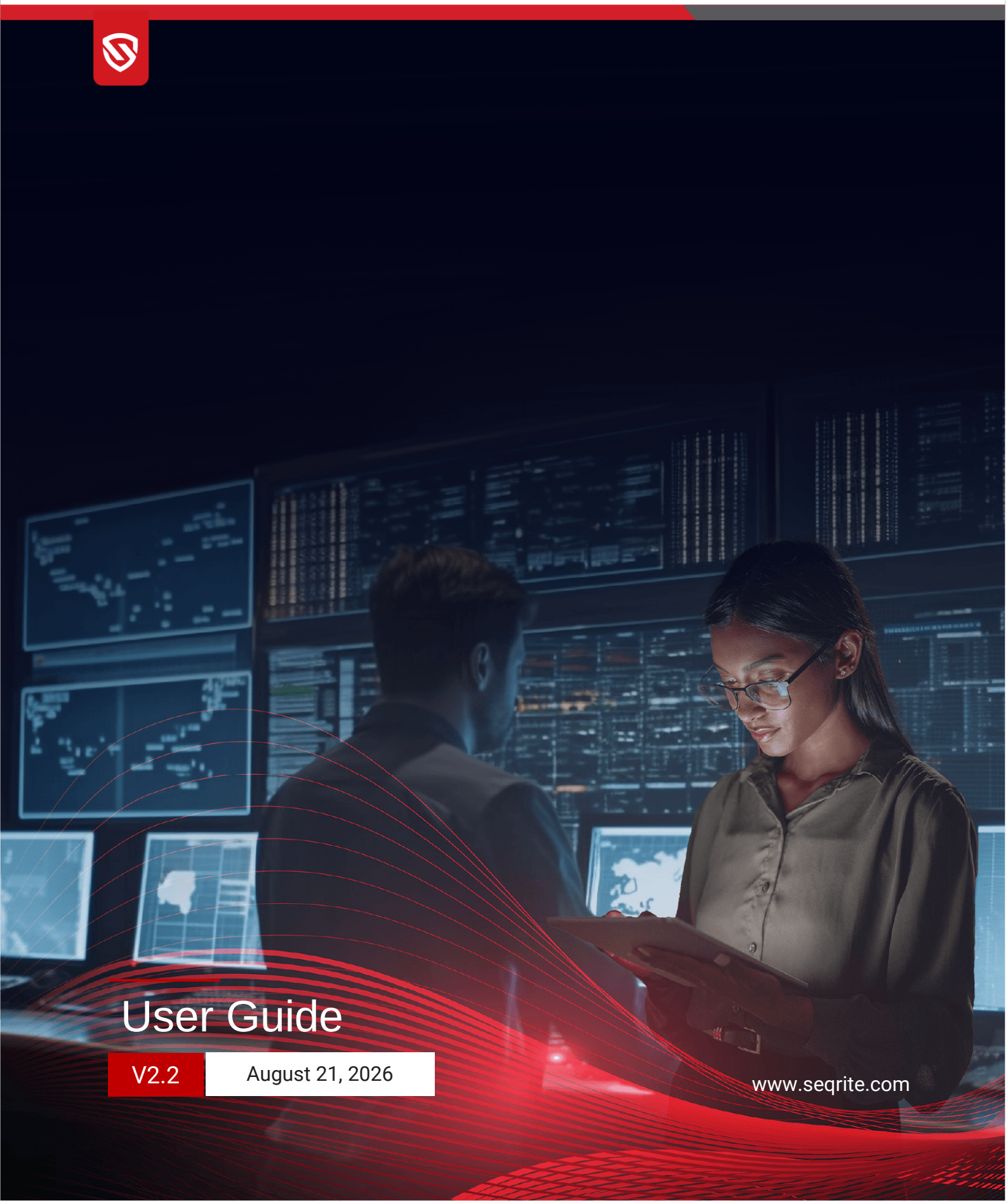
Seqrite Threat Intel

SEQRITE



User Guide

V2.2

August 21, 2026

www.seqrite.com

Copyright and License Information

Release Date
August 21, 2026

Contents

Version History

Doc Version	Date	Comment
1.0	March 12, 2025	Seqrite Threat Intel 1.0
1.1	March 25, 2025	Included section on Vulnerabilities and Adversaries along with other editorial and formatting edits.
1.2	April 25, 2025	Included section on Intel Submissions and support for STIX 2.0 file download format for Indicators, Adversaries and Vulnerability Intelligence along with other editorial and formatting updates.
1.3	May 20, 2025	Included section on Reports (RSS Feeds and Blogs) and Adversaries on Intrusion Sets (APT, Ransomware and Campaigns) and minor enhancements for improving usability.
1.4	October 10, 2025	• Seqrite Threat Intel is now accessible from Seqrite's Centralized Security Management Platform (CSM).
1.5	December 19, 2025	• STI - SMAP integration • Improved Intel submission workflow • Commercial feed for Enrichment
1.6	January 23, 2026	• Introduced sector–based IOC segregation
1.7	February 13, 2026	• IOC risk score life cycle is available to the users in the form of **graph** • Reports section is renamed to Cyber News
1.8	April 10, 2026	• Added support for bulk upload of IOCs • Added Multi-Factor Authentication (MFA) support • Added Forgot Password functionality • Duplicate IOC Submission Handling • Introduced **Audit Log** section to capture login, logout, and forgot password activities • Enhanced real-time IOC risk scoring • Support for STIX/TAXII 2.0 feed URL • Vulnerability Intelligence now displays severity scores according to CVSS 2.0, CVSS 3.x, and CVSS 4.0 standards • **Zero Day Vulnerabilities** are now displayed in the portal, and the tag is automatically removed once a patch is released

Doc Version	Date	Comment
1.9	August 21, 2026	• Users can now select and view any number of available columns across all configurable table views. • Enable support for IPv6 addresses in the IOC Value field for IP-type IOCs submitted through the Threat Intel Portal. • Users can now report an IOC as a **False Positive** directly within the portal by providing a reason for the report on the IOC Details page. • **Bulk Search API and License-Based Quotas** Introduced a new Bulk Search API that allows user to validate up to 1000 Indicators of Compromise (IOCs) in a single request. This update includes license-based daily quotas (resetting at 00:00 UTC) and a new **Search API** dashboard to track real-time usage and limits. • The data export limit has been increased from 5000 to 10,000 records across all modules, including Indicators, Adversaries, and Vulnerability Intelligence. • Introduced new **Target Sector** and **Target Country** multi-select filters to the Adversaries module. • NIST and CNA have been added as the primary sources of vulnerability information and scoring.

Introduction

Seqrite Threat Intel is a real-time threat intelligence solution that aggregates intel from various sources including QuickHeal's rich Telemetry. This Intel is further processed and disseminated over Seqrite Threat Intel Portal. It provides actionable insights tailored to industries like BFSI while ensuring compliance with regulatory requirements.

Seqrite Threat Intel 1.4 provides automated streams of useful threat information that enterprises can ingest into their security tools to block threats or derive helpful insights. This information includes traditional indicators of compromise (IOCs) such as malicious Domains, URLs, IP addresses, Malware hashes, Adversaries, Vulnerability Intelligence, Cyber Threats in the form of RSS Blogs, Intel sharing between all Tenant etc. Information related to all the threats are put together in STIX format and delivered to customers via the TAXII server.

Seqrite Threat Intel is powered by the Seqrite lab process and detects millions of threats every day. Information related to threats is messaged and put together in STIX format and delivered to customers via the TAXII server. The following page details how you can obtain Cyber Threat Intelligence (CTI) using the Trusted Automated Exchange of Intelligence Information (TAXII) services.

What is STIX?

- Structured Threat Information eXpression or STIX is a language format used to exchange CTI (Cyber Threat Intelligence). The STIX format is used to show information related to indicator objects, malware objects and relationship objects. Relationship objects link a common association between indicator and malware objects.
- The STIX feed is in a standardized JSON format and conveys CTI data that can be easily understood. It represents the common language where both entities client and server, can use STIX for a common method of communication.

What is TAXII?

- Trusted Automated Exchange of Intelligence Information or TAXII, is a transport protocol used to exchange CTI data over Hyper Text Transfer Protocol Secure (HTTPS).
- TAXII enables companies like Seqrite to share CTI with other users by defining an API that aligns with common sharing models.
- TAXII is specifically designed to support the exchange of CTI represented in STIX format.
- TAXII integration with security controls such as SIEM, SOAR, TIP, enables organizations to automate the sharing and consumption of threat intelligence, thereby enhancing their ability to detect, analyze, and respond to cyber threats.

The TAXII and STIX Relationship

- The open-source projects of TAXII and STIX standards were developed by the OASIS CTI Technical Committee for the prevention and mitigation of cyber-attacks. STIX indicates the cyber threat intelligence data and TAXII is the vehicle for the exchange of that information.
- TAXII is the mechanism for the transport of CTI represented in STIX format. You can use TAXII services to share cyber threat information in a secure and automated manner.

Relationship between Feeds and Collections

- As mentioned, STIX provides CTI data Feeds in JSON format. Feeds contain CTI data from various collections.
- A TAXII Collection is an interface to a database of CTI objects provided by a TAXII Server. It is used by TAXII Clients to request information from the TAXII Server.
- It is common to use the term Feeds when referring to STIX CTI threat data with the understanding that what comprises a CTI Feed is information from a Collection of CTI objects.

Cloud Deployment

The Seqrite Threat Intel now also operates as part of a cloud-based deployment through its integration with CSM **(Centralized Security Management)**.

Accessing the Seqrite Threat Intel

If you are an existing user follow the sign-in process using your credentials; if you are a new subscriber, complete the following three steps to get started.

A. Register with Seqrite Threat Intel/ Sign-Up with Seqrite Threat Intel
B. Set Password
C. Signing In

A. Register with Seqrite Threat Intel /Sign-Up with Seqrite Threat Intel

To access Seqrite Threat Intel, you must first register using a product key.
Note: You will receive the product key after signing the agreement and completing the milestone payment.
To register with Seqrite Threat Intel, follow these steps:

1. Enter the URL **https://csm.seqrite.com/csm/signup/sti** in the browser. The **Sign-Up** page is displayed.
2. Click **Register Here**.
   Register for Centralized Security Management page is displayed.
3. Select the **Threat Intel Product Key** checkbox, enter the product key, and click **Next**.
4. Enter the **Administrator Details** like First Name, Last Name, Business Email Address, Mobile No., Job Role, and click **Next**.
5. Enter the **Company Details** like, Company Name, Industry, Company Size, Country, State, City, Preferred Product Language, and click **Next**.
6. If the email address is incorrect, click **Click here to edit** to update the email address and click **Confirm**.

B. Set Password

Once you register successfully, you will receive an email with the activation link to set password. To set a password, follow these steps:

1. Click the activation link given in the email.
2. Enter password and click **Set Password**.
   The **Sign in** page is displayed.

C. Signing In

To access Seqrite Threat Intel, follow these steps:

1. Enter the email ID, password and click **Sign in**.
   The **Two- factor Authentication** page is displayed.
2. Enter the OTP you have received on your registered email address or registered phone number and click **Verify**.
   The **Seqrite Centralized Security Management License Agreement** page is displayed.
3. Agree with the terms of **SEQRITE END-USER LICENSE AGREEMENT** and click **Yes, I Agree.**
   The **Seqrite Centralized Security Management** dashboard is displayed.
4. Click **STI** on the left pane. The dashboard of Seqrite Threat Intel is displayed.

Forgot Password?

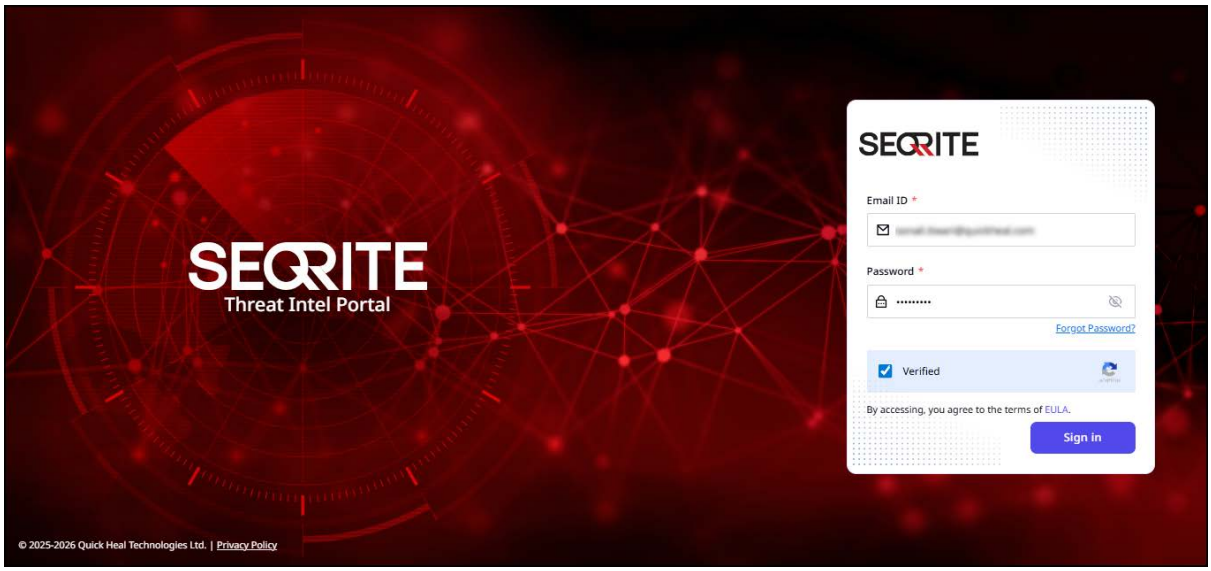
Follow these steps to reset your password:

1. Click **Forgot Password?** link on the **Sign in** page.
2. Enter your registered email ID, select the CAPTCHA checkbox and click **Recover**.
   Instructions for resetting the password will be sent to your registered email address.
3. Open the email with the subject line **Reset your password.**
4. Click **Set a new password** button provided in the email.
5. On the **Set Password** page, enter new password, confirm password and click **Set Password**.
6. Click **Go to Sign In!** and sign in with the new password.

On-Premises Deployment

Seqrite Threat Intel is a web-based application hosted in Customer premises.
To access this portal, follow these steps:

1. Go to **https://stip.seqrite.com/**.
2. On the **Sign In** page, login with the provided credentials.



3. Once authenticated, the user will land on the Dashboard.

Forgot Password?

Follow these steps to reset your password:

1. Click **Forgot Password?** link on the **Sign in** page.
2. Enter your registered email ID and click **Send Code**. The verification code/OTP will be sent to your registered email ID.
3. Enter the verification code and click **Verify Code**.
4. Enter new password, confirm password and click **Sign in**.
5. Click **Back to Login** and login with the new password.

Setting Up Organization and Analysts

An administrator sets up the organization's structure, assigns user roles, and can disable the account.

1. Setting up organization
   - Seqrite admin will create organizations within the portal.
   - Admins assign an Organization Admin for each created organization.
2. Adding Users
   - Organization Admins can add Analysts and assign roles such as:
     - Org Admin: Full access to manage the organization.
     - Org Analyst: Can view and analyse threat Intel data.
3. Disabling Accounts
   - Seqrite admins can disable organizations or specific analysts.
   - Seqrite Admin or Organization Admin can disable specific users of their organization.

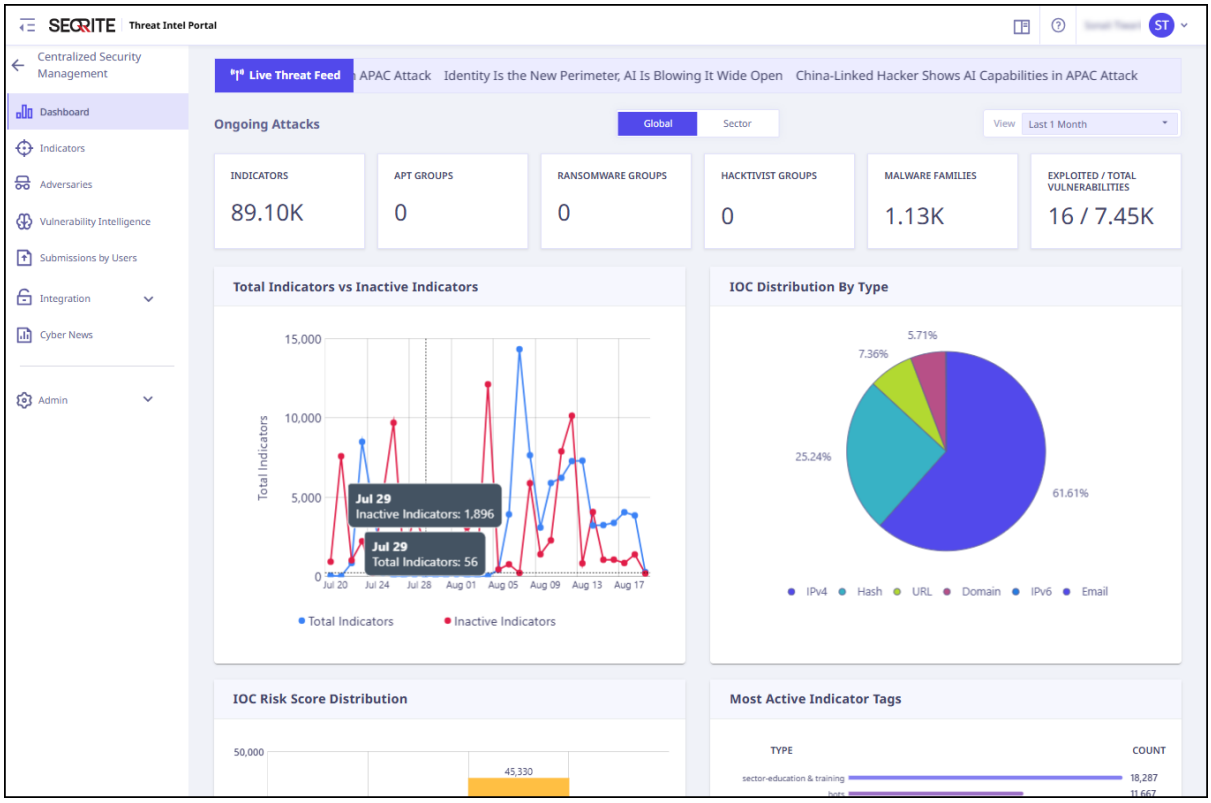
User Roles and Feature Access

The following table outlines the different user roles within Seqrite Threat Intel and their corresponding access permissions to various features.

Feature	**Org Admin**	**Org Analyst**
Dashboard	✅	✅
Indicator	✅	✅
Adversaries	✅	✅
Vulnerability Intelligence	✅	✅
Submissions By Users	✅	✅
Integration		
TAXII Details	✅	❌
Search API		
SMAP	✅	✅
Cyber News	✅	✅
Admin		
Add / View User	✅	❌
License	✅	❌
Audit Log	✅	❌

Dashboard

The dashboard is the default page that is displayed after you log on to the Seqrite Threat Intel portal. The dashboard helps to navigate easily to all the features or components of the Seqrite Threat Intel portal.



Dashboard Metrics

The dashboard gives a glimpse of predefined metrics related to Indicators of Compromise (IOC). Some (not limited to) pre-defined metrics are as follows.

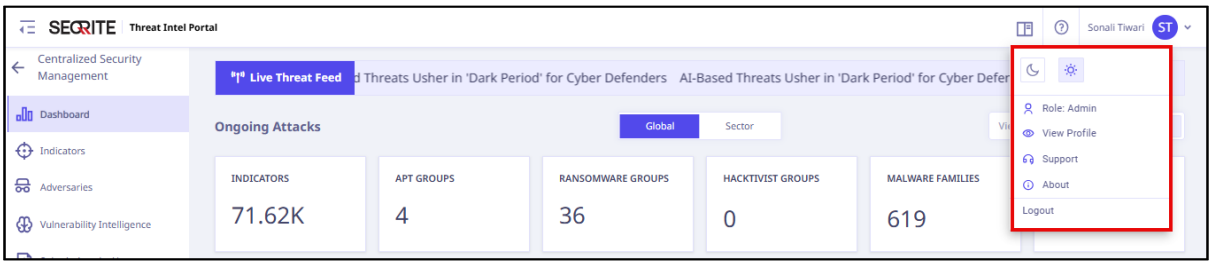
Section	Description
Live Threat Feed	Display all the latest Cyber Threat news reported from reputed and reliable sources.
Quick Statistics	Statistics on the Reported Indicators, APT Groups, Hacktivist Groups, Ransomware Groups, Exploitable CVEs.
Total Indicators vs Inactive Indicators	Timeline view of all reported active Indicators vs Inactive Indicators.
IOC Distribution by Type	It shows the breakdown of IOC by categories such as IPs, domains, or files.
IOC Risk Score Distribution	It gives visual representation of risk levels (low, medium, high) for detected IOC.
Most Active indicator Tags	Gives the type and count of the most active malware categories.

Section	Description
Top Products affected by CVEs	List of Products / applications which are most exploited by their vulnerabilities.
CVE Distribution by Severity	Distribution of all reported vulnerabilities based on their CVSS score as Critical, High, Medium and Low.
APTs (Advnaced Persistent Threats)	APTs (Advnaced Persistent Threats). Shows the top 10 active most targeted by APTs, top 10 sectors most targeted by APTs, and their top 10 victim distribution across globe.
Ransomware Groups	Displays the top 10 Ransomware Groups, top 10 sectors targeted by Ransomware, and their top 10 victim distribution across the globe.
Hacktivist Groups	Displays top 10 targeted Hacktivist, top 10 sectors targeted by hacktivist, and their top 10 victim distribution across the globe.
Malware	Displays top 10 trending malware category, top 10 trending malware families, and malware threat activity.
Top 10 Organizations targeted by Adversaries	Top 10 Organizations which are targeted by Adversaries.
Top 10 Sectors targeted by Adversaries	Top 10 Sectors which are targeted by Adversaries.
Top 10 Adversary Techniques	Top 10 techniques used by Adversaries to carry out a Cyber-attack.
Latest Adversaries	Shows recently active or newly observed threat actors.

All the above metrics on the Dashboard can be filtered to view Global Intel or Sector specific Intel.

User Profile

The User Profile section on the upper-right corner of the dashboard shows the name of the registered user and following options:



Role
Displays the role assigned to your user account.

View Profile
Displays your profile information, including:

- First Name
- Last Name
- Email
- Organization
- Sectors: The sectors associated with your organization.
- Switch to UTC: Controls how date and time values are displayed across the portal. When enabled, supported timestamps are displayed in UTC, when disabled, timestamps are displayed based on your local time zone settings.

Support
Provides access to support resources and assistance.

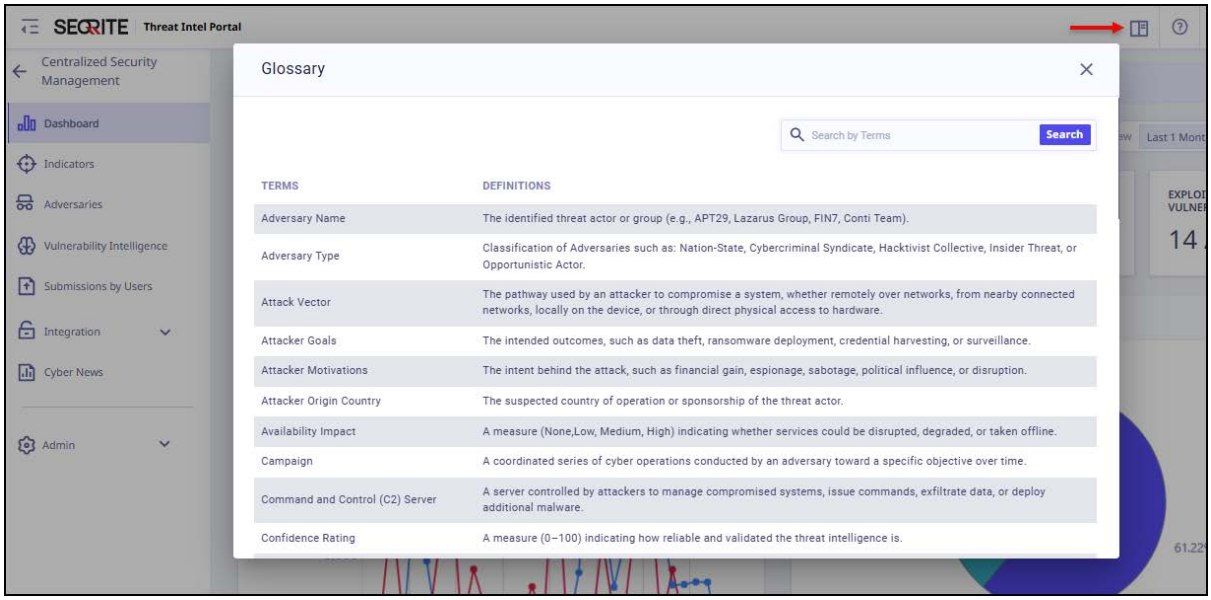
About
Displays information about the platform, including the current version, End User License Agreement (EULA), Privacy Policy, Legal Notices, and Open Source Compliance details.

Logout
Signs you out of the portal.

Theme Selection
Use the Dark Theme and Light Theme icons to switch between the available display themes.

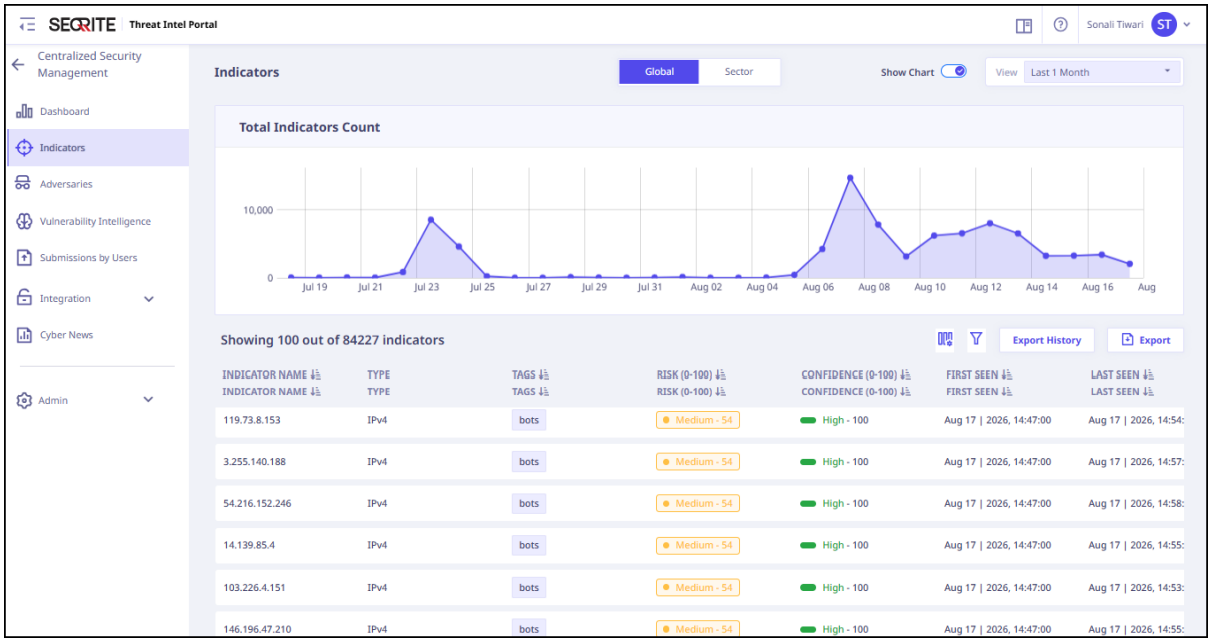
Glossary

Glossary provides clear definition of key terms and phrases used throughout the Seqrite Threat Intel. It helps users to understand words and concepts related to cyber threats, attacks, and security.



Indicators

The **Indicators** tab provides a detailed overview of all newly detected IOCs. IOC includes IP addresses, domain names, file hashes, and URLs that can be used to detect malicious activity. These indicators help to detect, analyse and respond to cyber threats effectively.



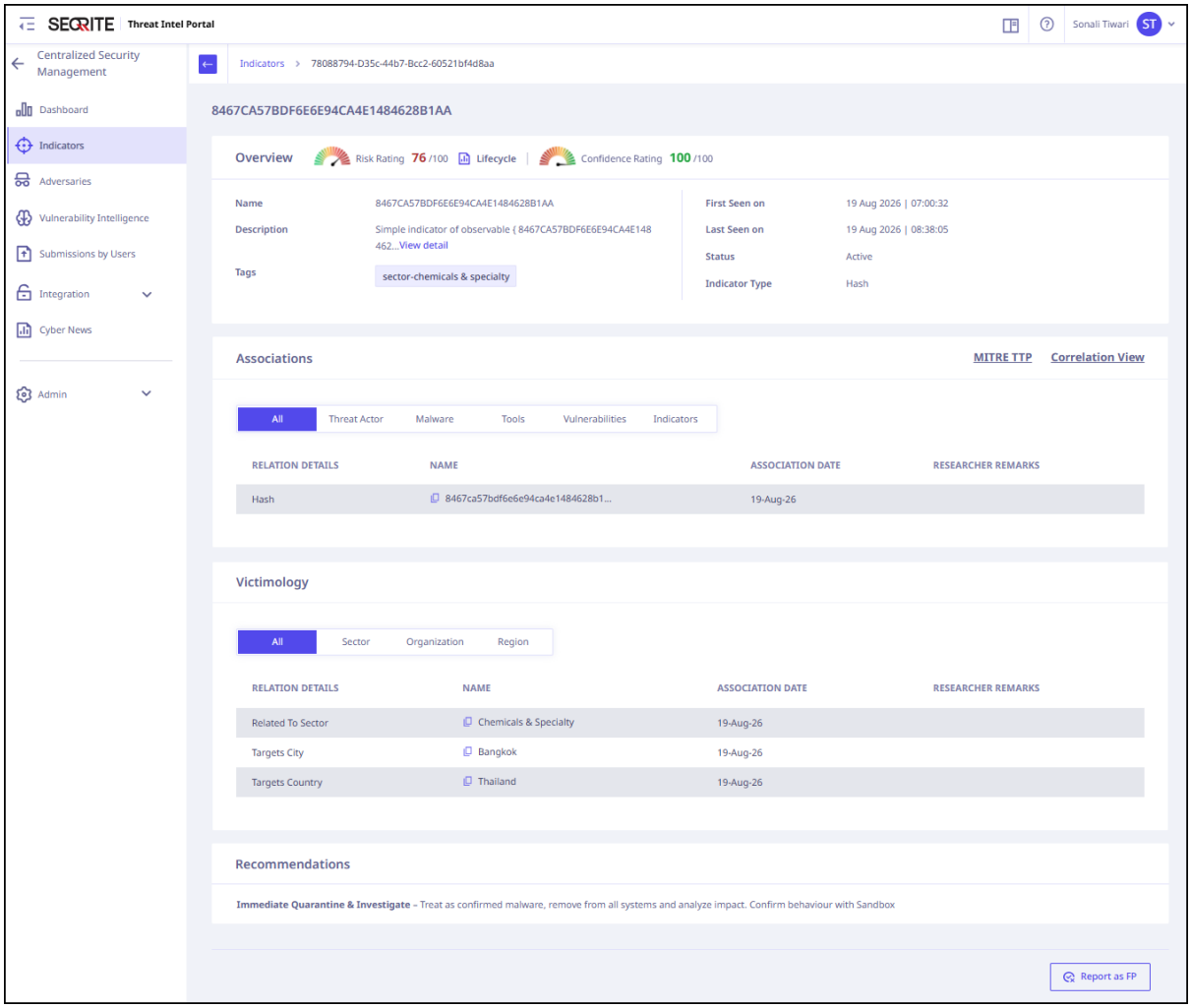
The **Indicators** tab provides graphical and tabular presentation of global and sector specific IOC. You can view the IOC details and filter the IOC chart by specific date range that is last 1 day, last 7 days, last 1 month, last 3 months, last 1 year, and can select a custom date range as well.

Viewing the IOC Details

You can view the IOC details such as description or IOC name, type of IOC, ratings, and first and last seen in the tabular format.

To view the details of each IOC:

1. On the Seqrite Threat Intel portal, click **Indicators** in the left pane.
2. On the **Indicators** page, select the indicator and click the **>** icon.
   The indicator details page displays the following details:



- **Indicator Overview**: Risk score, confidence score, and the description of the IOC.
- **IOC Risk Score Lifecycle:** The lifecycle of an IOC's risk score is now made available to the users in form of a graph**.**
- **Attributes**: Key properties such as source, detection date, type. Incase if IOC type as IP address we can get additional attributes such as Country, City, ASN, Geolocation, Hostname, Registrant Information, Open Ports by leveraging enrichment connectors.
- **TTP Mappings**: Links to tactics, techniques, and procedures associated with the IOC.
- **Associations**: Known relations with Threats Actors, Malware or IOCs.
- **Victimology**: Victimology is the study of who attackers target, helping analysts understand patterns across victims, such as industries, and regions.
- **Recommendations:** Recommended action for selected IOC.

Selecting Column from the Column Selector

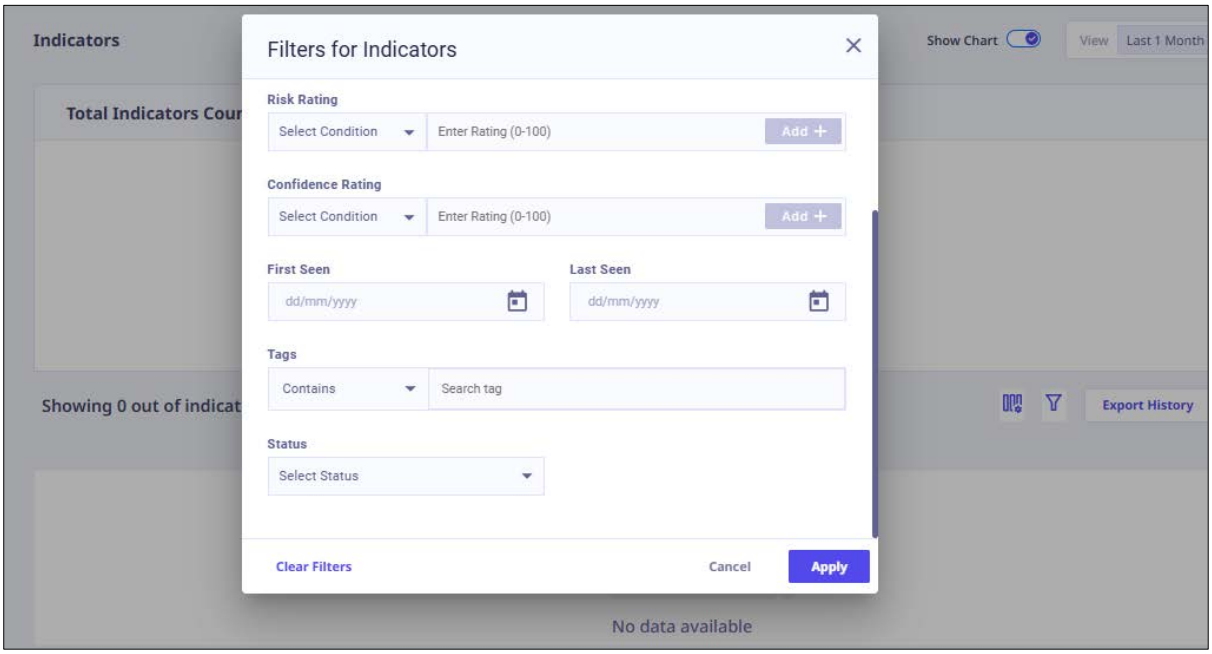
The Column Selector allows you to customize the table view. You can choose the desired column to display on a table.

- To choose columns, click on the **Indicators** page, and select the desired column.

Filtering the IOC List

You can filter the IOC list to refine results based on attributes or categories.
To filter the IOC list, follow these steps:

1. On the Seqrite Threat Intel portal, click **Indicators** in the left pane.
2. On the **Indicators** page, click .



3. Enter the attribute that is indicator name, type, risk ratings, confidence rating, first seen date, last seen date, tags, status (active/inactive), and click **Apply**.
   The system displays filtered data.

Exporting IOC as a CSV/STIX

You can download all IOCs currently visible on the page in the CSV or STIX format.
To export/download the IOCs:

1. On the Seqrite Threat Intel portal, click **Indicators** in the left pane.
2. On the **Indicators** page click **Export**, select the format that is CSV or STIX 2.1, and then click **Export**.

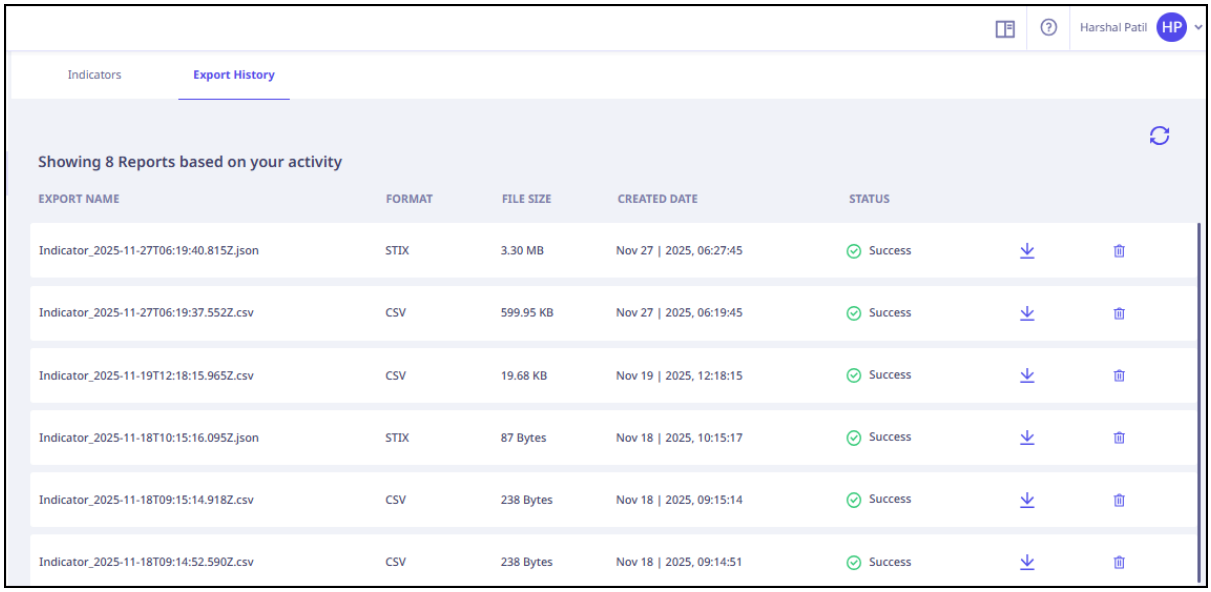
Viewing IOC Export History

Export History shows a record of all the Indicators of Compromise (IOCs) that have been exported by the user.

Export History provides a record that is export name, format (STIX or CSV), file size, created date, and status.

- To view the export history, either click **Export History** on the **Indicators** page.

The list of exported IOCs is displayed.

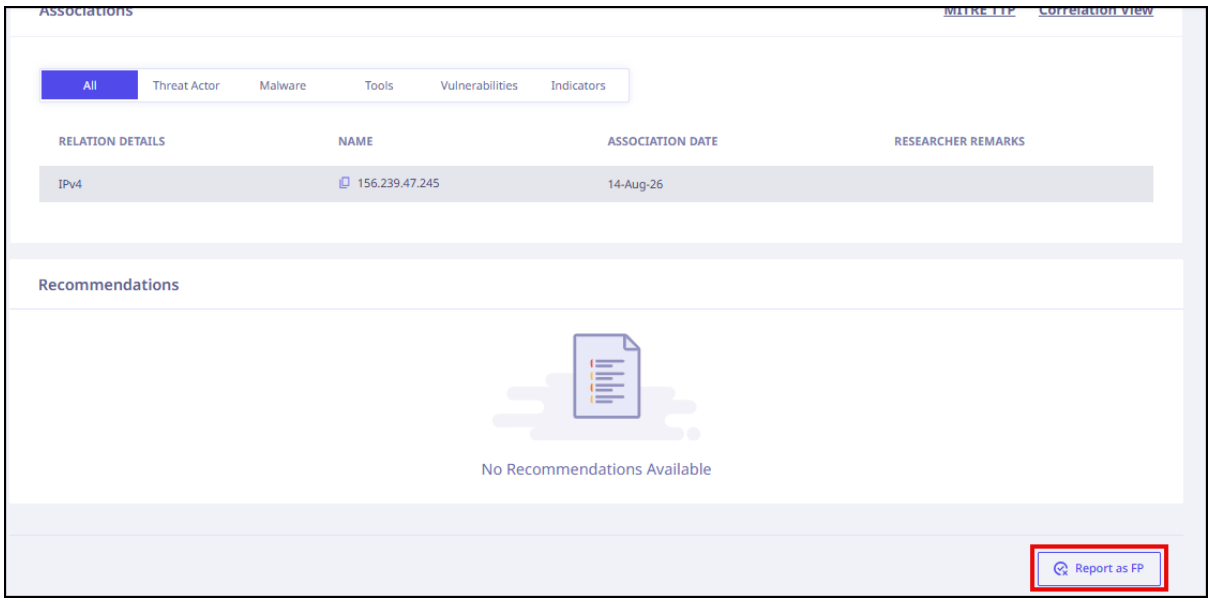


Reporting False Positive for IOCs

A **False Positive** occurs when a safe file, IP address, or domain is mistakenly identified as a threat (Indicator of Compromise). Reporting false positives helps improve threat detection accuracy and prevents safe items from being incorrectly blocked.

If you believe an IOC in the portal is incorrect, you can report it directly from the Seqrite Threat Intel interface.
To report the false positive for IOC, follow these steps:

1. On the Seqrite Threat Intel portal, click **Indicators** in the left pane.
2. On the **Indicators** page, select the indicator and click the **>** icon.
3. Click **Report as FP**.



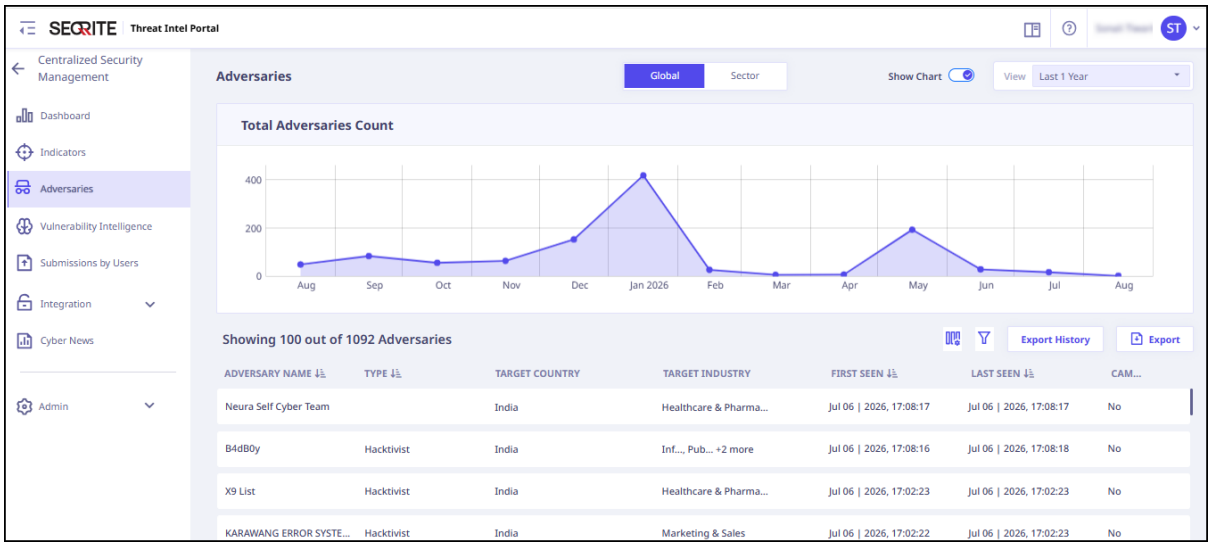
4. Enter the reason for reporting the indicator as a false positive and click **Submit**.

The system will send an email notification to the Seqrite's team with the relevant IOC and reporter details for review and validation.

Adversaries

An Adversary is any individual or a group that attempts harmful activities like cyber-attack or spying to threaten cyber resources.

The **Adversaries** tab gives information about the detected adversaries. Adversary details include adversary names, type, target country, target industry, first seen and last seen. These adversary details help to detect, analyse and respond to cyber threats effectively.

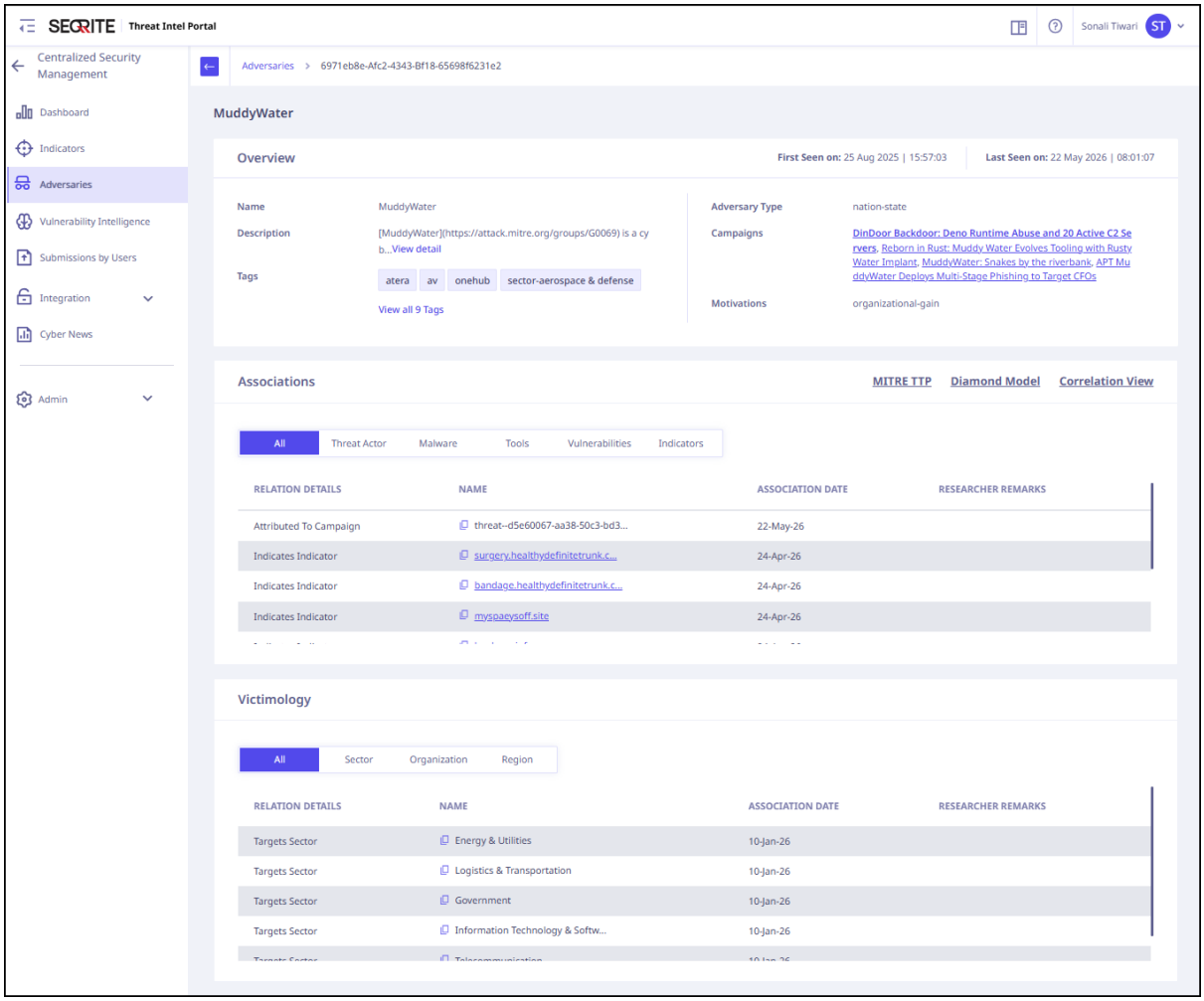


This intel offers a comprehensive view of threat actors, including their tactics, techniques, and associations. It helps in understanding attacker motives, targeted regions and targeted sectors. Organizations can use this intelligence to anticipate attacks and enhance threat-hunting capabilities.

Viewing the Adversary Details

You can view the adversary details such as adversary name, type, target country, target industry, first and last seen in the tabular format. To view the details of each adversary, follow these steps:

1. On the Seqrite Threat Intel portal, click **Adversaries** in the left pane.
2. On the **Adversaries** page, select the adversary and click the **>** icon.
   The adversary details page displays the following details:



- **Adversary Overview**: Adversary Name, Target Country, Target City, Target Sector, Attack Origination, Goals, Motivations, First Seen and Last Seen.
- **TTP Mappings**: Links to tactics, techniques, and procedures associated with the adversary.
- **Associations**: Known relations with Threats Actors, Malware, Tools, Vulnerabilities and IOCs.
- **Victimology**: Victimology is the study of who attackers target, helping analysts understand patterns across victims, such as industries, and regions.

Selecting Column from the Column Selector

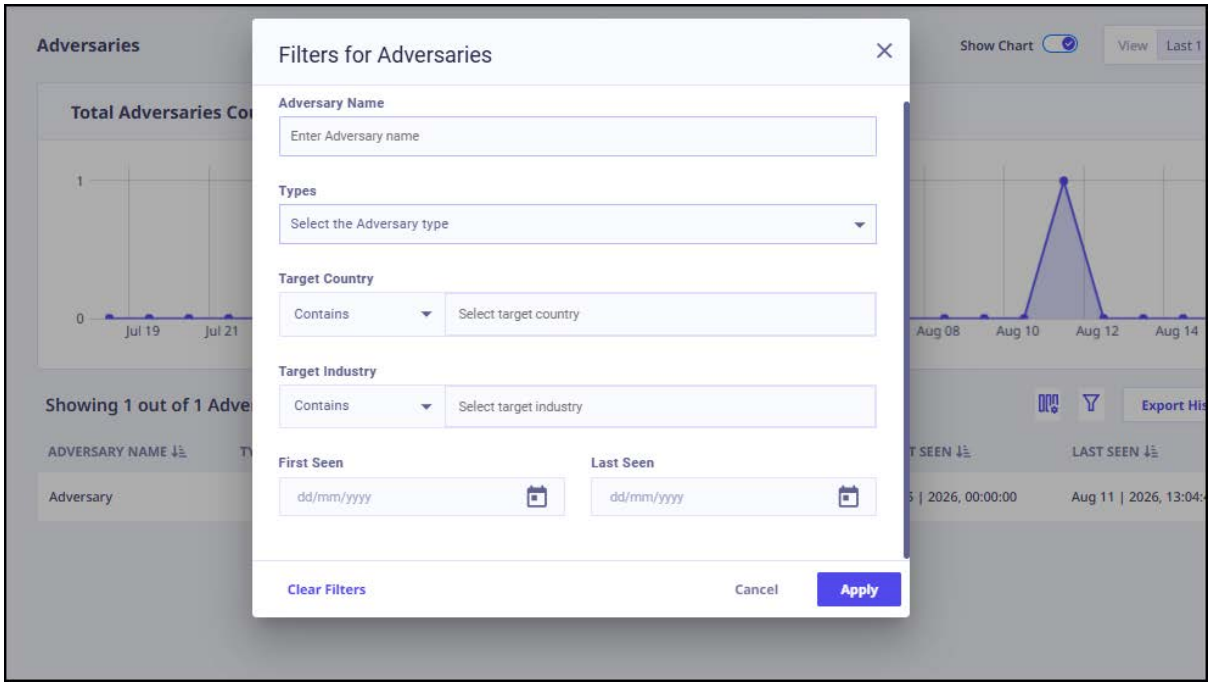
The Column Selector allows you to customize the table view. You can choose the desired column to display on a table.

- To choose columns, click  on the **Adversaries** page and select the desired column.

Filtering the Adversary List

You can filter the adversary list to refine results based on types.
To filter the adversary list, follow these steps:

1. On the Seqrite Threat Intel portal, click **Adversaries** in the left pane.
2. On the **Adversaries** page click .
3. Enter the attribute that is adversary name, type, target country, target industry, first seen date, or the last seen date, and click **Apply**.



The system displays filtered data.

Exporting Adversaries as a CSV/STIX

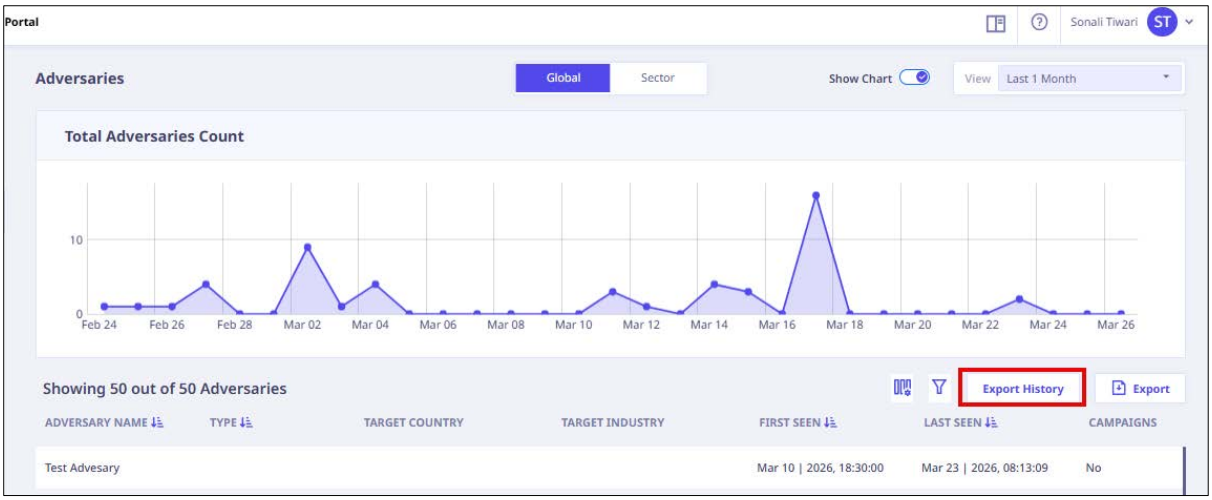
You can download all adversaries currently visible on the page in the CSV or STIX format.
To export/download the adversaries, follow these steps:

1. On the Seqrite Threat Intel portal, click **Adversaries** in the left pane.
2. On the **Adversaries** page click **Export**, select the format that is CSV or STIX 2.1, and then click **Export.**

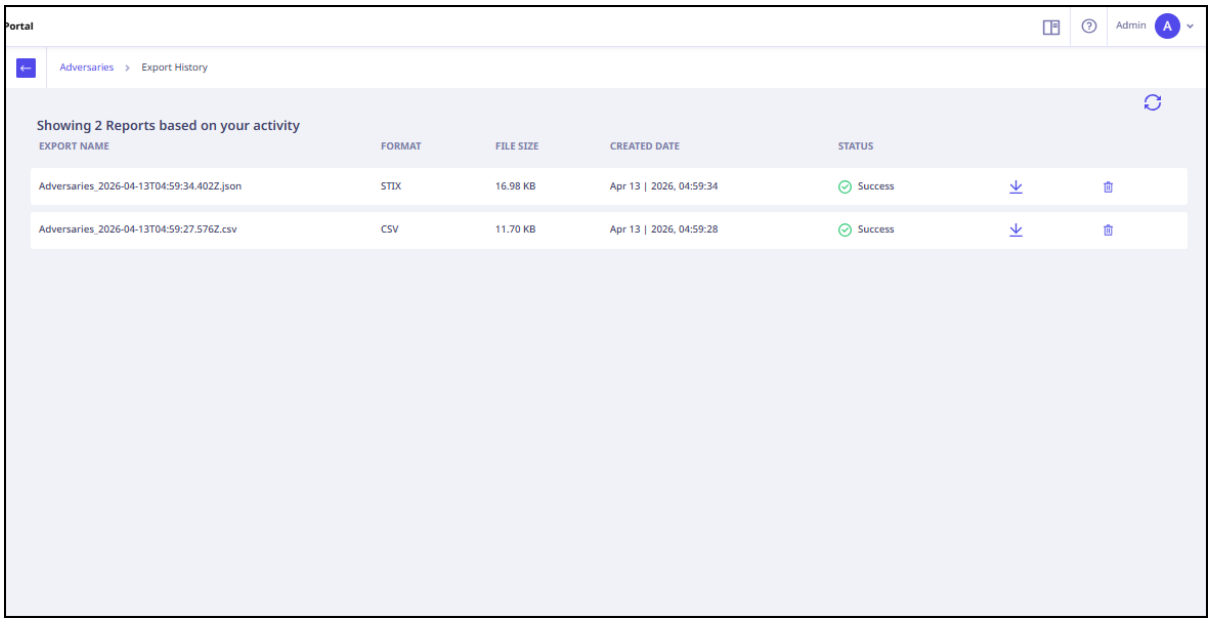
Viewing Adversary Export History

Export History shows a record of all the adversaries that have been exported by the user. Export History provides a record that is export name, format (STIX or CSV), file size, created date, and status.

- To view the export history, click **Export History** on the **Adversaries** page.

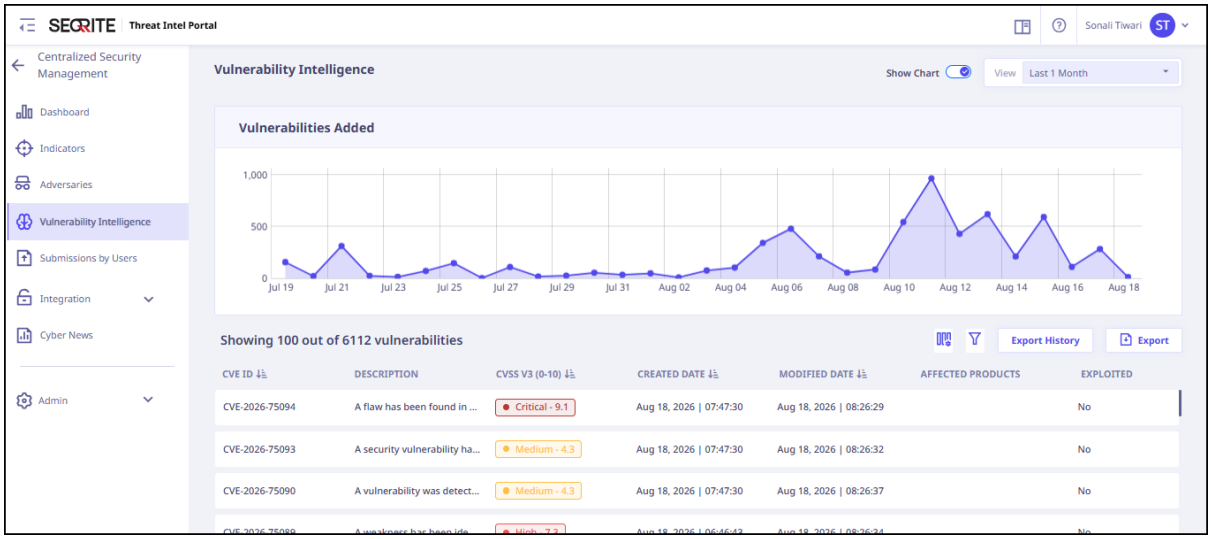


The list of exported adversaries is displayed.



Vulnerability Intelligence

Vulnerability intelligence provides insights into newly discovered vulnerabilities, including severity, exploitability, and affected systems. It includes patch details, associations with known threats. This helps organizations proactively mitigate security gaps and strengthen their defenses.



The **Vulnerability Intelligence** tab provides graphical and tabular presentation of detected vulnerabilities. You can view the vulnerability details and filter the vulnerability chart by specific date range that is last 1 day, last 7 days, last 1 month, last 3 months, and last 1 year.

Viewing the Vulnerability Details

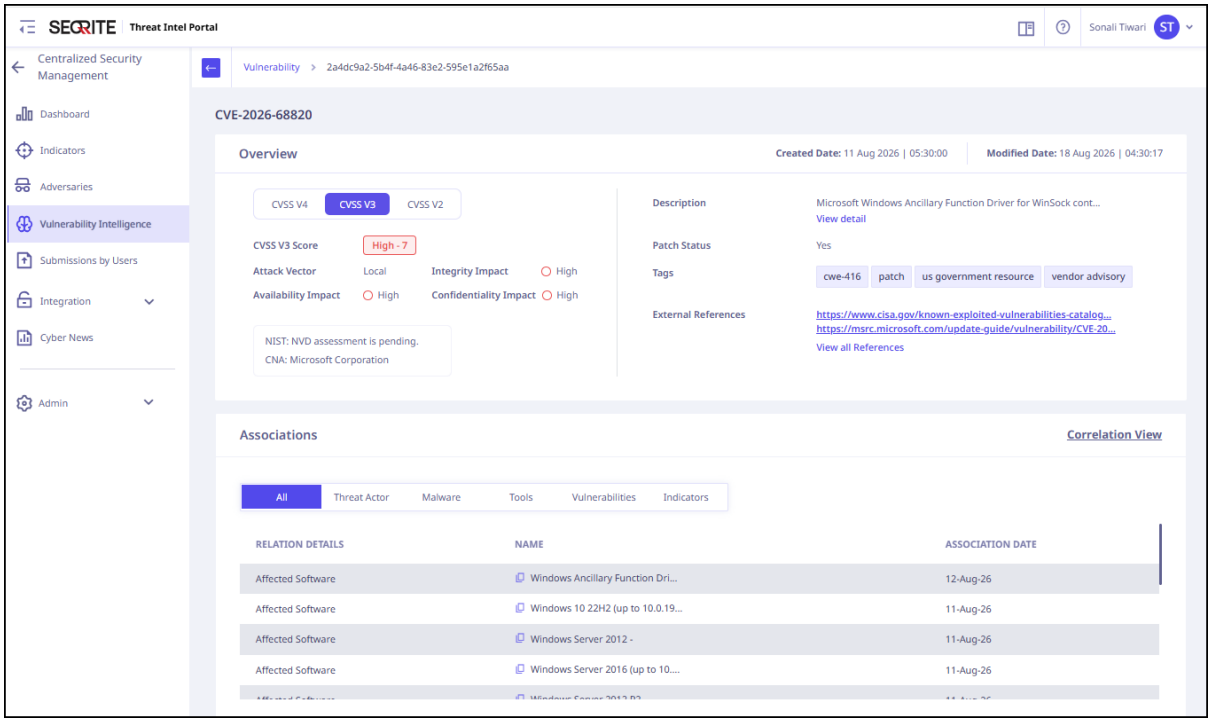
You can view the vulnerability details such as CVE ID, description, created date, modified date, CVSS2.0, CVSS3.0, CVSS3.1 and CVSS4.0 scores, confidence and exploited in the tabular format. You can filter and find the Vulnerabilities against the controls/products used in your organization.

Note:

- Vulnerabilities shown along with the icon are **Zero Day Vulnerability**. Once a patch is released, the **Zero Day** designation is removed from vulnerability.
- A vulnerability is classified as a **Zero-Day Vulnerability** until a patch is released and it remains actively exploitable, regardless of how much time has passed since its discovery.

To view the details of each vulnerability, follow these steps:

1. On the Seqrite Threat Intel portal, click **Vulnerability Intelligence** in the left pane.
2. On the **Vulnerability Intelligence** page, select the vulnerability and click the **>** icon. The vulnerability details page displays the following details:



- **Overview**: CVE Name/ID, Description, Tags, Attack Vendor, CVSS 2.0, CVSS 3.x, CVSS 4.0, Attack Vector, Description, Patch Status, affected products, risk score, External References, Confidentiality, Integrity, Availability (CIA) Impact, and NIST and CNA represent the sources of data.
- **Associations**: Known relations with Malware, IOCs or Threat Actors as well as techniques and procedures associated with exploiting the vulnerability.

Selecting Column from the Column Selector

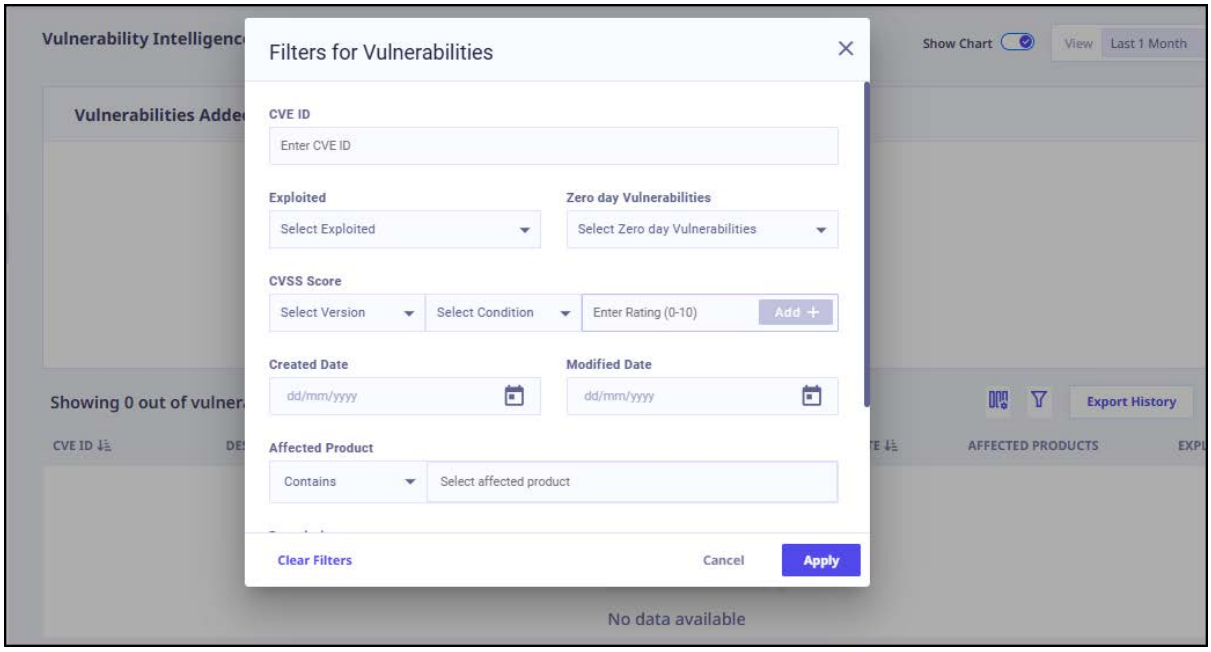
The Column Selector allows you to customize the table view. You can choose the desired column to display on a table.

- To choose columns, click on the Vulnerability Intelligence page, and choose the desired column.

Filtering the Vulnerability List

You can filter the vulnerability list to refine results based on CVSS V3 score or confidence ratings.
To filter the vulnerability list, follow these steps:

1. On the Seqrite Threat Intel portal, click **Vulnerability Intelligence** in the left pane.
2. On the **Vulnerability Intelligence** page click .
3. Enter the details that are, CVE ID, description, CVSS V3 score, confidence rating, created date, modified date, exploited, and then click **Apply**.



The system displays filtered data.

Exporting Vulnerabilities as a CSV/STIX

You can download all the vulnerabilities currently visible on the page in the CSV or STIX format.

To export/download vulnerabilities, follow these steps:

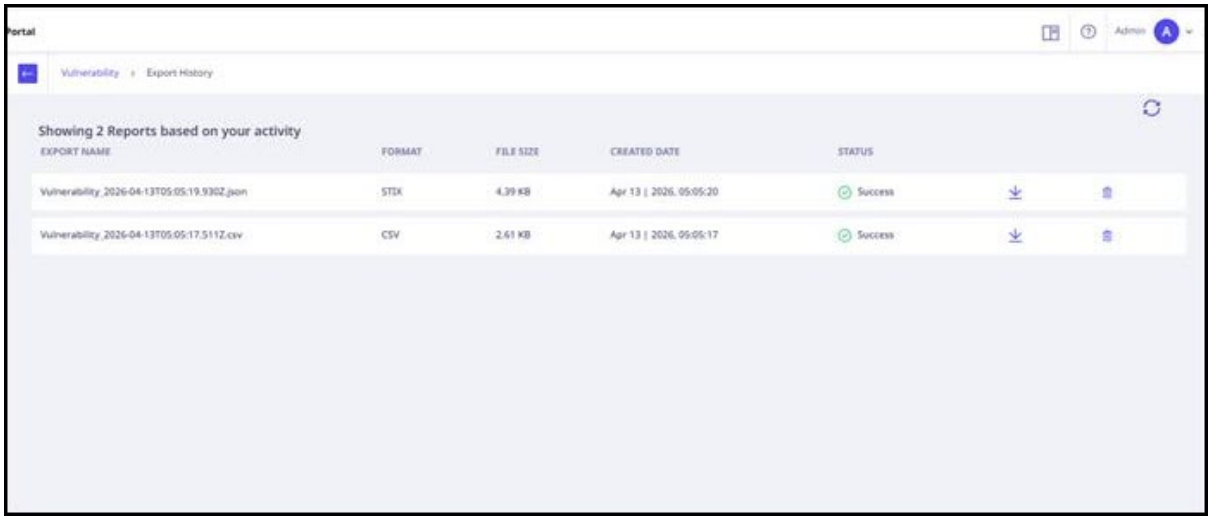
1. On the Seqrite Threat Intel portal, click **Vulnerability Intelligence** in the left pane.
2. On the **Vulnerability Intelligence** page click **Export**, select the format that is CSV or STIX 2.1, and then click **Export**.

Viewing Vulnerability Intelligence Export History

Export History shows a record of all the vulnerabilities that have been exported by the user. Export History provides a record that is export name, format (STIX or CSV), file size, created date, and status.

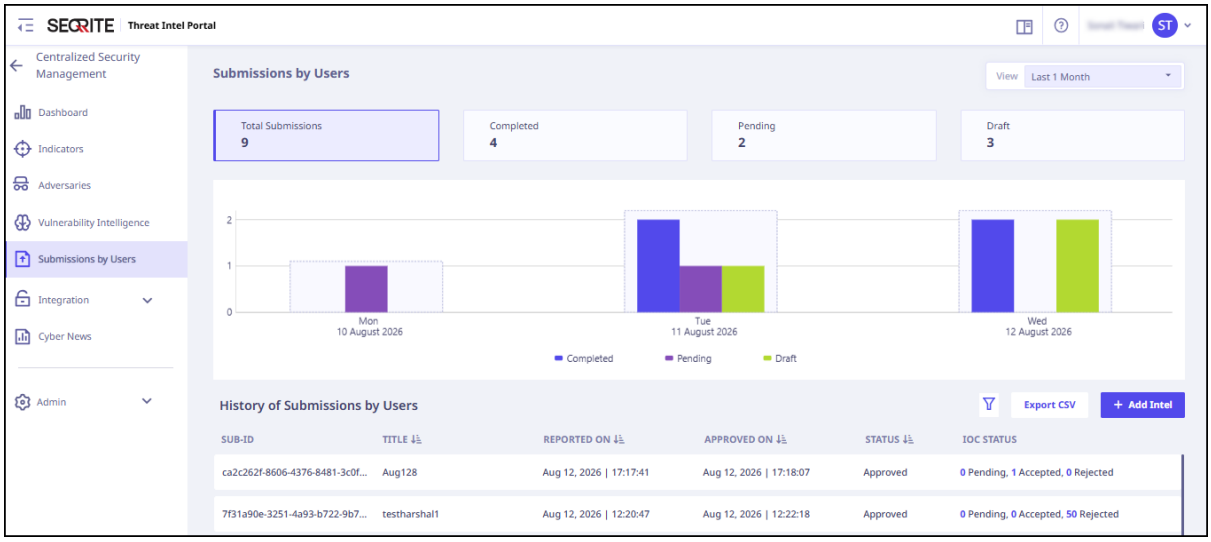
- To view the export history, click **Export History** on the **Vulnerability Intelligence** page.

The list of exported vulnerabilities is displayed.



Submissions by Users

Intel Submissions is the process of adding or sharing new threat intelligence data such as, IOCs, tactics, techniques, procedures, threat actors, malware signatures, or vulnerability details for analysis, correlation, and distribution. This helps to detect, investigate, and respond to threats more effectively. You can submit suspicious IOCs. These IOCs will be shared with the community post verification.



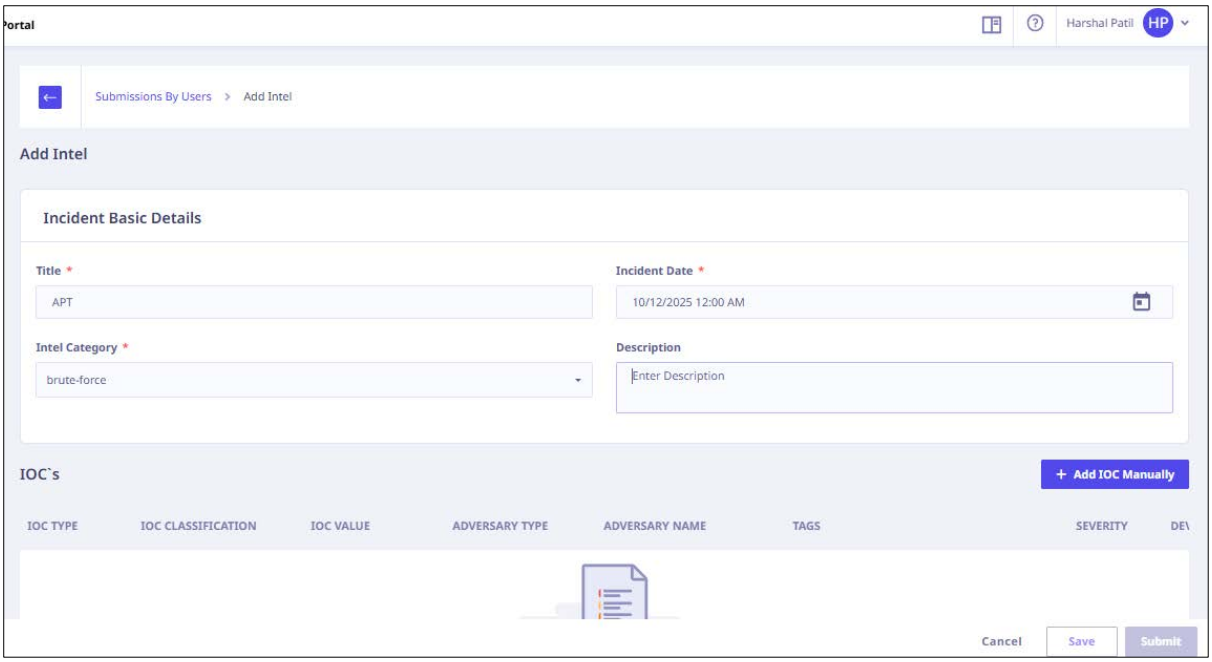
The **Submissions by Users** tab help you to view and analyze all the incoming intel. You can view the submitted intel details, their severity (critical, high, medium, low) and filter the intel by specific date range that is last 1 day, last 7 days, last 1 month, last 3 months, and last 1 year.

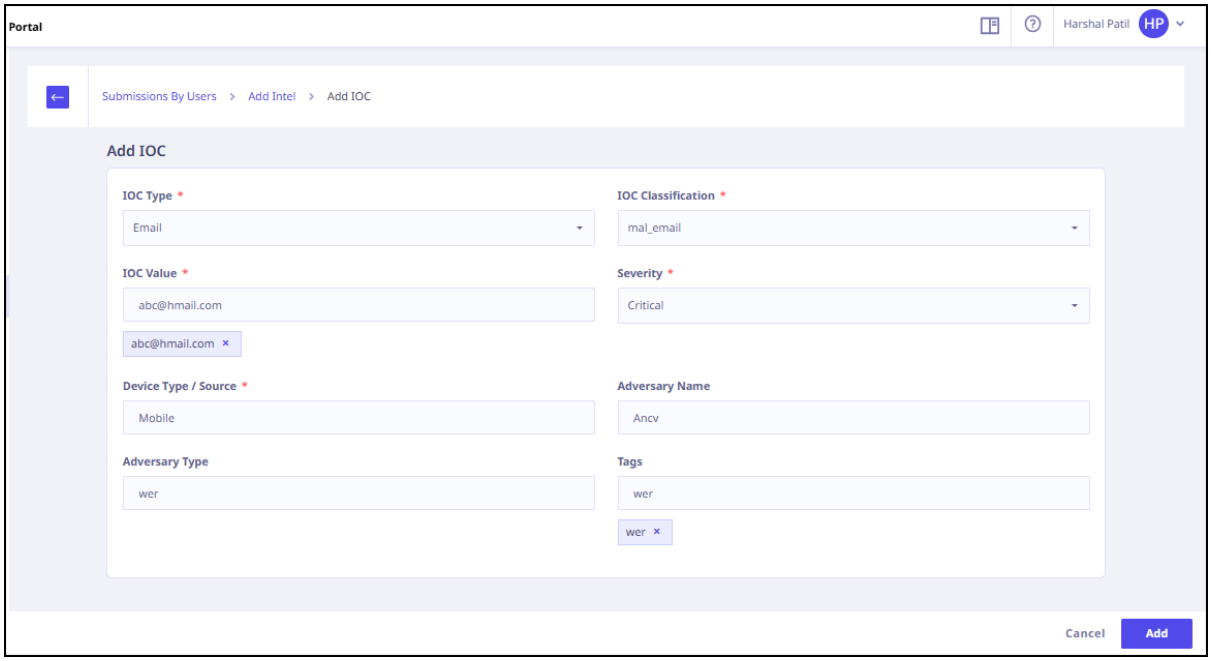
Adding New Intel

To add new intel, Organization admins have to follow these steps:

1. On the Seqrite Threat Intel portal, click **Submissions by Users** in the left pane.
2. On the **Submissions by Users** page, click **+ Add Intel**.
   The **Add New Intel** page is displayed.
3. Enter **Incident Basic Details**, that are Title, Incident Date, Intel Category and Description, and click **Add IOC Manually**.
4. Enter IOC details that are, IOC Type, IOC Classification, IOC Value, Severity, Device Type/Source, Adversary Name, Adversary Type, Tag, and click **Add**.
5. If you want to review the intel before submission, click **Save** else click **Submit**.

This provision is available to Organization Admins and Organization Analysts.





Note: The **Seqrite Admin** will approve the submitted intel.

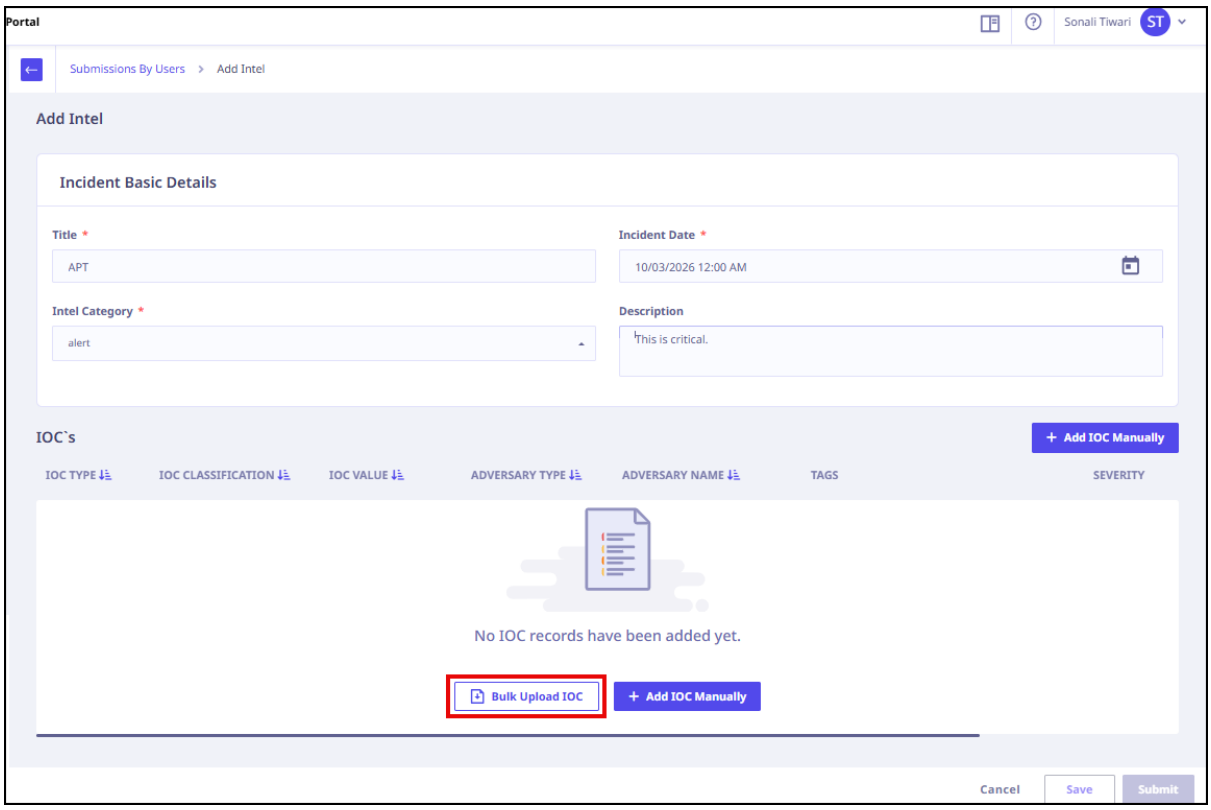
Bulk Upload of IOCs

You can upload multiple/bulk IOCs at once. You can download a CSV template, fill in IOC details and upload.
Note: Supported file type is .CSV only.

To bulk upload IOCs, follow these steps:

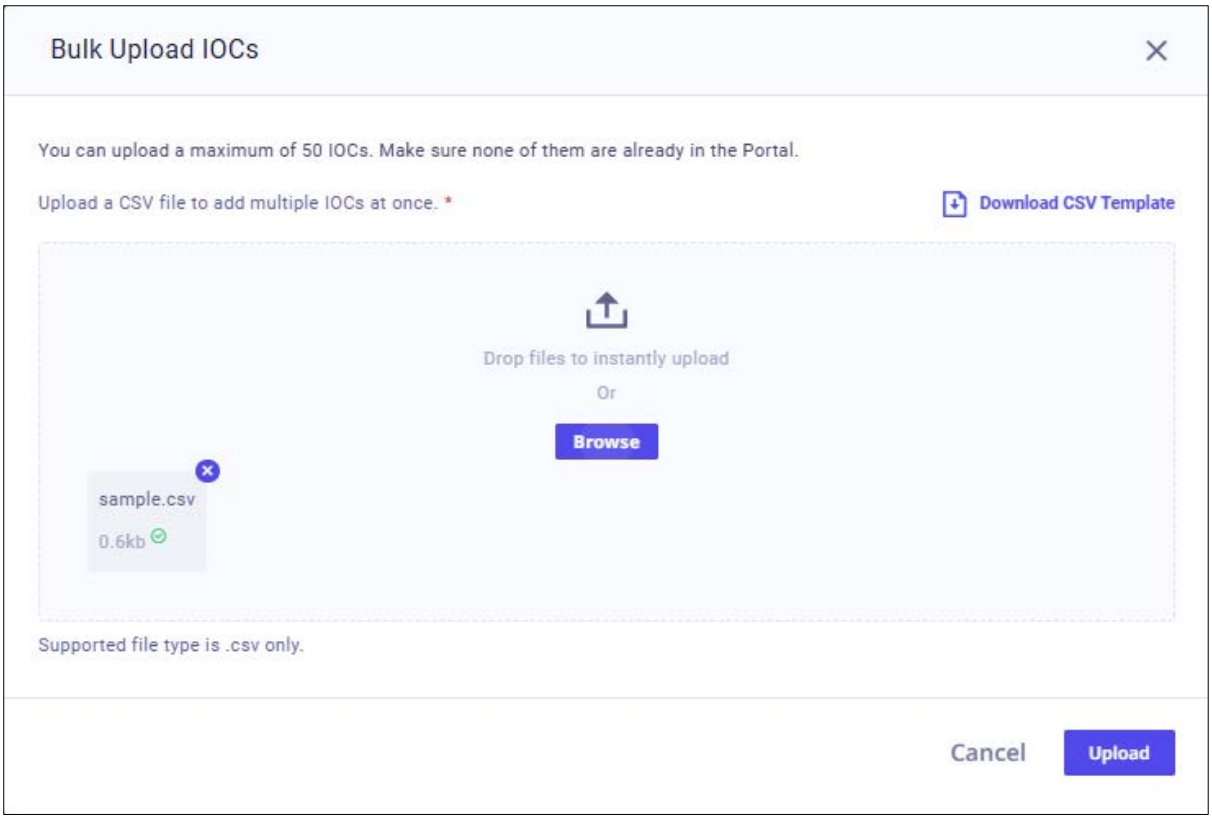
1. On the Seqrite Threat Intel portal, click **Submissions by Users** in the left pane.
2. On the **Submissions by Users** page, click **+ Add Intel**.
   The **Add New Intel** page is displayed.

3. Enter **Incident Basic Details** that are, Title, Incident Date, Intel Category, and Description and then click **Bulk Upload IOC**.



The **Bulk Upload IOCs** screen is displayed.

4. Click **Download CSV Template** to download the template.
5. Enter IOC details in the CSV file and upload the file.



Edit Intel

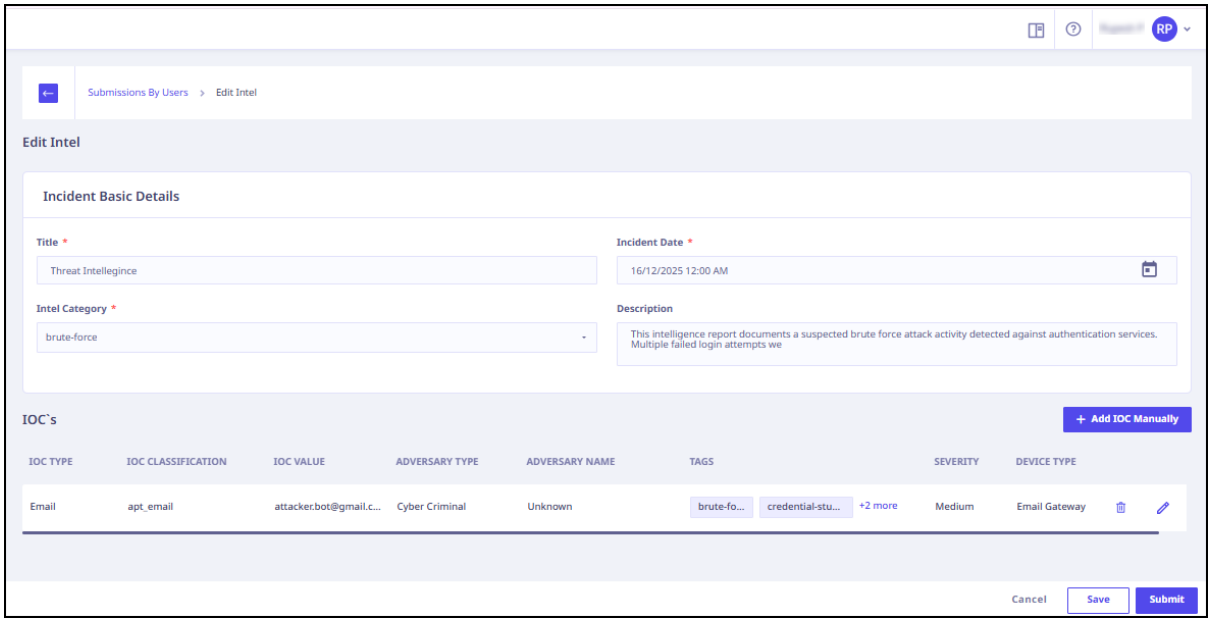
You can edit or delete intel and IOCs only while they are in **draft** stage.
To edit the intel, follow these steps:

1. On the Seqrite Threat Intel portal, click **Submissions by Users** in the left pane.
2. Click the intel with **Draft** status.
   The **Edit Intel** page appears.
3. Edit the details and click **Submit**.
4. To edit the IOC, select the IOC you want to edit and click **Edit**.
5. Edit the IOC details and click **Update**.
6. To delete the IOC, select the IOC and click **Delete**.

Viewing the Submitted Intel

You can view the intel submissions details such as Sub ID (Submission ID), title, , reported on, approved on, status and IOC status in the tabular format.
To view the details of each intel, follow these steps:

1. On the Seqrite Threat Intel portal, click **Submissions by Users** in the left pane.
2. On the **Submissions by Users** page, select the intel and click the **>** icon.
   The intel submission details page displays the following details:

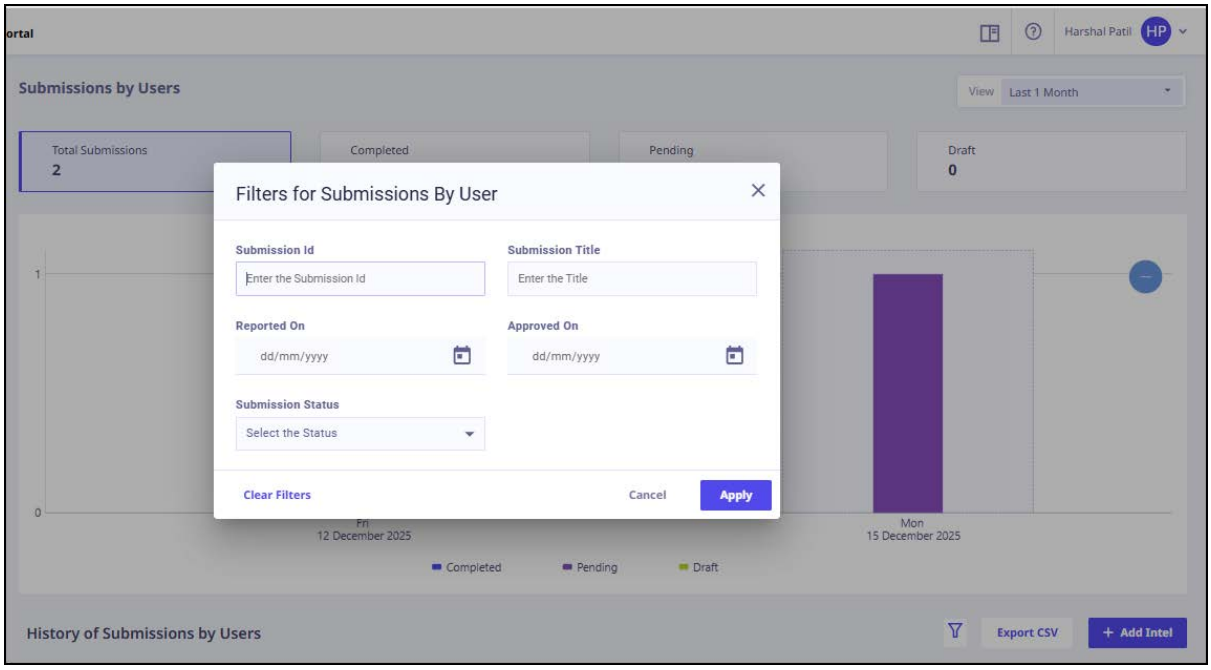


- **Primary Information**: For example, APT Category (Category, Name, Source IP, Description, APT Name, IOC Type, IOC Name)
- Linked IOCs and corresponding details.

Filtering the Submitted Intel

You can filter the intel submissions list to refine results based on submission ID, intel ID, submission title, reported on, approved on, and submission status.
To filter the intel submissions list, follow these steps:

1. On the Seqrite Threat Intel portal, click **Submissions by Users** in the left pane.
2. On the **Submissions by Users** page click .
3. Enter the details that are, submission ID, intel ID, submission title, reported on, approved on, and submission status and then click **Apply.**



The system displays filtered data.

Exporting Intel Submissions as a CSV

You can download all the intel submissions currently visible on the page in the CSV format.
To export/download intel submissions, follow these steps:

1. On the Seqrite Threat Intel porta, click **Submissions by Users** in the left pane.
2. On the **Submissions by Users** page click **Export CSV**.

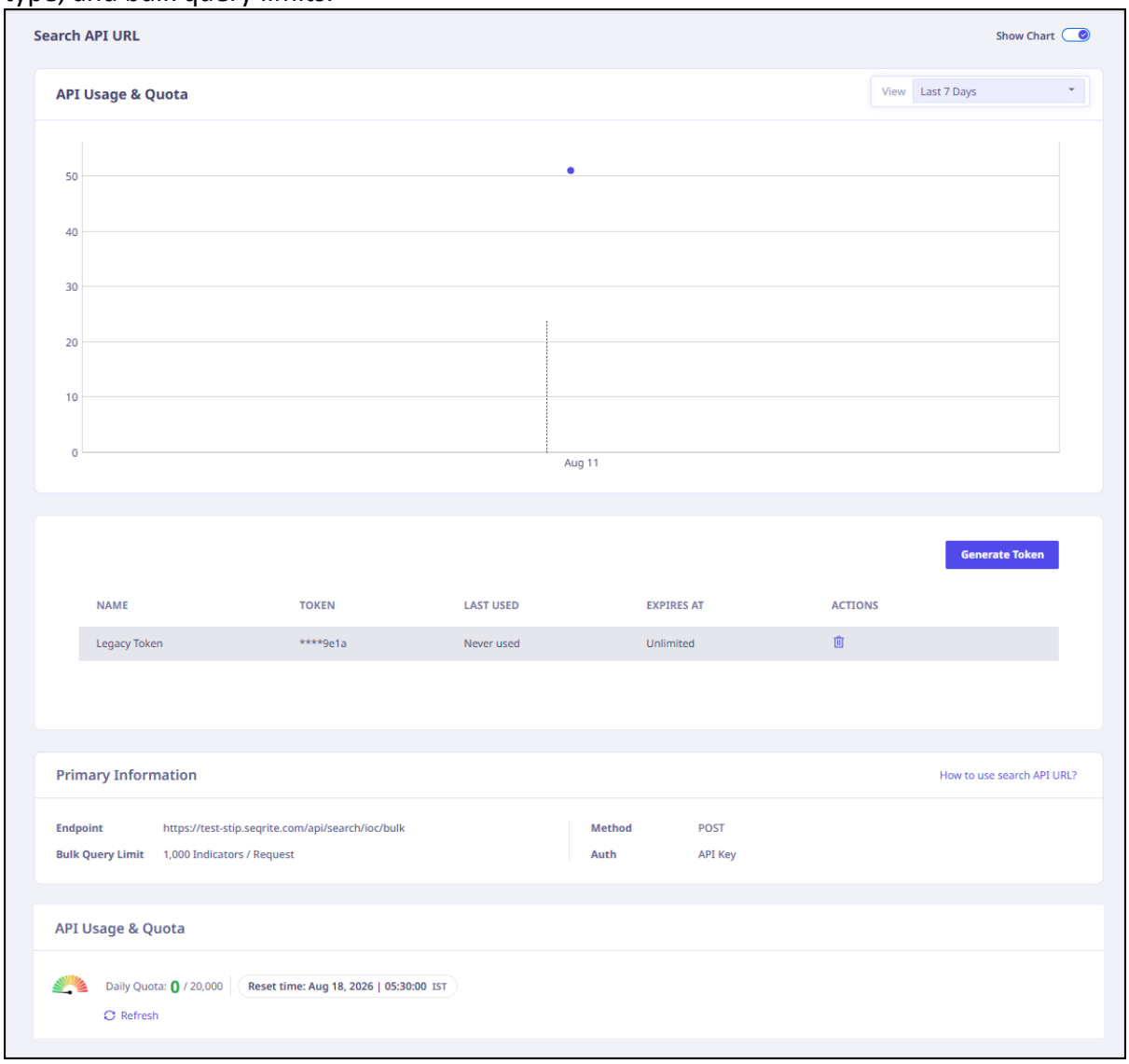
Integration

TAXII Details

Seqrite Threat Intel offers API-based lookups with a daily call limit. Organizations can leverage these APIs to obtain reputation data for Indicators of Compromise (IOCs). Depending on specific requirements, Seqrite Threat Intel can scale the daily API call quota to meet organizational needs.

Search API

The **Search API URL** section contains the details needed to access threat intelligence data through APIs. You can generate an authentication token, view API usage and quota information, and find details such as the API endpoint, supported method, authentication type, and bulk query limits.



You can generate an authentication token and view the details needed to securely integrate external applications, scripts, and security tools.

API Usage and Quota

Displays API consumption information through a graphical representation.

Generate Token

Creates an authentication token that is required to access the Search API and perform authorized requests.
To generate a token:

1. Click Generate Token.
2. Enter **Name** and specify the **Duration** (30 days, 60 days, 90 days, 1 year or unlimited) for which the token should remain valid.
3. Click **Generate Token**.
4. Copy and securely store the generated token, as it will be used to authenticate Search API requests.

Primary Information

- **Endpoint**
  Displays the API URL that applications and tools use to connect to the Threat Intelligence Platform.

- **Authentication (Auth)**
  Specifies the authentication method required to access the API, such as a bearer token.

- **Method**
  Indicates the supported HTTP request method (for example, GET or POST) used when sending API requests.

- **Bulk Query Limit**
  Displays the maximum number of indicators that can be searched in a single bulk API request.

API Usage and Quota

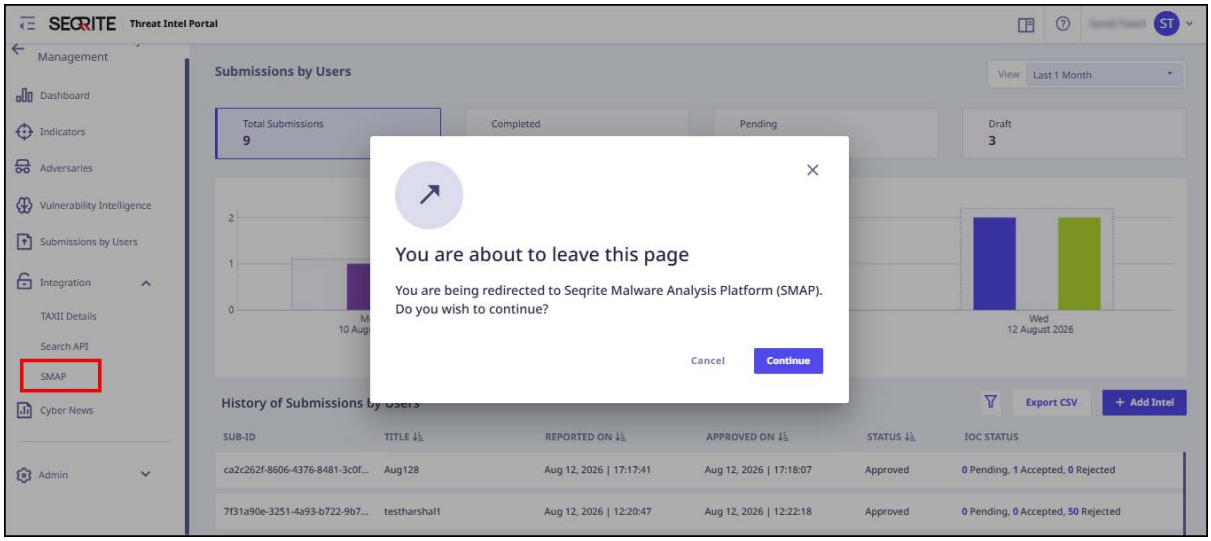
Displays the API usage details, including the daily quota limit and the date and time (IST) when the quota is reset.
Note: The Refresh updates and view the latest API usage and quota details.

SMAP

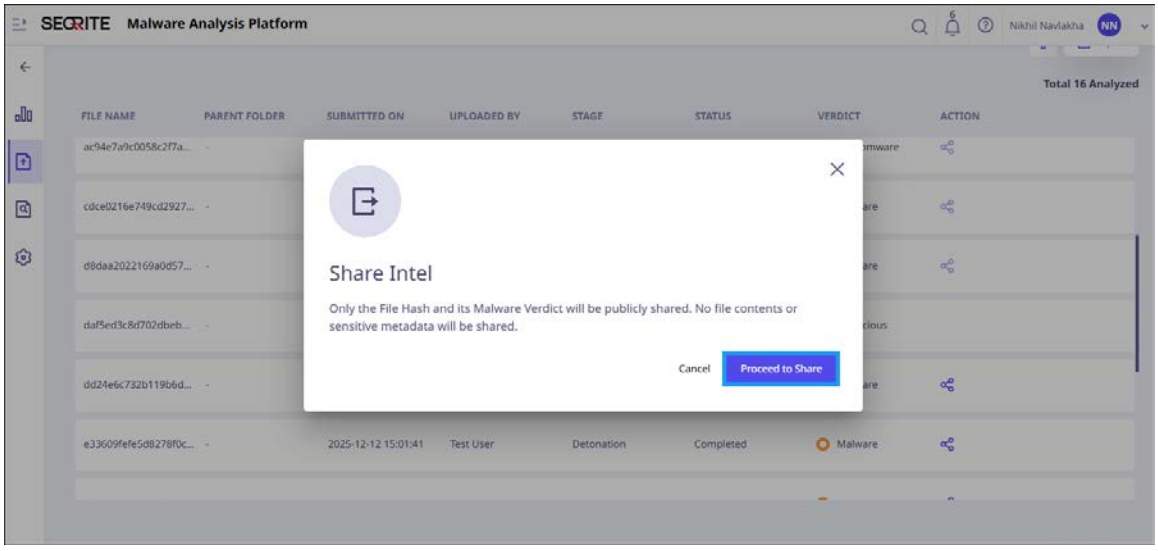
Seqrite Malware Analysis Platform (SMAP) is an advanced cybersecurity solution designed to analyze, detect and respond to evolving malware threats. The platform leverages multi-

stage processing, behavior-based detection, and deep forensic analysis to deliver comprehensive file Analysis.

This integration allows you to analyze suspicious files within SMAP and securely share any detected malware or ransomware with the SMAP community. On clicking **SMAP** tab, you will be redirected to **Seqrite Malware Analysis Platform** where you can perform static and behavior analysis of any suspicious file in an isolated environment.



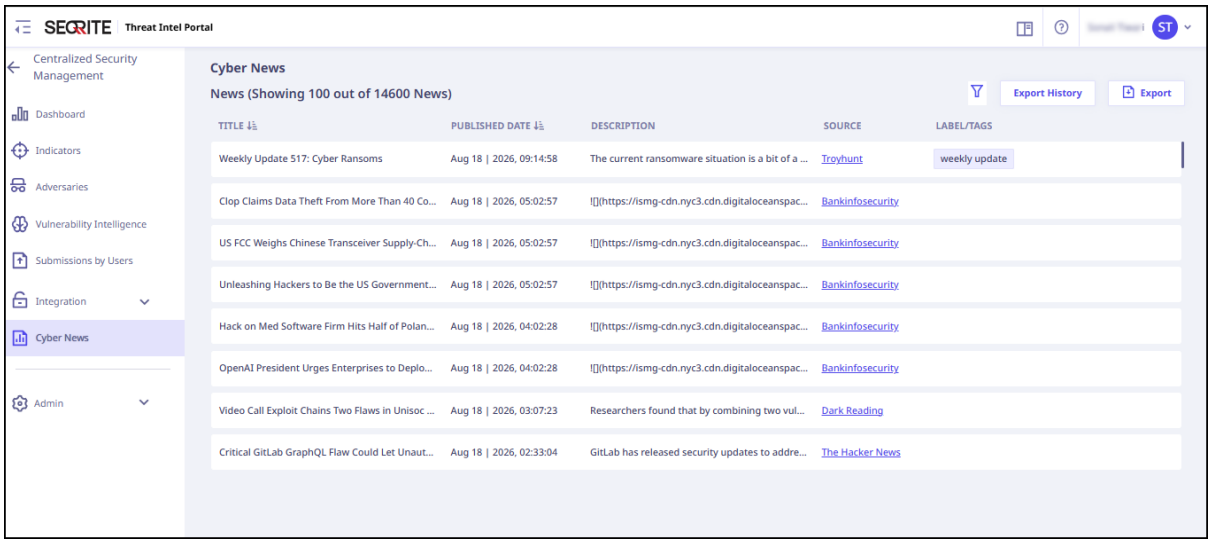
After analysis, if SMAP identifies a file as malicious or ransomware, you can choose to share it as intel (IOC) with the community.



Note: This is an add-on feature and requires activation. Please contact support team to enable it.

Cyber News

Seqrite Threat Intel continuously aggregates the latest cyber threat information from trusted RSS feeds and security blogs, enabling threat analysts to stay updated on global developments and derive actionable insights.

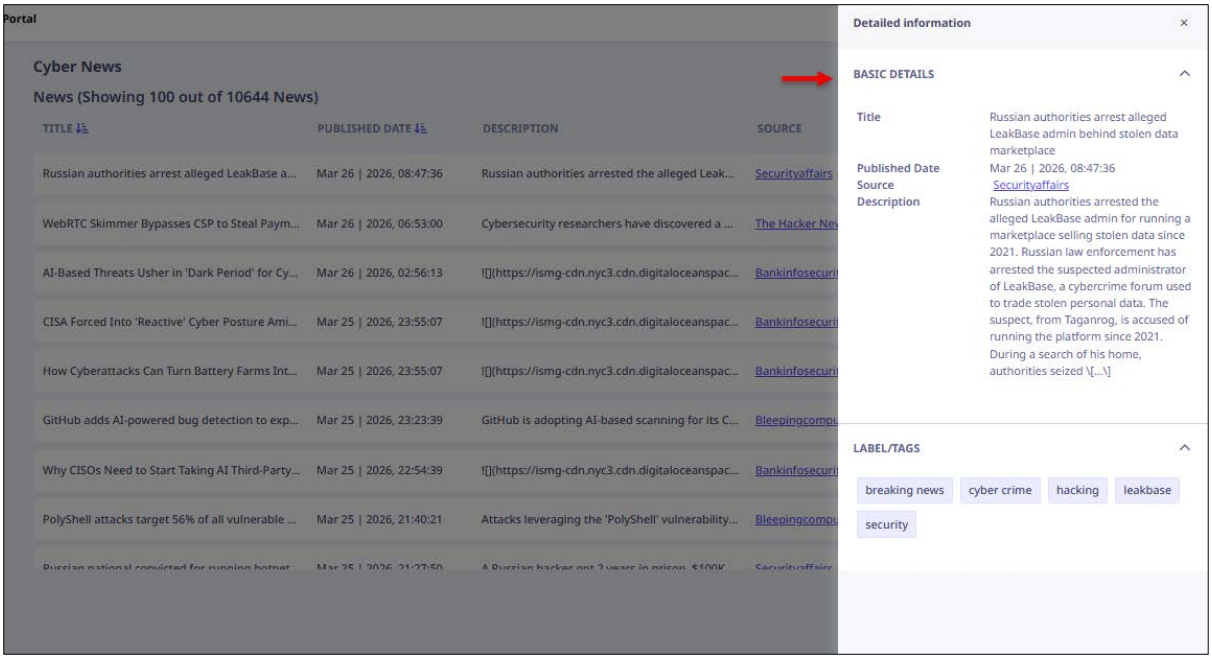


Viewing Cyber News

You can view cyber news in detail such as title, published date, source, source, description, and label/tags assigned to the cyber event. To view the cyber events, follow these steps:

1. On the Seqrite Threat Intel portal, click **Cyber News** in the left pane.

2. On the **Cyber News** page, select the cyber news and click the **>** icon.
   The **Detailed Information** page displays the following details:

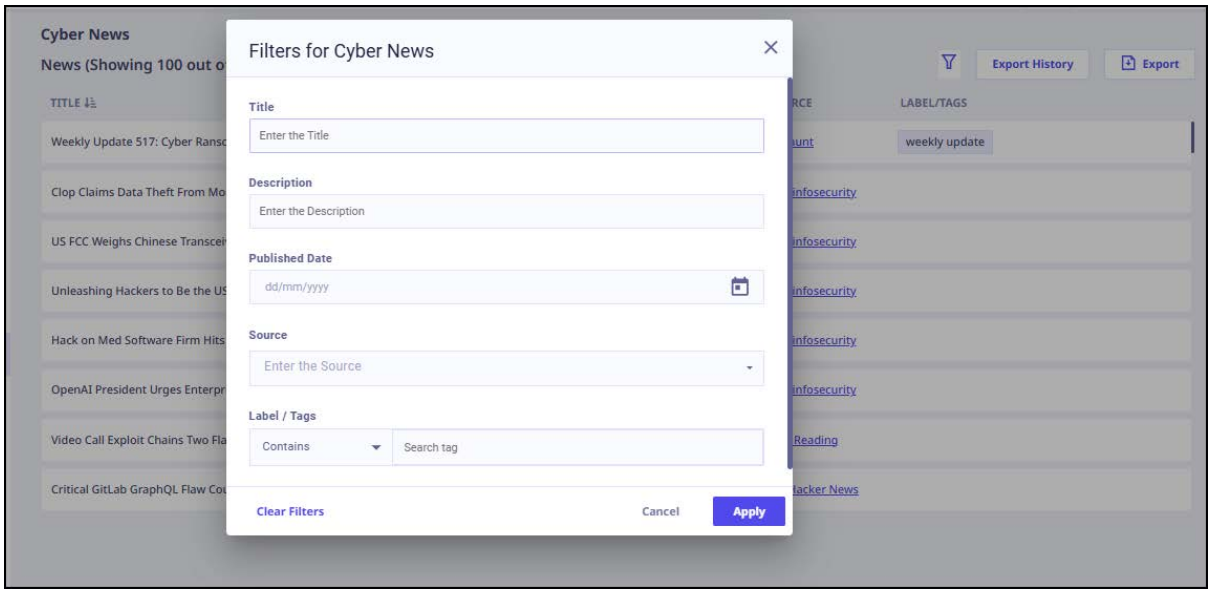


- **Basic Details**: title, published date, source, and description.
- **Label/Tag**: Shows the tags or labels assigned to the cyber news.

Filtering the Cyber News List

You can filter the cyber news list to refine results based on title, description, published date, source, and label.
To filter the cyber news list, follow these steps:

1. On the Seqrite Threat Intel portal, click **Cyber News** in the left pane**.**
2. On the **Cyber Events** page click .
3. Enter the details that are, title, description, published date, source, label and then click **Apply**.



The system displays filtered data.

Exporting Cyber News as a CSV/STIX

You can download all the cyber news currently visible on the page in the CSV or STIX format.
To export/download cyber news, follow these steps:

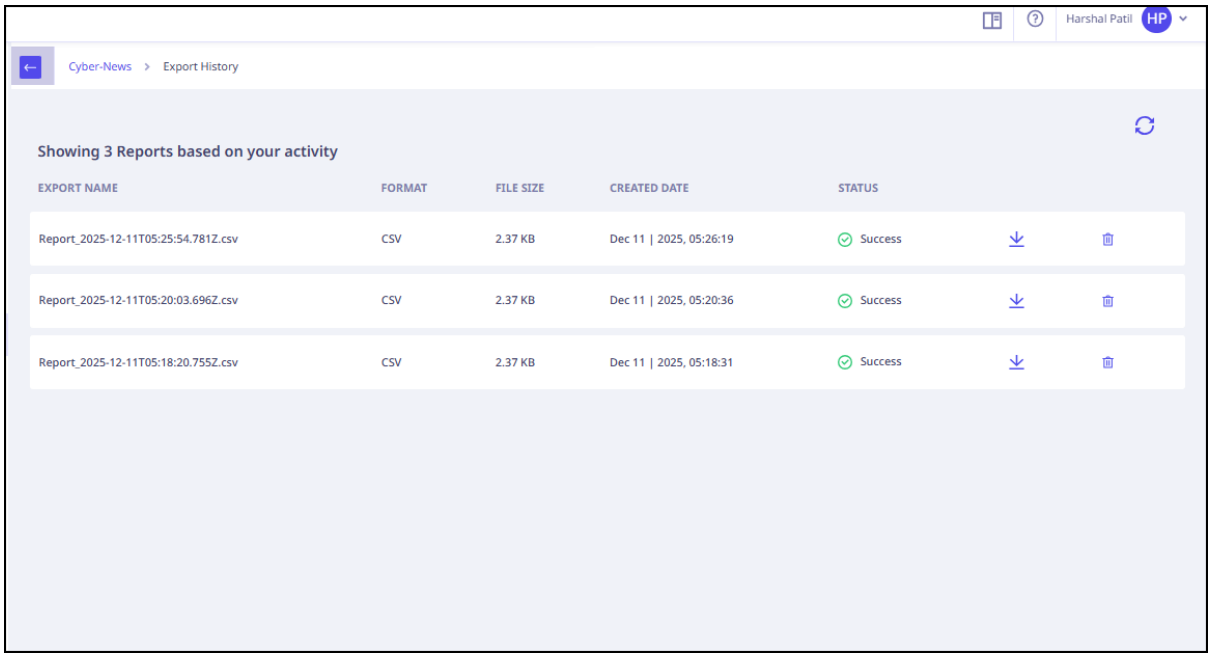
1. On the Seqrite Threat Intel portal, click **Cyber News** in the left pane.
2. On the **Cyber News** page click **Export**, select the format that is CSV or STIX 2.1, and then click **Export**.

Viewing Export History

Export History shows a record of when and what cyber news are exported by the user. This information tracks the usage of cyber news and can be useful in auditing and accountability purposes.
Export History provides a record that is report name, file size, created date, the format in which the cyber news were exported (STIX, CSV), and status.
To view the export history, follow these steps:

1. On the Seqrite Threat Intel portal, click **Cyber News** in the left pane**.**
2. On the **Cyber News** page click **Export History**.

The list of exported cyber news is displayed.



Admin

Within Seqrite Threat Intel, following user roles are present:

1. Org Admin: Org admin can view the organization details. Org admin has the authority to add and edit users, assign user roles, disable users, and view the license.
2. Org Analyst: Org Analyst can access all the tabs except Admin tab.

Users

Adding New User

For **Cloud Users**, Org Admin can add users through the Seqrite CSM console only.
To add a user, follow these steps:

1. On the Seqrite CSM page, click **Admin Users** on the left pane.
2. Click **+ Add User.**
   The **Add User** page is displayed.
3. Enter the user details and click **Add**.

For **On Premise Users**, Org Admin can add users in the Admin section.
To add a user, Follow these steps:

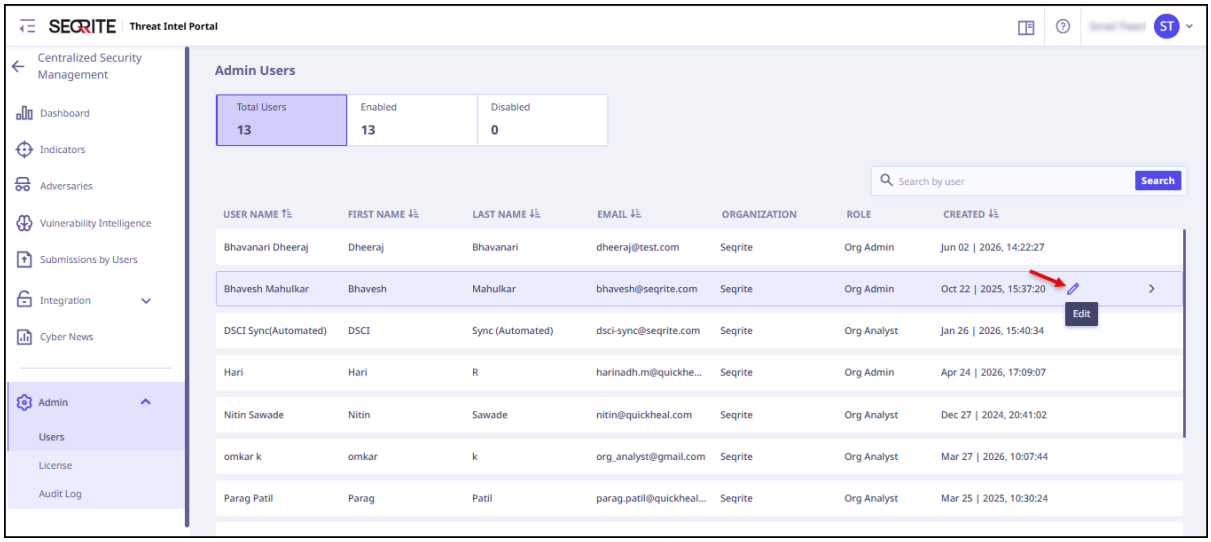
1. On the Seqrite Threat Intel portal, click **Admin** and select **Users** in the left pane.
2. Click **+ Add User.**
   The **Add User** page is displayed.
3. Enter the user details and click **Add**.

Editing a User

For **Cloud Users**, Org Admin can edit only **user role** in portal and all details through the Seqrite CSM console only.

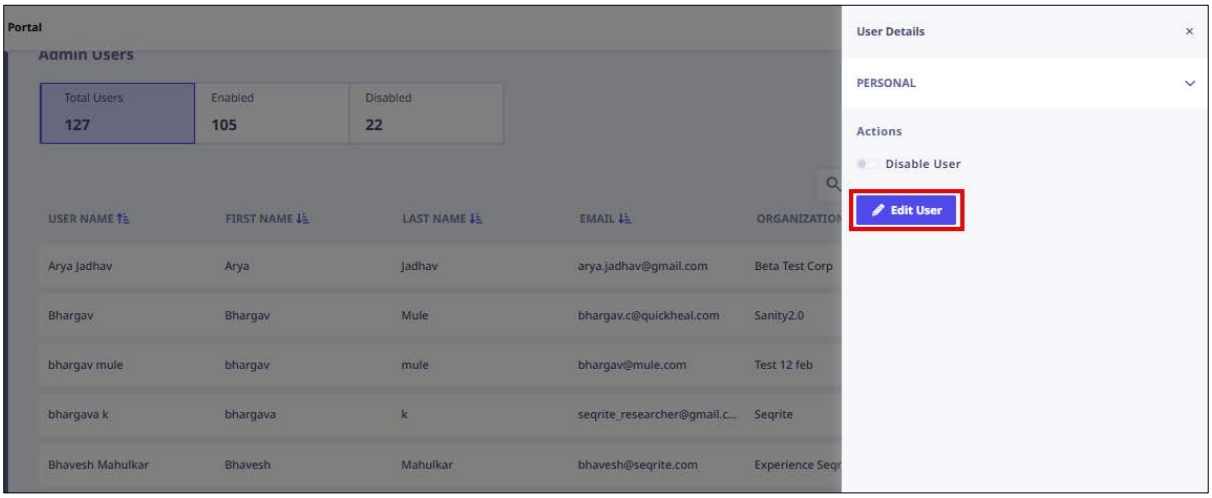
For **On Premise Users**, Org Admin can edit the existing user from the admin section.
To edit the existing user, follow these steps:

1. On the Seqrite Threat Intel portal, click **Admin** and select **Users** in the left pane.
2. On the **Admin Users** page, click the **Edit** icon for the user that you want to edit.

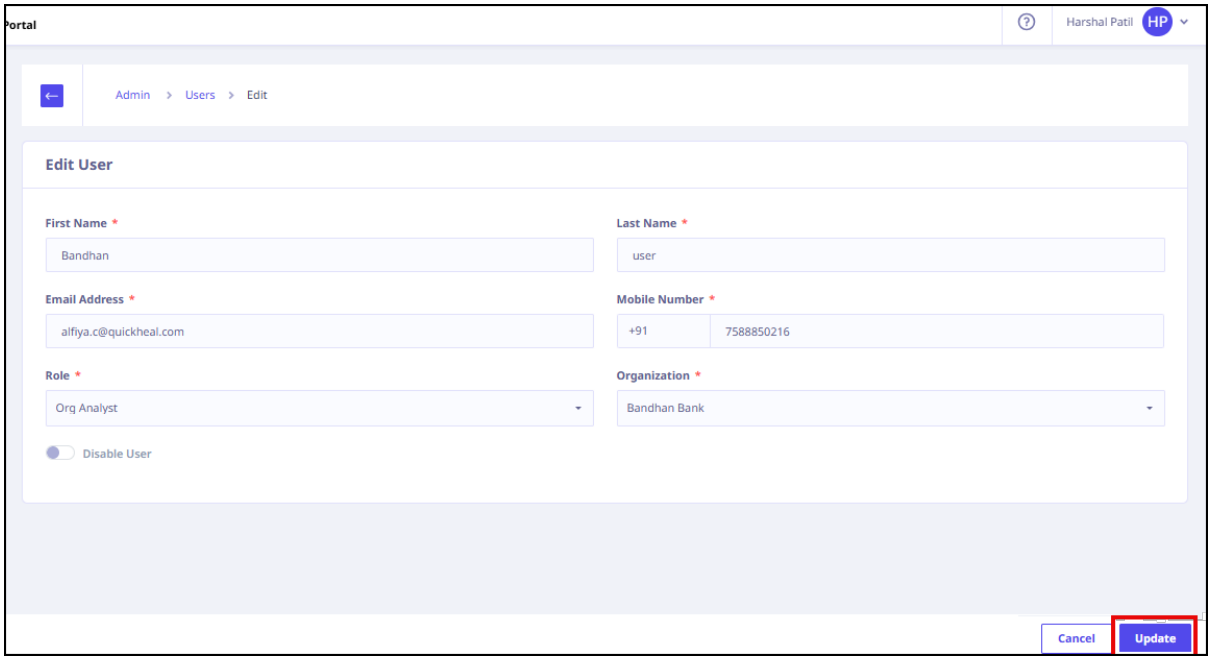


Or

4. Click >, a pop appears.



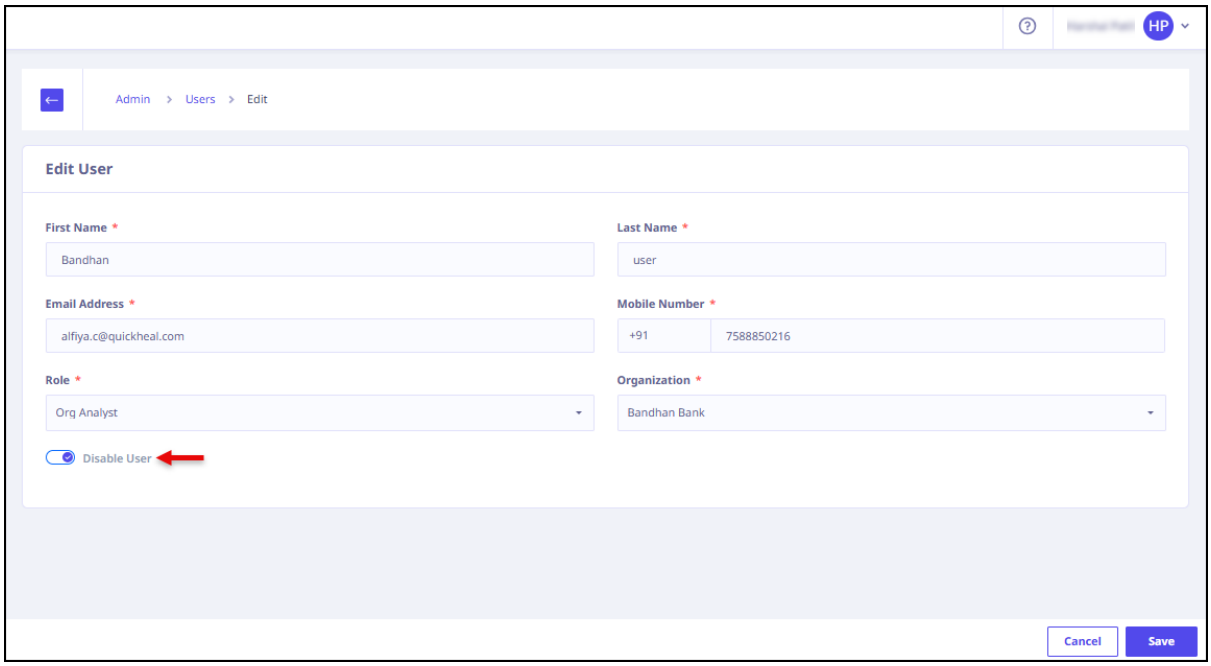
5. Click **Edit User**.
6. Edit the user details and click **Update**.



Disable a User

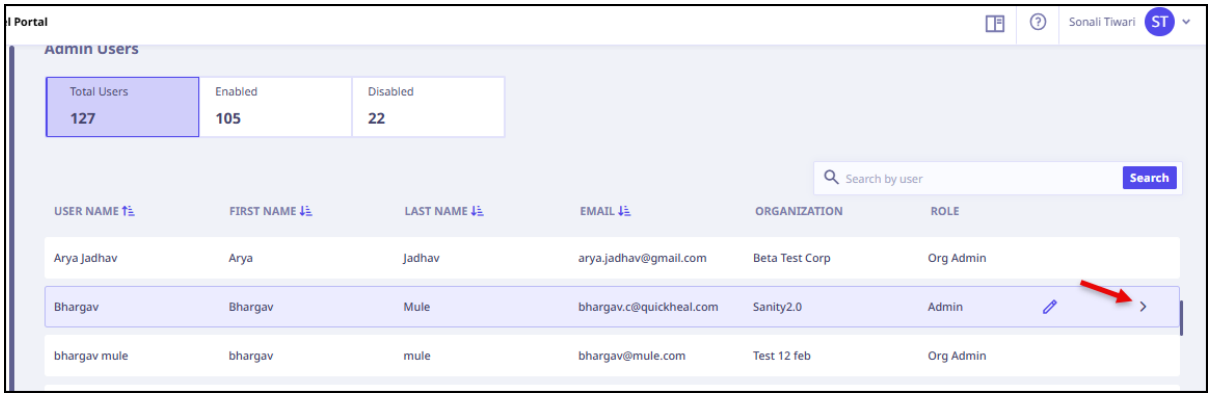
For **On Premise Users**, Org Admin can disable the user from the admin section.
To disable the user, follow these steps:

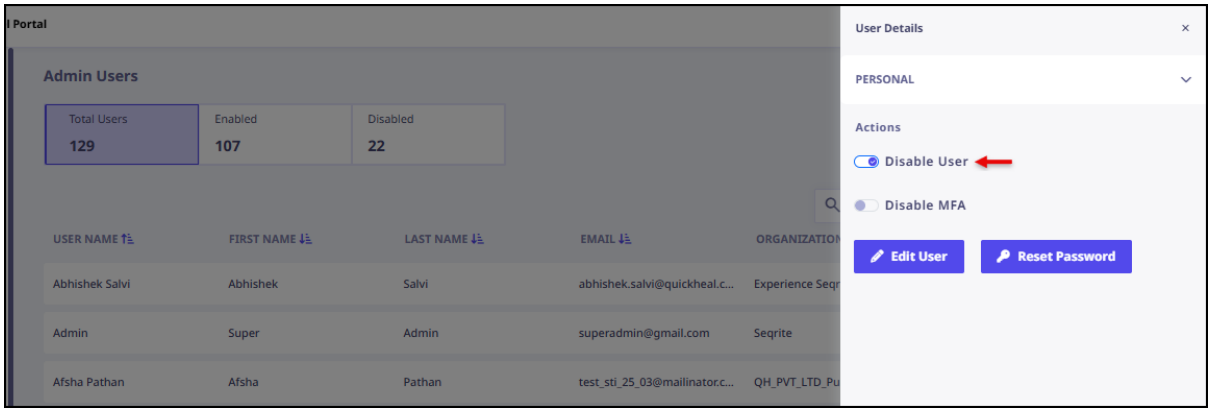
1. On the Seqrite Threat Intel portal, click **Admin** and select **Users** in the left pane.
2. On the **Admin Users** page, click the **Edit** icon for the user that you want to disable.
3. Switch the **Disable User** toggle and click **Save**.



Or

4. Click **>**, a pop appears.



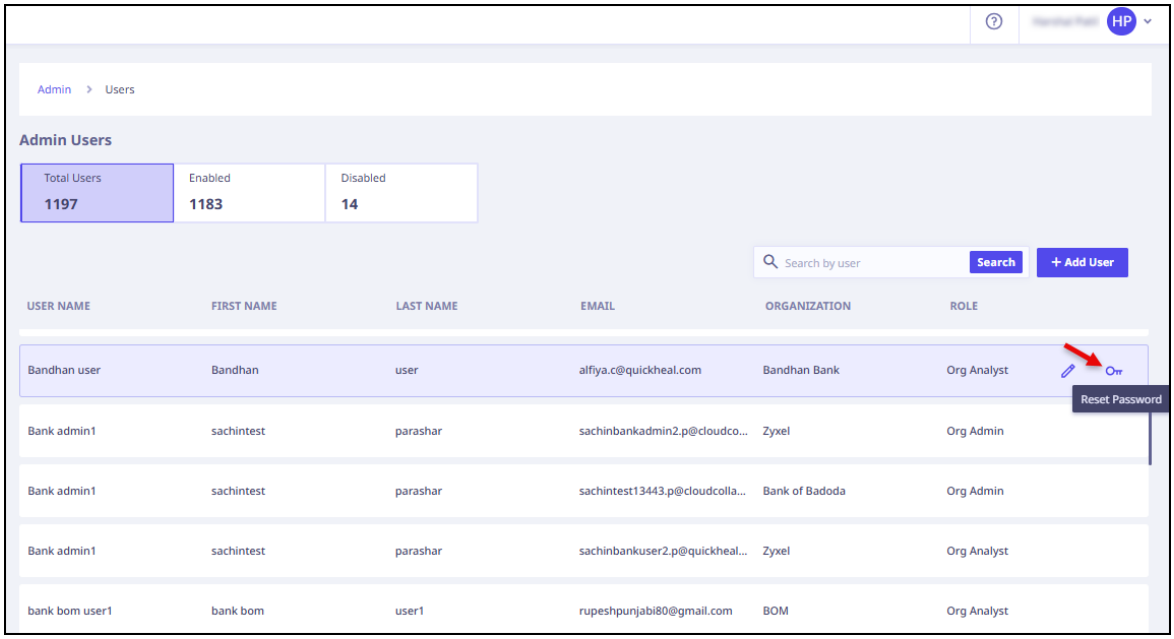


5. Switch the **Disable User** toggle.

Reset User Password

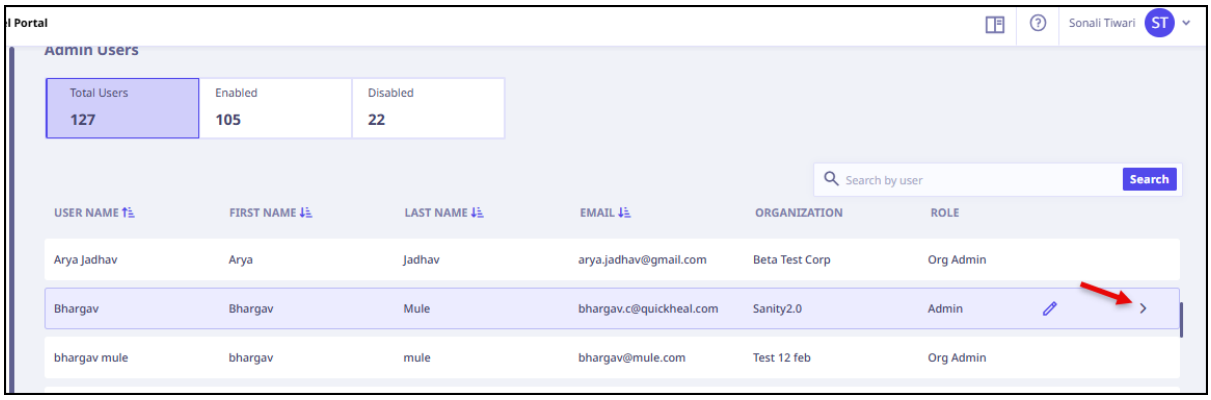
For **On Premise** Users, Org Admin can reset the user from the admin section. Following are the steps:

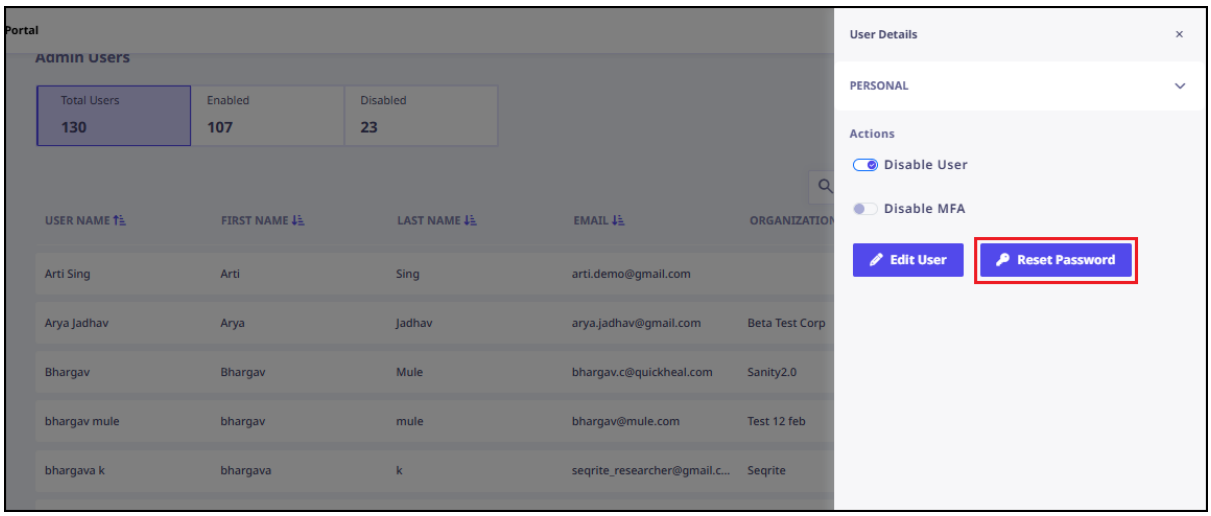
1. On the Seqrite Threat Intel portal, click **Admin** and select **Users** in the left pane.
2. On the **Admin Users** page, click the **Reset Password** icon for the user for whom you want to reset the password.



Or

3. Click **>**, a pop appears





4. Click **Reset Password**. A confirmation pop up appears.
5. Click **OK**.

An email is sent to the user with a new password.

License

This page is visible only to the admin user. On this page, admin can check the status of Seqrite Threat Intel license. The license details page gives details such as License status, Product key, License Expiry Date (UTC), No. of users allowed to access the Portal, and Bulk Search API quota.

Audit Log

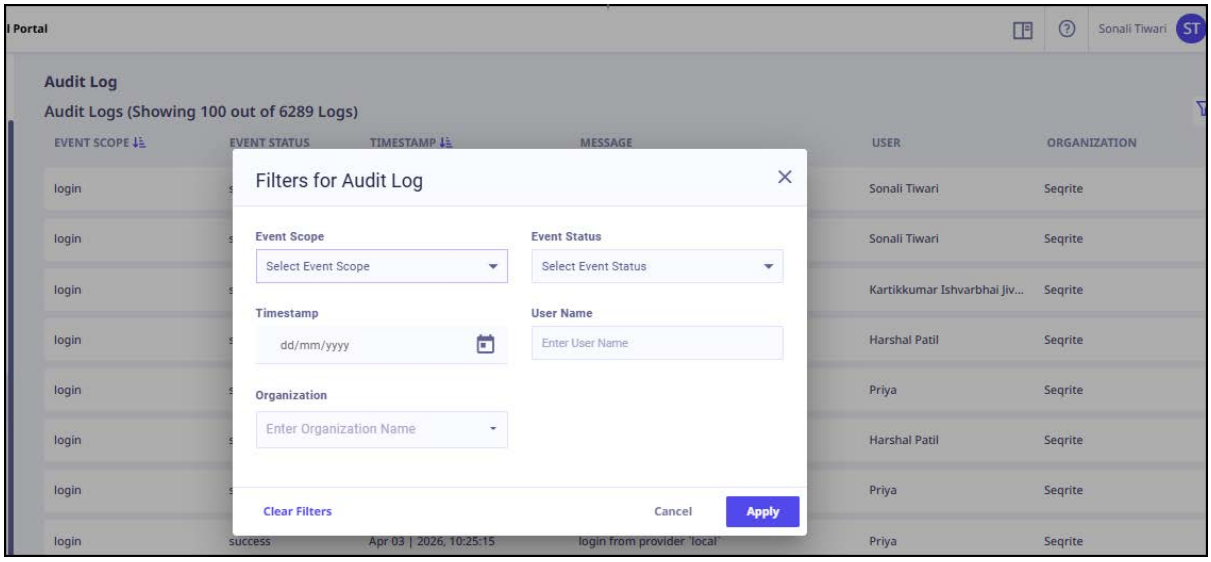
The **Audit Log** keeps record of login, logout, and forgot password activities in the system. It includes:

- **Event Scope**: The type of activity being recorded.
- **Event Status**: The outcome of the event, such as **Success** or **Error**.
- **Timestamp**: The exact date and time when the event occurred.
- **Message**: Description of action.
- **User**: The account or person who performed the action.
- **Organization**: The organization associated with the user.

Filtering Audit Log List

You can filter the audit log list to refine results event scope, event status, timestamp or username.
To filter the audit log list, follow these steps:

1. On the Seqrite Threat Intel portal, click **Admin** and select **Audit Log** in the left pane.
2. On the **Audit Log** page click .
3. Enter the details and click **Apply**.



The system displays filtered data.

Support

Head Office Contact Details

Quick Heal Technologies Limited
(Formerly known as Quick Heal Technologies Pvt. Ltd.)
Reg. Office: CTS No. 1442 to 1445 Thube Park, Shivaji Nagar, Pune – 411005.
Official Website: http://www.seqrite.com
Emails to: support@seqrite.com
Contact No.:

- **1800-212-7377**
  Monday to Saturday 9:00 AM to 8:00 PM (IST)

- **+91 7066027377**
  Monday to Saturday 9:00 AM to 8:00 PM (IST)

- **+91 9168625686**
  Monday to Friday 8:00 PM to 9:00 AM (IST)