ThreatConnect® Release Notes

Software Version 7.2

July 26, 2023

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 **4**
- ATT&CK Visualizer 5
  - Convert Existing Tags to ATT&CK Tags 9
- Built-In Enrichment: urlscan.io 12
- Report Dissemination 15
- New Import Option: Doc Analysis 17

Improvements **18**
- Threat Intelligence 18
- Enrichment 19
- Reporting 19
- Playbooks 19
- App Builder 19
- System Settings 20
- Organization Settings 20
- TC Exchange 21
- API & Under the Hood 21

Bug Fixes **22**
- Threat Intelligence 22
- Playbooks 22
- App Builder 23
- Attributes 23
- Threat Graph 23
- API & Under the Hood 23

Dependencies & Library Changes **24**

Maintenance Releases Changelog **25**
- 2023-09-26 7.2.1-M0926R [Latest] 25
  - Bug Fixes 25
- 2023-09-21 7.2.1-M0921R 25
  - Bug Fixes 25
- 2023-09-11 7.2.1-M0911R 25
  - Bug Fixes 25
- 2023-08-31 7.2.0-M0831R 25
  - Bug Fixes 25

2023-08-24 7.2.1 26
Bug Fixes 26
2023-08-10 7.2.0-M0810R 27
Bug Fixes 27
2023-08-03 7.2.0-M0803R 27
Bug Fixes 27
2023-08-03 7.2.0-M0803S 27
Bug Fixes 27

New Features and Functionality

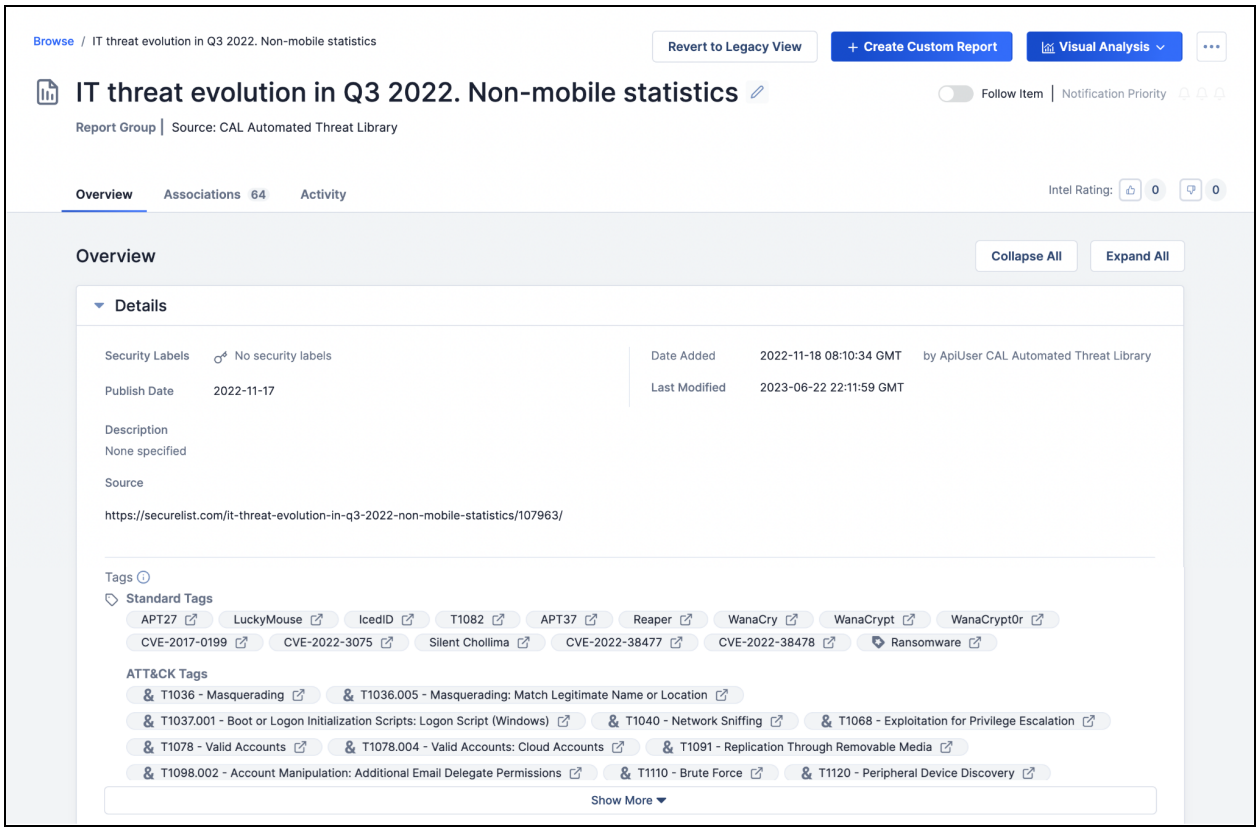
ATT&CK Visualizer

ThreatConnect's 7.2 release is packed with electrifying features and game-changing advancements that will enhance your cyber threat intelligence production, facilitate intelligence dissemination, and offer a big-picture view of patterns and trends. First off, we're immensely proud to debut **ATT&CK Visualizer**, a mighty new tool for cyber defense. This revolutionary feature brings the tried-and-true MITRE ATT&CK® Navigator view directly into ThreatConnect.

With ATT&CK Visualizer, we're supercharging your capability to assess tactics, techniques, and procedures (TTPs) used by individual threat groups. You can explore in-depth details about tactics, techniques, and sub-techniques and identify overlapping techniques used by different threat groups. You can also export this view as a sleek PNG file!

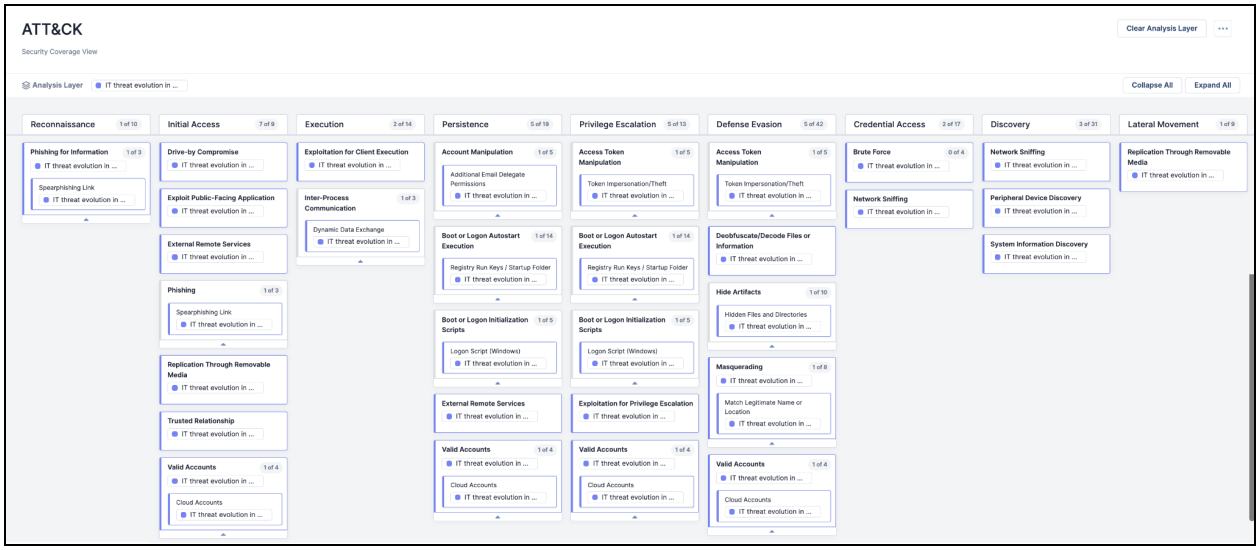
Unleash the power of ATT&CK Visualizer with these easy-to-use functionalities:

1. **Start with a Group's ATT&CK Tags**: To begin your journey, apply our new ATT&CK Tags to any Group. To streamline the representation of techniques and sub-techniques in ThreatConnect, we've implemented standardized, system-provided ATT&CK Tags for all TTPs. These Tags are distinguished by an **&** icon at the beginning and are conveniently grouped into their own section of the Tags list on a Group's **Details** screen or drawer. But that's not all! We have introduced an autocomplete feature that makes selecting these new Tags a breeze, significantly simplifying your tagging process and giving you a foundation to start mapping the techniques and sub-techniques used by that specific Group.



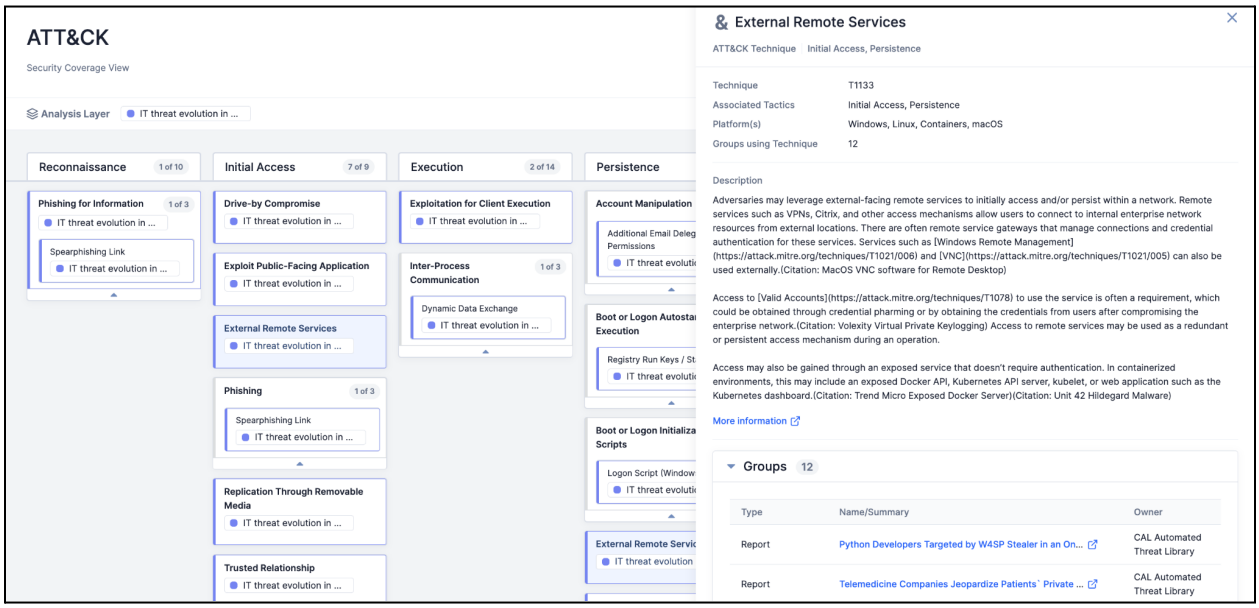
ATT&CK techniques and sub-techniques are represented as ATT&CK Tags

2. **Launch the Visualizer**: Once your Tags are in place, navigate to the Group's **Details** screen or drawer and simply click the **Visual Analysis** button and then select **Visualize ATT&CK**. This action will take you into the ATT&CK Visualizer, where you can explore and analyze the specific techniques and sub-techniques employed by your Group. You can also access the ATT&CK Visualizer from the **ATT&CK** option on the top navigation bar. From the Visualizer, you can start your analysis by clicking on **Add Analysis Layer** and selecting a single Group. You'll then be able to visualize that Group's unique techniques and sub-techniques.



Visualize techniques and sub-techniques used by a Group

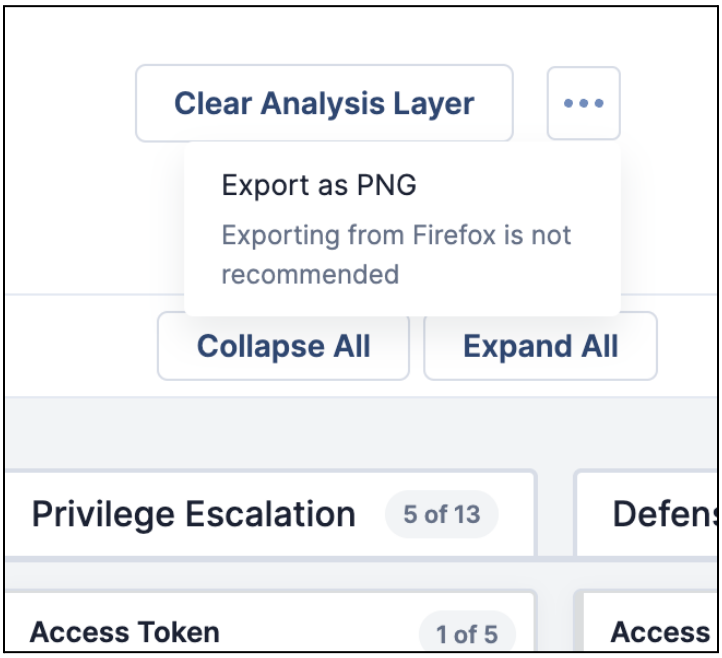
3. **Dive Deeper**: By clicking on any technique or sub-technique in the ATT&CK Visualizer, you can delve into a deeper layer of analysis. Discover more about the specific strategy employed, and find out which other Groups are using the same technique.



View details about a technique or sub-technique, and see which other Groups are using it

4. **Export Your insights**: Once your view is built in the ATT&CK Visualizer and you're satisfied with your analytical journey, you can easily export the Visualizer view as a PNG

file, allowing you to share your crucial insights with other stakeholders and thereby enabling a comprehensive and collaborative understanding of the threatscape.



Export the ATT&CK Visualizer view as a PNG file

With these steps, the ATT&CK Visualizer not only equips you with the tools to dissect and comprehend complex cyber-threat patterns, but also facilitates seamless sharing of your findings for wider intelligence dissemination.

The ATT&CK Visualizer is designed to adapt dynamically to the latest updates from MITRE regarding ATT&CK techniques and sub-techniques. If you have CAL™ enabled on your ThreatConnect instance, the ATT&CK Visualizer will be instantly populated with the most current data sourced directly from CAL. This ensures that your ATT&CK Tags remain synchronized with the newest and most relevant information provided by MITRE.

However, even if you haven't enabled CAL, you can still access your organization's essential ATT&CK data. The only difference is that you will have the latest MITRE data available to you during each ThreatConnect release cycle. This means that your cyber threat intelligence will always be readily available, continuously updated, and uninterrupted, regardless of your CAL status.

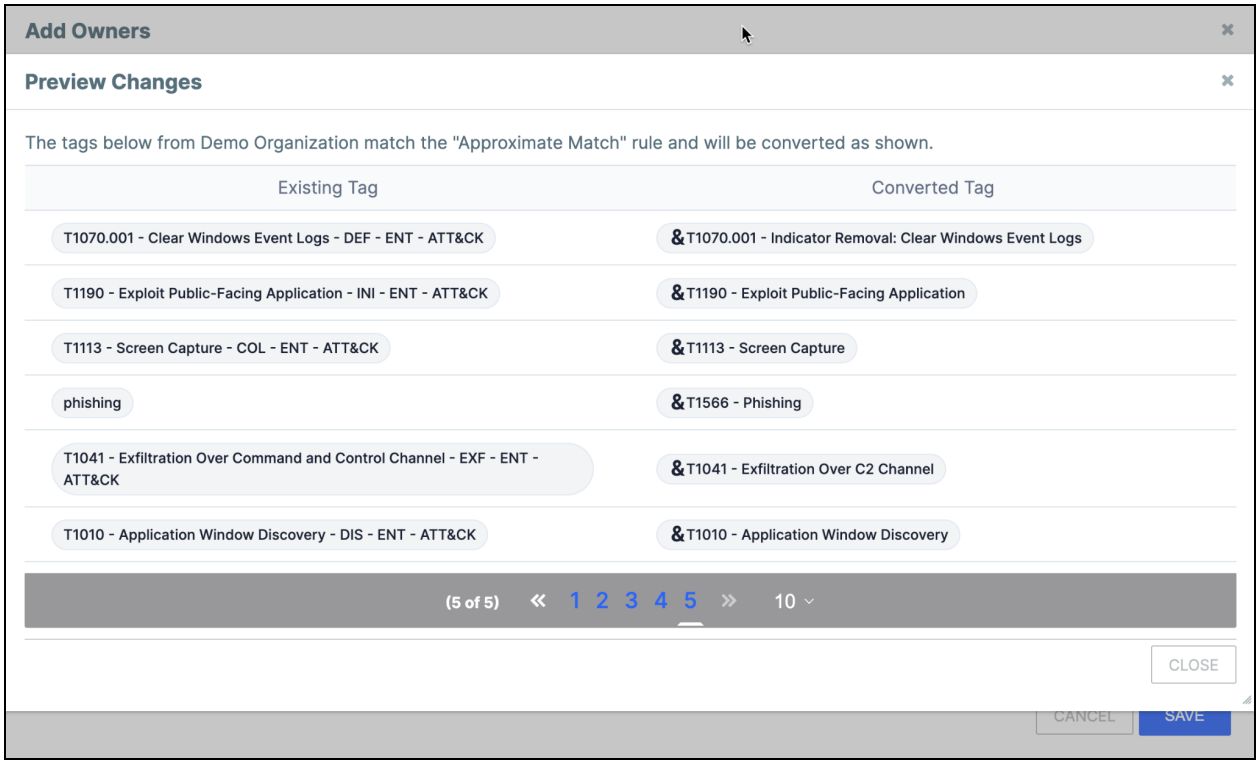
Convert Existing Tags to ATT&CK Tags

Prior to version 7.2, ThreatConnect users have employed their own tagging methods to represent MITRE ATT&CK data, but with the introduction of standard System Tags (see the next section, "Tag Normalization and Management," for more on this!), including ATT&CK Tags, you can now easily standardize the tagging process for ATT&CK. By converting the Tags you already have on your instance to ATT&CK Tags, you will benefit from enhanced visualization in the ATT&CK Visualizer and improved correlation of related Groups.

To facilitate a smooth transition between your existing Tags and the system-provided ATT&CK Tags, the **ATT&CK Tag Conversion** option has been added on the new **System Settings → Tags** tab. On this screen, System Administrators can convert the existing technique and sub-technique Tags on their instance to the new system-provided ATT&CK Tags via two options: **Exact Match** and **Approximate Match**.

- The **Exact Match** option converts existing Tags that have the same name as an ATT&CK technique (e.g, **Process Injection**) or the same combination of technique ID and name (e.g., **T1055 - Process Injection**) to the corresponding system ATT&CK Tag (e.g., **T1055 - Process Injection**).
- The **Approximate Match** option converts Tags starting with the letter "T" followed by a set of digits that map to a technique or sub-technique ID (e.g., T1055, T1055.001) to the corresponding system ATT&CK Tags. For example, Tags called **T1055**, **T1055 Process**, and **T1055 - Process Injection - DEF - ENT - ATT&CK** will all be converted to the system ATT&CK Tag **T1055 - Process Injection**. The **Approximate Match** option also includes the same conversion criteria as the **Exact Match** option—that is, when you enable the **Approximate Match** option for an owner, all of the exact matches are converted as well as the approximate matches.

You can choose which type of Tag conversion you want to implement for each owner individually, providing you with granular control over the process. For both conversion types, a preview option is available to review existing Tags before converting them, ensuring accuracy and a seamless conversion process. Note that both conversion options cannot be undone once they have been enabled in an owner.



Preview before converting existing Tags to system ATT&CK Tags

The conversion options take care of transitioning existing Tags to system ATT&CK Tags, and ThreatConnect automatically does the rest for new Tags. Whenever you create a Tag that meets the conditions of an **Exact Match** or **Approximate Match** rule you have implemented in an owner, that Tag will automatically convert to a system ATT&CK Tag. Even if you have not implemented any conversion rules in an owner, all new Tags that meet the conditions of the **Exact Match** rule will be converted to ATT&CK Tags.

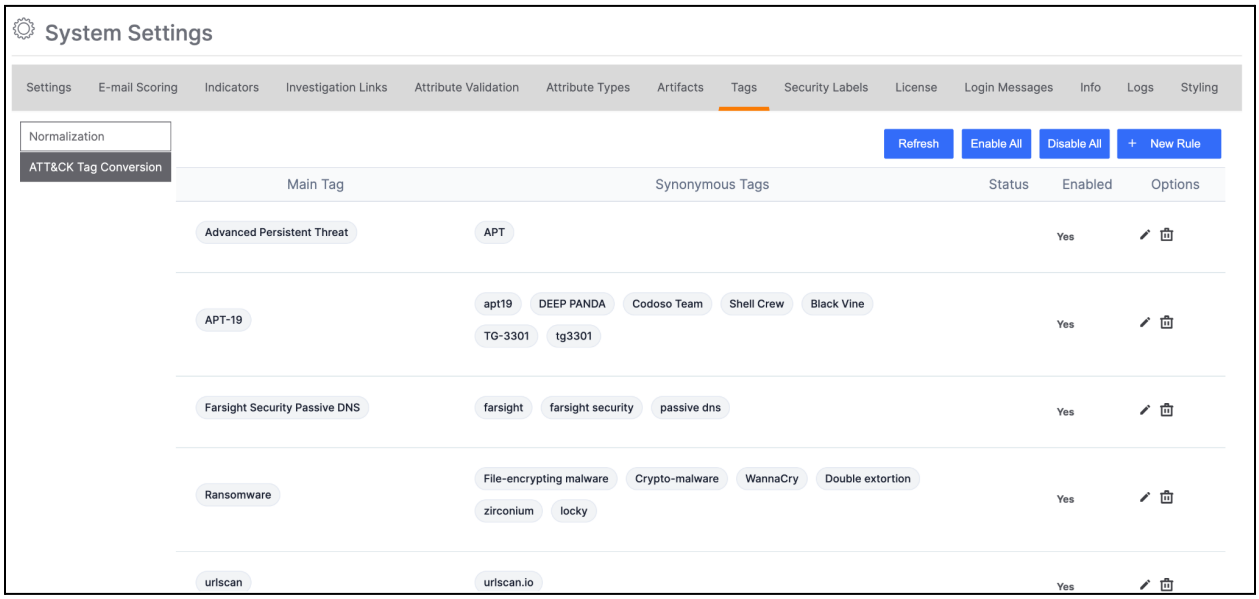
Tag Normalization and Management

Tags play a crucial role in ThreatConnect, allowing us to categorize and organize our data effectively. However, without a standardized approach to defining Tags, our data can quickly become disorganized and difficult to manage. In addition, as we add more data into ThreatConnect, we often find that we have created multiple Tags that essentially convey the same meaning, leading to confusion among users.

We developed our new Tag normalization feature to address these challenges. This feature aims to provide you with a standardized method for defining Tags while simplifying the management and consolidation of existing Tags within your system. Our ultimate goal is to

eliminate the need for time-consuming manual efforts and complex Playbooks to sift through Tags and make it easier to maintain and accurately categorize objects.

With the Tag normalization feature, found on the **Normalization** option on the new **System Settings → Tags** tab, System Administrators can set bespoke rules for Tag conversion. These rules unify synonymous Tags, which are different expressions of the same idea, into one main Tag. This operation streamlines Tag utilization across the system, mitigates any confusion, and guarantees precise data categorization.



*Configure Tag normalization rules in **System Settings***

Once a Tag rule is saved in the system, the Tag normalization feature will automatically pick it up, queue the conversion process, and convert all existing synonymous Tags to the designated main Tag. This conversion is systemwide, and it cannot be undone, so please review your Tag rules carefully to ensure accuracy before implementing them.

Tag normalization also includes the following notable functionalities:

- **Automatic Correction of Synonymous Tags**: After a normalization rule has been set for existing Tags, if users apply any synonymous Tags to Indicators, Groups, Victims, or Cases, those Tags will be converted to their corresponding main Tags. This real-time conversion ensures data consistency, saves time, and aligns new Tags with your predefined rules. Say goodbye to manual Tag adjustments, and enjoy a streamlined tagging process.
- **Automatic Error Detection and improved Rule Definition**: ThreatConnect 7.2 will help you maintain a clean and efficient tagging process by identifying errors during

Tag-rule creation and notifying System Administrators of any potential inconsistencies. For example, it won't allow you to define an existing main Tag as a synonymous Tag in a different rule, and it prevents duplication of synonymous Tags across rules. These enhancements encourage clear and distinct rule definitions, reduce confusion, and bolster overall data consistency.

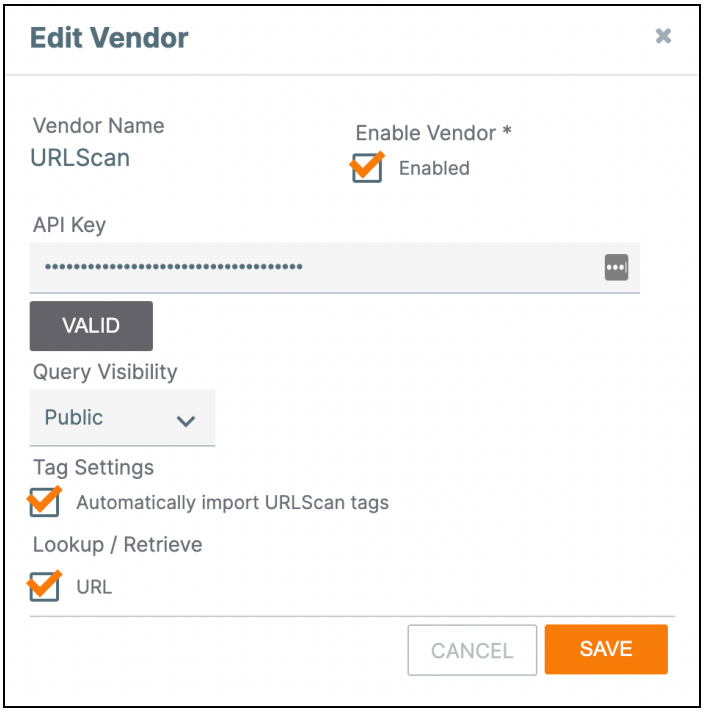
- **Visual Representation of Main Tags**: As part of our commitment to improving our user interface, we have introduced a visual representation of main Tags—that is, the icon—in various areas across ThreatConnect, including the **Details** screen and drawer, the **Browse** screen, and in Workflow Cases. This visual representation allows you to quickly identify and recognize your Organization's predefined tagging rules, improving efficiency and facilitating accurate data analysis.

The Tag icon with a star in it makes it easy to identify main Tags

Built-In Enrichment: urlscan.io

We are excited to introduce another powerful built-in enrichment feature in our 7.2 release, this time powered by urlscan.io. This seamless integration allows you to use the extensive URL scanning capabilities of urlscan.io directly within ThreatConnect, providing you with a more complete perspective on potential security threats and further boosting the depth and efficacy of your threat intelligence investigations.

System Administrators can enable this built-in enrichment by adding their urlscan.io API key to the **Enrichment Tools** section of the **Indicators** tab of **System Settings** and then selecting the **URL Address** Indicator type.

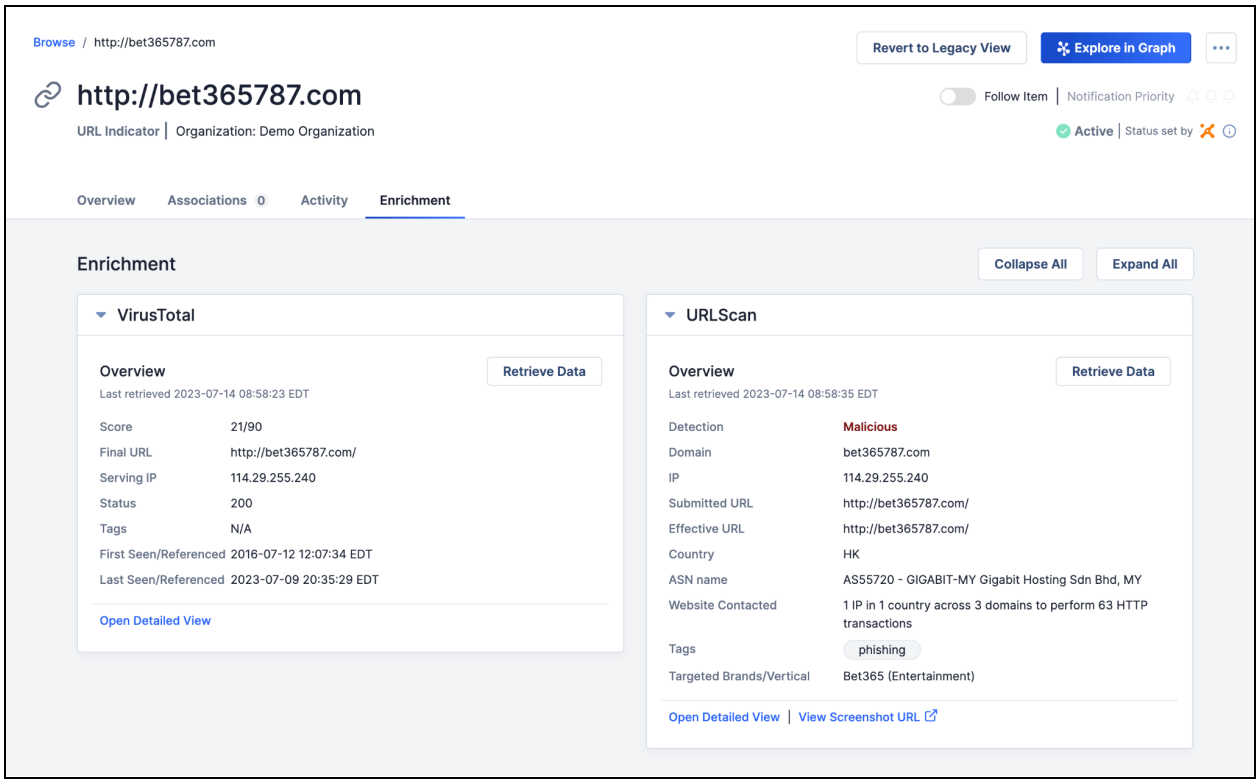


*Configure urlscan.io enrichment in **System Settings***

System Administrators will choose one of three scan visibility levels: public, private, or unlisted. This configuration setting determines how URLs are submitted to urlscan.io for scanning. System Administrators can align this visibility level to their specific requirements and privacy considerations.

We have also provided an option to automatically import urlscan.io tags as Tags applied to enriched URL Indicators. When this option is enabled, the tags provided by urlscan.io will be automatically added as Tags to the URL Indicator on which the urlscan.io enrichment was run.

Once the configuration for this enrichment has been completed, you can view enrichment details for URL Indicators on the **Enrichment** tab of the Indicators' **Details** screen.

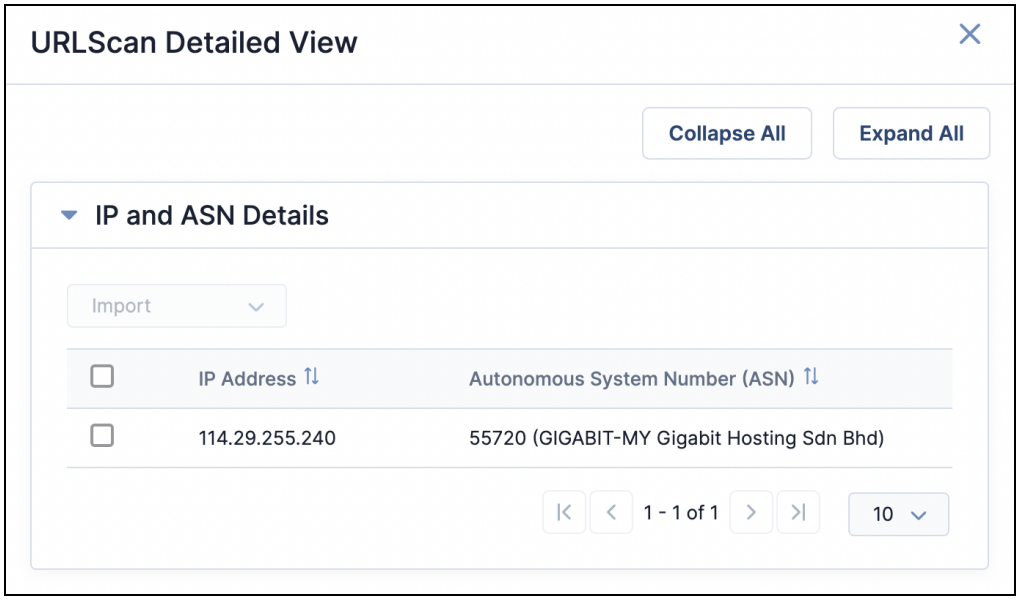


*urlscan.io data are provided on the **Enrichment** tab of an URL Indicator's **Details** screen*

When you navigate to a URL Indicator's **Enrichment** tab for the first time, information from urlscan.io is pulled and cached. Every time you revisit the **Enrichment** tab for a URL Indicator, cached data will be present. A new urlscan.io lookup is not made until the caching timer expires. To get the latest enrichment data from urlscan.io before the caching time limit expires, you can always click the **Retrieve Data** button on the **URLScan** card on the **Enrichment** tab.

To delve further into the information urlscan.io has about a URL, simply click the **Open Detailed View** link at the lower left of the **URLScan** card. This will open the **URLScan Detailed View** drawer, where you can access comprehensive details about URL addresses for research purposes.

In ThreatConnect 7.2, the **URLScan Detailed View** drawer provides the IP address and corresponding Autonomous System Number (ASN) associated with the URL Indicator. By establishing the connection between a URL, its IP address, and the associated ASN, analysts can gain a deeper understanding of the network infrastructure supporting the URL. This contextual information assists in assessing the reputation, trustworthiness, and potential security implications of both the URL itself and the hosting network to which it belongs.



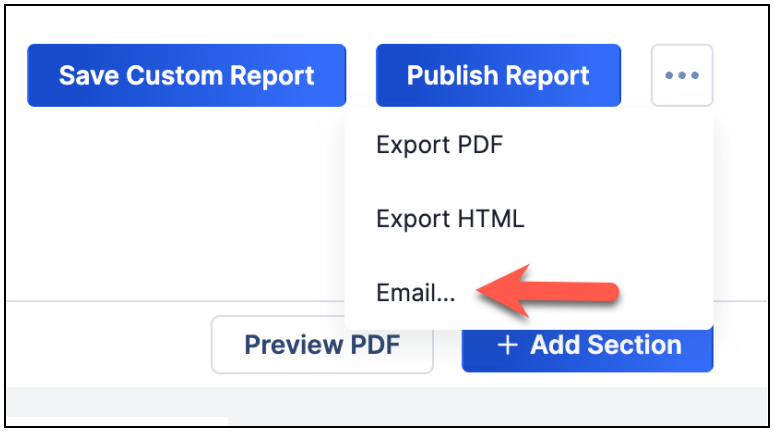
*The **URLScan Detailed View** drawer provides detailed enrichment information for URL Indicators*

urlscan.io also offers another impressive functionality: the ability to retrieve a screenshot linked to a specific URL. To open the screenshot for a URL Indicator in a new browser tab, simply click on the **View Screenshot URL** link at the lower left of the **URLScan** card..

We have also made the urlscan.io enrichment data points available in the ThreatConnect UI accessible via the v3 API. Simply append `?type=URLScan` to the `/api/v3/indicators/{indicatorId or indicatorSummary}/enrich` or `/api/v3/indicators/enrich` URIs when sending a POST request to either of these endpoints. This feature eliminates the need to navigate to the **Enrichment** tab in the UI, making the enrichment process more efficient and streamlined.

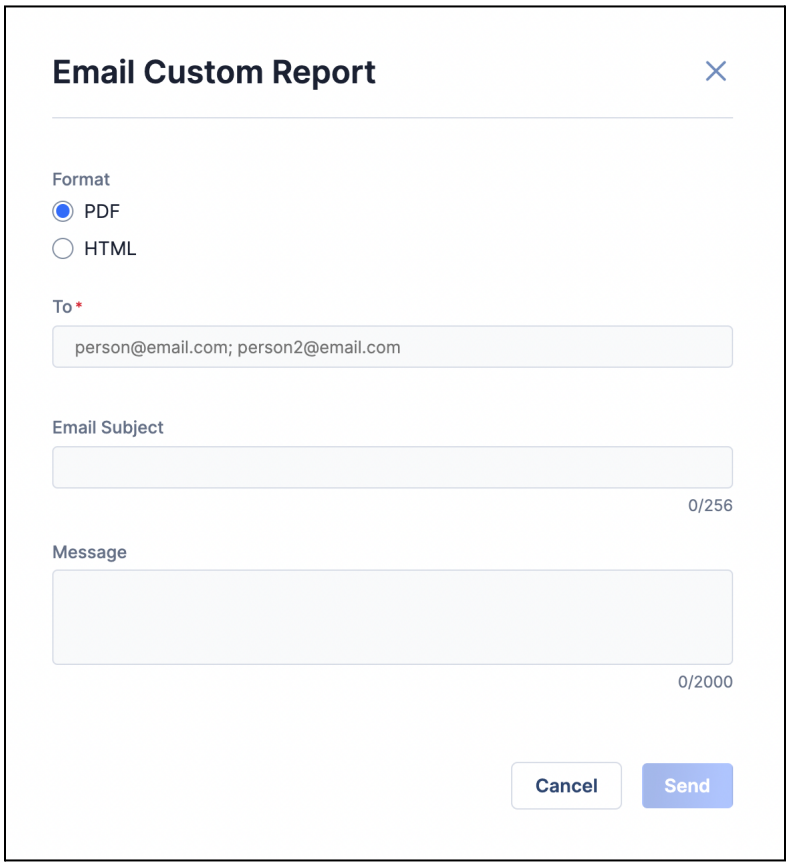
Report Dissemination

In version 7.2 of ThreatConnect, we continue to iterate on our in-platform reporting capabilities by adding an option for disseminating reports by email.



*Use the new **Email** option to quickly and easily disseminate reports by email*

You can leverage this new functionality to send an email with a report in PDF or HTML format directly from the ThreatConnect platform to a set of identified email addresses.

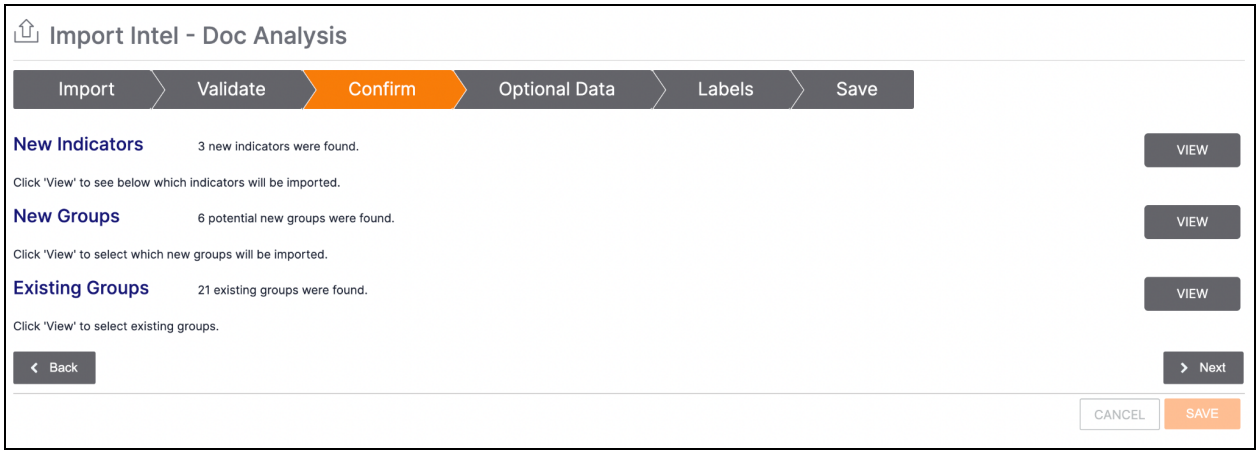


You can email reports in PDF or HTML format directly from ThreatConnect

This feature is intended to help reduce the amount of time you spend sending reports by bringing that functionality directly into the platform.

New Import Option: Doc Analysis

We often get feedback asking us to expand the methods available for getting information into ThreatConnect. In response to this feedback, we have added a new import option called **Doc Analysis** in 7.2. This capability leverages the same powerful API that powers the CAL Automated Threat Library (ATL) to parse text for Indicators and—for the first time—Groups that CAL knows about or are available in the your ThreatConnect instance. This feature allows you to import Groups into ThreatConnectin a way that previously was not available.



You can import Indicators and Groups with the new Doc Analysis capability

This feature, available under **Import** on the top navigation bar, works across owners to identify where you may have existing Groups that match the names of the Groups you are looking to import. This helps you better understand what already exists in your instance and what does not so that you can know where you are putting your information. It also helps you decide whether to add the new information to an existing Group or create a new Group in a different owner to keep track of the new information. We know that different customers map data differently, and we wanted this feature to be as accessible as possible to the widest number of our users.

It is important to note that while this feature does leverage an API written and maintained by CAL and the CAL dataset, it does *not* require you to have CAL turned on. If you have CAL turned off, you can still use this feature and rest assured that your information has not been captured. In such cases, you are leveraging CAL as a read-only resource.

Improvements

Threat Intelligence

- The following TQL parameters were added for Tags and are available in the v3 API as well:
    - **`techniqueId`** (String): The standard ID for specific MITRE ATT&CK techniques and sub-techniques (e.g., **`T1234`**, **`T1234.001`**). The value of this parameter is **null** for all non-ATT&CK Tags.
    - **`active`** (Boolean): Read-only field that can be **`false`** for certain ATT&CK Tags that become deprecated over time and will be excluded from places such as the ATT&CK Visualizer. The value of this parameter is **`true`** in all other cases.
    - **`normalized`** (Boolean): Read-only field that indicates if a Tag is defined as a main Tag within a Tag normalization rule.
- The new **Details** screen is now available for Document and Report Groups, with a new card (**Document File** for Documents and **Report File** for Reports) on the **Overview** tab. For Excel®, PDF, PowerPoint®, Word®, and HTML files, this card provides a thumbnail preview of the object's file and a link you can click to view the file in another browser tab. (These options are not available for Document files that are in the Malware Vault.) The card also displays information about the file, such as file name and type, and provides options for replacing and downloading the file.
- If CAL is disabled on your instance, the following sections of the **Details** screen will not be displayed:
    - The **CAL™ Classifiers** section of the **Details** card (new **Details** screen)
    - The **CAL™ Feeds** section of the **Owners & Feeds** card (new **Details** screen)
    - The **CAL™ Provider Information** section of the **Geolocation** card (new **Details** screen)
    - The **CAL™ Insights** section of the **Indicator Analytics** card (legacy **Details** screen)
- You can now reply to posts on the **Notes** card of the new **Details** screen.
- The **Last Modified** date for an Indicator will now be updated when the Indicator is associated to or dissociated from a Group, another Indicator, a Case, or an Artifact.

Enrichment

- You can now view and import passive DNS data from Farsight Security® for Address and Host Indicators on the **Enrichment** tab of the Indicator's **Details** screen. For Address Indicators, you can import Host Indicators identified by the enrichment, and for Host Indicators, you can import Address and Host Indicators identified by the enrichment. This enrichment option must be enabled by a System Administrator in **System Settings > Indicators > Enrichment Tools**. Note that unlike in other enrichment services in ThreatConnect, data are not retrieved from Farsight Security automatically when you click on an Address or Host Indicator's **Enrichment** tab for the first time; instead, you must click the **Retrieve Data** button to retrieve data for the first time. This improvement enables you to use the new **Details** screen to access the passive DNS functionality that was previously available only on the legacy **Details** screen.

Reporting

- You can now add the following new **Case Data** sections to a report: **Potential Group Associations**, **Potential Indicator Associations**, **Potential Case Associations**, **Timeline**, and **Notes**.

Playbooks

- You can now create a Run Profile for a logged Playbook execution from the **Execution Details** pane while viewing the results of an execution.

App Builder

- The App Builder feature now supports Python® 3.11 and TcEx 4.0.
    - By default, all new App projects use these versions.
    - Only Apps using TcEx 4.0.*x* can use Python 3.11. Apps using a TcEx version older than 4.0.*x* must use Python 3.6.
    - Only Apps using TcEx 4.0.*x* can use snippets.
    - Because the **Insert Code** functionality on the **Inputs** and **Outputs** tab of the **App Builder** screen employs snippets to place parameters into the Code Editor, this functionality is not available when working with Apps that use a

TcEx version older than 4.0.*x*. In this scenario, you now must manually write the code that references the parameter in the Code Editor in order to use the parameter in the App.

System Settings

- We have changed the way that version and commit info are presented on the **System Settings > Info > Information screen** to give System Administrators better insight into which build of ThreatConnect is running on their instance. The version number is still at the upper left of the screen. The commit has been shortened to 8 characters and can now be found at the lower left of the screen. Under the commit is the build, which is in the format **M*####X*,** where the "M" stands for "Maintenance Build," the hashtags represent the four-digit release date (i.e., the first set of two ***##*** characters are the two-digit month, and the second set of two ***##*** characters are the two-digit day), and the ***X*** is a modifier denoting one of three possibilities: **S** (deployed to a single customer only), **P** (a top-priority fix to address a customer outage), or **R** (required for all customers).
- The **tqlAssociationMonitorInterval** system setting now has a default value of 5 and is no longer available via the ThreatConnect **System Settings** UI.
- The description of the **tqlAssociationExecutionTime** system setting has been updated.
- The following new system settings were added:
    - **emailSesEnabled**: This setting determines whether to send emails with Amazon Simple Email Service (SES)™.
    - **emailSesAccessID**: This setting determines the Amazon Web Services® (AWS) access key ID to use for Amazon SES.
    - **emailSesSecretKey**: This setting determines the AWS secret access key to use for Amazon SES.
    - **emailSesRegion**: This setting determines the AWS Region to use for Amazon SES.

Organization Settings

- When changing a keychain variable to a text variable on the **Variables** tab of the **Organization Settings** screen, the **Value** field will immediately be reset instead of

displaying the value of the keychain variable once you select **TEXT** in the **Type** dropdown of the **Property** window.

TC Exchange

- The Notifications Center will now inform you about updates that are available for TC Exchange™ Apps.

API & Under the Hood

- A new System role, Exchange Admin, was added. A user with this role can implement the following v3 API endpoints to deploy locally written Apps directly to ThreatConnect and to run Apps locally for testing: **`/api/v3/apps/exchange/install`**, **`/api/v3/token/api`**, and **`/api/v3/token/svc`**. These endpoints may be used only by API users with the Exchange Admin System role.
- You can now use the v2 API and the management API to export Playbooks as Content Packs, enabling you to include all supporting Apps and other relevant data that the Playbooks rely on rather than just a JSON file. Note that this feature does not exist in the ThreatConnect UI at this time. To export a Playbook as a Content Pack, append **`?format=tcxp`** to the respective URIs for Playbook export:
    - v2 API: **`/api/v2/playbooks/<ID>/export?format=tcxp`**
    - Management API: **`/api/v1/management/playbooks/<groupXID>/download?format=tcxp`**

Bug Fixes

Threat Intelligence

- An issue causing an error to occur when returning to the new **Details** screen after using the legacy **Details** screen to add a File behavior association has been resolved.
- Only users with an owner role that has the **Full** permission level for Attribute Types (Organization Administrator for an Organization; Editor and Director for a Community or Source) will be able to use the batch Indicator import functionality. Previously, users with the **Create** permission level were able to use batch Indicator import, which was resulting in incomplete imports and errors. The change in permission requirements solves this problem.
- An issue causing an extraneous error message to be displayed when using the **Publish after Copy** option when contributing a Group to a Community or Source was fixed.
- An issue causing the number of observations for an Indicator to be incorrectly displayed as "1970-01-01" in the **Details** drawer was fixed.
- An issue causing the **Additional Owners** section of the **Owners & Feeds** card on the new **Details** screen to omit owners for File Indicators for which one hash is an exact match, but other fields are not because they are null in one of the owners, was resolved.
- The **TQL Queries** card on the **Associations** tab of the **Details** screen now has a **Status** column that displays whether each query is enabled or disabled.
- An issue causing the object counts on the **Artifacts** and **Cases** cards on the **Associations** tab of the **Details** screen to be incorrect was fixed.
- On the **Activity** tab of the new **Details** screen, usernames are now links to the user's profile.

Playbooks

- An issue causing the **Update Global Variable** Playbook App to throw an error when called within a Playbook Component has been resolved.
- An issue preventing Super Users from importing Playbooks into Organizations other than their home Organization has been resolved.

- When exporting a Playbook, any variable from an upstream App that is used as an input to a downstream App is exported so that when you import the Playbook on a different instance, those variables are in place and functional. Previously, if the input field in which the upstream variable was used took encrypted input (e.g., an API token), the Playbook would not be functional when imported into a different instance.
- When exporting a Playbook, a spinner will be displayed to let you know that the system is processing the export.
- An issue causing incorrect sort orders in the columns of the table on the **Playbooks** screen was fixed.

App Builder

- When deleting an input variable in the App Builder, you will now be presented with a window asking you to confirm the deletion.

Attributes

- An issue causing the value of Attribute timestamps to be displayed as **Invalid Value** when viewed in Firefox® was fixed.

Threat Graph

- An issue causing no UserAction Playbooks to be displayed in the **Select Playbook** window when using the **Run Playbook...** option for an Indicator in Threat Graph, even when there are active UserAction Playbooks for that Indicator type in the user's Organization, was fixed.

API & Under the Hood

- An issue causing duplicate key values to be created, resulting in a unique constraint error, when using the batch API to update custom Indicators has been resolved.
- An issue causing instance instability when parsing files that have very large numbers of Indicators has been resolved.
- A certain custom Organization role configuration was not providing expected permissions for editing Notes and adding Artifacts in Workflow Cases. This issue has been resolved.

Dependencies & Library Changes

- A library update was made to address an issue causing instances using JDK 11.18+ to trigger an infinite loop with web connections over SSL.

Maintenance Releases Changelog

2023-09-26 7.2.1-M0926R [Latest]

Bug Fixes

- An issue causing errors to occur in dashboard query cards including Tags applied to Workflow Cases via the v3 API was fixed.

2023-09-21 7.2.1-M0921R

Bug Fixes

- An issue causing the TQL Association Monitor to send multiple null pointer exceptions to error logs of Dedicated Cloud instances was fixed.

2023-09-11 7.2.1-M0911R

Bug Fixes

- An issue causing TQL queries using **hasIndicator()** containing references to certain Indicator values to return an error has been resolved.
- An issue causing Tags to be removed from objects after applying a Tag normalization rule that alters only the case of the Tag's text was fixed.

2023-08-31 7.2.0-M0831R

Bug Fixes

- An issue causing PUT requests for Group-to-Indicator associations in the v3 API to fail was fixed.

2023-08-24 7.2.1

Bug Fixes

- When adding an Attribute to an object, an issue was causing Attribute Types that exist in other owners on the ThreatConnect instance, but not in the object's owner, to be available for selection. Attempting to add an Attribute of one of these Attribute Types would cause an error. With this version of ThreatConnect, only Attribute Types that exist in the object's owner are provided for selection.
- MITRE ATT&CK sub-technique T1036.002 was missing from the ATT&CK Visualizer. It has now been added.
- When exporting Indicators or Groups from the **Browse** screen, the **Export Data** window was allowing only selection of no data types or all data types. This issue has been fixed.
- An issue causing delays and timeouts to occur when adding a new Indicator, Group, or Victim Asset association on the **Associations** tab of the new **Details** screen has been resolved.
- An issue causing Workflow Cases containing the same Artifact not to be included as potential Case associations for each other was resolved.
- An issue preventing the **Details** drawer from being displayed when clicking on certain results from the **Search** drawer (accessed via the magnifying-glass icon on the top navigation bar) was fixed.
- An issue limiting the number of available Attribute Types for an object to 100 on the new **Details** screen has been fixed.
- If your ThreatConnect password is changed (e.g., you change your password; your Organization Administrator changes your password), your password expiration date will now be reset.
- An issue causing the number of owners selected in the **My Intel Sources** selector to be displayed as 1 when no owners are selected was fixed.
- Potential associations no longer include Indicators and Groups associated to objects that are associated or potentially associated to a Case or Group. This change resolves performance issues stemming from large data sets.
- An issue causing hyperlinks in the **Description** section of the **Case Details** card for a Workflow Case not to be clickable when the hyperlink text exactly matches the URL has been fixed.
- An issue causing the wrong error code to be returned when using the v2 API to submit a POST request containing a file hash with a space in it was fixed.

- Your ability to modify Indicator Status now depends on the permissions you have in the Indicator's owner (which are determined by your user role in that owner) and whether your Organization has enabled the ability to change Indicator Status.

2023-08-10 7.2.0-M0810R

Bug Fixes

- An issue causing an error to occur when viewing the details for an associated Indicator on the **Associations** card of a Workflow Case was fixed.
- A concurrency issue that could affect system stability during ATT&CK Tag import or Tag normalization operations was fixed.

2023-08-03 7.2.0-M0803R

Bug Fixes

- An issue preventing the **Details** drawer from being displayed when clicking on certain results from the **Search** drawer (accessed via the magnifying-glass icon on the top navigation bar) was fixed.
- An issue preventing Organization-level metric data from receiving daily updates on ThreatConnect instances running MySQL® has been resolved.
- An issue limiting the number of available Attribute Types for an object to 100 on the new **Details** screen has been fixed.

2023-08-03 7.2.0-M0803S

Bug Fixes

- Performance improvements were made on the **Potential Associations** card on the **Associations** tab of the new **Details** screen.