



ThreatConnect.



NETWITNESS

# ThreatConnect® Release Notes

## Software Version 7.5

March 27, 2024

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

P: 1.800.965.2708 | F: 703.229.4489  
[www.ThreatConnect.com](http://www.ThreatConnect.com)



ThreatConnect® is a registered trademark of ThreatConnect, Inc.

OpenSearch® is a registered trademark of Amazon Web Services.

Docker® is a registered trademark of Docker, Inc.

AlmaLinux OS™ is a trademark of Linux Foundation.

Java® is a registered trademark of Oracle Corporation.

Python® is a registered trademark of Python Software Foundation.

Redis® is a registered trademark of Redis Ltd.



# Table of Contents

---

<b>New Features and Functionality</b>	<b>4</b>
Report Templates	4
Details Screen Custom View	10
<b>Improvements</b>	<b>13</b>
Threat Intelligence	13
API & Under the Hood	14
<b>Bug Fixes</b>	<b>15</b>
Threat Intelligence	15
API & Under the Hood	15
<b>Dependencies &amp; Library Changes</b>	<b>16</b>
<b>Maintenance Releases Changelog</b>	<b>17</b>



# New Features and Functionality

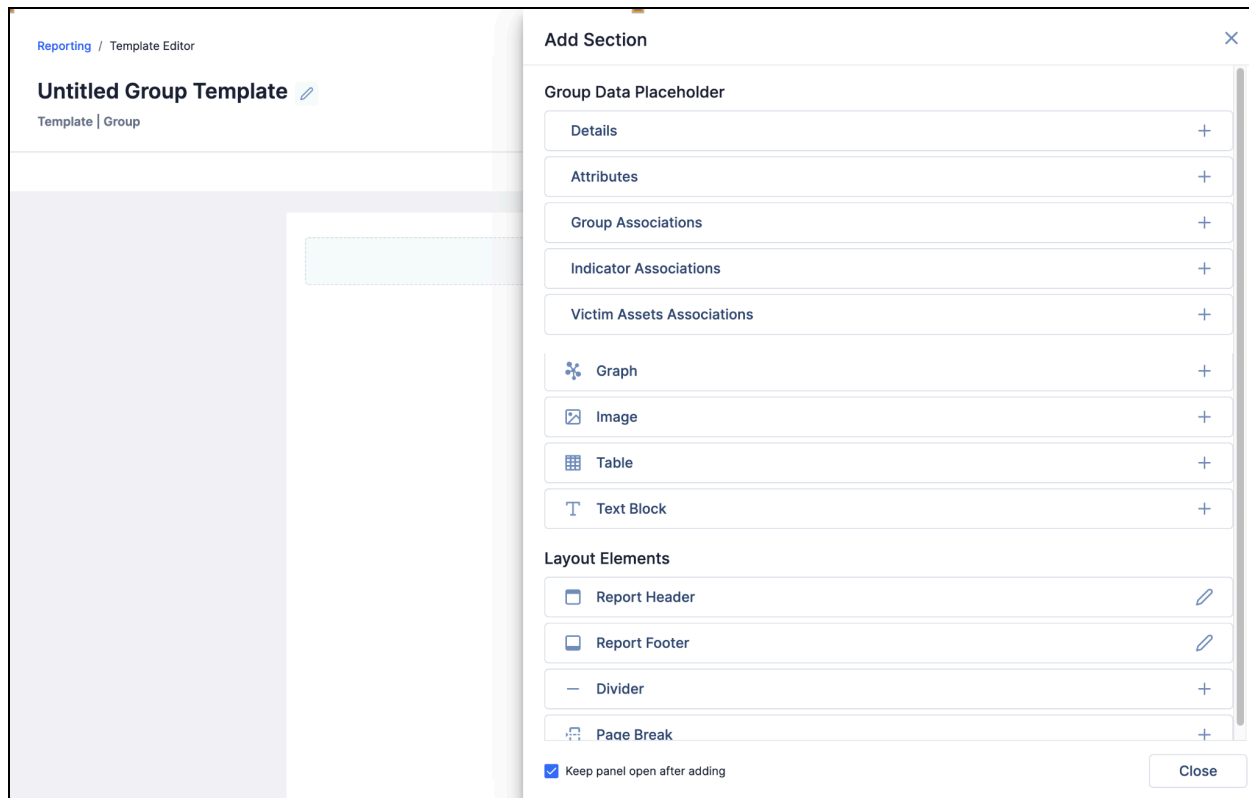
## Report Templates

Creating reports from scratch can be time consuming and challenging. That's why ThreatConnect® 7.5 introduces **report templates**, a feature designed to simplify and expedite the reporting process for you. Report templates allow you to define a standard format users can follow when they create reports in ThreatConnect, ensuring consistency across your team's reports and eliminating time spent creating reports from scratch. When building a report template, you can add content blocks with preconfigured text or visual elements, such as charts, images, tables, and saved graphs from Threat Graph, or placeholder sections that users can fill in after they create a report from the template.

In this release, we empower you with the capability to create Group report templates, which users in your Organization can employ when creating a report for a Group from the Group's **Details** screen.

To create a report template, navigate to the **Reporting** screen and click the **+ Create Group Template** button at the top right. The **Template Editor** will be displayed with a blank report template for Groups, including placeholder **Report Header** and **Report Footer** sections. From here, you can add sections from the following three categories:

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

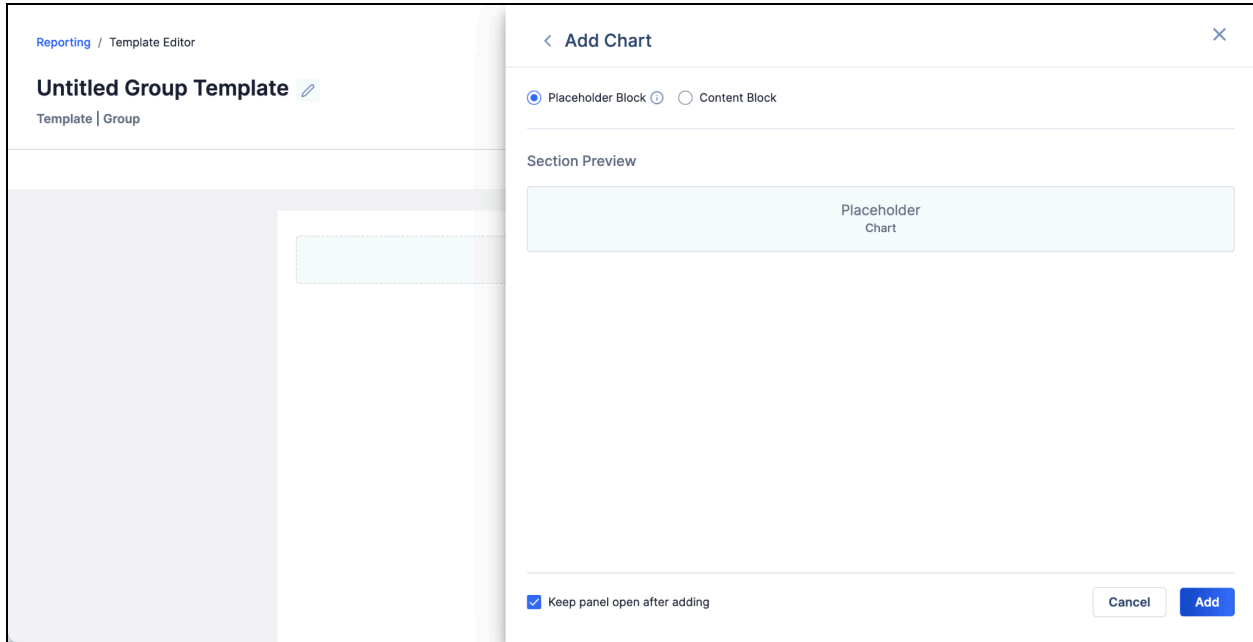


*Add content to your report template from the **Add Section** drawer*

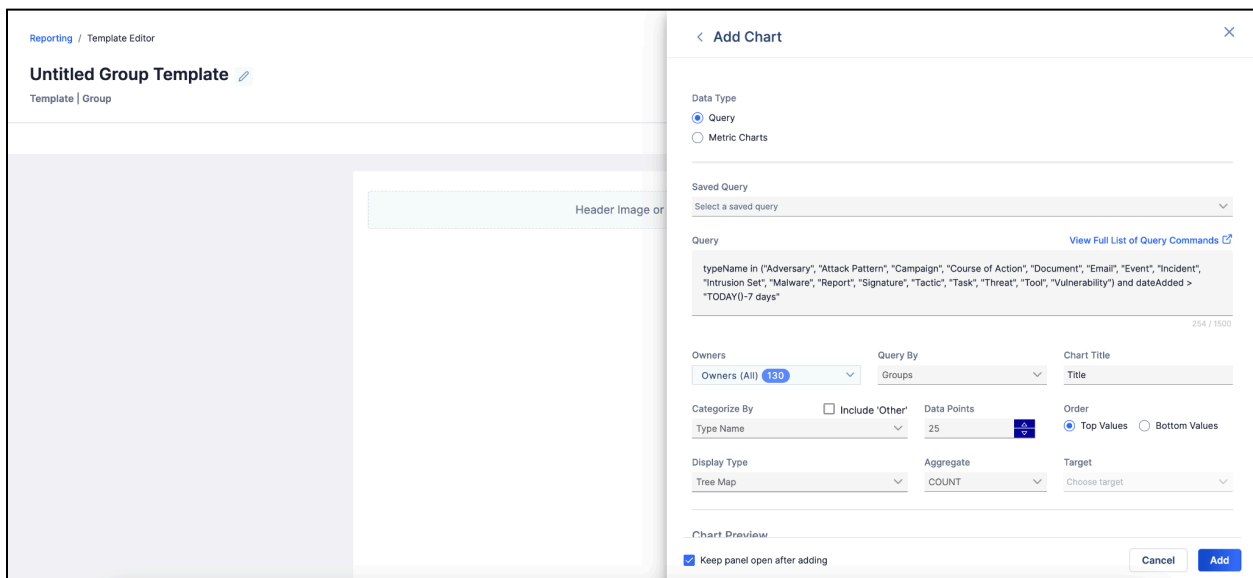
Each item in the **Group Data Placeholder** category enables you to add a placeholder block to the report template. When a user creates a report from the template for a Group, the information specific to that Group will be automatically inserted into the report, with the exception of the **Attributes**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



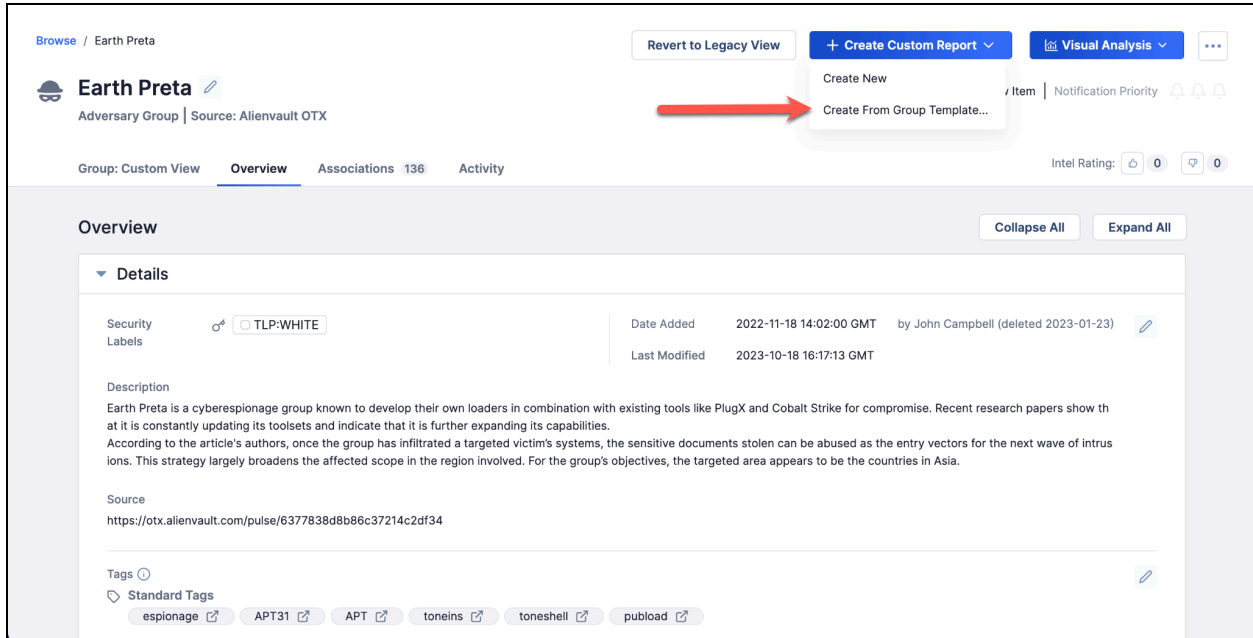
*Add placeholder blocks to direct users to add data into reports*



*Add content blocks to insert predefined data in a report 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 new **Templates** tab on the **Reporting** screen.

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



The screenshot displays the 'Earth Preta' group details page. At the top right, there is a '+ Create Custom Report' dropdown menu with a red arrow pointing to it. The dropdown menu is open, showing options: 'Create New', 'Create From Group Template...', and 'Create From Report Template...'. Below the menu, there are buttons for 'Revert to Legacy View' and 'Visual Analysis'. The main content area shows the 'Overview' tab selected, with a 'Details' section expanded. The 'Details' section includes fields for 'Security Labels' (TLP:WHITE), 'Date Added' (2022-11-18 14:02:00 GMT), 'Last Modified' (2023-10-18 16:17:13 GMT), 'Description', 'Source' (https://otx.alienvault.com/pulse/6377838d8b86c37214c2df34), and 'Tags' (Standard Tags: espionage, APT31, APT, toneins, toneshell, pubload).

### *Create a report for a Group from a Group 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.



Reporting / Custom Report Editor

Save Custom Report Publish Report

CUBA Custom Report

Preview PDF + Add Section

**Details** CUBA

Type: Malware  
 Owner: CAL Automated Threat Library  
 Security Labels: No security labels  
 Date Added: 2023-11-16 18:41:00 GMT  
 Last Modified: 2023-11-16 18:41:00 GMT  
 Tags: No tags

+ Add Above
Placeholder  
Group Data - Attribute
+ Add Below

**Group Associations** CUBA 1-5 of 5

Type	Name	Score	Status	Date Added	Last Modified
Report	Microsoft Rel...		Awaiting Upl...	07-11-2023	07-12-2023
Report	Microsoft: Un...		Awaiting Upl...	07-11-2023	07-12-2023
Report	RomCom Spi...		Awaiting Upl...	07-11-2023	07-12-2023
Report	Russia-Linke...		Awaiting Upl...	07-11-2023	07-12-2023
Report	RomCom hac...		Awaiting Upl...	07-10-2023	07-12-2023

*Placeholder blocks remind you to configure data for 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 exported in PDF or HTML format.



## 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.

**Top 10 tags used in Last 7 days**

file and directory discovery 141	data encrypted for impact 128	blog: dark reading 59	screenconnectwise 52
blog: red packet security ransomware feed 131	phishing 119	phishing: spearphishing attachment 51	software discovery: security software discovery 47
		phishing: spearphishing link 51	

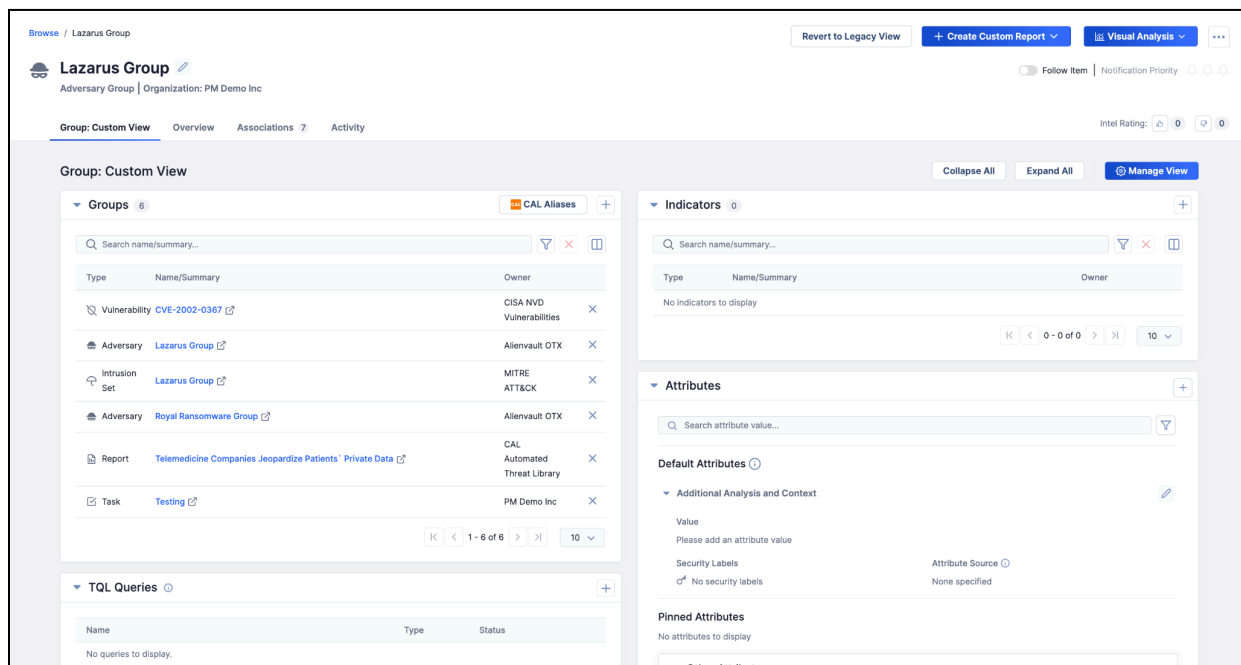
**Top 10 Indicators** 1-10 of 3789

Type	Summary	Owner	Added	Modified
🔗 Address	13.248.21...	PM Demo ...	02-28-2024	02-28-2024
🔗 Address	88.119.161...	CAL Auto...	03-02-2024	03-04-2024
🔗 Address	169.239.12...	CAL Auto...	03-02-2024	03-04-2024
🔗 Address	149.248.14...	CAL Auto...	02-22-2024	03-04-2024
🔗 Address	185.172.12...	CAL Auto...	02-29-2024	03-04-2024
🔗 Address	1.9.31	CAL Auto...	02-20-2024	03-05-2024
🔗 Address	108.61.86.1...	CAL Auto...	02-22-2024	03-04-2024
🔗 Address	79.137199...	CAL Auto...	03-02-2024	03-04-2024
🔗 Address	2.58.15.58	CAL Auto...	03-02-2024	03-04-2024
🔗 Address	5.39.221.47	CAL Auto...	03-02-2024	03-04-2024

*Report generated from a template with content blocks*

# Details Screen Custom View

As part of our ongoing effort to enhance the ThreatConnect user experience, in version 7.5 we are releasing version 1 of our new custom view for the **Details** screen. This new tab, available on Indicator and Group **Details** screens, enables you to select the cards you want to see and arrange them on the tab in the way that works best for you. This feature puts the layout of the **Details** screen in your hands, making it easier to highlight the information you find most valuable so you can make decisions faster.



Sample *Custom View* tab on a Group's *Details* screen

The screenshot displays the 'Indicator: Custom View' interface for the indicator '20.140.0.1'. The interface is organized into several sections:

- Header:** Shows the indicator ID '20.140.0.1', organization 'PM Demo Inc', and navigation options like 'Revert to Legacy View' and 'Explore in Graph'.
- Indicator: Custom View:** Contains a search bar and a table of groups.
 

Type	Name/Summary	Owner
Vulnerability	CVE-2021-44228	PM Demo Inc
Event	VT	PM Demo Inc
- VirusTotal:** Provides an overview of the indicator's status, including score (0/91), tags (N/A), domain name (N/A), country (US), and ASN (8070). It also shows first and last seen/referenced dates.
- Indicators:** A table listing various indicators associated with the main indicator.
 

Type	Name/Summary	Owner
Host	039n5tmdkhrfn5cun0y0sz02hj0b12.appsync-api.us-west-2.avsvmcloud.c...	PM Demo Inc
CIDR	178.162.192.0/16	PM Demo Inc
Address	178.162.203.225	PM Demo Inc
Address	178.162.217.109	PM Demo Inc
Host	1on45q99h4l7bg0cdae2sd02e2h.appsync-api.us-west-2.avsvmcloud.com	PM Demo Inc
Host	3263jc0g7ka370gmctjev.appsync-api.us-east-2.avsvmcloud.com	PM Demo Inc
Host	45au93jhkc27l6liq35.appsync-api.us-west-2.avsvmcloud.com	PM Demo Inc
Host	48vt0ms1tvg0pvlfp2ajz2v0ee25p.appsync-api.us-east-2.avsvmcloud.com	PM Demo Inc
Host	4981veeq1eq1q47iqvia.appsync-api.eu-west-1.avsvmcloud.com	PM Demo Inc
Host	4l7rgeqkrdb9jgf66n0l6l0teu.appsync-api.us-east-1.avsvmcloud.com	PM Demo Inc
- Intelligence Requirements:** A section at the bottom showing 0 requirements.

Sample *Custom View* tab on an Indicator's *Details* screen

Separate custom views are available for Indicator and Group **Details** screens and can be set as the default tab for each object type if desired, so that when you navigate to the **Details** screen, you will be directed to the **Custom View** tab instead of the **Overview** tab. Custom views are currently configured at the user level so that each user can customize their **Details** screen to their own preferences. In the future, we plan to enable you to import and export views so that they can be shared between users.

When configuring your custom view for Indicators or Groups, you can select cards from the **Overview**, **Associations**, and, for Indicators only, **Enrichment** tabs and place them according to several columned-layout options.

### Manage View ✕

Set this custom tab as the default tab for all Group details

---

Layout

2 Columns - 50/50 + Add Cards

- 1 Column - 100 🗑️
- 2 Columns - 50/50 🗑️
- 2 Columns - 60/40 🗑️
- 2 Columns - 40/60 🗑️

☰ Details 🗑️

☰ Indicator Associations 🗑️

☰ Attributes 🗑️

☰ Intelligence Requirement Associations 🗑️

☰ Notes 🗑️

Cancel Save

*Manage custom-view options by adding cards from across the **Details** screen tabs and placing them according to your preferred layout option*

Placing all the data you want to see for a Group or Indicator into one tab, arranged in the optimal layout for your needs, will help reduce the number of clicks necessary to find information in the platform and streamline your overall experience.



# Improvements

## Threat Intelligence

- The following changes were made to the **Attributes** card on the new **Details** screen:
  - The following sections will always be displayed on the **Attributes** card, even when a section has no Attribute data to display for an object:
    - **Default Attributes**: contains all default Attributes—except Description and Source, which are on the **Details** card—that have a value and placeholders for default Attributes that do not have a value;
    - **Pinned Attributes**: contains all pinned Attributes that have a value and are not default Attributes;
    - **Other Attributes**: contains all non-default, non-pinned Attributes that have a value.
  - Default Attributes apply across each object type in your Organization. For example, all Addresses have the same default Attribute Types, all Adversaries have the same default Attribute Types, etc.
  - All default Attributes without a value will have a placeholder displayed at the top of the **Default Attributes** section.
  - After you add a value to a default Attribute's placeholder, the Attribute will move to the bottom of the **Default Attributes** section.
  - When you delete the value for a default Attribute, a placeholder for the default Attribute will be moved to the top of the **Default Attributes** section.
  - Pinned Attributes are sorted in descending order based on the last modified date.
  - Pinning and unpinning Attributes will affect only the object whose **Details** screen you are viewing.
  - You can now do a keyword search for Attribute Type when adding an Attribute.
  - The **Default Attribute** checkbox has been removed from the **Add Attribute** window. Default Attributes can be set only in **Org Config > Attribute Preferences** or **Community Config > Attribute Preferences**.
- The character limit for the summary (name) of Group objects is now 200. When the summary is too long for its display area, you can hover over the part that is displayed to see a tooltip showing the entire name.
- A new configuration option was added to the **Data** tab of the **Contribute to Community/Source** window:

- **Ignore Hierarchy:** Select this checkbox to ignore [Group hierarchy rules](#) when associated Groups are copied.

## API & Under the Hood

- When using the `/v3/intelRequirements` API endpoint to create or update IRs, you can now specify an IR's category by name or ID. Previously, you could specify the IR's category by ID only.



# Bug Fixes

## Threat Intelligence

- Previously, when creating a Report Group without a document upload, the **Report File** card on the new **Details** screen would provide a different display, depending on whether the Report was uploaded via the ThreatConnect UI or the v3 or Batch API. Now the display is the same regardless of the creation method.
- Notifications for IR activity were not being displayed in the **Notifications Center**. This issue has been corrected.

## API & Under the Hood

- Fixed an issue where sending a PUT request with invalid data in the request body to the `/v3/security/users/{userId}` API endpoint would result in the user being updated with the invalid data, even though the API returned an error message. Also, new validation logic was added to the `/v3/security/users` endpoint for the `password` field, where this field is now required only when creating users and updating existing users without a password on ThreatConnect instances that do not have SAML enabled.
- An issue causing ATT&CK Tags to be excluded from v2 Batch API imports on HANA instances was fixed.
- An issue causing users without intel permissions to be logged out of ThreatConnect due to unnecessary permission checks was fixed.
- An issue causing an error to occur on the ContentPackService component when starting up the **tc-mon** server was resolved.
- The PDF viewer for Reports was modified to use internal resources only.
- An issue causing an error to occur repeatedly on systems with certain license configurations was fixed.
- Checks were added to prevent a null pointer exception from occurring.



# Dependencies & Library Changes

When installing ThreatConnect version 7.5.0 or newer, a containerized solution is now available using Docker® to simplify installations and reduce deployment times by packaging Java®, Python®, OpenSearch®, Redis®, and other supported dependencies together. The containerization deployment was tested on AlmaLinux OS™ version 9 and is the preferred method for all production and non-production systems starting with ThreatConnect version 7.5.



# Maintenance Releases Changelog

There have been no patch releases at this time. 7.5.0 is the latest version.