



ThreatConnect® Release Notes

Software Version 7.11

October 16, 2025



ThreatConnect® is a registered trademark, and CAL™ and TC Exchange™ are trademarks, of ThreatConnect, Inc.

OpenSearch® is a registered trademark of Amazon Web Services.

VirusTotal™ is a trademark of Google, Inc.

Google® is a registered trademark of Google LLC.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.

Security Assertion Markup Language™ and SAML™ are trademarks of OASIS, the open standards consortium where the SAML specification is owned and developed. SAML is a copyrighted © work of OASIS Open. All rights reserved.



Table of Contents

New Features and Functionality	5
Threat Actor Profiles	5
Actionable Search Updates	8
Consolidated Bulk Indicator Search Results	9
Bulk Actions on Consolidated Indicators	10
Dashboard Enhancements	11
Group by ATT&CK Tags	11
Global Dashboard Date Range	14
Metric Cards	15
Query Cards	16
Improvements	18
Threat Intelligence	18
ThreatAssess	18
Built-In Enrichment	19
Threat Graph	19
Search	20
Details Screen and Drawer	20
My Account	20
My Pages	21
Playbooks	21
Dashboards	21
Services	22
Workflow	22
Reporting	22
Installation and Deployment	22
API & Under the Hood	22
Bug Fixes	24
Attributes	24
Playbooks	24
Services	24
Installation and Deployment	24
Dependencies & Library Changes	25
Maintenance Releases Changelog	26



2025-11-13 7.11.1 [Latest]	26
Improvements	26
Bug Fixes	26



New Features and Functionality

ThreatConnect 7.11 takes the themes established in version 7.10 around standardization, streamlined user experience, and focus and builds upon them substantially to help you work smarter, find what you need faster, and confidently take action. This release is packed with enhancements and new features focused on helping you do your job more efficiently so you can spend more time doing analysis and less time remembering things like all the aliases for a given threat actor group.

Threat Actor Profiles

The marquee feature in ThreatConnect 7.11 is Threat Actor Profiles. This feature addresses a significant challenge experienced by many threat intelligence analysts: having to keep track of all the names used by vendors to refer to a particular threat actor group. The Threat Actor Profiles feature leverages the extensive CAL™ dataset to automatically identify all known aliases for a given threat actor represented by Adversary, Intrusion Set, and Threat Group objects in ThreatConnect. It then looks across the data in your ThreatConnect owners and consolidates all available threat actor data for those aliases and displays that information on a single Threat Actor Profile **Details** screen, similar to how [the unified view for Vulnerability Groups aggregates Vulnerability data across ThreatConnect owners on a single Details screen](#). The Attributes and associations that exist for the individual objects are all captured in this profile page so that you can quickly gather available context and make faster decisions.



G0021

Molerats

Threat Actor Profile | Unified View ⓘ

Group: Custom View **Overview** Associations 189 Activity Copy

Overview

Details

Security Labels: TLP:AMBER TLP:CLEAR

MITRE ID: [G0021](#)

Date Added: 2022-01-24 11:10:20 GMT
Earliest: Molerats
Source: AlienVault OTX

Last Modified: 2025-10-07 22:25:55 GMT
Most Recent: Gaza Hackers Team
Organization: PM Demo Inc

MITRE Description
Molerats is an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States. (Citation: DustySky)(Citation: DustySky2)(Citation: Kaspersky MoleRATs April 2019)(Citation: Cybereason Molerats Dec 2020)

Tags

Tags ⓘ
Standard Tags

- CVE-2017-0199 1
- dropbox 1
- Gaza Cybergang 3
- Incident Type: Espionage 1
- Molerats 3
- molerats 1
- office macro 1
- Suspected State Sponsor: Palestine 1
- Suspected Victim: Europe 1
- Suspected Victim: Israel 1
- Suspected Victim: Middle East 1
- Suspected Victim: Palestine 1
- Suspected Victim: United States 1
- T1059.007 - Command and Scripting Interpreter: JavaScript/JScript 1

Show More ▾

Attributes ⓘ 50

Included Groups & Aliases

Type	Name/Summary	Owner
Intrusion Set	Gaza Cybergang	Docs Test Community
Intrusion Set	Gaza Cybergang	PM Demo Inc
Intrusion Set	Gaza Cybergang	Docs Test Community
Threat	Gaza Hackers Team	PM Demo Inc
Adversary	Molerats	VulnCheck Intelligence
Intrusion Set	Molerats	MITRE ATT&CK
Intrusion Set	Molerats	Mandiant Advantage Threat Intelligence
Adversary	Molerats	AlienVault OTX
Intrusion Set	MOLERATS	CAL Automated Threat Library

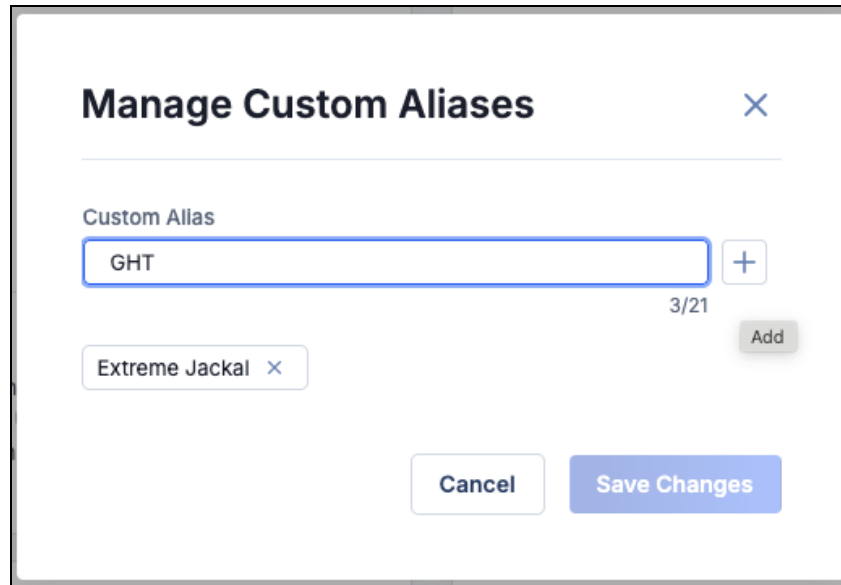
Aliases [Manage Custom Aliases](#)

MITRE Aliases ⓘ

- [Gaza Cybergang](#)
- [Molerats](#)
- [Operation Molerats](#)

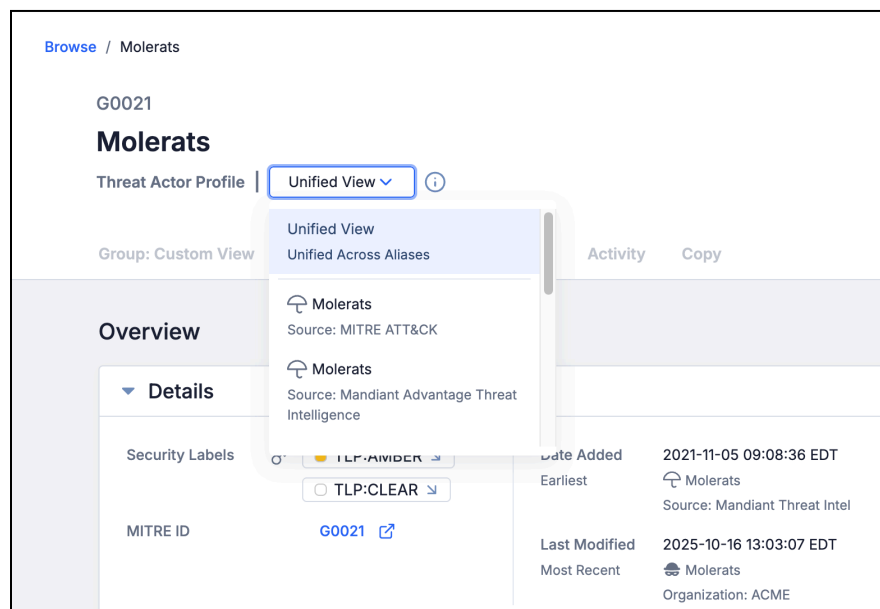
Threat Actor Profiles offer a unified view of threat data for Adversary, Intrusion Set, and Threat Groups representing the same actor with different aliases

Alias information from CAL is used for the initial consolidation. Once a Threat Actor Profile is created by the system, you can add custom aliases to it if you track the group under a different name or if a vendor releases another moniker for the threat. Names added as custom aliases are incorporated into the query used to connect the Groups included in the profile, which means that any Adversary, Intrusion Set, or Threat Group with a Name/Summary value matching any of the aliases (including custom aliases) that is subsequently added to your ThreatConnect owners will be included in the Threat Actor Profile.



Add and remove custom aliases from a Threat Actor Profile

If you want to view the **Details** screen for a version of one of the Groups included in a Threat Actor Profile—including the **Group: Custom View**, **Activity**, and **Copy** tabs, which are not available in the unified view—you can easily select the version's owner from the owner dropdown at the upper left.



You can select the unified view or a specific owner's version of an Adversary, Intrusion Set, or Threat Group included in a Threat Actor Profile

The unified view is shown by default for Groups that are part of a Threat Actor Profile. It is not available for Adversaries, Intrusion Sets, or Threats that do not have other Groups linked to



them via an alias recognized by CAL. If you do not want to see the unified view by default, you can disable this setting in the **Options** ... menu at the upper right of the Threat Actor Profile's **Details** screen. Note that the selection for this setting applies across all Threat Actor Profiles viewed from your user account. You cannot enable or disable it for individual Group objects, and your selection will not change the setting for other users on your ThreatConnect instance. And, of course, even if you disable the unified view as default, you can still see the unified view by switching to **Unified View** in the owner dropdown.

It's important to note that the correlation and aggregation of objects into Threat Actor Profiles does not involve any changes to the underlying data. The goal of this feature is to make it easier for you to get an understanding of what you know about a threat actor group and its activities while maintaining data integrity. Rather than having to search for every known alias and open each of those Group **Details** screens to read through the available context, you can now access all of this information in one place in a searchable, filterable format so that you can get to the point faster.

It may take a few days after upgrading to version 7.11 for all Threat Actor Profiles to be identified and consolidated. In particular, instances that have large amounts of data could experience delays in the availability of the unified view for Threat Actor Profiles as they complete the initial consolidation process. However, if you notice that Threat Actor Profiles are not available for eligible Groups after that period of time, please reach out to your Customer Success representative for assistance.

Important

Threat Actor Profiles are available on all ThreatConnect instances running version 7.11. You do not need to have CAL enabled to use this feature.

Actionable Search Updates

ThreatConnect 7.11 is packed with improvements to the bulk Indicator search feature that make it easier to find the data you're looking for. Among the updates are the ability to consolidate results for Indicators found in your ThreatConnect owners and to take bulk actions on consolidated Indicators. Continuing with the themes of standardization, streamlined experience, and focus, these feature updates eliminate the appearance of duplicates when you're searching for Indicators while maintaining the fidelity of the underlying data.



Consolidated Bulk Indicator Search Results

To ensure that your data are stored in a way that is true and traceable to the original source, separate versions of data objects are maintained in your [ThreatConnect owners](#). This segmented approach allows you to aggregate your data within a single system (i.e., a Threat Intelligence Platform) *and* identify where each piece of data came from. While this segmentation is great for maintaining the integrity of your sources and the analysis and enrichment they provide, it can be frustrating when you're looking for available information about an Indicator and find multiple copies in different owners that you have to correlate. When performing a bulk Indicator search of an uploaded file, this means that you will see results across a variety of owners, which in turn means your results set may be crowded with duplicates.

To solve this problem, ThreatConnect 7.11 provides the ability to enable deduplication of Indicators in bulk Indicator search results, allowing you to clear out all that noise and focus on a consolidated, easy-to-navigate results set. After you upload a file in bulk Indicator search, simply select **Enable Deduplication of Indicators** from the **Options** ... menu at the upper right of the screen. Your search results will then show a view where information on matching Indicators is consolidated into a single row for each Indicator. Once you select this setting, future searches will use the deduplicated view as the default—but you can always switch back to viewing each Indicator in its own row by selecting **Disable Deduplication of Indicators** from the **Options** ... menu.



The screenshot shows the ThreatConnect Search interface. At the top, there are navigation tabs: My Pages, Dashboards, Search & Create (selected), Tools, and Automation & Feeds. A search bar contains 'Search ThreatConnect...'. Below the search bar, there's a section for 'Bulk Search Indicators' with a search query 'ACR Stealer - Uncovering Attack Chains, Functionalities And IOCs.pdf' and a file icon. The search results are displayed in a table with columns: Type, Name/Summary, Owner, Tags, ThreatAssess, Date Added, and Last Modified. The results are consolidated into a single row for each unique indicator. A dropdown menu is open over the 'godfaetret.com' indicator, showing associated entities like 'CAL Automated Threat Library Source', 'Demo Data Community', and 'PM Demo Inc Organization'.

Type	Name/Summary	Owner	Tags	ThreatAssess	Date Added	Last Modified
Host Indicator	cybersecuritynews.com			Low 97		
Host Indicator	geotravelsgl.xyz		3	3	2025-09-15 08:00:03 GMT	2025-10-05 21:13:16 GMT
Host Indicator	godfaetret.com				2025-09-15 08:00:03 GMT	2025-10-05 21:13:13 GMT
Host Indicator	googleauthenticator.com				2025-09-15 08:00:03 GMT	2025-10-05 21:13:10 GMT
URL Indicator	https://cybersecuritynews.com/acr-stealer-uncovering-attack-chains/					
URL Indicator	https://geotravelsgl.xyz/ujjs/2ae					
URL Indicator	https://godfaetret.com/live/		4	6	2024-08-02 12:27:55 GMT	2025-10-05 21:13:34 GMT

Matching Indicators are consolidated into a single row in deduplicated bulk Indicator search results

Bulk Actions on Consolidated Indicators

As you further examine and investigate Indicators, you can select consolidated rows and take any of the following bulk actions available in the **Selection Actions** dropdown on the deduplicated Indicators:

- Add the Indicator to your Organization.
- Add Tags to the Indicators.
- Export the Indicators to a CSV file.

These actions make it easier for you to organize and manipulate your data so you can share key insights faster.



Type	Owner	Tags	ThreatAssess	Date Added	Last Modified
Address Indicator	2	10		2019-06-18 08:38:20 EDT	2025-08-21 04:26:29 EDT
Address Indicator	Technical Blogs ... Source	10	Medium 225	2019-06-18 08:38:16 EDT	2025-08-21 04:26:29 EDT
Address Indicator	Technical Blogs ... Source	14	Medium 225	2020-09-26 13:22:06 EDT	2025-08-20 21:40:10 EDT
Address Indicator	5	22		2021-10-14 06:28:06 EDT	2025-08-20 04:51:10 EDT
Address Indicator	4	17		2021-07-29 09:29:30 EDT	2025-08-19 21:43:22 EDT

Take bulk actions on deduplicated Indicators in your ThreatConnect owners identified in an uploaded file

Dashboard Enhancements

Group by ATT&CK Tags

You can now group your data by [ATT&CK Tags](#) when building Query charts in dashboards. This option can help you surface the most prevalent MITRE ATT&CK® techniques, look for the techniques used most often by particular threat actors, or keep an eye on trends in ATT&CK technique usage over time.

Group By

(Attribute) Adversary Motivation Type

Search...

Assignee Pseudonym (Task)
The pseudonym of the assignee of the task

ATT&CK Tag
The name of the ATT&CK Tag applied to a group

Created By
The user who created the group

Due Date (Task)
The due date of a task

Select **ATT&CK Tag** from the **Group By** options when building a Query chart in dashboards



To use this feature, select **ATT&CK Tag** in the **Group By** dropdown when creating or editing a Query card for a chart and complete the rest of the card's configuration, such as in the following example:

Edit Card [X]

Card Category: Query Card
Card Type: Custom Query Card

Card Title: Trending Attack Techniques - 7 days (35/255)
Display Type: Chart Table

Filters & Settings

Inherit dashboard-level owner selections

Owner: 71 Selected [X] [v]
Query By: Groups [v]

Advanced Query: typeName In ("Report") and dateAdded > "NOW() - 7 DAYS" [See syntax help...]

To make this query card obey the global dashboard date setting, replace the dates you wish to modify with \$startdate for the global start date and \$enddate for the global end date.

Group By: ATT&CK Tag [v]
Data Points: 10 [v]
Value Order: Top Bottom

Aggregate: Count [v]
Target: Select... [v] Include 'Other' [i]

Chart Display

Display Type: Vertical Bar Chart [v]
Color Scheme: ThreatConnect [v]
Scheme Type: Ordinal Linear
Card Width: 7 [v]
Card Height: 4 [v]

Bar Gap Size: 8 [v]
 Show x-axis [Optional label...]
 Show y-axis [Optional label...]
 Show legend [Legend]

Additional Settings

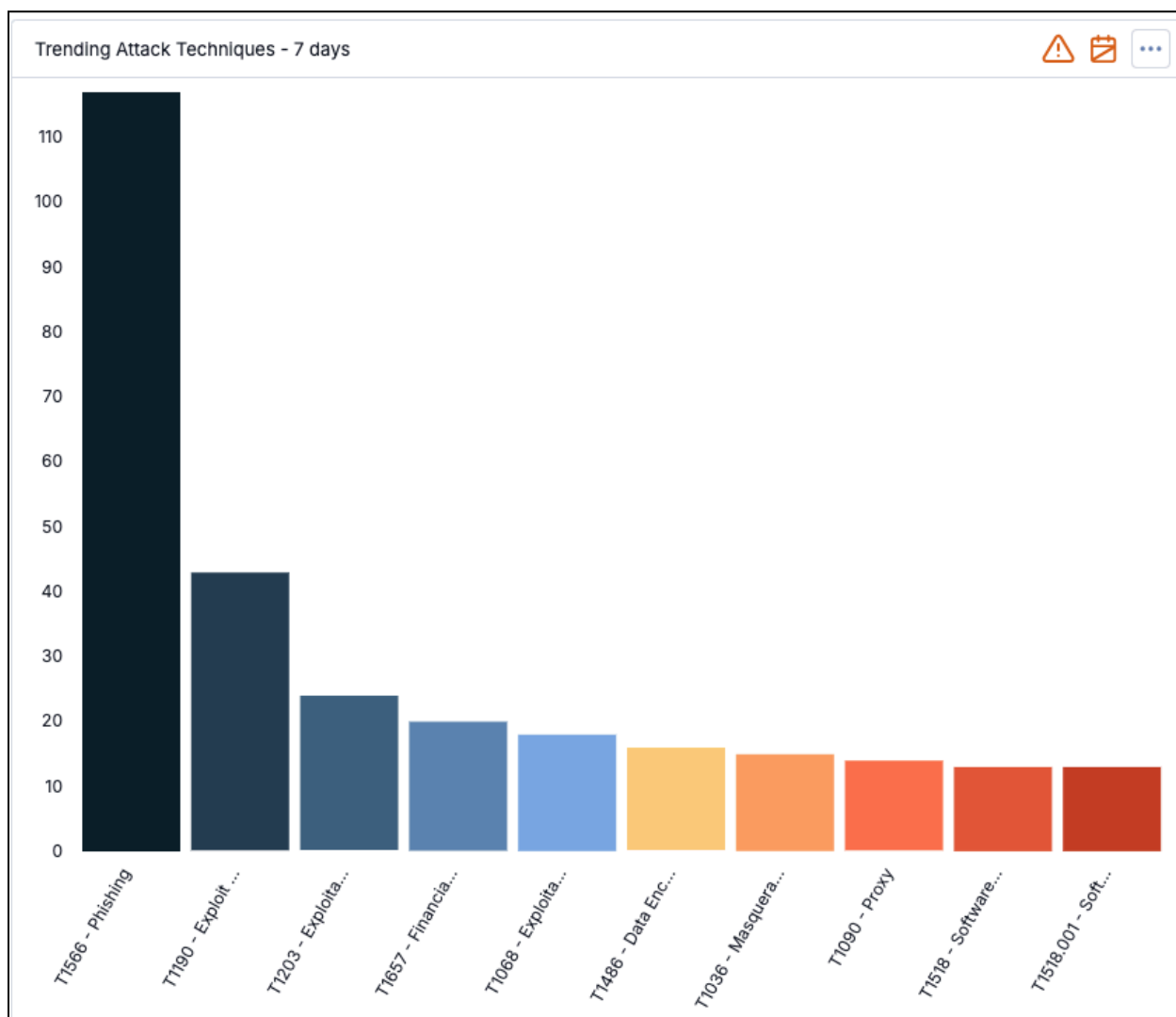
Disable tooltips Use gradient fill
 Show grid lines

Example Query card configuration with ATT&CK Tag grouping

This example shows the configuration for a Query card that displays the most prevalent ATT&CK techniques over the previous 7 days. To surface the desired metrics, the chart



queries by Groups using a [ThreatConnect Query Language \(TQL\)](#) query to find Report Groups added to the selected ThreatConnect owners within the past 7 days. The rationale is that Reports added to ThreatConnect in that timeframe are likely recently published, and inclusion of the ATT&CK Tags on the Report objects indicates that the Reports describe activity that used the particular techniques represented by the ATT&CK Tags. In other words, by looking for recent Reports and grouping them by the new **ATT&CK Tag** option, you can surface the techniques that have been most prevalent in the defined timeframe. The following Query card shows the result of the example configuration:



Top 10 ATT&CK techniques for the past 7 days



Global Dashboard Date Range

In ThreatConnect 7.11, we're proud to introduce a much-awaited enhancement to dashboards: the ability to apply date range filters across multiple cards in a dashboard. Before version 7.11, ThreatConnect dashboards offered filtering solely by data source, leaving date ranges to be individually managed for each card. This process often led to cumbersome individual adjustments, hindering seamless dynamic changes across the dashboard. Now, you can now choose a date range that applies to your entire dashboard. Each card configured to inherit the global dashboard date range will dynamically adjust to reflect that range.

Note

The global dashboard date range applies only to Metric and Query cards. It is not available for Widget cards.

When setting a global date range, you can choose from among the following options: **Today**, **Last 7 Days**, **Last 30 Days**, **Last 60 Days**, and **Custom Dates and Times**. You can fine-tune the time selection down to the second in the **Custom Dates and Times** option.

Dashboards / Nation State Adversary Dashboard

Nation State Adversary Dashboard

Owners 50

Top 10 Adversary Threat Intelligence

20% Helix Kitten Total: 49

5.8% russia Total: 14

APT28 Total: 14

Sofacy Total: 12

DNC Total: 10

Global Dashboard Date Range ⓘ

Last 7 Days


Date & Time Range

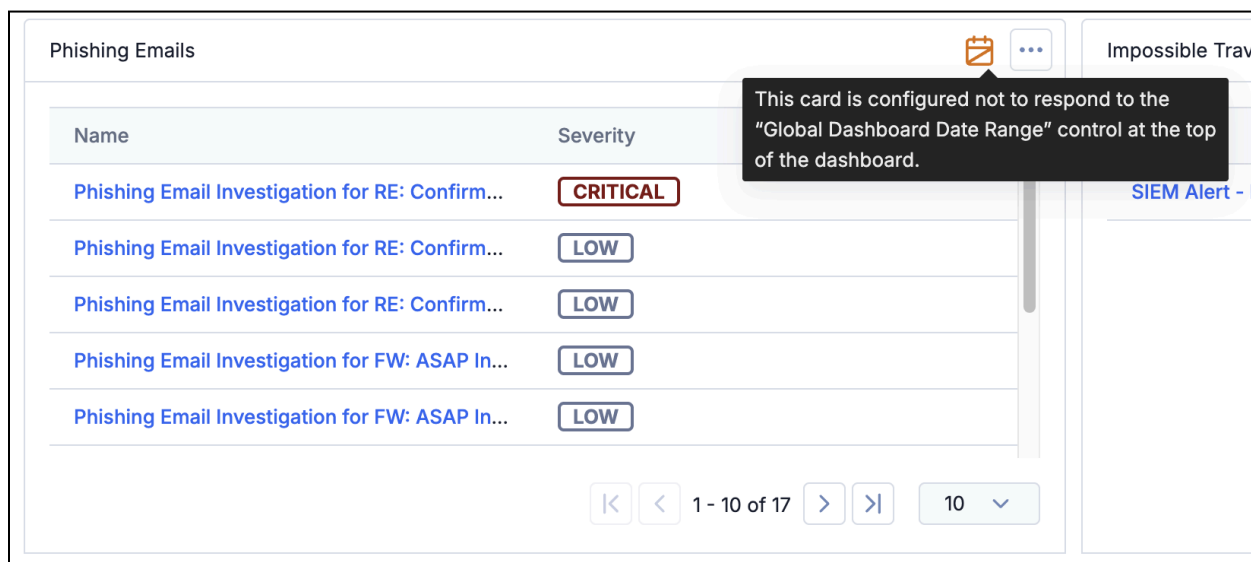
2025-10-09 15:36:28 — 2025-10-16 15:36:28

Cancel Apply

Select the global dashboard date range



Dashboard cards that do not use the global dashboard date range display the  icon in their header.



Name	Severity
Phishing Email Investigation for RE: Confirm...	CRITICAL
Phishing Email Investigation for RE: Confirm...	LOW
Phishing Email Investigation for RE: Confirm...	LOW
Phishing Email Investigation for FW: ASAP In...	LOW
Phishing Email Investigation for FW: ASAP In...	LOW

Dashboard cards that do not use the global dashboard date range are easy to spot

The global dashboard date range feature is configured differently for Metric cards and Query cards.

Metric Cards

Metric cards offer a straightforward approach to global date inheritance. When adding or editing a Metric card, simply select the **Inherit global dashboard date range** checkbox in the configuration to ensure that the card uses the global dashboard date range. Leave the checkbox unselected if you want to use dates configured specifically for that Metric card.



Add New Card ✕

Card Category: Metrics Card ▼ Card Type: Activities ▼

Card Title *
Activities 10/255

Filters & Settings

Inherit dashboard-level owner selections Short date format

Inherit global dashboard date range ⓘ Sum across owners ⓘ

Owner
6 Selected × ▼

Date Range: Last 7 Days ▼ Date Range *: 2025-11-05 — 2025-11-12

Metric Types *
7 Selected × ▼ Date Order: Ascending Descending

Select the *Inherit global dashboard date range* checkbox for Metric cards

Query Cards

To configure a Query card to use the global dashboard date range, use the following placeholder variables instead of specific dates or time windows in the **Advanced Query** parameter: **\$startdate** for the global start date and **\$enddate** for the global end date.

Before global date range selection was available for dashboards, managing date filters on Query cards was a manual process in which you had to edit the **Advanced Query** parameter whenever you wanted to change a Query card's date range. For instance, a dashboard card showing Workflow Cases created in the last 30 days might have had an **Advanced Query** parameter like `dateAdded >= "TODAY() - 30 days"`. This parameter had to be modified every time you wanted the dashboard to gather data for different date ranges—and if you had other Query cards, you had to modify each card's date range individually.

Now, with the global dashboard date range feature, the process is much simpler. For example, by adjusting the **Advanced Query** parameter to `dateAdded >= $startdate`, the Query



card becomes adaptable to display data from various time frames selected in the global dashboard date range, such as the last 7, 30, or 60 days. Similarly, to configure the Query card to accommodate a custom date range, adjust the **Advanced Query** parameter to include both start and end dates (`dateAdded >= $startdate and dateAdded <= $enddate`). This method enables you to make changes only once to each card (i.e., to enter the placeholder variables) rather than edit every single Query card whenever you want to adjust the dates.



Improvements

Threat Intelligence

ThreatAssess

- To enable quicker processing of high-priority data sets, there are now two monitors for ThreatAssess changes—one for high- and medium-priority changes (High-Priority ThreatAssess Monitor), such as changes made to Indicators in the ThreatConnect UI and via the v3 API, and one for low-priority changes (Low-Priority ThreatAssess Monitor), such as changes made to Indicators via the V2 Batch API—as well as a separate monitor for CAL changes to Indicators (CAL Feedback Monitor). Each monitor has its own logging process.
- The **threatAssessMonitorInterval** and **threatAssessRefreshInterval** system settings were removed.
- Four new system settings were added:
 - **threatAssessMonitorHighPriorityInterval**: The interval, in minutes, at which high- and medium-priority updates to ThreatAssess scores are made.
 - **threatAssessMonitorLowPriorityInterval**: The interval, in minutes, at which low-priority updates to ThreatAssess scores are made.
 - **CALFeedbackMonitorInterval**: The interval, in minutes, at which the CAL Feedback Monitor looks for CAL updates to Indicators.
 - **CALDailyDeltaTargetRetrieval**: The date (YYYYMMDD) for which CAL will attempt to sync data. If no value is provided, CAL will attempt to sync on the current day. Changing this value is not recommended unless you need CAL to sync data from a previous time period. If you enter a date, CAL will attempt to sync data changes detected on that date. If no data are returned for that day, CAL will attempt to sync data changes from the next day.
- The **threatAssessIntervalCount** system setting was renamed to **threatAssessBatchSize**.
- On the **ThreatAssess** tab of the **Account Settings** screen, the following two buttons were added:
 - **VIEW CURRENT QUEUE**: View a real-time breakdown of the current number of Indicators in the ThreatAssess queue, as well as an option to refresh the queue. You can use the breakdown to measure response times to various actions.



- **REINITIALIZE THREATASSESS**: Reinitialize ThreatAssess for all Indicators on the ThreatConnect instance. If you proceed with this option, all Indicators will keep their existing score, but will be flagged for reassessment and placed in a queue for processing. This process may take multiple days for ThreatConnect instances with large numbers of Indicators, so it should be used with caution.

Built-In Enrichment

- You can now access real-time intelligence from Google® TI for Address, File, Host, and URL Indicators via the existing [VirusTotal™ built-in enrichment](#):
 - System Administrators can configure the enrichment by navigating to **System Settings > Indicators > Enrichment Tools** and editing the **VirusTotal / Google TI** vendor.
 - The API key (VirusTotal or Google TI) entered in the configuration determines the source of the data provided by the enrichment.
 - If a Google TI API key is entered, then the enrichment information is provided in a **Google Threat Intelligence** card on the **Enrichment** tab of an Indicator's **Details** screen.
 - If a VirusTotal API key is entered, then the enrichment information is provided in a **VirusTotal** card on the **Enrichment** tab of an Indicator's **Details** screen.
 - The **Google Threat Intelligence Detailed View** drawer displays a new **Contributing Factors** card that provides deeper insight into vendor analyses.

Threat Graph

- Threat Graph now has **Undo** and **Redo** buttons, allowing you to undo and redo up to 10 pivots in ThreatConnect, CAL, or enrichment services. In particular, if a pivot returns more results than you can work with or process, you can easily remove all of the pivots at once and try a new one. You can also undo and redo node removals. Note that this feature applies only to changes made in a single session, as actions taken in a Threat Graph are not “remembered” after the Threat Graph has been closed. Also, the undo/redo functionality does not currently apply to layout changes. If you make a layout change, such as moving a node or selecting a new layout, and then click **Undo**, the layout change *and* the change made before the layout change will be undone, as the undo operation is applied to the earlier change. If you click **Redo**, the earlier change will be redone, but the layout change will not.



- In Threat Graph, you can now hover over a node with a truncated name to view a tooltip with the object's full name. Note that this hover works only on the node itself, not on the text box with the node's name below the node.

Search

- You can now select the columns displayed in the results table on the **Search: All Object Types** screen for searches in your ThreatConnect owners and in a file uploaded via the bulk Indicator search feature.
- A column for Tags was added to the results table on the **Search: All Object Types** screen. In bulk Indicator search, if Indicator deduplication is enabled, the **Tags** column shows a deduplicated list of Tags applied to all versions of the Indicator.
- After you upload a file to the bulk Indicator search feature on the **Search: All Object Types** screen, you can click on the file upload area to view a details drawer containing information about the file, including its name, the date it was last modified, and the number of known and known Indicators found in the file.
- You can now bulk delete returned objects on the **Search: Tags**, **Search: Victim Assets**, and **Search: Victims** screens.

Details Screen and Drawer

- The **Details** screen and **Details** drawer for Indicators now display a "[Known Good](#)" label for Indicators that are on a public safelist. This label is provided as part of CAL enrichment, which means that [you must have CAL enabled on your ThreatConnect instance and in your Organization for it to be displayed](#). Note that this label is not yet available for the unified view on the Indicator **Details** drawer.
- The **Tags** card on the **Details** screen for the unified view for Vulnerability Groups and Threat Actor Profiles, as well as on the **Details** drawer for the unified view for Indicators, now consolidates all Tags from all owners into a single list. Click on each Tag to see the owners using that Tag.
- On the **Details** screen for a Vulnerability Group, you can now enable or disable the unified view as default from any owner, not just the unified view itself.

My Account

- The **My Account** screen, formerly **My Profile**, has been redesigned to provide a clean, easy-to-use interface:



- The **General** tab (formerly **Overview**) provides intuitive groupings of settings, an **Enable Authenticator** button for enabling multifactor authentication that replaces the **Authenticator** tab in previous versions, and a link to the ThreatConnect Terms of Service for your instance.
- The **Follow** tab (formerly **Follow Settings**) has a sidebar that organizes the owners and objects you follow into a set of results tables, one for each owner or object type. Intelligence Requirements and Victims are new additions to the object types displayed on this tab.
- The **Variables** tab displays a sleeker table of the file, keychain, and text variables you create for your user account.
- The **Activity** tab displays a more streamlined table of your user account's activities on your ThreatConnect instance.
- The **Spaces** tab has been removed, because the **Spaces** feature is deprecated.
- You can toggle dark mode on and off with a new, easy-to-find **Dark Mode** toggle at the upper right of the **My Account** screen header.

My Pages

- You can now add up to 25 bookmarked pages in **My Pages**. In addition, a **Manage My Pages...** option has been added that allows you to reorder pages, remove pages, and edit page names.

Playbooks

- The Event Trigger has a new **Status Change** action type that allows you to configure the Trigger to fire when the Status of an Event Group is changed in the ThreatConnect UI or via the v3 or V2 Batch API.

Dashboards

- The UI for adding and editing dashboard cards was revamped to provide a more streamlined and user-friendly experience.
- When viewing details for a dashboard Query card with a table that queries by Indicators, Groups, Victims, Victim Assets, or Tags, you can now click a **Run Query** button that takes you to the query results on the **Search** screen for the object type.



Services

- The **Services** screen has been redesigned, providing a streamlined interface, customizable column selection, and a details drawer for each Service.

Workflow

- The maximum length for the Description of a Workflow Case has been increased to 4000 characters. A character count was added to the Description to help you track its length.

Reporting

- When adding a query chart to a report with a **Target of Time to Detect** or **Time to Respond**, you can now configure the **Time Units**.

Installation and Deployment

- All MDB **maxsession** system properties are now persisted during installation.
- In containerized deployments, the OpenSearch container can now be configured to use any user.

API & Under the Hood

- When using the V2 Batch API to update an existing Document or Report Group that contains a file attachment, the Group is now correctly updated without having its file status reset to "Awaiting Upload."
- You can now retrieve the CAL score for Indicators using the v3 API by adding the **fields** query parameter to your request and setting its value to **threatassess**.



- When using the v3 API to update an existing Case or Workflow Task that has an assignee, you can now remove the assignee by including the following in the request body:

```
{
  "assignee" : {
    "type" : "None"
  }
}
```

- In V2 Batch API input files, you can now define an Indicator's summary using either the **summary** field or the field that contains the Indicator's value for the specified Indicator type (e.g., the **ip** field allows you to define an Address Indicator's IPv4 or IPv6 address value).
- You can now retrieve associated platforms and tactics for ATT&CK Tags using the v3 API by adding the **fields** query parameter to your request and setting its value to one of the following:
 - **tactics**: Returns associated tactics for ATT&CK Tag objects in requests sent to the Tags v3 API endpoint.
 - **platforms**: Returns associated platforms for ATT&CK Tag objects in requests sent to the Tags v3 API endpoint.
 - **tags.tactics**: Returns associated tactics for ATT&CK Tag objects in requests sent to the Cases, Groups, Indicators, Intelligence Requirements, or Victims endpoint.
 - **tags.platforms**: Returns associated platforms for ATT&CK Tag objects in requests sent to the Cases, Groups, Indicators, Intelligence Requirements, or Victims endpoint.



Bug Fixes

Attributes

- Line-wrapping issues in Attributes that do not support Markdown were resolved.

Playbooks

- The **ThreatConnect Groups Operations** and **ThreatConnect Attributes** Playbook Apps were updated to support copying of the **External Date Added**, **External Date Expires**, **External Last Modified**, **First Seen**, and **Last Seen** fields. This fix solves an issue that was preventing the values for these fields from being displayed on the **Details** card on the **Details** screen for Reports copied into ThreatConnect via Playbooks using those Apps.

Services

- Only System Administrators can now access the **Permissions** dropdown and **Allow all** checkbox for owner selection when creating or editing a Playbook Trigger or Service API App on the **Services** screen. This update addresses a permissions conflict in which users with certain System roles were unable to edit a Service after giving Organizations other than their home Organization permission to use the Service App.

Installation and Deployment

- An issue preventing the **metadata.xml** file for Security Assertion Markup Language™ (SAML™)-enabled instances from being generated was resolved.



Dependencies & Library Changes


- ThreatConnect is now running OpenSearch® version 3.2.0.



Maintenance Releases Changelog

2025-11-13 7.11.1 [Latest]

Improvements

- The Doc Analysis Import feature is now called Document Parsing Import to more clearly differentiate it from the [CAL Doc Analysis Service](#).
- System Administrators can use the new **aiPoweredImportEnabled** system setting to turn on or off the AI-powered features of Document Parsing Import for their ThreatConnect instance. The setting is turned on by default. If the setting is turned on, then users will see “🌟 AI-powered” under the **Document Parsing** option in the  and **Create & Import** dropdowns and on the **Import** tab of the **Import Intel - Document Parsing** screen. If the setting is turned off, then “🌟 AI-powered” will not be displayed for those options, and [MITRE ATT&CK AI classification](#) will not be available for parsed Groups in Document Parsing Import.
- Services may now show a status of **Pending** to indicate that they are still loading on the **Services** screen. After they load, the status will change to **Inactive**, **Running**, or **Failed**.
- The “breadcrumb” navigation on the **Details** screen for Groups, Indicators, and Intelligence Requirements now directs you to the **Search** screen for the object type instead of the **Legacy Browse** screen.
- Performance enhancements were made for Indicator confidence deprecation and for ThreatAssess. In addition, to prevent unnecessary ThreatAssess refreshes, Indicator confidence deprecation now triggers a refresh of an Indicator's ThreatAssess score only when the Indicator's Confidence Rating drops to 90, 70, 50, 30, 1, or 0.
- System and audit logs now capture detailed logout events, including user ID, session ID, timestamp, logout method, source IP, and details for errors or anomalies that occurred during logout.

Bug Fixes

- An issue preventing data from being populated into the **Known Exploited Vulnerabilities (KEV)** card on the unified view of the **Details** screen for some Vulnerability Groups was fixed.



- Intelligence Requirements were returning partial keyword matches. This behavior has been corrected.
- The following issues for dashboard cards for custom user metrics with keyed data series were resolved:
 - Card configuration is missing options for selecting series data.
 - Card displays data from only a subset of the owners selected in the card's configuration.
- An issue causing an error to occur when adding an Attribute that has a custom Attribute type defined in more than one owner on a ThreatConnect instance was fixed.
- Performance for potential-association queries was improved on SingleStore instances.
- The Audit Log in the Playbook Designer now shows the 100 most recent entries. Please note that if a Playbook has more than 100 changes, only the 100 most recent changes will be available in the Audit Log.