ThreatConnect® Release Notes

Software Version 7.6

June 12, 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 **5**
- Reporting: Generic and Case Templates 5
  - Case Templates 5
  - Generic Templates 10
- Reporting: Enhancements 13
  - CAL ATL AI-Generated Summaries in Reports 13
  - ATT&CK Tags in Reports 15
- Enhanced Search 17
  - Step 1: Access the New Search Screen 17
  - Step 2: Enter Keywords 18
  - Viewing Search Result Details 20
  - Filtering Search Results 21
- Clear Context 23
  - Tags Across Owners 23
  - Indicator Details Drawer 24

Improvements **26**
- Threat Intelligence 26
- Reporting 27
- System Settings 28
- Workflow 28
- API & Under the Hood 28

Bug Fixes **30**
- Threat Intelligence 30
- ATT&CK Visualizer 30
- API & Under the Hood 30

Dependencies & Library Changes **31**

Maintenance Releases Changelog **32**
- 2024-08-29 7.6.3-M0829R [Latest] 32
  - Bug Fixes 32
- 2024-08-21 7.6.3 32
  - Bug Fixes 32
- 2024-08-09 7.6.2-M0809R 33
  - Bug Fixes 33

2024-07-24 7.6.2 33
Improvements 33
Bug Fixes 33
2024-06-26 7.6.1 34
Improvements 34
Bug Fixes 34
CAL Updates **35**
2024-07-15 CAL 3.8 [Latest] 35
Feature Update: MITRE ATT&CK 15.1 Framework 35
Improvements 35

New Features and Functionality

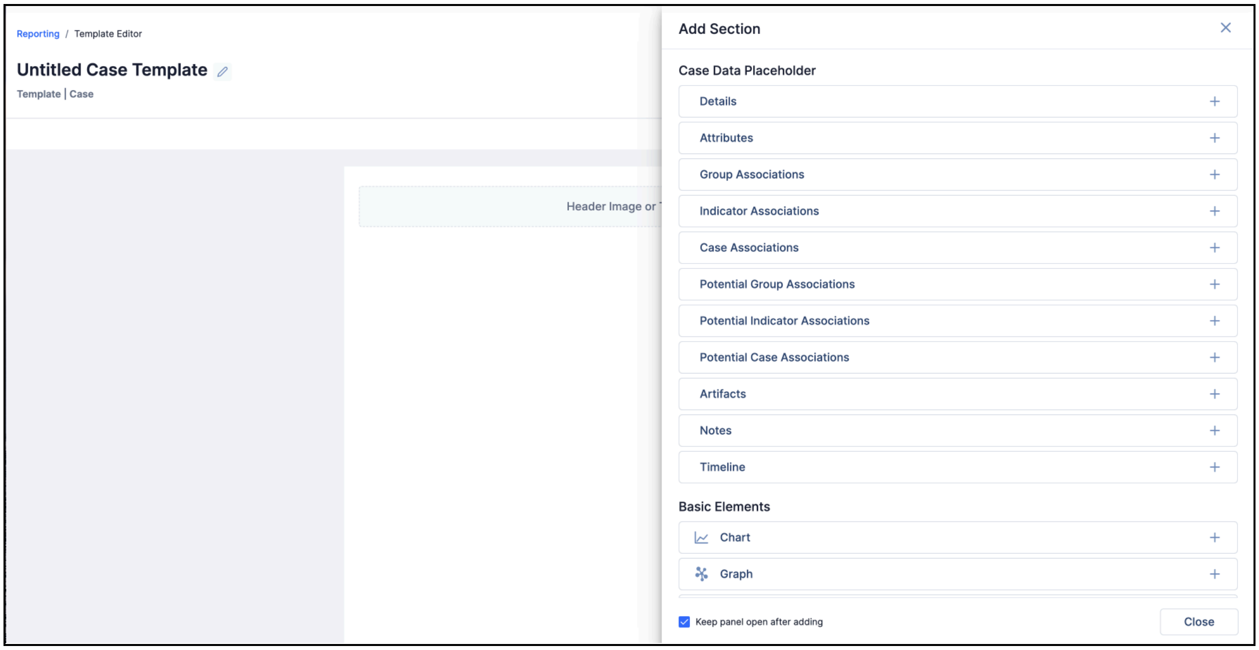
Reporting: Generic and Case Templates

ThreatConnect 7.6 continues to streamline and enhance report creation by introducing Case and generic report templates. These additions build on the foundation provided by Group report templates in ThreatConnect 7.5, further empowering you to efficiently generate reports tailored to your specific needs, whether you're documenting threat intelligence, incident response activities, or other security-related information. In particular, generic templates provide you with the ability to craft executive or strategic report templates that are designed to convey top-level insights and recommendations to stakeholders within your organization.

Case Templates

To create a Case report template, navigate to the **Reporting** screen, click **+ Create Template** at the top right, and select **Case** from the dropdown. The **Template Editor** will open and display a blank report template for Cases, including placeholder **Report Header** and **Report Footer** sections. From here, you can add sections from the following three categories:

- **Case Data Placeholder**: This category contains Case details, Attributes, associations, potential associations, Artifacts, Notes and Timeline information.
- **Basic Elements**: This category contains charts, graphs, images, tables, and text blocks.
- **Layout Elements**: This category contains headers, footers, page dividers, and page breaks.

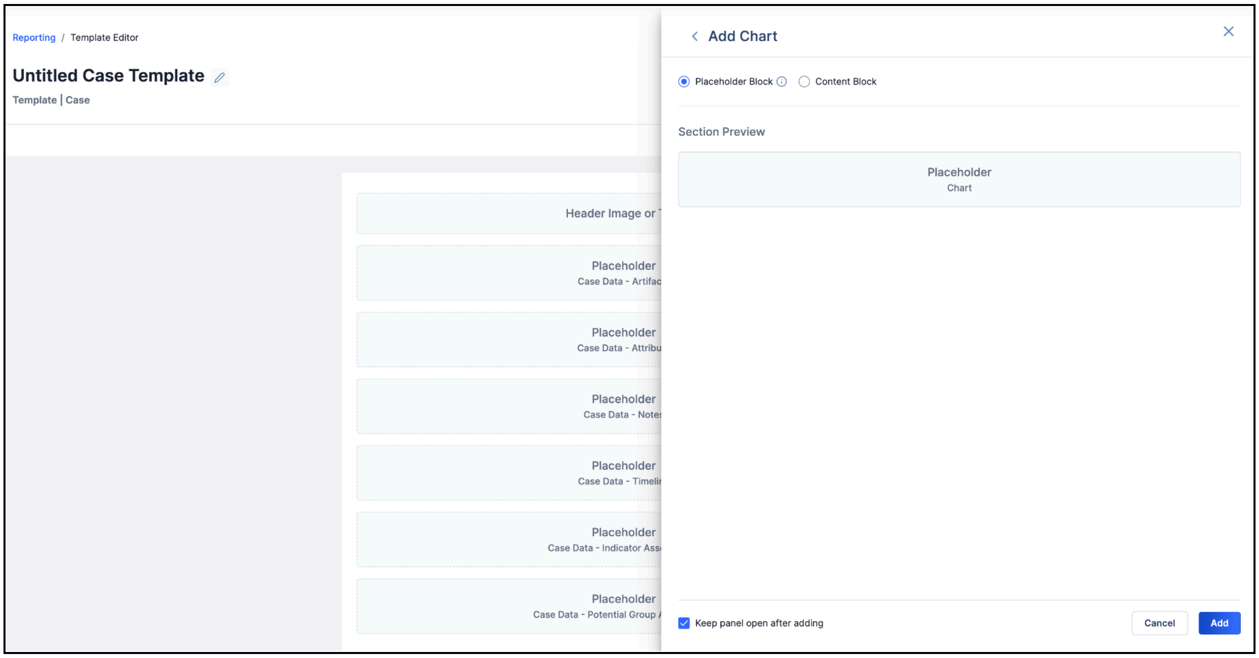


*Add content to your Case report template from the **Add Section** drawer*

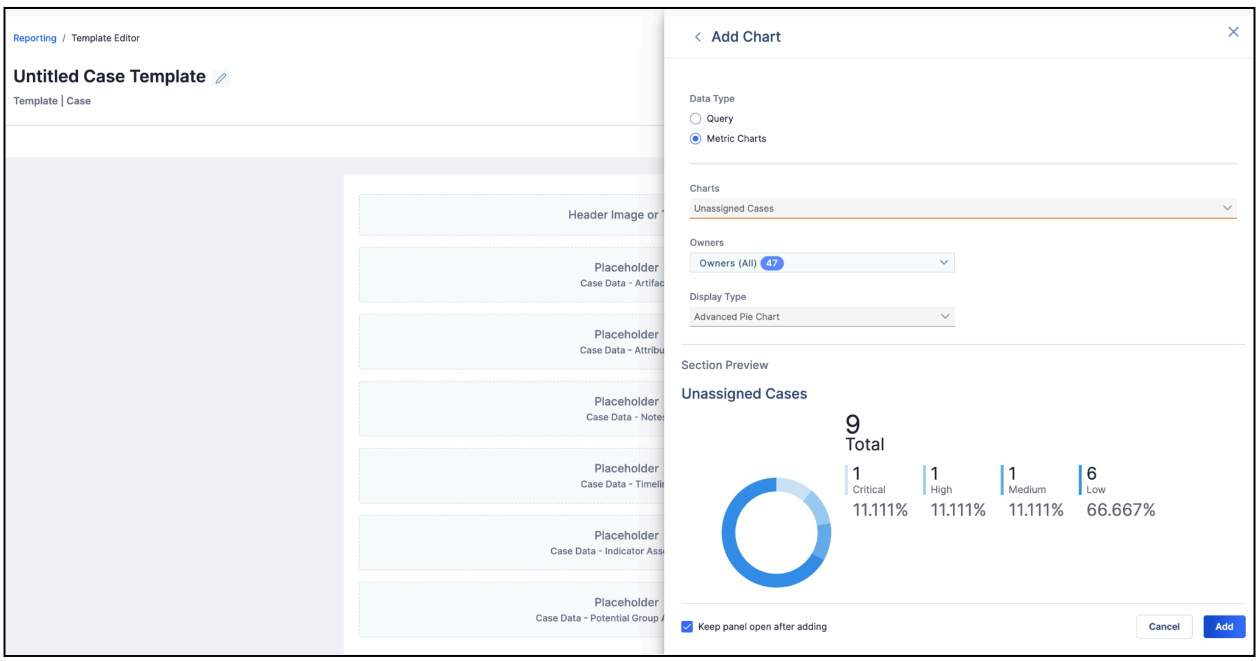
Each item in the **Case Data Placeholder** category enables you to add a placeholder block to the report template. When a user creates a report from the template for a Case, the information specific to that Case will be automatically inserted into the report, with the exception of the **Attributes** and **Notes** placeholder blocks, which the user will need to edit to select a specific Attribute and Note, respectively, to add to the report.

Each item in the **Basic Elements** category provides two ways to add a section to a report template: **Placeholder Block** and **Content Block**. Placeholder blocks indicate where the user should configure specific elements—query and metric charts, saved graphs from Threat Graph, images, query-based and preset tables, and text blocks—when generating a report from the template. Content blocks populate pre-configured data for the same types of elements directly into the report.

Finally, each item in the **Layout Elements** category adds a formatting feature to a report template.



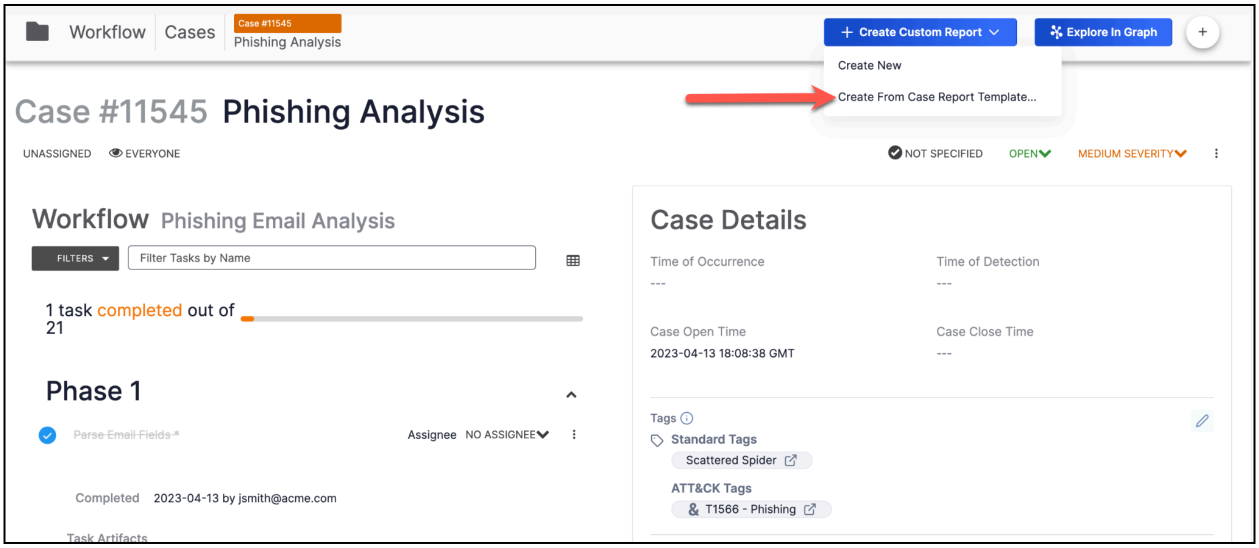
Add placeholder blocks to direct users to add data into Case reports



Add content blocks to insert predefined data in a Case report template

After you have finished creating your Case report template, click the **Save Template** button to save it. All saved templates can be accessed on the **Templates** tab on the **Reporting** screen.

Once you have saved your Case report template, users in your Organization can utilize it to generate a report for a Case by navigating to the Case, clicking **+ Create Custom Report**, selecting **Create From Case Report Template...**, and choosing the template to use to create the report.



Create a report for a Case from a Case report template

When creating a report from a template containing placeholders, the placeholders act as prompts within the report layout, indicating where users should insert specific information. As users fill in these placeholders with relevant data, the report takes form, ensuring that all elements are integrated into the report.

When creating a report from a template containing content blocks, the configured data will automatically populate in those sections of the report. Users also have the flexibility to customize these content blocks, adding or modifying query or predefined elements as needed to tailor the report to their specific requirements.

Users also have the flexibility to add extra elements as necessary to finalize the report. Once completed, these reports can be saved, published, or shared via email or as exported PDF or HTML files.

Details #11545 Phishing Analysis

State	Open
Resolution	Not Specified
Severity	MEDIUM
Time of Occurrence	
Time of Detection	
Case Open Time	2023-04-13 18:08:38 GMT
Case Close Time	
Standard Tags	Scattered Spider
ATT&CK Tags	Phishing
Description	https://resources[.]infosecinstitute[.]com/the-phishing-response-playbook/ https://www[.]incidentresponse[.]com/playbooks/phishing Phase 1 - Initial Data Ingestion Phase 2 - Investigation/Analysis Phase 3 - Containment/Eradication Phase 4 - Recovery Phase 5 - Threat Intelligence Deep Dive Phase 6 - Retrospective

Course of Action Taken #11545 Phishing Analysis

Attribute Source	
Date Added	05-15-2024
Last Modified	05-15-2024

Value

1)Sender Information: The sender's email address is examined for any irregularities or signs of spoofing. This includes checking for misspellings, unusual domain names, or discrepancies between the sender's name and email address.
2)The content of the email is scrutinized for indicators of phishing. This involves looking for common phishing tactics such as urgent requests for personal information, unsolicited attachments or links, and generic greetings.

Group Associations #11545 Phishing Analysis

1-4 of 4 Part 1 of 2

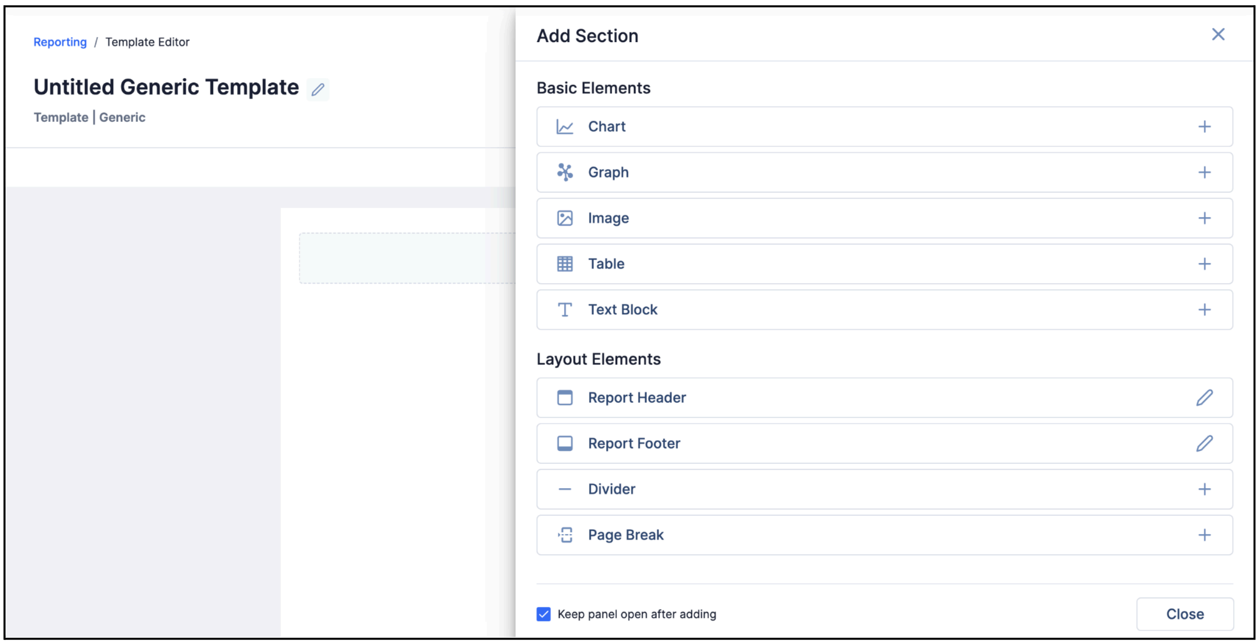
Type	Name	Score	Status	Date Added	Last Modified
Incident	20130325A: DPHK Driveby			03-25-2013	05-15-2024
Incident	20130202A: tcoga.net Watering Hole			02-02-2013	05-15-2024

Report generated from a Case template

Generic Templates

To create a generic report template, navigate to the **Reporting** screen, click **+ Create Template** at the top right, and select **Generic** from the dropdown. The **Template Editor** will open and display a blank report template, including placeholder **Report Header** and **Report Footer** sections. From here, you can add sections from the following two categories:

- **Basic Elements**: This category contains charts, graphs, images, tables, and text blocks.
- **Layout Elements**: This category contains headers, footers, page dividers, and page breaks.

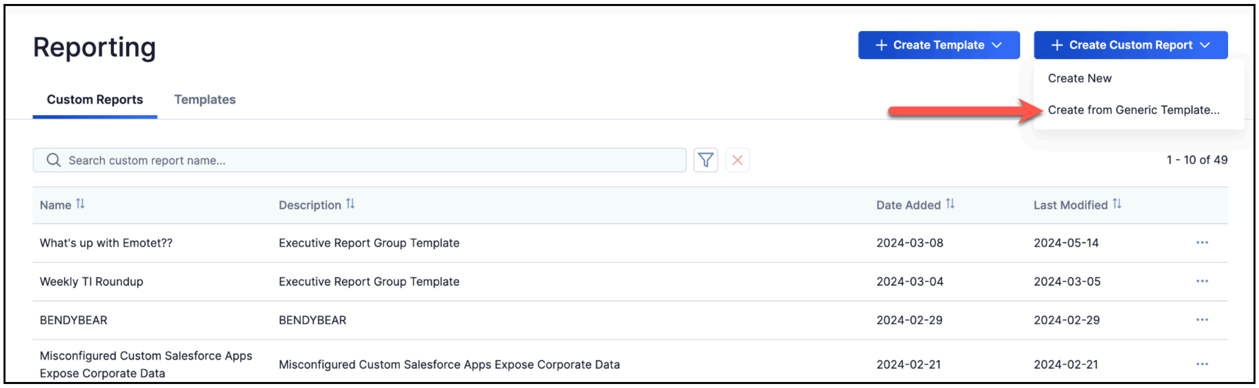


*Add content to your generic report template from the **Add Section** drawer*

As with Group and Case report templates, you can add **Placeholder Block** and **Content Block** sections for the items in the **Basic Elements** category and formatting features for the items in the **Layout Elements** category. Because the template is generic, you cannot add Group- or Case-specific data, but you can always add this information when you build a report from the template.

After you have finished creating your report template, click the **Save Template** button to save it. All saved templates can be accessed on the **Templates** tab on the **Reporting** screen.

Once you have saved your generic report template, users in your Organization can utilize it to generate a report by navigating to the **Reporting** screen, clicking **+ Create Custom Report** at the top right, selecting **Create from Generic Template…**, and choosing the template to use to create the report.



Create a report from a generic report template

Generic report templates can be used to generate executive threat intelligence reports and other types of publications, providing relevant context for emerging threats, trends, and industry-specific attack vectors.

Tip: Format text blocks to create visually appealing reports that make it easy for readers to identify the information they need the most.

ThreatConnect.

Executive Report:

Business Critical Processes Targeted by Threat Actors

Executive Summary

- Overview: Emotet is a versatile and sophisticated malware strain known for its ability to deliver secondary payloads, such as ransomware and information stealers.
- Risks: Emotet spreads through malicious email attachments, exploiting vulnerabilities in systems to compromise networks and steal sensitive data.
- Mitigation: Implement robust email security measures, conduct regular employee training on phishing awareness, and deploy advanced threat detection solutions

Keypoints

1. Top Five Malware Threats: The report identifies the top five malware threats currently affecting the organization's cybersecurity posture, including Emotet, TrickBot, Ryuk, WannaCry, and NotPetya.
2. Overview of Each Threat: For each malware threat, the report provides a brief overview, highlighting key characteristics, propagation methods, and potential risks to the organization.
3. Risks Posed by Each Threat: The report outlines the specific risks posed by each malware threat, such as data breaches, financial losses, operational disruptions, and reputational damage.
4. Mitigation Strategies: For each malware threat, the report suggests appropriate mitigation strategies to strengthen the organization's defenses and reduce the likelihood of successful cyberattacks. These strategies include implementing security controls, conducting employee training, developing incident response plans, and maintaining regular backups.

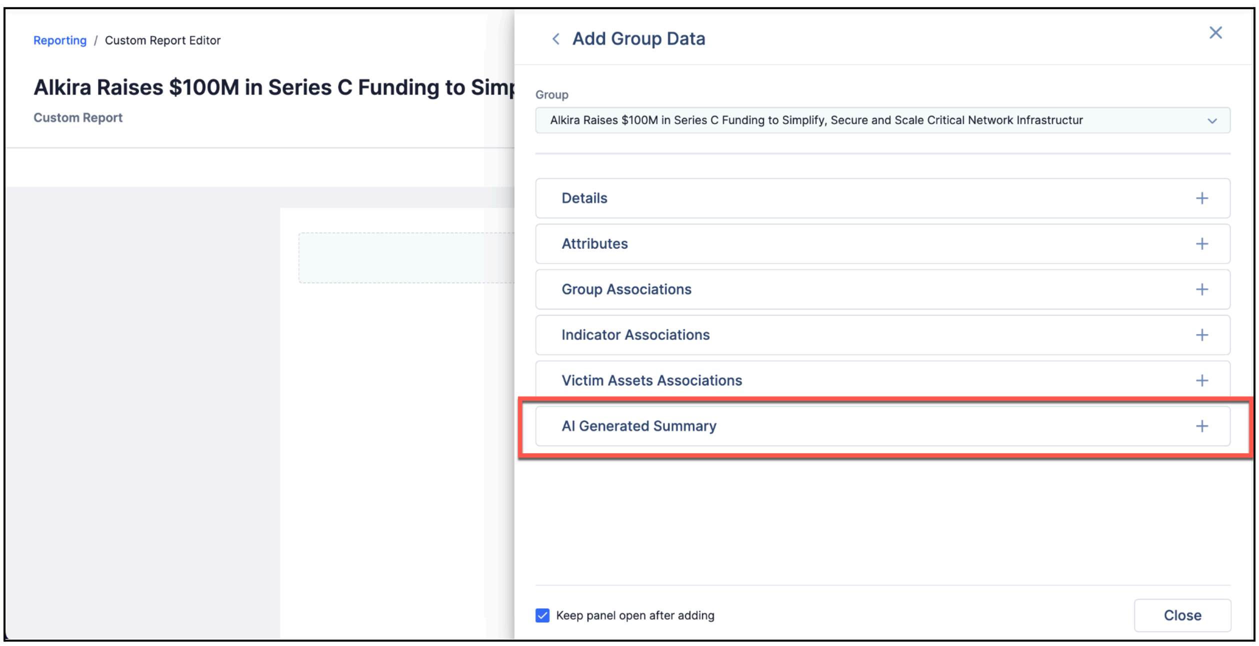
Format text blocks in reports and generic templates to create visually appealing publications

Reporting: Enhancements

ThreatConnect 7.6 delivers two other powerful additions to the reporting feature: CAL™ Automated Threat Library (ATL) AI-generated summaries and ATT&CK® Tags.

CAL ATL AI-Generated Summaries in Reports

We introduced AI-generated summaries for Report objects in the **CAL Automated Threat Library** Source in ThreatConnect 7.4, and now we expand their integration into our reporting feature. When adding data for a CAL ATL Report Group to a report, you can now select the **AI Generated Summary** option to insert the contents of the **AI Insights** section from the Report's **Details** screen into the report. This material will provide the report's readers with succinct, high-value information that they can use to make quick decisions and take impactful actions.



*Add **AI Generated Summary** from the **Group Data** section for CAL ATL Reports*

ThreatConnect.

Details

Alkira Raises $100M in Series C Funding to Simplify, Secure and Scale Critical Network Infrastructur

Type	Report
Owner	CAL Automated Threat Library
Security Labels	No security labels
Date Added	2024-05-16 11:10:06 GMT
Last Modified	2024-05-16 11:10:06 GMT
Standard Tags	Blog: Dark Reading; NAICS: 51 - Information; NAICS: 518 - Computing Infrastructure Providers, Data Processing, Web Hosting, Related Services; NAICS: 52 - Finance And Insurance; NAICS: 523 - Securities, Commodity Contracts, Other Financial Investments And Related Activities; NAICS: 512 - Motion Picture And Sound Recording Industries
ATT&CK Tags	Software Discovery: Security Software Discovery; Phishing

AI Generated Summary

Alkira Raises $100M in Series C Funding to Simplify, Secure and Scale Critical Network Infrastructur

- Alkira, a network infrastructure as a service (NaaS) provider, has raised $100 million in Series C funding to simplify, secure, and scale critical network infrastructure.
- The funding round was led by Tiger Global Management, with additional investment from Dallas Venture Capital, Geodesic Capital, and NextEquity Partners.
- The company's total funding raised to date is now $176 million.
- Alkira's platform provides on-demand network infrastructure, integrated security, and networking services available globally.
- The platform allows businesses to seamlessly deploy, manage, and optimize their entire network infrastructure to prioritize efficiency, agility, security, and scalability.
- Alkira's differentiators include its ability to securely connect any cloud, any on-prem location, any remote user or app to any other point of presence, and its platform to build global, secure networks in minutes.

Alkira, a network infrastructure as a service (NaaS) provider, has raised $100 million in Series C funding to simplify, secure, and scale critical network infrastructure. The funding round was led by Tiger Global Management, with additional investment from Dallas Venture Capital, Geodesic Capital, and NextEquity Partners. Alkira's platform provides on-demand network infrastructure, integrated security, and networking services available globally, allowing businesses to seamlessly deploy, manage, and optimize their entire network infrastructure to prioritize efficiency, agility, security, and scalability. The company's differentiators include its ability to securely connect any cloud, any on-prem location, any remote user or app to any other point of presence, and its platform to build global, secure networks in minutes.

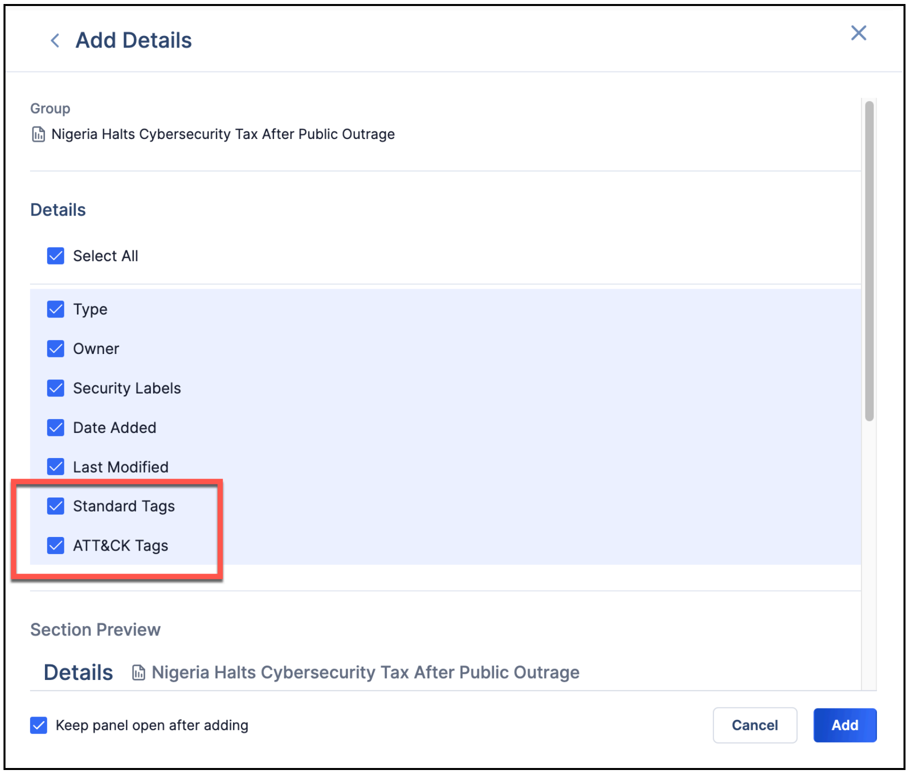
The AI-generated summary adds impactful details about CAL ATL Reports to your reports

ATT&CK Tags in Reports

In ThreatConnect 7.6, we separate ATT&CK Tags from standard Tags for Group and Case data in reports, enabling you to ensure that your reports' readers have a holistic view of threat intelligence and Workflow data so they can make more informed decisions and develop more targeted response strategies.

View standard Tags and ATT&CK Tags separately in reports

In previous versions of ThreatConnect, standard Tags and ATT&CK Tags were combined in a single **Tags** option in the **Details** section for Group Data and Case Data in the **Report Editor**. Now, you'll find them as two separate options: **Standard Tags** and **ATT&CK Tags**. Add one or both according to your report's requirements.



Add standard and ATT&CK Tags separately in reports

Enhanced Search

We're thrilled to introduce the beta version of Enhanced Search in ThreatConnect 7.6, aimed at making searching simpler and more effective. This beta launch marks the beginning of an exciting journey towards enhancing your search experience and laying the groundwork for future improvements.

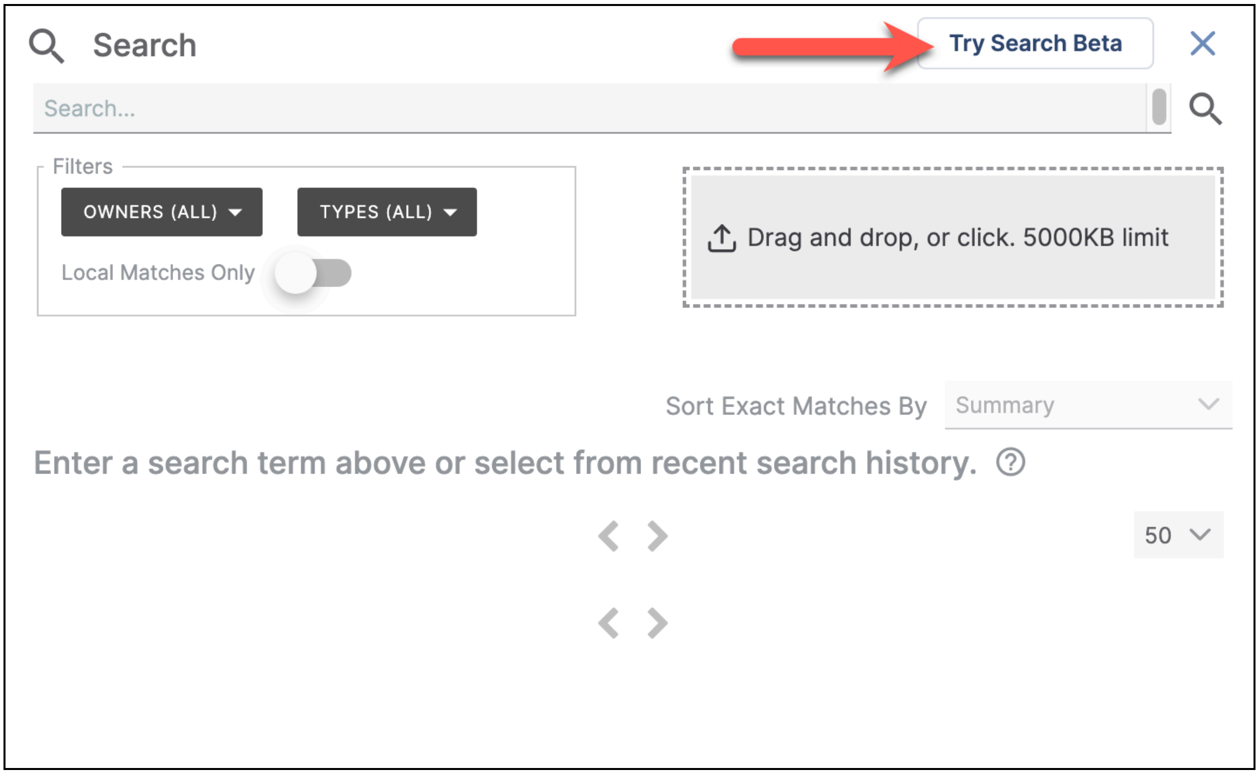
First, this new version of search unveils a clean, new look! Our updated search interface allows you to quickly search the data in all of your ThreatConnect owners and find exactly what you need. To do so, it scans for the keywords you enter across all object types, including any Attributes, Tags, Artifacts, Victim Assets, file contents, and signature contents associated with those objects. You can search for one keyword, multiple keywords, or even a specific phrase.

Additionally, you have the flexibility to filter search results by object type (Cases, Indicators, Groups, Tags, and Victims) and then refine your search further by specifying owners, Group types, Indicator types, and dates. This precision helps you focus on exactly what you need. The new search also lets you sort the results, helping you prioritize what's important, and allows you to choose previously searched keywords from your search history.

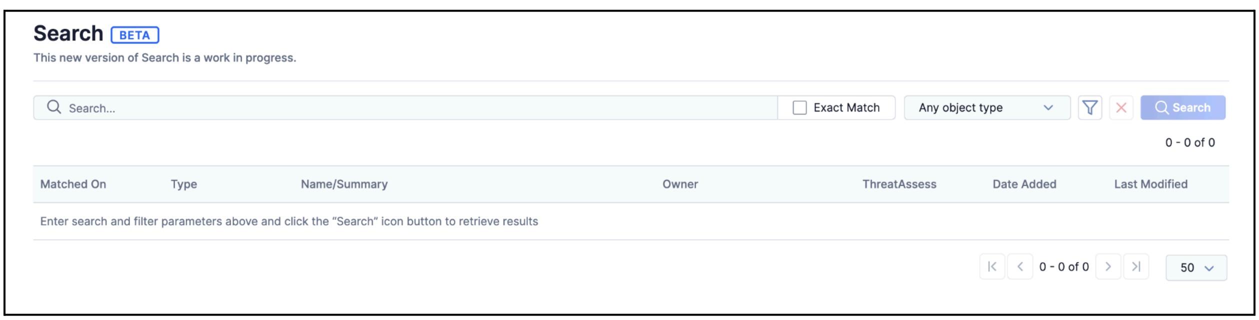
Let's take a look at how it works.

Step 1: Access the New Search Screen

Start by clicking **Search** on the top navigation bar. Then click **Try Search Beta** at the top right of the **Search** drawer to open the new **Search** screen.



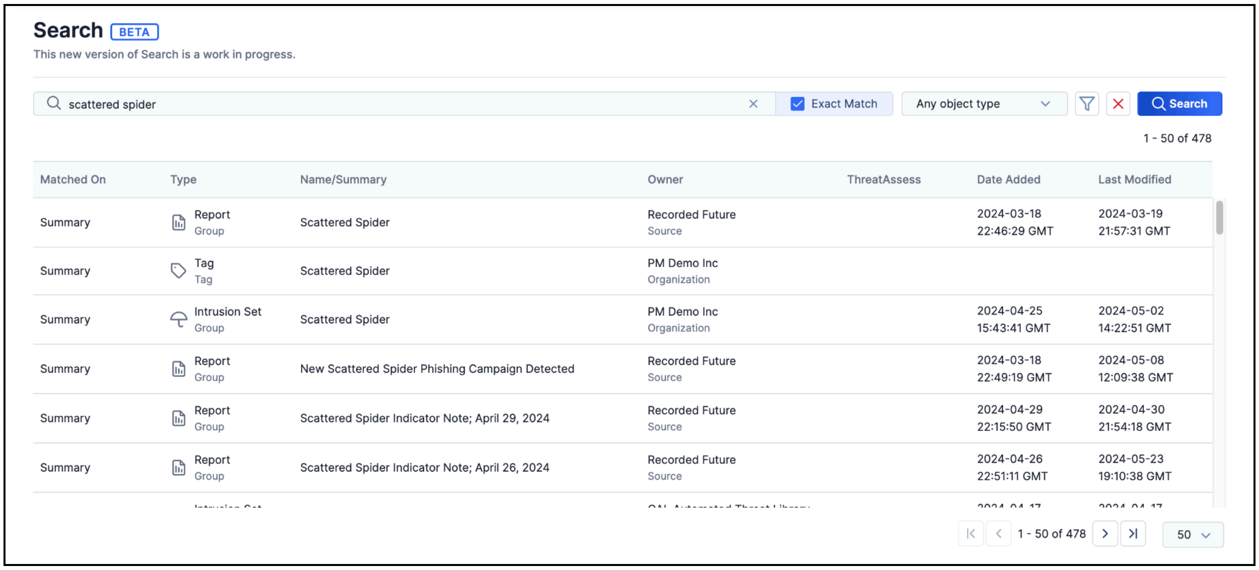
*Access the new **Search** screen from the **Search** drawer*



*The new **Search** screen provides a clean interface with flexible filtering and sorting*

Step 2: Enter Keywords

Enter your search keywords into the search bar. Select the **Exact Match** checkbox to the right of the search bar if you want to search for an exact phrase. Then press **Enter** on your keyboard or click **Search** to initiate the search and view the results, which are displayed in a structured and informative manner.



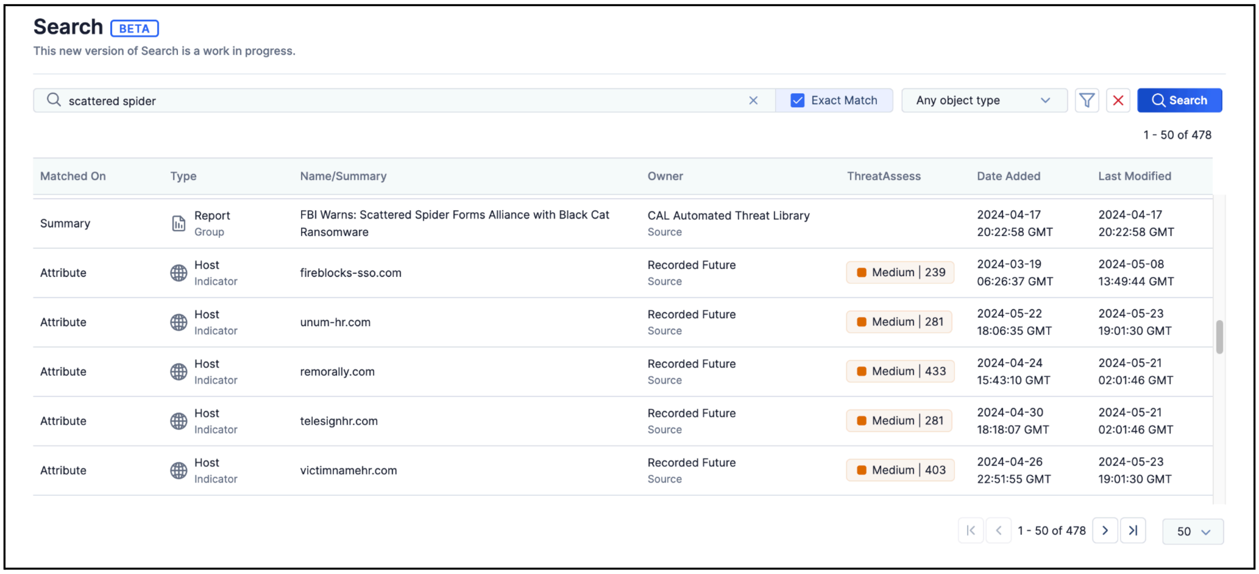
Search results for "scattered spider" (exact match)

Each row in the results table represents an object returned by the search, with the type (Case, Group, Indicator, Tag, or Victim) and subtype (Group type or Indicator type for Groups and Indicators, respectively) of the object provided in the **Type** column and the object's name provided in the **Name/Summary** column. The **Matched On** column provides the data type on which the query matched, such as the object's summary, the value of one of the object's Attributes, the name of a Tag on the object, the contents of the signature file uploaded to an object that is a Signature Group, the contents of the file uploaded to an object that is a Document or Report Group, the description of a Task for an object that is a Workflow Case, or the summary of a Victim Asset for an object that is a Victim. The table also lists each result's owner, ThreatAssess score (for results that are Indicators), the date the result was added to the owner, and the date that the result was last modified.

The search results are ranked by relevance, with objects whose summaries match the query being displayed at the top, followed by objects with matching metadata (e.g., an Attribute, a Tag, signature file contents, a Task description in a Case). This order enables you to quickly identify and focus on the most important information returned by the search, but you can also sort your search results by any of the table columns except for the **Matched On** and **ThreatAssess** columns.

In our example search, an exact match for "scattered spider" was found in the summary for multiple objects across multiple owners, including Report Groups in a Source and an Intrusion Set and Tag in the user's Organization.

In addition, results further down in the table show “scattered spider” in Attributes of multiple Host Indicators.



Matched On	Type	Name/Summary	Owner	ThreatAssess	Date Added	Last Modified
Summary	Report Group	FBI Warns: Scattered Spider Forms Alliance with Black Cat Ransomware	CAL Automated Threat Library Source		2024-04-17 20:22:58 GMT	2024-04-17 20:22:58 GMT
Attribute	Host Indicator	fireblocks-sso.com	Recorded Future Source	Medium | 239	2024-03-19 06:26:37 GMT	2024-05-08 13:49:44 GMT
Attribute	Host Indicator	unum-hr.com	Recorded Future Source	Medium | 281	2024-05-22 18:06:35 GMT	2024-05-23 19:01:30 GMT
Attribute	Host Indicator	remorally.com	Recorded Future Source	Medium | 433	2024-04-24 15:43:10 GMT	2024-05-21 02:01:46 GMT
Attribute	Host Indicator	telesignhr.com	Recorded Future Source	Medium | 281	2024-04-30 18:18:07 GMT	2024-05-21 02:01:46 GMT
Attribute	Host Indicator	victimnamehr.com	Recorded Future Source	Medium | 403	2024-04-26 22:51:55 GMT	2024-05-23 19:01:30 GMT

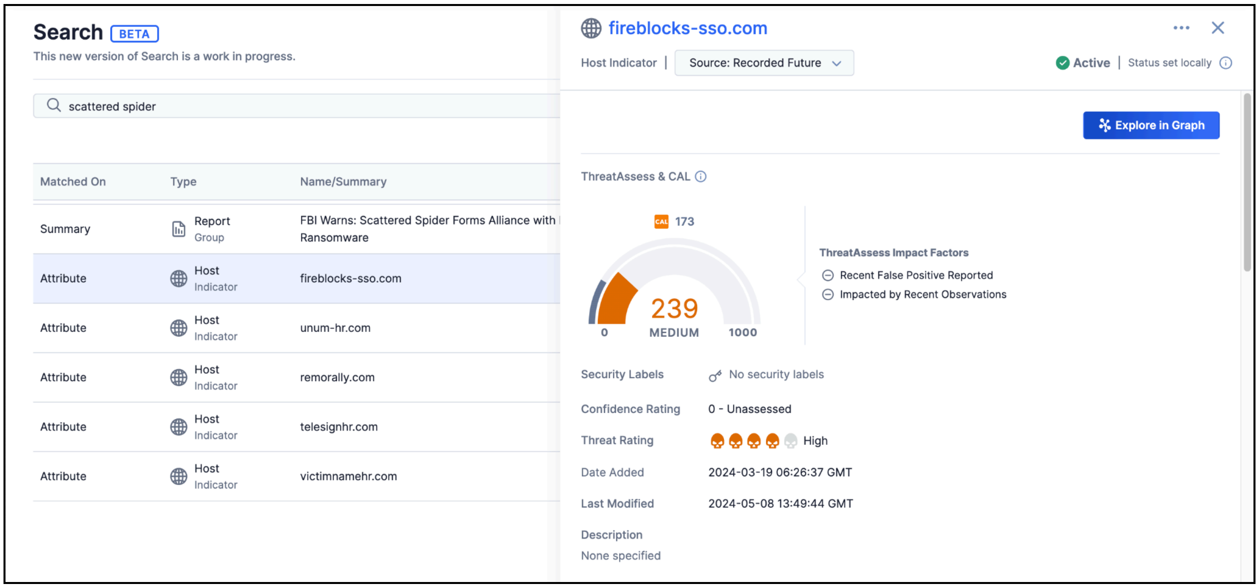
Search results showing matched-on Attributes of Host Indicators

The results provided by our Enhanced Search allow you to see where and how your search term is referenced across different data types in all of your ThreatConnect owners, offering a more interconnected view of potential threats.

The new interface also saves your recent searches. When you click the search bar, you will see a list of the search terms you used most recently. You can select any of them and then click **Search** to revisit your past search and view the results. Terms for which the **Exact Match** checkbox was selected are displayed in double quotes. You can select these terms without re-selecting the **Exact Match** checkbox.

Viewing Search Result Details

To better understand your search results, you can click any item in the results table to open its **Details** drawer (which, for Indicators, has a brand-new interface that provides more information, context, and functionality; see the [“Indicator Details Drawer” section](#) for more on this improved feature!).

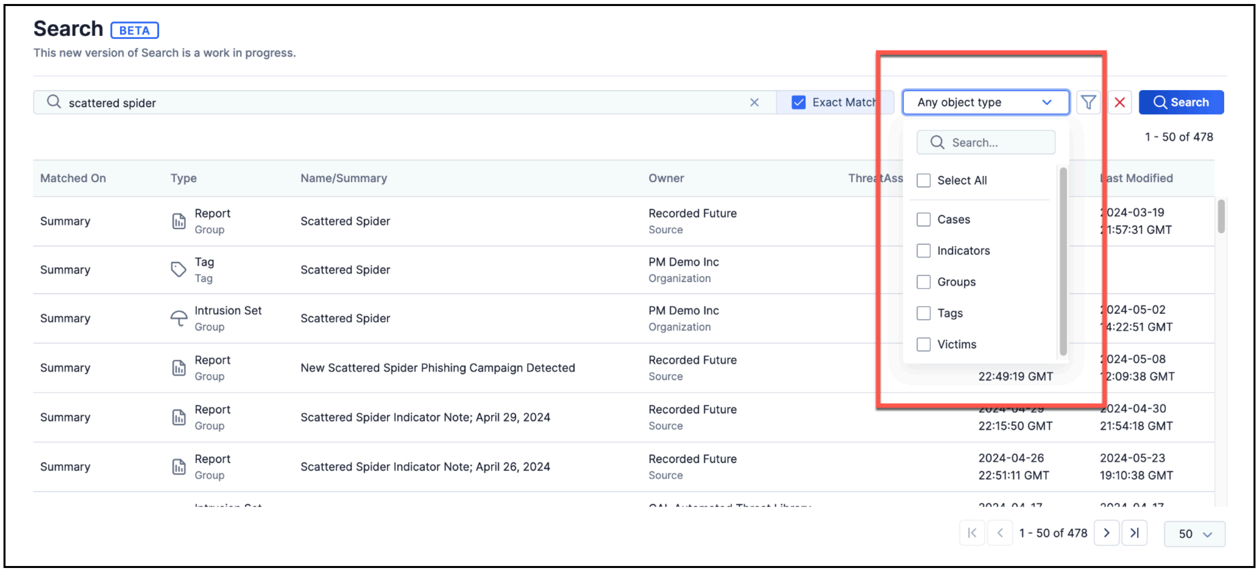


*Click on a search result to view its **Details** drawer*

The **Details** drawer in Enhanced Search allows you to view detailed information on the object without leaving the main search results page, saving time, reducing the cognitive load of switching contexts, and enhancing the overall relevance and value of your results.

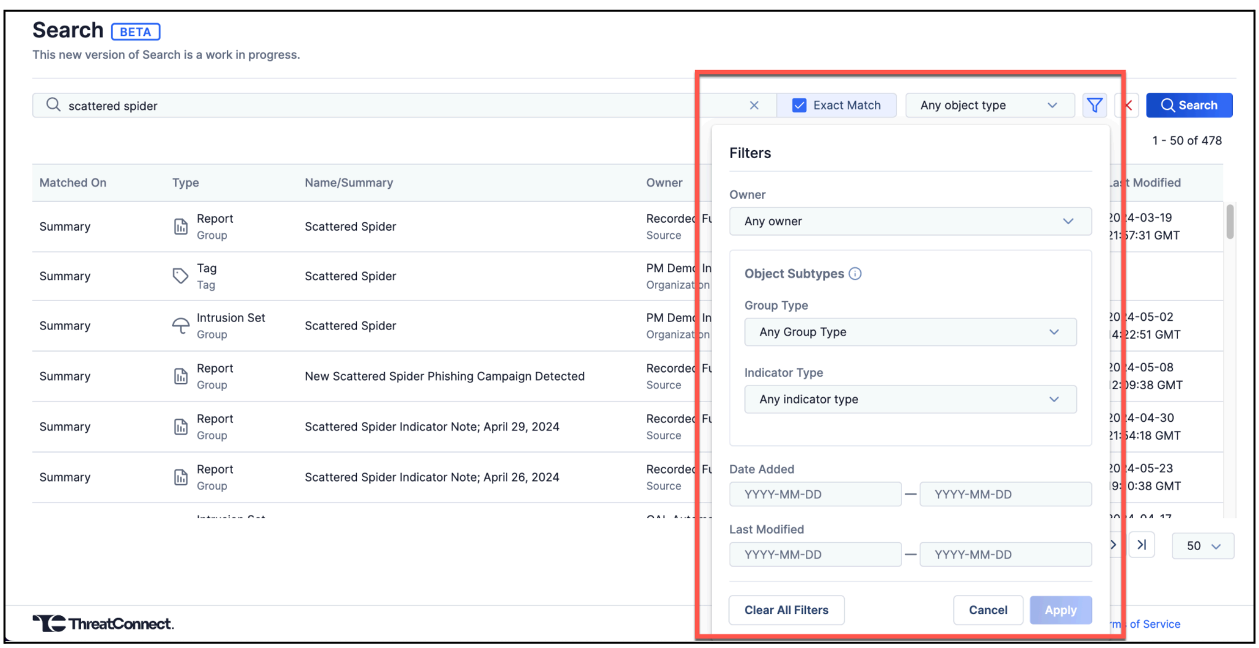
Filtering Search Results

You can filter your search results to narrow them down to exactly what you are looking for. First, use the dropdown to the right of the **Exact Match** checkbox to filter your results by object type. After making your selections, run your search again to apply the filters.



Filter your search results by object type

You can further refine your search results by using the **Filters** menu to filter by owner, object subtype (for Indicators and Groups only), creation date, and last modified date. After making your selections, click **Apply** in the **Filters** menu to apply these filters to your search results.



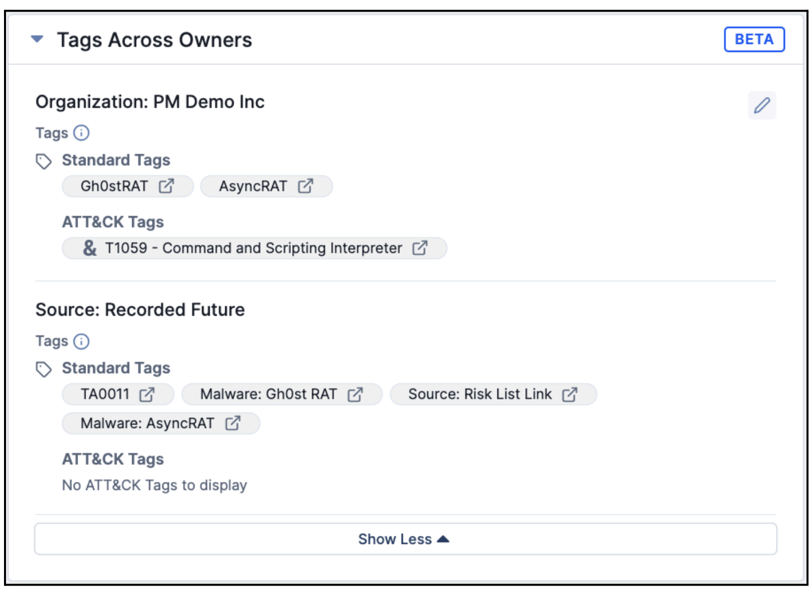
*The **Filters** menu provides more options for narrowing down your search results*

Clear Context

“Clear Context” is the name of a strategic initiative ThreatConnect is undertaking in 2024–2025. The goal is to provide our users with easily understandable and actionable context around a Group or Indicator. Each feature in this initiative focuses on improving a specific area of the platform to make it easier to understand the available information and make faster decisions. In ThreatConnect 7.6, our Clear Context initiative brings you two impactful features for Indicators: **Tags Across Owners** and the new Indicator **Details** drawer.

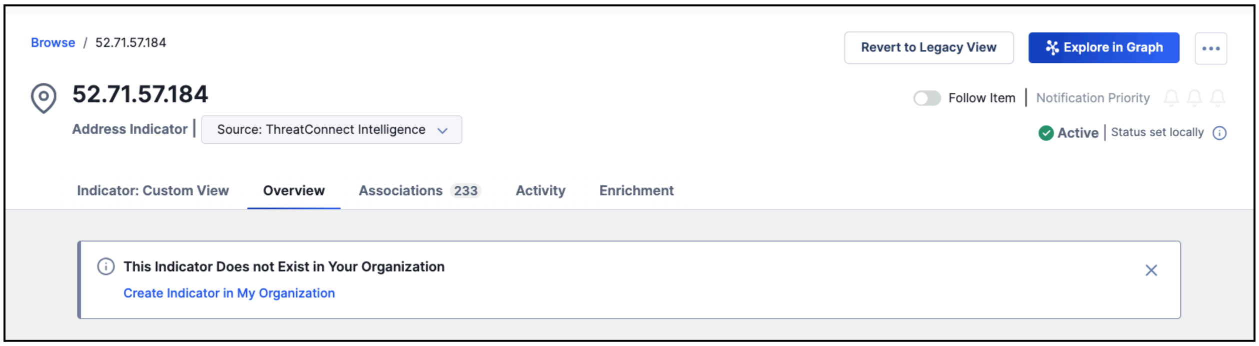
Tags Across Owners

The first feature in the Clear Context initiative is **Tags Across Owners**. This capability is currently in beta and can be turned on or off by a System Administrator in **System Settings**. It is turned off by default. When the feature is turned on, the **Tags Across Owners** card will be available on the **Details** screen and **Details** drawer for Indicators. This card displays all Tags that exist on that Indicator in all of the Indicator's owners to which you have access. The **Tags Across Owners** card enables you to quickly contextualize an Indicator without having to open the **Details** screen or drawer for the object in each owner.



View Tags on an Indicator across all owners in which that Indicator exists

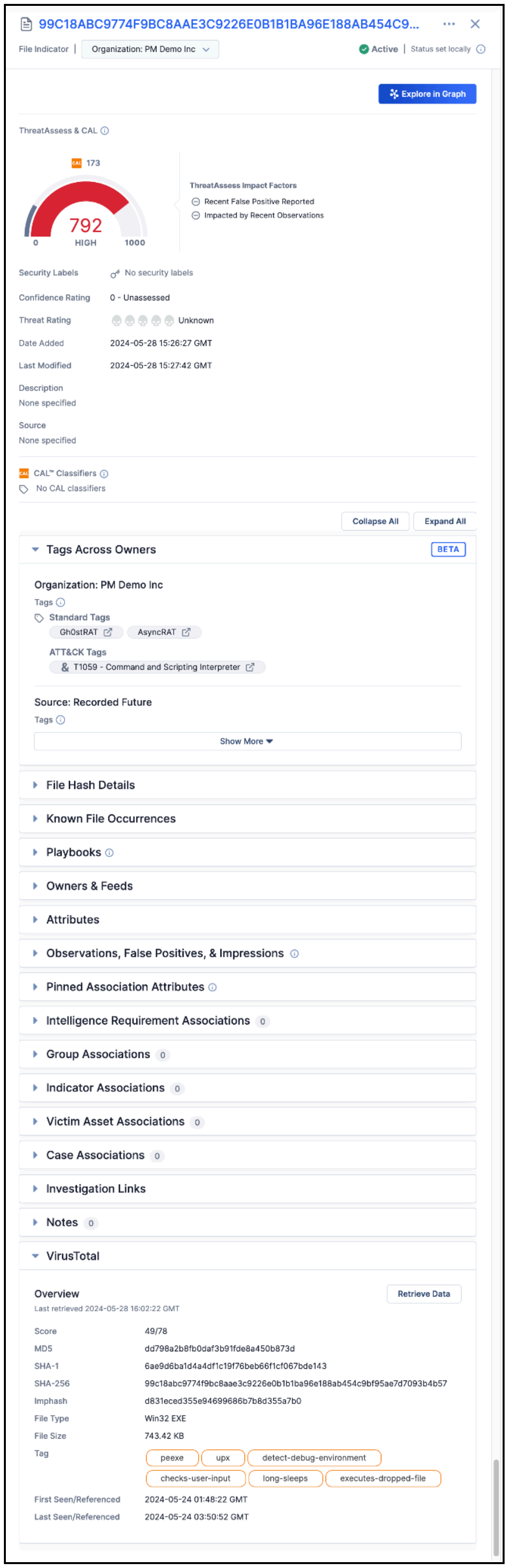
In addition, when you view the **Details** screen for an Indicator that does not exist in your Organization, you will see a banner at the top of the **Overview** and **Indicator: Custom View** tabs that will provide an option to quickly and easily add the Indicator to your Organization with a single click. This functionality enables you to create a copy of the Indicator and add Tags to it without having to worry about the original owner overwriting the changes.



Add an Indicator to your Organization with a single click

Indicator Details Drawer

Our other Clear Context feature for version 7.6 of ThreatConnect is an updated Indicator **Details** drawer intended to streamline your experience and make it easier for you to get the context you need for an Indicator when and where you need it. The new drawer displays the **Tags Across Owners** card, if enabled, and includes cards for features such as enrichment services, UserAction Playbooks, and Notes, all of which were unavailable in the previous version of the Indicator **Details** drawer.



*View more information, including **Tags Across Owners** and data from enrichment services, in the updated **Details** drawer*

Improvements

Threat Intelligence

- You can now import and export custom views for the **Details** screen. These options are available via the ··· menu at the top right of the **Manage View** drawer. When you export a custom view, a **.tccv** file will be downloaded onto your local drive and can be used for future imports.

  > **Warning**: Do not modify the contents of a **.tccv** file. Otherwise, users may encounter errors when trying to import the file into ThreatConnect.

- The maximum number of keywords you can use when defining a query for an Intelligence Requirement (IR) is now determined by your System Administrator, with an upper limit of 300. When you create or modify the keywords for an IR, the interface will display the maximum number of keywords allowed on your instance and will not allow you to exceed the limit.
- A new field for Event Groups was added: **Event Type**. This field, which can be blank or have a value of **Alert** or **Campaign**, is available on the **Details** card of the **Overview** or **Group: Custom View** tab of the **Details** screen. It is also queryable by ThreatConnect Query Language (TQL).
- The new **Details** screen now displays a "CAL Status Lock Enabled" message at the top right, next to the Indicator Status, when the CAL Status Lock has been turned on for the Indicator.
- The user interface for adding a Case to the **Case Associations** card on the **Associations** tab of an Indicator's or Group's **Details** screen has been updated. When you click **Add Association +** on the **Case Associations** card, you are now given the option to add an existing Case or a new Case. Each option takes you to a more streamlined window to perform the respective function.
- HTML and Markdown are now rendered consistently in Attributes.
- The following changes were made to the process of contributing a Group in an Organization to a Community or Source:
    - Asynchronous processing was added to enable the contribute operation to function partially as a background process, increase the speed of the operation, and prevent timeout errors caused by large numbers of Groups in a single contribute operation from occurring. As such, once you click **SAVE** in the

Contribute to Community/Source window, each Group and associated Group will be mapped to existing target Groups and new Groups and then added to a queue for further enrichment. The queue will copy metadata and associated Indicators in the background, enabling you to navigate elsewhere in ThreatConnect instead of waiting for the entire operation to complete.
    - An issue preventing Indicator-to-Indicator associations and File Actions from being included in the contribute operation was fixed.
    - “Loading” windows are now displayed during the time it takes for the system to process each step in the **Contribute to Community/Source** window.
    - New columns were added to the table on the **Sharing** tab to provide detailed information on the start and end times and status (**Processing**, **Complete**, or **Error**) of each contribute operation, as well as error messages when applicable.
    - A warning message will now be displayed on the **Save** step of the **Contribute to Community/Source** window to inform you when you attempt to copy more than the system's recommended maximum number of associated Groups (300).

Reporting

- You can now create a report for a Group from a Group report template via a Group's **Details** drawer.
- When you are adding or editing a chart in a report or report template or opening a report or report template that contains charts, a “Loading” window will be displayed during the time it takes the system to generate the chart. If the chart times out, a message to that effect will be displayed. If you experience a timeout, it is recommended that you limit the number of owners for the data in the chart or increase the value of the **Custom TQL Timeout** field on the **Overview** tab of the **My Profile** screen.
- The following improvements were made to tables in reports:
    - Tables now always display the full **Name** field without truncation.
    - Tables now support page breaks. Group and Case association tables and **Basic Element** tables have a limit of 80 rows. Tables for Case Notes and Group and Case Attributes do not have row limits.

System Settings

- The following new system settings were added:
    - **copyRecalculateVotesEnabled**: This setting determines whether to perform Indicator vote calculations when copying Groups to a Community (i.e., calculate the average Threat and Confidence Ratings for Indicators associated to the Group being copied). If you have a large dataset on your instance and are concerned about performance during data copy operations, it is recommended to turn this setting off.
    - **intelligenceRequirementKeywordLimit**: This setting determines the maximum number of keywords allowed across all **Keyword Tracking** sections of an IR.
    - **multiSourceViewEnabled**: This setting turns on or off support for viewing unified information across owners (i.e., viewing the Tags applied to an Indicator across all of its owners on the **Tags Across Owners** card on the Indicator's **Details** screen and drawer).
    - **searchRefreshQueryLimit**: This setting determines the LIMIT clause on all queries run by the **TC - Search Refresh** App.
    - **searchRefreshThreadPool**: This setting determines the number of threads the **TC - Search Refresh App** can run concurrently.
    - **searchRefreshRequestLimit**: This setting determines the number of documents the **TC - Search Refresh App** can send to OpenSearch® in one bulk request.

Workflow

- Performance improvements were made to Artifact lookups.

API & Under the Hood

- When creating or updating an Intelligence Requirement (IR) with the `/v3/intelRequirements` API endpoint, the `keywords` field will enforce the keyword limit configured in system settings. (The default keyword limit for IRs is 300.)
- The following endpoints were added to the v3 API:
    - `/v3/jobs`: Retrieves details about Jobs in the API user's Organization.
    - `/v3/job/executions`: Retrieves details about Job executions in the API user's Organization.

- `/v3/playbooks`: Retrieves details about Playbooks in the API user's Organization.
- `/v3/playbook/executions`: Retrieves details about Playbook executions in the API user's Organization.

Bug Fixes

Threat Intelligence

- Objects that match on an included IR keyword in one field and an excluded keyword in a different field were being included in the IR results set when they should have been excluded. This issue has been corrected.

ATT&CK Visualizer

- ATT&CK view names can now include special characters.

API & Under the Hood

- An issue causing slow v2 API performance on certain instances when including Indicator Attribute data in the response was resolved.

Dependencies & Library Changes

- There are no new dependencies or library changes for ThreatConnect version 7.6.0.

Maintenance Releases Changelog

2024-08-29 7.6.3-M0829R [Latest]

Bug Fixes

- Interactive Mode for Playbooks was not working. This issue has been corrected.

2024-08-21 7.6.3

Bug Fixes

- An issue causing an error to occur when using the Tag normalization feature in **System Settings** was resolved.
- When selecting users during App configuration, the name of a user variable was being displayed rather than its possible values. This issue has been corrected, and the App now saves the selected value for the user variable.
- When installing or migrating to a containerized ThreatConnect instance, you now must follow a new set of steps to preserve the folder ThreatConnect uses as a staging area to run TC Exchange™ Apps (usually located at **/opt/threatconnect/exchange**) as a Docker® mount. These steps have been added to *ThreatConnect Installation Guide_Containerized Deployment* and *ThreatConnect Migration Guide_Containerized Deployment*.
- When cloning a Playbook Trigger, filters on the original Trigger were not being copied over to the clone Trigger. This issue has been resolved.
- Execution of TQL queries on the **Associations** tab of a Group's **Details** screen was failing when cross-owner associations were enabled. This issue was resolved, and performance of this feature was improved.
- An issue causing Apps in the App Builder to revert to an older version when the ThreatConnect instance is restarted was fixed.

2024-08-09 7.6.2-M0809R

Bug Fixes

- An issue causing dashboard owner selections to be cleared after upgrade to 7.6.2 was resolved.
- An issue causing an error to occur when performing a batch import involving file hash merges was fixed.
- An issue causing Tags in a Community or Source to be excluded from responses for GET requests to the `/v3/tags` API endpoint unless the Community or Source was specified in the request was fixed.

2024-07-24 7.6.2

Improvements

- When executing a Playbook with a UserAction Trigger, the available Playbooks will now be listed alphabetically by Trigger name.
- When creating an IR, the **Retrieve Results** button has been removed from Step 3 (**View Results**). This step will show you the first 1000 results (500 local and 500 global). If you want to retrieve additional results, you may do so in the **Results** section of the **Keyword Tracking & Results** card on the **Overview** tab of the IR's **Details** screen after you have finished creating the IR.

Bug Fixes

- An issue causing an extraneous exception to be written to the logs when creating a Post for a Group on the Group's legacy **Details** screen was resolved.
- An issue causing the CAL Status Lock to be turned off for certain Indicators after an instance has been restarted was resolved.
- The preview option for file attachments on the **Report File** and **Document File** cards on the **Details** screen for a Report Group and a Document Group, respectively, is offered only for PDF and HTML files. If you click the thumbnail image for any other file type, an error message will be displayed at the bottom left of the screen.
- An issue preventing certain Organizations from being deleted was resolved.

- An error caused by selecting Groups returned from CAL with no name in the Doc Analysis import was fixed.
- Document files attached when creating a new Group were not being displayed on the associated Document Group's **Details** screen. This issue has been fixed.

2024-06-26 7.6.1

Improvements

- The descriptions for the **appBuilderMaxDebugSessionMinutes**, **intelligenceRequirementKeywordLimit**, and **multiSourceViewEnabled** settings on **System Settings** > **Settings** were updated for clarity.

Bug Fixes

- Display issues that were occurring when adding an associated Artifact or Case from table view of the **Associations** card on an object's legacy **Details** screen were fixed.
- An issue preventing execution details for nested Components from being displayed on the **Execution** screen for a Playbook was fixed.
- Formatting issues occurring in code blocks in **Text Block** sections of reports were resolved.
- An issue preventing posts (notes on the new **Details** screen) for some objects from saving was resolved.

CAL Updates

2024-07-15 CAL 3.8 [Latest]

Feature Update: MITRE ATT&CK 15.1 Framework

- The MITRE ATT&CK® 15.1 update adds 43 new techniques and sub-techniques. In ThreatConnect, the ATT&CK Tags corresponding to this update can be leveraged in features like **Browse**, **Search**, Intelligence Requirements, ATT&CK Visualizer, and Threat Graph.
- MITRE ATT&CK automatic AI classification for Doc Analysis import, the ThreatConnect Intelligence Anywhere, and the **CAL Automated Threat Library** Source can now automatically identify 121 MITRE ATT&CK techniques and sub-techniques with a 95% confidence for the results.

Improvements

- Improvements were made to the **AI Insights** for Report Groups in the **CAL Automated Threat Library** Source to provide more complete and accurate summaries.
- Users leveraging CAL are now limited to 500 file hash information lookups for previously unobserved files per day per ThreatConnect instance.
- Updates were made to support the availability of Doc Analysis import features in Playbooks.
- CAL Safelist updates were made to include over 80 .gov Host and URL resources.

