# ThreatConnect® Release Notes

Software Version 7.8

January 15, 2025

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

# Table of Contents

**New Features and Functionality** **5**
Actionable Search 5
AbuseIPDB Enrichment 7
Hyperlink Support in Reports 10
Threat Graph Enhancements 12
New Layout Options 12
Disable Auto Layout 13
TQL Generator (Beta) 14
New Details Screen: Copy Tab 15
Intel 360: Intelligence Reviews 16
**Improvements** **17**
Threat Intelligence 17
Enrichment 17
Search 18
Threat Graph 18
MITRE ATT&CK 18
System Settings 18
Reports 19
API & Under the Hood 19
**Bug Fixes** **20**
Browse 20
Details Drawer 20
System and Organization Settings 20
Playbooks 20
API & Under the Hood 20
**Dependencies & Library Changes** **21**
**Maintenance Releases Changelog** **22**
2025-04-18 7.8.2-M0418R [Latest] 22
Bug Fixes 22
2025-03-24 7.8.2-M0324R 22
Bug Fixes 22
2025-03-19 7.8.2-M0319R 22
Bug Fixes 22

2025-03-14 7.8.2-M0314R 22

Bug Fixes 22

2025-03-05 7.8.2 23

Improvements 23

Bug Fixes 23

2025-02-05 7.8.1 24

Improvements 24

Bug Fixes 25

**CAL Updates 27**

2025-01-06 CAL 3.10 [Latest] 27

NEW! CAL ATL AI Feedback! 27

Updated Feature: Hourly CAL ATL Updates! 27

Updated Feature: MITRE ATT&CK 16.0 28

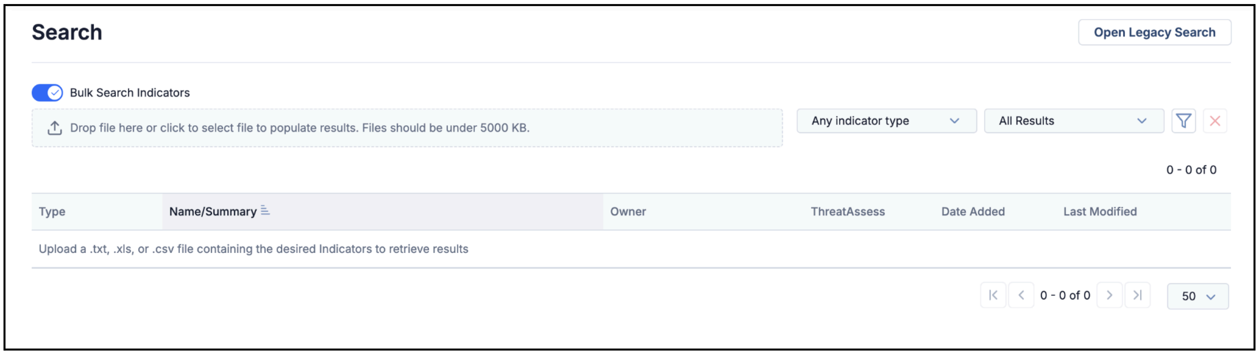
Other Updates 28

# New Features and Functionality

## Actionable Search

ThreatConnect 7.8 takes your ability to search and analyze Indicator data to the next level with the introduction of **Actionable Search**. This powerful new feature parses and displays up to 1,024 Indicators from an uploaded file. From there, you can filter the Indicators for further investigation, add Indicators to your Organization, and view context on Indicators in your ThreatConnect owners, enabling you to efficiently process and analyze large volumes of IOC data directly in ThreatConnect.

To access Actionable Search, turn on the new **Bulk Search Indicators** toggle on the **Search** screen.



Search

Bulk Search Indicators

Drop file here or click to select file to populate results. Files should be under 5000 KB.

0 - 0 of 0

| Type | Name/Summary | Owner | ThreatAssess | Date Added | Last Modified |
|---|---|---|---|---|---|
| Upload a .txt, .xls, or .csv file containing the desired Indicators to retrieve results | | | | | |

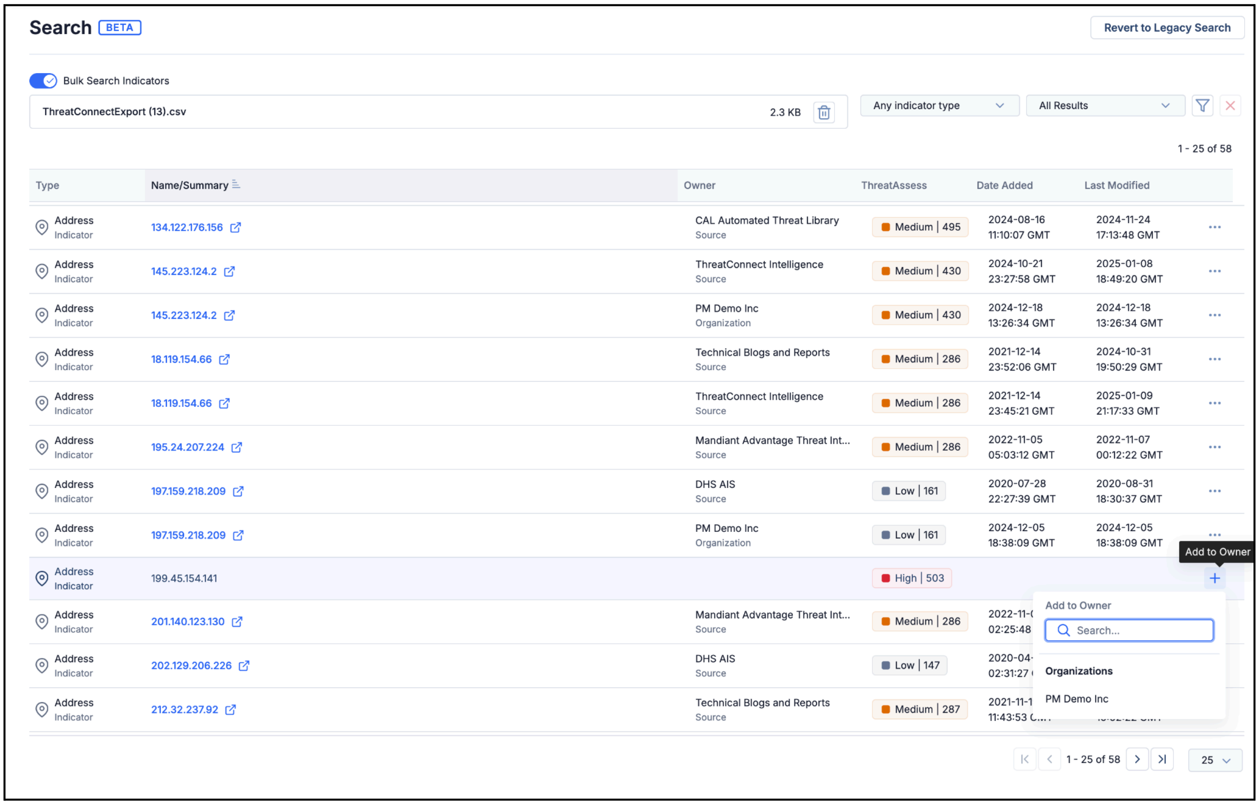
0 - 0 of 0

*Turn on the **Bulk Search Indicators** toggle to access Actionable Search*

Then upload a **.txt**, **.csv**, or **.xls** file containing IOCs in the area under the toggle, and ThreatConnect will automatically parse the Indicators, search for them across the platform, and display the results:

- **Known Indicators**: Known Indicators are Indicators that exist in at least one of your ThreatConnect owners. For these Indicators, Actionable Search will provide key insights, including the owner, the ThreatAssess score, the date the Indicator was first added to ThreatConnect, and the date the Indicator was last modified in ThreatConnect. You can use the options in the ⋯ menu to view the Indicator in Threat Graph, view the Indicator's **Details** screen, or delete the Indicator from its owner in ThreatConnect.
- **Unknown Indicators**: Unknown Indicators are Indicators that do not exist in any of your ThreatConnect owners. For unknown Indicators that CAL™ has information on,

Actionable Search will display a ThreatAssess score to help you evaluate potential risks. To add an unknown Indicator to your Organization, click **+**.



| Type | Name/Summary | Owner | ThreatAssess | Date Added | Last Modified |
|---|---|---|---|---|---|
| Address<br>Indicator | 134.122.176.156 | CAL Automated Threat Library<br>Source | Medium \| 495 | 2024-08-16<br>11:10:07 GMT | 2024-11-24<br>17:13:48 GMT |
| Address<br>Indicator | 145.223.124.2 | ThreatConnect Intelligence<br>Source | Medium \| 430 | 2024-10-21<br>23:27:58 GMT | 2025-01-08<br>18:49:20 GMT |
| Address<br>Indicator | 145.223.124.2 | PM Demo Inc<br>Organization | Medium \| 430 | 2024-12-18<br>13:26:34 GMT | 2024-12-18<br>13:26:34 GMT |
| Address<br>Indicator | 18.119.154.66 | Technical Blogs and Reports<br>Source | Medium \| 286 | 2021-12-14<br>23:52:06 GMT | 2024-10-31<br>19:50:29 GMT |
| Address<br>Indicator | 18.119.154.66 | ThreatConnect Intelligence<br>Source | Medium \| 286 | 2021-12-14<br>23:45:21 GMT | 2025-01-09<br>21:17:33 GMT |
| Address<br>Indicator | 195.24.207.224 | Mandiant Advantage Threat Int...<br>Source | Medium \| 286 | 2022-11-05<br>05:03:12 GMT | 2022-11-07<br>00:12:22 GMT |
| Address<br>Indicator | 197.159.218.209 | DHS AIS<br>Source | Low \| 161 | 2020-07-28<br>22:27:39 GMT | 2020-08-31<br>18:30:37 GMT |
| Address<br>Indicator | 197.159.218.209 | PM Demo Inc<br>Organization | Low \| 161 | 2024-12-05<br>18:38:09 GMT | 2024-12-05<br>18:38:09 GMT |
| Address<br>Indicator | 199.45.154.141 | | High \| 503 | | |
| Address<br>Indicator | 201.140.123.130 | Mandiant Advantage Threat Int...<br>Source | Medium \| 286 | 2022-11-(<br>02:25:48 | |
| Address<br>Indicator | 202.129.206.226 | DHS AIS<br>Source | Low \| 147 | 2020-04-<br>02:31:27 | |
| Address<br>Indicator | 212.32.237.92 | Technical Blogs and Reports<br>Source | Medium \| 287 | 2021-11-1<br>11:43:53 | |

*View parsed Indicators and add unknown Indicators to your Organization*

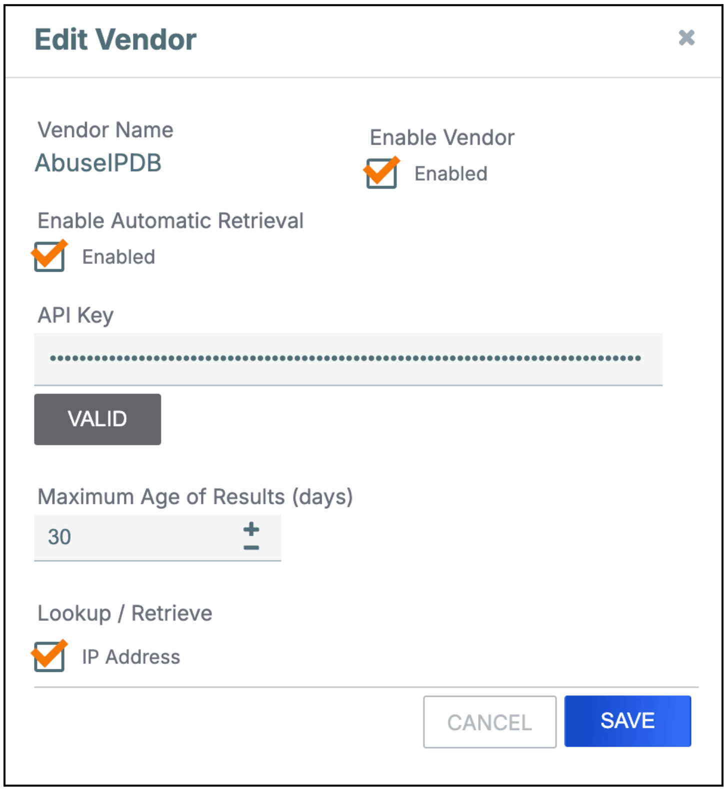
You can use the filters provided in Actionable Search to refine your search results, enabling you to triage and process the Indicators efficiently:

- **Filter by Indicator type**: Filter the results set to IP Addresses, domains, file hashes, or other Indicator types.
- **Filter by known or unknown Indicators**: Easily distinguish between Indicators ThreatConnect knows about and those it does not.
- **Filter by owner, date added, "last modified" date, or ThreatAssess score**: Use the **Filters** ▽ menu to further narrow your results. For example, you can select predefined ThreatAssess score ranges to focus on Indicators classified as Low, Medium, High, or Critical risk levels, or set a custom ThreatAssess score range for more specific filtering.

# AbuseIPDB Enrichment

We are excited to introduce yet another powerful built-in enrichment feature in our 7.8 release, this time powered by AbuseIPDB. This easy-to-use integration allows you to check the real-time enrichment of IP addresses with the Confidence of Abuse percentage provided by AbuseIPDB. You can use this information to determine the risk level of IP addresses interacting with your network or systems to prevent future attacks.

System Administrators can enable this built-in enrichment by editing the options for AbuseIPDB in **System Settings** > **Indicators** > **Enrichment Tools**, adding and validating their AbuseIPDB API key, and selecting the **IP Address** Indicator type. The **Maximum Age of Results (days)** parameter in the configuration represents the recency period you'd like to define for threat intelligence data. IP addresses that were malicious in the past may have been remediated or reassigned. By limiting results based on age, this setting helps avoid false positives and ensures the data remain relevant and actionable.



Edit Vendor

Vendor Name: AbuseIPDB

Enable Vendor: ☑ Enabled

Enable Automatic Retrieval: ☑ Enabled

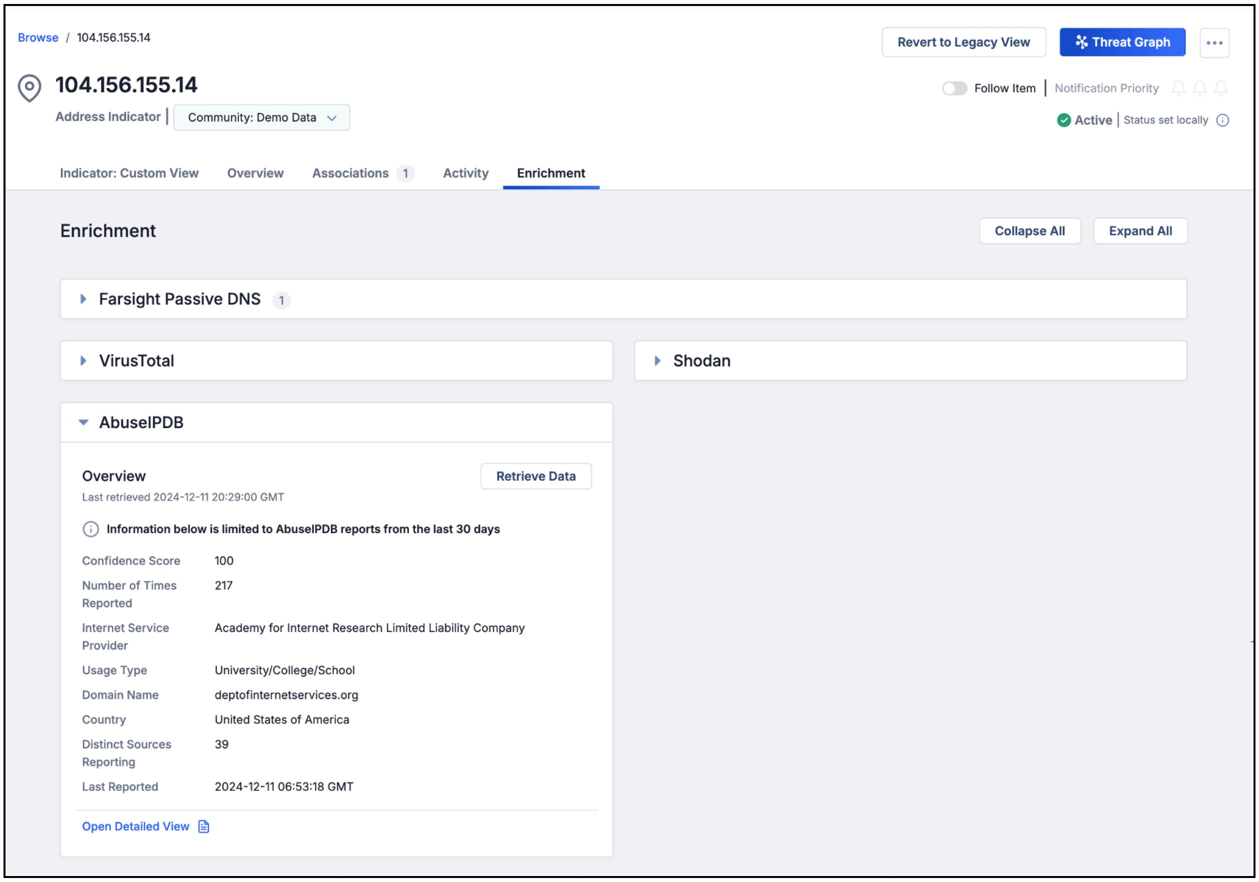
API Key: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

Maximum Age of Results (days): 30

Lookup / Retrieve: ☑ IP Address

*Configure the AbuseIPDB enrichment in* ***System Settings***

Once the configuration for this enrichment has been completed, you can view enrichment details for Address Indicators on the **Enrichment** tab of the Indicator's **Details** screen.



Enrichment

AbuseIPDB

Overview

Last retrieved 2024-12-11 20:29:00 GMT

Information below is limited to AbuseIPDB reports from the last 30 days

|  |  |
|---|---|
| Confidence Score | 100 |
| Number of Times Reported | 217 |
| Internet Service Provider | Academy for Internet Research Limited Liability Company |
| Usage Type | University/College/School |
| Domain Name | deptofinternetservices.org |
| Country | United States of America |
| Distinct Sources Reporting | 39 |
| Last Reported | 2024-12-11 06:53:18 GMT |

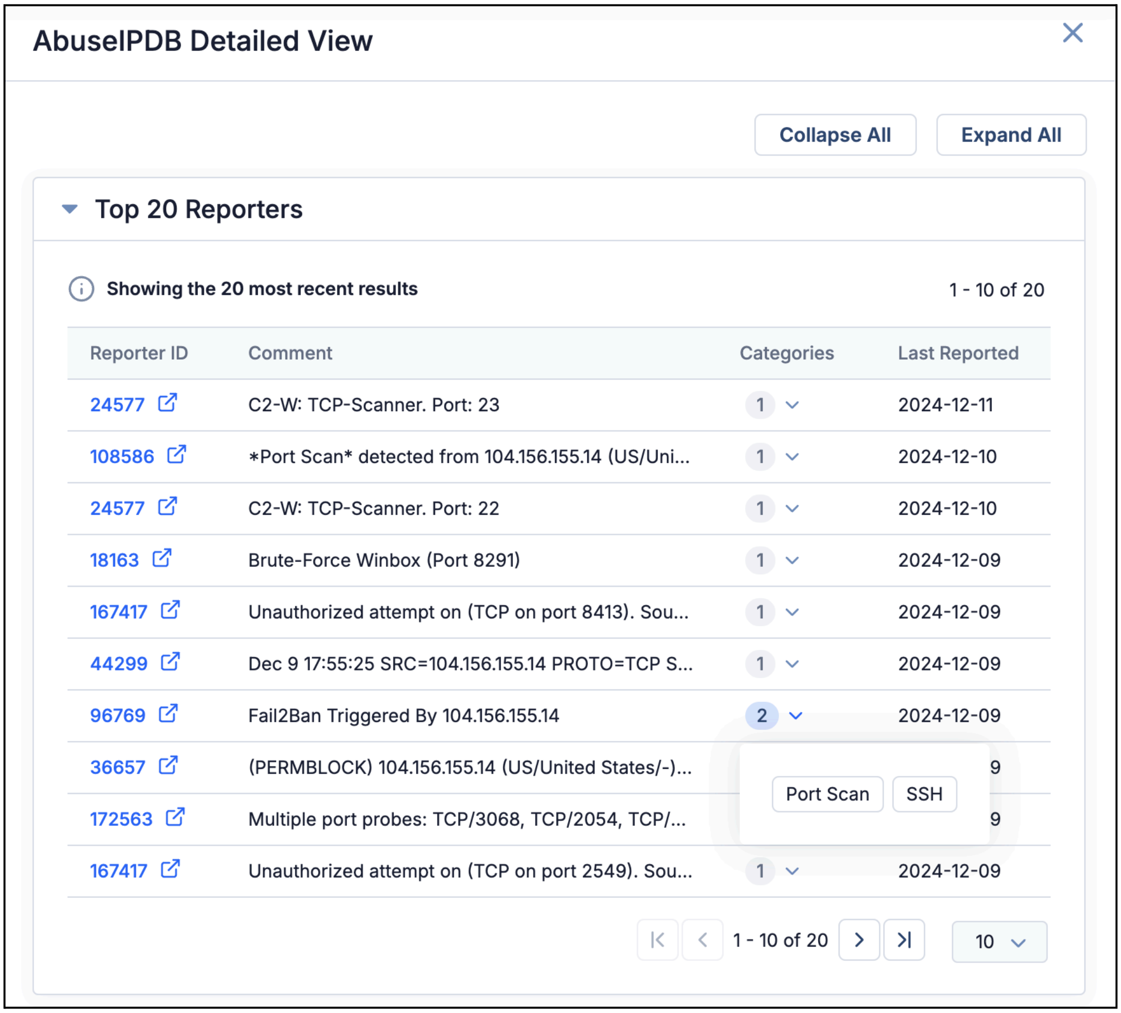
*View AbuseIPDB data on the **Enrichment** tab of an Address Indicator's **Details** screen*

When you navigate to an Address Indicator's **Enrichment** tab for the first time after the AbuseIPDB enrichment has been activated, information from AbuseIPDB is pulled and cached. Every time you revisit the **Enrichment** tab for the Indicator, cached data will be displayed until a new AbuseIPDB lookup is made after the caching time limit expires. To get the latest enrichment data from AbuseIPDB before the caching time limit expires, you can always click the **Retrieve Data** button on the **AbuseIPDB** card.

To delve further into the information about an IP address' reporters in AbuseIPDB, click **Open Detailed View** at the lower left of the **AbuseIPDB** card. This will open the **AbuseIPDB Detailed View** drawer, which displays the following information for the 20 most recent reports submitted by different users (or automated systems) about potentially malicious activity for the IP address:

- **Reporter ID**: A unique identifier assigned to the individual or system that submitted the report about suspicious activity. These IDs are clickable links that direct you to the reporter's AbuseIPDB profile page, which lists all of the IP addresses they have reported and provides their credibility standing rating in AbuseIPDB. Note that reporters with private AbuseIPDB profiles will have no further information displayed on their profile page in Abuse IPDB.

- **Comment**: The malicious activity associated with the reported IP address as described by the reporter.
- **Categories**: The number of malicious activity types reported for the IP address. Expand the entry in this column to view the specific types.
- **Last Reported**: The date when the report was submitted.



AbuseIPDB Detailed View

Top 20 Reporters

Showing the 20 most recent results

1 - 10 of 20

| Reporter ID | Comment | Categories | Last Reported |
|---|---|---|---|
| 24577 | C2-W: TCP-Scanner. Port: 23 | 1 | 2024-12-11 |
| 108586 | *Port Scan* detected from 104.156.155.14 (US/Uni... | 1 | 2024-12-10 |
| 24577 | C2-W: TCP-Scanner. Port: 22 | 1 | 2024-12-10 |
| 18163 | Brute-Force Winbox (Port 8291) | 1 | 2024-12-09 |
| 167417 | Unauthorized attempt on (TCP on port 8413). Sou... | 1 | 2024-12-09 |
| 44299 | Dec 9 17:55:25 SRC=104.156.155.14 PROTO=TCP S... | 1 | 2024-12-09 |
| 96769 | Fail2Ban Triggered By 104.156.155.14 | 2<br>Port Scan<br>SSH | 2024-12-09 |
| 36657 | (PERMBLOCK) 104.156.155.14 (US/United States/-)... | | 9 |
| 172563 | Multiple port probes: TCP/3068, TCP/2054, TCP/... | | 9 |
| 167417 | Unauthorized attempt on (TCP on port 2549). Sou... | 1 | 2024-12-09 |

*View the top 20 reports from AbuseIPDB for an IP address*

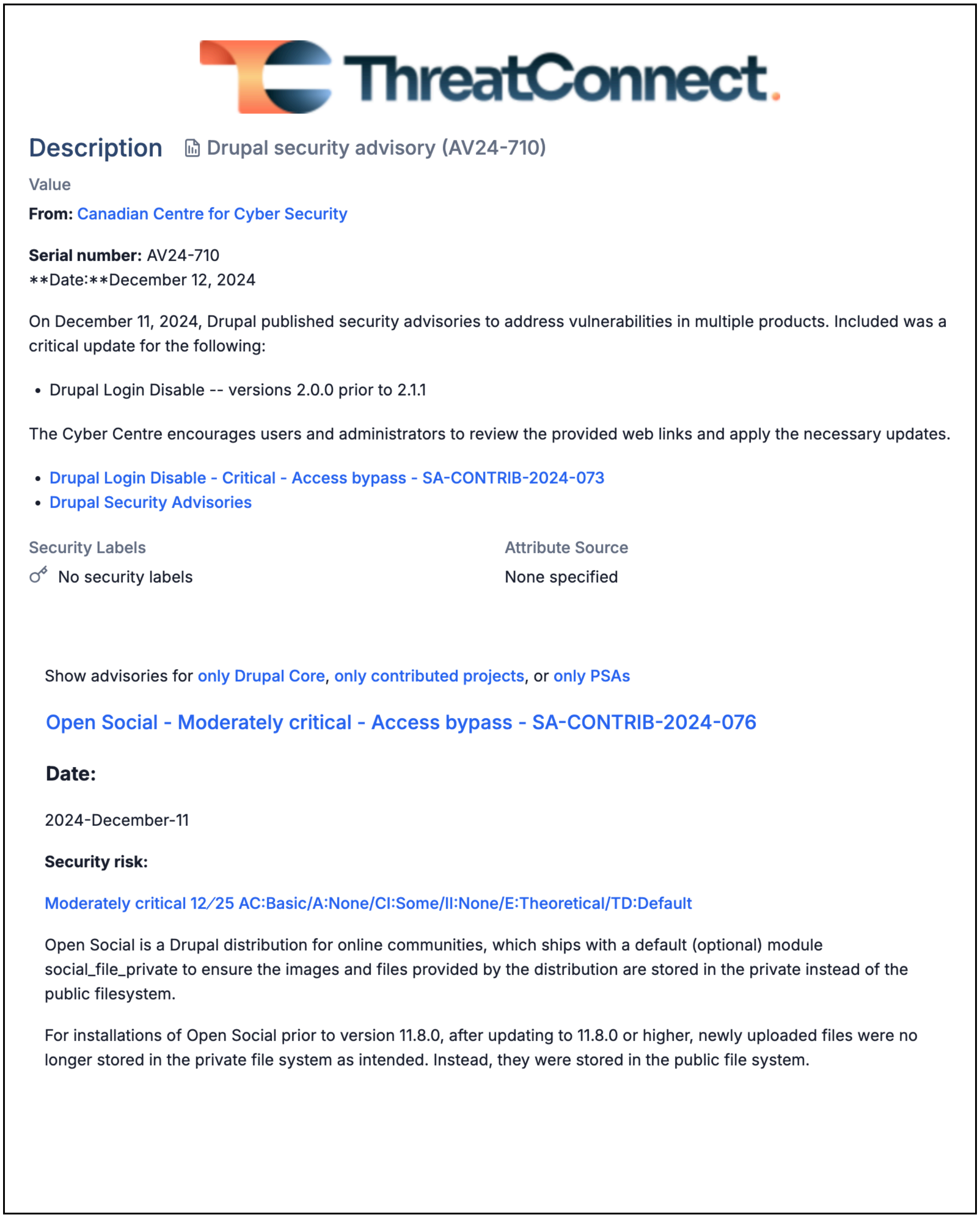
# Hyperlink Support in Reports

ThreatConnect 7.8 makes it quicker and easier for the readers of your reports to access shared data by allowing you to include hyperlinks in some of the reports' sections. This feature, which must be enabled by a System Administrator, supports hyperlinks in the following report sections:

- **Text Block**
- **Attributes** (including Group Description)
- Case Description (in the **Details** section for Cases)
- Case **Notes**

This feature is turned off by default. If it is not turned on, hyperlinks in reports will continue to be sanitized. To turn the feature on, System Administrators should select the **allowReportingHyperlinks** checkbox in **System Settings > Settings**.

Once the feature is turned on, hyperlinks in the supported sections will be clickable in previewed and published reports, allowing for seamless navigation to the linked resources. When you click on a hyperlink in the report editor or when previewing a report, a message will be displayed advising you to ensure the link is safe before proceeding.



ThreatConnect.

## Description

Drupal security advisory (AV24-710)

Value

**From:** Canadian Centre for Cyber Security

**Serial number:** AV24-710
**Date:**December 12, 2024

On December 11, 2024, Drupal published security advisories to address vulnerabilities in multiple products. Included was a critical update for the following:

- Drupal Login Disable -- versions 2.0.0 prior to 2.1.1

The Cyber Centre encourages users and administrators to review the provided web links and apply the necessary updates.

- Drupal Login Disable - Critical - Access bypass - SA-CONTRIB-2024-073
- Drupal Security Advisories

| Security Labels | Attribute Source |
|---|---|
| No security labels | None specified |

Show advisories for only Drupal Core, only contributed projects, or only PSAs

### Open Social - Moderately critical - Access bypass - SA-CONTRIB-2024-076

**Date:**

2024-December-11

**Security risk:**

Moderately critical 12∕25 AC:Basic/A:None/CI:Some/II:None/E:Theoretical/TD:Default

Open Social is a Drupal distribution for online communities, which ships with a default (optional) module social_file_private to ensure the images and files provided by the distribution are stored in the private instead of the public filesystem.

For installations of Open Social prior to version 11.8.0, after updating to 11.8.0 or higher, newly uploaded files were no longer stored in the private file system as intended. Instead, they were stored in the public file system.

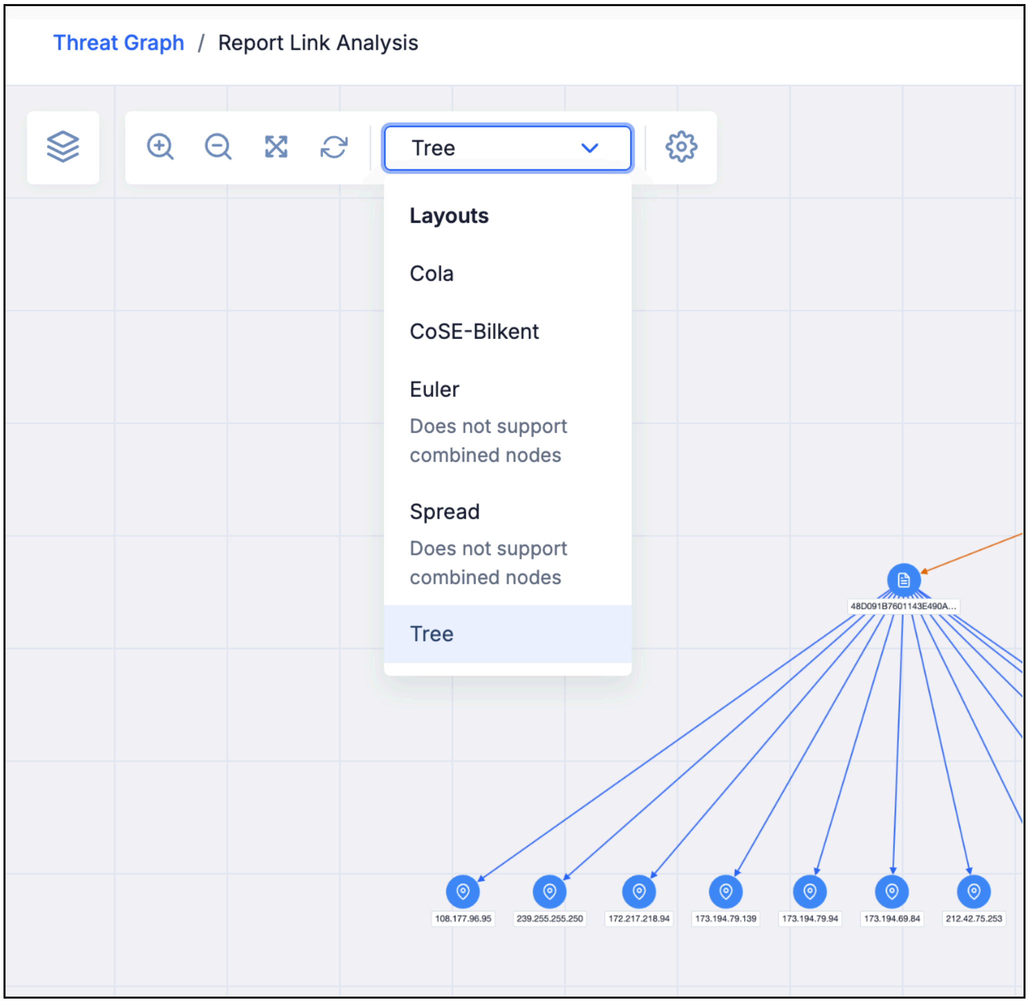
*Clickable hyperlinks make it easier for report readers to view shared data*

This feature enhances the report creation process, making it easier to share and access related resources while maintaining security controls.

# Threat Graph Enhancements

## New Layout Options

In ThreatConnect 7.8, you can now choose from a set of five layouts when organizing data in Threat Graph. These layouts include a few options that support combined nodes, such as those for Groups with similar alias information in CAL, and are accessible via a new menu at the top left of Threat Graph.



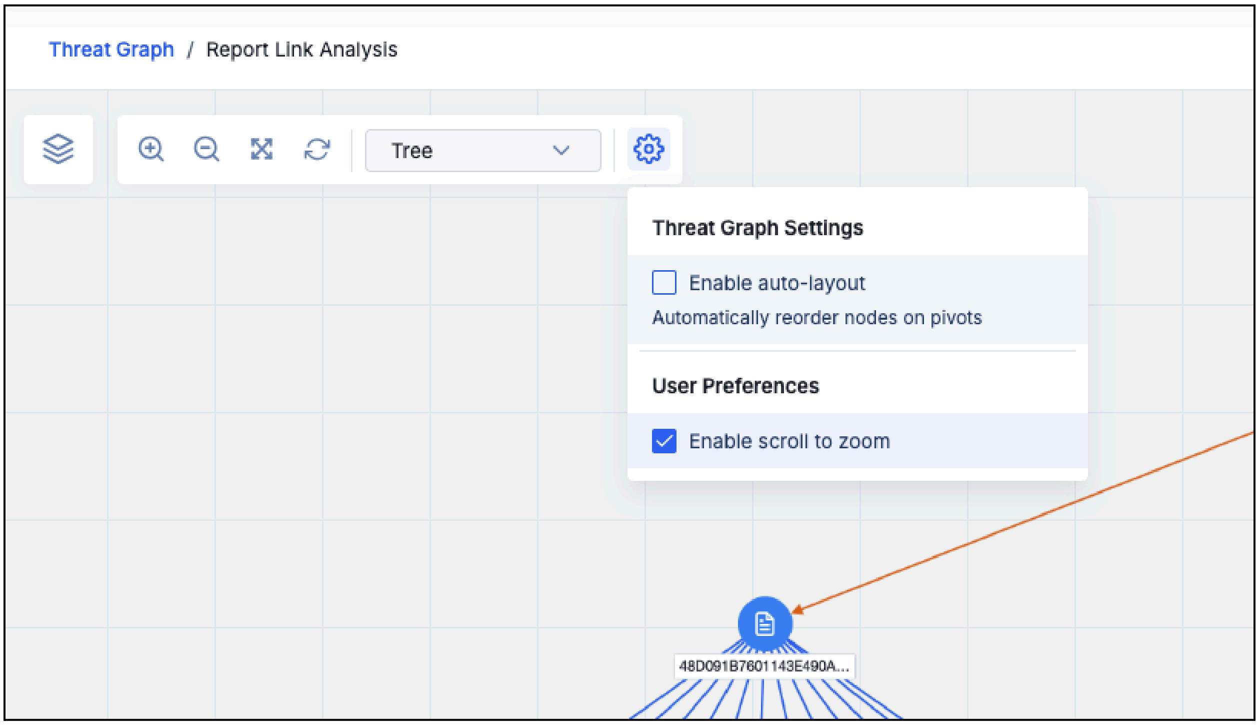
*You can choose from five Threat Graph layout options*

With these layout options, you can quickly visualize your data in different ways, which may help you notice relationships and trends that were unclear or previously overlooked or prompt you to adjust your analytical conclusions. Some of the new options may also be better suited for communication than the original, default layout (CoSE-Bilkent). For example, the Tree layout orients data in a hierarchical formation, which can be helpful for clearly communicating the relationships between Threat Actor groups like Intrusion Sets and other data such as Malware or Indicators.

As we consider adding support for even more layout options in the future, please feel free to reach out to your Customer Success Manager with ideas for Threat Graph layouts that would help you more effectively visualize your data!

## Disable Auto Layout

In addition to the new layout options, you can now disable the setting that causes a Threat Graph to automatically re-organize when you pivot on a node. The inability to disable the autolayout setting was a significant friction point for many analysts who use the Threat Graph feature extensively in their day-to-day work, so we hope that this addition to ThreatConnect 7.8 makes your work in Threat Graph easier and more convenient.



Threat Graph Settings

□ Enable auto-layout

Automatically reorder nodes on pivots

User Preferences

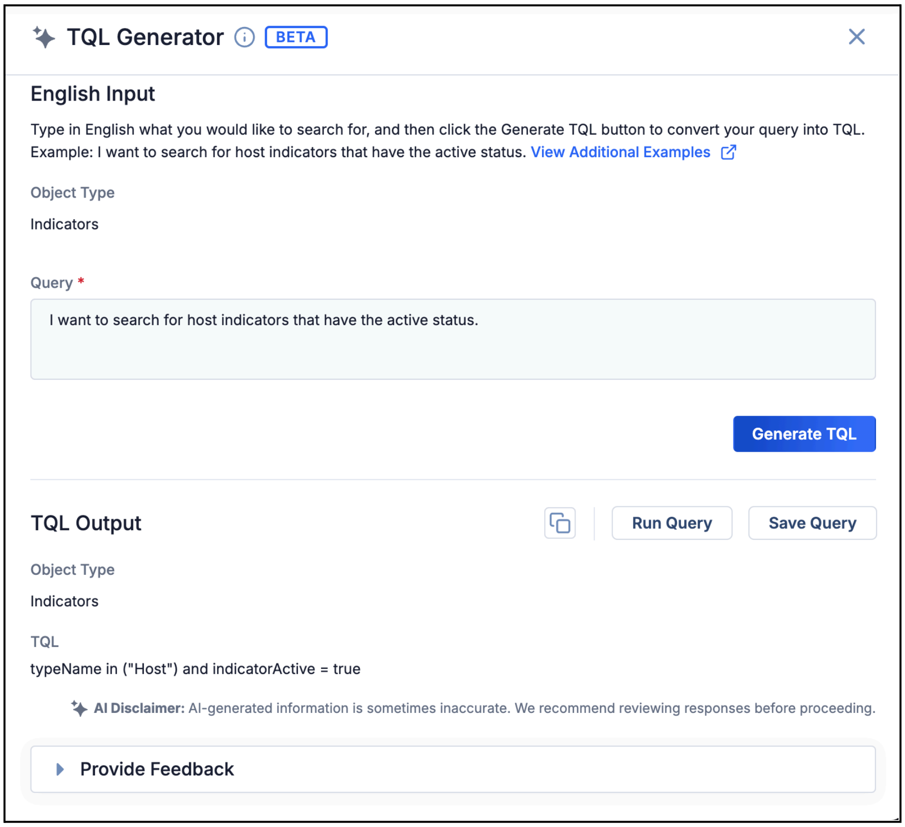
☑ Enable scroll to zoom

*Clear the **Enable auto-layout** checkbox to prevent Threat Graph from reorganizing the nodes after pivoting*

When this setting is turned off, any new objects added to a Threat Graph via pivots will be added to the left side of the graph. You can choose one of the new layout options to organize the data, or you can move the nodes around manually.

# TQL Generator (Beta)

As part of this release, we introduce the beta version of the TQL Generator, an AI-powered utility available on the **Browse** screen that translates plain-English prompts into ThreatConnect Query Language (TQL), enabling you craft useful TQL queries without requiring an extensive understanding of TQL.



English Input

Type in English what you would like to search for, and then click the Generate TQL button to convert your query into TQL. Example: I want to search for host indicators that have the active status. View Additional Examples

Object Type

Indicators

Query *

I want to search for host indicators that have the active status.

TQL Output

Object Type

Indicators

TQL

typeName in ("Host") and indicatorActive = true

**AI Disclaimer:** AI-generated information is sometimes inaccurate. We recommend reviewing responses before proceeding.

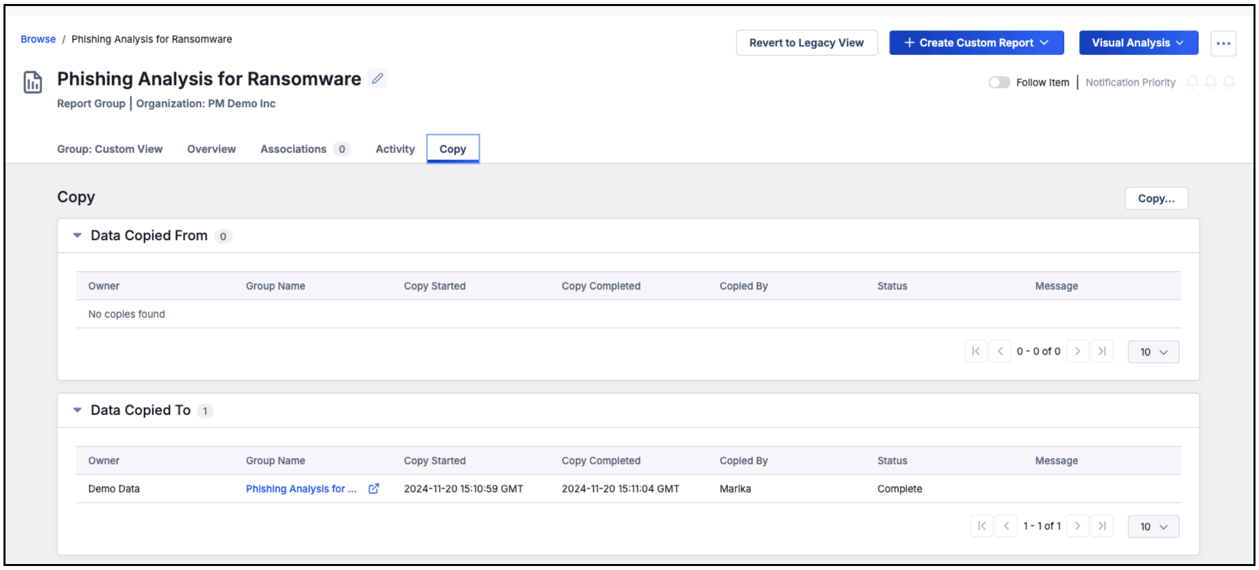
*The TQL Generator utility is available on the **Browse** screen*

Integrated directly into ThreatConnect, this AI helper intuitively understands the ThreatConnect data model and user interface, empowering you to quickly access targeted data sets. It also collects customer feedback to inform future improvements. This innovation aims to streamline your workflows and enhance the effectiveness of security operations by simplifying data retrieval.

As previously mentioned, this feature is in beta as of ThreatConnect 7.8. On instances running version 7.8.0, it is disabled by default and requires an explicit opt-in. Please reach out to your Customer Success representatives if you are interested in having it turned on for your instance. On instances running version 7.8.1 or later, a System Administrator can turn it on by navigating to **System Settings** > **Settings**, selecting **Feature Flags** on the left sidebar, and selecting the **aiTqlGenerationEnabled** checkbox in the **Beta** section at the bottom of the screen.

## New Details Screen: Copy Tab

In 7.8, we bring the ability to copy and share Group data, previously available only on the legacy **Details** screen, to the new **Details** screen. You can now copy Group data to and from different owners (Sources, Communities, and Organizations) without reverting to the legacy view.



Phishing Analysis for Ransomware

Report Group | Organization: PM Demo Inc

Copy

Data Copied From 0

| Owner | Group Name | Copy Started | Copy Completed | Copied By | Status | Message |
|---|---|---|---|---|---|---|
| No copies found | | | | | | |

0 - 0 of 0 | 10

Data Copied To 1

| Owner | Group Name | Copy Started | Copy Completed | Copied By | Status | Message |
|---|---|---|---|---|---|---|
| Demo Data | Phishing Analysis for ... | 2024-11-20 15:10:59 GMT | 2024-11-20 15:11:04 GMT | Marika | Complete | |

1 - 1 of 1 | 10

*The new **Copy** tab provides the same functionality as the legacy **Sharing** tab*

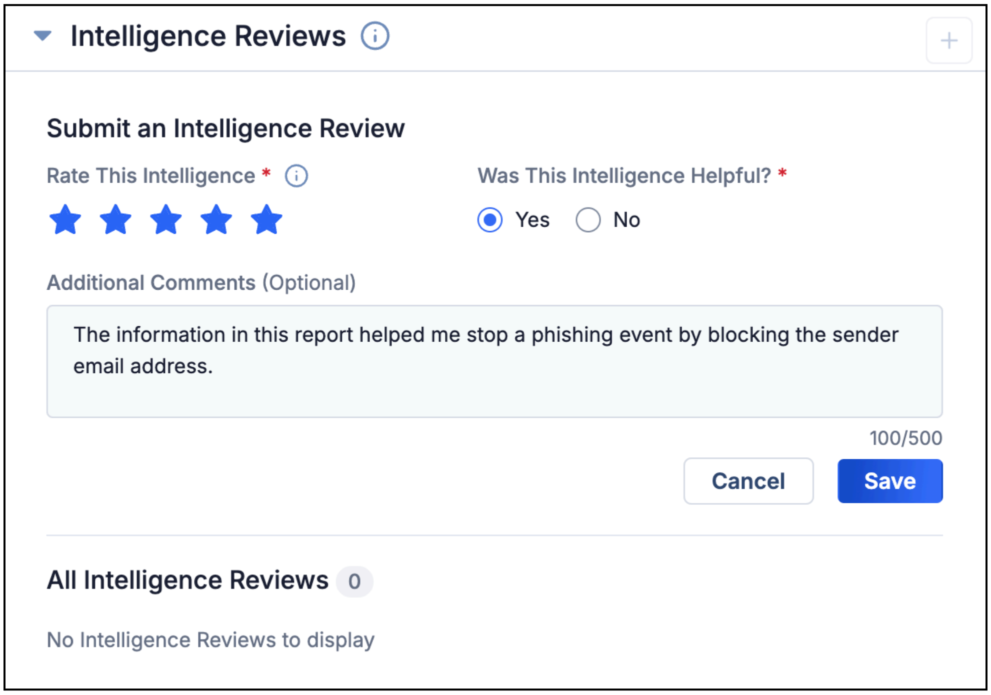
Additionally, in an effort to reduce complexity and confusion, we reduced the number of words used to refer to the act of copying data from one owner to another. Previously, this functionality was referred to as "copy," "share," and "contribute"in different areas of the platform, which was confusing. Starting in ThreatConnect 7.8, the word "copy" will take the place of all of these terms.

It is important to note that this release does not make the ability to publish Group data from a Community available on the new **Details** screen. The option to publish a Group in a Community, which is a necessary step when using the Cross-Intel Sharing App to share Group data across ThreatConnect instances, is available only on the legacy **Details** screen at this time, but will be added to the new **Details** screen in a future release.

# Intel 360: Intelligence Reviews

Many threat intelligence teams struggle to collect quality feedback from their stakeholders. Oftentimes they produce and send out intelligence, but hear little or nothing about whether the information was valuable, useful, or helpful. This is a significant issue because threat intelligence teams and analysts rely on the intelligence life cycle feedback loop to refine intelligence requirements and collection and production priorities. Without that information, CTI teams find it difficult to measure the effectiveness of their work. This sometimes leads upper management to view CTI as a “nice to have” rather than a “must have.”

In an effort to help our users tackle these challenges, we are releasing Intelligence Reviews. This feature is the first in our Intel 360 strategic initiative, which is aimed at helping ThreatConnect users measure the effectiveness of the intelligence they produce and make adjustments to make sure they are using available resources in the most effective way.



Intelligence Reviews

Submit an Intelligence Review

Rate This Intelligence * ★★★★★

Was This Intelligence Helpful? * ● Yes ○ No

Additional Comments (Optional)

The information in this report helped me stop a phishing event by blocking the sender email address.

100/500

All Intelligence Reviews 0

No Intelligence Reviews to display

*You can use Intelligence Reviews to add feedback to Reports*

With Intelligence Reviews, stakeholders can add feedback to Report Group objects on their **Details** screen. All user types can add feedback, including Read Only users, but each user can only add one review per object. In a future release, we plan to build upon this feature by adding the ability to visualize feedback in dashboards. We are also assessing how we might integrate AI to use the feedback to identify common themes and potential next steps for CTI teams.

# Improvements

## Threat Intelligence

- The **Attributes** card on the new **Details** screen and **Details** drawer now has the ability to be viewed in table and card format. Table format is the default view, and both formats support pagination, filtering, and keyword search for Attribute value. Table view displays two tables: **Unfilled Default Attributes** (displayed at the top of the card to remind you to provide values for these Attributes) and **All Filled Attributes**. You can customize the columns displayed in the **All Filled Attributes** table.
- The following new fields are now displayed on the **Details** card for Groups and Indicators if the fields have a value: **First Seen**, **Last Seen**, **External Date Added**, **External Date Expires**, and **External Last Modified**.
- Object subtype filters were added to the **Results** table on an IR's **Details** screen, allowing you to filter by Group and Indicator subtype.
- When on the **Associations** tab of an object's **Details** screen, or when viewing one of the associations cards on the **Custom View** tab, you can now click on an association's row to view the associated object's **Details** drawer.
- You can now copy the contents of the **AI-Generated Summary** for a CAL ATL Report to your clipboard by clicking ⧉ at the upper right of the **AI insights** card on the Report's **Details** screen.
- When viewing an object's legacy **Details** screen, the owner is now displayed at the upper-left corner of the screen instead of the upper right.
- With the addition of Intelligence Reviews, the Group Intel Rating feature was removed from ThreatConnect. The thumbs-up and thumbs-down icons are no longer displayed on the Group **Details** screen, and the `upVote` and `downVote` request body fields are no longer available in the v3 API.
- The Tracks functionality has been deprecated.

## Enrichment

- The **URLScan** card on the **Enrichment** tab of a URL Indicator's **Details** screen now provides a **View Results on URLScan.io** link, providing you with quick and direct access to comprehensive urlscan.io data.

## Search

- The new **Search** screen introduced in ThreatConnect 7.6 is no longer in beta and is the default screen when you click 🔍 on the right of the top navigation bar. You can still access the legacy search feature by clicking **Open Legacy Search** at the top right of the **Search** screen.
- When viewing search results, you can now click on a result's **Name/Summary** to view its **Details** screen.

## Threat Graph

- To give you a consistent in-platform experience and simplify terminology usage, we have changed all "Explore In Graph" and "Graph" references to "Threat Graph."
- You can now remove nodes from a Threat Graph directly from the node menu.
- A **View Only This** option has been added to the Threat Graph legend, enabling you to filter a Threat Graph view to a single object type.
- The Threat Graph legend now shows only object types that are currently being displayed in the Threat Graph rather than all object types. This creates a cleaner, less cluttered legend display.

## MITRE ATT&CK

- The **Details** screen for ATT&CK® Tags now displays **Associated Tactics** and **Platform(s)** fields on the **Details** card. The v3 API provides read access to these fields through the new `tactics` and `platform` fields, respectively, included in response bodies.
- The T-codes for ATT&CK Tags are now consistently displayed, including in reports and dashboards.

## System Settings

- The following new system settings were added:
  - **allowReportingHyperlinks**: If turned on, this setting will allow active hyperlinks in the **Text Block**, **Attributes** (including Group Description), Case Description (in the **Details** section for Cases), and Case **Notes** sections of reports. It is turned off by default.

    - **systemExclusionListApiAccess**: This setting is a comma-separated list of API user IDs that are allowed to use the v3 API to edit the systemwide Indicator Exclusion List for their ThreatConnect instance.
    - **v3ApiReadOnlyReports**: If turned on, this setting allows API users with read-only permissions to use the v3 API to make updates to false positives and observations.

## Reports

- When viewing or publishing a report, you are now given the option to remove all empty sections at one time.

## API & Under the Hood

- You can now use the `techniqueID` field in the v3 API to apply MITRE ATT&CK® T-codes as ATT&CK Tags in ThreatConnect.
- A new `/v3/security/exclusionLists` endpoint that API users with the requisite permissions can use to create, retrieve, update, and delete custom Indicator Exclusion Lists at the System and owner levels was added to the v3 API.
- Support for reporting false positives and observations for Indicators was added to the `/v3/indicators` endpoint.

# Bug Fixes

## Browse

- An issue causing some of the filters for Indicators on the **Browse** screen to scroll off the display and become inaccessible when viewed on small monitors was fixed.

## Details Drawer

- An issue preventing the **Details** drawer for a Workflow Case from being closed with the Escape key when being viewed from the **Search** screen or the **Details** screen for an Intelligence Requirement has been corrected.

## System and Organization Settings

- The following improvements were made to address issues that were occurring when editing System- and Organization-level variables:
  - You cannot change the type of an existing variable.
  - The value of keychain and file variables will not be displayed when editing a variable.

## Playbooks

- An issue preventing a certain Playbook from being imported was resolved.

## API & Under the Hood

- An issue causing incorrect Tags to be applied to data when using the v3 API to apply the Tags was fixed.
- An issue preventing deletion of certain Organizations was resolved.
- The cache size limitation for Organizations has been removed.

# Dependencies & Library Changes

- There are no new dependencies or library changes for ThreatConnect version 7.8.0.

# Maintenance Releases Changelog

## 2025-04-18 7.8.2-M0418R [Latest]

### Bug Fixes

- An issue preventing deletion of certain DataStores was fixed.

## 2025-03-24 7.8.2-M0324R

### Bug Fixes

- An issue causing Playbooks with a Case Trigger to execute twice for Cases with a Resolution value of **New** has been fixed.

## 2025-03-19 7.8.2-M0319R

### Bug Fixes

- An issue causing an Indicator's observations count to increment each time a PUT request was made to its endpoints in the v3 API was fixed.

## 2025-03-14 7.8.2-M0314R

### Bug Fixes

- When importing Indicators via the V2 Batch API, the "last modified" date for Indicators that already exist in the target owner was being overwritten with the "last modified" date of the imported Indicator. This issue has been fixed.
- Performance issues on Tag lookups were resolved.

# 2025-03-05 7.8.2

## Improvements

- You can now pivot on DNS Resolutions for Address and Host Indicators in Threat Graph. To access this option, click on an Address or Host Indicator node and select **Pivot in ThreatConnect** › **Indicators** › **DNS Resolutions** from the node's menu.
- The following custom Indicator-to-Indicator association types have been added as defaults to all ThreatConnect instances: Address to Indicators, Host to Indicators, URL to Indicators, File to Indicators, and EmailAddress to Indicators. Each association maps the primary Indicator type to all other Indicator types. System Administrators can view and edit these associations by selecting **Associations** on the sidebar of **System Settings** › **Indicators**.
- The V2 Batch API now accepts an `association` array in batch input files. The `association` array lets you define Indicator-to-Group, Group-to-Indicator, Group-to-Group, and Indicator-to-Indicator associations to create during the batch job. Associations may be made between Indicators and Groups included in the batch file, as well as those that exist in the owner in which the batch job is creating or updating data. Also, responses for `GET /v2/batch/{id}?includeAdditional=true` API requests now include counts of successful and unsuccessful associations in the specified batch job.
- Instances running on Red Hat® Enterprise Linux® (RHEL) 8 can now use Podman for containerized deployments.

## Bug Fixes

- Some Tags that matched to IR keywords were not being highlighted in the **Result Details** drawer. This issue has been corrected.
- In the **Results** table on an IR's **Details** screen, the **Date Added** and **Last Modified** columns will now populate for global results for which this information is available.
- Markdown text in Description Attributes was not wrapping properly. This issue has been fixed.
- Ordered lists in Markdown were displaying only a single digit for line items greater than 9. This issue has been resolved.
- When adding new Indicator associations to an object, the **New Indicators** view of the **Add Indicators** window was not rendering a scrollbar, preventing access to the **Additional Details** card and **Save** and **Cancel** buttons. This issue has been resolved.

- GET requests to the `/v3/security/users` endpoint in the v3 API were always returning a count of 0. This issue was fixed.
- An issue causing latency in Playbook execution and logging of errors in Environment Servers at rest was resolved.
- An issue causing duplicate IndicatorWorkflow error log statements has been resolved.
- Error logging has been removed for Whois broker requests except at the DEBUG level.

# 2025-02-05 7.8.1

## Improvements

- Hourly CAL ATL updates are now available for On-Premises ThreatConnect instances.
- **System Settings** › **Settings** has a new tab, **Feature Flags**, that displays settings for turning on and off certain systemwide features, such as CAL, cross-owner associations, and v3 API bulk delete. These settings were previously available on various other tabs of **System Settings** › **Settings**. In addition, the **Feature Flags** tab on the left sidebar has a **Beta** section that allows you to turn on and off beta features for your ThreatConnect instance. As of ThreatConnect 7.8.1, the feature covered in this section is the TQL Generator, which is turned on and off via the new **aiTqlGenerationEnabled** system setting.

> **Note**: If you update a system setting and click **SAVE** on **System Settings** › **Settings** › **Feature Flags**, but do not see the update reflected in your ThreatConnect instance's behavior, restart your ThreatConnect instance.

- **Account Settings** › **Organizations** › edit an Organization › **Organization Information** › **Permissions** and **Account Settings** › **Communities/Sources** › edit a Community or Source › **Community/Source Information** have a new, user-friendly layout.
- A new **abuseIpdbConfidenceScore** TQL parameter that lets you filter Indicators enriched with AbuseIPDB by their AbuseIPDB confidence score was added.
- The **appCatalogServer** system setting now applies to Feed API Services. When you turn on this setting, the **Allow App Distribution** option is included in the **Options** ⋮ menu for Feed API Services on the **TC Exchange™ Settings** screen.
- Updates were made to the Doc Analysis Import tool to enhance its parsing capabilities.

- Clear error messaging is now displayed when you try to perform an action on an IR result that represents an object that has since been deleted from its owner.
- RSA NetWitness® Orchestrator is now supported on ThreatConnect Dedicated Cloud instances running SingleStore®.
- Instructions for rotating the nginx container access logs were added to the installation and upgrade guides for ThreatConnect instances running a containerized solution using Docker®.

## Bug Fixes

- The RiskIQ® built-in enrichment service is no longer available, because Microsoft® has discontinued the RiskIQ Community Edition.
- An issue preventing Groups being imported via the Doc Analysis Import feature from being associated to Groups selected for association on the **Save** step of the **Import Intel** window was fixed.
- An issue causing the **Last Modified** and **Date Added** timestamps on the **Associations** tab of the **Details** screen to display "Invalid Date" when viewed in the Safari® browser was fixed.
- An issue causing errors to occur when viewing an object's **Details** screen in a Source whose name contains certain special characters was fixed.
- TQL queries containing certain syntax errors were not being caught and flagged for the user to fix when entered in the advanced search feature on the **Browse** screen. This issue was corrected.
- An issue preventing POST requests to the `/v3/indicators` endpoint from creating a File Indicator in an owner when it exists in a different owner was fixed.
- Fields provided in POST requests for Email Groups to the `/v3/groups` endpoint were not being populated if a value for the optional `from` field was not specified. This issue was resolved.
- An issue causing errors to occur on SingleStore instances when sending requests to the `/v2/indicators/observed` endpoint was resolved.
- An issue causing case sensitivity defined in a custom Indicator type to be ignored when associating Indicators of that type to a Group was fixed.
- An error was occurring when using the urlscan.io enrichment service in the v3 API to enrich certain URL Indicators. This issue has been fixed.
- An issue causing uploaded Report Group files to get stuck in "Awaiting Upload" status was fixed.

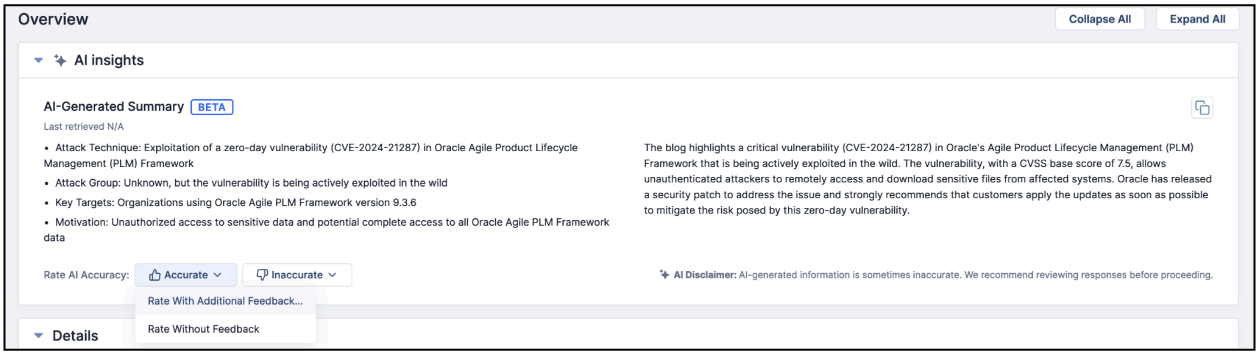
- An issue causing multiple warning messages to be sent to logs after an Organization has been deleted was fixed.
- ThreatConnect instances running version 7.7.3 in a containerized solution using Docker were automatically overwriting the value contained in the OpenSearch URL (**OPENSEARCH_URL**). This issue was corrected. In addition, support for setting more SMTP variables (**TC_SMTP_PORT**, **TC_SMTP_SSL**, and **TC_SMTP_TLS**) was added as well as a variable for shared memory size for Postgres® (**POSTGRES_SHM_SIZE**).
- Support for using a different certificate for connecting to the SAML Identity Provider (IdP) was added to ThreatConnect instances running a containerized solution using Docker. A section on enabling SAML was added to the installation, upgrade, and migration guides for ThreatConnect instances running a containerized solution using Docker. The guide for installing and configuring SAML now applies only to operating system deployments of ThreatConnect.

# CAL Updates

## 2025-01-06 CAL 3.10 [Latest]

### NEW! CAL ATL AI Feedback!

You can now provide direct feedback about what is working and what needs improvements in the AI summaries for CAL Automated Threat Library (ATL) Reports! Use the new **Rate AI Accuracy** feature on the **AI Insights** card to let us know if you find the summaries to be helpful, if they have problems, or if you have specific ideas about how they could be improved. The feedback is anonymously collected and used to create improvements to future AI summaries in ATL.



- Attack Technique: Exploitation of a zero-day vulnerability (CVE-2024-21287) in Oracle Agile Product Lifecycle Management (PLM) Framework
- Attack Group: Unknown, but the vulnerability is being actively exploited in the wild
- Key Targets: Organizations using Oracle Agile PLM Framework version 9.3.6
- Motivation: Unauthorized access to sensitive data and potential complete access to all Oracle Agile PLM Framework data

The blog highlights a critical vulnerability (CVE-2024-21287) in Oracle's Agile Product Lifecycle Management (PLM) Framework that is being actively exploited in the wild. The vulnerability, with a CVSS base score of 7.5, allows unauthenticated attackers to remotely access and download sensitive files from affected systems. Oracle has released a security patch to address the issue and strongly recommends that customers apply the updates as soon as possible to mitigate the risk posed by this zero-day vulnerability.

**AI Disclaimer:** AI-generated information is sometimes inaccurate. We recommend reviewing responses before proceeding.

*Provide feedback on AI summaries for CAL ATL Reports directly from the **Details** screen*

### Updated Feature: Hourly CAL ATL Updates!

The CAL Automated Threat Library now delivers fresh insights more frequently throughout the day, empowering you with up-to-date information from trusted open-source intelligence providers. Access Indicators, MITRE ATT&CK mappings, AI-powered summaries, industry insights, and more—faster than ever before.

- **Timely intelligence:** 33 blogs are now updated hourly for quicker access to critical insights.
- **Enhanced coverage:** Five additional sources will be updated multiple times daily for even greater visibility.
- **Continuous improvements:** More sources are under evaluation, so expect more updates to more sources more often…soon!

For Dedicated Cloud customers, the **CAL Automated Threat Library v1** Job App was updated to deliver hourly updates starting on January 8, 2025. For customers with On-Premises instances, the update is delivered automatically with the ThreatConnect 7.8.1 release. Please feel free to reach out to your Customer Success Manager with questions about this feature.

## Updated Feature: MITRE ATT&CK 16.0

ThreatConnect version 7.8 includes an update to MITRE ATT&CK 16.0, which adds 19 new techniques and sub-techniques, 33 new types of software, 11 new groups, 6 new campaigns, and 1 new course of action.

All MITRE ATT&CK framework items (techniques, software, groups, campaigns, course of action) can be visualized when modeling and exploring relationships in ATT&CK Visualizer and Threat Graph (i.e., when pivoting with CAL) and can be directly identified in textual content when using ThreatConnect Intelligence Anywhere, the Doc Analysis Import feature, and the Doc Analysis Playbook App. They can also be leveraged from the **Browse** screen, ThreatConnect's search engine, and in Intelligence Requirements.

## Other Updates

- Improvements were made to the ordering of results for Intelligence Requirements Global preview and daily results to provide more valuable matches to keywords.
- The CAL Safelist was expanded to include more trusted domains. With this update, CAL protects you from the distraction of an additional 1600+ Indicators in the ThreatConnect platform as well as makes this information clear in the ThreatConnect CAL integration with Polarity. CAL is working to constantly improve the accuracy of your threat intelligence, allowing you to focus on real threats while providing contextual insights and minimizing unnecessary noise in analyst research, document analysis, Indicator queries, and automated workflows across both ThreatConnect and Polarity.