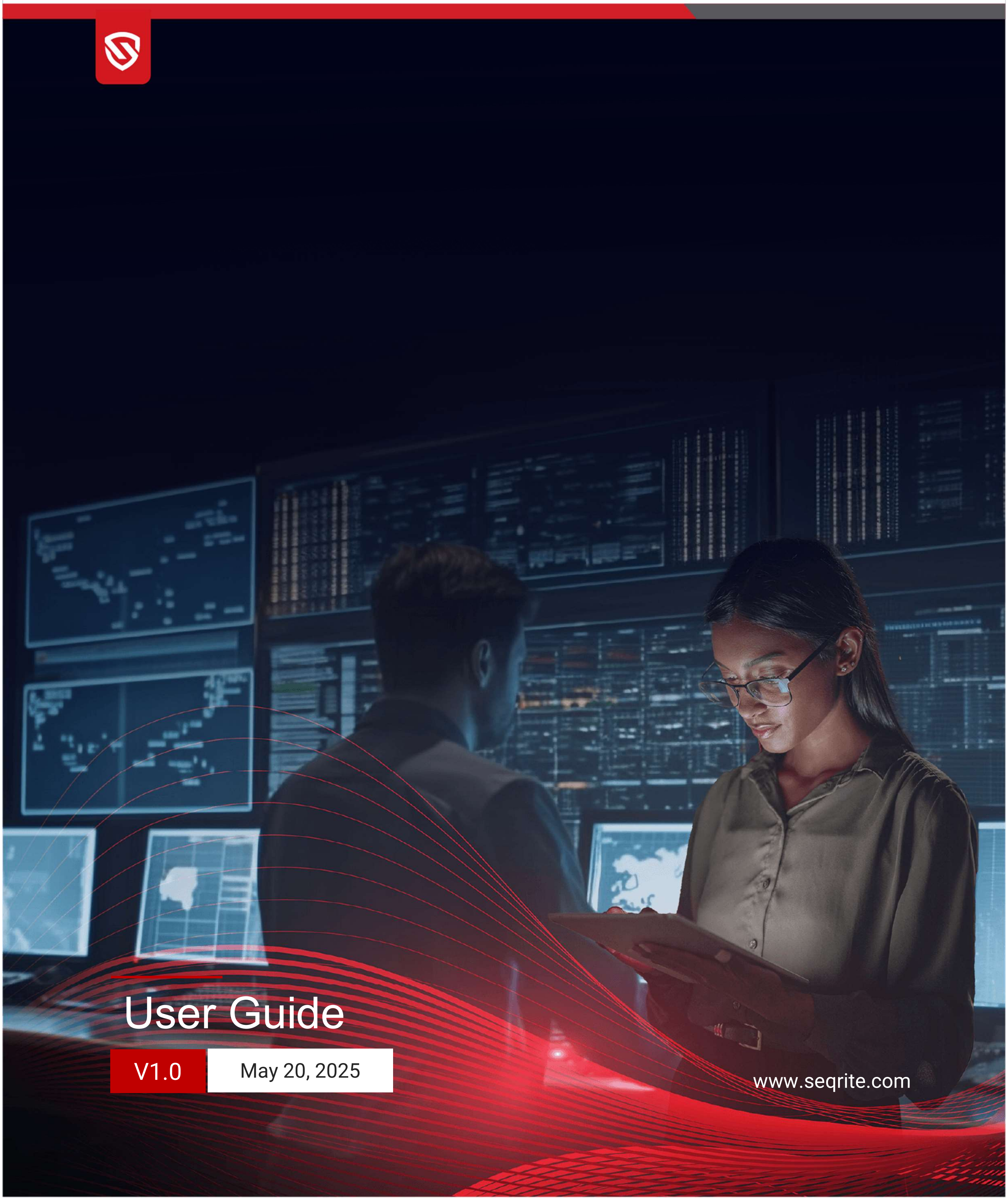
Seqrite Threat Intelligence

SEQRITE



User Guide

V1.0 May 20, 2025

www.seqrite.com

Contents

1. Version History 4
2. Introduction 5
3. Getting Started 7
Accessing the Seqrite Threat Intelligence 7
Setting Up Organizations and Analysts 7
4. Dashboard 8
Dashboard Metrics 8
User Profile 8
Glossary 9
5. Indicators 10
Viewing the IoC Details 10
Selecting Column from the Column Selector 11
Filtering the IoC List 11
Exporting IoC as a CSV/STIX 12
Viewing IoC Export History 12
6. Adversaries 14
Viewing the Adversary Details 14
Selecting Column from the Column Selector 15
Filtering the Adversary List 15
Exporting Adversaries as a CSV/STIX 16
Viewing Adversary Export History 16
7. Vulnerability Intelligence 17
Viewing the Vulnerability Details 17
Selecting Column from the Column Selector 18
Filtering the Vulnerability List 18
Exporting Vulnerabilities as a CSV/STIX 19
Viewing Vulnerability Intelligence Export History 19
8. Submissions by Users 21
Adding New Intel 21
Viewing the Submitted Intel 22
Filtering the Submitted Intel 23
Exporting Intel Submissions as a CSV 24
9. Reports 25

Viewing Reports 25
Filtering the Reports List 26
Exporting Reports as a CSV/STIX 26
Viewing Export History 26
10. Admin 28
Organizations 28
Editing Organization 29
Disable Organization 29
Users 30
Disable a User 31
Reset User Password 32
Approve Intel 32
Viewing the Approve Intel 33
Filtering the Intel Submissions List 33
Approve/Reject Submitted Intel 34
11. Support 36

Version History

Doc Version	Date	Comment
1.0	March 12, 2025	Seqrite Threat Intelligence 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.

Introduction

Seqrite Threat Intelligence 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 Intelligence 1.0 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, and more. Information related to threats is messaged and put together in STIX format and delivered to customers via the TAXII server.

Seqrite Threat Intelligence 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

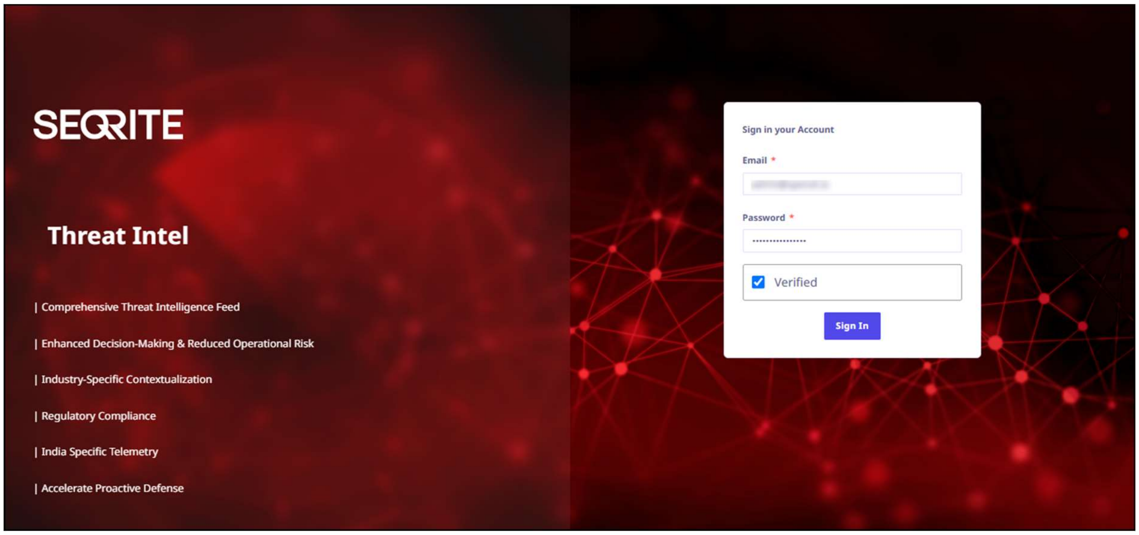
- As mentioned, STIX provides CTI data Feeds in JSON format. Feeds contain CTI data from Collections.
- A TAXII Collection is an interface to a database of CTI objects provided by a TAXII Server. It is used by TAXII Clients to request information from the TAXII Server.
- It is common to use the term 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.

Getting Started

Accessing the Seqrite Threat Intelligence

Seqrite Threat Intelligence is a web-based application hosted on Seqrite’s server.
To access this portal, follow these steps:

1. Users are to plug in their USB dongle on their endpoint (Desktop or Laptop).
2. Go to https://stip.seqrite.com/.
3. On the Sign In page, login with the provided credentials.



Threat Intel

| Comprehensive Threat Intelligence Feed

| Enhanced Decision-Making & Reduced Operational Risk

| Industry-Specific Contextualization

| Regulatory Compliance

| India Specific Telemetry

| Accelerate Proactive Defense

Sign in your Account

Email *

Password *

☑ Verified

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

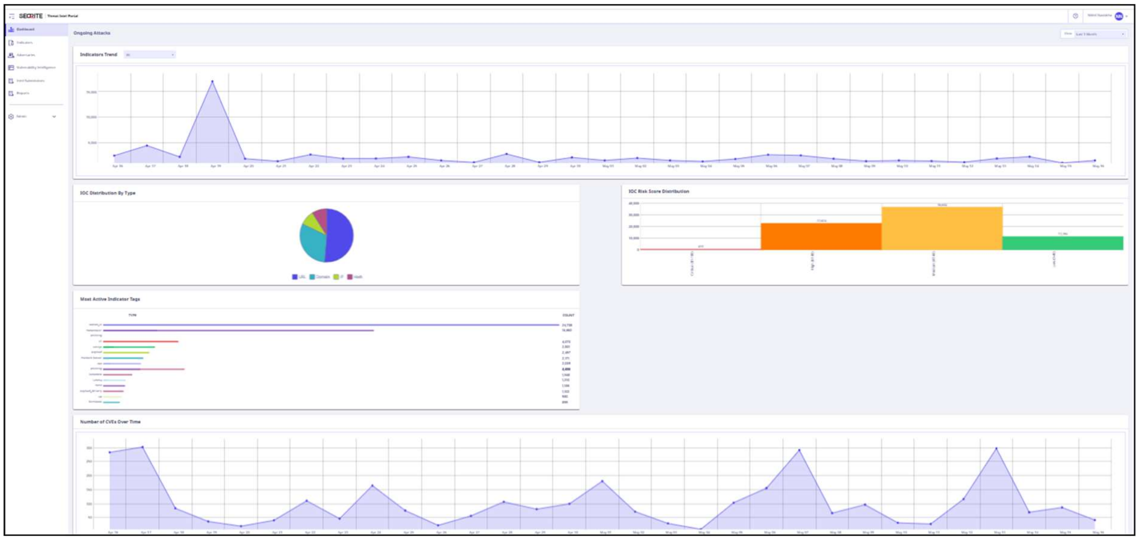
Setting Up Organizations and Analysts

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 intelligence data.
3. **Disabling Accounts**
   - Seqrite admins can disable organizations or specific analysts.
   - Seqrite Admin or Organization Admin can disable specific users of their organization.

Dashboard

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



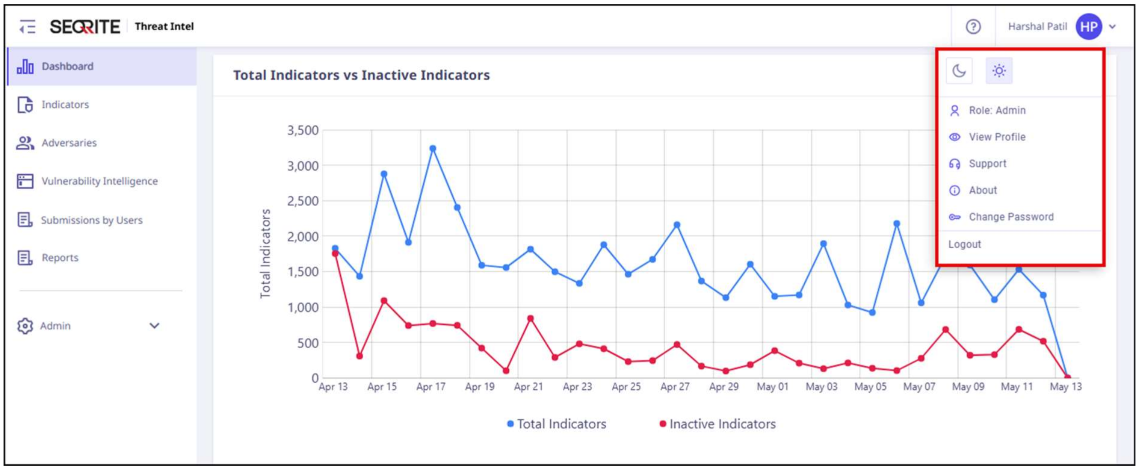
Dashboard Metrics

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
Indicators Trend	It gives a visual representation of IoC trends over time.
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.

User Profile

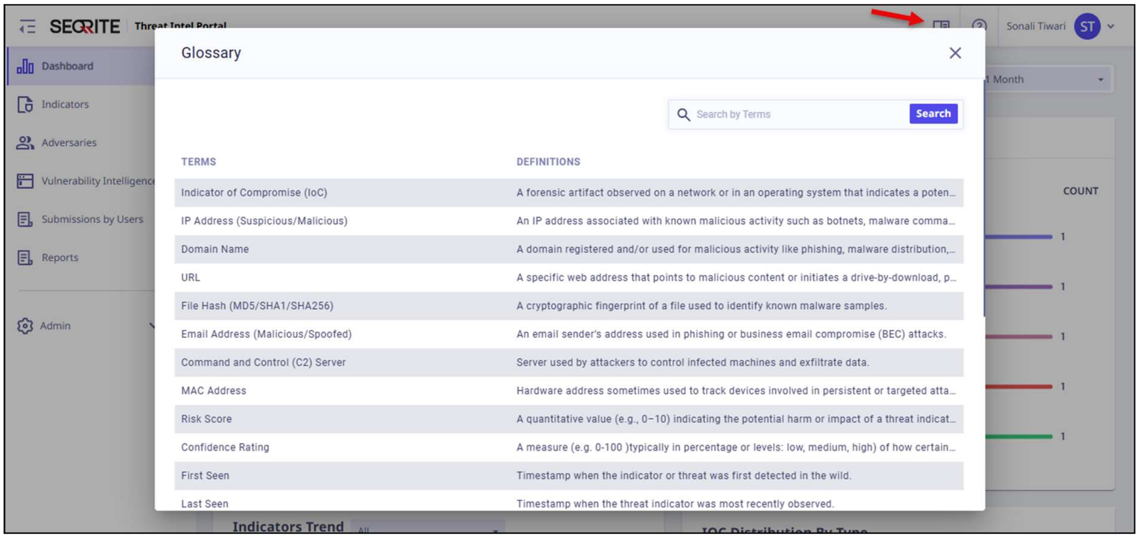
The User Profile section on the upper-right corner of the dashboard shows the name of the registered user.



When you click the logged-in username, the options are displayed: Role, View Profile, Support, About, Change Password, and Logout.

Glossary

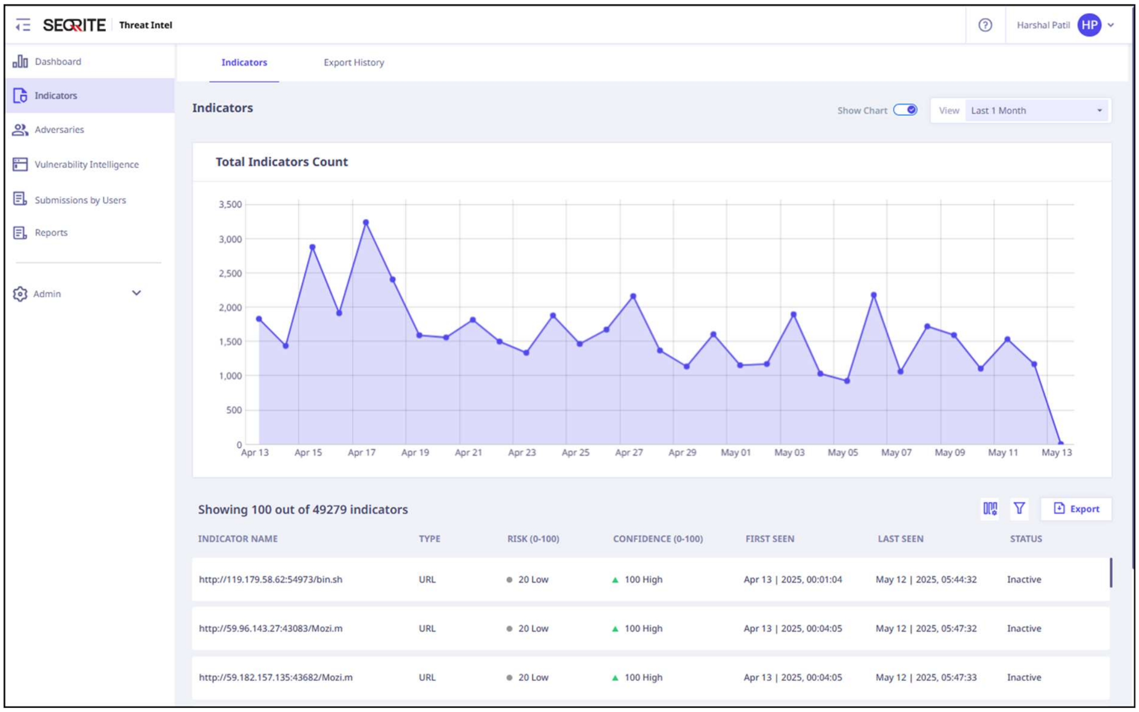
Glossary provides clear definition of key terms and phrases used throughout the Seqrite Threat Intelligence. It helps users to understand words and concepts related to cyber threats, attacks, and security.



TERMS	DEFINITIONS
Indicator of Compromise (IoC)	A forensic artifact observed on a network or in an operating system that indicates a poten...
IP Address (Suspicious/Malicious)	An IP address associated with known malicious activity such as botnets, malware comma...
Domain Name	A domain registered and/or used for malicious activity like phishing, malware distribution,...
URL	A specific web address that points to malicious content or initiates a drive-by-download, p...
File Hash (MD5/SHA1/SHA256)	A cryptographic fingerprint of a file used to identify known malware samples.
Email Address (Malicious/Spoofed)	An email sender's address used in phishing or business email compromise (BEC) attacks.
Command and Control (C2) Server	Server used by attackers to control infected machines and exfiltrate data.
MAC Address	Hardware address sometimes used to track devices involved in persistent or targeted atta...
Risk Score	A quantitative value (e.g., 0–10) indicating the potential harm or impact of a threat indicat...
Confidence Rating	A measure (e.g. 0-100)typically in percentage or levels: low, medium, high) of how certain...
First Seen	Timestamp when the indicator or threat was first detected in the wild.
Last Seen	Timestamp when the threat indicator was most recently observed.

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.



View: Last 1 Month

Showing 100 out of 49279 indicators

INDICATOR NAME	TYPE	RISK (0-100)	CONFIDENCE (0-100)	FIRST SEEN	LAST SEEN	STATUS
http://119.179.58.62:54973/bin.sh	URL	● 20 Low	▲ 100 High	Apr 13 | 2025, 00:01:04	May 12 | 2025, 05:44:32	Inactive
http://59.96.143.27:43083/Mozi.m	URL	● 20 Low	▲ 100 High	Apr 13 | 2025, 00:04:05	May 12 | 2025, 05:47:32	Inactive
http://59.182.157.135:43682/Mozi.m	URL	● 20 Low	▲ 100 High	Apr 13 | 2025, 00:04:05	May 12 | 2025, 05:47:33	Inactive

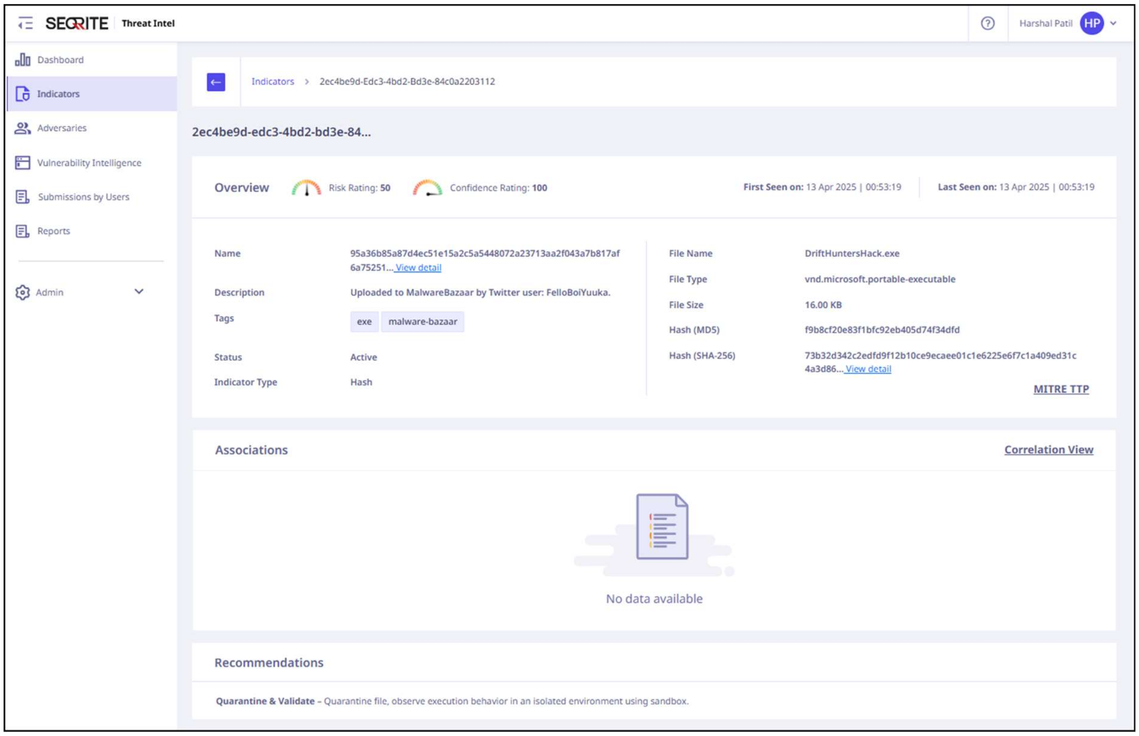
The **Indicators** tab provides the graphical and tabular presentation of IoC. You can view the IoC details and filter the IoC chart by specific date range that is last 1 day, last 7 days, last 1 month, last 3 months, last 1 year, and can select a custom date range as well.

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 Intelligence 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:



Indicators > 2ec4be9d-Edc3-4bd2-Bd3e-84c0a2203112

2ec4be9d-edc3-4bd2-bd3e-84...

Overview Risk Rating: **50** Confidence Rating: **100** **First Seen on:** 13 Apr 2025 | 00:53:19 **Last Seen on:** 13 Apr 2025 | 00:53:19

Name	95a36b85a87d4ec51e15a2c5a5448072a23713aa2f043a7b817af 6a75251... View detail	File Name	DriftHuntersHack.exe
Description	Uploaded to MalwareBazaar by Twitter user: FelloBoiYuuka.	File Type	vnd.microsoft.portable-executable
Tags	exe malware-bazaar	File Size	16.00 KB
		Hash (MD5)	f9b8cf20e83f1bfc92eb405d74f34dfd
Status	Active	Hash (SHA-256)	73b32d342c2edfd9f12b10ce9ecaee01c1e6225e6f7c1a409ed31c 4a3d86... View detail
Indicator Type	Hash		

MITRE TTP

Associations Correlation View

No data available

Recommendations

Quarantine & Validate – Quarantine file, observe execution behavior in an isolated environment using sandbox.

- **Indicator Overview**: Risk score, confidence score, and the description of the IoC.
- **Attributes**: Key properties such as source, detection date, and type.
- **TTP Mappings**: Links to tactics, techniques, and procedures associated with the IoC.
- **Associations**: Known relations with Threats Actors, Malware or IoCs.
- **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.

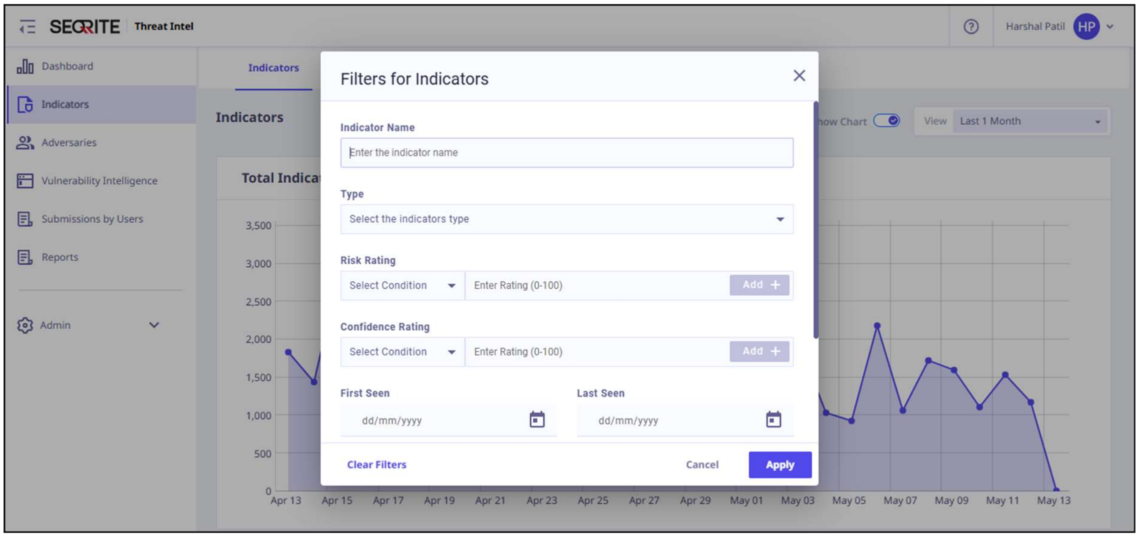
- To choose columns, click on the **Indicators** page, and select the desired column.

Note: You can choose up to 7 columns to display.

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 Intelligence portal, click **Indicators** in the left pane.
2. On the **Indicators** page, click .



3. Enter the attribute that is indicator name, type, ratings, first seen date, or the last seen date, and click **Apply**.
   The system displays filtered data.

Exporting IoC as a CSV/STIX

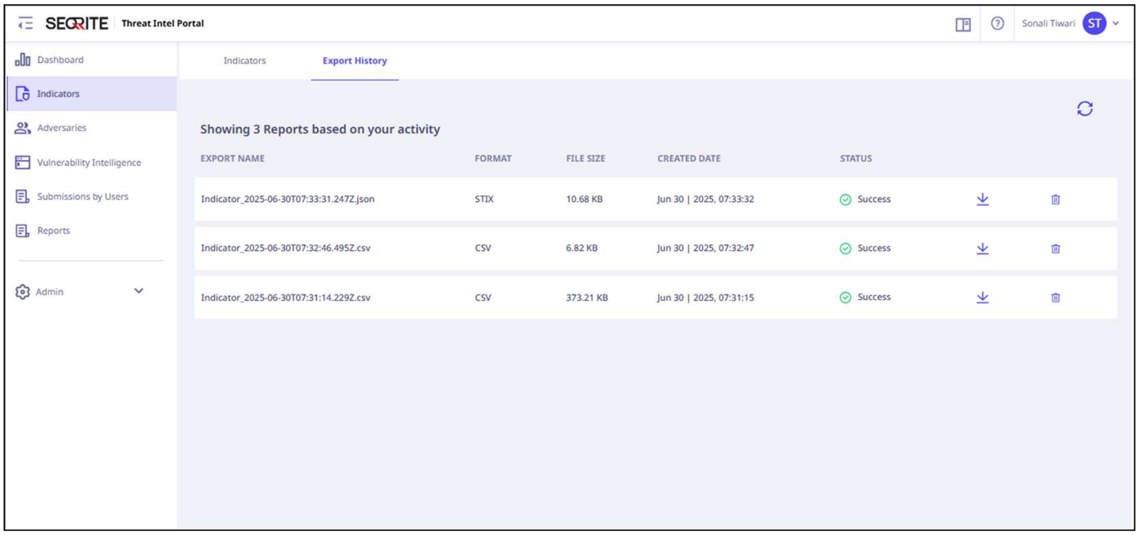
You can download all IoCs currently visible on the page in the CSV or STIX format.

To export/download the IoCs:

1. On the Seqrite Threat Intelligence 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.



Showing 3 Reports based on your activity

EXPORT NAME	FORMAT	FILE SIZE	CREATED DATE	STATUS
Indicator_2025-06-30T07:33:31.247Z.json	STIX	10.68 KB	Jun 30 | 2025, 07:33:32	Success
Indicator_2025-06-30T07:32:46.495Z.csv	CSV	6.82 KB	Jun 30 | 2025, 07:32:47	Success
Indicator_2025-06-30T07:31:14.229Z.csv	CSV	373.21 KB	Jun 30 | 2025, 07:31:15	Success

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

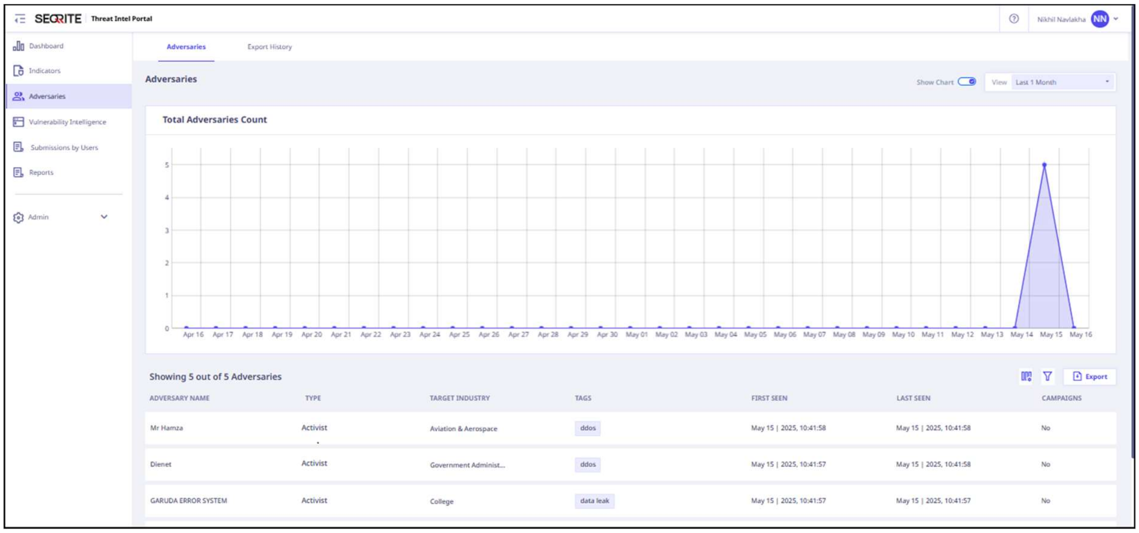
- To view the export history, click **Export History** on the **Indicators** page.

The list of exported IoCs is displayed.

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.



Showing 5 out of 5 Adversaries

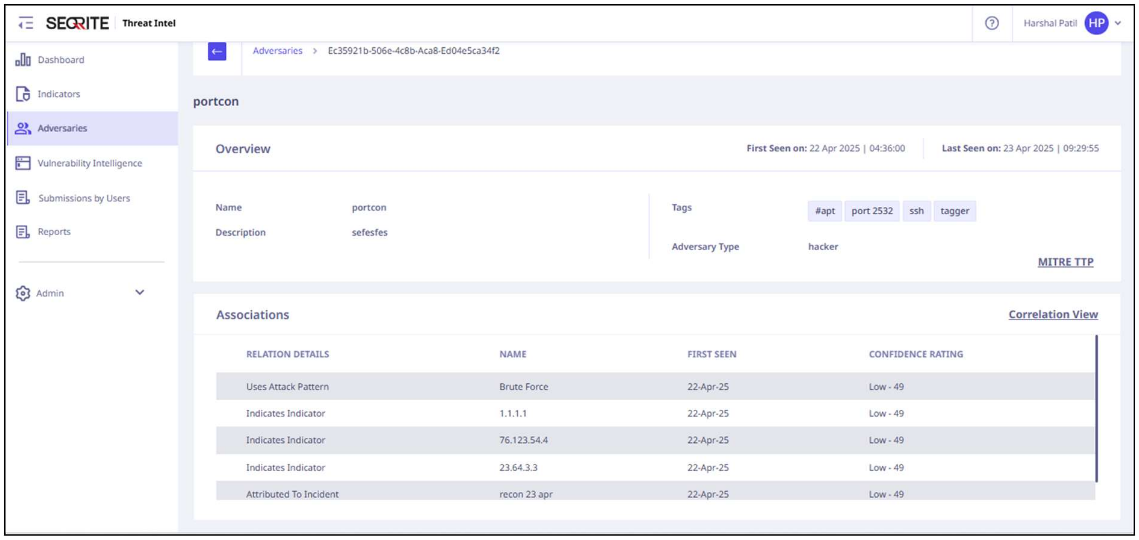
ADVERSARY NAME	TYPE	TARGET INDUSTRY	TAGS	FIRST SEEN	LAST SEEN	CAMPAIGNS
Mr Hamza	Activist	Aviation & Aerospace	ddos	May 15 | 2025, 10:41:58	May 15 | 2025, 10:41:58	No
Dienet	Activist	Government Administ...	ddos	May 15 | 2025, 10:41:57	May 15 | 2025, 10:41:58	No
GARUDA ERROR SYSTEM	Activist	College	data leak	May 15 | 2025, 10:41:57	May 15 | 2025, 10:41:57	No

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 Intelligence 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:



portcon

Overview

First Seen on: 22 Apr 2025 | 04:36:00 **Last Seen on:** 23 Apr 2025 | 09:29:55

Name portcon

Description sefesfes

Tags #apt port 2532 ssh tagger

Adversary Type hacker

Associations

RELATION DETAILS	NAME	FIRST SEEN	CONFIDENCE RATING
Uses Attack Pattern	Brute Force	22-Apr-25	Low - 49
Indicates Indicator	1.1.1.1	22-Apr-25	Low - 49
Indicates Indicator	76.123.54.4	22-Apr-25	Low - 49
Indicates Indicator	23.64.3.3	22-Apr-25	Low - 49
Attributed To Incident	recon 23 apr	22-Apr-25	Low - 49

- **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 or IoCs.

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.

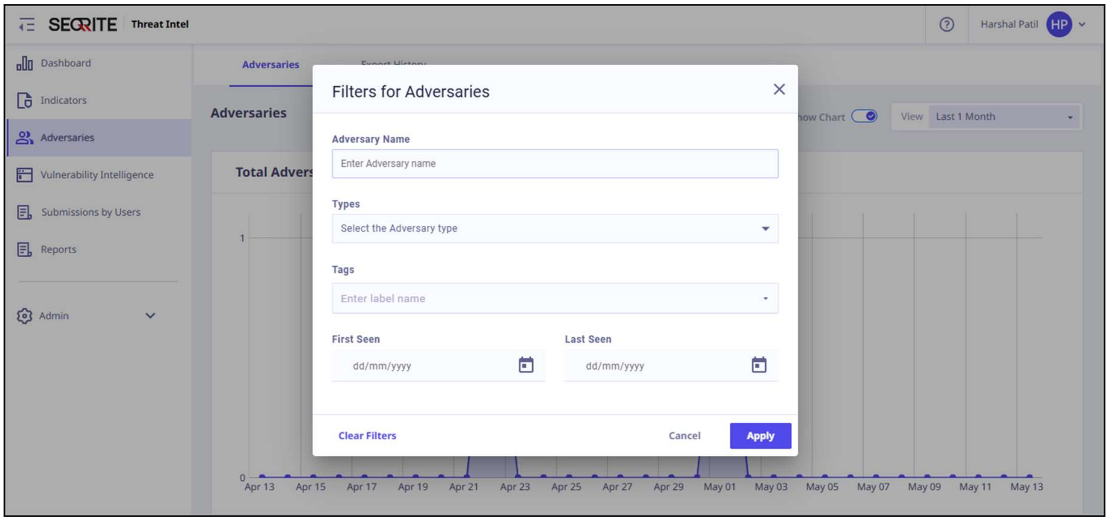
- To choose columns, click on the **Adversaries** page and select the desired column.

Note: You can choose up to 7 columns to display.

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 Intelligence portal, click **Adversaries** in the left pane.
2. On the **Adversaries** page click .
3. Enter the attribute that is adversary name, type, first seen date, or the last seen date, and click **Apply**.



Filters for Adversaries

Adversary Name: Enter Adversary name

Types: Select the Adversary type

Tags: Enter label name

First Seen: dd/mm/yyyy

Last Seen: dd/mm/yyyy

The system displays filtered data.

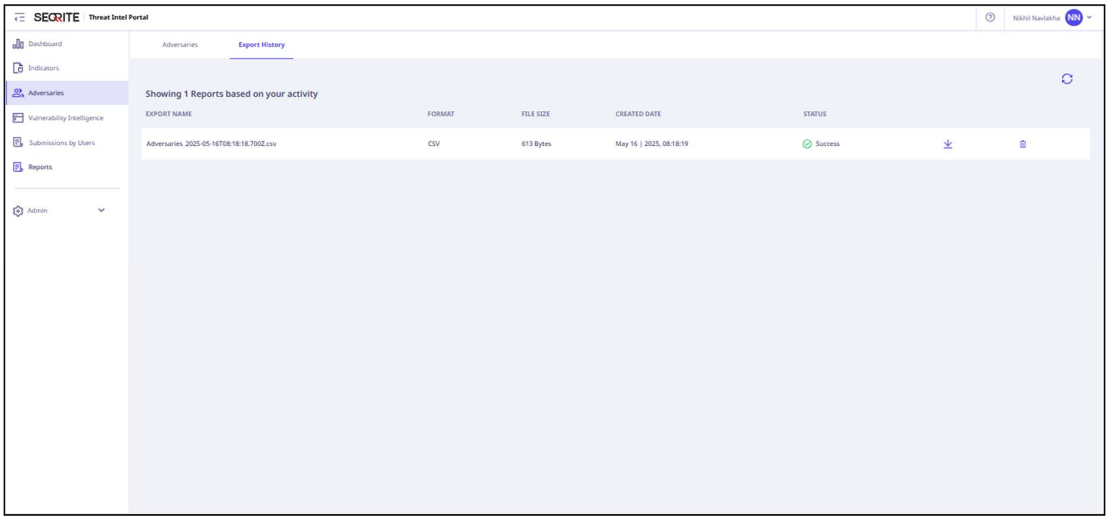
Exporting Adversaries as a CSV/STIX

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 Intelligence 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.



Showing 1 Reports based on your activity

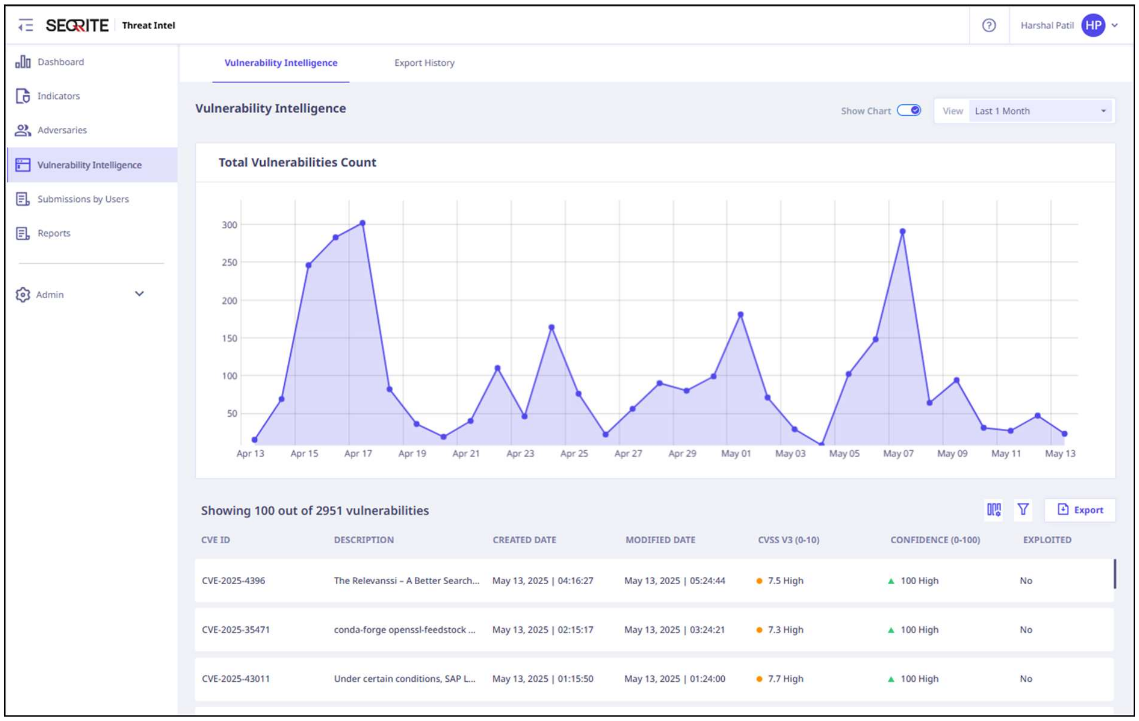
EXPORT NAME	FORMAT	FILE SIZE	CREATED DATE	STATUS
Adversaries_2025-05-16T08:18:18.700Z.csv	CSV	613 Bytes	May 16 | 2025, 08:18:19	Success

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.



Vulnerability Intelligence

Showing 100 out of 2951 vulnerabilities

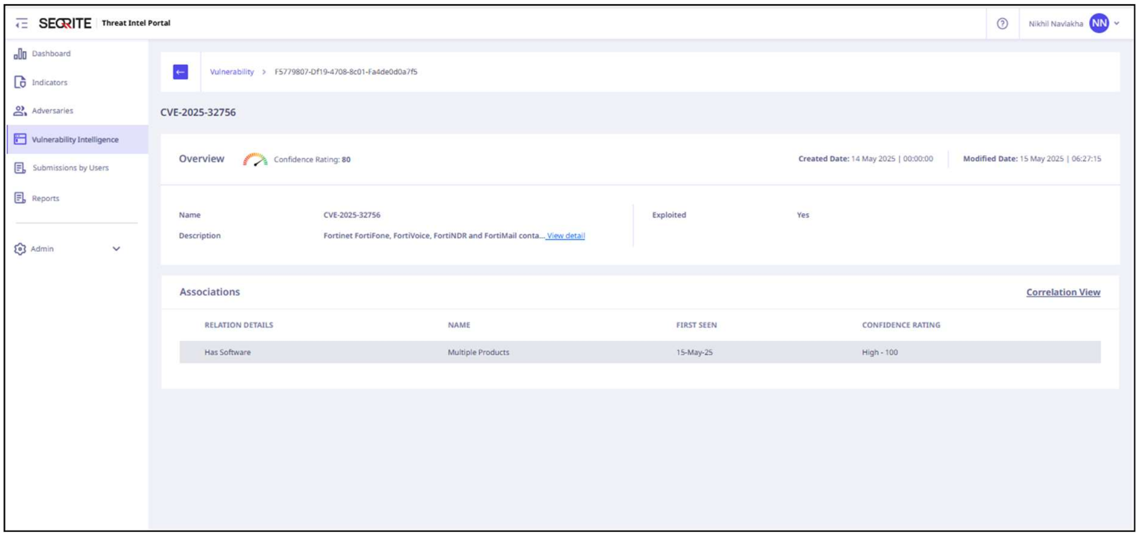
CVE ID	DESCRIPTION	CREATED DATE	MODIFIED DATE	CVSS V3 (0-10)	CONFIDENCE (0-100)	EXPLOITED
CVE-2025-4396	The Relevanssi – A Better Search...	May 13, 2025 | 04:16:27	May 13, 2025 | 05:24:44	● 7.5 High	▲ 100 High	No
CVE-2025-35471	conda-forge openssl-feedstock ...	May 13, 2025 | 02:15:17	May 13, 2025 | 03:24:21	● 7.3 High	▲ 100 High	No
CVE-2025-43011	Under certain conditions, SAP L...	May 13, 2025 | 01:15:50	May 13, 2025 | 01:24:00	● 7.7 High	▲ 100 High	No

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, CVSS V3 Score, confidence and exploited in the tabular format. To view the details of each vulnerability, follow these steps:

1. On the Seqrite Threat Intelligence 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:



Vulnerability > F5779807-Df19-4708-8c01-Fa4de0d0a7f5

CVE-2025-32756

Overview Confidence Rating: **80**

Created Date: 14 May 2025 | 00:00:00 **Modified Date:** 15 May 2025 | 06:27:15

Name CVE-2025-32756

Description Fortinet FortiFone, FortiVoice, FortiNDR and FortiMail conta... View detail

Exploited Yes

Associations

RELATION DETAILS	NAME	FIRST SEEN	CONFIDENCE RATING
Has Software	Multiple Products	15-May-25	High - 100

- **Overview**: CVE Name/ID, Description, Tags, CVSS Score, affected products, risk score, External References, Confidentiality, Integrity, Availability (CIA) Impact.
- **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.

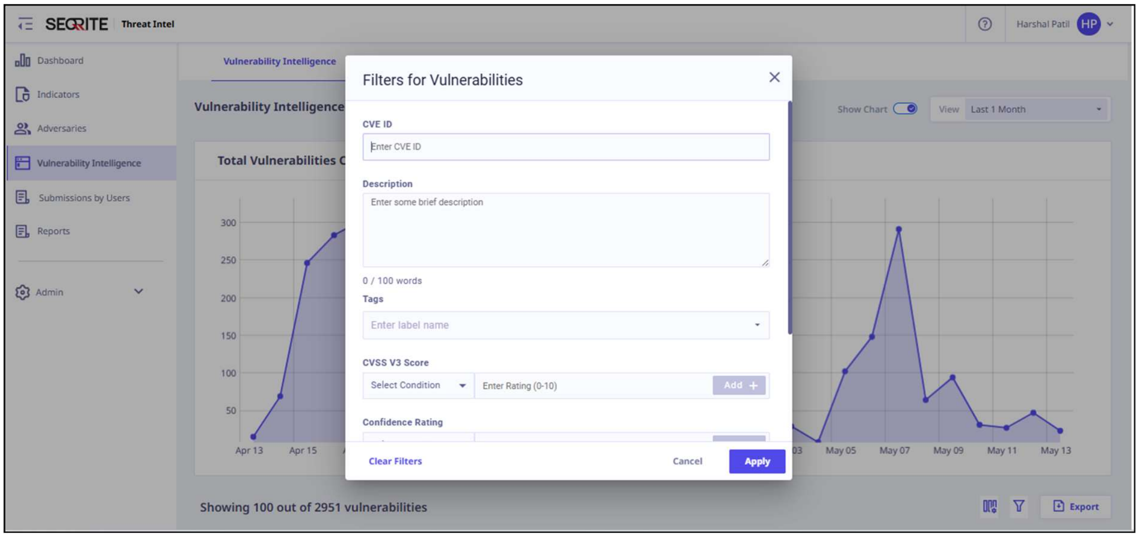
- To choose columns, click on the Vulnerability Intelligence page, and choose the desired column.

Note: You can choose up to 7 columns to display.

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 Intelligence 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**.



Filters for Vulnerabilities

CVE ID: Enter CVE ID

Description: Enter some brief description

0 / 100 words

Tags: Enter label name

CVSS V3 Score: Select Condition | Enter Rating (0-10) | Add +

Confidence Rating

Clear Filters | Cancel | Apply

Showing 100 out of 2951 vulnerabilities

The system displays filtered data.

Exporting Vulnerabilities as a CSV/STIX

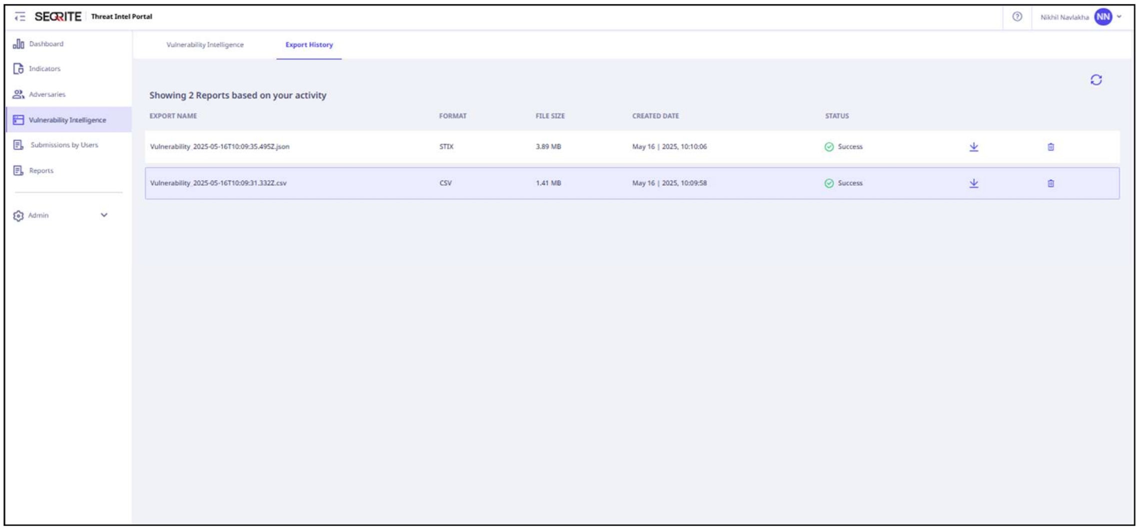
You can download all the vulnerabilities currently visible on the page in the CSV or STIX format.

To export/download vulnerabilities, follow these steps:

1. On the Seqrite Threat Intelligence 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.



Showing 2 Reports based on your activity

EXPORT NAME	FORMAT	FILE SIZE	CREATED DATE	STATUS		
Vulnerability_2025-05-16T10:09:35.495Z.json	STIX	3.89 MB	May 16 | 2025, 10:10:06	✓ Success	⤓	🗑
Vulnerability_2025-05-16T10:09:31.332Z.csv	CSV	1.41 MB	May 16 | 2025, 10:09:58	✓ Success	⤓	🗑

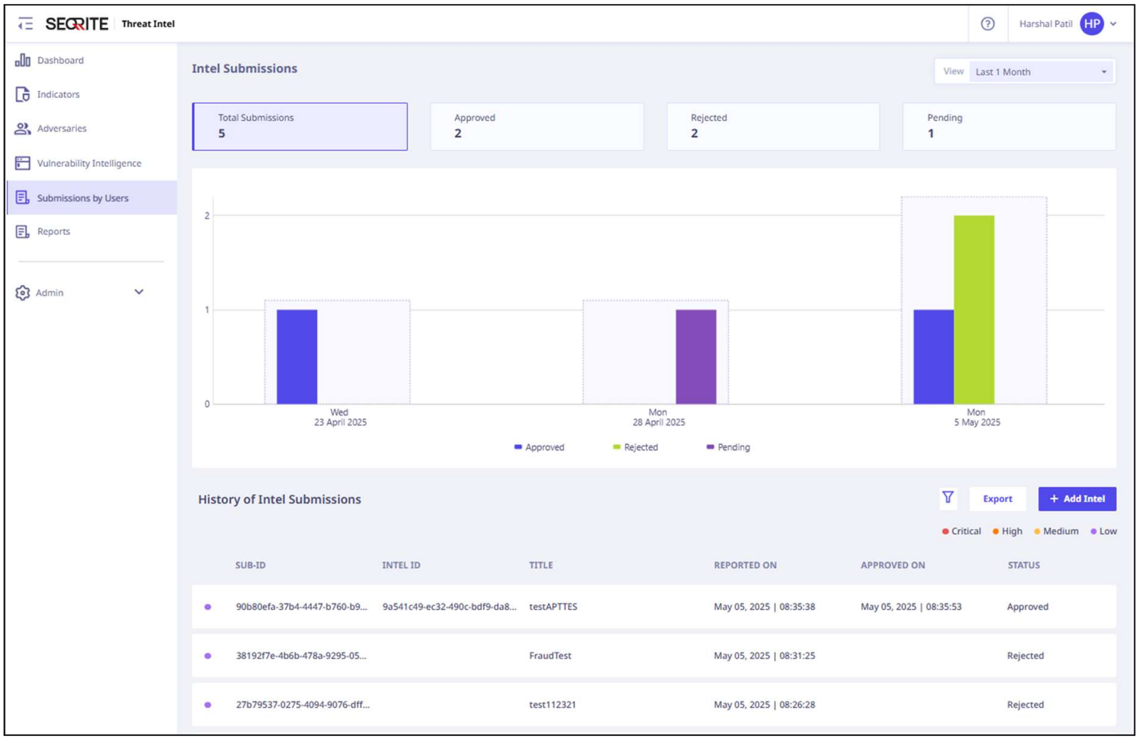
Export History provides a record that is export name, format (STIX or CSV), file size, created date, and status.

- 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.



Intel Submissions

View: Last 1 Month

Total Submissions: 5

Approved: 2

Rejected: 2

Pending: 1

History of Intel Submissions

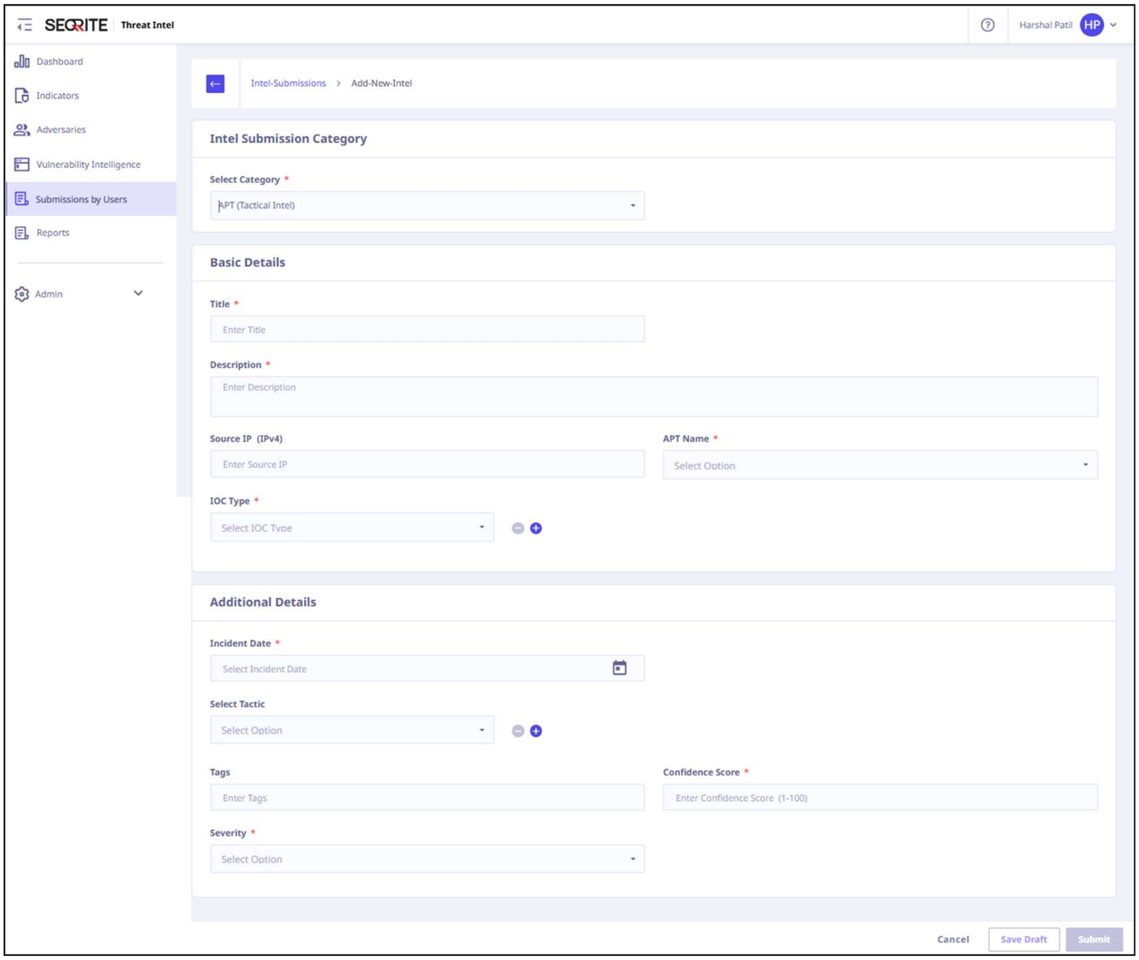
SUB-ID	INTEL ID	TITLE	REPORTED ON	APPROVED ON	STATUS
90b80efa-37b4-4447-b760-b9...	9a541c49-ec32-490c-bdf9-da8...	testAPTTES	May 05, 2025 | 08:35:38	May 05, 2025 | 08:35:53	Approved
38192f7e-4b6b-478a-9295-05...		FraudTest	May 05, 2025 | 08:31:25		Rejected
27b79537-0275-4094-9076-dff...		test112321	May 05, 2025 | 08:26:28		Rejected

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 a new intel, follow these steps:

1. On the Seqrite Threat Intelligence 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. Select the **Category** from the list, enter **Basic Details** and **Additional Details**.
4. If you want to review the intel before submission, click **Save Draft** else click **Submit**.



Intel Submission Category

Select Category *: APT (Tactical Intel)

Basic Details

Title *: Enter Title

Description *: Enter Description

Source IP (IPv4): Enter Source IP

APT Name *: Select Option

IOC Type *: Select IOC Type

Additional Details

Incident Date *: Select Incident Date

Select Tactic: Select Option

Tags: Enter Tags

Confidence Score *: Enter Confidence Score (1-100)

Severity *: Select Option

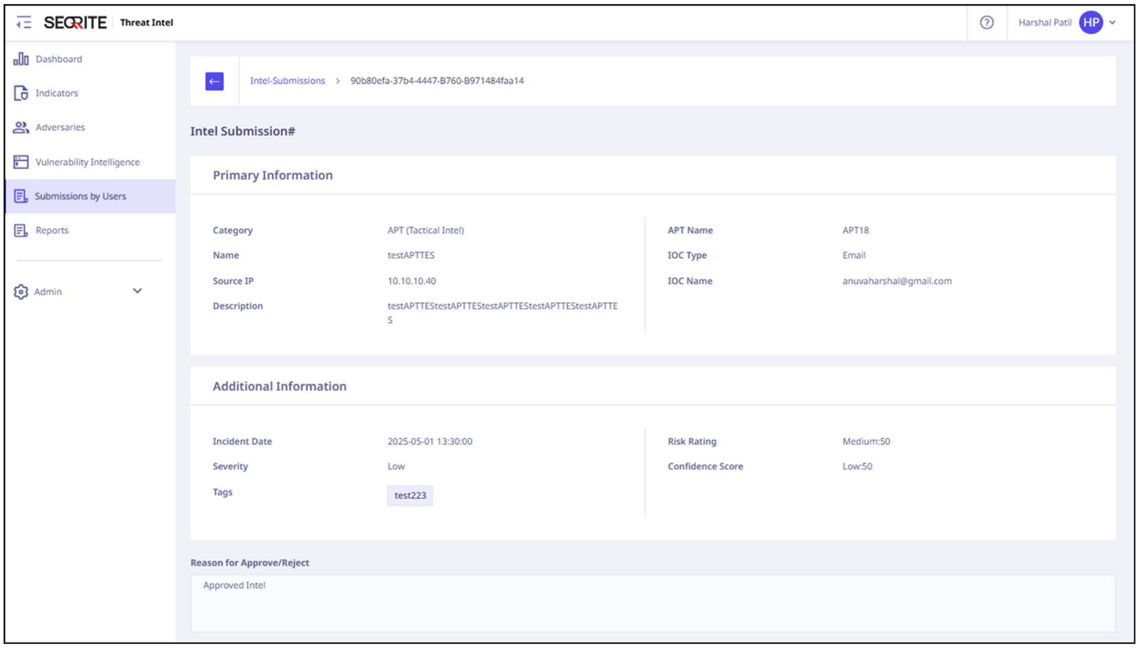
This provision is also available to Org/Regulated Entity Admins as well.

Viewing the Submitted Intel

You can view the intel submissions details such as severity (Critical, High, Medium, Low) highlighted with the color codes, Sub ID (Submission ID), Intel ID, title, reported on, approved on, and the status in the tabular format.

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

1. On the Seqrite Threat Intelligence 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:



Intel Submission#

Primary Information

Category	APT (Tactical Intel)	APT Name	APT18
Name	testAPTTES	IOC Type	Email
Source IP	10.10.10.40	IOC Name	anuvaharshal@gmail.com
Description	testAPTTEStestAPTTEStestAPTTEStestAPTTEStestAPTTES		

Additional Information

Incident Date	2025-05-01 13:30:00	Risk Rating	Medium:50
Severity	Low	Confidence Score	Low:50
Tags	test223		

Reason for Approve/Reject

Approved Intel

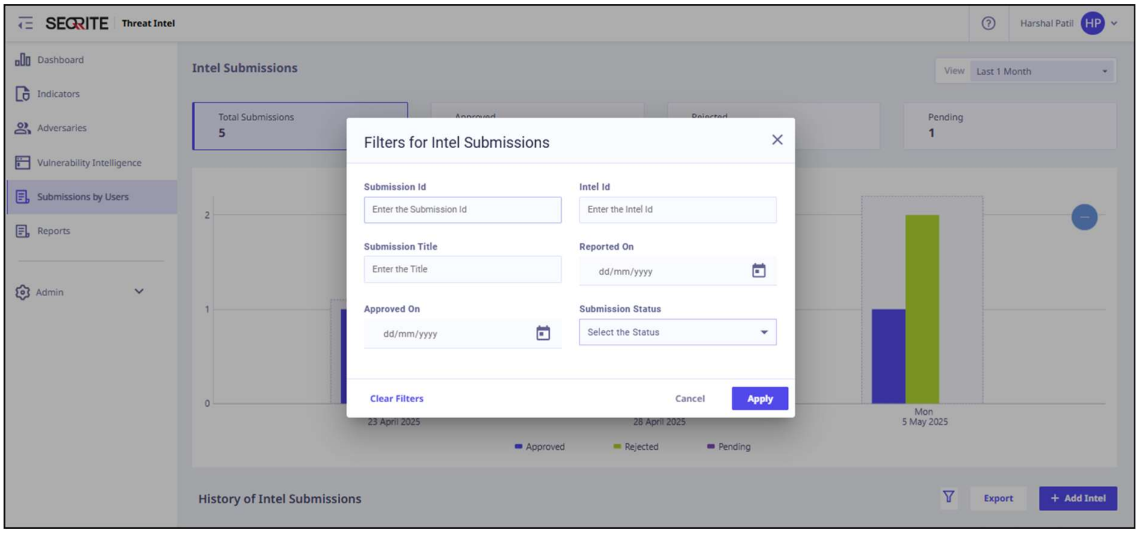
- **Primary Information**: For example, APT Category (Category, Name, Source IP, Description, APT Name, IoC Type, IoC Name)
- **Additional Information**: Incident Date, Severity, Tags, Risk ratings, and Confidence Core.
- **Reason for Approve/Reject**: Shows reason for intel approval or rejection.

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 Intelligence 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.

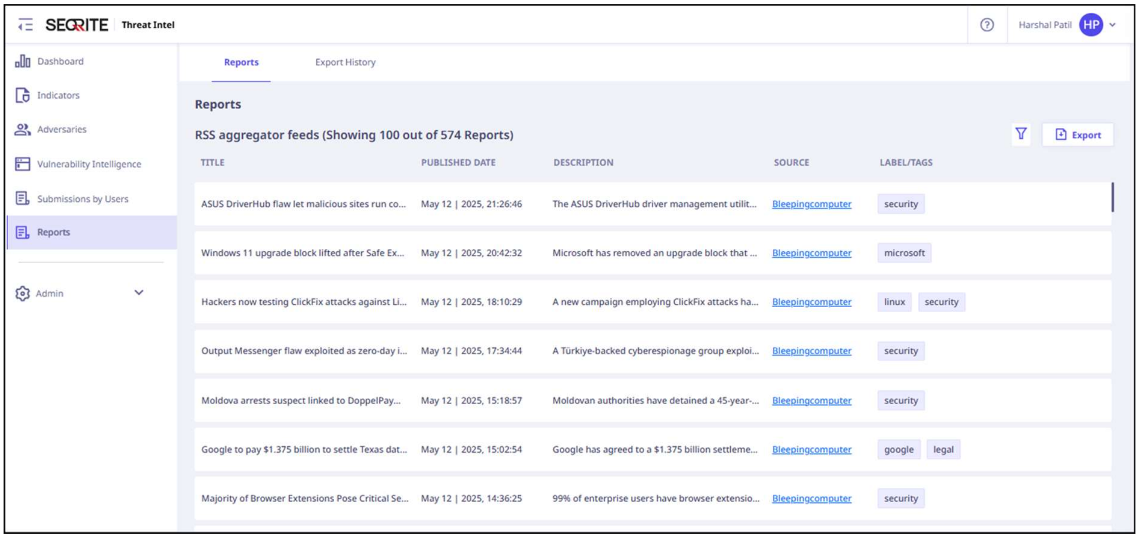
Exporting Intel Submissions as a CSV

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 Intelligence porta, click **Submissions by Users** in the left pane.
2. On the **Submissions by Users** page click **Export CSV**.

Reports

Seqrite Threat Intelligence 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.



Reports

RSS aggregator feeds (Showing 100 out of 574 Reports)

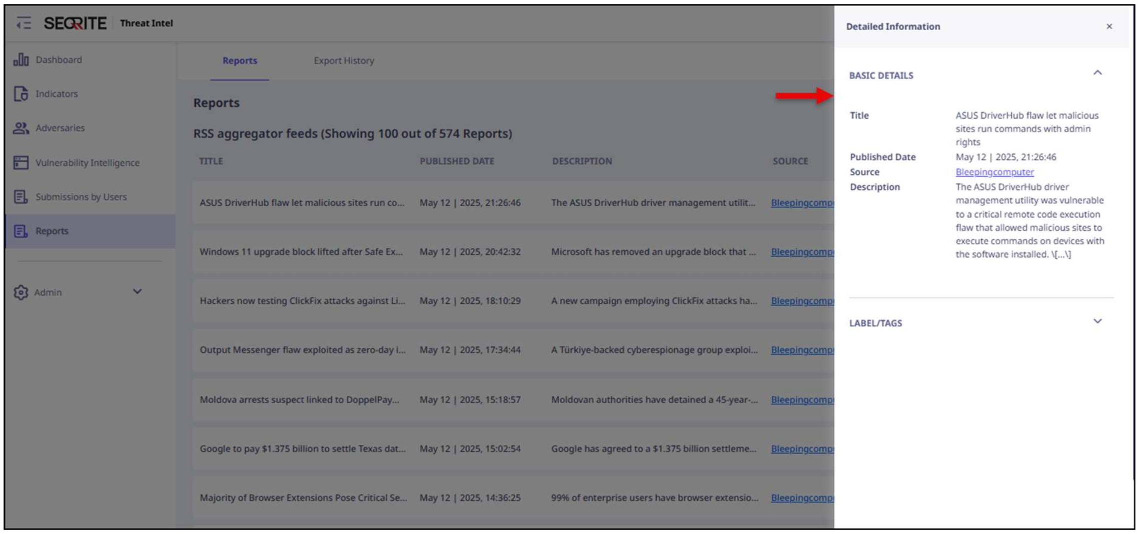
TITLE	PUBLISHED DATE	DESCRIPTION	SOURCE	LABEL/TAGS
ASUS DriverHub flaw let malicious sites run co...	May 12 | 2025, 21:26:46	The ASUS DriverHub driver management utilit...	Bleepingcomputer	security
Windows 11 upgrade block lifted after Safe Ex...	May 12 | 2025, 20:42:32	Microsoft has removed an upgrade block that ...	Bleepingcomputer	microsoft
Hackers now testing ClickFix attacks against Li...	May 12 | 2025, 18:10:29	A new campaign employing ClickFix attacks ha...	Bleepingcomputer	linux security
Output Messenger flaw exploited as zero-day i...	May 12 | 2025, 17:34:44	A Türkiye-backed cyberespionage group exploi...	Bleepingcomputer	security
Moldova arrests suspect linked to DoppelPay...	May 12 | 2025, 15:18:57	Moldovan authorities have detained a 45-year-...	Bleepingcomputer	security
Google to pay $1.375 billion to settle Texas dat...	May 12 | 2025, 15:02:54	Google has agreed to a $1.375 billion settleme...	Bleepingcomputer	google legal
Majority of Browser Extensions Pose Critical Se...	May 12 | 2025, 14:36:25	99% of enterprise users have browser extensio...	Bleepingcomputer	security

Viewing Reports

You can view a report detail such as title, published date, source, source, description, and label/tags assigned to the report. To view the reports, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Reports** in the left pane.

2. On the **Reports** page, select the report and click the **>** icon.
   The **Detailed Information** page displays the following details:



Reports

RSS aggregator feeds (Showing 100 out of 574 Reports)

TITLE	PUBLISHED DATE	DESCRIPTION	SOURCE
ASUS DriverHub flaw let malicious sites run co...	May 12 | 2025, 21:26:46	The ASUS DriverHub driver management utilit...	Bleepingcomp
Windows 11 upgrade block lifted after Safe Ex...	May 12 | 2025, 20:42:32	Microsoft has removed an upgrade block that ...	Bleepingcomp
Hackers now testing ClickFix attacks against Li...	May 12 | 2025, 18:10:29	A new campaign employing ClickFix attacks ha...	Bleepingcomp
Output Messenger flaw exploited as zero-day i...	May 12 | 2025, 17:34:44	A Türkiye-backed cyberespionage group exploi...	Bleepingcomp
Moldova arrests suspect linked to DoppelPay...	May 12 | 2025, 15:18:57	Moldovan authorities have detained a 45-year-...	Bleepingcomp
Google to pay $1.375 billion to settle Texas dat...	May 12 | 2025, 15:02:54	Google has agreed to a $1.375 billion settleme...	Bleepingcomp
Majority of Browser Extensions Pose Critical Se...	May 12 | 2025, 14:36:25	99% of enterprise users have browser extensio...	Bleepingcomp

Detailed Information

BASIC DETAILS

Title: ASUS DriverHub flaw let malicious sites run commands with admin rights
Published Date: May 12 | 2025, 21:26:46
Source: Bleepingcomputer
Description: The ASUS DriverHub driver management utility was vulnerable to a critical remote code execution flaw that allowed malicious sites to execute commands on devices with the software installed. \[...\]

LABEL/TAGS

- **Basic Details**: Report title, description, published date, source, and description.

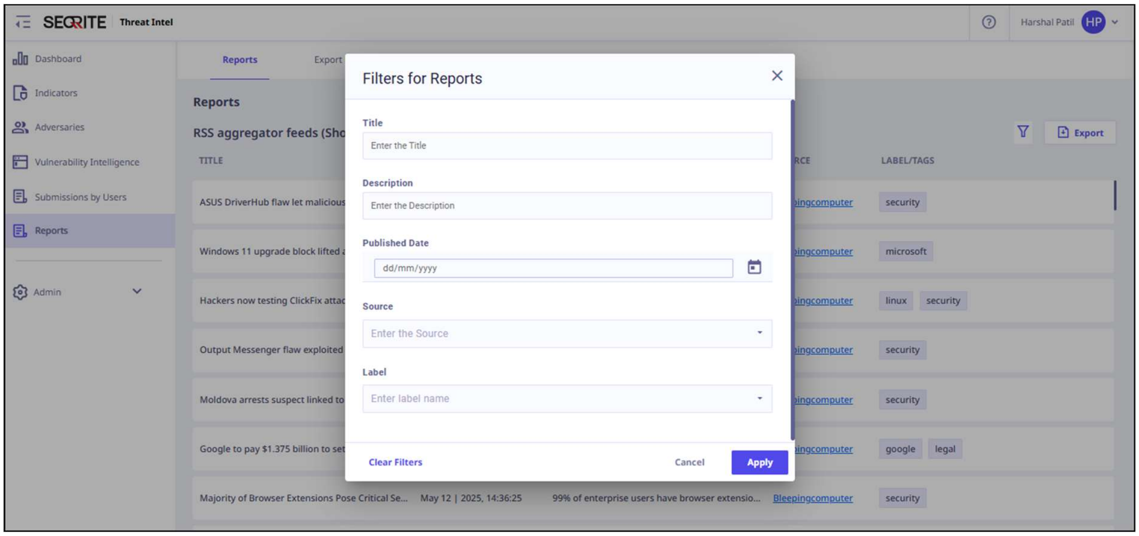
- **Label/Tag**: Shows the tags or labels assigned to the report.

Filtering the Reports List

You can filter the reports list to refine results based on title, description, published date, source, and label.

To filter the reports list, follow these steps:

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



The system displays filtered data.

Exporting Reports as a CSV/STIX

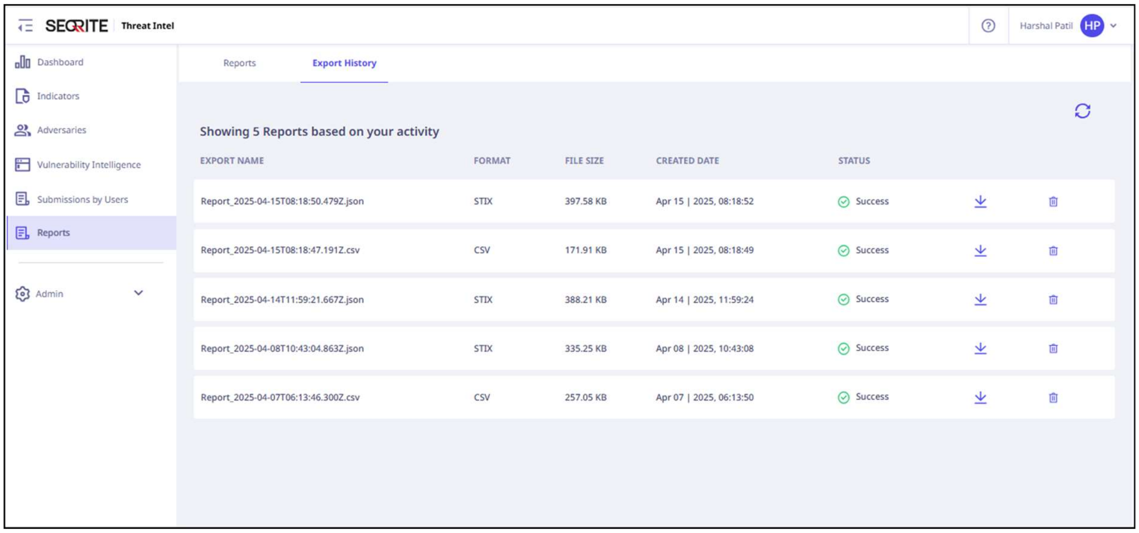
You can download all the reports currently visible on the page in the CSV or STIX format.

To export/download reports, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Reports** in the left pane.
2. On the **Reports** 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 reports are exported by the user. This information tracks the usage of reports and can be useful in auditing and accountability purposes.



Showing 5 Reports based on your activity

EXPORT NAME	FORMAT	FILE SIZE	CREATED DATE	STATUS
Report_2025-04-15T08:18:50.479Z.json	STIX	397.58 KB	Apr 15 | 2025, 08:18:52	Success
Report_2025-04-15T08:18:47.191Z.csv	CSV	171.91 KB	Apr 15 | 2025, 08:18:49	Success
Report_2025-04-14T11:59:21.667Z.json	STIX	388.21 KB	Apr 14 | 2025, 11:59:24	Success
Report_2025-04-08T10:43:04.863Z.json	STIX	335.25 KB	Apr 08 | 2025, 10:43:08	Success
Report_2025-04-07T06:13:46.300Z.csv	CSV	257.05 KB	Apr 07 | 2025, 06:13:50	Success

Export History provides a record that is report name, file size, created date, the format in which the reports were exported (STIX, CSV), and status.

To view the export history, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Reports** in the left pane**.**
2. On the **Reports** page click **Export History**.

The list of exported reports is displayed.

Admin

Within Seqrite Threat Intelligence, Seqrite admin has the authority to add and edit organizations, add users, and assign user roles, and edit and disable user.
The following user roles are present in Seqrite Threat Intelligence:

1. Admin: Admins have all the privileges to add and edit organization, add and edit user, assign user role, and disable organization and user.
2. Org Admin: Org admin can add, edit, and disable users under their organization.
3. Org Analyst: Org analyst can access only Dashboard and Indicators tabs.

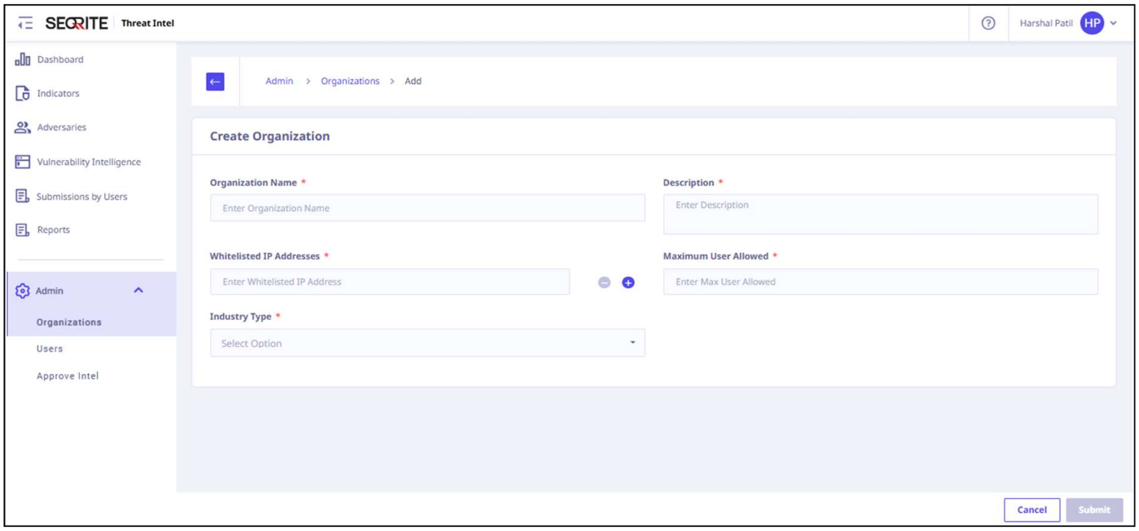
Organizations

The **Organizations** tab allows you to manage organizations within Seqrite Threat Intelligence. It allows you to add a new organization, edit an existing organization, and disable the organization as needed.

Adding Organization

To add the organization, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Admin** and select **Organizations** in the left pane.
2. On the **Admin Organizations** page, click **+Add Organization**.
   The **Create Organization** page is displayed.

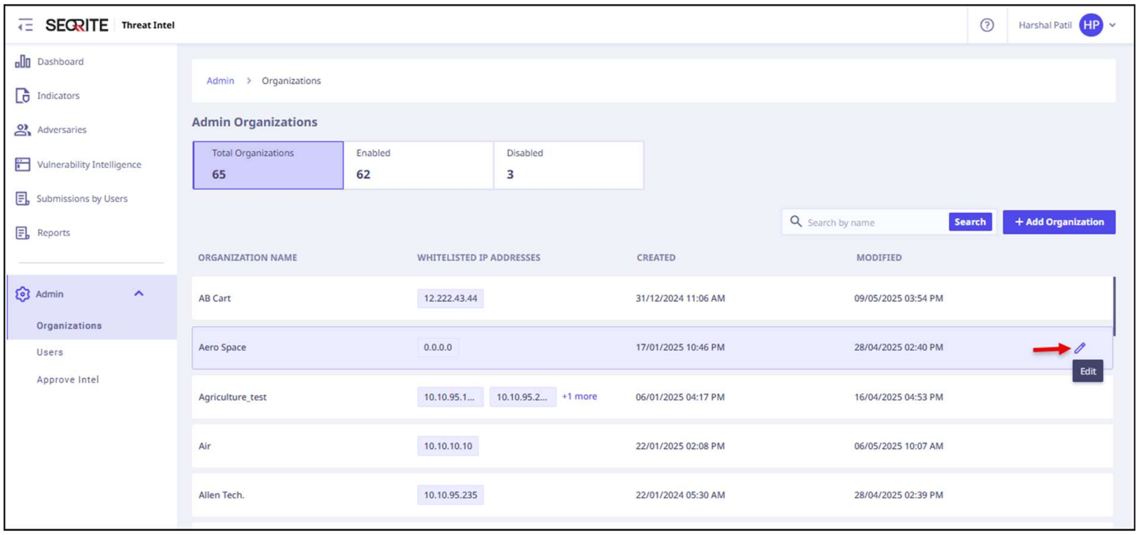


3. Enter the organization name, description, and whitelisted IP address.
4. Select the industry type from the list and click **Save**.

Editing Organization

To modify or edit the existing organization, follow these steps:

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

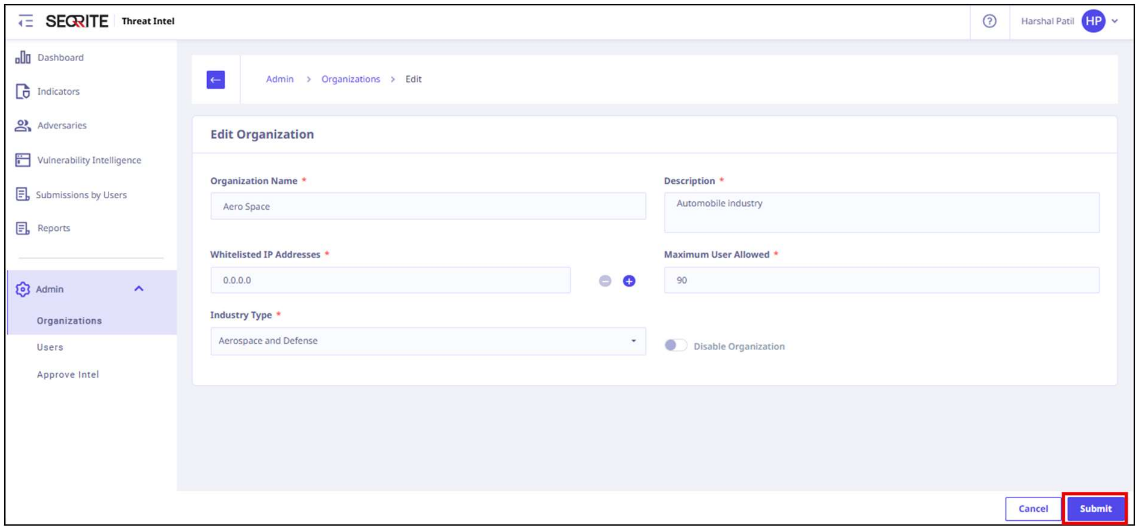


Admin Organizations

Total Organizations 65
Enabled 62
Disabled 3

ORGANIZATION NAME	WHITELISTED IP ADDRESSES	CREATED	MODIFIED
AB Cart	12.222.43.44	31/12/2024 11:06 AM	09/05/2025 03:54 PM
Aero Space	0.0.0.0	17/01/2025 10:46 PM	28/04/2025 02:40 PM
Agriculture_test	10.10.95.1... 10.10.95.2... +1 more	06/01/2025 04:17 PM	16/04/2025 04:53 PM
Air	10.10.10.10	22/01/2025 02:08 PM	06/05/2025 10:07 AM
Allen Tech.	10.10.95.235	22/01/2024 05:30 AM	28/04/2025 02:39 PM

3. Edit the organization details and click **Save**.



Edit Organization

Organization Name * Aero Space

Description * Automobile industry

Whitelisted IP Addresses * 0.0.0.0

Maximum User Allowed * 90

Industry Type * Aerospace and Defense

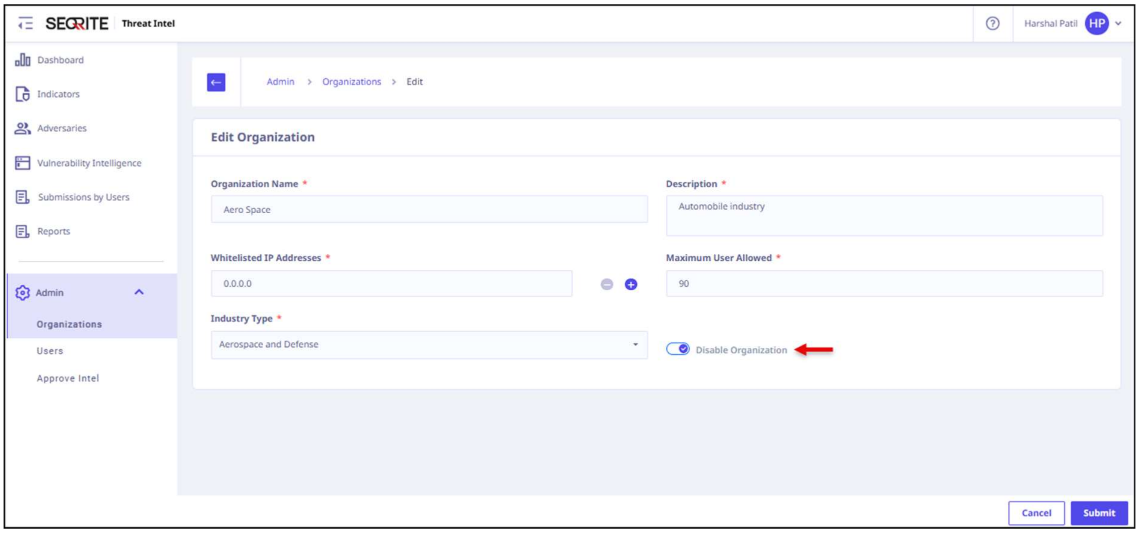
○ Disable Organization

Disable Organization

To disable the organization, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Admin** and select **Organizations** in the left pane.
2. On the **Admin Organizations** page, click the **Edit** icon for the organization that you want to disable.

3. Switch the **Disable Organization** toggle and click **Save**.



Edit Organization

Organization Name * Aero Space

Description * Automobile industry

Whitelisted IP Addresses * 0.0.0.0

Maximum User Allowed * 90

Industry Type * Aerospace and Defense

Disable Organization

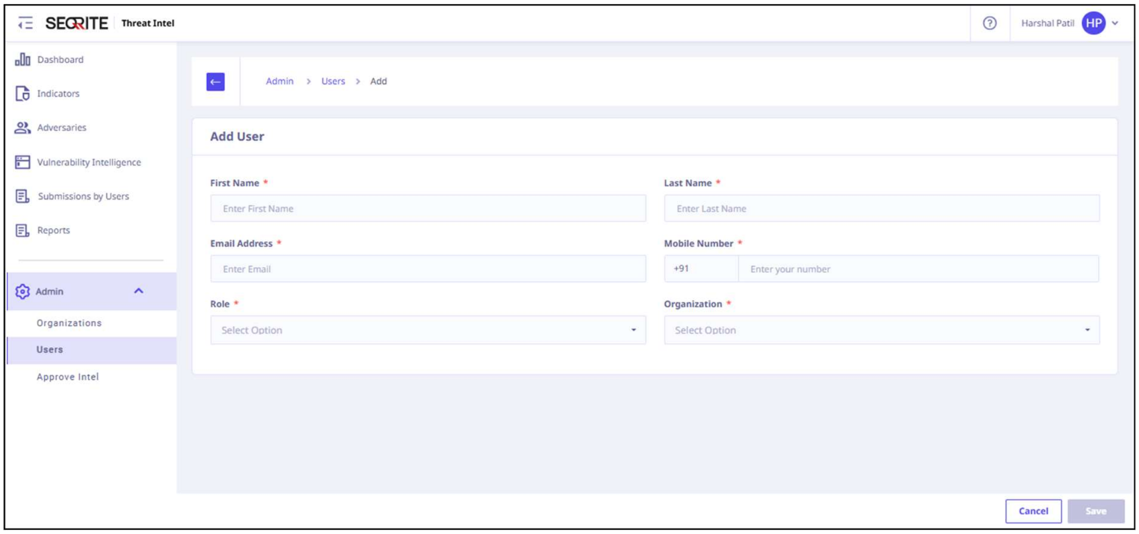
Users

The **Users** tab allows you to view, manage, add users, and assign appropriate roles to users. It provides an overview of all role types within the Seqrite Threat Intelligence. You can also edit user details and disable users as needed.

Adding a User

To add a user, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Admin** and select **Users** in the left pane.
2. On the **Admin Users** page, click **+Add User**.
   The **Add User** page is displayed.



Add User

First Name * Enter First Name

Last Name * Enter Last Name

Email Address * Enter Email

Mobile Number * +91 Enter your number

Role * Select Option

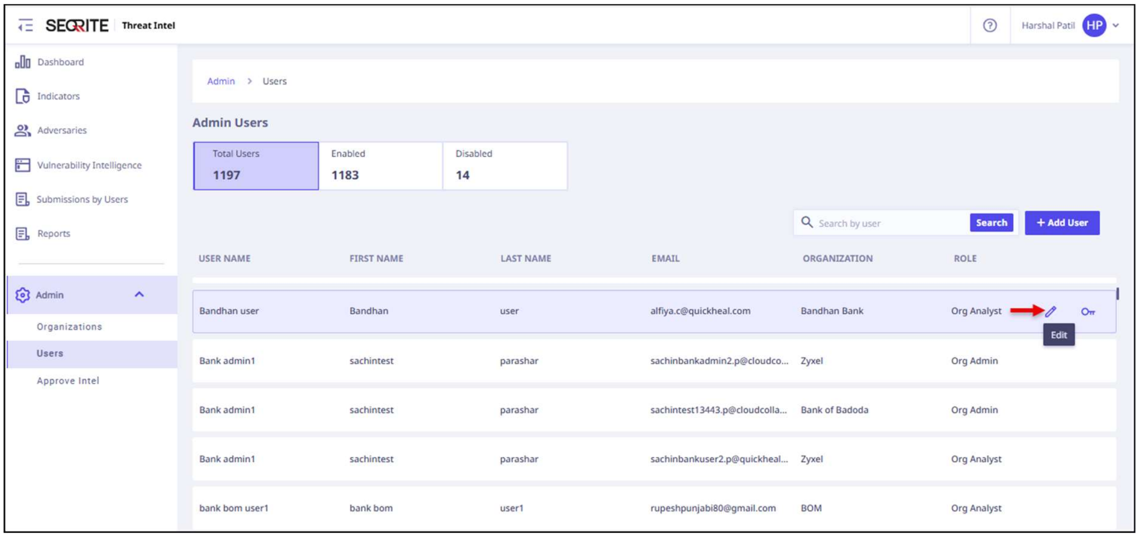
Organization * Select Option

3. Enter first name, last name, email address, and mobile number.
4. Select the role and organization from the respective lists and click **Save**.

Editing a User

To modify or edit the existing user, follow these steps:

1. On the Seqrite Threat Intelligence 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.

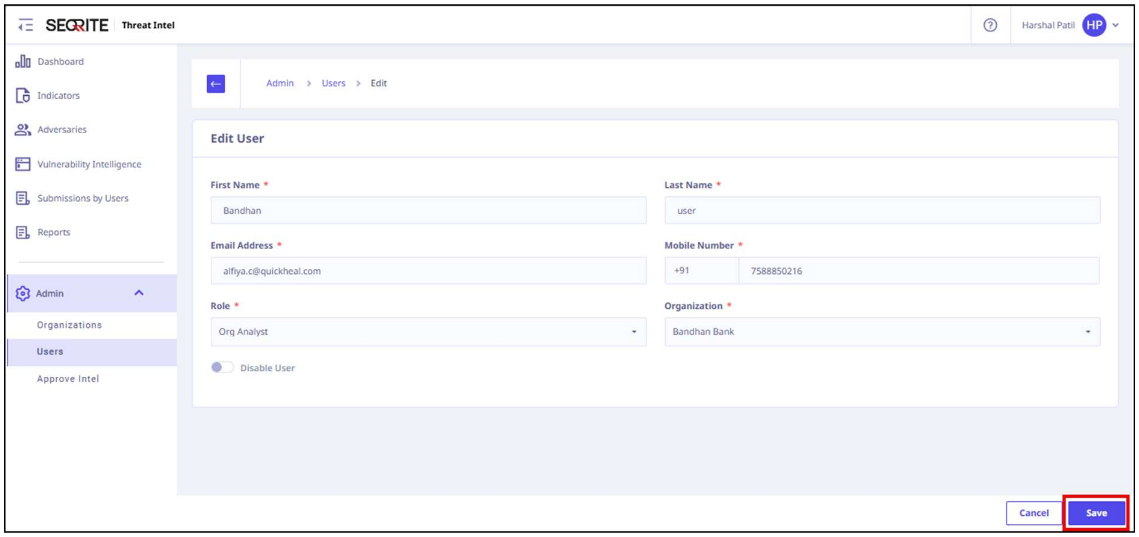


Admin Users

Total Users	Enabled	Disabled
1197	1183	14

USER NAME	FIRST NAME	LAST NAME	EMAIL	ORGANIZATION	ROLE
Bandhan user	Bandhan	user	alfiya.c@quickheal.com	Bandhan Bank	Org Analyst
Bank admin1	sachintest	parashar	sachinbankadmin2.p@cloudco...	Zyxel	Org Admin
Bank admin1	sachintest	parashar	sachintest13443.p@cloudcolla...	Bank of Badoda	Org Admin
Bank admin1	sachintest	parashar	sachinbankuser2.p@quickheal...	Zyxel	Org Analyst
bank bom user1	bank bom	user1	rupeshpunjabi80@gmail.com	BOM	Org Analyst

3. Edit the user details and click **Save**.



Edit User

First Name * Bandhan

Last Name * user

Email Address * alfiya.c@quickheal.com

Mobile Number * +91 7588850216

Role * Org Analyst

Organization * Bandhan Bank

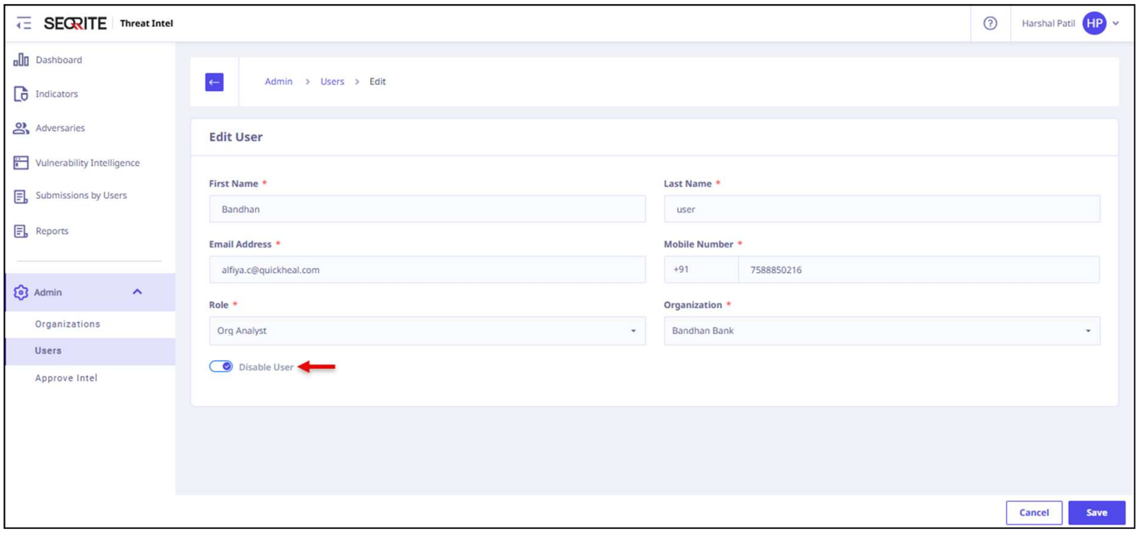
Disable User

This provision is available to Org Admins as well.

Disable a User

To disable a user, follow these steps:

1. On the Seqrite Threat Intelligence 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**.



Edit User

First Name *	Last Name *
Bandhan	user
Email Address *	Mobile Number *
alfiya.c@quickheal.com	+91 7588850216
Role *	Organization *
Org Analyst	Bandhan Bank

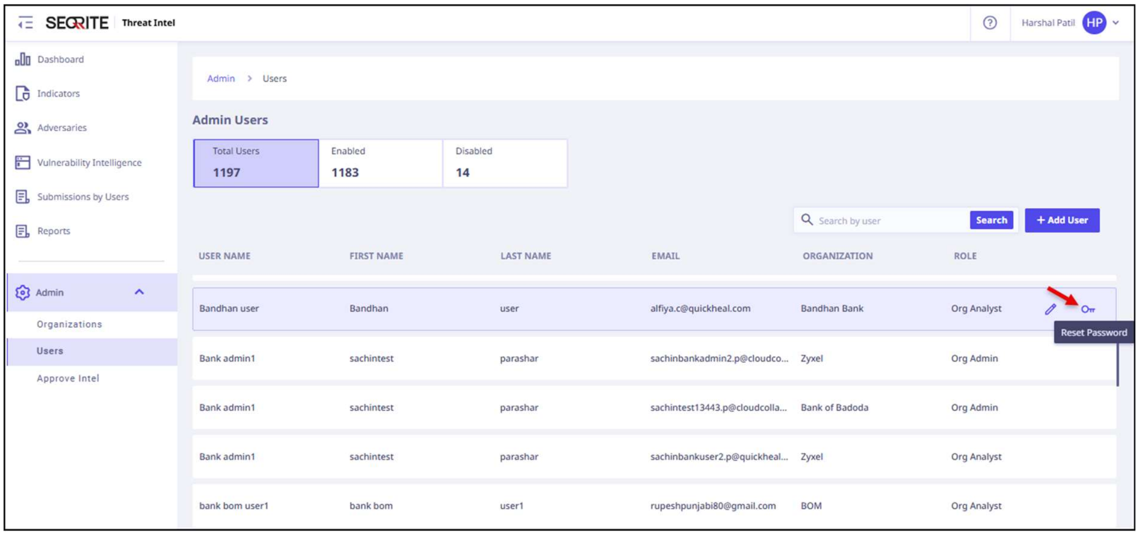
Disable User

This provision is available to Org Admins as well.

Reset User Password

To reset the user password, follow these steps:

1. On the Seqrite Threat Intelligence 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.



Admin Users

Total Users	Enabled	Disabled
1197	1183	14

USER NAME	FIRST NAME	LAST NAME	EMAIL	ORGANIZATION	ROLE
Bandhan user	Bandhan	user	alfiya.c@quickheal.com	Bandhan Bank	Org Analyst
Bank admin1	sachintest	parashar	sachinbankadmin2.p@cloudco...	Zyxel	Org Admin
Bank admin1	sachintest	parashar	sachintest13443.p@cloudcolla...	Bank of Badoda	Org Admin
Bank admin1	sachintest	parashar	sachinbankuser2.p@quickheal...	Zyxel	Org Analyst
bank bom user1	bank bom	user1	rupeshpunjabi80@gmail.com	BOM	Org Analyst

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

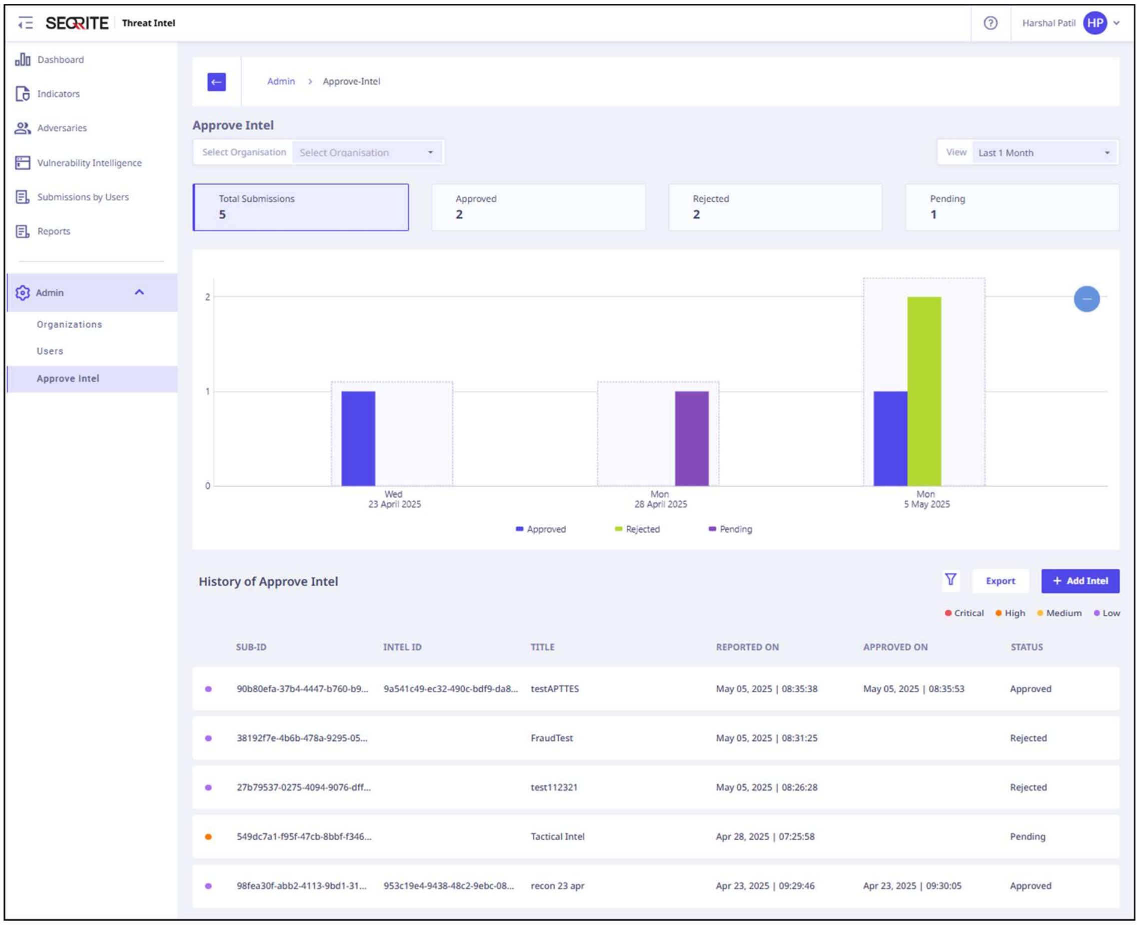
Approve Intel

The Approve Intel tab allows you to review and approve all intel submitted by users. Seqrite Admin will review and approve intel entries before they are published. Additionally, Seqrite Admin can add new intel and can also view the intel submissions categorized by organization.

Viewing the Approve Intel

Seqrite Admin can view the intel submissions details such as severity (Critical, High, Medium, Low) highlighted with the color codes, Sub ID (Submission ID), Intel ID, title, reported on, approved on, and the status in the tabular format.
To view the details of each intel, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Admin** and select **Approve Intel** in the left pane.
2. On the **Approve Intel** page, select the intel and click the **>** icon.



Total Submissions	Approved	Rejected	Pending
5	2	2	1

	SUB-ID	INTEL ID	TITLE	REPORTED ON	APPROVED ON	STATUS
●	90b80efa-37b4-4447-b760-b9...	9a541c49-ec32-490c-bdf9-da8...	testAPTTES	May 05, 2025 | 08:35:38	May 05, 2025 | 08:35:53	Approved
●	38192f7e-4b6b-478a-9295-05...		FraudTest	May 05, 2025 | 08:31:25		Rejected
●	27b79537-0275-4094-9076-dff...		test112321	May 05, 2025 | 08:26:28		Rejected
●	549dc7a1-f95f-47cb-8bbf-f346...		Tactical Intel	Apr 28, 2025 | 07:25:58		Pending
●	98fea30f-abb2-4113-9bd1-31...	953c19e4-9438-48c2-9ebc-08...	recon 23 apr	Apr 23, 2025 | 09:29:46	Apr 23, 2025 | 09:30:05	Approved

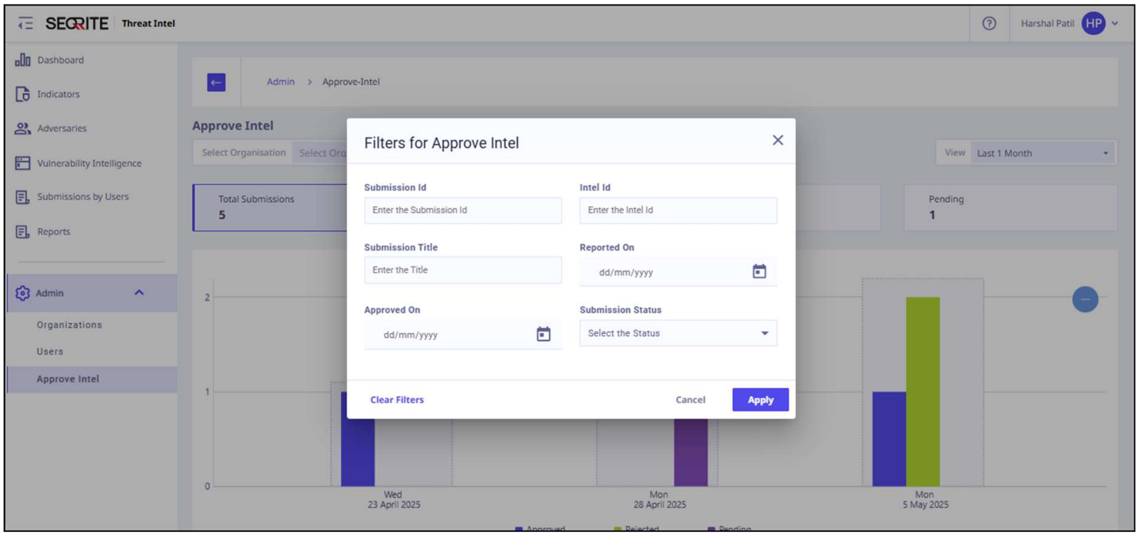
The approve intel page displays details such as, Primary Information, Additional information and TTP mappings submitted by intel submitter.

Filtering the Intel Submissions List

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

1. On the Seqrite Threat Intelligence portal, click **Admin** and select **Approve Intel** in the left pane.
2. On the **Approve Intel** 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**.



Filters for Approve Intel

Submission Id: Enter the Submission Id	Intel Id: Enter the Intel Id
Submission Title: Enter the Title	Reported On: dd/mm/yyyy
Approved On: dd/mm/yyyy	Submission Status: Select the Status

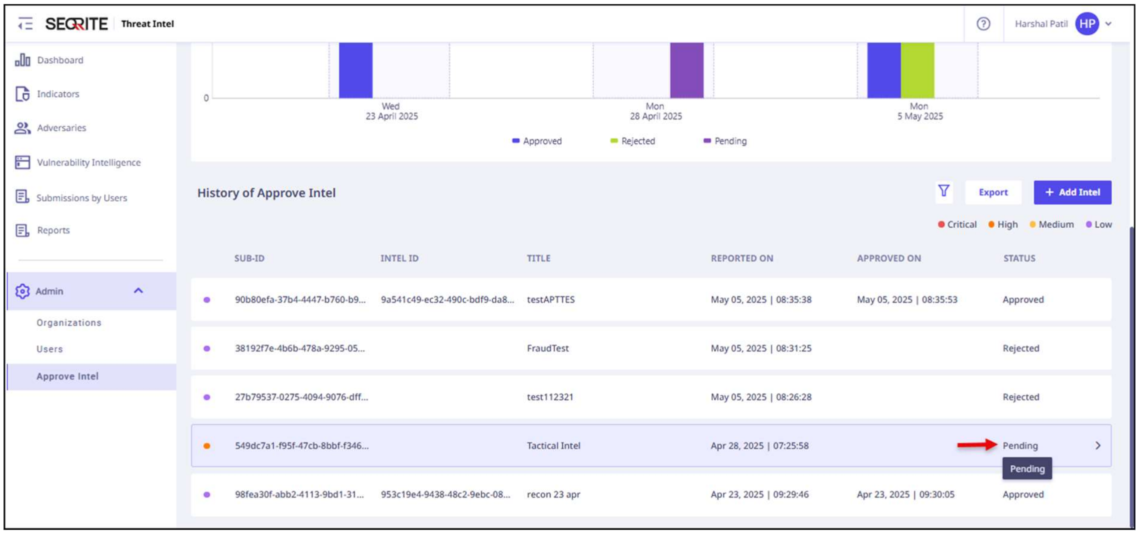
The system displays filtered data.

Approve/Reject Submitted Intel

You can review and evaluate the submitted intel for accuracy and relevance. Based on your assessment, you can either approve the intel to publish or reject if it does not meet the required standards.

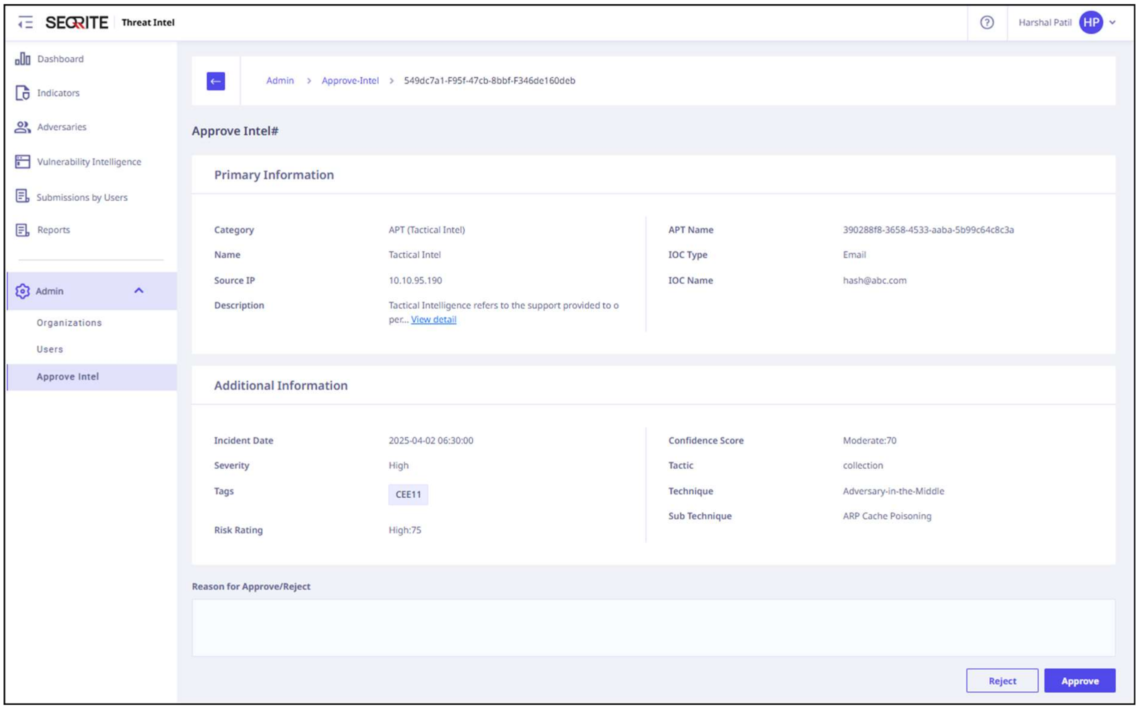
To approve/reject intel submissions, follow these steps:

1. On the Seqrite Threat Intelligence portal, click **Admin** and select **Approve Intel** in the left pane.
2. On the **Approve Intel** page, click the intel you want to approve. The intel submission details page displays the following details:



History of Approve Intel

	SUB-ID	INTEL ID	TITLE	REPORTED ON	APPROVED ON	STATUS
●	90b80efa-37b4-4447-b760-b9...	9a541c49-ec32-490c-bdf9-da8...	testAPTTES	May 05, 2025 | 08:35:38	May 05, 2025 | 08:35:53	Approved
●	38192f7e-4b6b-478a-9295-05...		FraudTest	May 05, 2025 | 08:31:25		Rejected
●	27b79537-0275-4094-9076-dff...		test112321	May 05, 2025 | 08:26:28		Rejected
●	549dc7a1-f95f-47cb-8bbf-f346...		Tactical Intel	Apr 28, 2025 | 07:25:58		Pending
●	98fea30f-abb2-4113-9bd1-31...	953c19e4-9438-48c2-9ebc-08...	recon 23 apr	Apr 23, 2025 | 09:29:46	Apr 23, 2025 | 09:30:05	Approved



Approve Intel#

Primary Information

Category	APT (Tactical Intel)	APT Name	390288f8-3658-4533-aaba-5b99c64c8c3a
Name	Tactical Intel	IOC Type	Email
Source IP	10.10.95.190	IOC Name	hash@abc.com
Description	Tactical Intelligence refers to the support provided to o per... View detail		

Additional Information

Incident Date	2025-04-02 06:30:00	Confidence Score	Moderate:70
Severity	High	Tactic	collection
Tags	CEE11	Technique	Adversary-in-the-Middle
		Sub Technique	ARP Cache Poisoning
Risk Rating	High:75		

Reason for Approve/Reject

3. Click **Approve** to approve the intel else click **Reject**.

Support

For any issues or queries:

- Contact Seqrite Support at support@seqrite.com.
- Refer to the FAQs in the Seqrite Threat Intelligence.