ThreatConnect® Release Notes

Software Version 7.0

January 18, 2023

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

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

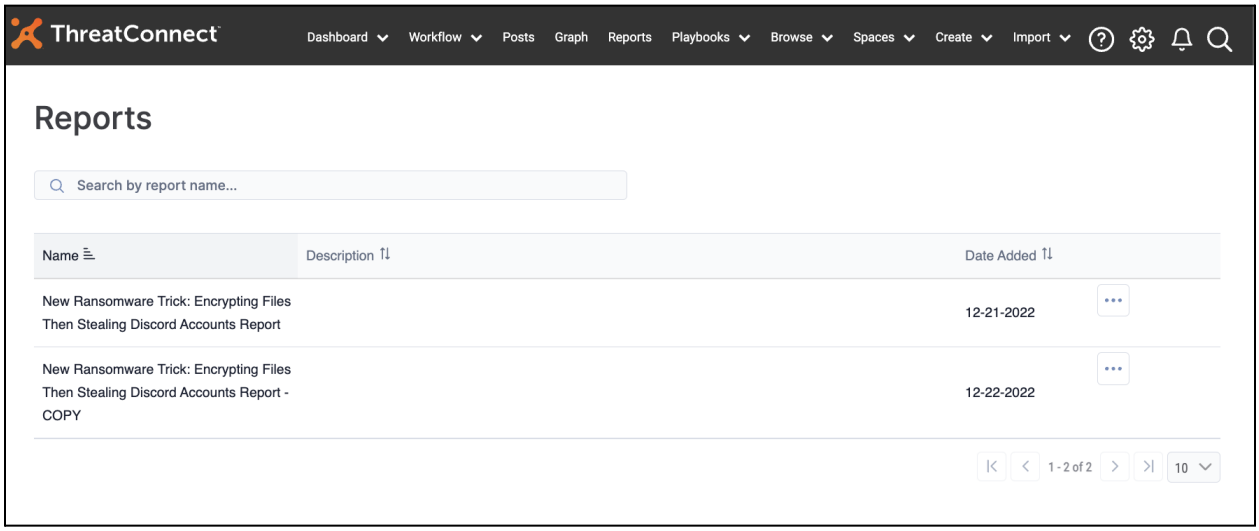
Table of Contents

New Features and Functionality

Reporting Version 1

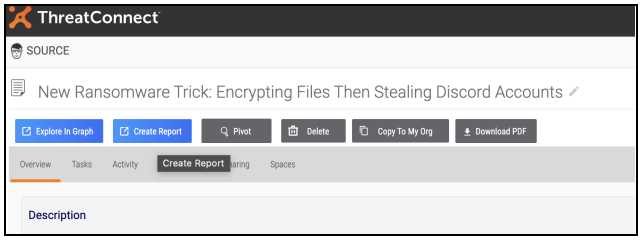
Creating custom reports enables analysts to communicate the value of TI Ops by putting the right information in front of the right people at the right time. With Reporting version 1, we have developed a native reporting engine that you can use to create reports directly from the ThreatConnect Platform, eliminating the need to copy and paste data from ThreatConnect into another document, spreadsheet, or editor. In version 1, reporting is available for all Group object types.

A new **Reports** screen, easily accessible from the top navigation bar, has been added to centralize all reports you and other users in your Organization have created. Search and filtering capabilities on this screen allow you to easily find and view reports.



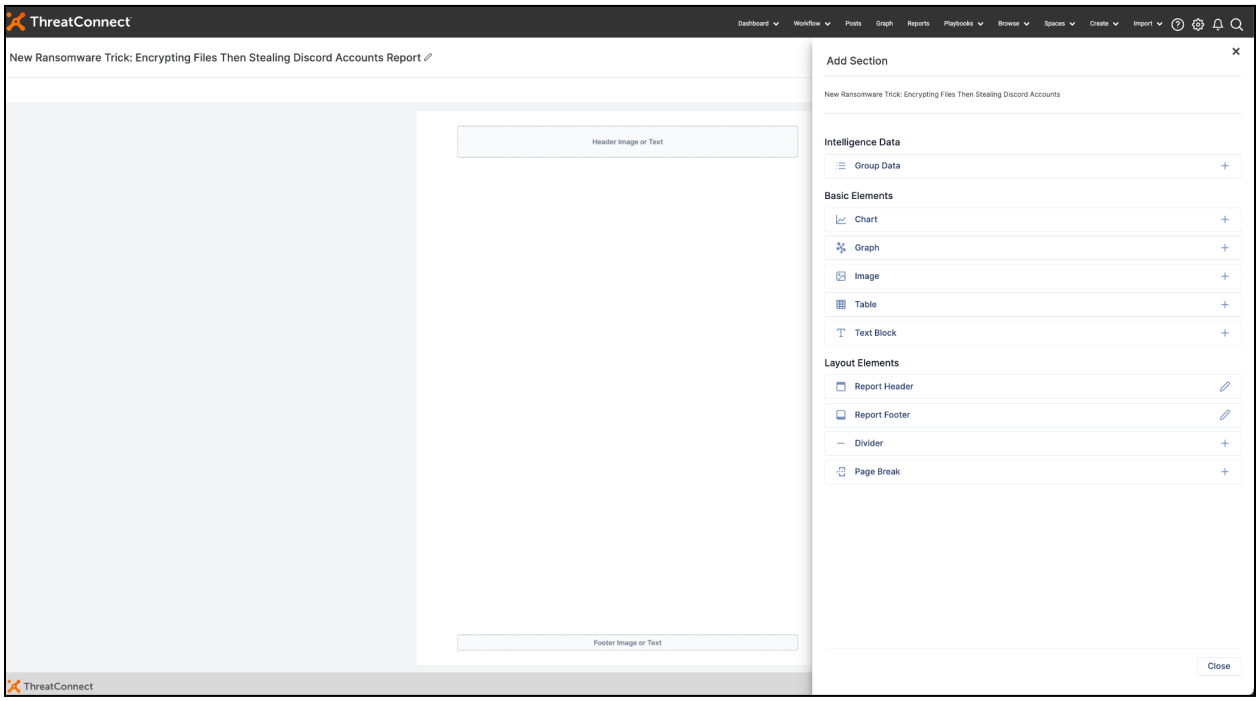
*The **Reports** screen allows you to search and filter the reports you and other users in your Organization have created*

To create a new report, navigate to any Group object's **Details** screen or **Details** drawer and click the **Create Report** button.



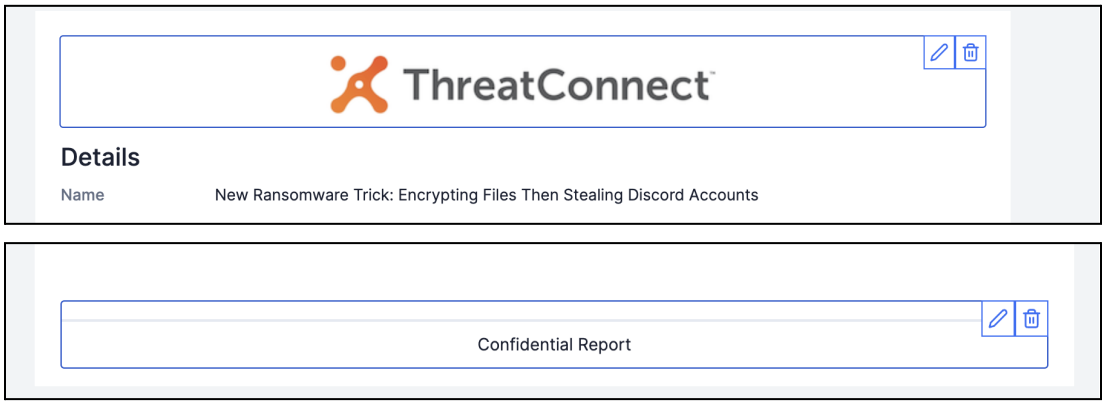
*Click the **Create Report** button from the **Details** screen or drawer for a Group object*

The **Report Editor** will open in a new browser tab.



*Use the **Report Editor** to add elements to your report*

In the **Report Editor**, you can customize headers and footers with images or text to be displayed on every page.

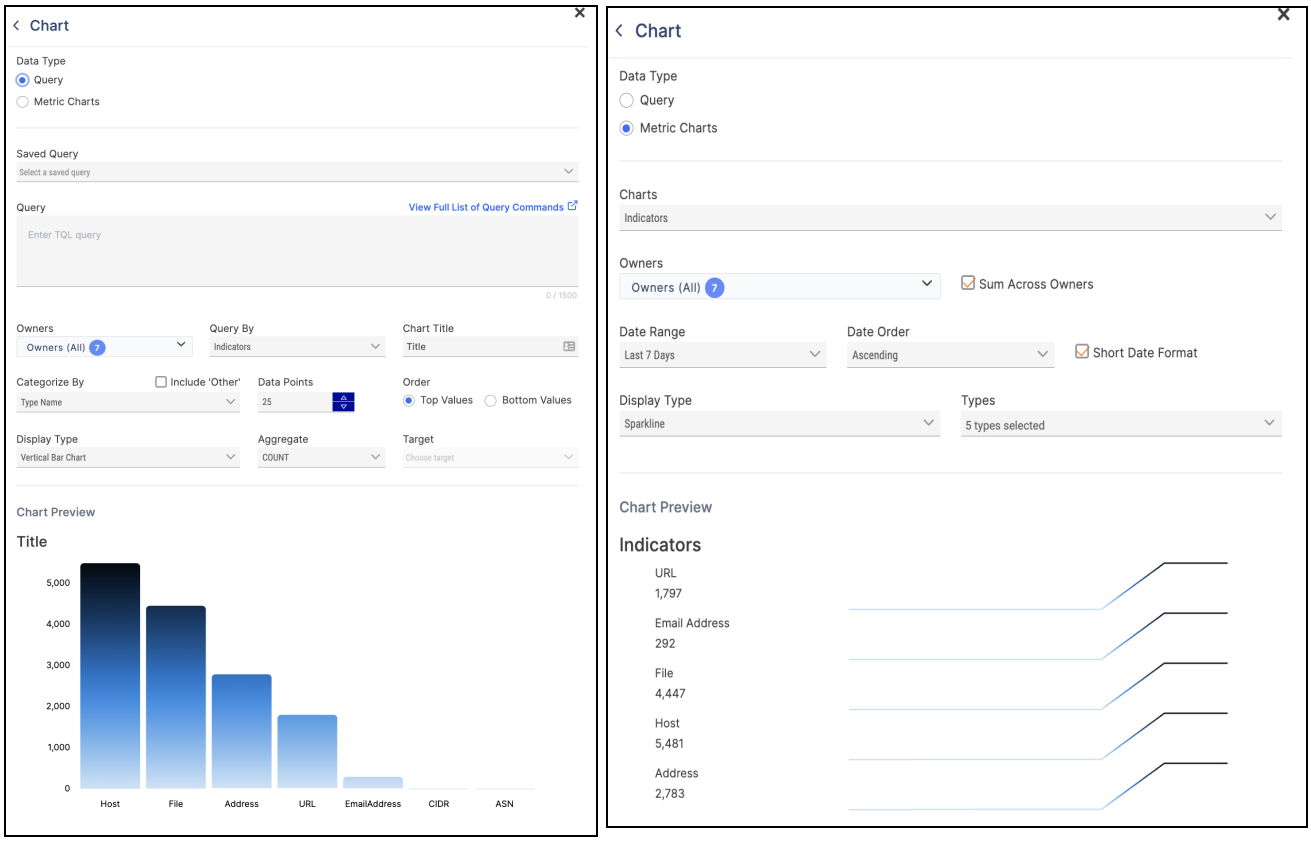


Add headers and footers to your report

Use the **Group Data** widget to add identifying details (e.g., name, type, owner, Tags), Attributes, and associations directly from Groups.

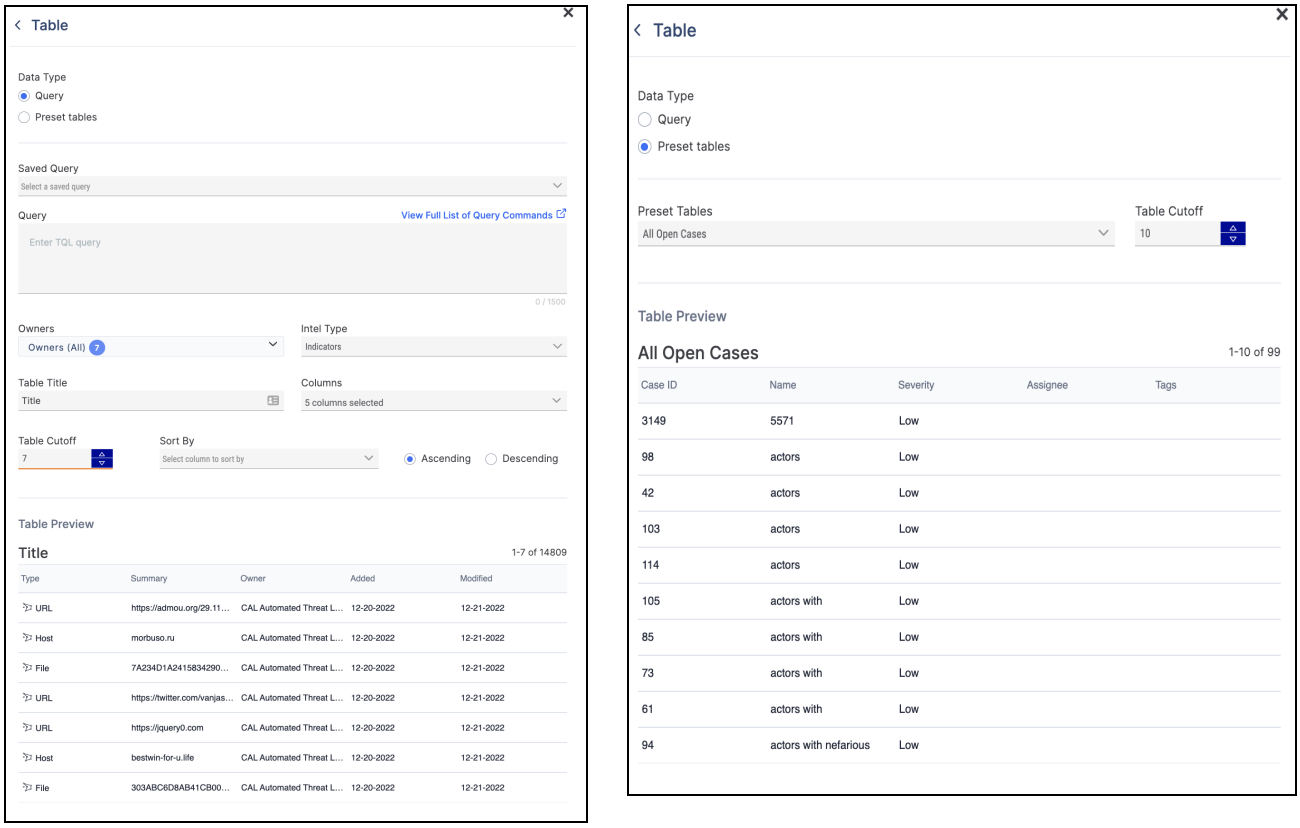
Easily add Group details, Attributes, and associations to reports

You can build custom charts using saved ThreatConnect Query Language (TQL) queries or TQL queries you build on the fly to add to your report. Metrics charts, including system metrics, user metrics, Case metrics, and Playbook metrics, are also available.



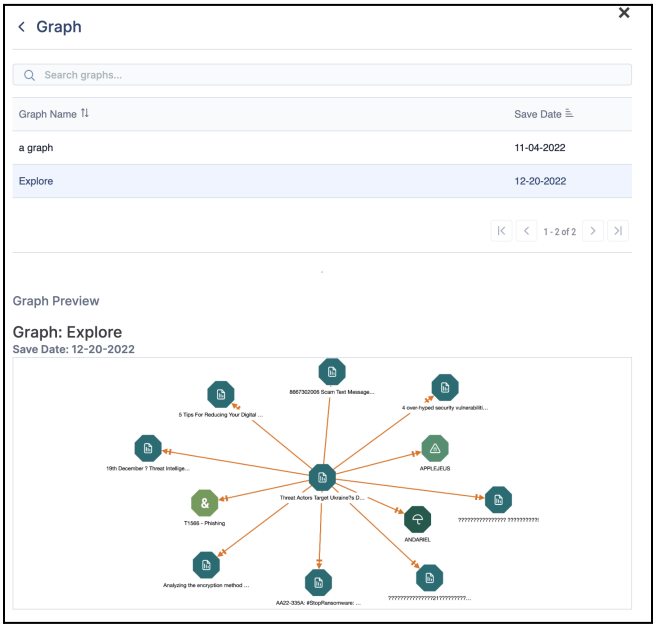
Add custom charts based on TQL queries and metrics to reports

You can also add custom tables that use saved TQL queries or TQL queries you build on the fly to your report.



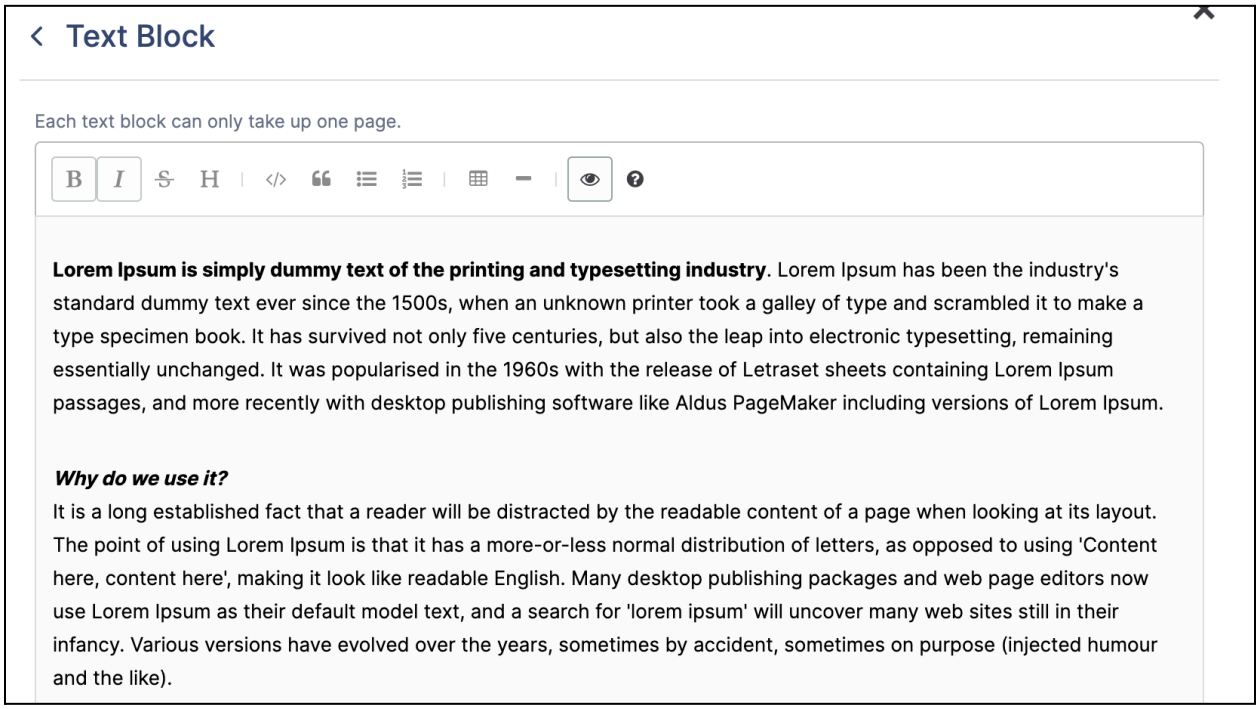
Add custom tables based on TQL queries to reports

Enhance your investigation reports by including saved graphs from Threat Graph.



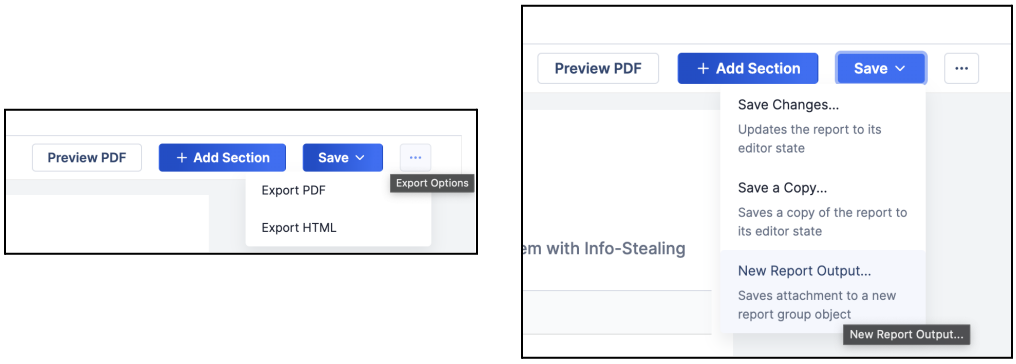
Add saved graphs from Threat Graph to reports

Provide more context to your reports by entering information into text blocks, which fully support Markdown.



Add text blocks, which support Markdown, to reports

Finally, you can export reports in PDF or HTML format or save them as a Report Group object and disseminate them via a ThreatConnect link.



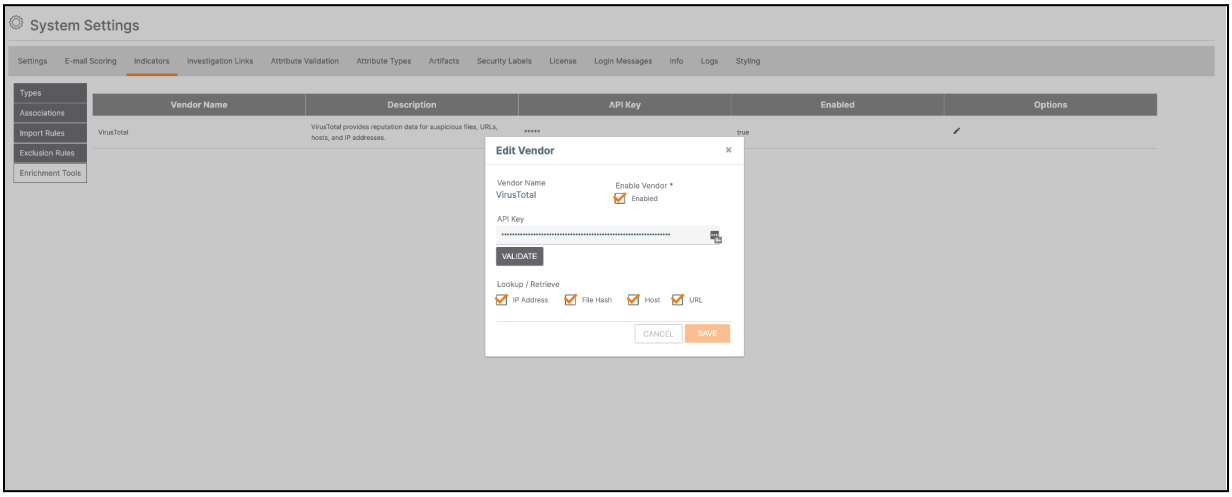
Export Reports or save them as a Report Group object in ThreatConnect

Native Reporting in ThreatConnect is a powerful, easy-to-use tool to showcase the value of TI Ops in your organization.

Built-In Enrichment

Threat intelligence enrichment helps to remove false positives and deliver actionable intelligence for threat investigation and other security operations. With built-in enrichment in ThreatConnect 7.0, you can get out-of-the-box consolidated views of enrichment on IOCs from VirusTotal™ without building Playbooks or sifting through additional websites.[1]

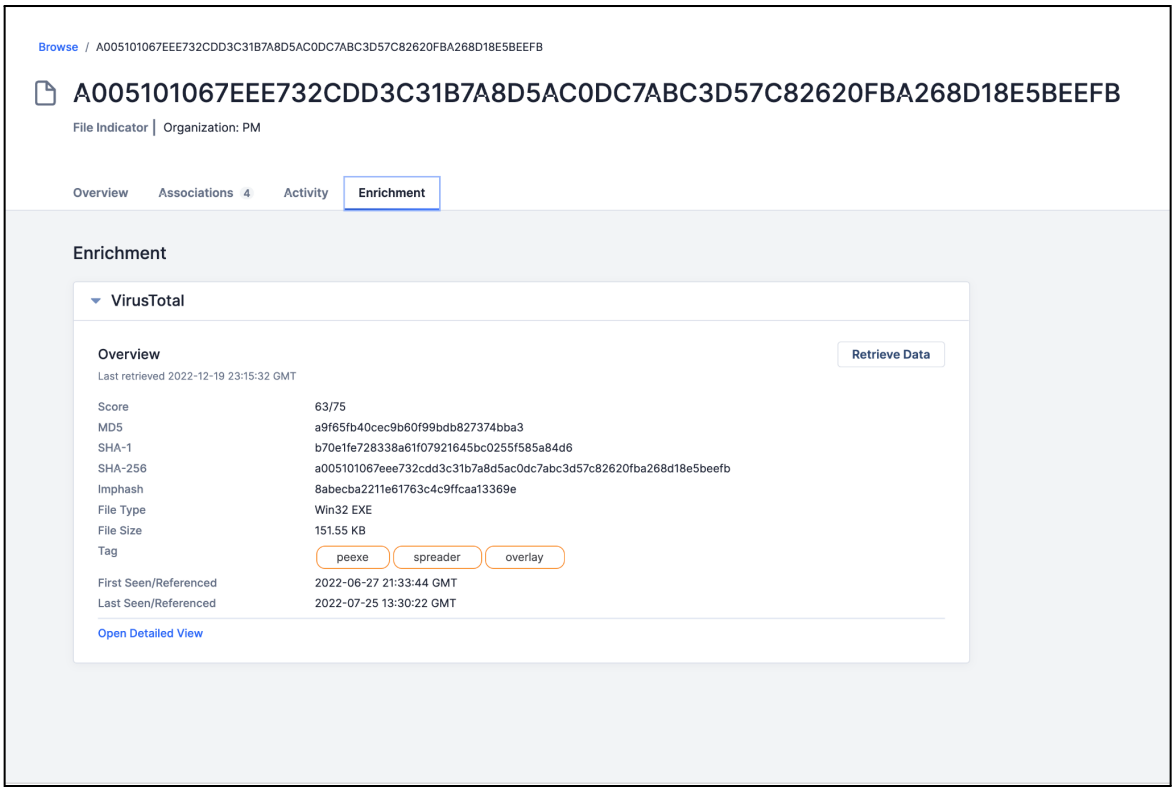
You can enable built-in enrichment by adding your VirusTotal API key to the **Enrichment Tools** section of the **Indicators** tab of **System Settings**. After validating the API key, you can select the Indicator types (Address, File, Host, or URL) you would like to be able to look up in VirusTotal.



*Configure VirusTotal enrichment for available Indicator types in **System Settings***

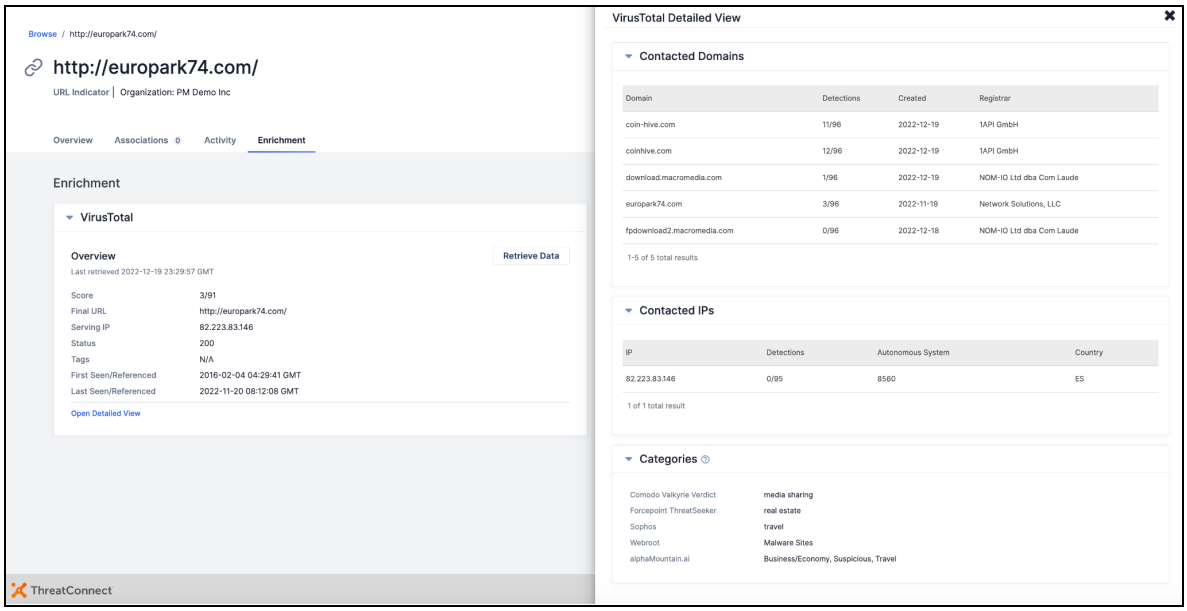
Once the API key is saved, you can view enrichment details for IP addresses, URLs, Hosts, and Files on the **Enrichment** tab of the new view of an Indicator's **Details** screen (more on the new **Details** view in the "Revamped Details Screen" section!). To prevent exhaustion of current quota limits, built-in enrichment features will not automatically enrich every Indicator. When you click an Indicator's **Enrichment** tab for the first time, overview information from VirusTotal is pulled and cached. A caching timer is set in your instance's system settings (**System Settings**→**Settings**→**Storage**→**Third Party Enrichment**). Every time you revisit the **Enrichment** tab for an Indicator, cached data will be present. A VirusTotal lookup is not made until the caching timer expires. To get the latest enrichment details from VirusTotal before the caching time limit expires, you can always click the **Retrieve Data** button on the **Enrichment** tab.

[1] VirusTotal™ is a trademark of Google, Inc.



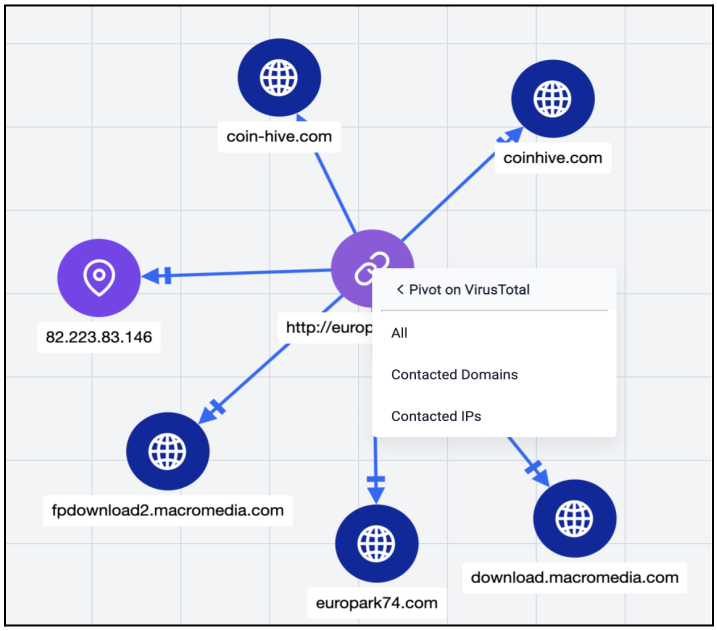
*VirusTotal data are provided on the **Enrichment** tab of an Indicator's **Details** screen*

To take a deeper dive into the information VirusTotal knows about an Indicator, you can click the **Open Detailed View** link.This view shows relationships like domains and IP addresses that URLs have contacted, domain-to-IP address mappings over time, host-to-URL relationships, etc.



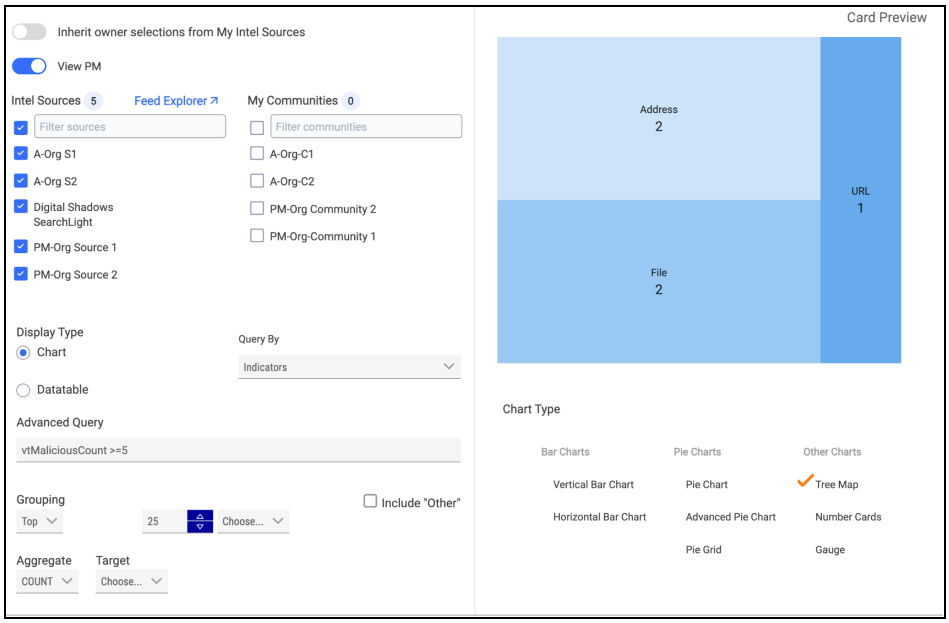
*The **VirusTotal Detailed View** provides detailed enrichment information for an Indicator*

These relationships can also be visualized in Threat Graph. With the 7.0 release, each Address, File, Host, and URL Indicator node in Threat Graph provides an option to enrich with VirusTotal, adding nodes for objects such as Contacted IPs, Contacted URLs, Contacted Domains, and Subdomains. Pivoting on these Indicator relationships from VirusTotal in ThreatGraph can help you spot patterns and get a more complete picture of your investigation.



Pivoting on VirusTotal enrichment data gives you more insight into an Indicator's relationships

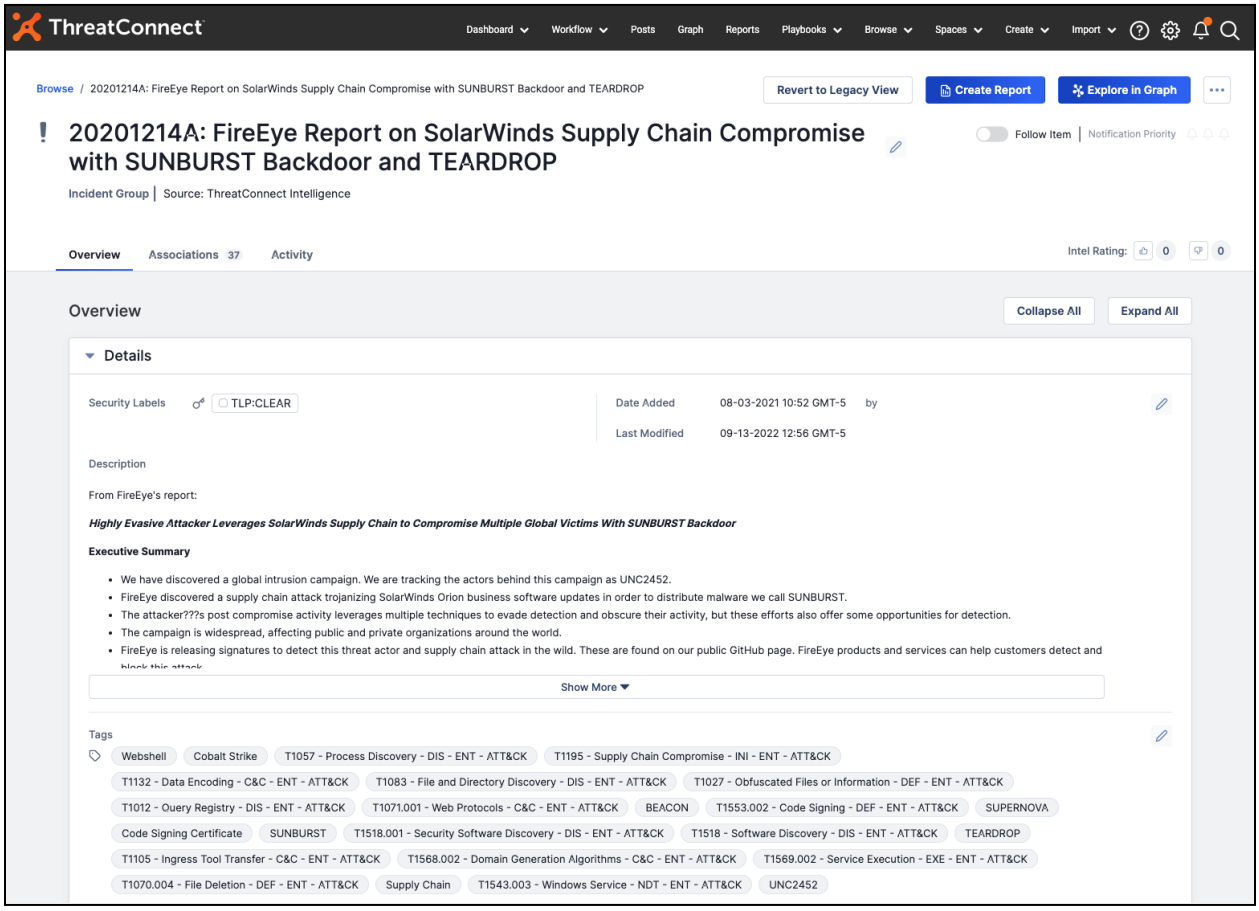
The VirusTotal Score for an Indicator is also queryable via TQL. You can use **vtMaliciousCount >= *<score>*** to query Indicators of interest based on a specific VirusTotal Score. You can also use TQL expressions involving this parameter to filter Indicators on the **Browse** screen and when building dashboards.



*Use the **vtMaliciousCount** TQL parameter to filter dashboard query cards*

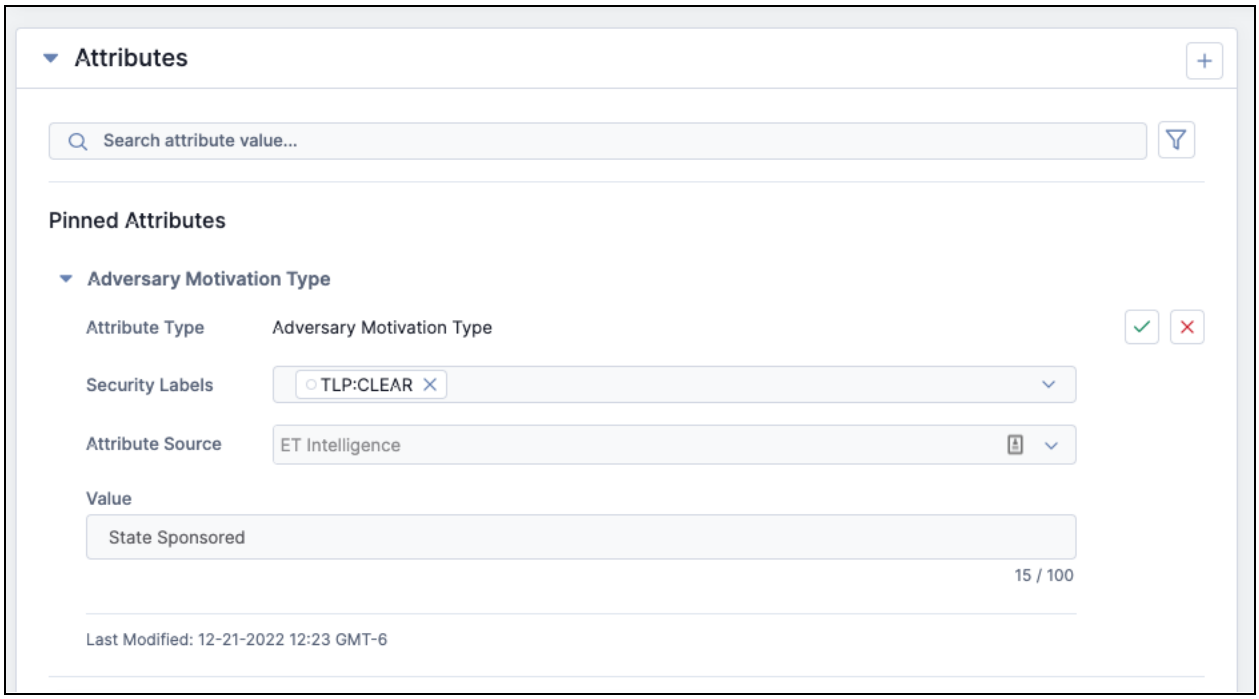
Revamped Details Screen

In ThreatConnect version 6.7, we added the ability to associate objects across owners in ThreatConnect, making it easier to build a fuller understanding of the wealth of information available related to a given threat. In ThreatConnect version 7.0, we are doubling down on that functionality while also demonstrating our commitment to Threat Intelligence producers and consumers by releasing our updated **Details** UI.



*The new **Details** view makes it easier for you to view, find, and track information about objects*

The updated **Details** screen offers a cleaner, more intuitive layout and adds the ability to search, filter, and pin Attributes that are of particular interest to a user or team.

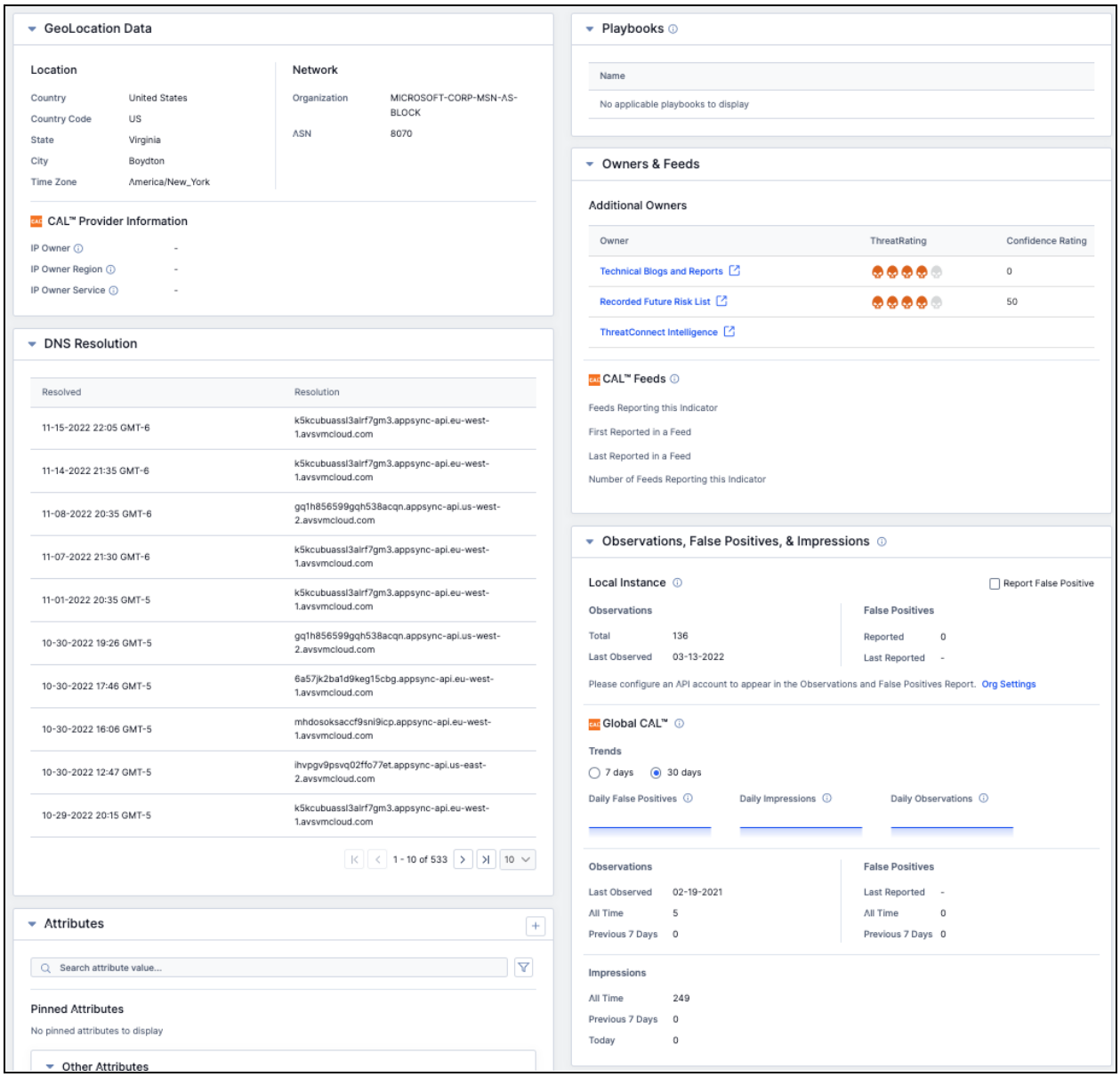


View the most important Attributes quickly by pinning them

These added capabilities will help you more quickly get the information you need to make decisions faster.

In addition, you can now view global data from CAL™ in a more logical way in the new **Details** view alongside local data from your ThreatConnect instance.[2] This format gives you a clearer, more holistic view of the threat posed by a given Indicator and enables you to easily understand which information is from CAL and which information is from your local instance.

[2] CAL™ is a trademark of ThreatConnect, Inc.



View global CAL data in context alongside local data from your ThreatConnect instance

These updates to the **Details** screen are in response to user feedback we've received over the years about ease of use and the UI/UX, and they are the first in a series of updates we will be doing over the course of upcoming releases. Please share any and all feedback on the new **Details** view and the other features in ThreatConnect 7.0 with us via ProductBoard or through your Customer Success Manager.

Improvements

Threat Intelligence

- A new Signature Group type was added: KQL (Microsoft® KQL).[3]
- When adding an association from an object's **Details** screen, the **Add Groups** or **Add Indicators** window now displays an overlay indicating that it is loading data. If the load operation times out, a message will be displayed to inform you of this outcome.
- You can now export selected Groups to a comma-separated values (CSV) file from the **Browse** screen.
- Previously, when creating a cross-owner association between two objects, you needed to have edit permissions in both owners. Now, as long as you have edit permissions in one of the owners and at least read-only permissions in the other owner, you can create the association.

Playbooks

- When you hover over the hashtag (**#**) for a Playbook Trigger, App, or Operator, the outputs will now be displayed in alphabetical order.
- When you import a Playbook with an App that was configured to use a particular Environment at the time of the Playbook's export and that Environment exists on your instance, then that Environment will automatically be selected in the App's configuration upon import.

Playbook Services

- On the **Services** tab of the **Playbooks** screen, the **API Path** for a Service App will be a clickable hyperlink to the full URL path if the App's configuration has designated that the API path destination has a UI.

[3] Microsoft® is a registered trademark of Microsoft Corporation.

System Settings

- The following new system setting was added:
  - **thirdPartyEnrichmentCacheLimit**: This setting determines the number of days that third-party enrichment data are cached.

Account Settings

- The following limits have been removed from ThreatConnect:
  - Organization Indicator limit
  - Organization document storage limit
  - Community and Source Indicator limit
  - Community and Source document storage limit
  - System Indicator limit
  - System document storage limit

Organization Settings

- When creating a Job for an App, the version number for each available App is now displayed next to the App's name in the **Run Program** dropdown on the **Program** step of the **Add Job** drawer.

API & Under the Hood

- Previously, you could use the v3 API to create cross-owner associations between existing objects only. Now you can now use it to simultaneously create a new object in an owner in which you have edit permissions and create a cross-owner association to that object.
- You can now view and update a Group's Intel Rating (formerly known as upvotes and downvotes) in the v3 API.
- When working with File Indicators in the v3 API, you can use the **merge** mode to merge separate File Indicators containing different file hash types into a single File Indicator containing those file hashes.

- The following query parameters are now available in the v3 API:
    - **dnsResolution**: For Address Indicators, returns a list of Hosts that have resolved to the Address, presently or historically. For Host Indicators, returns a list of Addresses that have resolved to the Host, presently or historically, and geographic information within ThreatConnect and CAL for those Addresses.
    - **enrichment**: For Indicator types for which the VirusTotal enrichment service has been enabled, returns the VirusTotal Score (malicious count) for an Indicator and the date and time when this information was last retrieved in ThreatConnect.
    - **geoLocation**: For Host Indicators, returns a list of Addresses that have resolved to the Host, presently or historically, and geographic information within ThreatConnect and CAL for those Addresses. For Address Indicators, returns address geographic information within ThreatConnect and CAL for the Indicator.
    - **investigationLinks**: Returns a list of Investigation Links for an Indicator.
    - **whois**: Returns a list of Whois information for a Host Indicator.
- Responses for Indicators and Groups in the v3 API will now include a **legacyLink** field that includes a link to the object's legacy **Details** screen.

Bug Fixes

Dashboards

- An issue causing the **Active Cases** dashboard card to display no results when Communities or Sources were selected as owners in the card's configuration has been fixed.

Threat Intelligence

- An issue causing batch Indicator import operations to bypass the **indicatorStatusLock** system setting was fixed.
- An issue causing some fields in the CSV file from an Email export to be blank was fixed.

Threat Graph

- When pivoting on Indicators in ThreatConnect for an Indicator whose type does not have any available custom associations for that relationship, the displayed message with that information will no longer overflow into the **Pivot in ThreatConnect** menu header.
- An issue causing an error to occur when pivoting on Indicators in ThreatConnect for certain Groups has been resolved.

Attributes

- An issue causing Attributes for Groups and Cases to expose potential malicious redirects by not sanitizing HTML properly in Markdown has been resolved.

Playbooks

- An issue causing owners to appear multiple times in Playbook configurations via the **${OWNER}** variable and in the **Owner** field for Triggers was resolved.

Feed Services

- Selection or deselection of the **Verify TC SSL** checkbox in the configuration for a Feed Service now remains consistent from when it is initially set in the Feed Deployer and when the Feed Service's configuration is edited on the **Services** tab of the **Playbooks** screen.
- An issue causing the **Type** and **Service** fields to show default values instead of values specific to the configured Service when editing a Feed Service has been fixed.
- An issue causing feeds deployed by the Feed Deployer to display an incorrect Source owner when editing a Job for the feed has been fixed.

Dependencies & Library Changes

- There are no new dependencies or library changes for ThreatConnect version 7.0.

Maintenance Releases Changelog

2023-02-08 7.0.1 [Latest]

Dependencies & Library Changes

- Python® 3.11 is now supported.[4]

Improvements

- Critical-error dialog windows have been replaced by a **Data Inconsistency** notification that should allow you to continue working in ThreatConnect and give you more information on the issue that has occurred. This notification window will be displayed at the bottom left of the screen and contain details about the error that you can share with your administrator.
- When an invalid system license is applied, the reason that the license is invalid will now be provided in the system logs and via API response.
- Permissions on Job subfolders created by Playbooks are now set upon creation of the subfolders rather than just after creation.
- The timezone selected in your user profile will now be displayed in timestamps in the following areas in the Workflow Cases UI:
    - **Case Details** card: **Case created** timestamp, **last updated** timestamp
    - **Phases and Tasks**: timestamp for Task due dates, timestamp for completion of automated Tasks
    - **Attributes** card: **Date Added** timestamp
    - **Artifacts** card: timestamp in the **Date** column
    - **Notes** card: timestamp for when each Note was added
    - **Timeline** card: timestamp for each item when the item is expanded

Bug Fixes

- An issue causing an application error to occur when attempting to access the **Associations** tab from the new **Details** screen of certain objects has been resolved.

[4] Python® is a registered trademark of Python Software Foundation.

- An issue causing corrupted variable values when reusing Playbook Components has been fixed.
- An issue causing Tag autocompletion to be case sensitive has been resolved.
- When upgrading your version of ThreatConnect, the ThreatConnect installer will now prompt you for super user credentials and then automatically update the database schema.
- An issue causing an error to occur when using the **createdBy** filter in a nested TQL query has been fixed.
- A number of formatting and other UI issues on the **Potential Associations** card on the **Associations** tab of the new **Details** screen have been resolved.
- An issue causing an error when using the v3 API to create a Case with a custom Attribute type that exists at both the System and Organization level was fixed.
- An issue causing an error to occur when adding a Note to a Task in a Workflow Case and when refreshing the browser after a Note has been added to a Task has been fixed.
- The list of countries in the **Country** Attribute Validation Rule has been alphabetized, with “United States” at the top of the list.
- An issue causing Case Triggers to fire outside of filter conditions has been fixed.
- An issue preventing notification emails from being sent when remotely executed Jobs failed was resolved.
- An issue preventing the **Update Global Variable** Playbook App from resolving variables when applying the Set operation in an Iterator Operator has been fixed.
- When an API user is unable to retrieve an object because they do not have an Organization role that conveys the requisite permissions, a notification to this effect will now be sent.
- An issue causing newly loaded Service Apps not to be available in the App Builder has been resolved.
- When adding a Trigger to a Playbook, an issue preventing custom Trigger Services that include an entered search term as a label from being displayed in the results has been fixed.
- An issue causing disabled Service Apps to start automatically when edited was resolved.

2023-02-03 7.0.0b

Bug Fixes

- An issue causing the owner of a Workflow Case to change to a Super User's Organization when the Super User modifies the Case has been resolved.
- An issue causing extraneous fields to be returned when sending requests to the **`/v3/cases`** API endpoint has been resolved.

2023-01-27 7.0.0a

Bug Fixes

- An issue causing Apps to fail when trying to use the **`source`** field for v3 API Attribute endpoints has been resolved.
- An issue causing the **Attributes** card on the **Overview** tab of the new **Details** screen to be very small when a Playbook on the **Playbooks** card has a very long description has been fixed.