ThreatConnect® Release Notes

Software Version 7.10

July 30, 2025

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

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

Table of Contents

New Features and Functionality

Vulnerability Enhancements

Having all your data on an object in one place can maximize your understanding of the object while minimizing the amount of time you spend building that understanding. In version 7.10 of ThreatConnect®, we are thrilled to introduce a **unified view for Vulnerability objects**. This feature, which is available on a Vulnerability's **Details** screen, combines all information about the Vulnerability in all of your ThreatConnect owners in a single view. This consolidation, which identifies and connects Vulnerability objects with the same name/summary in your ThreatConnect owners, happens automatically after your instance is upgraded to 7.10, starting with the most recently added Vulnerabilities. It may take a few days after upgrading to version 7.10 for all matching Vulnerabilities to be identified and consolidated. However, if you notice that the unified view is not available for Vulnerability objects after that period of time, please reach out to your Customer Success representative for assistance.

The unified view for Vulnerabilities enables you to streamline your research and trust that when you visit a Vulnerability's **Details** screen, you are seeing all available information across all of your ThreatConnect owners, including all Attributes, Tags, and associations added to all individual versions of the Vulnerability. It also reduces the need to use ThreatConnect Query Language (TQL) to automate the creation of associations to Vulnerabilities in other owners or to create cross-owner associations manually when adding context to a Vulnerability in your ThreatConnect instance, as you can view and filter all associations for all versions of a Vulnerability without additional steps.

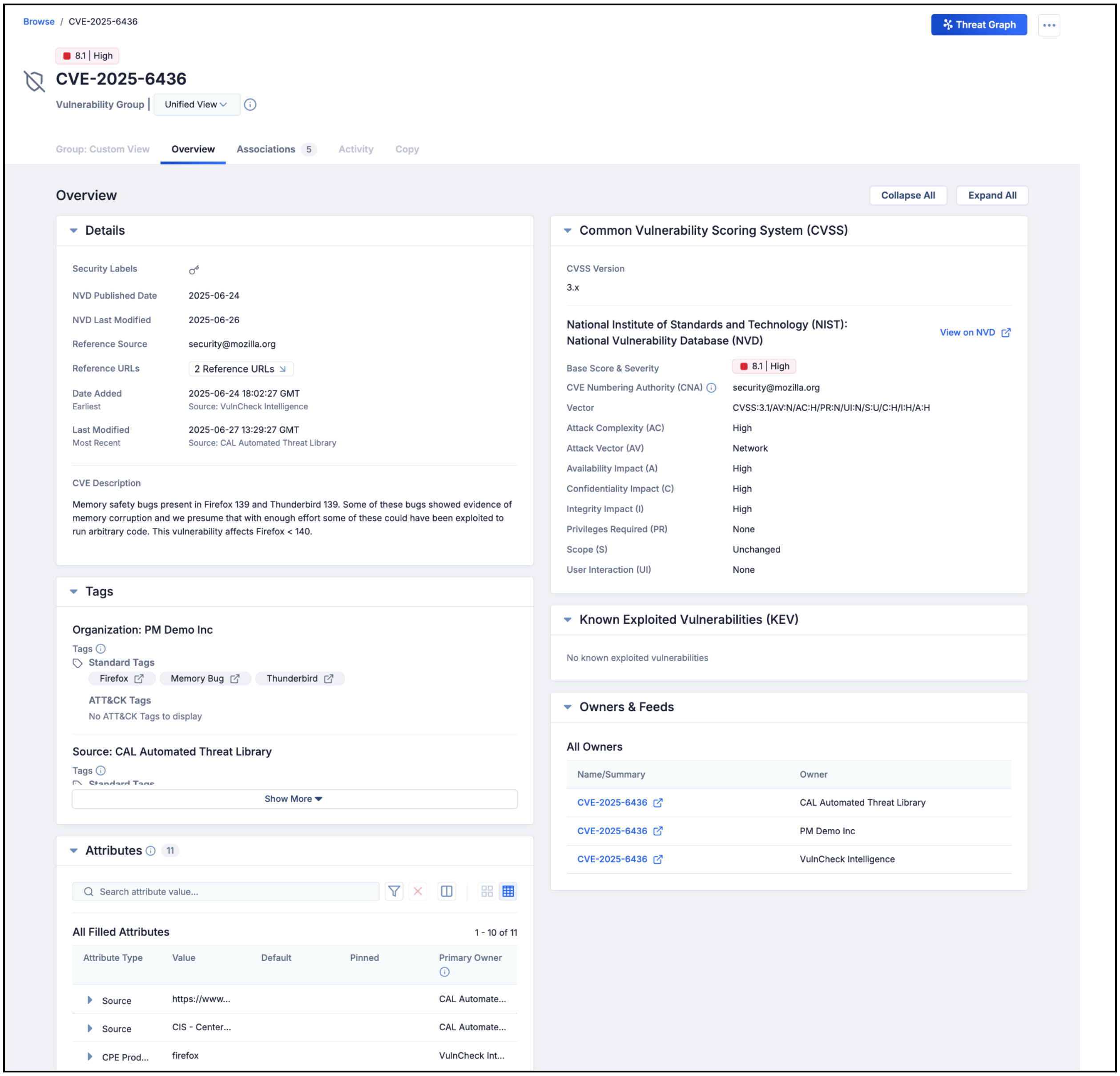
ThreatConnect 7.10 also delivers another highly impactful improvement for Vulnerability objects: the addition of **Common Vulnerability Scoring System (CVSS) and Known Exploited Vulnerabilities (KEV) data**. Cards for CVSS and KEV data are now provided on the **Details** screen and **Details** drawer for all Vulnerability objects, including in the new unified view. You can leverage this information to sharpen your understanding of a Vulnerability and streamline your decision making about the severity of the threat the Vulnerability poses to your organization.

Unified View for Vulnerabilities

The unified view is shown by default for Vulnerabilities that exist in more than one of your ThreatConnect owners. It is not available for Vulnerabilities that exist in only one of your ThreatConnect owners.

The unified view for Vulnerabilities covers two **Details** screen tabs: **Overview** and **Associations**. The **Overview** tab aggregates read-only information about the Vulnerability's details, Tags, Attributes, CVSS data, KEV data, and other owners and feeds from all versions of the Vulnerability in all of your ThreatConnect owners. Similarly, the **Associations** tab aggregates read-only information about the Vulnerability's associated Intelligence Requirements (IRs), Groups, Indicators, and Victim Assets in all of your ThreatConnect owners.

Note: Artifact and Case associations and potential associations are not currently available on the **Associations** tab of the unified view for Vulnerabilities.



CVE-2025-6436

Overview

Details

Security Labels	
NVD Published Date	2025-06-24
NVD Last Modified	2025-06-26
Reference Source	security@mozilla.org
Reference URLs	2 Reference URLs
Date Added Earliest	2025-06-24 18:02:27 GMT Source: VulnCheck Intelligence
Last Modified Most Recent	2025-06-27 13:29:27 GMT Source: CAL Automated Threat Library

CVE Description

Memory safety bugs present in Firefox 139 and Thunderbird 139. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 140.

Tags

Organization: PM Demo Inc

Tags

Standard Tags

Firefox Memory Bug Thunderbird

ATT&CK Tags

No ATT&CK Tags to display

Source: CAL Automated Threat Library

Tags

Show More

Attributes 11

Search attribute value...

All Filled Attributes 1 - 10 of 11

Attribute Type	Value	Default	Pinned	Primary Owner
Source	https://www...			CAL Automate...
Source	CIS - Center...			CAL Automate...
CPE Prod...	firefox			VulnCheck Int...

Common Vulnerability Scoring System (CVSS)

CVSS Version

3.x

National Institute of Standards and Technology (NIST): National Vulnerability Database (NVD)

View on NVD

Base Score & Severity	8.1 | High
CVE Numbering Authority (CNA)	security@mozilla.org
Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Attack Complexity (AC)	High
Attack Vector (AV)	Network
Availability Impact (A)	High
Confidentiality Impact (C)	High
Integrity Impact (I)	High
Privileges Required (PR)	None
Scope (S)	Unchanged
User Interaction (UI)	None

Known Exploited Vulnerabilities (KEV)

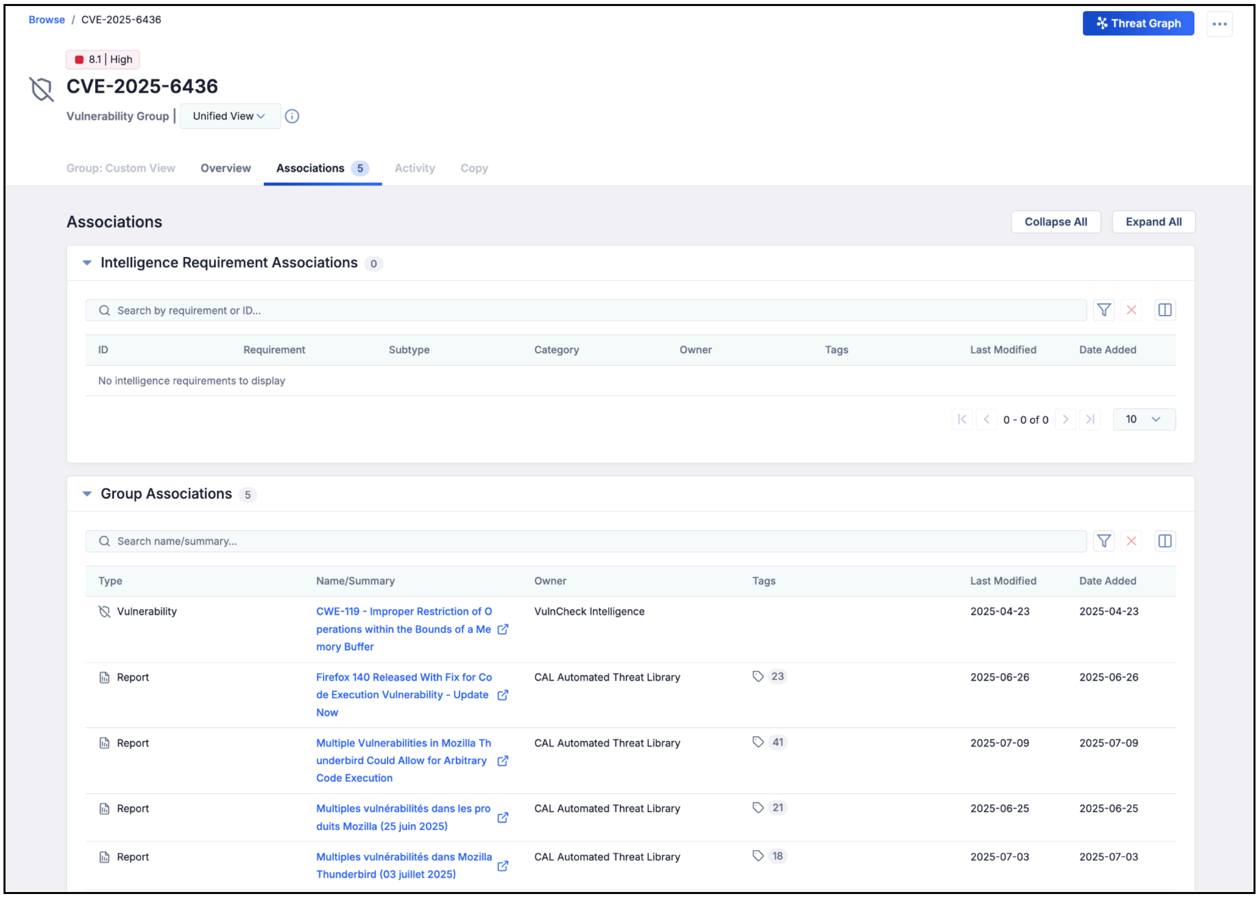
No known exploited vulnerabilities

Owners & Feeds

All Owners

Name/Summary	Owner
CVE-2025-6436	CAL Automated Threat Library
CVE-2025-6436	PM Demo Inc
CVE-2025-6436	VulnCheck Intelligence

View overview data from all owners in a Vulnerability's unified view



CVE-2025-6436

Associations

Intelligence Requirement Associations 0

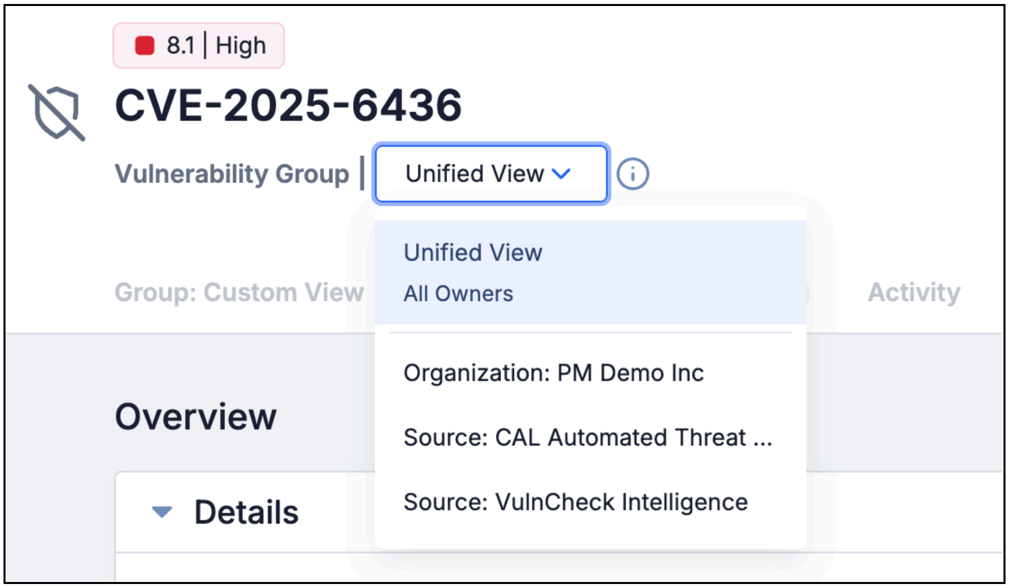
ID	Requirement	Subtype	Category	Owner	Tags	Last Modified	Date Added
No intelligence requirements to display							

Group Associations 5

Type	Name/Summary	Owner	Tags	Last Modified	Date Added
Vulnerability	CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	VulnCheck Intelligence		2025-04-23	2025-04-23
Report	Firefox 140 Released With Fix for Code Execution Vulnerability - Update Now	CAL Automated Threat Library	23	2025-06-26	2025-06-26
Report	Multiple Vulnerabilities in Mozilla Thunderbird Could Allow for Arbitrary Code Execution	CAL Automated Threat Library	41	2025-07-09	2025-07-09
Report	Multiples vulnérabilités dans les produits Mozilla (25 juin 2025)	CAL Automated Threat Library	21	2025-06-25	2025-06-25
Report	Multiples vulnérabilités dans Mozilla Thunderbird (03 juillet 2025)	CAL Automated Threat Library	18	2025-07-03	2025-07-03

View associations data from all owners in a Vulnerability's unified view

If you want to view the **Details** screen for a specific version of the Vulnerability—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.


8.1 | High
CVE-2025-6436
Vulnerability Group | Unified View
Group: Custom View
Activity
Unified View
All Owners
Organization: PM Demo Inc
Source: CAL Automated Threat ...
Source: VulnCheck Intelligence
Overview
Details

You can select the unified view or a specific owner's version of a Vulnerability

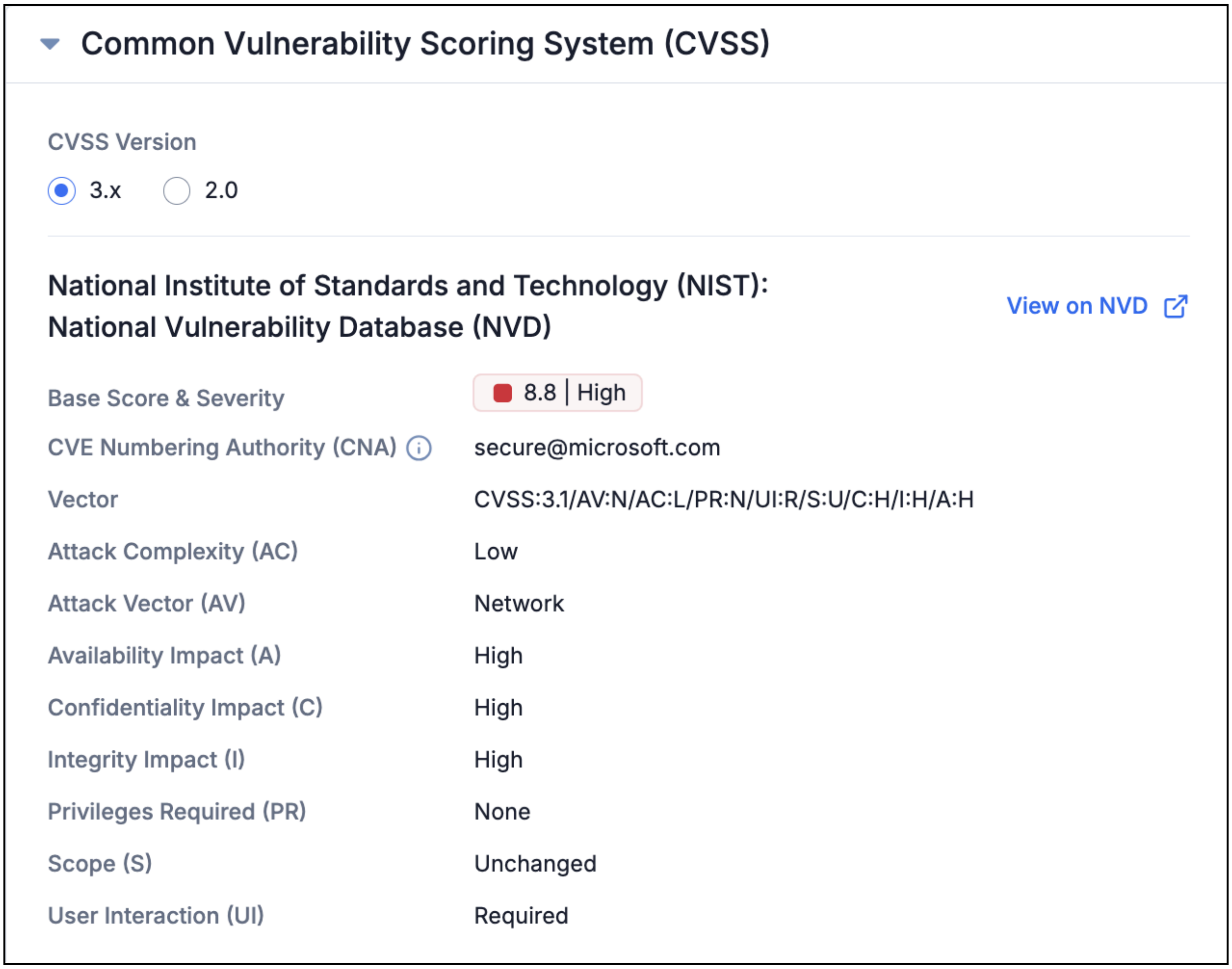
If you do not want to see the unified view by default, you can disable this setting in the **Options** ⋯ menu at the upper right of the Vulnerability's **Details** screen. Note that the selection for this setting applies to all Vulnerability objects in all owners for your user account. You cannot enable or disable it for individual Vulnerabilities, 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.

CVSS and KEV Data for Vulnerabilities

The new Common Vulnerability Scoring System (CVSS) and Known Exploited Vulnerabilities (KEV) cards are available on the **Details** drawer and **Overview** tab of the **Details** screen for all Vulnerability objects in ThreatConnect 7.10. The information in these two cards is the same for all versions of a Vulnerability in your ThreatConnect owners, as well as in the new unified view for Vulnerabilities. In ThreatConnect 7.10, these cards are displayed and populated on the **Details** screen for all Vulnerability objects regardless of whether they have a unified view or not.

Common Vulnerability Scoring System (CVSS) Card

The data displayed on the **Common Vulnerability Scoring System (CVSS)** card are pulled directly from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) or VulnCheck, eliminating the need to navigate to that site and sift through data there. If more than one CVSS version is available for a given Vulnerability, the **CVSS Version** section at the top of the card will provide options to select the version you want the card to display. This information is sourced directly from NVD or VulnCheck and does not undergo any additional validation or enrichment before being shown in ThreatConnect.



CVSS Version

● 3.x ○ 2.0

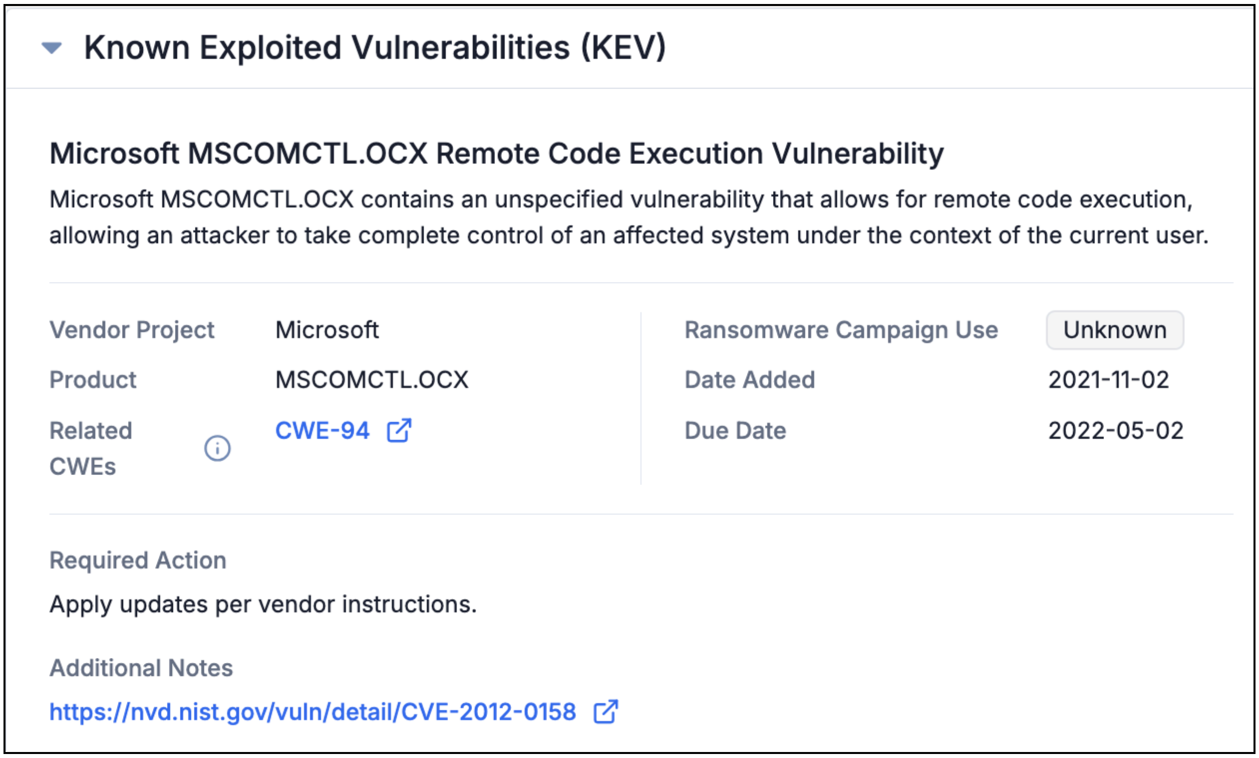
National Institute of Standards and Technology (NIST): National Vulnerability Database (NVD)

Base Score & Severity	🟥 8.8 | High
CVE Numbering Authority (CNA)	secure@microsoft.com
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Attack Complexity (AC)	Low
Attack Vector (AV)	Network
Availability Impact (A)	High
Confidentiality Impact (C)	High
Integrity Impact (I)	High
Privileges Required (PR)	None
Scope (S)	Unchanged
User Interaction (UI)	Required

View CVSS data, including different CVSS versions, for a Vulnerability

Known Exploited Vulnerabilities (KEV) Card

The data displayed on the **Known Exploited Vulnerabilities (KEV)** card are pulled directly from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities Catalog or VulnCheck, eliminating the need to navigate to that site and sift through data there. The card also provides links to related Common Weakness Enumerations (CWEs) and any additional relevant information. This information is sourced directly from CISA or VulnCheck and does not undergo any additional validation or enrichment before being shown in ThreatConnect.



▾ Known Exploited Vulnerabilities (KEV)

Microsoft MSCOMCTL.OCX Remote Code Execution Vulnerability

Microsoft MSCOMCTL.OCX contains an unspecified vulnerability that allows for remote code execution, allowing an attacker to take complete control of an affected system under the context of the current user.

Vendor Project	Microsoft	Ransomware Campaign Use	Unknown
Product	MSCOMCTL.OCX	Date Added	2021-11-02
Related CWEs ⓘ	CWE-94	Due Date	2022-05-02

Required Action

Apply updates per vendor instructions.

Additional Notes

https://nvd.nist.gov/vuln/detail/CVE-2012-0158

View KEV data for a Vulnerability

ATT&CK RQ Financial Impact

ThreatConnect 7.10 introduces **ATT&CK RQ Financial Impact, a new Financial Impact overlay option in the ThreatConnect ATT&CK Visualizer**. This feature, powered by ThreatConnect Risk Quantifier (RQ), shows the relative amount of potential financial loss from an attack on your company using a particular MITRE ATT&CK® technique or set of techniques. You can use this information to deepen your understanding of the financial risk that a given threat actor group or malware family, among other things, may pose to your company and make more informed decisions.

ThreatConnect RQ calculates Financial Impact by leveraging over 40 years of loss data from sources such as insurance claims, 10-K filings, and proprietary research to build models specific to industry type and company size. It then customizes the calculation by applying your company's firmographics, such as industry sector and gross revenue, which your Organization Administrator provides when configuring the feature.

Configure ATT&CK RQ Financial Impact

To use ATT&CK RQ Financial Impact, it must be turned on for your ThreatConnect instance and configured for your Organization.

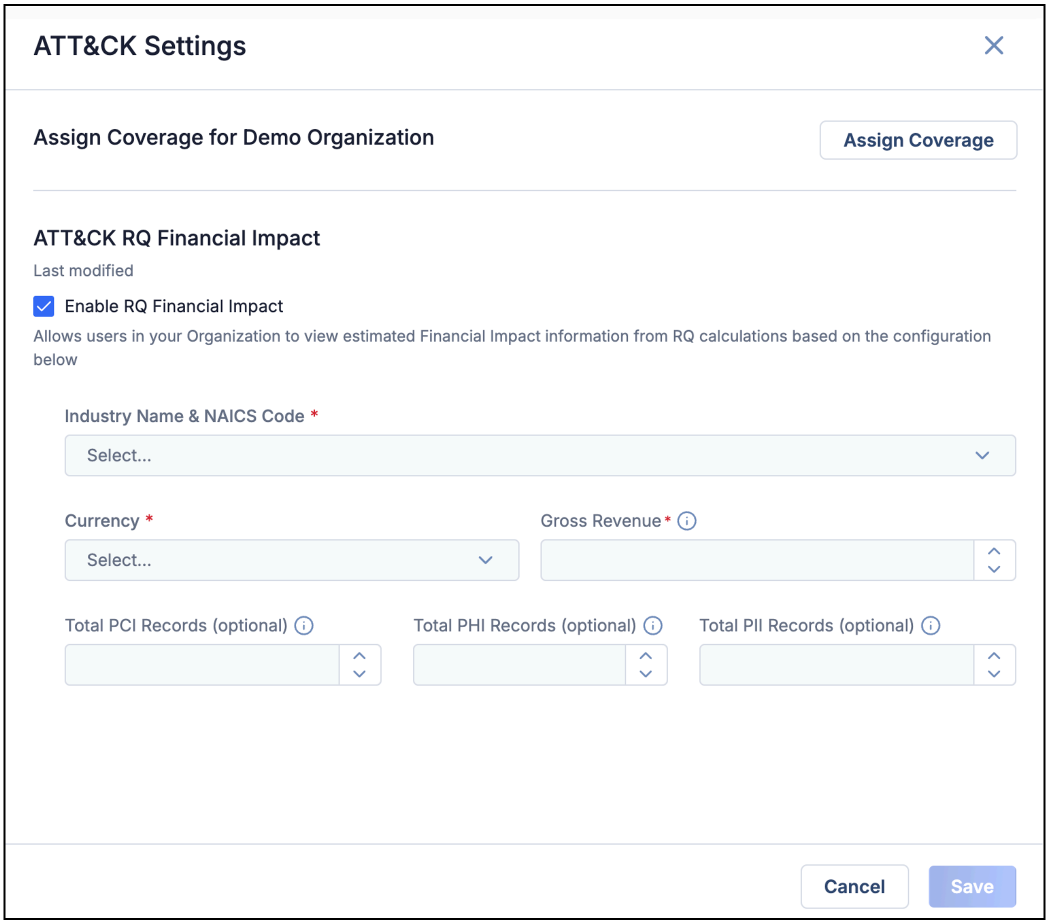
System Configuration

To turn on ATT&CK RQ Financial Impact for a ThreatConnect instance, a System Administrator must select the checkbox for the **financialImpactEstimates** system setting in **System Settings** > **Settings** > **Feature Flags**. *This setting is turned off by default.*

Organization Configuration

After ATT&CK RQ Financial Impact is turned on for your ThreatConnect instance, Organization Administrators must follow these steps to enable it for their Organization and configure it with key parameters unique to their company's risk profile:

1. Select **ATT&CK** from the **Tools** menu on the top navigation bar.
2. Click **Settings** ⚙ at the upper right of the **ATT&CK** screen.
3. Fill out the fields on the **ATT&CK Settings** drawer as follows:



ATT&CK Settings

Assign Coverage for Demo Organization

ATT&CK RQ Financial Impact

Last modified

☑ Enable RQ Financial Impact

Allows users in your Organization to view estimated Financial Impact information from RQ calculations based on the configuration below

Industry Name & NAICS Code * Select...

Currency * Select...

Gross Revenue *

Total PCI Records (optional)

Total PHI Records (optional)

Total PII Records (optional)

- **Enable RQ Financial Impact**: Select this checkbox to turn on ATT&CK RQ Financial Impact for your Organization.
- **Industry Name & NAICS Code**: Select the North American Industry Classification System (NAICS) name and code that most closely fits your company's industry.
- **Currency**: Select the currency to use for Financial Impact data in the ATT&CK Visualizer. Currently, the following options are available: **Australian Dollar (AUD)**, **Euro (EUR)**, **Pound Sterling (GBP)**, and **US Dollar (USD)**.
- **Gross Revenue**: Enter your company's gross annual revenue in the currency selected in the **Currency** dropdown.
- **Total PCI Records**: (Optional) Enter your company's total number of payment card industry (PCI) records.
- **Total PHI Records**: (Optional) Enter your company's total number of protected health information (PHI) records.
- **Total PII Records**: (Optional) Enter your company's total number of personally identifiable information (PII) records.

> **Note**: The information entered in these fields is unique to each Organization and is not shared across ThreatConnect or ThreatConnect Risk Quantifier instances.

4. Click **Save** to save your Organization's ATT&CK RQ Financial Impact configuration.

> **Important**: Please ensure that your Organization's security coverage is up to date to allow for the highest level of accuracy in the ATT&CK RQ Financial Impact calculation.

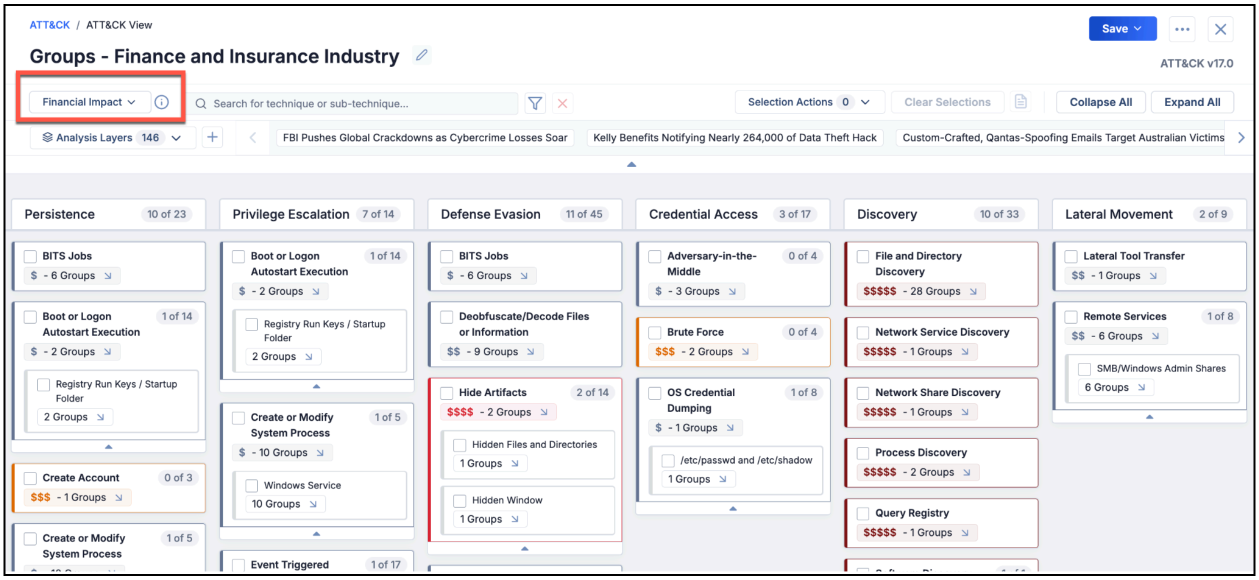
Please allow up to about 10 minutes for Financial Impact data to populate. Similarly, if you change the currency in an existing ATT&CK RQ Financial Impact configuration, updates may take up to 10 minutes to populate, during which time no Financial Impact data will be available in standard ATT&CK views.

Financial Impact Overlay in Standard ATT&CK Views

After the ATT&CK RQ Financial Impact feature has been enabled and configured and data from ThreatConnect RQ have been populated, you can use the feature in standard ATT&CK views in the ATT&CK Visualizer.

> **Note**: The Financial Impact overlay is not available for imported ATT&CK views.

Like Technique Prevalence, Threat Group Comparison, and Security Coverage, Financial Impact is an overlay that you apply to a standard ATT&CK view for a set of Groups. It uses color coding and currency symbols to represent the relative amount of potential financial risk that each ATT&CK technique or sub-technique poses to your company. The **Analysis Layers** dropdown at the upper left displays a legend defining the risk levels, which range from **$ (Very Low Potential Cost)** to **$$$$$ (Very High Potential Cost)**, where the currency symbol will be the one selected in the feature's configuration. And like the other overlays, the Financial Impact overlay can be exported to a JSON or PNG file.


ATT&CK / ATT&CK View
Groups - Finance and Insurance Industry
Save
ATT&CK v17.0
Financial Impact
Search for technique or sub-technique...
Selection Actions 0
Clear Selections
Collapse All
Expand All
Analysis Layers 146
FBI Pushes Global Crackdowns as Cybercrime Losses Soar
Kelly Benefits Notifying Nearly 264,000 of Data Theft Hack
Custom-Crafted, Qantas-Spoofing Emails Target Australian Victims

Persistence 10 of 23
- BITS Jobs — $ - 6 Groups
- Boot or Logon Autostart Execution 1 of 14 — $ - 2 Groups
  - Registry Run Keys / Startup Folder — 2 Groups
- Create Account 0 of 3 — $$$ - 1 Groups
- Create or Modify System Process 1 of 5

Privilege Escalation 7 of 14
- Boot or Logon Autostart Execution 1 of 14 — $ - 2 Groups
  - Registry Run Keys / Startup Folder — 2 Groups
- Create or Modify System Process 1 of 5 — $ - 10 Groups
  - Windows Service — 10 Groups
- Event Triggered 1 of 17

Defense Evasion 11 of 45
- BITS Jobs — $ - 6 Groups
- Deobfuscate/Decode Files or Information — $$ - 9 Groups
- Hide Artifacts 2 of 14 — $$$$ - 2 Groups
  - Hidden Files and Directories — 1 Groups
  - Hidden Window — 1 Groups

Credential Access 3 of 17
- Adversary-in-the-Middle 0 of 4 — $ - 3 Groups
- Brute Force 0 of 4 — $$$ - 2 Groups
- OS Credential Dumping 1 of 8 — $ - 1 Groups
  - /etc/passwd and /etc/shadow — 1 Groups

Discovery 10 of 33
- File and Directory Discovery — $$$$$ - 28 Groups
- Network Service Discovery — $$$$$ - 1 Groups
- Network Share Discovery — $$$$$ - 1 Groups
- Process Discovery — $$$$$ - 2 Groups
- Query Registry — $$$$$ - 1 Groups

Lateral Movement 2 of 9
- Lateral Tool Transfer — $$ - 1 Groups
- Remote Services 1 of 8 — $$ - 6 Groups
  - SMB/Windows Admin Shares — 6 Groups

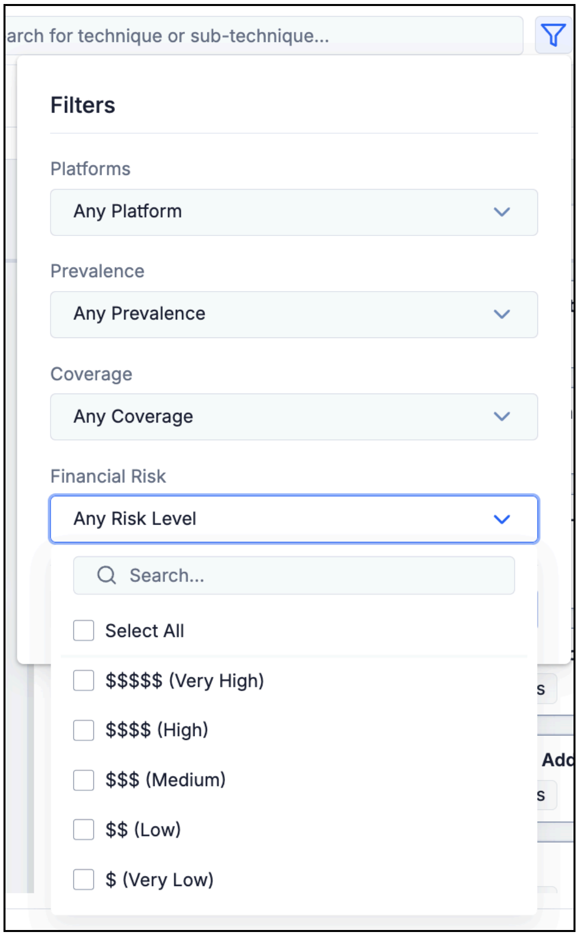
Standard ATT&CK view with Financial Impact coverage applied

Financial Impact Enhancements

ATT&CK RQ Financial Impact comes with two additional features that can be used with any overlay in standard ATT&CK views.

Filter by Financial Risk Categories

In ThreatConnect 7.10, the **Filters** menu in standard ATT&CK views includes a new **Financial Risk** dropdown. This new filter can be combined with the existing filters for platform, technique prevalence, and security coverage, allowing you to prioritize and focus on techniques based on their potential financial consequences.



arch for technique or sub-technique...

Filters

Platforms

Any Platform

Prevalence

Any Prevalence

Coverage

Any Coverage

Financial Risk

Any Risk Level

Search...

□ Select All

□ $$$$$ (Very High)

□ $$$$ (High)

□ $$$ (Medium)

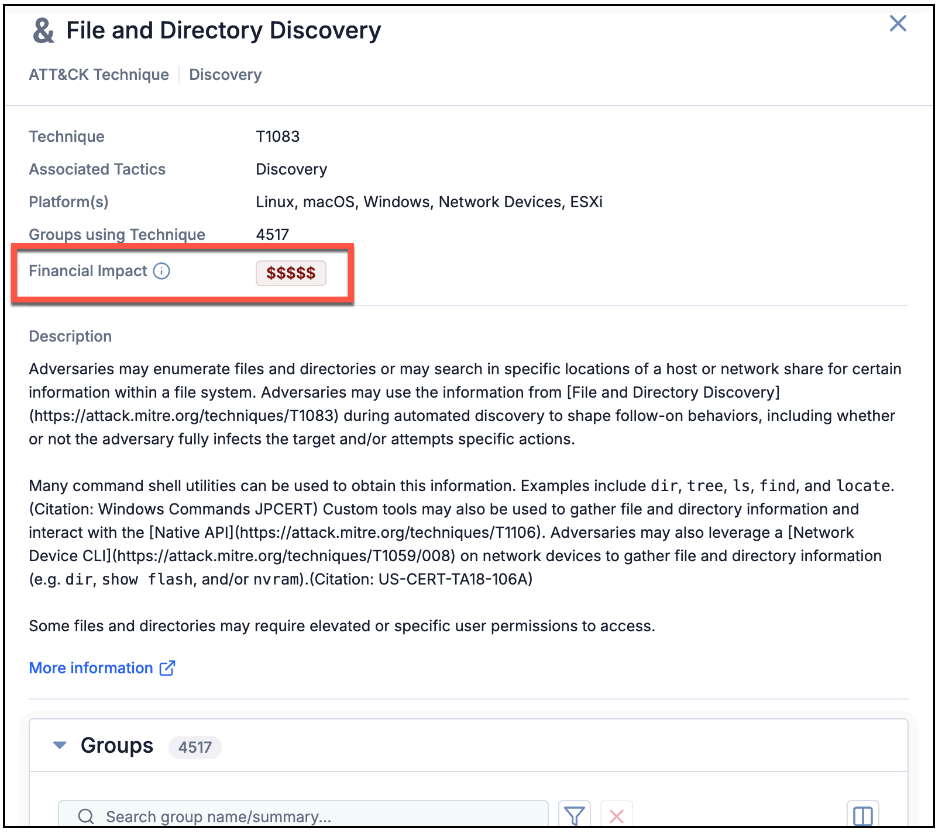
□ $$ (Low)

□ $ (Very Low)

Filter your ATT&CK view to show only techniques that pose a particular level of financial risk

View Financial Impact in Selection Details Drawer

In ThreatConnect 7.10, the **Selection Details** drawer displays a technique's or sub-technique's Financial Impact level, providing you with quick insights into its financial risk.



File and Directory Discovery

ATT&CK Technique | Discovery

Technique	T1083
Associated Tactics	Discovery
Platform(s)	Linux, macOS, Windows, Network Devices, ESXi
Groups using Technique	4517
Financial Impact	$$$$$

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

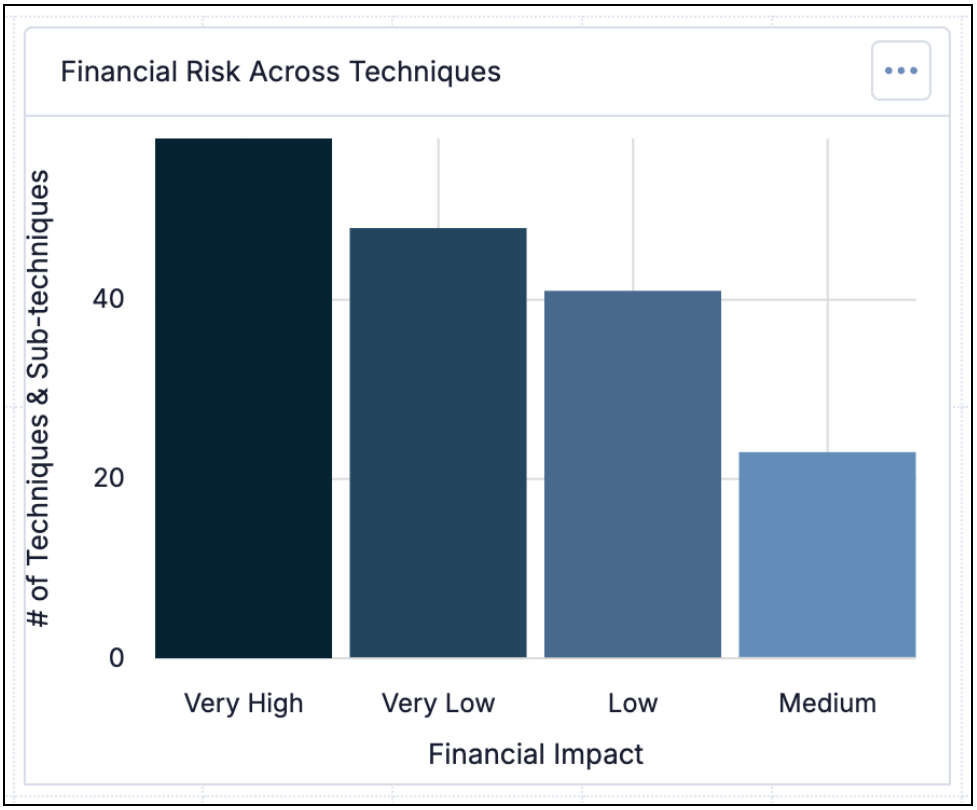
Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`. (Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Some files and directories may require elevated or specific user permissions to access.

View a technique or sub-technique's Financial Impact in its ***Selection Details*** *drawer*

Financial Impact in Dashboard Query Cards

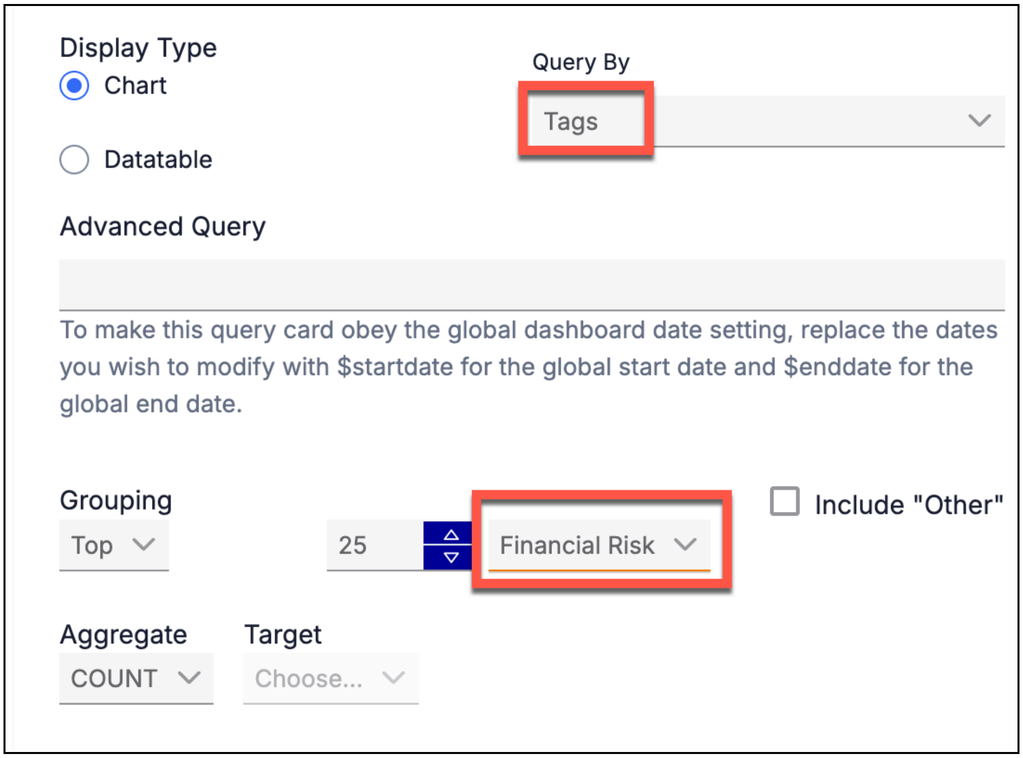
Finally, you can leverage ATT&CK RQ Financial Impact in dashboards by creating a query card displaying the number of techniques and sub-techniques in each risk level. This information can give you deeper insights into your company's distribution of risk and help you prioritize your response strategies.



View the number of techniques and sub-techniques in each risk level in dashboards

To build this query card, make the following selections in Step 2 (**Query**) of the card's configuration:

- Select **Tags** from the **Query By** dropdown.
- Select **Financial Risk** as the Grouping.



Display Type

● Chart

○ Datatable

Query By: Tags

Advanced Query

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.

Grouping: Top | 25 | Financial Risk

□ Include "Other"

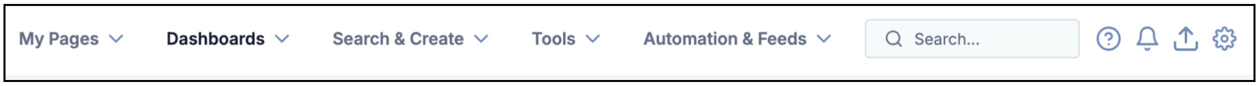
Aggregate: COUNT

Target: Choose...

Configure dashboard query cards to show Financial Impact data

Navigation Redesign

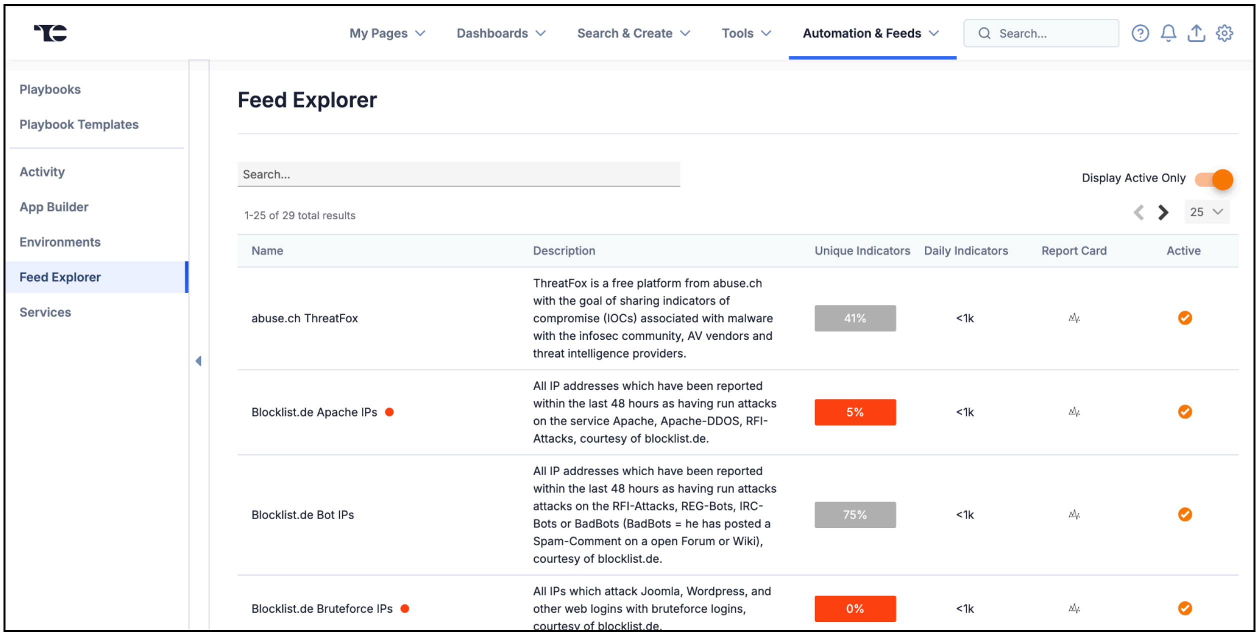
ThreatConnect 7.10 brings a **new, streamlined top navigation bar** to the UI, making it easier to find the features you want and delivering a cleaner look and feel.



The new top navigation bar provides a cleaner, more functional interface

Nested Navigation

The new top navigation bar groups features together intuitively in nested dropdown menus for a sleeker look. For example, the **Tools** menu houses options for the ATT&CK Visualizer, Reporting, Threat Graph, and Workflow, and the **Automation & Feeds** menu contains Playbooks, Playbook Templates, Activity, App Builder, Environments, Feed Explorer, and Services. In addition, a new vertical sidebar for options that share a main menu allows you to quickly navigate between features. You can collapse this sidebar if you want to make more room for the content on the rest of the screen.



Feed Explorer

1-25 of 29 total results

Name	Description	Unique Indicators	Daily Indicators	Report Card	Active
abuse.ch ThreatFox	ThreatFox is a free platform from abuse.ch with the goal of sharing indicators of compromise (IOCs) associated with malware with the infosec community, AV vendors and threat intelligence providers.	41%	<1k		✓
Blocklist.de Apache IPs ●	All IP addresses which have been reported within the last 48 hours as having run attacks on the service Apache, Apache-DDOS, RFI-Attacks, courtesy of blocklist.de.	5%	<1k		✓
Blocklist.de Bot IPs	All IP addresses which have been reported within the last 48 hours as having run attacks attacks on the RFI-Attacks, REG-Bots, IRC-Bots or BadBots (BadBots = he has posted a Spam-Comment on a open Forum or Wiki), courtesy of blocklist.de.	75%	<1k		✓
Blocklist.de Bruteforce IPs ●	All IPs which attack Joomla, Wordpress, and other web logins with bruteforce logins, courtesy of blocklist.de.	0%	<1k		✓

Use the vertical sidebar to navigate between grouped features

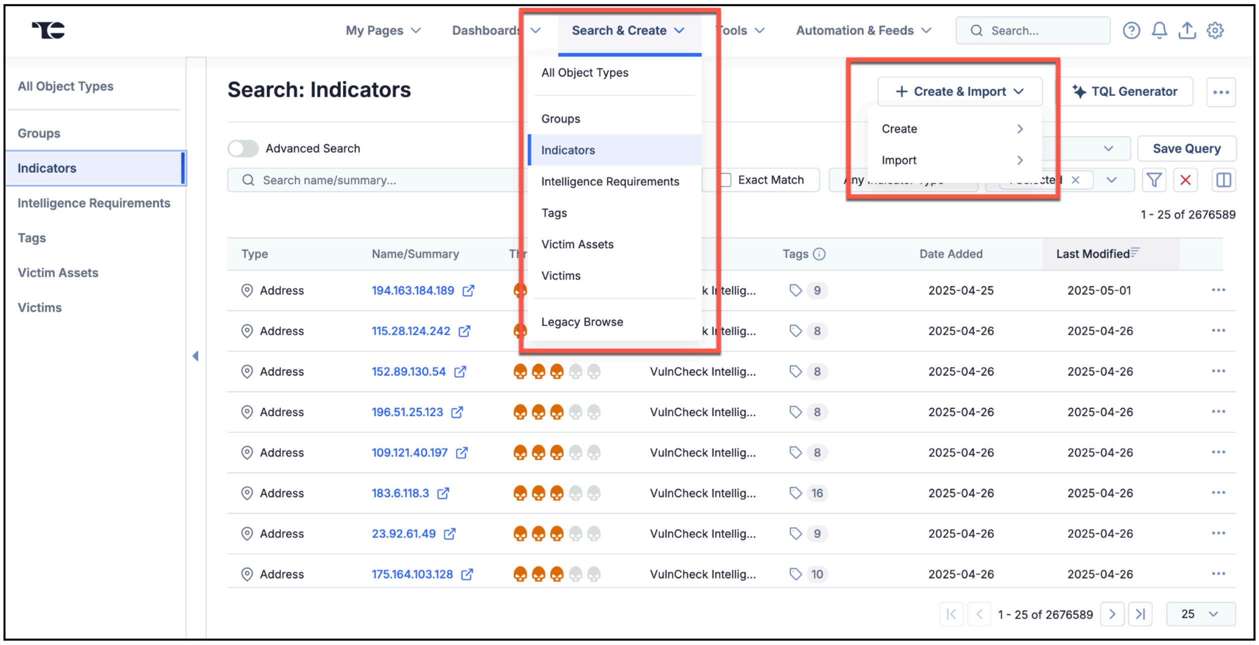
If your display is too small to accommodate the top navigation bar, a **Menu** ☰ icon on the top left of the screen will provide access to all of the options on the top navigation bar instead.

Feature Rearrangement

In addition to the options that have been moved into nested menus, some other features have been moved, added, or otherwise given a makeover. For example, the **Import** menu, which provides access to Doc Analysis import, Email import, Indicator import, and Signature import, has become an icon menu (⇧) between **Settings** ⚙ and **Notifications** 🔔 . (You can also access import options on relevant object-specific **Search** screens—more on this shortly!) The **Help** ? icon is now a dropdown with shortcuts to the ThreatConnect Knowledge Base, the ThreatConnect Support email, the ThreatConnect Developer Hub, and ThreatConnect release notes.

The **Settings** ⚙ menu has been reorganized for better usability. Some of its options include **My Account** (formerly **My Profile**) on top, a section with administrative settings, an option to navigate to deprecated features (**Posts** and **Spaces**), and an option to set the screen you are currently viewing as your homepage in ThreatConnect.

Perhaps most notably, **Search**, **Create**, and **Browse** have been combined under a new **Search & Create** menu, with the **Create** options embedded in **Create** (IRs and Victims) or **Create & Import** (Groups and Indicators) buttons on the object-specific **Search** pages. Many features familiar in **Browse** are available in **Search**'s object-specific pages, which we encourage you to use instead of **Browse**. However, the **Browse** interface is still available under the **Legacy Browse** option in the **Search & Create** menu.

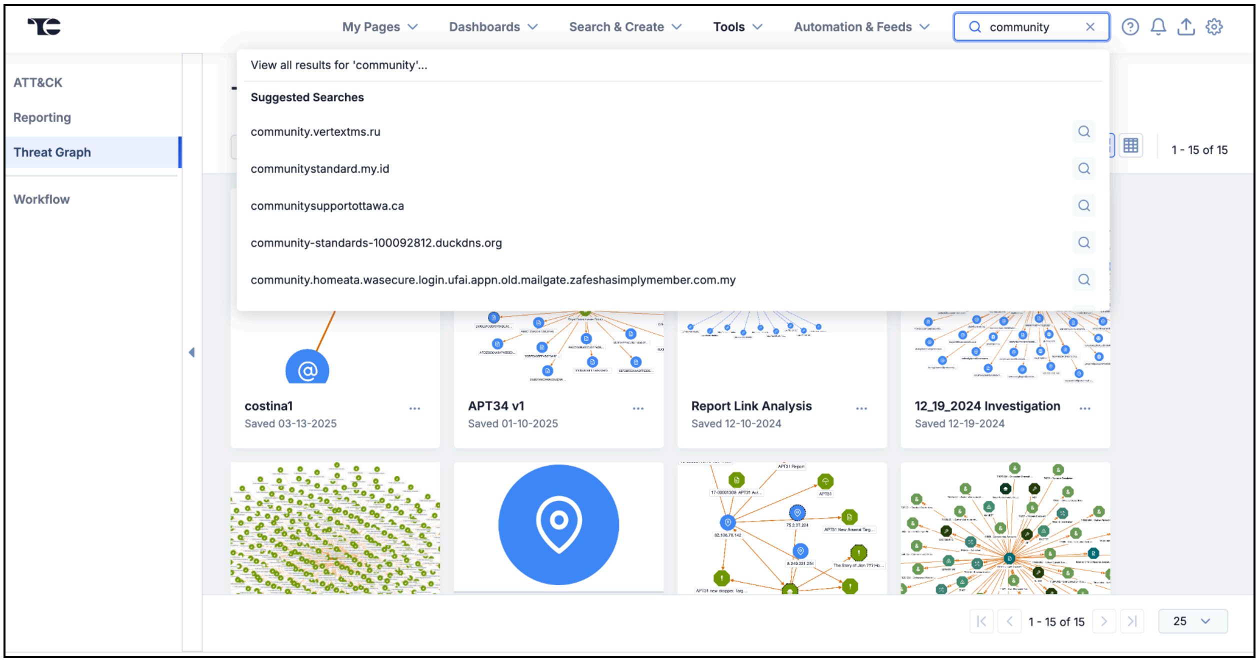


Type	Name/Summary	Th		Tags	Date Added	Last Modified
Address	194.163.184.189	●	k Intellig...	9	2025-04-25	2025-05-01
Address	115.28.124.242	●	k Intellig...	8	2025-04-26	2025-04-26
Address	152.89.130.54	●●●○○	VulnCheck Intellig...	8	2025-04-26	2025-04-26
Address	196.51.25.123	●●●○○	VulnCheck Intellig...	8	2025-04-26	2025-04-26
Address	109.121.40.197	●●●○○	VulnCheck Intellig...	8	2025-04-26	2025-04-26
Address	183.6.118.3	●●●○○	VulnCheck Intellig...	16	2025-04-26	2025-04-26
Address	23.92.61.49	●●●○○	VulnCheck Intellig...	9	2025-04-26	2025-04-26
Address	175.164.103.128	●●●○○	VulnCheck Intellig...	10	2025-04-26	2025-04-26

*Use **Search & Create** to access the **Search** screen, **Create** button, and legacy **Browse***

Navigation Search Bar

With the space gained from these changes, we have added a search bar to the top navigation bar so that you can quickly start looking for information or objects from whatever screen you're on without having to navigate to the **Search** screen.



community

View all results for 'community'...

Suggested Searches

- community.vertextms.ru
- communitystandard.my.id
- communitysupportottawa.ca
- community-standards-100092812.duckdns.org
- community.homeata.wasecure.login.ufai.appn.old.mailgate.zafeshasimplymember.com.my

costina1
Saved 03-13-2025

APT34 v1
Saved 01-10-2025

Report Link Analysis
Saved 12-10-2024

12_19_2024 Investigation
Saved 12-19-2024

Use the new top navigation search bar to search for data from any screen in ThreatConnect

My Pages

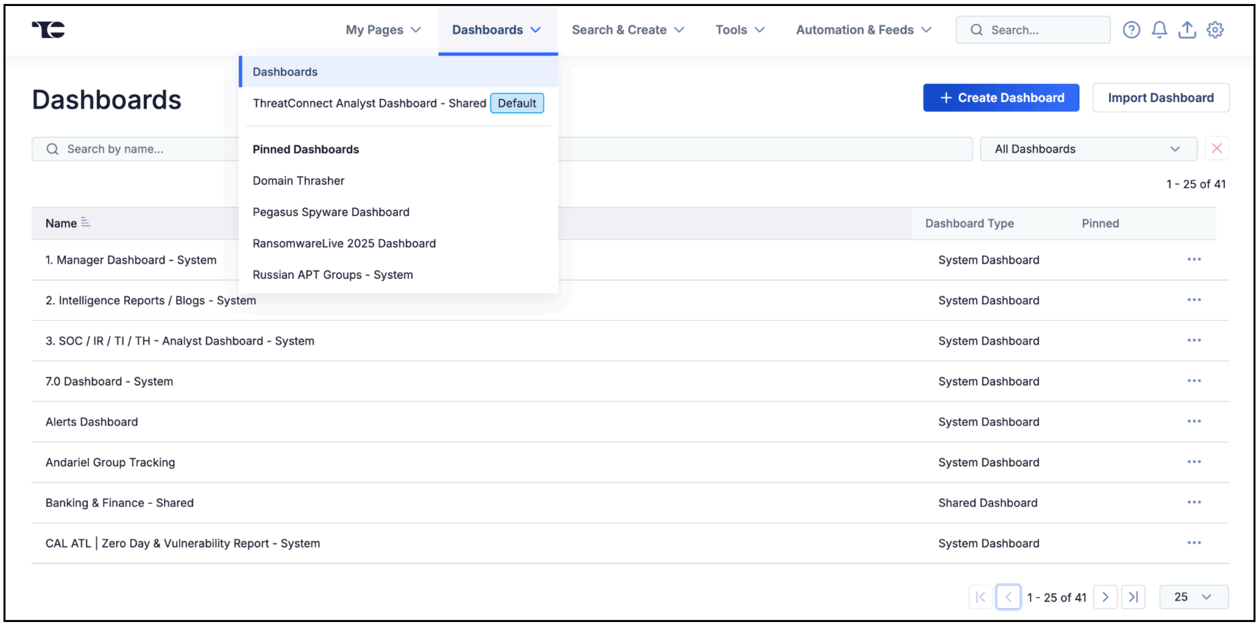
In addition to the other navigation changes, you now have the option to **select up to 10 pages from anywhere in ThreatConnect that will appear as quick links** in the **My Pages** dropdown. To add a page, you only need to navigate to the page, select **Add to My Pages** from the **My Pages** dropdown, and save a name for the shortcut. This new feature allows you to maintain a list of the pages you visit most often without needing to rely on browser bookmarks.

Hint: You can use **My Pages** to bookmark filtered object-specific **Search** screens. For example, you can use it to create a shortcut to **Search: Indicators** filtered to show only Hosts in your Organization. You can also use it to bookmark the **Posts** or **Spaces** screen if you still use those screens and do not want to navigate to them through the **Deprecated Features** option in the **Settings** ⚙ menu.

Important: Note that, as of ThreatConnect 7.10, you cannot change the saved name for a screen in the **My Pages** dropdown. However, a quick workaround is to navigate to the page, save it again in **My Pages** with the new name, and then delete the entry with the previous name.

Dashboards Landing Page

ThreatConnect 7.10 debuts a **new dashboards landing page** where you can view, search, and take action on your dashboards. From this new page, you can view all of your dashboards: My Dashboards, shared dashboards (i.e., Organization-level dashboards), and System dashboards. You can also create and import dashboards, search for and filter dashboards, manage (e.g., export, copy, rename, save, share, and delete) dashboards, select a default dashboard, and pin up to 10 dashboards that will be displayed in your **Pinned Dashboards** list under the **Dashboards** option on the top navigation bar.



Dashboards

1 - 25 of 41

Name	Dashboard Type	Pinned
1. Manager Dashboard - System	System Dashboard	
2. Intelligence Reports / Blogs - System	System Dashboard	
3. SOC / IR / TI / TH - Analyst Dashboard - System	System Dashboard	
7.0 Dashboard - System	System Dashboard	
Alerts Dashboard	System Dashboard	
Andariel Group Tracking	System Dashboard	
Banking & Finance - Shared	Shared Dashboard	
CAL ATL | Zero Day & Vulnerability Report - System	System Dashboard	

1 - 25 of 41 25

*View and manage all of your dashboards from the new **Dashboards** landing page, and quickly navigate to pinned dashboards from the top navigation bar*

Toggle to Legacy Navigation

If you still prefer to use the previous version of the top navigation bar, you can toggle back to it with the **Switch to Legacy Navigation** option in the **Settings** ⚙ menu. However, keep in mind that this older version does not include **My Pages**, the search bar, the ability to set a custom homepage, or a direct link into the new **Dashboards** landing page.

Actionable Search Version 2

ThreatConnect 7.10 significantly enhances the powerful Actionable Search feature, first introduced in ThreatConnect 7.8. Building on the ThreatConnect search engine's ability to parse and analyse Indicators from uploaded files, as well as display and filter the data you already have in your ThreatConnect owners, these new updates will bring even greater efficiency and flexibility to your threat intelligence workflows.

Actionable Search in 7.10 improves the unstructured import capability of the **Bulk Search Indicators** feature, enabling you to **ingest unstructured Indicator data from four more file types**. You can then use another new feature—**bulk actions**—to add multiple unknown Indicators (that is, Indicators that do not exist in any of your ThreatConnect owners) or Indicators in your Communities and Sources to your Organization at once, as well as add Tags to or export multiple known Indicators in a single action. These enhancements empower you to process and manage large volumes of diverse IOC data easily and quickly. You can also leverage bulk actions to add Tags and export objects when searching data in your ThreatConnect owners in the **All Object Types** view.

Unstructured Indicator Import File Types

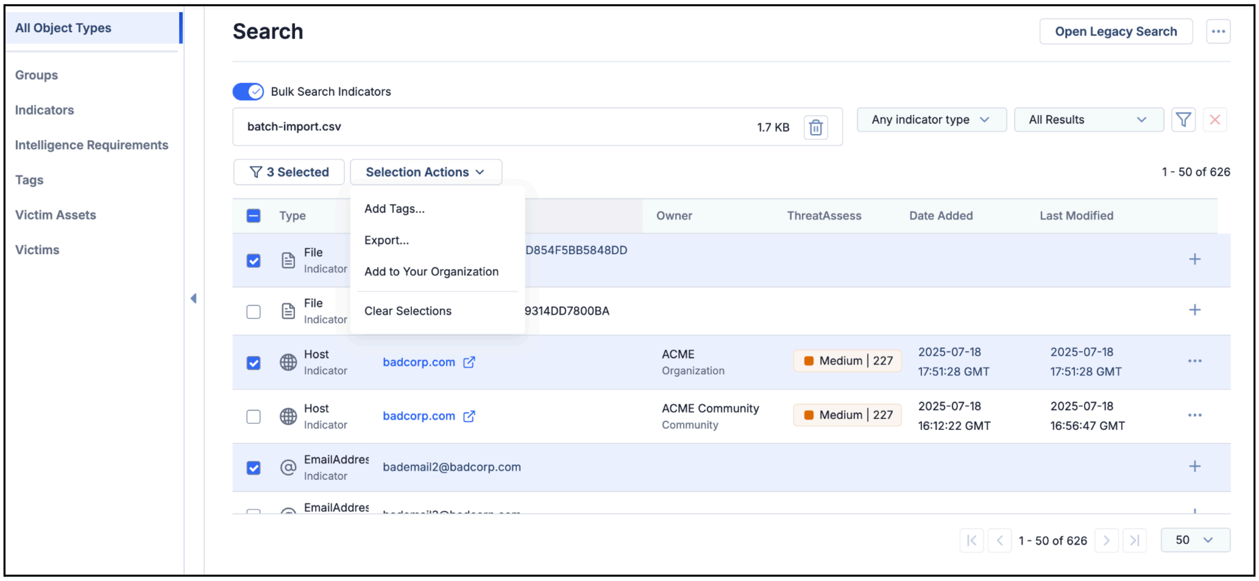
Building on the file upload capabilities introduced in ThreatConnect 7.8, which allow you to ingest Indicators from .txt, .csv, and .xls files, Actionable Search in ThreatConnect 7.10 significantly expands its import functionality by allowing you to directly upload .doc, .xlsx, .json, and .pdf files in Bulk Search. ThreatConnect will intelligently parse these files, automatically identifying and extracting known and unknown Indicators. This new capability eliminates the need for manual sifting, allowing you to process the information in unstructured reports and spreadsheets quickly.

Bulk Actions in Search

When searching in a dataset you uploaded in the **Bulk Search Indicators** view or across all object types in your ThreatConnect owners, you can now select multiple objects and then use the new **Selection Actions** dropdown to perform an action on objects in this curated set at one time:

- **Add Tags...**: Use this option to add Tags to all selected objects in the results table in owners for which your user account has permission to create data. In the **Bulk Search Indicators** view, if you do not have any known Indicators selected, then this option will not be available, as Tags cannot be added to an Indicator that does not yet exist in ThreatConnect. If you have selected known and unknown Indicators, then the Tags will be applied only to the known Indicators.

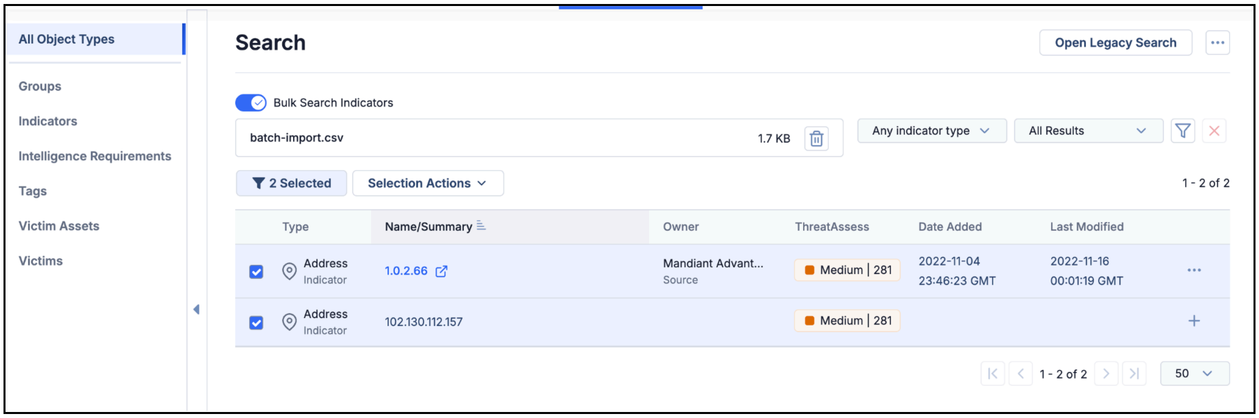
- **Export…**: Use this option to export all selected objects in the results table to a .csv file. In the **Bulk Search Indicators** view, if you do not have any known Indicators selected, then this option will not be available, as Indicators that do not yet exist in ThreatConnect cannot be exported. If you have selected known and unknown Indicators, then only the known Indicators will be exported.
- **Add to Your Organization**: Use this option, available only in the **Bulk Search Indicators** view, to add all selected Indicators in the results table to your Organization. This is a useful way to add multiple unknown Indicators from a file to your Organization, as well as to add multiple Indicators from other ThreatConnect owners to your Organization.



	Type		Owner	ThreatAssess	Date Added	Last Modified
☑	File Indicator	D854F5BB5848DD				
□	File Indicator	9314DD7800BA				
☑	Host Indicator	badcorp.com	ACME Organization	Medium | 227	2025-07-18 17:51:28 GMT	2025-07-18 17:51:28 GMT
□	Host Indicator	badcorp.com	ACME Community Community	Medium | 227	2025-07-18 16:12:22 GMT	2025-07-18 16:56:47 GMT
☑	EmailAddres Indicator	bademail2@badcorp.com				
□	EmailAddres					

*Use the new **Selection Actions** menu to perform bulk actions on selected objects*

You can also now quickly filter the results table to display only the items you have selected across all pages of the table, making it quick and simple for you to visualize a curated dataset.



batch-import.csv 1.7 KB

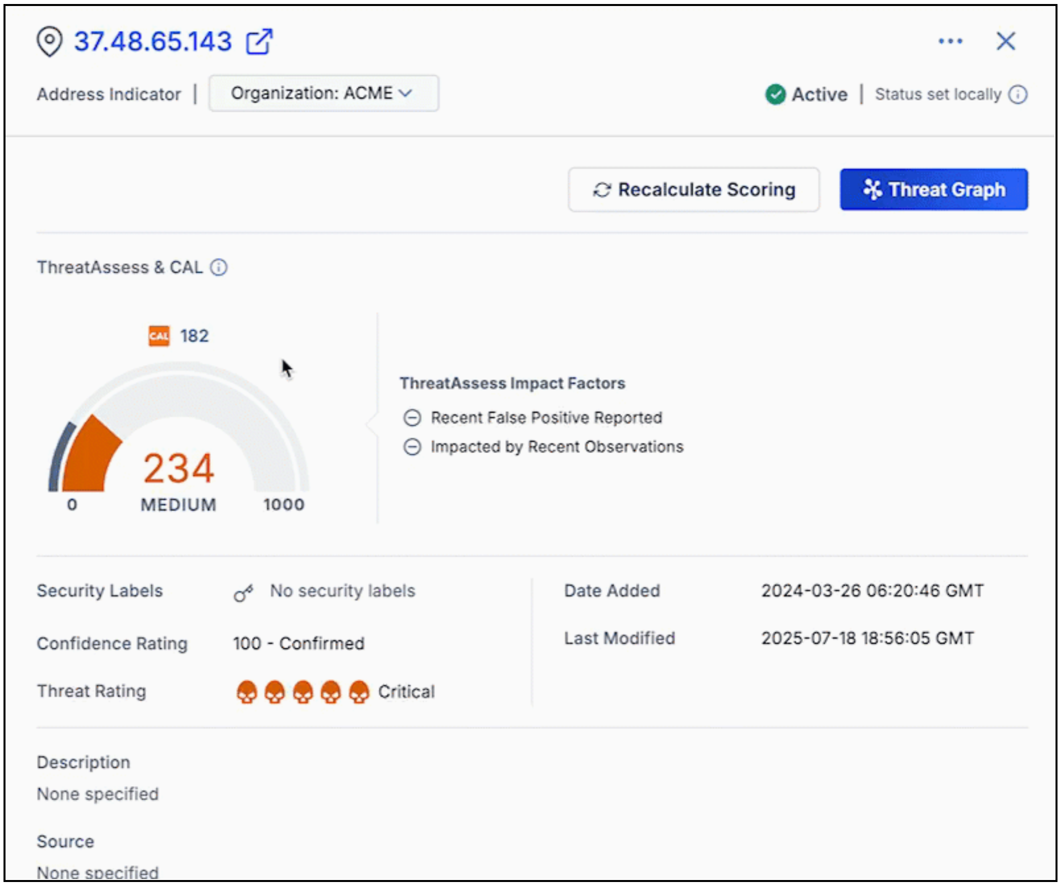
	Type	Name/Summary	Owner	ThreatAssess	Date Added	Last Modified
☑	Address Indicator	1.0.2.66	Mandiant Advant... Source	Medium | 281	2022-11-04 23:46:23 GMT	2022-11-16 00:01:19 GMT
☑	Address Indicator	102.130.112.157		Medium | 281		

View only selected objects from your results set

These enhancements to the **Search: All Object Types** feature provide you with an increased degree of flexibility and control over your data, enable you to work more quickly and efficiently, and simplify data sharing, ingestion, and record keeping.

Recalculate ThreatAssess Score On Demand

In the ThreatConnect 7.10 release, we add the ability to manually recalculate the ThreatAssess score for an Indicator directly from the Indicator **Details** screen and drawer. The new **Recalculate Scoring** button allows you to instantly refresh the ThreatAssess score for an Indicator—for example, after you update the Indicator's Threat Rating or Confidence Rating—without needing to wait for the ThreatAssess monitor to run at its scheduled time. This feature provides you with direct control to ensure that an Indicator's ThreatAssess score is accurate and up to date when working with ever-changing Indicator context during an investigation.



37.48.65.143

Address Indicator | Organization: ACME

Active | Status set locally

ThreatAssess & CAL

CAL 182

234 MEDIUM

ThreatAssess Impact Factors

⊖ Recent False Positive Reported

⊖ Impacted by Recent Observations

Security Labels	No security labels	Date Added	2024-03-26 06:20:46 GMT
Confidence Rating	100 - Confirmed	Last Modified	2025-07-18 18:56:05 GMT
Threat Rating	Critical		

Description

None specified

Source

None specified

***Recalculate Scoring** updates an Indicator's ThreatAssess score in an instant*

Improvements

Dashboards

- The screen for individual dashboards has been redesigned to provide a sleeker, more functional interface.
- You can now collapse the header area in dashboards to allow more screen area for the rest of the feature. In addition, the header for individual dashboards has been redesigned for improved navigation and user experience.
- The color scheme options for dashboard cards have been updated.
- The following System dashboards have been added to all 7.10 instances, providing you with a variety of built-in solutions to track and analyze high-impact trends and data:
    - **Strategic Intel - Observed on IoCs and Reports**: This dashboard shows Indicators, Malware, ATT&CK Patterns, Vulnerabilities, Intrusion Sets, and Adversaries that have reported observations. It can be used to quickly identify threats that are currently active.
    - **Andariel Group Tracking**: Use this dashboard to track Andariel activity. Andariel is a threat group with a likely nexus to North Korea. The dashboard shows Andariel-related indicators of compromise and intelligence. It also gives you a quick overview of intelligence metrics related to recent reporting on, and activity conducted by, the group, based on the data available in your ThreatConnect instance.
    - **Lazarus Group Dashboard**: This dashboard gives you a quick way to access strategic and tactical intelligence related to Lazarus Group. Lazarus Group is a threat group with a likely nexus to North Korea. Use this dashboard to collect metrics on intelligence related to Lazarus Group and quickly access recently released reporting and reported indicators of compromise associated with the group.
    - **Medusa Ransomware Tracking**: This dashboard provides quick access to metrics on Indicators, Groups, and owners with information mentioning the Medusa ransomware, as well as Indicators, ATT&CK techniques, Vulnerabilities, and reporting related to Medusa.
    - **Pegasus Spyware Dashboard**: This dashboard provides an overview of tactical and strategic intelligence metrics, as well as an easy-to-find list of relevant Indicators and recent reporting related to the spyware.

    - **Russian APT Groups Dashboard**: This dashboard aggregates available strategic and tactical intelligence on the following threat actor groups with a likely nexus to Russia: APT28, APT29, FIN7, Energetic Bear, Turla Group, and Sandworm.
    - **ThreatConnect Geo-Actor PIRs**: This dashboard shows Intelligence Requirement results related to IRs designed to gather information related to Russia-, China-, Iran-, North Korea–, and Middle East–based threat actor groups. In order to populate this dashboard, you should work with your Customer Success representatives to make sure the relevant IRs exist in your ThreatConnect instance.

Search

- In all **Search** screens except **Bulk Search Indicators**, the **Owners** filter has been moved out of the **Filters** ▽ menu to help you quickly and easily select the owners whose data you want to search.
- Attribute filters added in the **Filters** ▽ menu on the **Search: Groups**, **Search: Indicators**, and **Search: Victims** screen will now persist across sessions and page refreshes.
- You can now follow and unfollow IRs from their **Options** ··· menu on the **Search: Intelligence Requirements** screen.
- Bulk Indicator Search can now parse up to 8000 Indicators from a single file.
- Bulk Indicator Search can now parse and filter on custom Indicator types configured for your ThreatConnect instance.

ATT&CK

- Standard and imported views in the ATT&CK Visualizer now display the MITRE ATT&CK version (currently 17.0) at the upper right of the screen. The correct version number will also now be included in JSON files exported from the ATT&CK Navigator.
- You can now collapse the header area in ATT&CK views to allow more screen area for the rest of the feature.

Threat Graph

- The Threat Graph landing page has been redesigned. You can display it in card or list view, and each Threat Graph's **Options** ⋯ menu provides a new option to save a copy in addition to the pre-existing options to rename or delete.

Reporting

- You can now configure whether headers and footers for Reports and Report Templates should be displayed on all pages, the first page only, or all pages except the first page.
- In Reports created with the Reporting feature, the **Summary** column in tables now contains clickable hyperlinks to ThreatConnect objects if your ThreatConnect instance is configured to allow hyperlinks in Reporting.

Threat Intelligence

- Users, including API users, with read-only permissions in an owner can now update the status of Event Groups in the owner if the **readOnlyUserUpdatesAllowed** system setting is turned on. Note that this system setting was previously named **v3ApiReadOnlyReports**.

Administrative Settings

- The Reverse Whois feature has been deprecated:
    - **System Settings**: The **Advanced - Reverse WhoIs** section and the settings it included have been removed.
    - **Organization Settings**: The **Reverse Whois** section on the **Settings** tab has been removed.
    - **Community Config** and **Source Config**: The **Settings** tab has been removed.
- The following new system settings were added:
    - **commonBucketMonitorEnabled**: This system setting turns the Common Bucket Monitor on or off, which enables the unified view for Vulnerabilities. It is enabled by default.

    - **financialImpactEstimates**: When turned on, this system setting turns on RQ ATT&CK Financial Impact, allowing Organization Administrators to configure Financial Impact in the ATT&CK Visualizer.
- The following system settings were updated:
    - **readOnlyUserUpdatesAllowed** (formerly **v3ApiReadOnlyReports**): When turned on, this system setting allows users, including API users, with read-only permissions in an owner to report false positives and observations for Indicators and update the status for Event Groups.
- The Redis® system settings for Playbooks have been removed from the **System Settings** screen in ThreatConnect and can now be configured only with the installer.

Miscellaneous

- Browser tab titles for ThreatConnect pages have been updated to be more informational and content specific.

API & Under the Hood

- You can now retrieve unified view data for Vulnerability Groups using the v3 API. To include unified view data for Vulnerability Group objects in a response body, add the `fields` query parameter to the request and set its value to one or both of the following:
    - `common`: Includes details such as CVSS and KEV data for a given Vulnerability.
    - `linkedGroups`: Includes details about all Vulnerability Groups that share the same name/summary as the "common" Vulnerability Group and exist in your owners.
- You can now retrieve Financial Impact and risk data for ATT&CK Tags using the v3 API. To include Financial Impact and risk data for ATT&CK Tag objects in a response body, add the `fields` query parameter to the request and set its value to `financialImpact`.
- The connection to the containerized Postgres® database can now be a secure transport layer security (TLS) connection based on a customer certificate.
- The connection to the containerized Redis database can now be a secure TLS connection based on a customer certificate.
- Support for adding certificates to the Trust Store for Java® and Python® was added for containerized ThreatConnect deployments.

- Support was added to set up and control cipher suites in the ThreatConnect installer.
- ThreatConnect containers can now be configured to use Amazon Web Services® (AWS) for document storage.
- MDB `maxsession` properties set directly in the **threatconnect.xml** file for operating-system deployments are no longer lost during upgrade.
- ThreatConnect containers can be configured to use any unique identifier (UID). Previously, only UID=1000 could be used.

Bug Fixes

Threat Intelligence

- Tags are now listed in alphabetical order on the new **Details** screen.
- An issue preventing Indicator activity logs from displaying entries for changes to Indicator Status made through the V2 Batch API was corrected.
- An issue causing observation counts to be too high was resolved.

Search

- An issue causing **Search: All Object Types** to exclude results for search terms enclosed by non-space, non-special characters when **Exact Match** is turned off has been fixed.

Threat Graph

- An issue preventing Super Users from viewing Threat Graphs in Organizations other than their home Organization was corrected.

Playbooks

- The **Time** column in Playbook audit logs was being sorted incorrectly. This issue has been resolved.
- An issue preventing users with an Organization role of App Developer from saving labels for Playbooks has been resolved.

Workflow

- Performance improvements were made in the Workflow Cases UI.

Administrative Settings

- Support was added for setting a value containing one or more slash characters (**/**) for the **documentAwsBucketName** system setting.

Apps & Jobs

- An issue causing **Organization Settings** › **Apps** › **Jobs** to show incorrect Job start times, which made it look like Jobs were not running according to schedule, was fixed.
- An intermittent issue causing Jobs to fail when modifying system data, mainly during feed ingest, under periods of high load was fixed.

API

- The OpenAPI Specification for the v3 API now includes complete documentation for the `groups/v3/security/exclusionLists` endpoint.
- When creating a Group-to-Group association in a PUT request to the `/v3/groups` endpoint, targeting a Group by its XID in the request body no longer creates a duplicate Group and uses it in the association.

Dependencies & Library Changes

- There are no new dependencies or library changes for ThreatConnect version 7.10.0.

Maintenance Releases Changelog

2025-11-13 7.10.2-M1113R [Latest]

Bug Fixes

- 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.

2025-09-25 7.10.2-M0926R

Bug Fixes

- When navigating to a deep-link URL in their ThreatConnect instance, users with multifactor authentication (MFA) enabled were being redirected to their default dashboard screen after login instead of to the URL. This issue has been corrected.
- An issue preventing variables for Intelligence Requirements from being passed through Playbooks with Intelligence Requirement Triggers, causing `VARIABLE_NOT_FOUND` errors to occur, was resolved. Note that this resolution resulted in changes to some of the variable names, which may require you to update variable selections throughout the Playbook.
- An issue causing the TQL Generator to be available even when the feature was turned off in the system settings was fixed.

2025-09-22 7.10.2-M0922R

Bug Fixes

- The default logout interval on SAML-enabled instances was increased to 14400 seconds (4 hours). This update resolves an issue that was causing users on these instances to be automatically logged out after 600 seconds (10 minutes).

2025-09-18 7.10.2

Improvements

- Improved system performance by fixing a Playbooks memory issue that could cause slowdowns over time. The application now automatically cleans up references to long-running background processes that used Sleep/Delay, to prevent performance degradation.
- All plain-text passwords have been removed from the `.env` file and should be set as environment variables instead.
- Performance and logging improvements were made to the monitor that ingests unified Vulnerability Group data from CAL™.

Bug Fixes

- Improvements were made to the owner selector on the **Search** screens to allow more owners to be displayed in the scrollable area.
- An issue causing discrepancies between Indicators returned on the **Search: All Object Types** screen and the **Search: Indicators** screen has been resolved.
- When API users made DELETE requests via the v3 API for a Group they don't have permission to delete, a success message was being returned, even though the Group was (correctly) not deleted. This issue has been fixed.
- The **JS Report** Service was fixed to allow it to work in a fully distributed ThreatConnect environment where the Redis server is secured with certificate-based TLS encryption, using a custom certificate authority (CA) signed certificate.
- On ThreatConnect instances with Security Assertion Markup Language™ (SAML™) enabled, the user's logout interval can no longer be accessed or modified on the user's **My Profile** screen or when editing the user's account in **Organization Settings**. Instead, the logout interval set by the identity provider (IdP) is enforced for all users across the instance.

2025-08-28 7.10.1-M0828R

Bug Fixes

- Instances with configured proxies are no longer blocked from seeing CAL data in the ThreatConnect UI.
- An issue preventing SAML logins was corrected.
- Upgrades to version 7.10.1 of ThreatConnect were being blocked if the Redis password was set during a previous upgrade to 7.10.0. This issue has been resolved.

2025-08-22 7.10.1

Improvements

- When exporting Indicators from the **Search: Indicators** screen, you can now include ThreatAssess score in the CSV file.
- The following new system setting was added:
    - **threatDeprecationIntervalCount**: This setting determines the number of Indicators that are deprecated each time the Indicator Deprecation Monitor runs. Increasing its value will help instances that are severely behind on their Indicator deprecations to catch up. However, setting this value too high may prevent the Indicator Deprecation Monitor from finishing its deprecations in a single execution, which would cause it to skip the next execution and negate the benefit of increasing the value.

Bug Fixes

- An issue preventing the title of some Cases Metrics dashboard cards from being displayed when the cards are populated with data was fixed.
- In a saved Threat Graph, if there are objects that a user does not have permission to access, then the user will not be able to open the Threat Graph.
- Users with Community roles that do not allow data deletion in a Community or Source were being allowed to delete individual objects on the **Search: All Object Types** screen. This issue has been corrected. Users with high-level administrative access such as System Administrators should ensure that they have a Community role that

allows deletion in Communities and Sources in which they will need that access to data.

- The **Search: All Object Types** screen was omitting custom Indicator types from the search results when filtering on Group types unless all Indicator types were selected or the custom Indicator types were selected individually. In addition, Bulk Indicator Search was not including custom Indicator types in the search results. These issues have been fixed.
- The **Result Details** drawer for search results on the **Search: All Object Types** screen was not highlighting partial matches (i.e., keywords that are part of other terms, such as **bad** in **badguy.com**). This issue was resolved.
- Initialization of Indicator confidence deprecation now requires only that the Indicator have a Confidence Rating rather than a Confidence Rating and a Threat Rating.
- An issue preventing deletion of owners containing objects that have associations to objects in other owners was fixed.
- When attempting to install an App that requires a newer version of ThreatConnect than the one you have installed, you will now see an error message with information about the required version.
- An issue causing activation of the Recorded Future Intelligence Engine Service App to fail after the App has been upgraded was fixed.
- An issue causing an error to occur when installing ThreatConnect and SAML at the same time was fixed.
- Logging dependency vulnerabilities were remedied.
- A vulnerability associated with single sign-on (SSO) was resolved.
- An issue causing latency when switching the **Attributes** card on an object's **Details** screen from the table view to the detailed view has been resolved.

2025-08-08 7.10.0-M0808R

Improvements

- ThreatConnect instances with CAL enabled will now check for new Vulnerability Groups every 30 minutes.

Bug Fixes

- An issue that sometimes prevented new Vulnerability Groups from being created via the v3 API was fixed.

- An issue causing errors to occur when identifying and consolidating Vulnerabilities for the unified view has been resolved.

2025-08-06 7.10.0-M0806R

Improvements

- Performance improvements were made in the identification and consolidation of Vulnerabilities for the unified view.