ThreatConnect® Release Notes

Software Version 7.7

September 18, 2024

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

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

Table of Contents

New Features and Functionality

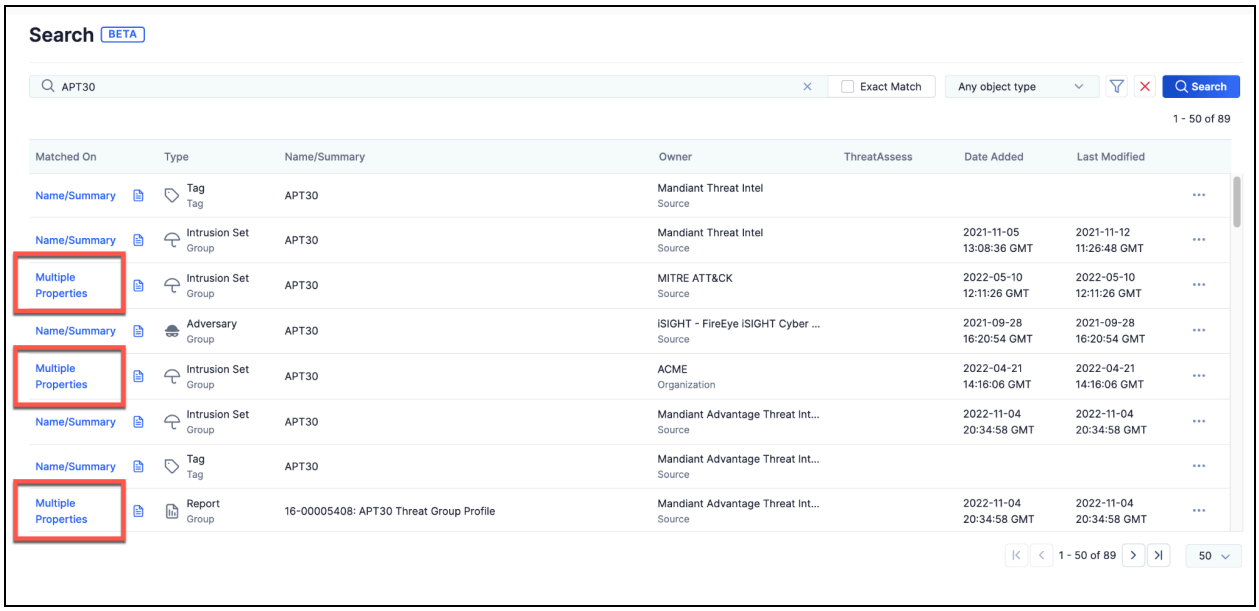
Enhanced Search Version 2

ThreatConnect 7.7 brings thoughtful improvements to the Enhanced Search functionality we introduced in ThreatConnect 7.6, providing you with a more intuitive and powerful tool for navigating your security data. This update refines your user experience by offering detailed match insights, a new filtering option, and the ability to take action on your search results directly from the **Search** screen. With these improvements, you can efficiently understand and operationalize your search results.

Enhanced Match Insights

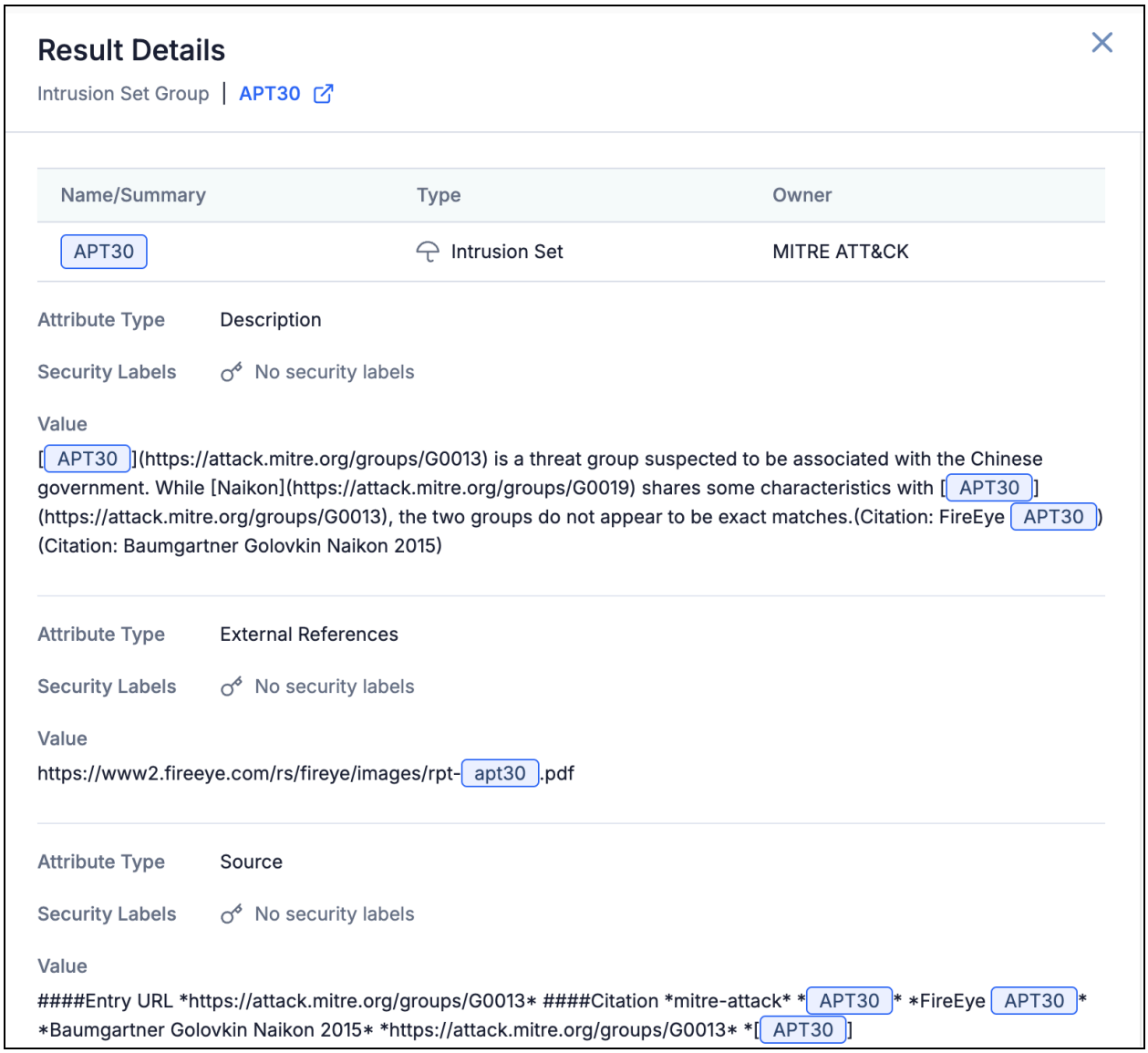
In ThreatConnect 7.7, the Search feature not only detects the presence of keywords in the intelligence in your owners, but also lets you know when the keywords were found in multiple places within a piece of intelligence and highlights all the specific locations within each object where the keywords were found.

Just as in ThreatConnect 7.6, when you perform a keyword search, the **Matched On** column in the results table displays the data type on which the query matched, such as the object's Name/Summary, an Attribute, or a Tag, giving you a clear understanding of how the object matched the search term. ThreatConnect 7.7 adds **Multiple Properties** to the possible values in the **Matched On** column so that you can easily identify objects that matched the search term in multiple places.



The ***Matched On*** *column displays* ***Multiple Properties*** *when a keyword matches in more than one place*

If you need more information on where a search term has matched within an object, you can click the link in the **Matched On** column or the icon next to it to display a **Result Details** drawer highlighting each area that contains the match. This feature provides a comprehensive view of each of your search results, enhancing your understanding of the context surrounding the search term's occurrence.



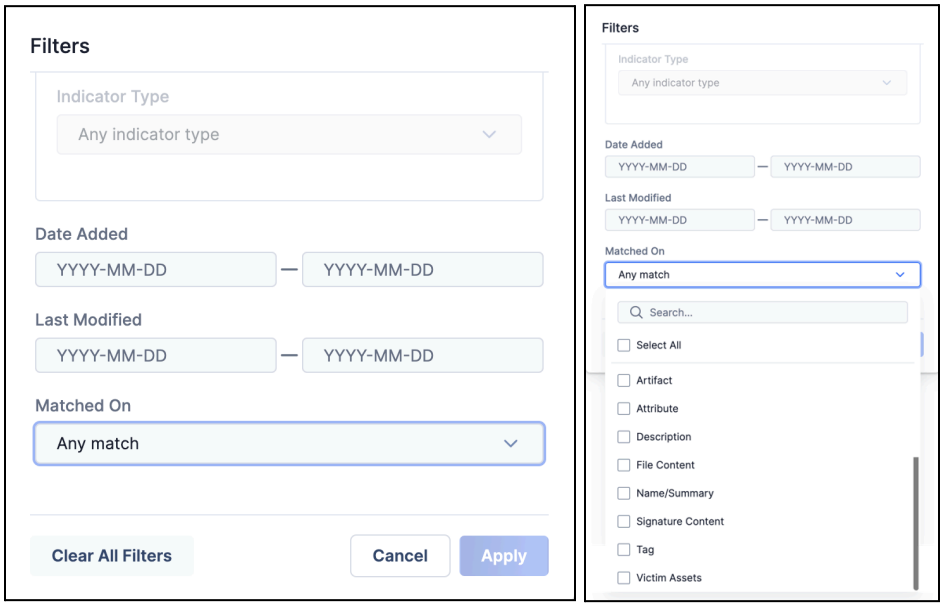
*The **Result Details** drawer highlights the areas in an object that matched your search term*

"Matched On" Filtering Option

The ability to filter search results has been expanded significantly in this release. You can now filter your search results by selecting specific field types from the **Matched On** filter. For instance, if you select **Artifacts** from the filter, the results table will exclusively display entries for which the search term has matched the names of Artifacts associated with Workflow Cases in your Organization.

To use the filter, open the **Filters** menu at the upper right of the **Search** screen, scroll to the bottom, click the **Matched On** dropdown, and choose the field(s) to which you want to

narrow your search results. Once you have made your selections, click **Apply** to update the results table.

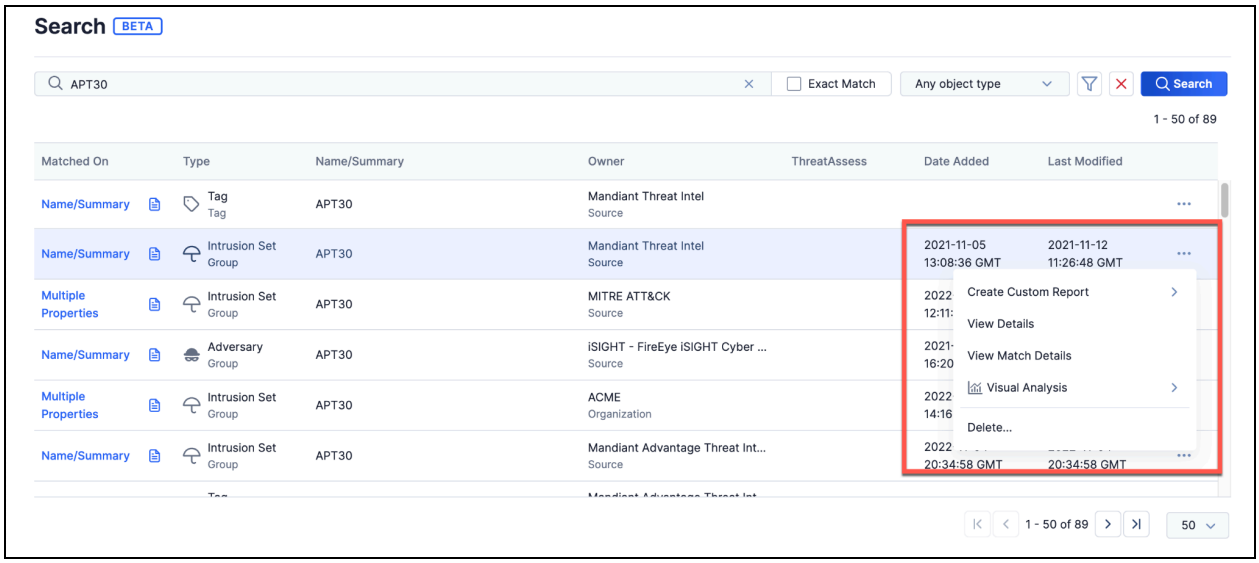


*Filter search results to specific fields in the **Matched On** column*

This new filtering option empowers you to drill down into your data with greater precision, making it easier to find exactly what you need.

Actionable Context Menu

Finally, we have introduced a quick-access context menu that enables you to perform relevant actions on objects directly from the search results table. Each object type has a slightly different context menu, which you can open by clicking **Options** ••• at the end of a result's row.



Perform actions and view more details on a search result directly from the new context menu

Options for Indicators

- **Add to Exclusion List**: Organization Administrators can add the Indicator to their Organization-level Indicator Exclusion List.
- **Change Status to Inactive** or **Change Status to Active**: If your user account has the requisite permissions in the Indicator's owner, you can change the status of the Indicator.
- **Explore in Graph**: Visualize, explore, and analyze the Indicator's associations in Threat Graph.
- **View Details**: View the Indicator's **Details** drawer.
- **View Match Details**: View the fields in the Indicator object on which your search term matched.
- **Delete**: If your user account has the requisite permissions in the Indicator's owner, you can delete the Indicator from the owner.

Options for Groups

- **Create Custom Report**: Create a report for the Group from scratch or from a Group report template.
- **View Details**: View the Group's **Details** drawer.
- **View Match Details**: View the fields in the Group object on which your search term matched.
- **Visual Analysis**: Select from the following options:

    - **Explore in Graph**: Visualize, explore, and analyze the Group's associations in Threat Graph.
    - **Visualize ATT&CK**: Open the ATT&CK Visualizer with the Group added as an analysis layer within a new ATT&CK® view.
- **Delete**: If your user account has the requisite permissions in the Group's owner, you can delete the Group from the owner.

Options for Cases

- **Create Custom Report**: Create a report for the Case from scratch or from a Case report template.
- **Explore in Graph**: Visualize, explore, and analyze the Case's associations in Threat Graph.
- **View Details**: View the Case's **Details** drawer.
- **View Match Details**: View the fields in the Case object on which your search term matched.
- **Delete**: If your user account has the requisite permissions in your Organization, you can delete the Case from the Organization.

Options for Tags

- **Explore in Graph**: Visualize, explore, and analyze the Tag's associations in Threat Graph.
- **View Details**: View the Tag's **Details** drawer.
- **View Match Details**: View the fields in the Tag object on which your search term matched.
- **Delete**: If your user account has the requisite permissions in the Tag's owner, you can delete the Tag from the owner.

Options for Victims

- **View Details**: View the Victim's **Details** drawer.
- **View Match Details**: View the fields in the Victim object on which your search term matched.
- **Delete**: If your user account has the requisite permissions in the Victim's owner, you can delete the Victim from the owner.

Reporting: Customize Group and Case Templates

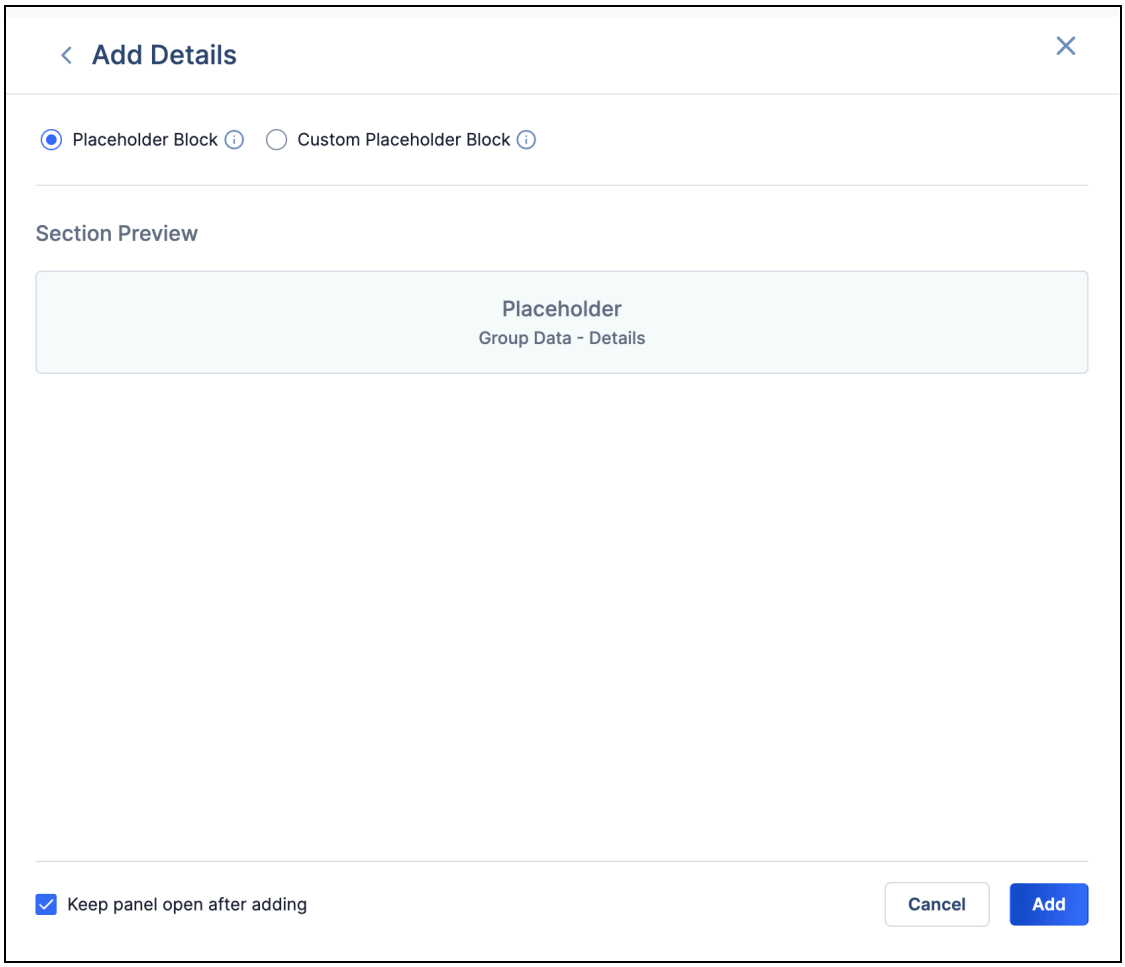
ThreatConnect 7.7 introduces custom placeholder blocks, which provide the ability to preset Group and Case report templates with selected details, Attributes of selected Attribute Types, and advanced filters for Group, Indicator, and (for Group report templates only) Victim Asset associations. This new feature empowers you to efficiently generate detailed and customized reports that meet your organization's specific needs.

Configuring Custom Placeholder Blocks in a Report Template

Custom placeholder blocks are available in the following **Group Data Placeholder** and **Case Data Placeholder** sections when creating a Group or Case report template in the **Template Editor**:

- **Details**
- **Attributes**
- **Group Associations**
- **Indicator Associations**
- **Victim Assets Association** (Group report templates only)

When creating or editing a Group or Case report template, click **+ Add Section** at the upper right to open the **Add Section** drawer. Then click **+** for one of the sections in the foregoing list. You will be provided with two options: **Placeholder Block** and **Custom Placeholder Block**.



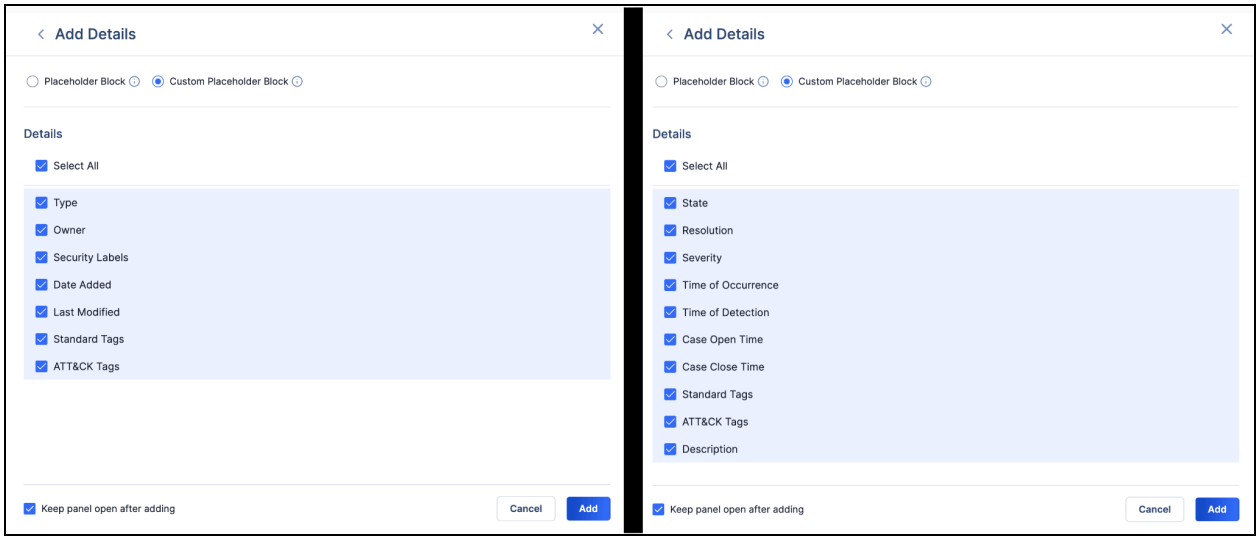
Add a placeholder block or custom placeholder block to a report template

Select **Custom Placeholder Block**, and then configure the placeholder block to include only the information that you want a report using the template to display, as described next for each type of section.

Details

For Group and Case report templates, the **Details** custom placeholder block lets you choose the **Details** data fields to include in a report.

> ⓘ **Tip**: Use the placeholder block when you want to include all **Details** fields for a Group or Case in reports built from the report template. Use the custom placeholder block when you want to display only a subset of **Details** fields for a Group or Case in reports built from the report template.



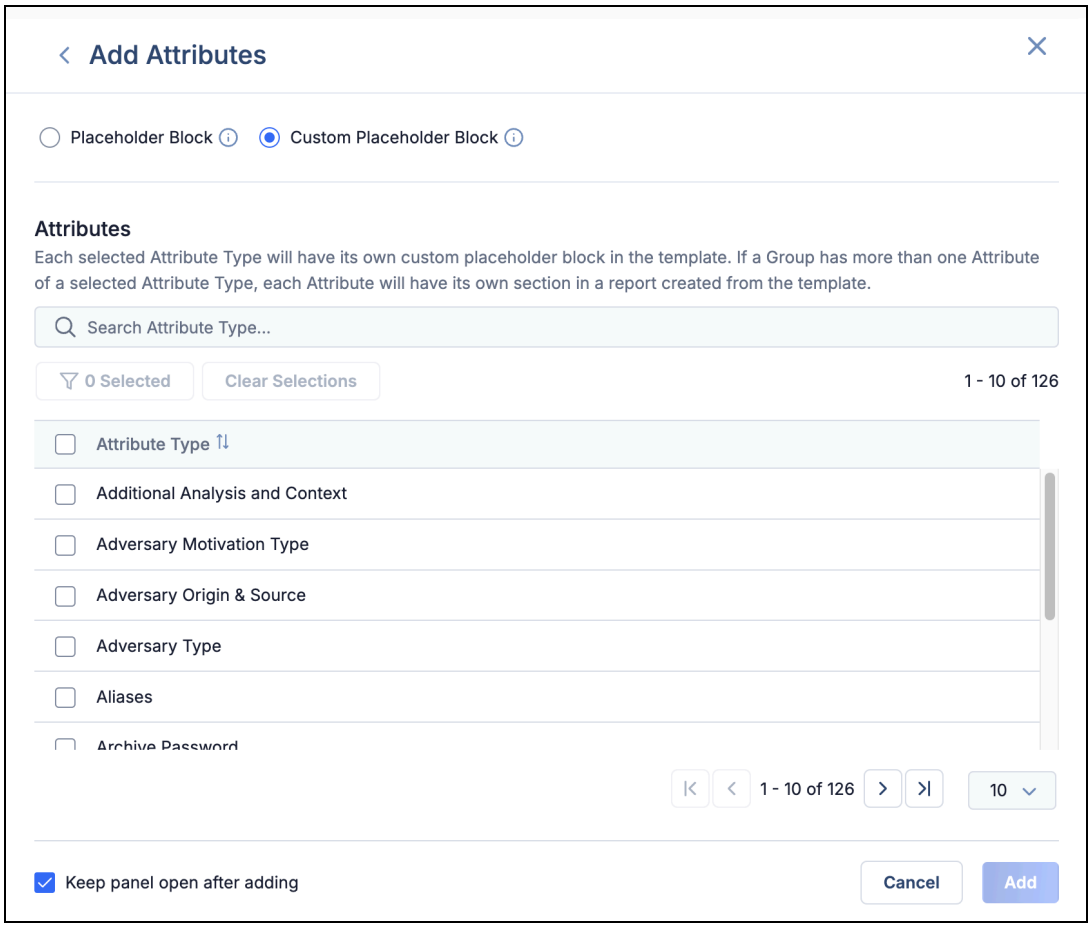
*Choose the **Details** fields to add to a Group (left) or Case (right) custom placeholder block*

By default, all **Details** fields are selected. Deselect the fields you don't want, keep the selections for the fields you do want, and click **Add**. A **Custom Placeholder** section for **Details** will be added to the report template. When a user creates a report from the template, a **Details** section displaying only the fields you selected will be included in the report.

Attributes

For Group and Case report templates, the **Attributes** custom placeholder block lets you choose the Attribute Types you want to include in a report. Each Attribute the Group or Case has of each selected Attribute Type will be displayed in its own section in the report.

> ⓘ **Tip**: Use the placeholder block when you want a user creating a report from the template to select specific Attributes to include in the report. Use the custom placeholder block when you want to display all Attributes of a specific set of Attribute Types for a Group or Case in reports built from the report template.



Choose the Attribute Types for which to create a custom placeholder block (shown for Group, but almost identical for Case)

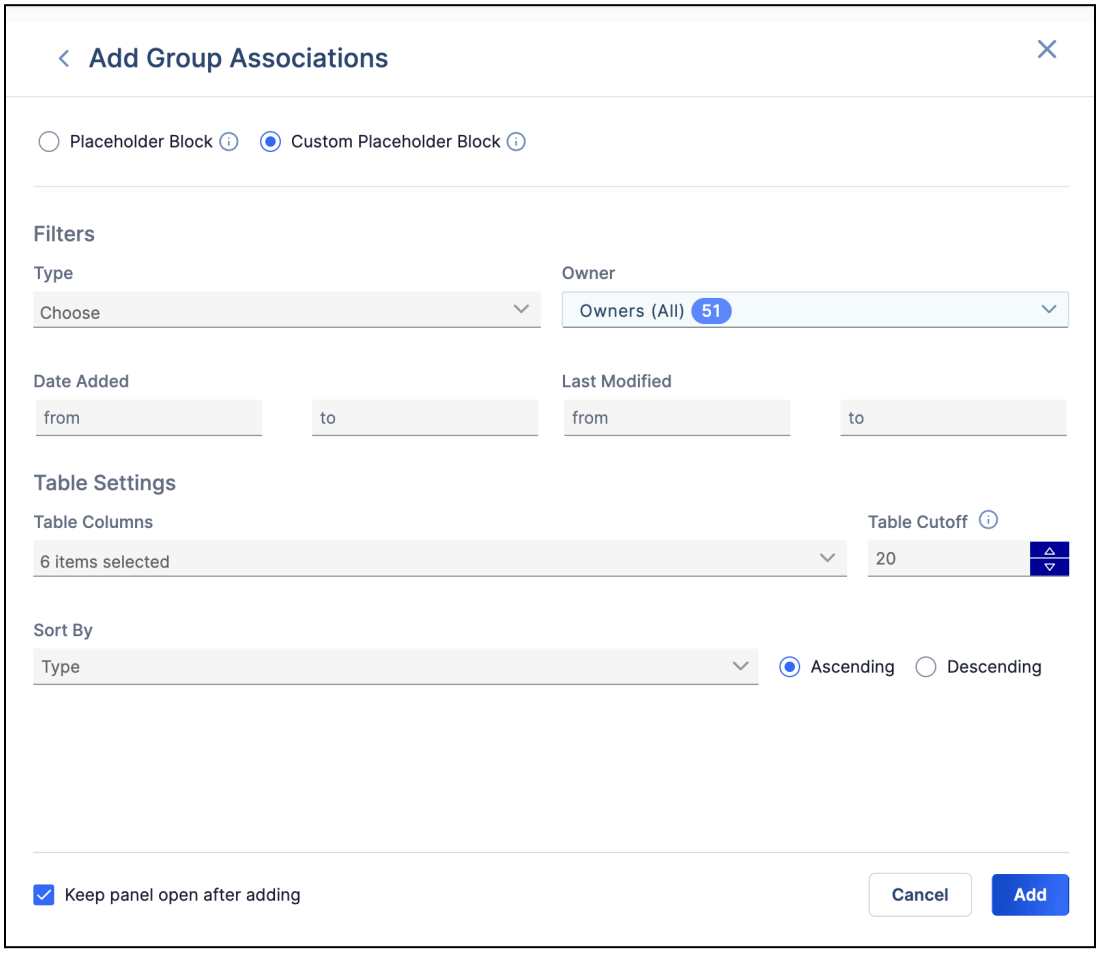
Select the Attribute Types you want to include, and click **Add**. A **Custom Placeholder** section for each Attribute Type will be added to the report template. When a user creates a report from the template, a section for each Attribute the Group or Case has for each selected Attribute Type will be included in the report, without further configuration required from the user.

Group and Indicator Associations

For Group and Case report templates, the **Group Associations** and **Indicator Associations** custom placeholder blocks let you add filters to display only associated Groups and Indicators, respectively, of the selected types, owners, dates added, and last modified dates, ensuring that reports created from the template include only the most relevant Group and Indicator associations. You can adjust the **Table Settings** to specify which columns to include in the associations table and the maximum number of associations to show. You can

also specify which column the associations table should be sorted by and the sort order (ascending or descending).

> **Tip**: Use the placeholder block when you want to display a table containing all associated Groups or Indicators, with all available table columns, for a Group or Case in reports built from the report template. Use the custom placeholder block when you want to filter the associated Groups or Indicators displayed for a Group or Case and to customize the display settings for the associations table in reports built from the report template.



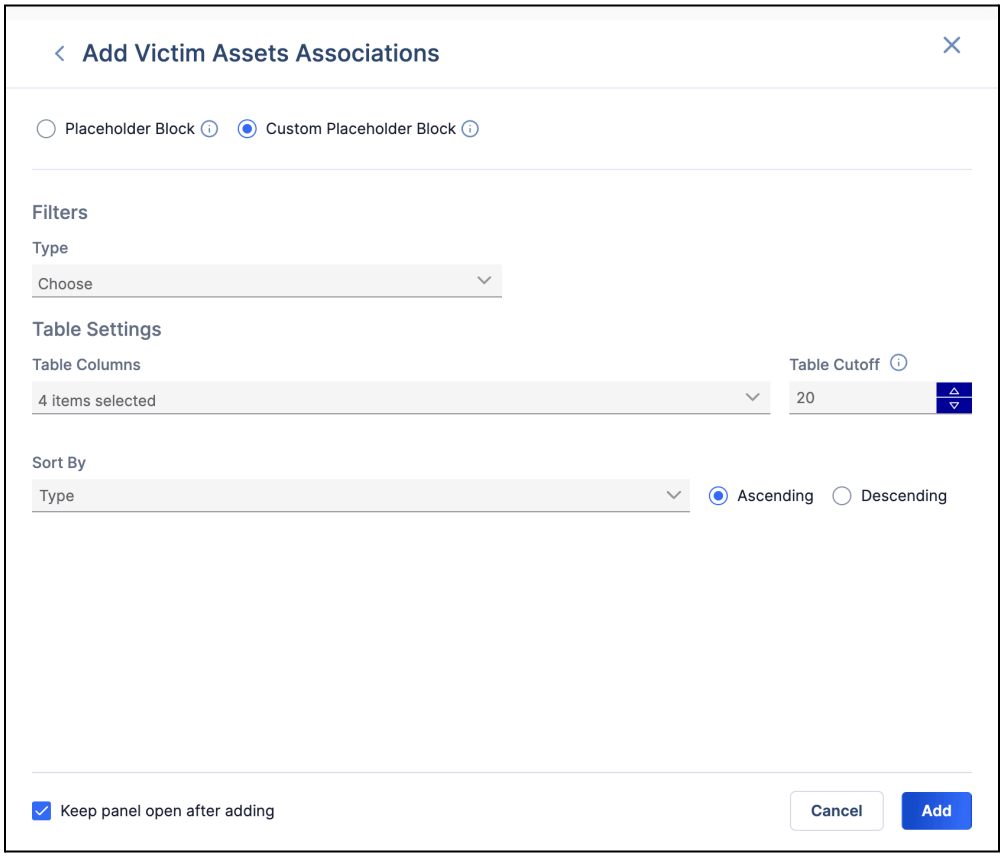
Configure the filters and table settings for a Group Associations table in a custom placeholder block (identical for Indicator Associations)

Make your selections, and click **Add**. A **Custom Placeholder** section for Group or Indicator associations will be added to the report template. When a user creates a report from the template, a table displaying the Group's or Case's associated Groups or Indicators, configured to the specifications in the report template, will be included in the report.

Victim Assets Associations

For Group report templates only, the **Victim Assets Associations** custom placeholder block lets you select the types of associated Victim Assets to display, ensuring that reports created from the template include only the most relevant Victim Asset associations. You can adjust the **Table Settings** to specify which columns to include in the associations table and the maximum number of associations to show. You can also specify which column the associations table should be sorted by and the sort order (ascending or descending).

> **Tip**: Use the placeholder block when you want to display a table containing all associated Victim Assets, with all available table columns, for a Group in reports built from the report template. Use the custom placeholder block when you want to filter the associated Victim Assets displayed for a Group and to customize the display settings for the associations table in reports built from the report template.



Configure the filters and table settings for a Victim Assets Associations table in a custom placeholder block (Group report templates only)

Make your selections, and click **Add**. A **Custom Placeholder** section for Victim Asset associations will be added to the report template. When a user creates a report from the

template, a table displaying the Group's associated Victim Assets, configured to the specifications in the report template, will be included in the report.

Creating a Report From a Customized Template

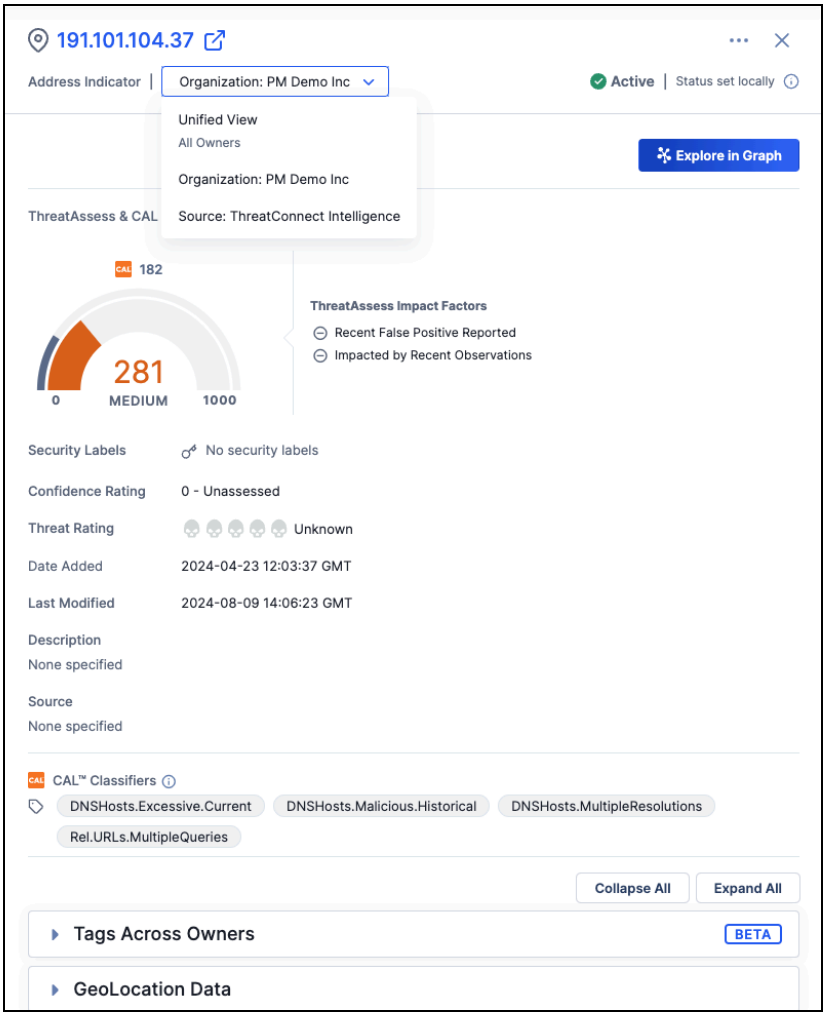
After you have saved a Group or Report report template with custom placeholder blocks, you and other users can utilize it to generate reports for a Group or Case, respectively. The custom placeholder blocks in the report will display only the information you have selected and will not require any further configuration. After generating the report, review the contents to ensure they meet your needs. You can edit any section, including those created from custom placeholder blocks, to modify its content, enabling further customization. This flexible approach allows you to create comprehensive and tailored reports efficiently.

Unified View: Indicator Details Drawer

Over the past several releases, we've added functionality intended to make it easier to find and understand context around Indicators. In ThreatConnect 7.7, we are taking this work a step further and introducing a **Unified View** option on the Indicator **Details** drawer available in various areas of ThreatConnect, including the **Browse** screen and Threat Graph. This new option displays a version of the Indicator **Details** drawer showing information from all of the Indicator's owners to which you have access, enabling you to view critical contextual information without having to visit each version of the Indicator in each of its different owners.

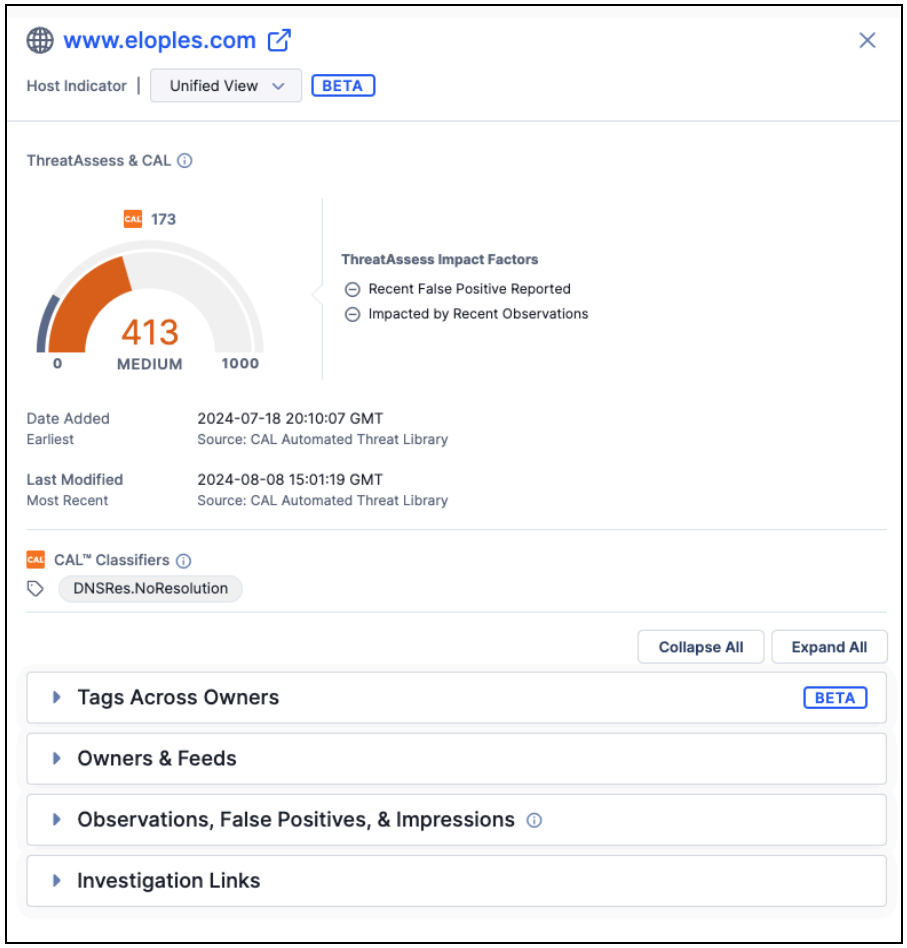
The **Unified View** option is available in the **Owners** dropdown at the top left of the Indicator **Details** drawer. Please keep in mind that this option is available only for Indicators and is a beta feature in this version of ThreatConnect.

Note: Your System Administrator must turn on the **multiSourceViewEnabled** system setting for the **Unified View** option to be available on your ThreatConnect instance.



*Use the **Owners** dropdown to change to the unified view for an Indicator*

After you select **Unified View**, the Indicator **Details** drawer will show information about the Indicator from all the owners you have access to in which the Indicator exists. The available data include the earliest date added, which shows when the Indicator was first added to any of the owners, and the most recent "last modified" date, which shows when the Indicator was last modified in any of the owners. In addition, the drawer will display a few select cards: the **Tags Across Owners** card introduced in ThreatConnect 7.6; **Owners & Feeds** (which shows the Indicator's Threat Rating and Confidence rating in all its owners to which you have access); **Observations, False Positives, & Impressions**; and **Investigation Links**.



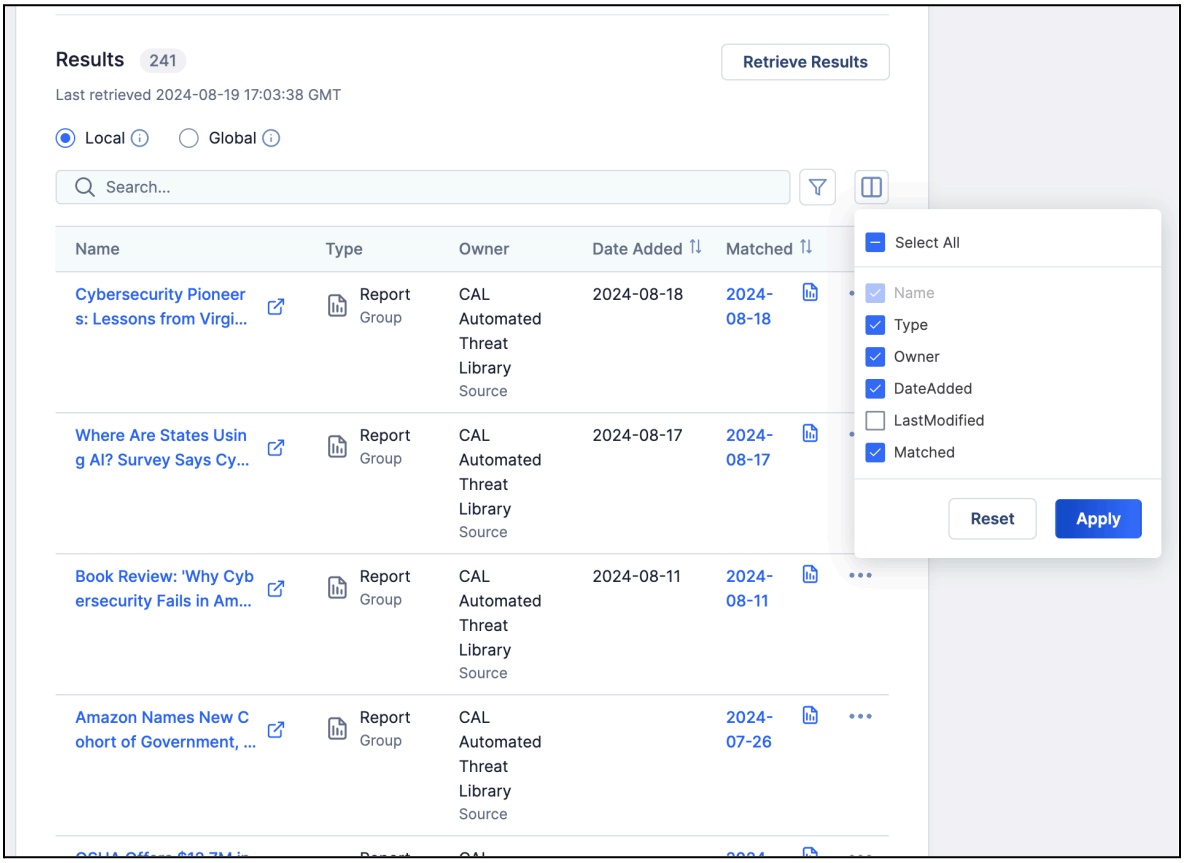
*Unified view of an Indicator's **Details** drawer shows its earliest date added and most recent "last modified" date*

Intelligence Requirements Filters

We continue to make incremental improvements and enhancements to our Intelligence Requirement (IR) feature. In this version of ThreatConnect, we introduce additional filtering options on IR results and basic **Browse** screen filters for IRs. IRs look at all available information in an instance, and sometimes that investigation brings historical data to the surface. The new filter options for IR results will help you focus your processing and analysis efforts on items that are most recent. With these new options, you can filter your IR results list by date added and "last modified" date so you can focus on just the things that are in a specific timeframe of interest.

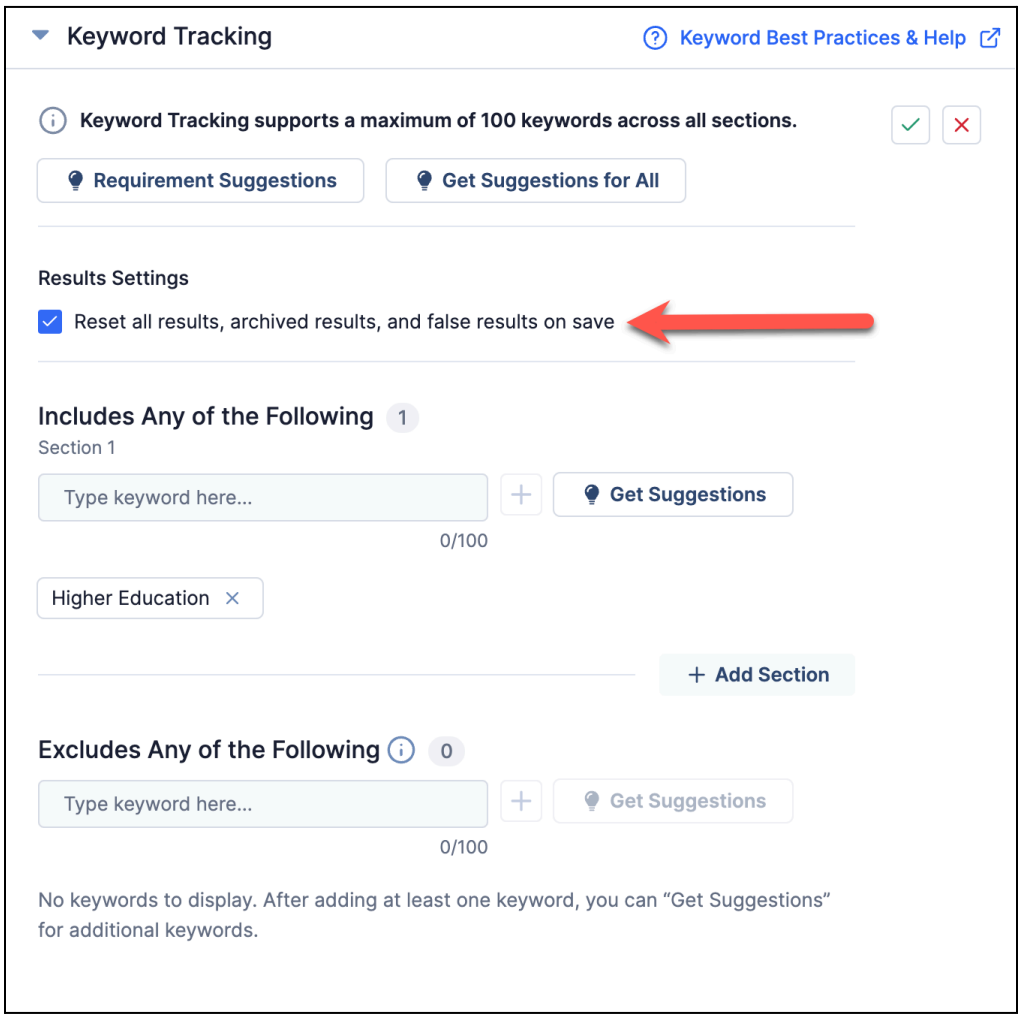
Date Added and Last Modified Filters for IR Results

On an IR's **Details** screen, the results table on the **Keyword Tracking & Results** card now displays a new **Date Added** column by default, and you can use the column selector to add a **Last Modified** column as well.These columns are both sortable, allowing you to order your IR results by the date when they were first added or last modified in their owner.



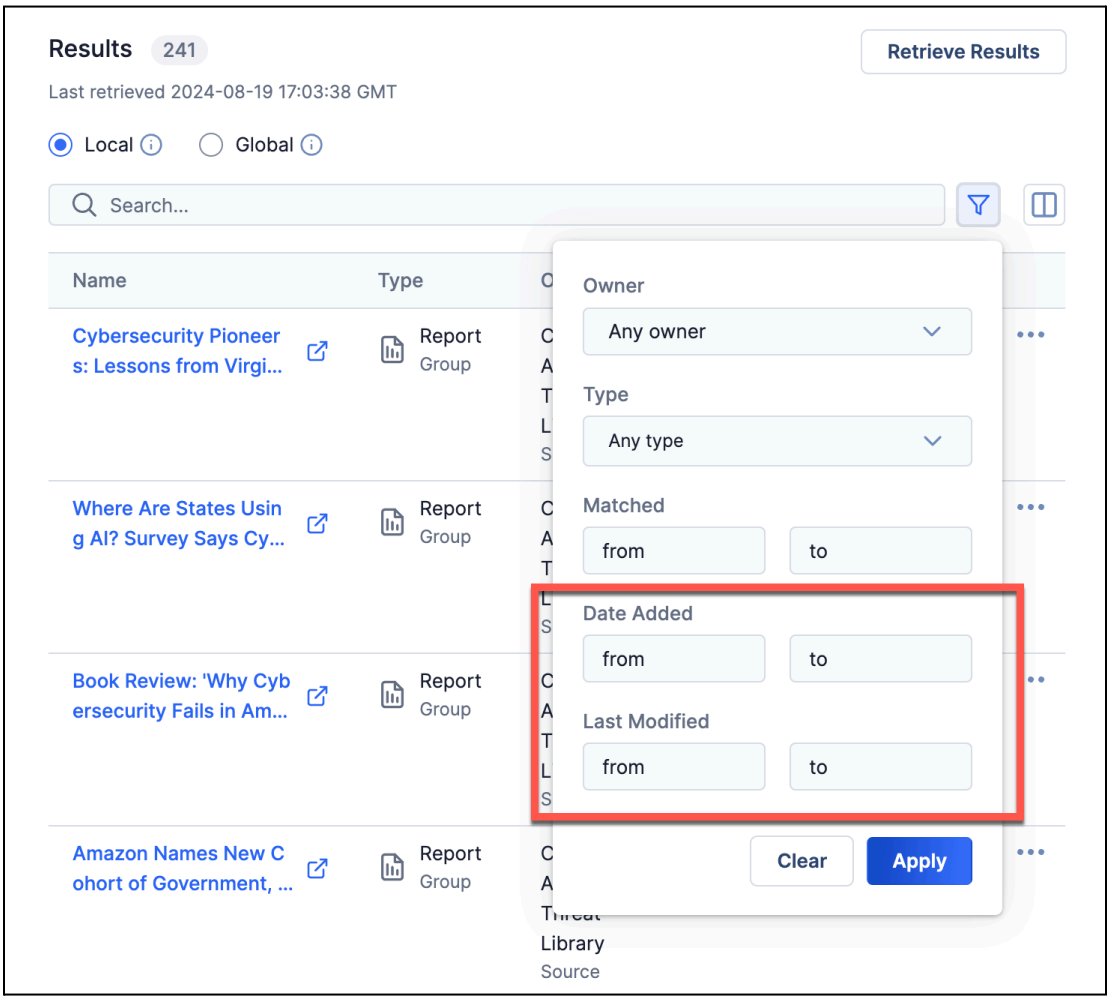
View and sort by IR results by date added and "last modified" date

It is important to note that IRs created in your Organization prior to your ThreatConnect instance's update to 7.7 will not immediately have data populated into the **Date Added** and **Last Modified** columns of their results table. In order to populate these columns for legacy results (i.e., results matched prior to the instance's update to 7.7), expand the **Keyword Tracking** section of the **Keyword Tracking & Results** card, click at the upper right to edit the card, select the **Reset all results, archived results, and false results on save** checkbox, and then click at the upper right to save the changes. This will reset the IR's results and populate the two date fields for all legacy results. If you do not want to reset an IR's results, all results generated after the update to 7.7 will have the date fields populated, but the legacy results will not have data in those fields.



*Reset your IR's results to populate the **Date Added** and **Last Modified** columns for legacy results*

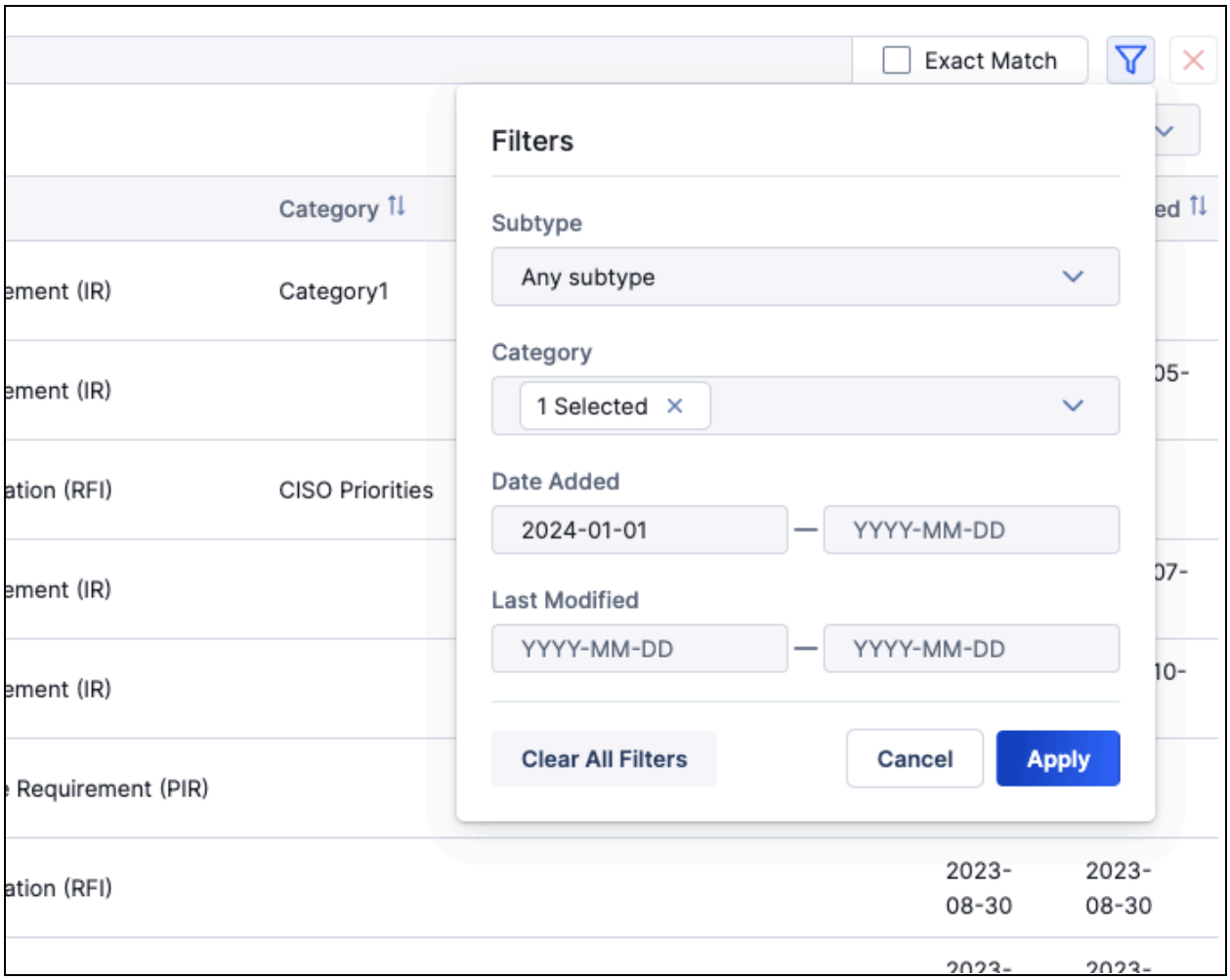
The filters for **Date Added** and **Last Modified** can be accessed via **Filters** menu at the upper right of the results table.



***Date Added** and **Last Modified** ranges are now in the **Filters** dropdown*

Basic Browse Screen Filters for Intelligence Requirements

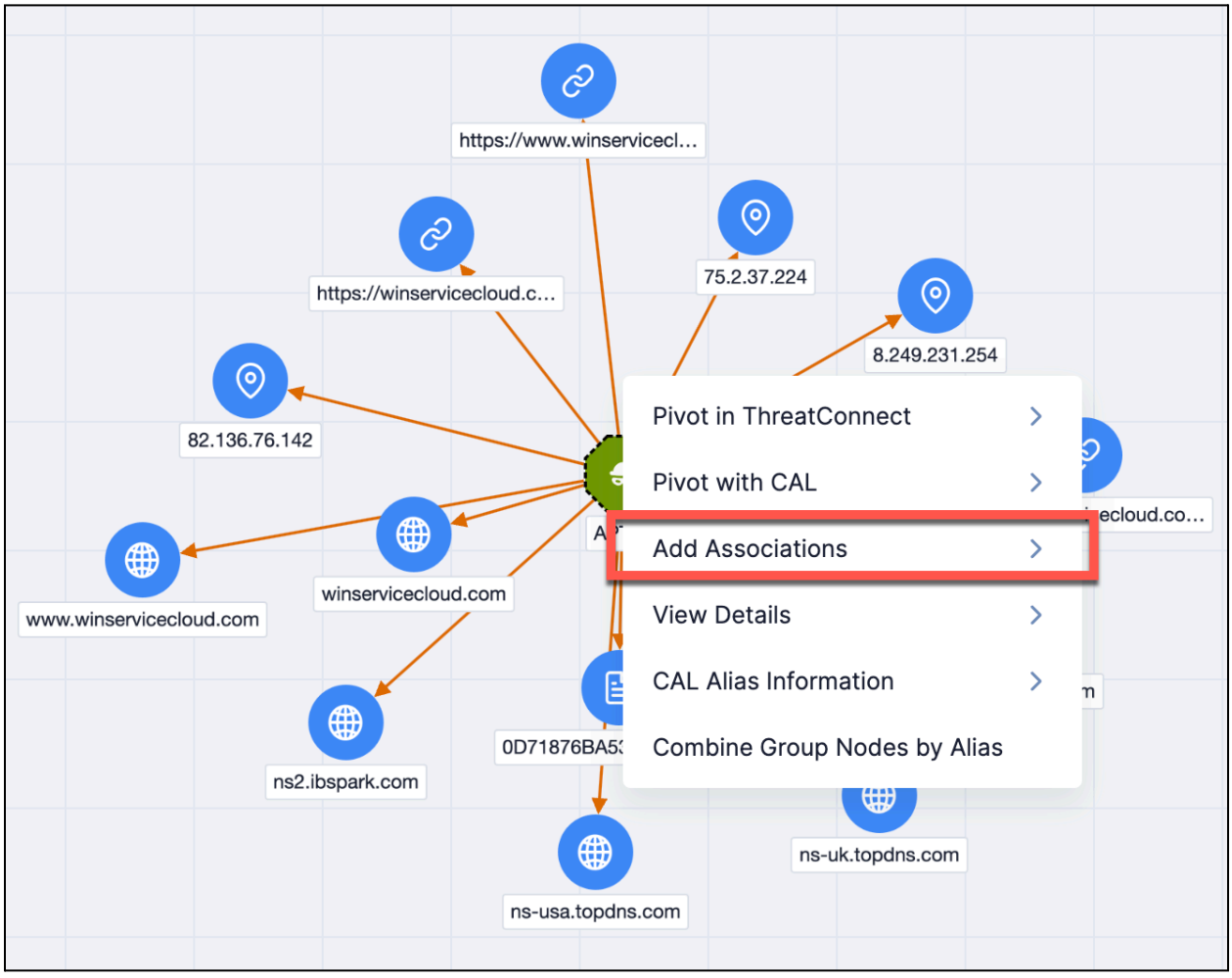
While ThreatConnect has historically supported IR filtering by ThreatConnect Query Language (TQL), IRs did not have basic filters available on the **Browse** screen. As of ThreatConnect 7.7, you can now filter IRs in the **Browse** screen UI by subtype, category, date added, and "last modified" date. These options are available in the new **Filters** menu at the upper right of the table.



*The **Browse** screen now provides options to filter IRs*

Threat Graph: Add Associations

We've received countless pieces of feedback around the Threat Graph feature since its release a few years ago. In ThreatConnect 7.7, we are pleased to share that, in response to your feedback, we have introduced the ability to add associations directly in the graph. We know many analysts prefer to work in link analysis tools like the ThreatConnect Threat Graph. With this update, you will now be able to build out your work without having to leave the graph. In this version of ThreatConnect, you can add Indicator-to-Group associations, Group-to-Indicator associations, and Group-to-Group associations without leaving the graph. You can also add multiple associations at once, and those associations are reflected not only in Threat Graph, but also on the **Associations** tab of the object's **Details** screen and on the **Associations** card on the object's legacy **Details** screen. We hope this update helps you streamline your research and analysis going forward.



Add associations to an object directly from Threat Graph

Improvements

Threat Intelligence

- When an Indicator's status is updated by a user or through certain system processes, its **Last Modified** date, as well as the **Last Modified** date of all copies of that Indicator in all owners on the ThreatConnect instance if the **indicatorStatusLock** system setting is turned off, will be updated. This change will be noted on the **Activity** tab of the **Details** screen for each copy of the Indicator, except when the Indicator's status is changed via the v2 Batch API.
- The TQL Auto Associate feature is now available for IRs, enabling you to assign up to two TQL queries to an IR—one for Groups and one for Indicators. You may access this feature on the **TQL Queries** card on the **Associations** tab of an IR's **Details** screen.

Browse and Details

- Organization Administrators can now set default custom views for the **Custom View** tab on the **Details** screen—one for Groups and one for Indicators. This is a great option when you want to take the guesswork away from your users and provide them with a view that is ideal for your Organization's needs. When a default custom view has been set, users in the Organization have the option to select it or use a custom view of their own. To set a custom view for your Organization, navigate to the new **Default Custom Views** tab of the **Organization Config** screen and import a **.tccv** file for Indicators or Groups into the corresponding section. You can also delete a custom view from this screen. Alternatively, you can build the view you want on the **Custom View** tab of an object's **Details** screen and then select **Set View as Org Default** from the ··· menu on the **Manage View** drawer to set that view as the Organization's custom default view for the object type (Group or Indicator). Once a default custom view has been set for Groups or Indicators, users in the Organization can select the **Enable org default view** checkbox in the **Manage View** drawer from the **Custom View** tab of an object's **Details** screen if they want to use the Organization's default view.
- The **Tags** filter on the **Browse** screen has been updated to a more intuitive and user-friendly design. In addition, you can now search by ATT&CK technique ID when doing a **Basic** search, as well as filter by the date the Tag was last used. When doing an **Advanced** search, there is now a tooltip to the left of the search bar that lets you

know whether your TQL query is valid and provides more information on the errors found in invalid queries.

- Following on the update of the Indicator **Details** drawer in ThreatConnect 7.6, we have updated the Group **Details** drawer in ThreatConnect 7.7. The new format gives you an efficient way to get easy-to-read context on a Group while working in areas of the platform such as Browse, Threat Graph, and Search. As with the Indicator **Details** drawer, the Group **Details** drawer includes cards for features such as UserAction Playbooks, Attributes, associations, and Notes. The updated Group **Details** drawer is available for all Group types except Email, Signature, and Task.
- The new Indicator and Group **Details** drawer now has a pop-out icon next to the object's name that lets you open the object's **Details** screen in a new browser tab.

Reporting

- When adding a **Group Data** section to a report, you can now select a different Group in the section's configuration instead of having to go back to the **Add Group Data** menu to swap the Group.
- When adding a **Case Data** section for **Details** or **Attributes** to a report, you can now select a different Case in the section's configuration instead of having to go back to the **Add Case Data** menu to swap the Case.
- The format of Attributes in ThreatConnect's reporting feature has been adjusted to provide a more useful and efficient display. The Attribute's **Value** is now on top, followed by **Security Labels** and **Attribute Source** on the next line. The **Date Added** and **Last Modified** fields have been removed.

Search

- The default view for the ThreatConnect search engine is now set to whichever view you most recently used. If you click **Try Search Beta** from the legacy **Search** drawer, then the new **Search** screen will be your default view the next time you click the magnifying glass at the upper right of the top navigation bar. If you click **Revert to Legacy Search** from the **Search** screen, then the legacy **Search** drawer will be your default view.
- You can now sort the results table on the new **Search** screen by the **Name/Summary** column. Note that the names of some Report Groups in the **CAL Automated Threat Library Source** currently have a space at the beginning of their Name/Summary,

which will cause them to appear to be out of order (i.e., at the top of the list or at the bottom of the list) when the **Name/Summary** column is sorted.

- You can now sort the results table on the new **Search** screen by the **ThreatAssess** column, enabling you to bubble results with the highest or lowest ThreatAssess score to the top of the table.
- On the new **Search** screen, all **Exact Match** searches in your recent search history will be enclosed in double quotes so you can easily identify that you were searching for an exact phrase. If you re-run one of these searches, it does not matter whether you select the **Exact Match** checkbox or not, as the system will no longer surround the search term with an extra set of quotes.
- In addition to **[.]**, **[:]**, and **[@]**, the **Search** screen now recognizes the following defanged character sequences: **[dot]**, **h..p://**, **h..ps://**, and **f.p://**.

Threat Graph

- A number of design and functionality improvements were made to the Threat Graph feature, including the following:
    - Graph Objects **drawer**: The **Details** table, which displays information about the objects shown in Threat Graph, has been renamed as the **Graph Objects** drawer and it is more intuitive to open, view, and use. You can easily open it by clicking the **View Table** button at the upper right of the **Threat Graph** screen. New features in the redesigned table are pagination, a column selector, separate columns for object type and name, and an options menu in each row for actions such as adding an object to an owner, running a Playbook on the object, and removing the object from the Threat Graph.
    - **Legend**: The icon to open the legend has been moved to the new toolbar at the top left of the Threat Graph. The legend's UI has been updated to match the look and feel of other areas of ThreatConnect. The objects in the legend are now grouped by object type, and there is a search bar, as well as a **Select All** option, at the top.
    - **Layout controls**: The layout controls have been moved to a toolbar at the top left of the Threat Graph, and **Scroll to zoom** is now a toggle on that strip instead of an option under a gear-wheel icon. The **Options** ··· menu has moved to the top right of the Threat Graph, and the **Save** option that was previously in that menu is now a separate **Save Graph** button at the top right.
    - **Screen Header**: The name of the Threat Graph you are viewing and a link to the main **Graph** screen (the screen that displays all saved Threat Graphs in

your Organization) are now displayed in the upper left corner of a Threat Graph.

- **Nodes**:
  - Objects that exist in multiple owners now have a dashed border around their node instead of a solid black border.
  - All Group nodes are now the same color, with the Group type differentiated by the icon in the node. Similarly, all Indicator nodes are now the same color, with the Indicator type differentiated by the icon in the node.
  - The arrows that connect nodes have been simplified for a cleaner look and feel.

MITRE ATT&CK

- The ThreatConnect ATT&CK Visualizer and ATT&CK Tags have been updated to include MITRE ATT&CK® 15.1 data. These updates will be automatically deployed for all ThreatConnect instances, including those that do not have CAL™ turned on.

User Administration

- Support was added for API tokens with configurable expiration times. The expiration time is defined when creating or editing an API user, with the default and upper limit defined in the **apiUserDefaultTokenExpiration** and **apiUserMaxTokenExpiration** system settings, respectively.
- Accounts Administrators can now create user accounts with a System role of API User in On-Premises and Dedicated Cloud ThreatConnect instances.

System Settings

- The following new system settings were added:
  - **apiUserDefaultTokenExpiration**: This setting determines the default lifetime, in days, for an API user account token.
  - **apiUserMaxTokenExpiration**: This setting specifies the maximum lifetime, in days, that can be configured for an API user account token.

UI/UX

- The following changes were made to the ThreatConnect UI to provide a more consistent and comfortable user experience:
    - The tabbed navigation bar for the following screens has been updated to match that of the **System Settings** screen: **Account Settings**, **Community Config**, **Community Info**, **Source Config**, **Source Info**, **Org Config**, **Org Settings**, and **My Profile**.
    - As part of our efforts to refine the ThreatConnect UI to be more visually friendly and consistent, we have changed the color of many of the clickable buttons in the UI from orange to blue.
    - In the **Dashboard** dropdown on the top navigation bar, the options for importing and creating a dashboard were redesigned.

API & Under the Hood

- The **threatconnect/app/log** folder is now a Docker® mount, which means the logs will now be local to the host machine. In addition, the **threatconnect-docker.zip** files have been upgraded.
- You can now configure the maximum allocation of memory for your Redis® and OpenSearch® Docker containers.

Bug Fixes

Search

- An issue causing extra text to be added to owner hyperlinks in legacy **Search** drawer results was fixed.

Threat Intelligence

- When copying a Group from one owner to another, ATT&CK Tags on associated Indicators were being copied as standard Tags, creating duplicate Tags on target Indicators that already had those ATT&CK Tags applied to them before the copy operation. In addition, if the Indicators with duplicate Tags were included in a subsequent copy operation, an error would occur. This issue was resolved, and the duplicate standard Tags are automatically removed when an instance is updated to version 7.7 of ThreatConnect.
- **#totalhash** is no longer supported as an Investigation Link.

Threat Graph

- The **Last Seen** column was removed from the table in the **Graph Objects** drawer (formerly known as the **Details** table) in Threat Graph.

Owner Administration

- An issue preventing Organizations containing Tags with cross-owner associations from being deleted was fixed.

API & Under the Hood

- Efficiency improvements were made for ThreatAssess.

Dependencies & Library Changes

- ThreatConnect is now running Redis 7.2.4.
- ThreatConnect is now running Java® 17.

Maintenance Releases Changelog

There have been no patch releases at this time. 7.7.0 is the latest version.