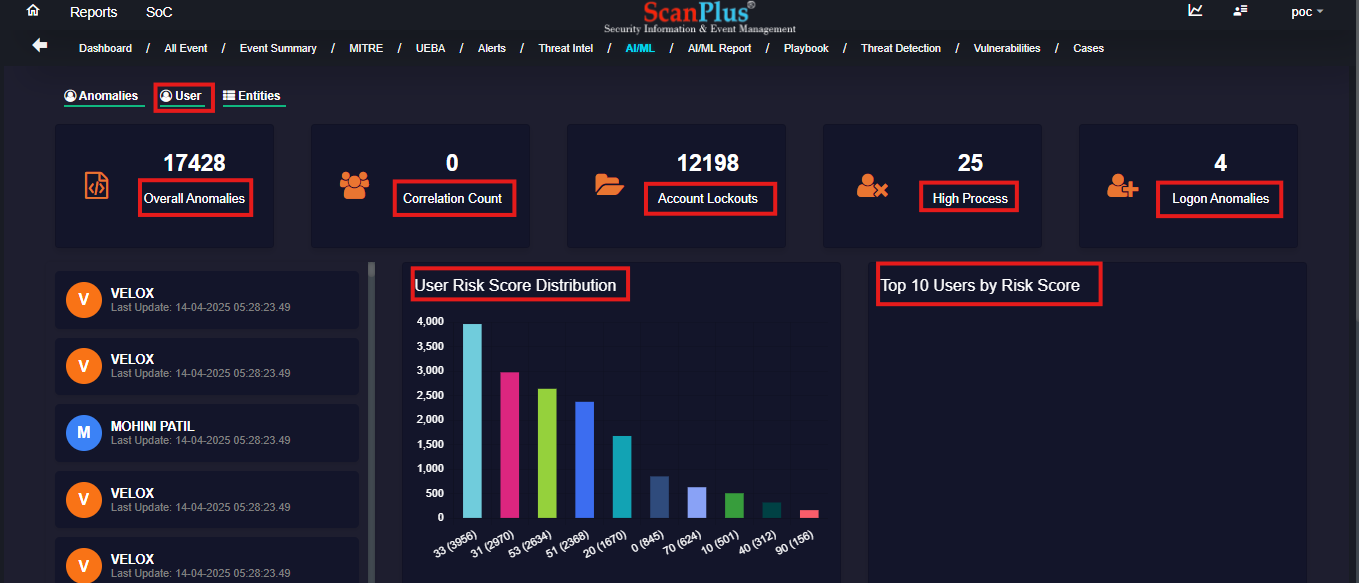
* **Anomalies**
* **Number Of Events Ingested:** This section displays total number of events ingested.
* **Anomalies Detected:** Total number of events flagged as suspicious or abnormal.
* **Tracking Users and Entities:** Number of users and entities associated with those anomalies.
* **Recent Anomalies:** This section provides a list of the most recent abnormal activities identified.
* **Anomaly Trend:** A line graph showing anomaly types (User Login Failed and User Login Success) and their corresponding anomaly counts.

# 

* **Top 10 Anomalous Activities:** A donut chart showing the most frequent types of anomalies.
* **Anomaly Trend:** A line graph showing anomaly types and their corresponding anomaly counts.
* **Anomaly Report Statistics:** Admin can view detail report of anomaly.
* **Top 10 Risky User:** This section displays users with the highest number of anomaly events, indicating higher risk.

# 

* **User**
* **Overall Anomalies:** This section displays total anomalies detected across all users.
* **Correlation Count:** Indicates the number of anomalies that were correlated across multiple users, systems, or data sources to identify a broader threat pattern.
* **Account Lockouts:** Reflects the total user account lockout events detected.
* **High Process:** Refers to abnormally high resource-consuming processes or unusual executable activity by users.
* **Logon Anomalies:** Events that signify suspicious or unexpected user login behavior.
* **User Risk Score Distribution:** Distribution of users by their aggregated risk scores.
* **Top 10 Users by Risk Score:** List of the most critical users based on cumulative anomaly impact.



* **Anomaly Trends:** A line or bar chart indicating the count of anomalous events detected.
* **Watchlisted Users:** Lists users who have been flagged due to consistent high-risk behaviour.
* **Top 10 Users by Risk Score Gain:** Displays the top 10 users who have shown the most significant increase in risk scores.

# 

* **Entities**
* **Entity Risk Score Distribution:** Displays the distribution of entities by risk score with Bar Chart.
* **Top 10 Entities by Risk Score:** Highlights the top 10 entities with the highest risk scores with Line Chart.
* **Anomaly Trends:** Indicates how many anomalies were detected during a specific period.

# 

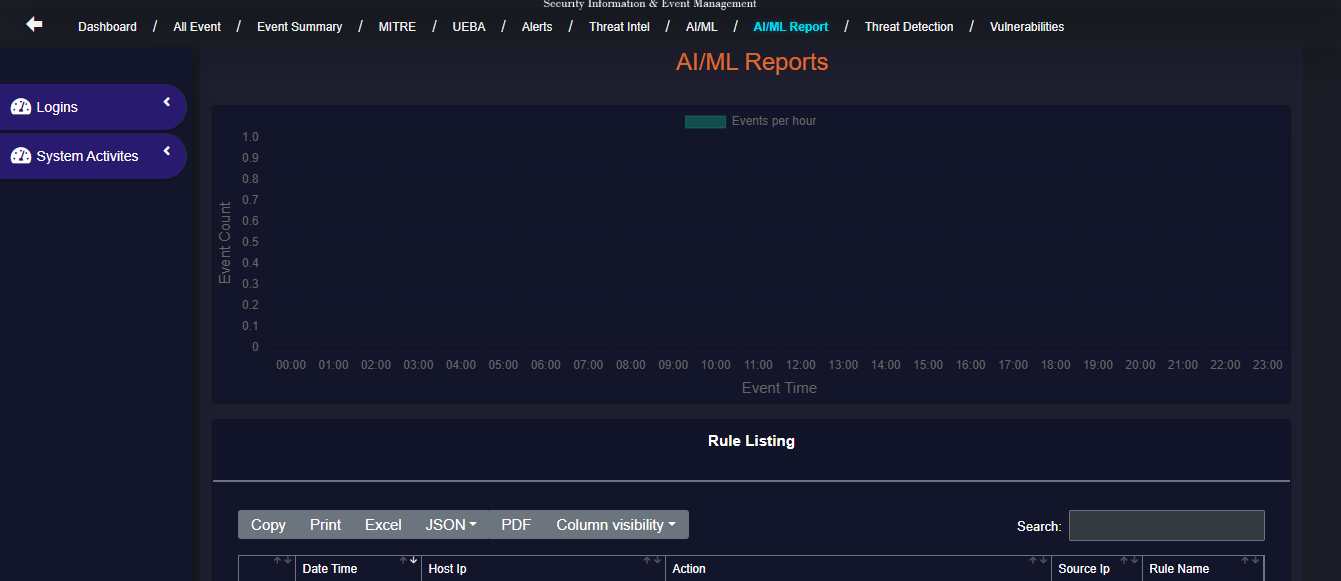
* **Watchlisted Entities:** Displays the list of entities that have been flagged for high-risk behavior based on AI/ML analysis.
* **Anomaly Trend:** This graph tracks the number of anomalies detected per month, helping visualize how entity-related risks have evolved over time.

# 

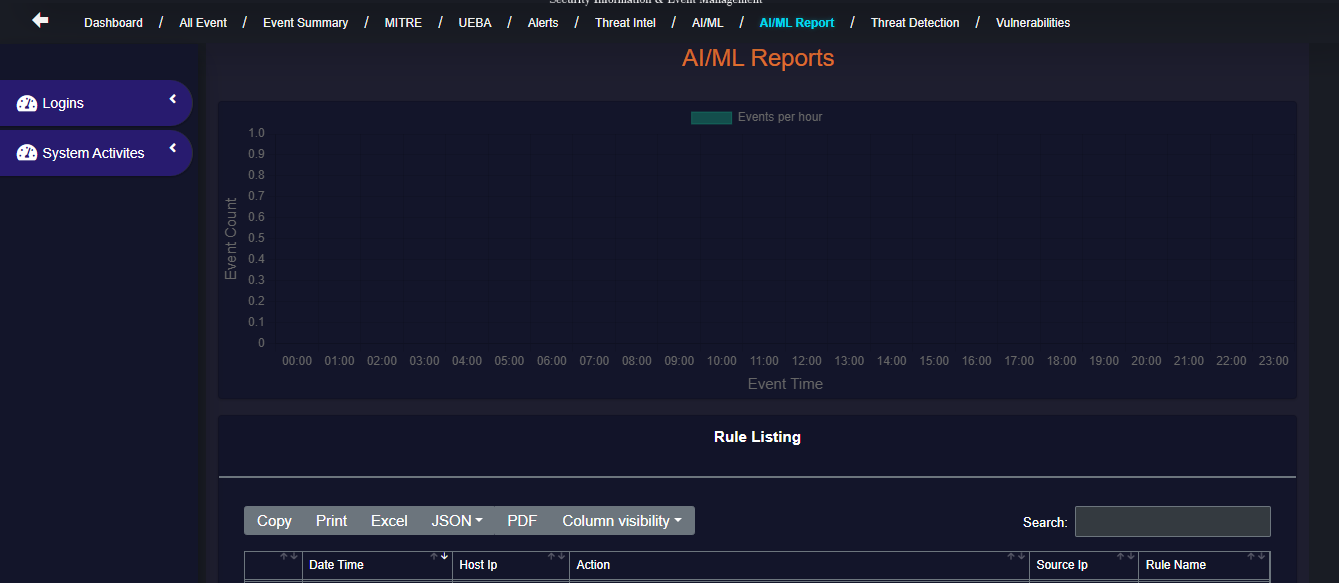
# AI/ML Reports

* **Logins**
* **Successful Logins:** Displays detailed analytics on successful login events, such as time-based trends and

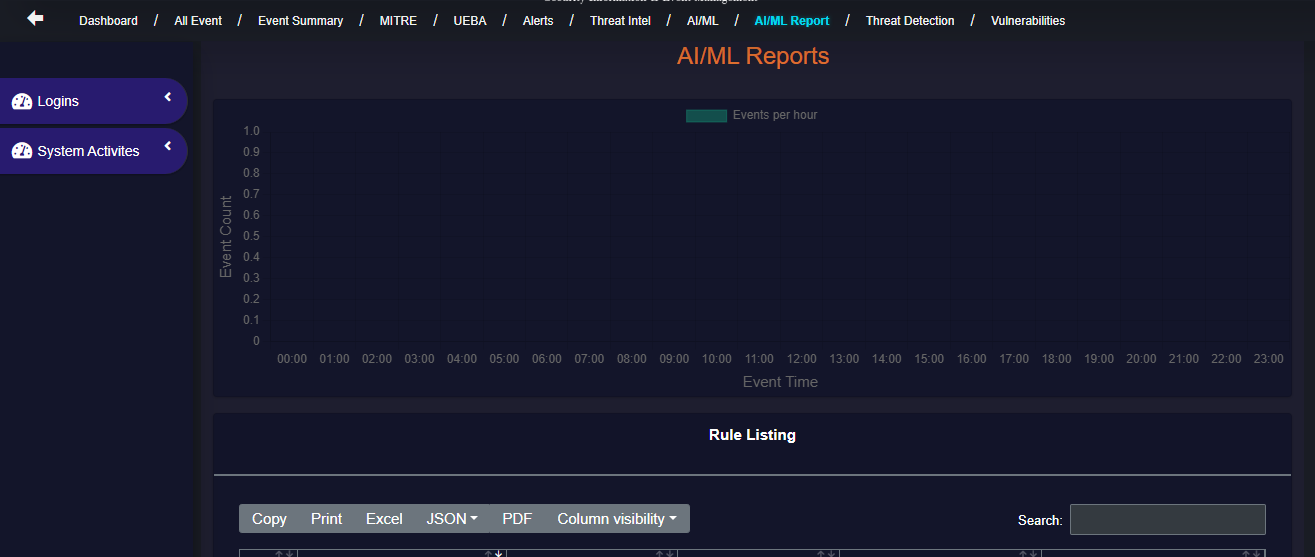
event counts.



* **Failed Logins:** Analyzed unsuccessful login attempts, helping detect anomalies and security threats.



* **System Activities**
* **Process Created:** Enables users to viewCreated process here.



* **Process Deleted:** Enables users to view Deleted process here.

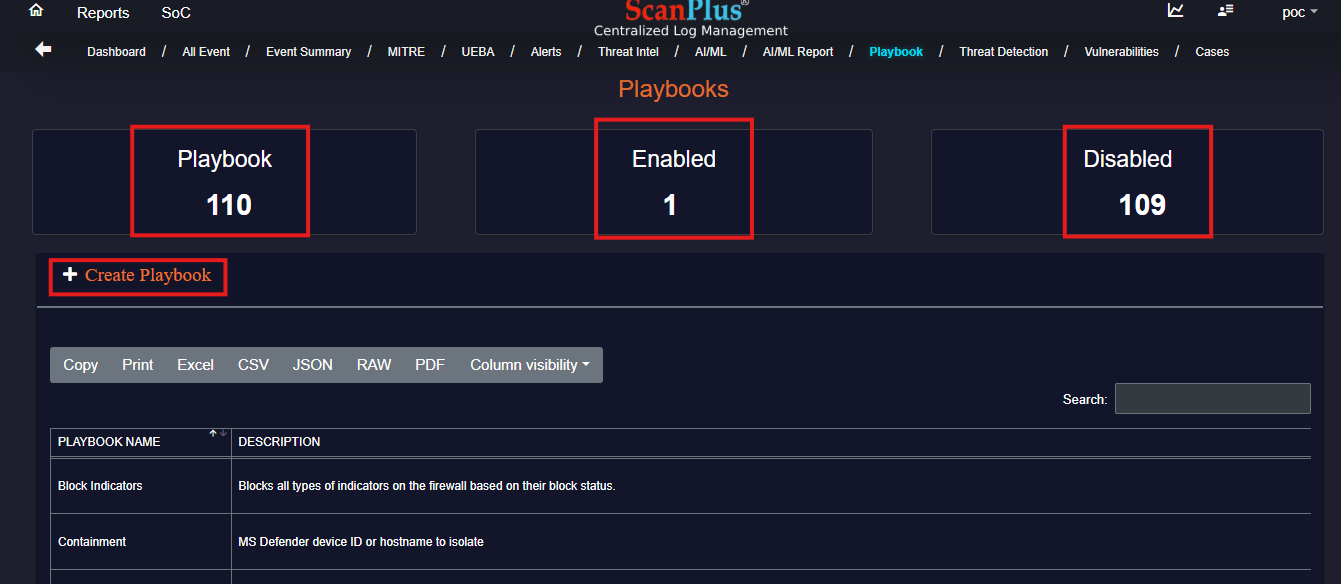
# 

# Threat Detection

# Threat Detection is the process of identifying malicious activities or threats (like malware, unauthorized access, insider threats, etc.) in a network, system, or application before they cause harm.

# Playbook

* **Playbook:** Total number of playbooks created.
* **Enabled:** Number of playbooks currently active and ready to execute.
* **Disabled:** Number of playbooks that exist but are currently turned off or inactive.
* **Create Playbook:** Button to initiate the creation of a new playbook.
* **Playbook Listing Table:** Table displays all available playbooks with relevant metadata.



# Vulnerabilities

* **Severity:** Displays the count of vulnerabilities by severity using ring chart.
* **IP Addresses:** Shows affected IP addresses and their distribution.
* **Vulnerability Table:**Table providing detailed data for each vulnerability.

# 

* **Assigned Ticket in ITSM:** Displays a list of tickets that have been automatically or manually raised in the IT Service Management (ITSM) module based on detected security alerts and vulnerabilities.

# 

# Insight Converter

# SIEM Dashboard Generator

# Here it will generate the different types of the charts like pie chart, bar chart, line chart, doughnut chart, radar chart etc.

# Here we can see all this types of details for below given 3 types.

# It has 3 different types…

# 1. Login Success/Failure

# 2. Severity Distribution

# 3. Attack Type Distribution

# 

# 

# 

# 

# 

# Cases

* **Rule Name:** Displays the Rule Name.
* **Severity:** Shows cases severity.
* **Assign Playbook:**Can select playbook to assign.
* **Playbook:** Playbook can be configured, not configured or undefined from here**.**

# 

# LOGOUT

User can Logout using below displayed option



Thank you for using our product. We hope this user manual has been helpful in guiding you through its features and functionalities. If you have any questions or require further assistance, please do not hesitate to contact our support team at **support@velox.co.in**

We are here to help!