



# ThreatConnect® Release Notes

Software Version 7.0

January 18, 2023



# Table of Contents

---

<b>New Features and Functionality</b>	<b>4</b>
Reporting Version 1	4
Built-In Enrichment	10
Revamped Details Screen	14
<b>Improvements</b>	<b>17</b>
Threat Intelligence	17
Playbooks	17
Playbook Services	17
System Settings	18
Account Settings	18
Organization Settings	18
API & Under the Hood	18
<b>Bug Fixes</b>	<b>20</b>
Dashboards	20
Threat Intelligence	20
Threat Graph	20
Attributes	20
Playbooks	20
Feed Services	21
<b>Dependencies &amp; Library Changes</b>	<b>22</b>
<b>Maintenance Releases Changelog</b>	<b>23</b>
2023-05-31 7.0.2h [Latest]	23
Bug Fixes	23
2023-05-23 7.0.2g	23
Bug Fixes	23
2023-05-19 7.0.2f	23
Bug Fixes	23
2023-05-09 7.0.2e	23
Bug Fixes	23
2023-04-13 7.0.2c	24
Bug Fixes	24
2023-03-28 7.0.2b	24
Bug Fixes	24



2023-03-22 7.0.2a	24
Bug Fixes	24
2023-03-09 7.0.2	24
Improvements	24
Bug Fixes	25
2023-02-15 7.0.1a	27
Improvements	27
2023-02-08 7.0.1	27
Improvements	27
Bug Fixes	28
2023-02-03 7.0.0b	29
Bug Fixes	29
2023-01-27 7.0.0a	29
Bug Fixes	29

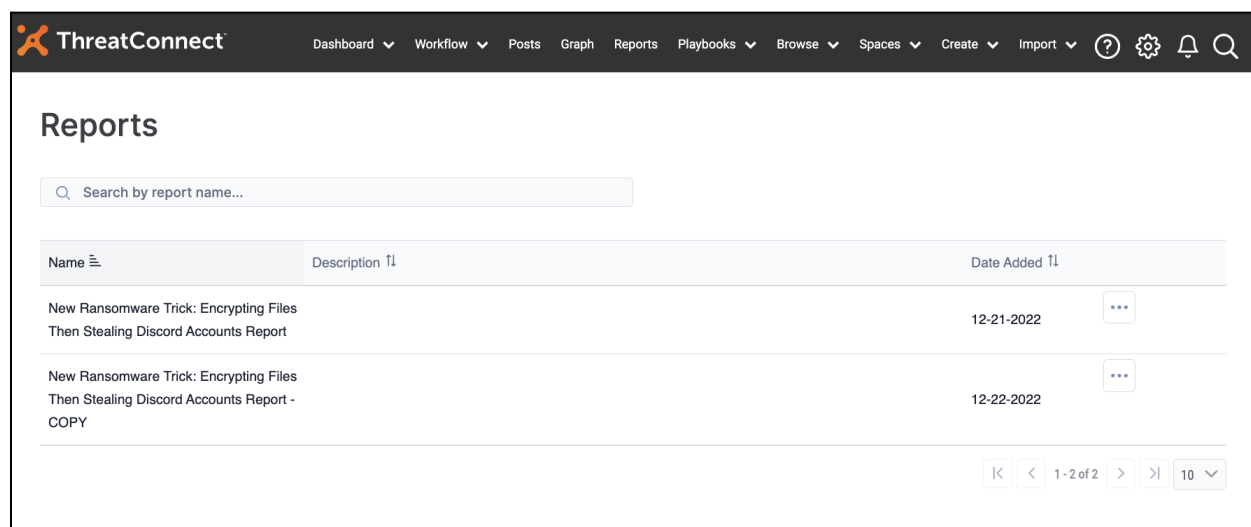


# New Features and Functionality

## Reporting Version 1

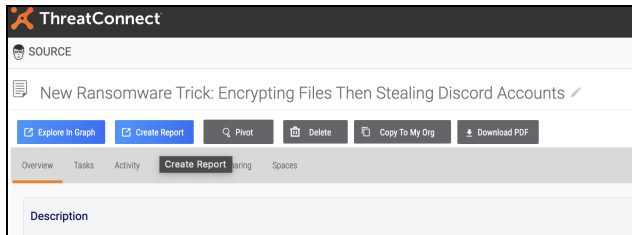
Creating custom reports enables analysts to communicate the value of TI Ops by putting the right information in front of the right people at the right time. With Reporting version 1, we have developed a native reporting engine that you can use to create reports directly from the ThreatConnect Platform, 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.



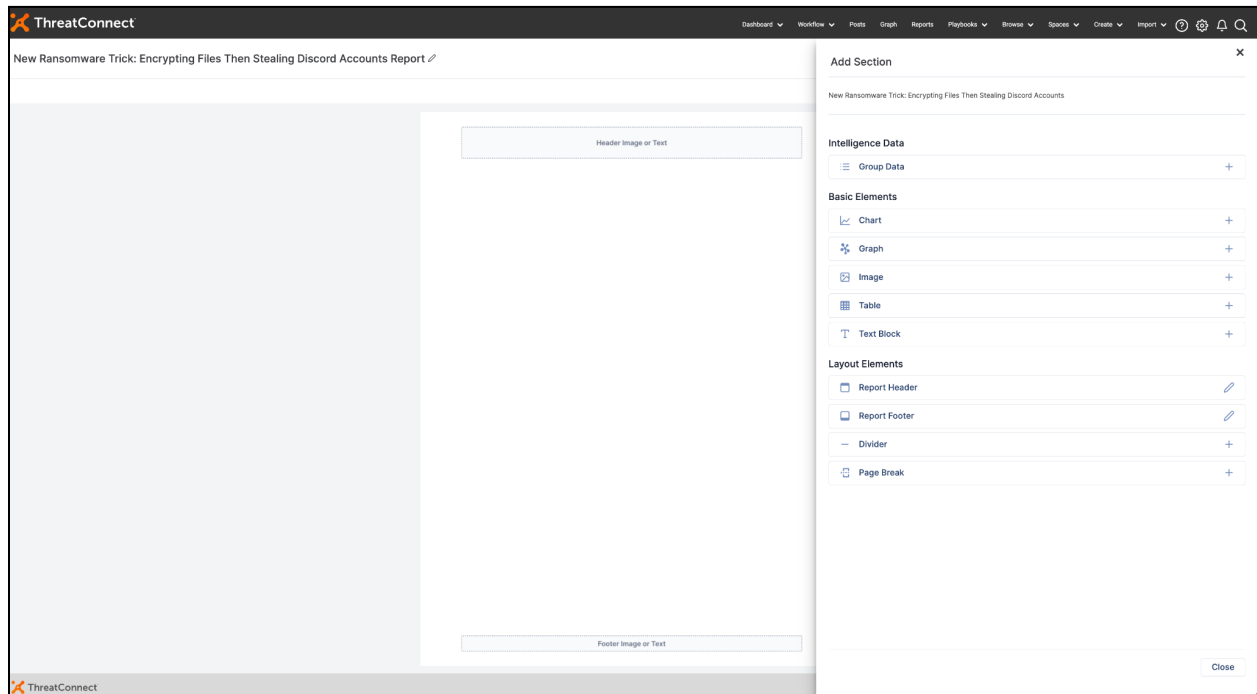
*The **Reports** screen allows you to search and filter the reports you and other users in your Organization have created*

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

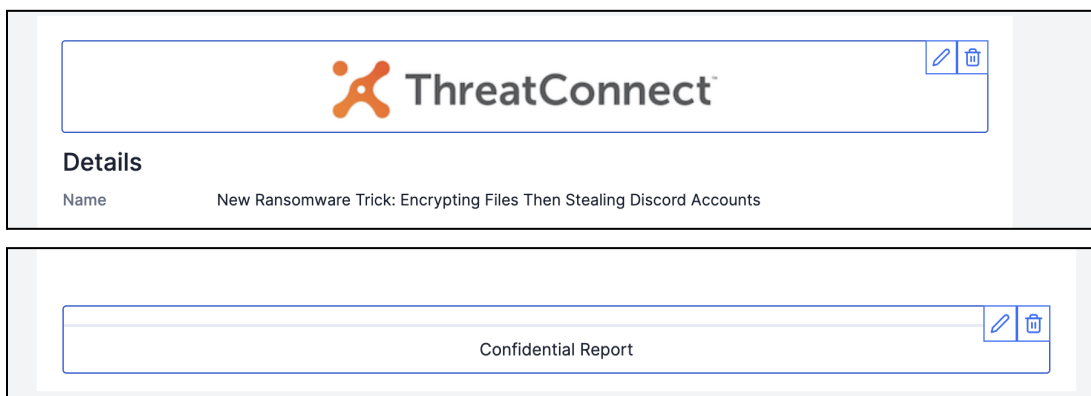
The **Report Editor** will open in a new browser tab.



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

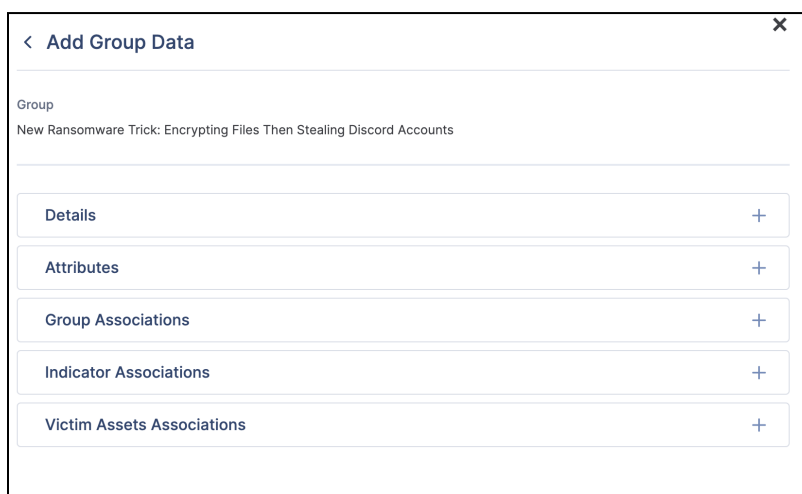


In the **Report Editor**, you can customize headers and footers with images or text to be displayed on every page.



*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.



The left screenshot shows the 'Chart' configuration interface with the 'Query' data type selected. It includes a 'Query' input field, a 'Saved Query' dropdown, and various configuration options like 'Owners', 'Query By', 'Chart Title', 'Categorize By', 'Data Points', 'Order', 'Display Type', 'Aggregate', and 'Target'. A 'Chart Preview' section shows a bar chart titled 'Title' with categories: Host (5,000), File (4,447), Address (2,922), URL (1,797), EmailAddress, CIDR, and ASN.

The right screenshot shows the 'Chart' configuration interface with 'Metric Charts' selected. It includes a 'Charts' dropdown, 'Owners' dropdown, 'Date Range', 'Date Order', 'Short Date Format', 'Display Type', and 'Types' dropdown. A 'Chart Preview' section shows a sparkline chart with categories: URL (1,797), Email Address (292), File (4,447), Host (5,481), Address (2,783).

*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.



**< Table**

Data Type  
 Query  
 Preset tables

Saved Query  
Select a saved query

Query  
Enter TQL query [View Full List of Query Commands](#)

Owners  
Owners (All) Intel Type  
Indicators

Table Title  
Title Columns  
5 columns selected

Table Cutoff  
7 Sort By  
Ascending Descending

Table Preview  
**Title** 1-7 of 14809

Type	Summary	Owner	Added	Modified
URL	https://admo.u.org/20.11...	CAL Automated Threat L...	12-20-2022	12-21-2022
Host	morbuso.ru	CAL Automated Threat L...	12-20-2022	12-21-2022
File	7A234D1A2415834280...	CAL Automated Threat L...	12-20-2022	12-21-2022
URL	https://twitter.com/vanjas...	CAL Automated Threat L...	12-20-2022	12-21-2022
URL	https://query0.com	CAL Automated Threat L...	12-20-2022	12-21-2022
Host	bestwin-for-u.life	CAL Automated Threat L...	12-20-2022	12-21-2022
File	303ABC6D8AB41CB00...	CAL Automated Threat L...	12-20-2022	12-21-2022

**< Table**

Data Type  
 Query  
 Preset tables

Preset Tables  
All Open Cases Table Cutoff  
10

Table Preview  
**All Open Cases** 1-10 of 99

Case ID	Name	Severity	Assignee	Tags
3149	5571	Low		
98	actors	Low		
42	actors	Low		
103	actors	Low		
114	actors	Low		
105	actors with	Low		
85	actors with	Low		
73	actors with	Low		
61	actors with	Low		
94	actors with nefarious	Low		

*Add custom tables based on TQL queries to reports*

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

**< Graph**

Search graphs...

Graph Name	Save Date
a graph	11-04-2022
Explore	12-20-2022

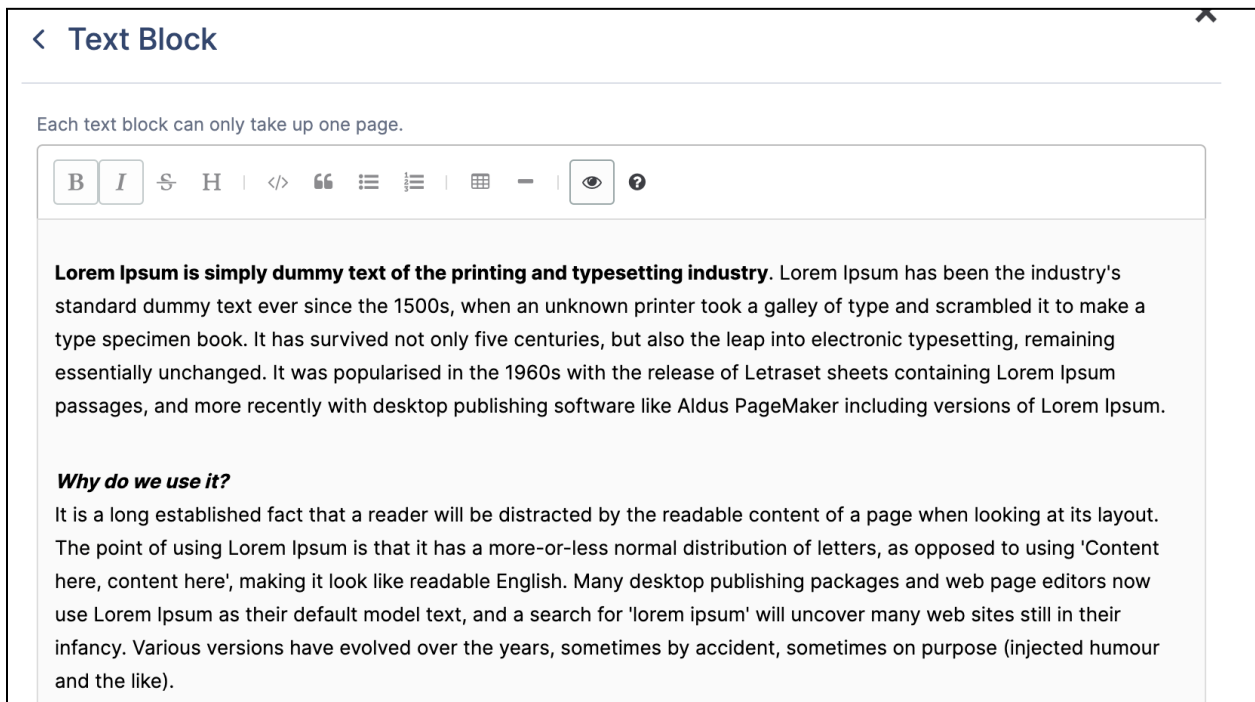
Graph Preview  
**Graph: Explore**  
Save Date: 12-20-2022

*Add saved graphs from Threat Graph to reports*



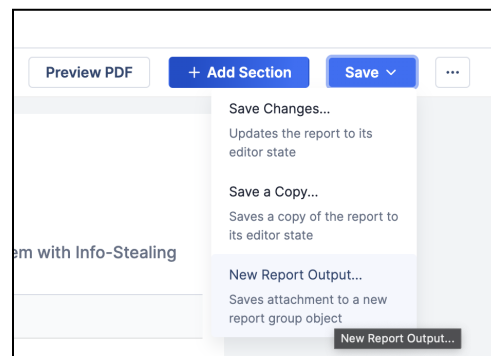
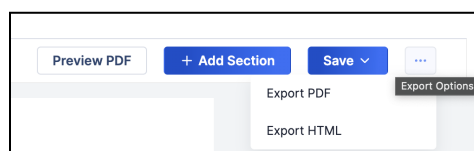


Provide more context to your reports by entering information into text blocks, which fully support Markdown.



*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*

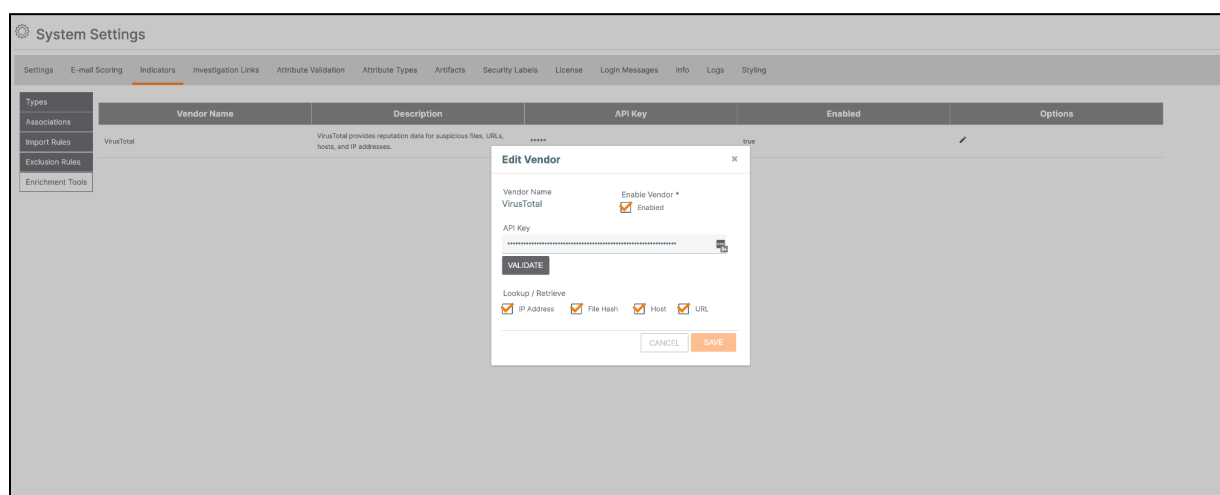
Native Reporting in ThreatConnect is a powerful, easy-to-use tool to showcase the value of TI Ops in your organization.



# 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.<sup>1</sup>

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.

<sup>1</sup> VirusTotal™ is a trademark of Google, Inc.



Browse / A005101067EEE732CDD3C31B7A8D5AC0DC7ABC3D57C82620FBA268D18E5BEEFB

**A005101067EEE732CDD3C31B7A8D5AC0DC7ABC3D57C82620FBA268D18E5BEEFB**  
File Indicator | Organization: PM

Overview Associations 4 Activity **Enrichment**

### Enrichment

**VirusTotal**

**Overview** Retrieve Data

Last retrieved 2022-12-19 23:15:32 GMT

Score	63/75
MD5	a9f65fb40cec9b60f99bdb827374bba3
SHA-1	b70e1fe728338a61f07921645bc0255f585a84d6
SHA-256	a005101067eee732cdd3c31b7a8d5ac0dc7abc3d57c82620fba268d18e5beefb
Imphash	8abecba2211e61763c4c9ffcaa13369e
File Type	Win32 EXE
File Size	151.55 KB
Tag	<span>peexe</span> <span>spreader</span> <span>overlay</span>
First Seen/Referenced	2022-06-27 21:33:44 GMT
Last Seen/Referenced	2022-07-25 13:30:22 GMT

[Open Detailed View](#)

*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.



**Enrichment**

**VirusTotal**

**Overview**

Last retrieved 2022-12-19 23:29:57 GMT [Retrieve Data](#)

Score	3/91
Final URL	http://europark74.com/
Serving IP	82.223.83.146
Status	200
Tags	N/A
First Seen/Referenced	2018-02-04 04:28:41 GMT
Last Seen/Referenced	2022-11-20 08:12:08 GMT

[Open Detailed View](#)

**VirusTotal Detailed View**

**Contacted Domains**

Domain	Detections	Created	Registrar
coin-hive.com	11/96	2022-12-19	IAPM GmbH
coinhive.com	12/96	2022-12-19	IAPM GmbH
download.macromedia.com	1/96	2022-12-19	NOM-ID Ltd dba Com Laude
europark74.com	3/96	2022-11-19	Network Solutions, LLC
fpdownload2.macromedia.com	0/96	2022-12-18	NOM-ID Ltd dba Com Laude

1-5 of 5 total results

**Contacted IPs**

IP	Detections	Autonomous System	Country
82.223.83.146	0/95	8560	ES

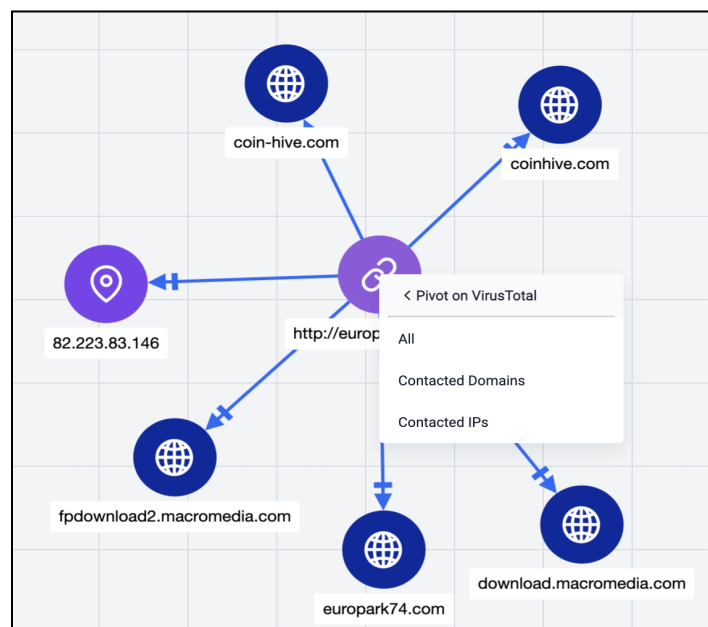
1 of 1 total result

**Categories**

Comodo Valkyrie Verdict	media sharing
Forcepoint ThreatSeeker	real estate
Sophos	travel
Webroot	Malware Sites
alphaMountain.ai	Business/Economy, Suspicious, Travel

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.

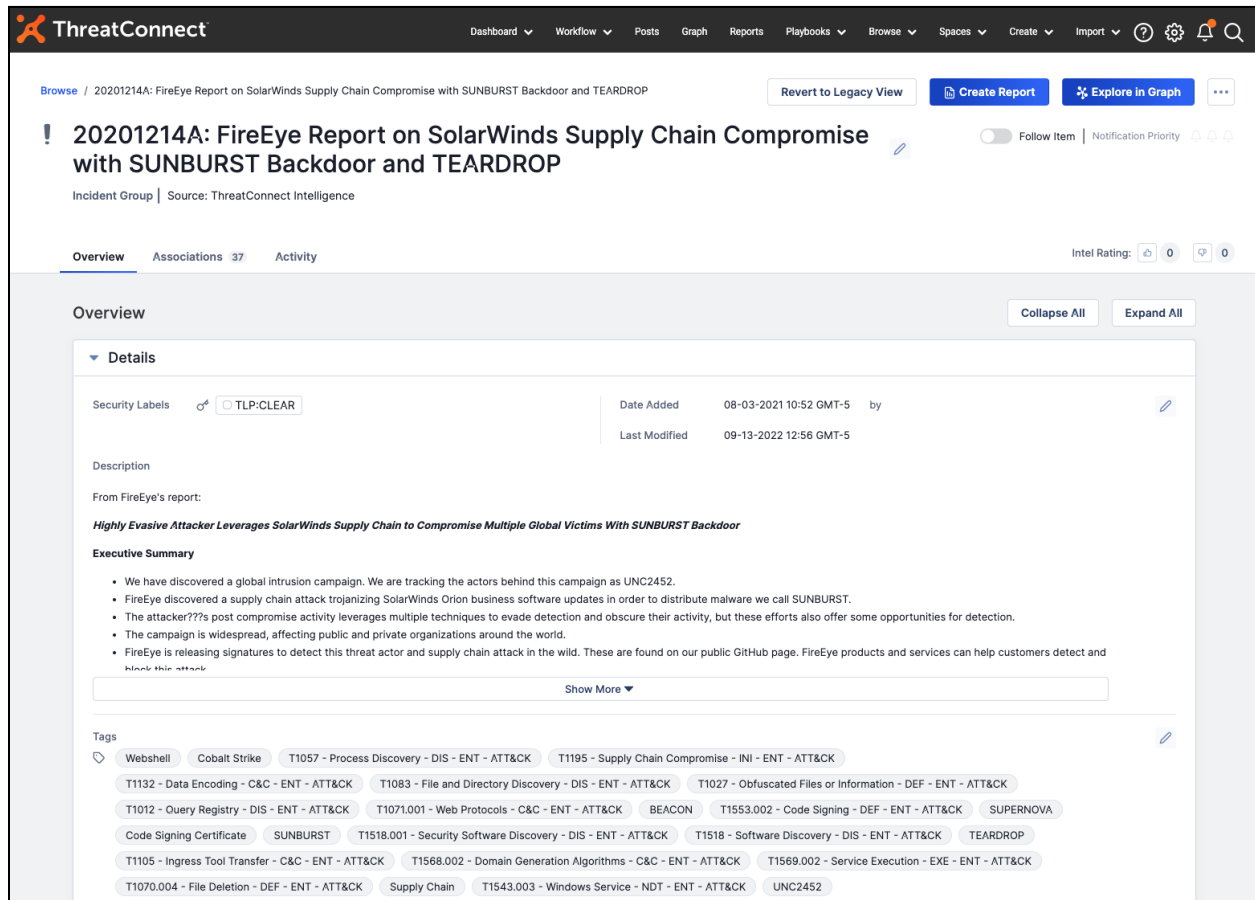
The screenshot displays the configuration interface for a dashboard card. On the left, the 'Advanced Query' field contains the TQL expression `vtMaliciousCount >=5`. The 'Display Type' is set to 'Chart', and the 'Query By' dropdown is set to 'Indicators'. The 'Grouping' is set to 'Top' with a value of 25. The 'Aggregate' is set to 'COUNT'. The 'Card Preview' on the right shows a tree map chart with three categories: 'Address' (2), 'File' (2), and 'URL' (1). Below the preview, the 'Chart Type' section shows 'Tree Map' selected with a checkmark.

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.



Attributes +

Search attribute value... 🔍

**Pinned Attributes**

Adversary Motivation Type ✓ ✗

Attribute Type	Adversary Motivation Type
Security Labels	<input type="text" value="TLP:CLEAR"/> <span>✗</span>
Attribute Source	ET Intelligence <span>📄</span> <span>▼</span>
Value	<input type="text" value="State Sponsored"/> <span>15 / 100</span>

Last Modified: 12-21-2022 12:23 GMT-6

*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.<sup>2</sup> 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.

<sup>2</sup> CAL™ is a trademark of ThreatConnect, Inc.



### GeoLocation Data

<b>Location</b>		<b>Network</b>	
Country	United States	Organization	MICROSOFT-CORP-MSN-AS-BLOCK
Country Code	US	ASN	8070
State	Virginia		
City	Boydton		
Time Zone	America/New_York		

**CAL™ Provider Information**

IP Owner	-
IP Owner Region	-
IP Owner Service	-

### DNS Resolution

Resolved	Resolution
11-15-2022 22:05 GMT-6	k5kcubuassl3airf7gm3.appsync-api.eu-west-1.avsvmcloud.com
11-14-2022 21:35 GMT-6	k5kcubuassl3airf7gm3.appsync-api.eu-west-1.avsvmcloud.com
11-08-2022 20:35 GMT-6	gq1h856599qh538acqn.appsync-api.us-west-2.avsvmcloud.com
11-07-2022 21:30 GMT-6	k5kcubuassl3airf7gm3.appsync-api.eu-west-1.avsvmcloud.com
11-01-2022 20:35 GMT-5	k5kcubuassl3airf7gm3.appsync-api.eu-west-1.avsvmcloud.com
10-30-2022 19:26 GMT-5	gq1h856599qh538acqn.appsync-api.us-west-2.avsvmcloud.com
10-30-2022 17:46 GMT-5	6a57k2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud.com
10-30-2022 16:06 GMT-5	mhdosoksaccf9snl9icp.appsync-api.eu-west-1.avsvmcloud.com
10-30-2022 12:47 GMT-5	ihvpgv9psvq02ffo77et.appsync-api.us-east-2.avsvmcloud.com
10-29-2022 20:15 GMT-5	k5kcubuassl3airf7gm3.appsync-api.eu-west-1.avsvmcloud.com

1 - 10 of 533

### Attributes

Search attribute value...

**Pinned Attributes**  
No pinned attributes to display

**Other Attributes**

### Playbooks

Name

No applicable playbooks to display

### Owners & Feeds

**Additional Owners**

Owner	ThreatRating	Confidence Rating
<a href="#">Technical Blogs and Reports</a>	🔴🔴🔴🟡	0
<a href="#">Recorded Future Risk List</a>	🔴🔴🔴🟡	50
<a href="#">ThreatConnect Intelligence</a>		

**CAL™ Feeds**

Feeds Reporting this Indicator

First Reported in a Feed

Last Reported in a Feed

Number of Feeds Reporting this Indicator

### Observations, False Positives, & Impressions

Report False Positive

**Local Instance**

<b>Observations</b>		<b>False Positives</b>	
Total	136	Reported	0
Last Observed	03-13-2022	Last Reported	-

Please configure an API account to appear in the Observations and False Positives Report. [Org Settings](#)

**Global CAL™**

Trends

7 days  30 days

Daily False Positives  Daily Impressions  Daily Observations

<b>Observations</b>		<b>False Positives</b>	
Last Observed	02-19-2021	Last Reported	-
All Time	5	All Time	0
Previous 7 Days	0	Previous 7 Days	0

**Impressions**

All Time	249
Previous 7 Days	0
Today	0

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).<sup>3</sup>
- 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.

---

<sup>3</sup> 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

2023-05-31 7.0.2h [Latest]

## Bug Fixes

- An issue causing Playbook execution delays was fixed.

2023-05-23 7.0.2g

## Bug Fixes

- A certain custom Organization role configuration was not providing expected permissions for editing Notes and adding Artifacts in Workflow Cases. This issue has been resolved.
- When filtering Workflow Cases, the reported total number of results returned was not matching the actual number of Cases returned. This issue was fixed.

2023-05-19 7.0.2f

## Bug Fixes

- An issue causing an out-of-memory error to occur when using the v2 API to retrieve Indicators by a Tag that is assigned to a very large number of Indicators was fixed.
- An issue causing **GET** requests to **/v3/security/users** not to return a full set of details to API users was fixed.

2023-05-09 7.0.2e

## Bug Fixes

- A memory leak caused by completed Playbooks with Components or Iterators not clearing from internal collections was fixed.



## 2023-04-13 7.0.2c

### Bug Fixes

- An issue causing memory leaks leading to out-of-memory errors to occur when using Playbooks containing Delay Operators or Apps that have a Retry Flag has been resolved.

## 2023-03-28 7.0.2b

### Bug Fixes

- An issue causing abnormally long Playbook execution times has been fixed.

## 2023-03-22 7.0.2a

### Bug Fixes

- An issue causing the **Playbooks** card not to be displayed on the new **Details** screen has been resolved.

## 2023-03-09 7.0.2

### Improvements

- In some multi-server deployments, certain screens, such as the Playbooks **Activity** screen, may not function properly because of networked blocked app message broker hosts. This enhancement supports a graceful fallback mechanism to allow the ThreatConnect UI to connect to the main application server.
- Batch import no longer deletes documents in OpenSearch® one by one before re-importing.<sup>4</sup> It now uses a proper batch API to delete documents in OpenSearch.

---

<sup>4</sup> OpenSearch® is a registered trademark of Amazon Web Services.





## Bug Fixes

- An issue preventing Apps in Playbook Components using an Environment Server from receiving variables has been resolved.
- Attributes that display a Pivot icon on the legacy Details screen now display a Pivot button on the new Details screen.
- Checkboxes for enabling Whois lookups and DNS tracking were added to the **Whois** and **DNS Resolution** cards, respectively, on the new **Details** screen for relevant Indicator types.
- The value of the **#trg.tc.username** output variable for Case Triggers is now the username of the Case's assignee.
- On Dashboard Indicator and Group metric cards, clicking on multi-word object types (e.g., Course of Action, Email Address) has been causing a **Browse** screen filter with no or incorrect data to be displayed. This issue has been fixed.
- The default response for **PUT** and **POST** operations on certain v3 API endpoints has been updated to include a limited set of fields. Additional fields may be included in the response by using the **fields** query parameter. This change resolves an issue that was causing **PUT** and **POST** operations to have lengthy run times. The following v3 API endpoints were affected by this change:
  - /v3/artifacts
  - /v3/cases
  - /v3/groups
  - /v3/indicators
  - /v3/tasks
  - /v3/victims
  - /v3/workflowEvents
  - /v3/workflowTemplates
- An issue preventing Read Only Commenters from being able to add a Note on the new **Details** screen for a Task Group was fixed.
- An issue causing updates to the **Description** field on the **Details** card on the **Overview** tab of the new **Details** screen to update the **Last Modified** timestamp for all of the object's Attributes has been fixed.
- The data returned from the **OPTIONS** method have been updated for multiple v3 API endpoints.
- An issue causing excessive memory usage on some instances has been resolved.
- **Event Date** and **Status** fields have been added to the **Details** card of the **Overview** tab of the new **Details** screen for Event and Incident Groups.



- An issue causing Attribute filters to be removed from the **Browse** screen when a string search is applied was resolved.
- Super Users can now save Workflows to Organizations other than their home Organization.
- An issue causing invalid results to be returned on the **Browse** screen when clicking on the bar of a graph in a new Dashboard query card involving the **createdBy** Grouping for Groups has been resolved.
- Previously, when editing an Attribute on the new **Details** screen, there was no way to save a new source. A **Save Source** button has now been added.
- An issue causing URLs in Attributes to be displayed as live hyperlinks has been fixed.
- An issue causing extraneous logging to occur when configuring Indicator deprecation was fixed.
- An issue preventing Tag auto-completion suggestions from being offered on the new **Details** screen has been resolved.
- An issue causing incorrect values to be displayed in the **Used** column in the **Import License** section of **System Settings > Settings** after making changes such as adding certain user types has been fixed.
- After clicking on the **Learn more about it** link in the ThreatConnect search feature for an Indicator that does not exist in one of your owners and then clicking on the **Details** icon in the **Details** drawer that is displayed for the Indicator, the **Details** screen for a different Indicator was being displayed. This issue was resolved.
- An issue causing Whois data to be displayed on the new **Details** screen for Indicators for which Whois is not enabled has been resolved.
- Activation of a Workflow Playbook that is assigned to a Workflow Task and has reached the maximum number of versions was producing a foreign key constraint exception. This issue has been fixed.
- In some cases, Playbook Servers with a large number of Workers can have contention and slow execution around a logging resource for Apps (e.g., Logger) and all Playbook Operators. This issue has been resolved.
- An issue preventing Artifacts from being added to a Workflow Task via the v3 API has been resolved.
- An issue causing Playbooks containing certain Group Triggers with filters for specific Tag names to execute when any Tag is applied to a Group of the Trigger type has been resolved.
- Lists of Organization variables in Playbook App configurations are now scrollable.



## 2023-02-15 7.0.1a

### Improvements

- An issue causing an application error to occur when attempting to create associations to Groups from the new **Details** screen has been fixed. This issue was occurring only when working in an Organization with the Workflow feature disabled.
- An issue causing Tags not to provide autocomplete options or to provide autocomplete options for Tags that did not exist on the user's instance was resolved.
- An issue causing URLs to render as active hyperlinks on the **Attributes** card and in the **Description** section of the **Details** card on the **Overview** tab of the new **Details** screen was fixed.
- An issue causing all Attribute timestamps to update when the **Description** Attribute in the **Details** card on the **Overview** tab of the **Details** screen is updated was resolved.

## 2023-02-08 7.0.1

### 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.
- 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.