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

Table of Contents

New Features and Functionality

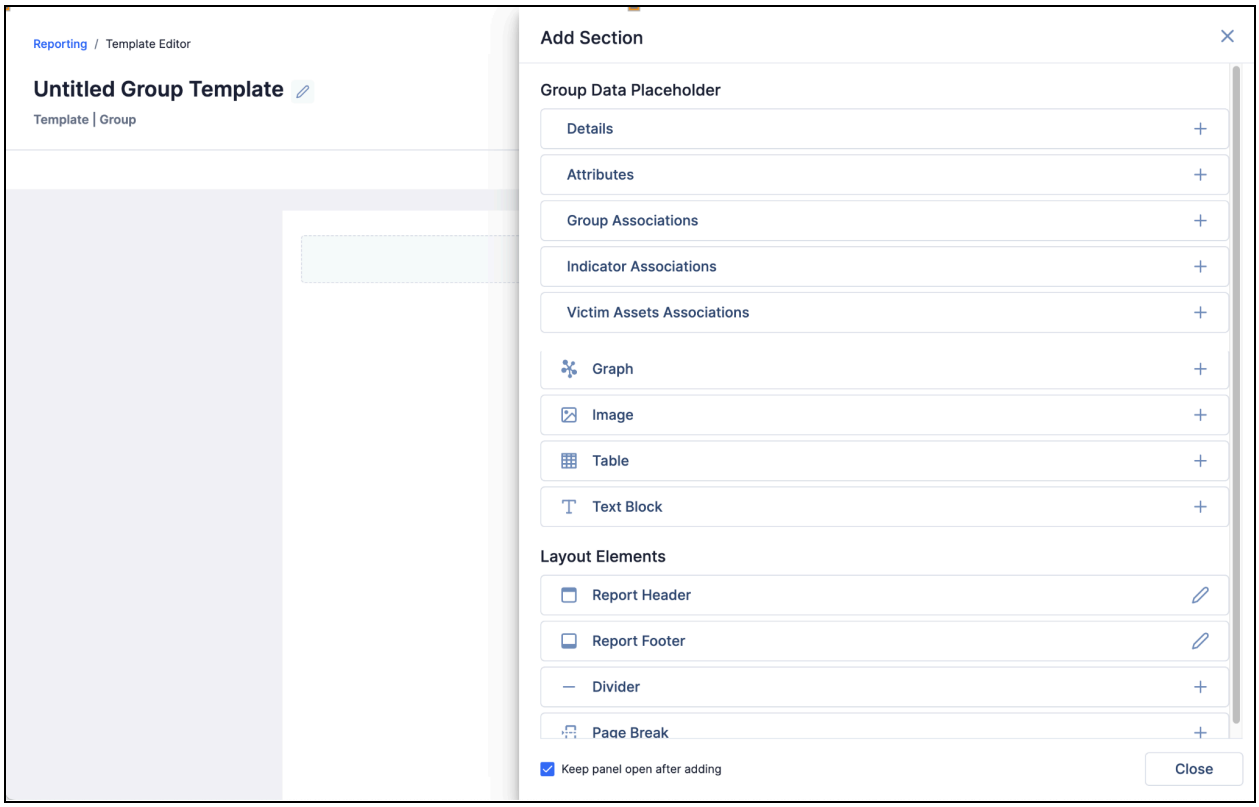
Report Templates

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.

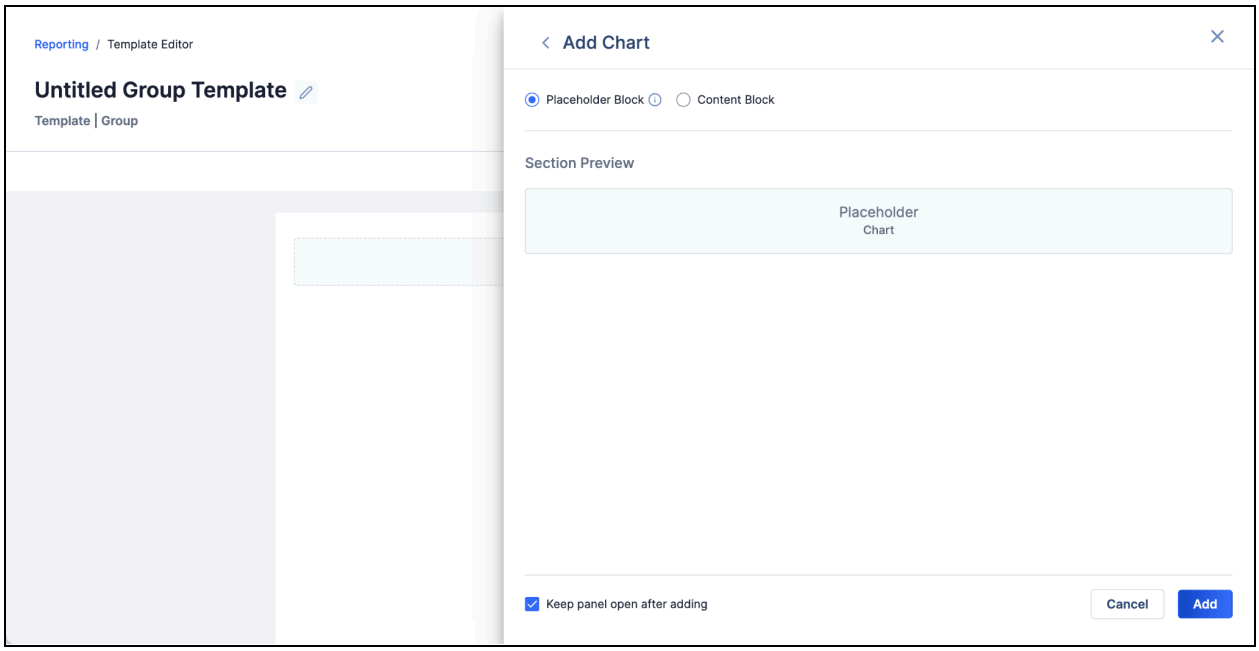


*Add content to your report template from the **Add Section** drawer*

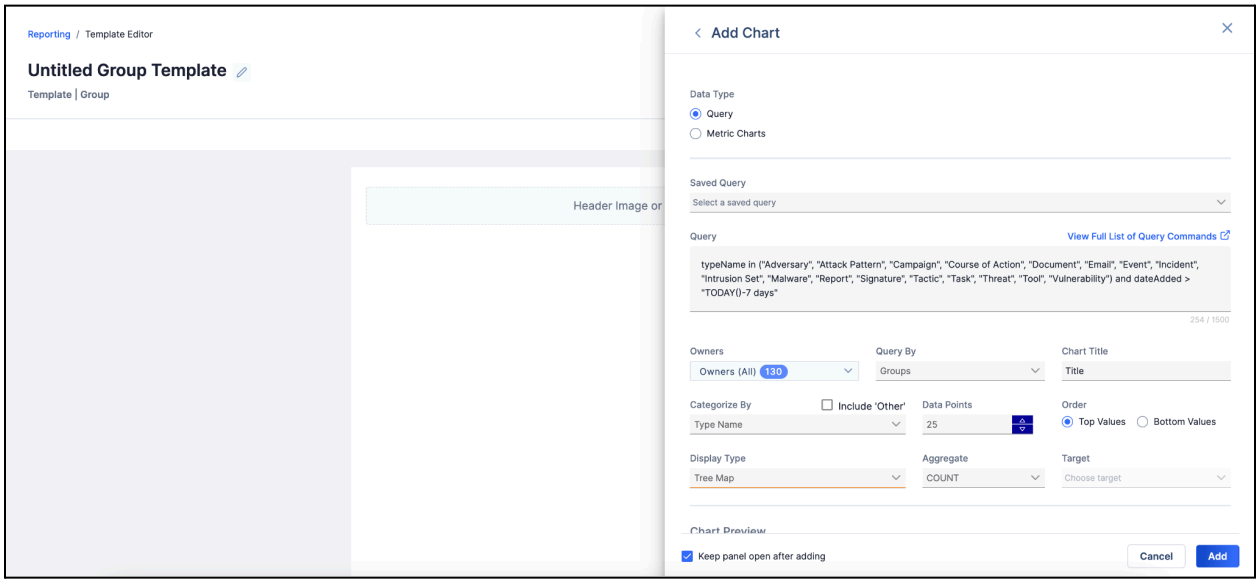
Each item in the **Group Data Placeholder** category enables you to add a placeholder block to the report template. When a user creates a report from the template for a Group, the information specific to that Group will be automatically inserted into the report, with the exception of the **Attributes**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



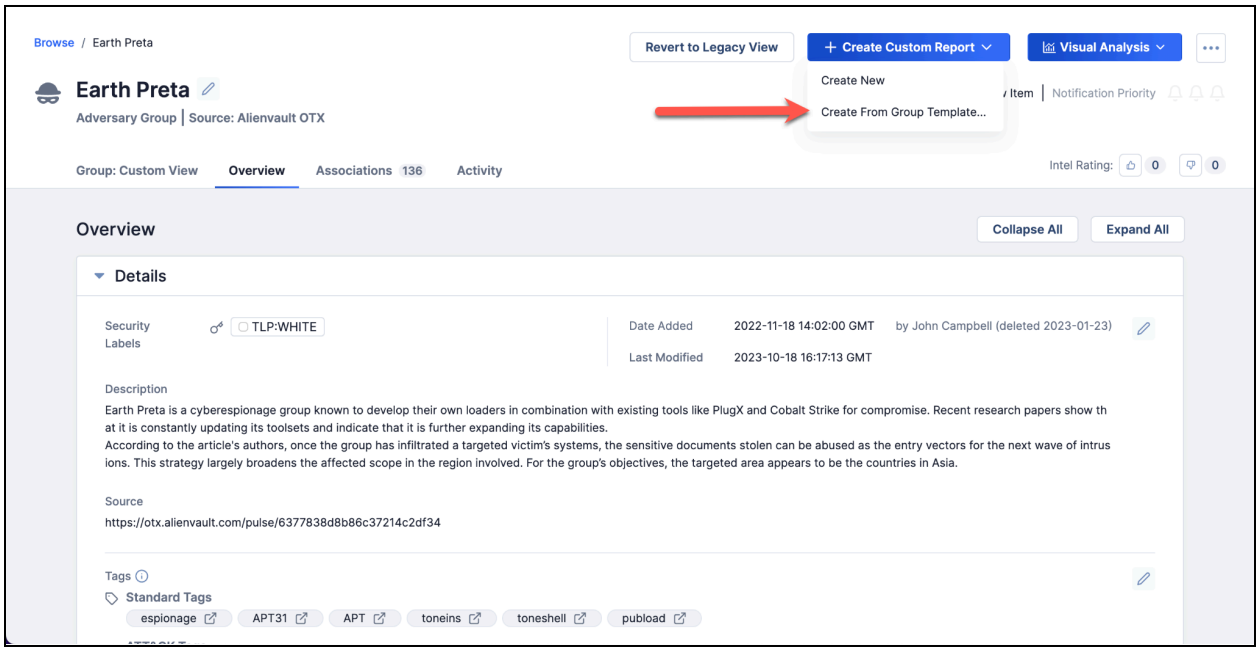
Add placeholder blocks to direct users to add data into reports



Add content blocks to insert predefined data in a report template

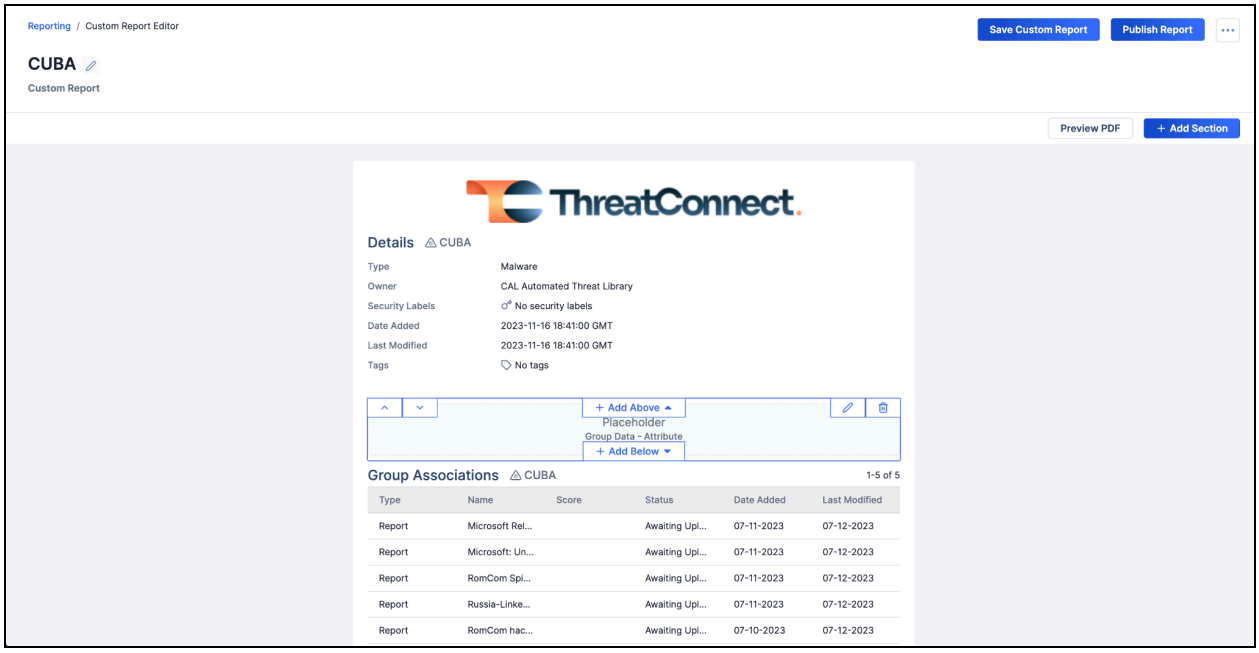
After you have finished creating your report template, click the **Save Template** button to save it. All saved templates can be accessed on the new **Templates** tab on the **Reporting** screen.

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.



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.



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.

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.

ThreatConnect.

Top 10 tags used in Last 7 days

Top 10 Indicators

1-10 of 3789

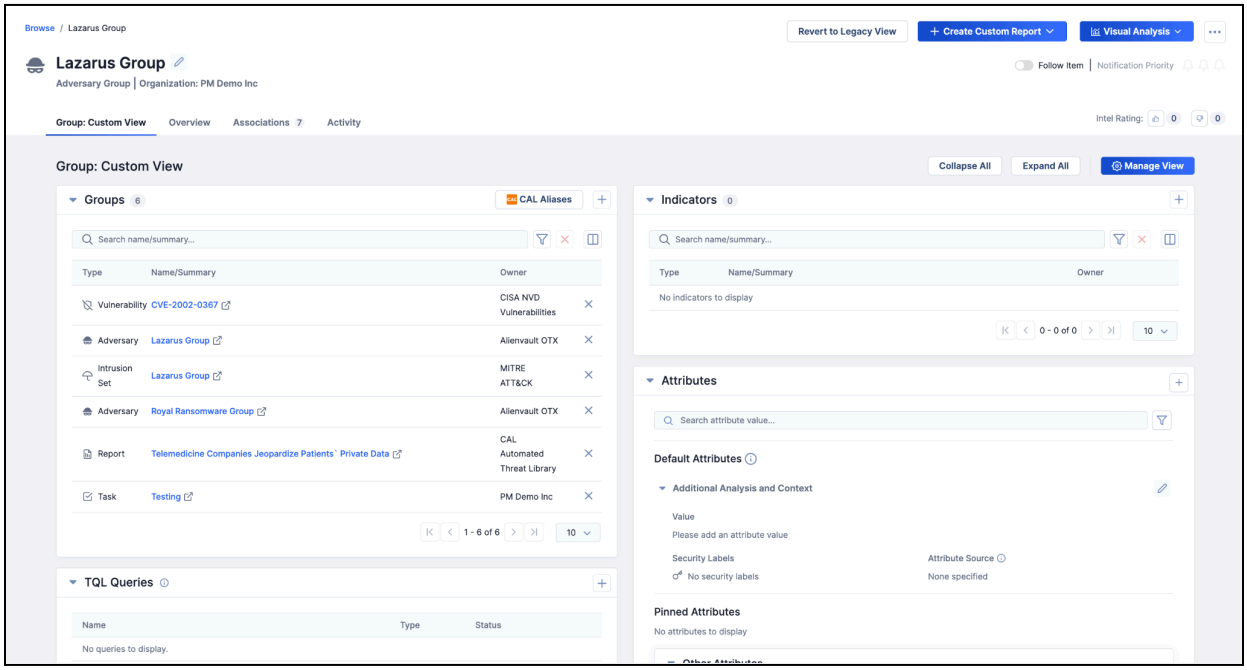
Type	Summary	Owner	Added	Modified
Address	13.248.21...	PM Demo ...	02-28-2024	02-28-2024
Address	88.119.161....	CAL Auto...	03-02-2024	03-04-2024
Address	169.239.12...	CAL Auto...	03-02-2024	03-04-2024
Address	149.248.14...	CAL Auto...	02-22-2024	03-04-2024
Address	185.172.12...	CAL Auto...	02-29-2024	03-04-2024
Address	1.9.3.1	CAL Auto...	02-20-2024	03-05-2024
Address	108.61.86.1...	CAL Auto...	02-22-2024	03-04-2024
Address	79.137.199....	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

2

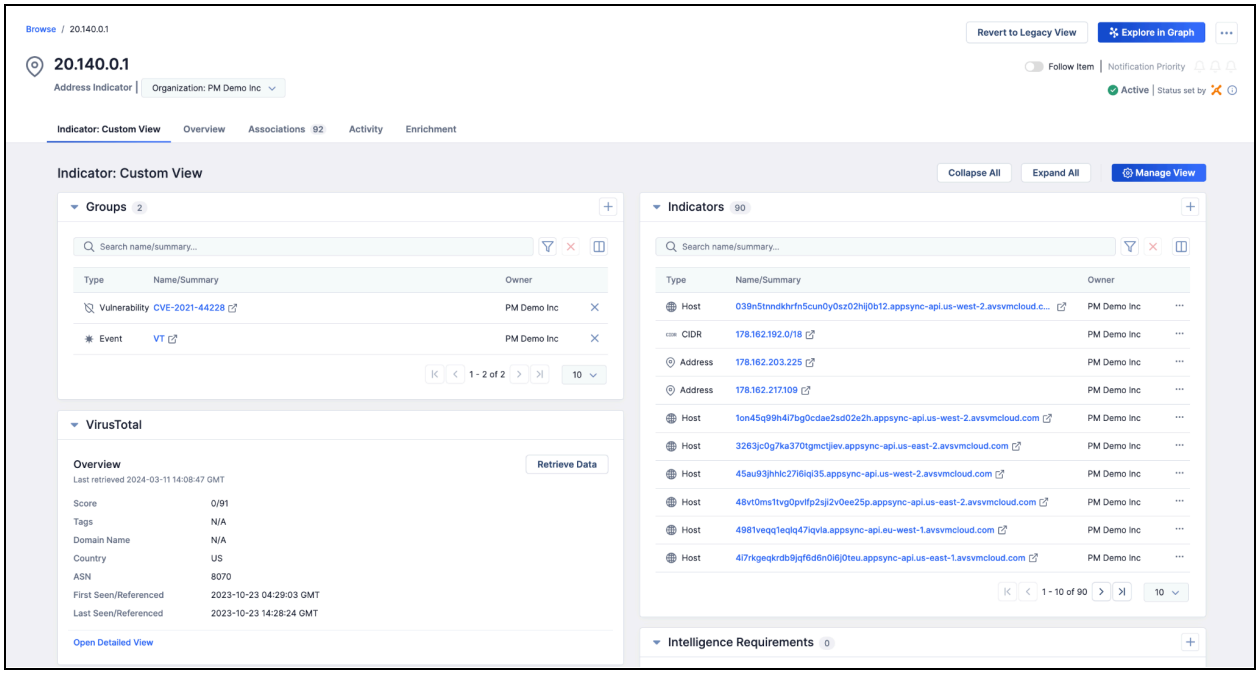
Report generated from a template with content blocks

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.



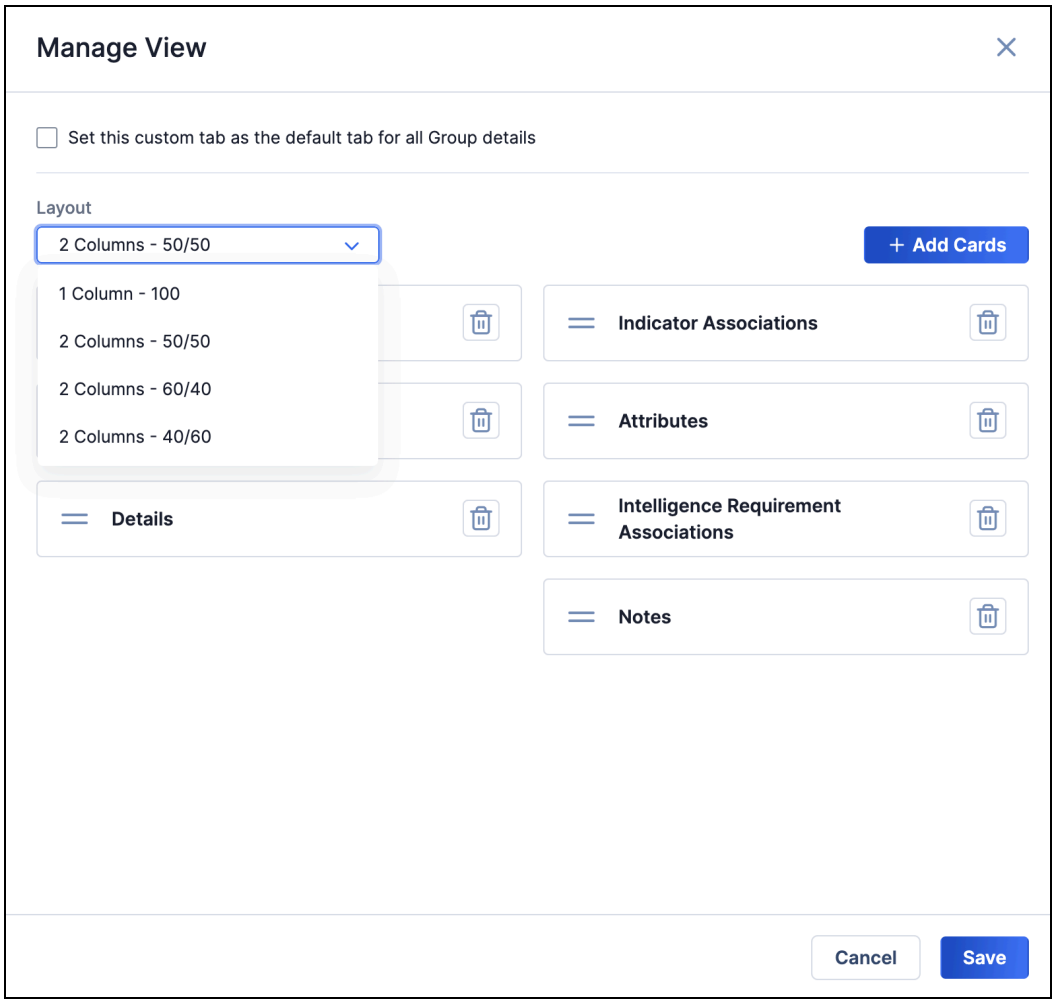
*Sample **Custom View** tab on a Group's **Details** screen*



*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 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

2024-05-09 7.5.2-M0509R [Latest]

Bug Fixes

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

2024-05-01 7.5.2

Improvements

- The following new system setting was added. This setting resolves an issue that was causing Playbooks for terminated App Builder debug sessions to remain on the Worker for up to 24 hours.
    - **appBuilderMaxDebugSessionMinutes**: The maximum amount of time, in minutes, that an App Builder debug session can run on a Worker before being terminated. App Builder debug mode should be used only in non-production ThreatConnect instances.

Bug Fixes

- Certain IR results being returned by dashboard Query cards were providing invalid hyperlinks. These hyperlinks have been removed.
- An error was occurring when sorting dashboard Query cards with IR results datatables by Type. This error has been fixed.
- When selecting a Tag name in the **FILTERS** selector on the **Browse** screen, the TQL generated for the strings “And” and “and” was causing invalid results to be returned. This issue was corrected.
- An issue preventing the **Description** field on the **Details** card of the **Details** screen from wrapping text containing Markdown was resolved.
- When configuring a custom Trigger in a Playbook, an issue was causing an incomplete list of available owners to be provided. This issue has been resolved.

- An issue preventing the Domain-Spinning Workbench Playbook Templates from being installed via the **TC Exchange Settings** screen was fixed.
- An issue preventing changes to Attribute order in Workflows from being saved was fixed.
- An issue preventing GET requests to the `/v3/tags` API endpoint for Tags applied to a Group or Indicator from returning Tags in a Community or Source was fixed.
- When using TQL to filter on owner names, entering a keyword that exactly matched to an owner name would cause other owners whose names were partial matches to be excluded. This issue has been resolved.
- An issue causing certain multiselect dropdowns for Playbook Triggers to erroneously display selected items when the Trigger is edited for the first time was resolved.
- Page-scrolling issues that occurred when displaying a Note associated with a Workflow Task were resolved.

2024-04-03 7.5.1

Improvements

- When returning AI insights for Report Groups in the CAL™ Automated Threat Library (ATL) Source via the v3 API, the `insights` field in the API response is now a JSON object that includes the following subfields: `summary`, `app`, and `bullets`. Previously, the value of the `insights` field in API responses was a string.
- The following new system setting was added:
    - **caseAssessMonitorEnabled**: This setting turns the Case ThreatAssess monitor off.

Bug Fixes

- On the **Details** screen, an issue was causing investigation links opened in a new tab to direct to an incorrect URL. This issue has been resolved.
- An error that was occurring when clicking on the **Groups** card on the **Associations** tab of the **Details** screen was fixed.
- For File Indicators containing a SHA256 value and that have multiple owners, the new **Details** screen was not displaying the Indicator's owner and owner list in the header. This issue has been fixed.
- An issue causing latency when contributing a Group to a Community or Source containing a large number of objects was fixed.

- An issue preventing certain Group types from being published after they were contributed to a Community or Source when ignoring Group hierarchy was fixed.
- An issue preventing the data copy algorithm from performing duplicate operations under certain circumstances was fixed.
- Playbooks using a retry property were getting stuck and not completing, but would appear to be running on the Worker on which they were executing. This issue was fixed.
- Enabling the CAL Status Lock for an Indicator will apply the lock only to the copy of the Indicator whose **Details** screen you are viewing. Other versions of that Indicator in other owners will not be affected.
- An issue causing the Case ThreatAssess monitor to reopen closed cases during processing was fixed.
- An issue causing the color scheme and scores for a saved imported ATT&CK view to be removed after the ATT&CK view's metadata were edited has been fixed.
- An issue causing entries in the **Notifications Center** to link to the wrong object was fixed.
- All functionalities and buttons that should not be accessible to Read Only Users are no longer visible to these users in the UI.
- Previously, Groups with the same summary (name) associated to a Workflow Case were all being listed together under one of the Group types on the Case's **Associations** card. Now, they are listed separately, each under its own Group type.
- An issue causing the display of Playbook audit logs to be inconsistent was fixed.

CAL Updates

2024-04-29 CAL 3.7 [Latest]

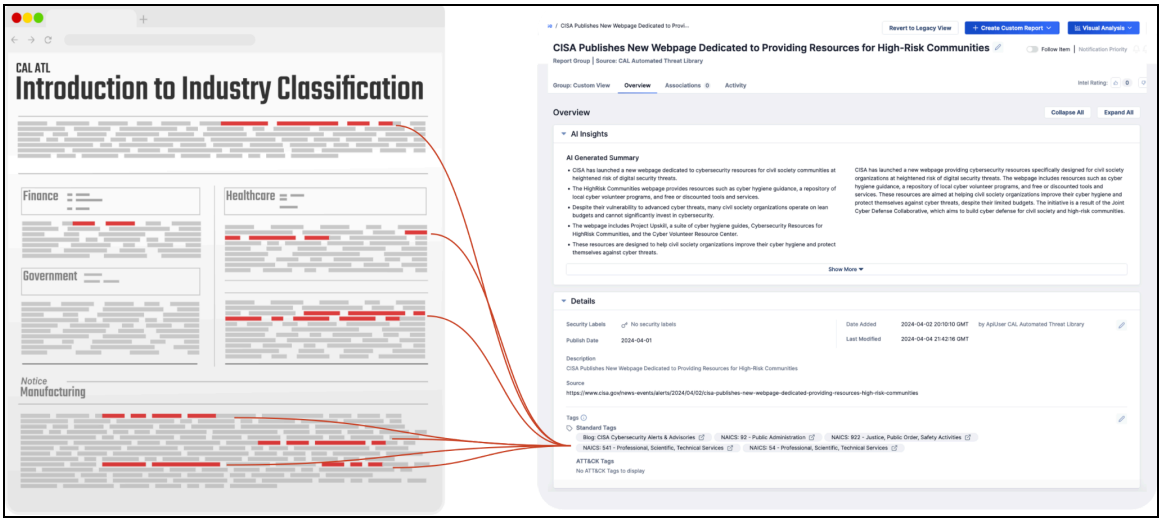
New Features

CAL ATL Industry Classification

It can be overwhelming and difficult to sift through cybersecurity intelligence reports and blogs that offer valuable information to organization defenders. Not all information is relevant to your organization's industry-specific security needs and structures.

CAL ATL industry classification uses natural language processing (NLP) to classify ATL Reports by industry, creating machine-readable components that can be leveraged throughout ThreatConnect via industry Tags that you can pivot on, including in Threat Graph, and as industry-based keyword suggestions for IRs. You can use these Tags and keyword suggestions to streamline your CTI analysis in a number of ways, including the following:

- Use industry characteristics to prioritize the most essential CAL ATL Reports for review.
- Save time by removing irrelevant content from queries and IRs.
- Provide focused information that lets you stay on top of emerging industry topics and threats.
- Identify and leverage industry topics to make recommendations for funding and for your organization's cybersecurity controls, training, and awareness programs.



CAL ATL uses NLP to review ATL Report contents and identify relevant industries via Tags

ATL Blog Additions

Manually collecting and analyzing threat intelligence, especially unstructured data, from various sources is time consuming and error prone. CAL ATL automates, aggregates, and analyzes intelligence from more than 70 authoritative publishers generating open-source intelligence. AI and NLP automatically extract critical information into pivot points that can help you prioritize, filter, and highlight the most relevant information for your role and organization, such as Indicators; MITRE ATT&CK® tactics, techniques, and threat actor aliases; and Vulnerabilities from the National Vulnerability Database (NVD).

The following new sources are now included in CAL ATL:

- CERT-UA news (Ukrainian Language)
- CIS - Center for Internet Security (Advisories)
- CIS - Center for Internet Security (Alerts)
- Government of Canada Alerts and Advisories
- JPCERT Coordination Center Official Blog
- JPCERT (Japanese Language)
- Kyberturvallisuuskeskus - Alerts (Finnish Language)
- Kyberturvallisuuskeskus - Information Security Now! (Finnish Language)
- Kyberturvallisuuskeskus - Vulnerabilities (Finnish Language)
- NCSC Reports, Guidance and Blog-post
- RedPacket Security Posh C2
- RedPacket Security Pikabot C2
- The DFIR Report

Improvements

- Improvements were made to special-character handling in global IR results.
- Suggested MITRE ATT&CK keywords in IRs are now capitalized to align with the format of these terms in ATT&CK Tags.