ThreatConnect® Release Notes

Software Version 7.3

October 4, 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

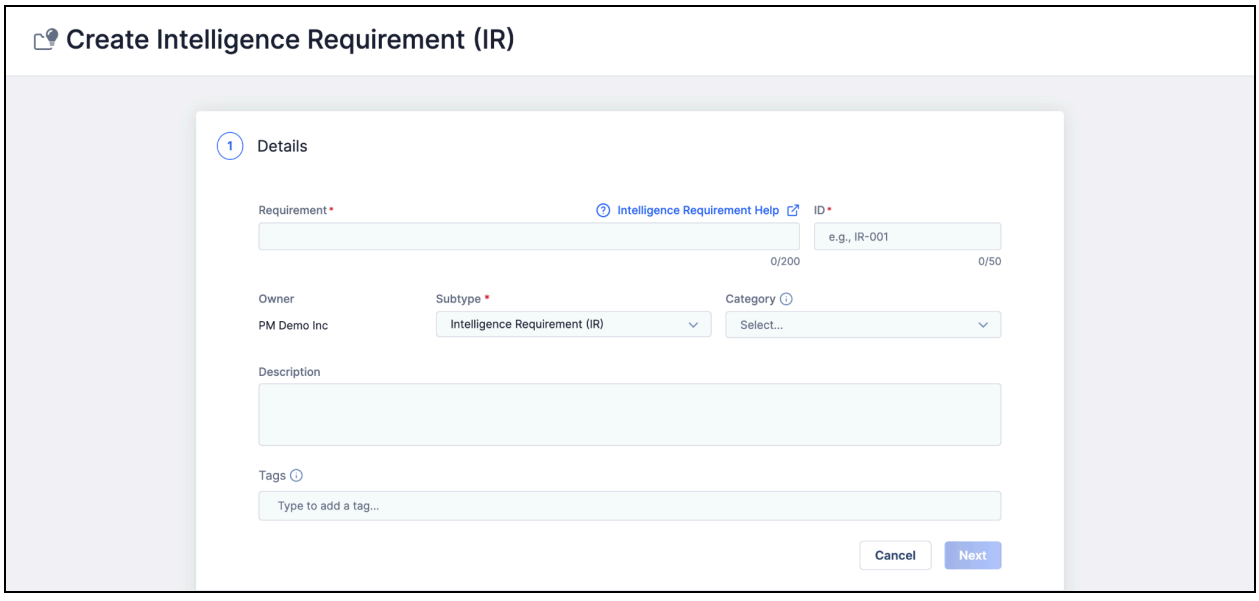
New Features and Functionality

Intelligence Requirements

In ThreatConnect 7.3, we are pleased to announce the release of a first-of-its-kind Intelligence Requirement (IR) capability designed to increase analyst efficiency and effectiveness. This capability provides a central location where analysts can capture their team's requirements, as well as a powerful new querying functionality that automatically identifies and tracks information likely related to requirements, requests for information (RFIs), and general research efforts.

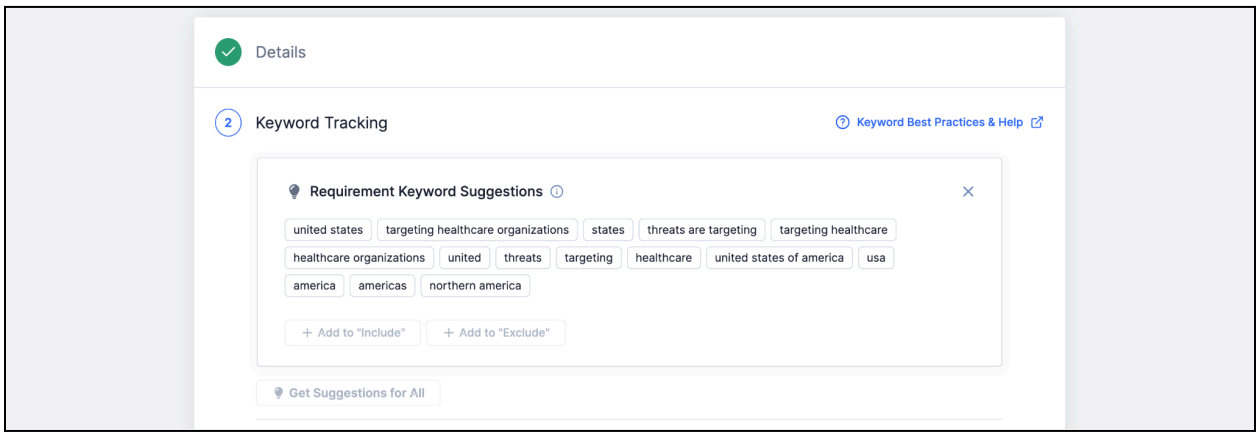
With the ThreatConnect Intelligence Requirement feature, you can add your requirements to ThreatConnect in a newly designed UI. This creator contains three steps in which you provide data about an IR, define a keyword query, and preview the information in your ThreatConnect instance that might match the IR.

In step 1 (**Details**) of the **Create Intelligence Requirement (IR)** screen, you provide the text of the IR, a unique identification number for the IR, and other basic information, including a Description Attribute and Tags.



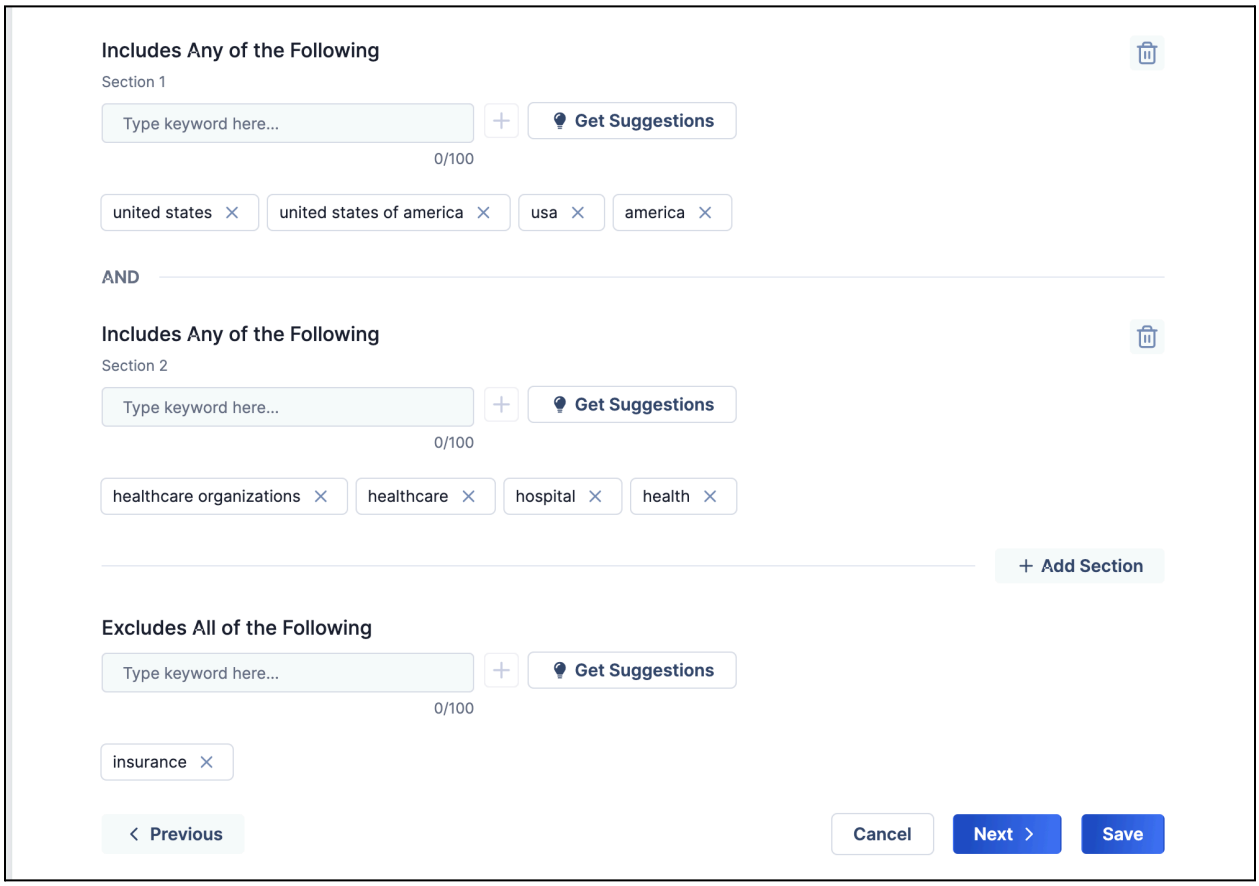
*Capture basic Intelligence Requirement data in step 1 of the new **Create Intelligence Requirement (IR)** UI*

After you enter all required information in the **Details** step, you are directed to step 2 (**Keyword Tracking**). In the first part of this step, you are presented with a set of keyword suggestions based on the text you entered in the **Requirement** field in the **Details** step. In this version of the Intelligence Requirement feature, you can expect suggestions for potential aliases of keywords recognized in the **Requirement** field based on geolocation, MITRE ATT&CK® tactics and techniques, intrusion sets, tools, and malware families. For example, if the **Requirement** text is "What threats are targeting healthcare organizations in the United States?", the keyword suggestions will look like those in the next screenshot. Note that several variations of "United States" are included in the suggestions, such as "states," "United States of America," "USA," "America," etc. The next version of this feature will add alias keyword suggestions for industries.



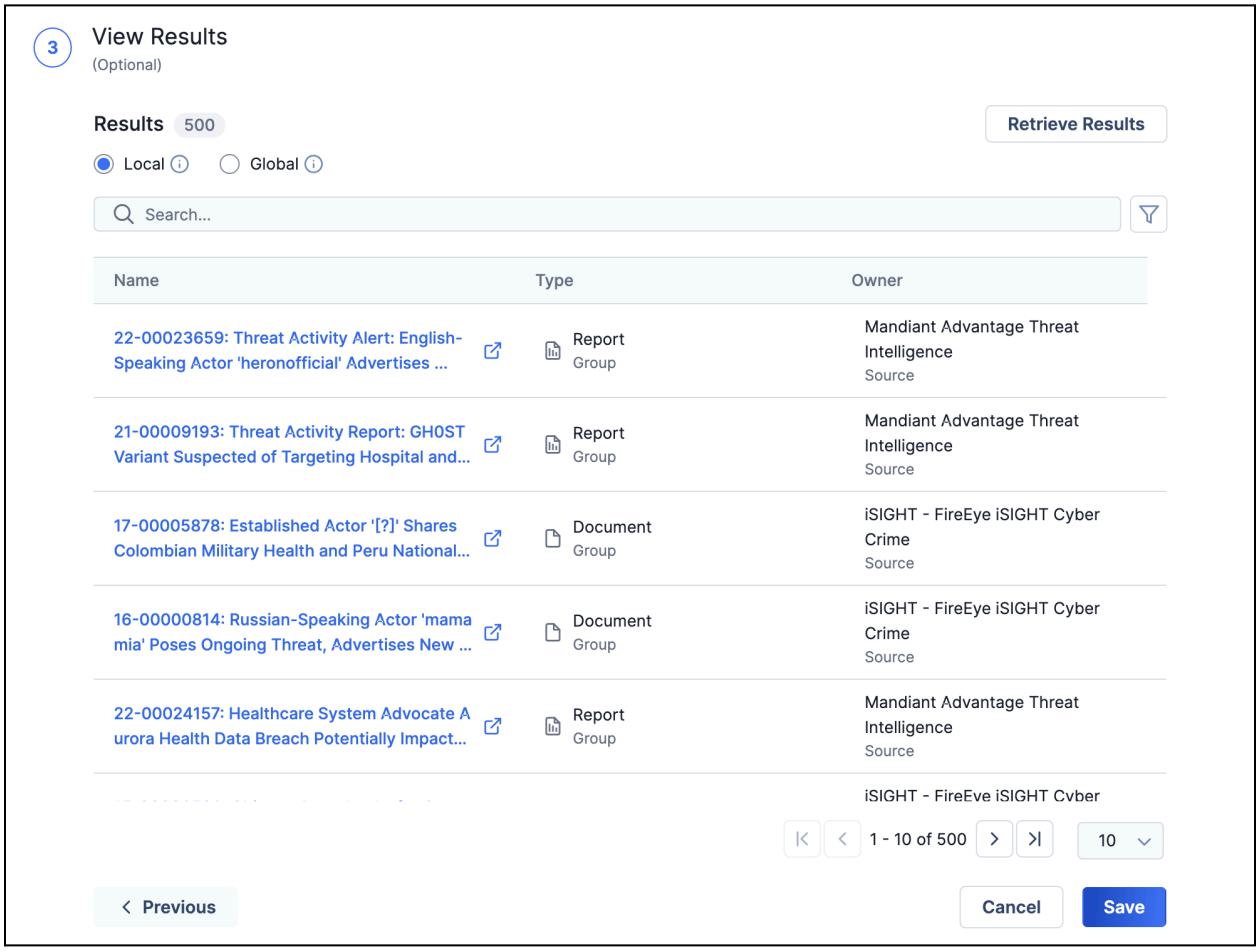
The first part of step 2 of the IR creator suggests keywords for your query

The second part of step 2 helps you build a logic-based query. You can add up to five **Includes** sections and one **Excludes** section, where each section contains a set of keywords that you can select from the suggestions or enter manually. The next screenshot shows an example of what the **Keyword Tracking** step looks like after being populated with two **Includes** sections and one **Excludes** section, where each **Includes** section has four keywords and the **Excludes** section has one keyword. On the backend, ThreatConnect converts this query to something like ["united states" OR "united states of america" OR "USA" or "america"] AND ["healthcare organizations" OR "healthcare" OR "hospital" OR "health"] AND NOT ["insurance"].



In the second part of step 2, you build a logical query from selected keywords

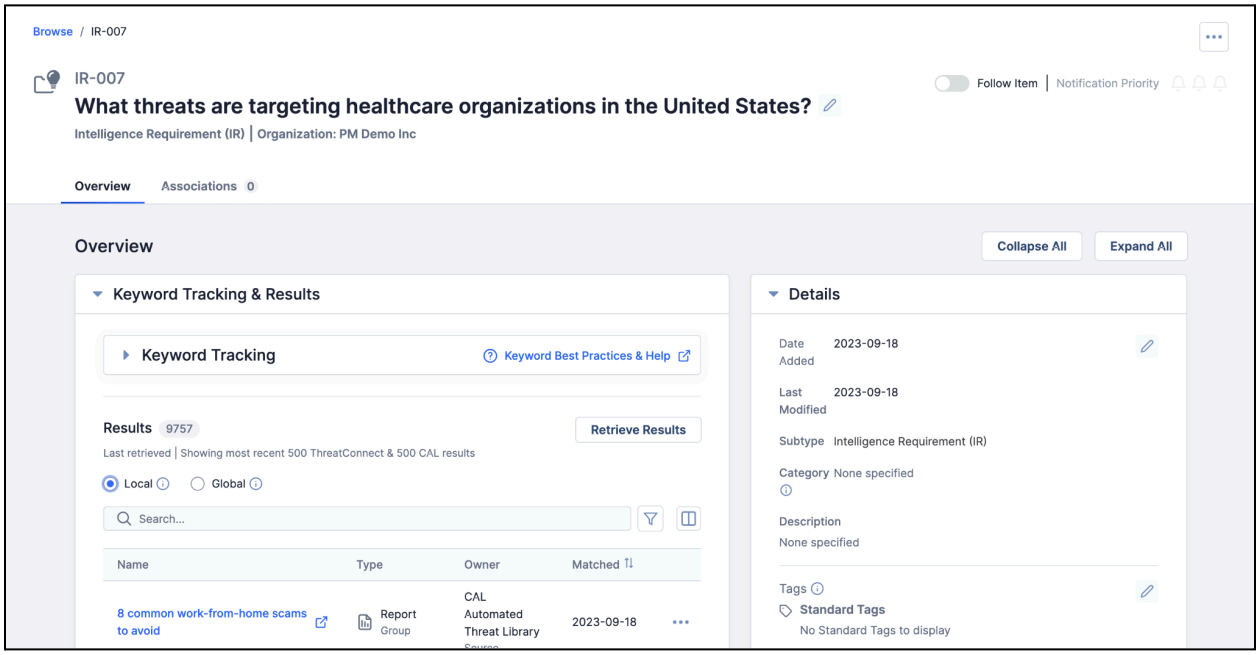
When you are satisfied with your query, you can either click **Save** to save the IR or move on to step 3 (**View Results**), where you can view preliminary results for the query. The query searches across everything you have access to in your instance, including all Attributes, Tags, and the contents of Report files.



Step 3 of the IR creator displays preliminary query results

Step 3 provides two types of results: **Local**, which are results from information available in your ThreatConnect instance, and **Global,** which are results from the ThreatConnect Global Intelligence Dataset. The ThreatConnect Global Intelligence Dataset has historically been known as CAL™, but it is called the ThreatConnect Global Intelligence Dataset for IRs because of a key difference in its functionality: If a ThreatConnect instance has opted out of CAL participation, it can still fully leverage the data in the ThreatConnect Global Intelligence Dataset. The **Global** results set is treated as read only for instances that do not participate in CAL, and no telemetry of any kind is shared with or captured by CAL.

After reviewing the results in step 3, you can click **Save,** or you can go back to the previous step and refine your keyword query to ensure you are getting the results you expect and will find most useful. After you save the IR, you will be directed to the new IR **Details** screen.



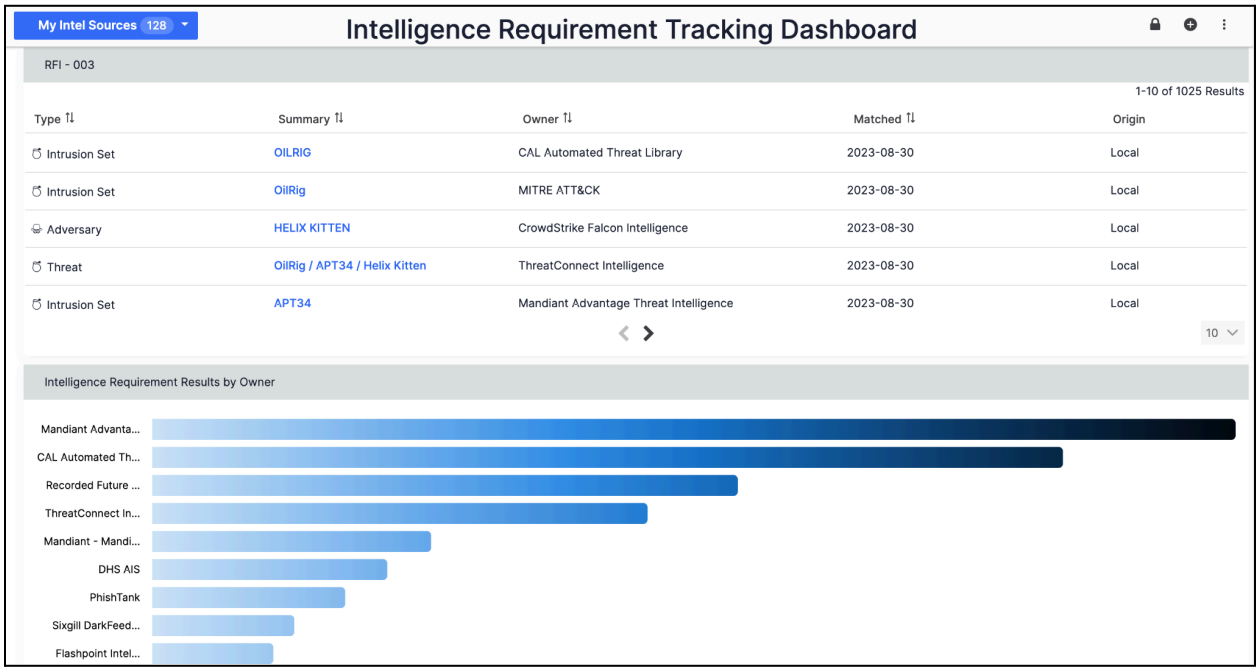
*The IR **Details** screen is a central location for all data related to an IR*

The results shown on the IR **Details** screen are updated nightly and can be updated on demand by clicking the **Retrieve Results** button. If you are assigned IRs or areas of responsibility related to IRs, you can use these screens as a sort of to-do list that shows the most recently matched information. The IR **Details** screen will reduce or eliminate the need to weed through all of the available information coming in from sources and feeds every day, enabling you to focus on reviewing the information that is most likely to be relevant to your searches.

In addition to the UI, the first iteration of the IR functionality includes v3 API support via the following endpoints:

- `/v3/intelRequirements`: This endpoint allows API users to create, retrieve, update, and delete IR objects.
- `/v3/intelRequirements/categories`: This endpoint allows API users to retrieve IR categories.
- `/v3/intelRequirements/results`: This endpoint allows API users to retrieve, update (i.e., archive results, associate results to IRs, and mark results as false results), and delete results for IR keyword queries.
- `/v3/intelRequirements/subtypes`: This endpoint allows API users to retrieve IR subtypes.

Finally, in this first iteration of the IR functionality, you can leverage ThreatConnect Query Language (TQL) to create dashboard cards showing how the sources and feeds you have deployed are answering your defined requirements. You can also create dashboard cards to aggregate results for a set of IRs if you are tracking multiple requirements at once and want to see what's new for all of those requirements in one place.



Use TQL to create dashboard cards to track IR results and evaluate how your feeds are performing against your requirements

ThreatConnect will be adding additional functionality for IRs over the next several releases. Please share any and all feedback on IRs with your Customer Success Manager or Customer Success Engineer so that we can use your experiences and suggestions to inform our updates.

ATT&CK Visualizer Version 2

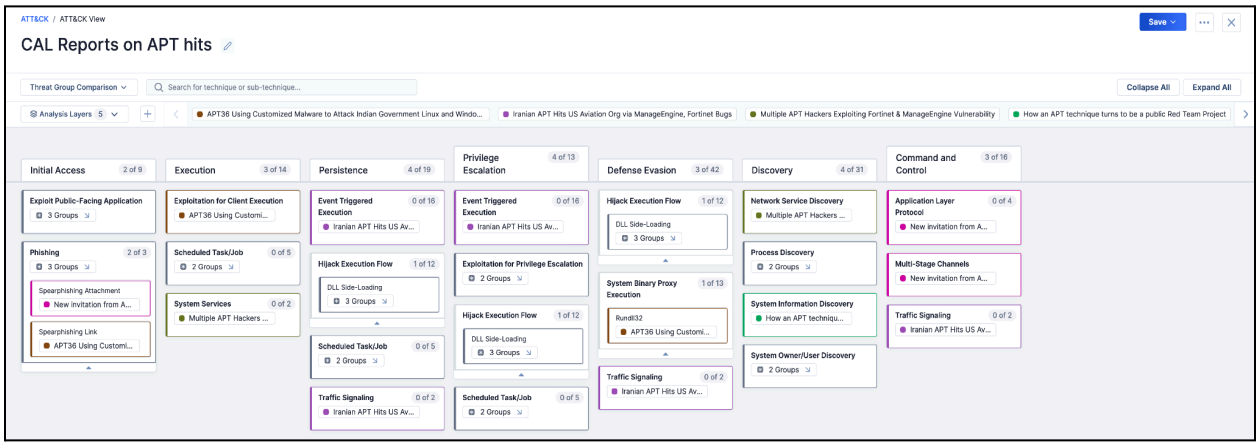
In this latest version of the ATT&CK Visualizer, we are thrilled to unveil three game-changing new functionalities: **Threat Group Comparison View**, **Technique Prevalence View**, and **Advanced Group Filtering**. In addition, we introduce the ability to save your views and export them as JavaScript® Object Notation (JSON) files, enhancing collaboration and knowledge sharing across your organization.

Threat Group Comparison View

In ThreatConnect 7.3, you can now add multiple analysis layers (Groups) to an ATT&CK view, enabling you to visualize shared techniques and sub-techniques and conduct in-depth analysis with ease and precision.

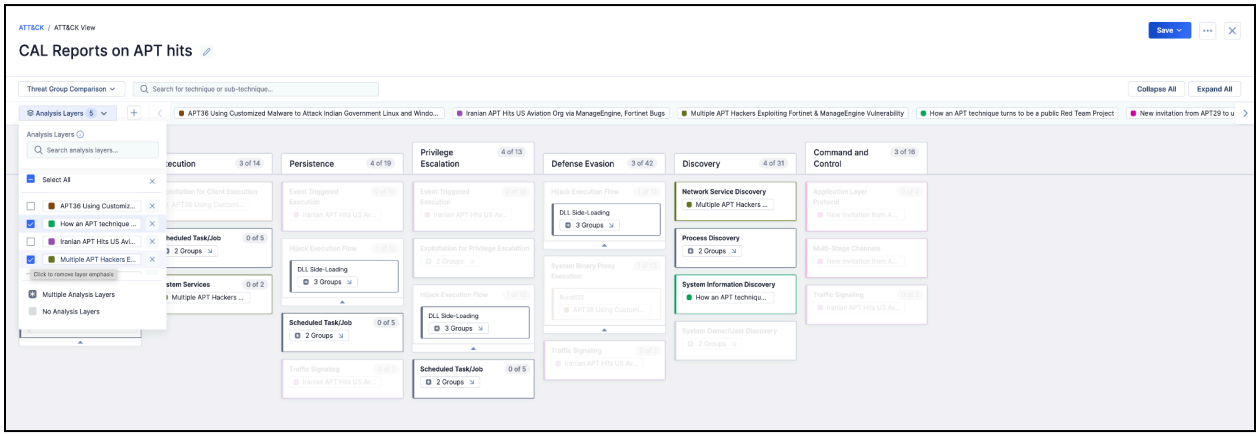
When you click **ATT&CK** on the top navigation bar, you will be directed to a new **ATT&CK** screen that displays all of the ATT&CK views you have saved. (Yes, you can save your ATT&CK views now—more on this new functionality in a bit!) From there, click the **Create ATT&CK View** button to display the ATT&CK Visualizer, where you can build a new ATT&CK view by clicking the **+** button to the right of the **Analysis Layers** dropdown to search for and add threat groups of interest, instantly revealing shared techniques and sub-techniques among the selected Group objects.

We refer to this view as the **Threat Group Comparison** view. Every technique or sub-technique will display the Group that uses it, and each Group and the technique and/or sub-technique box containing it will be displayed in a color assigned to the Group. Techniques and sub-techniques used by multiple Groups are displayed in gray boxes. (We recommend that you check out this view in light and dark mode to see which you like better!) In addition, when a technique or sub-technique is used by multiple Groups, the number of Groups is displayed. You can click on the box containing the number of Groups to view the Groups' names. This new ability to identify shared techniques and sub-techniques among threat groups will empower you to make more informed decisions regarding your security strategies, ensuring effective defense prioritization and keeping you ahead of evolving threats.



*Add multiple Groups to find common techniques in **Threat Group Comparison** view*

For an even more precise and targeted threat analysis, you can now deselect specific Groups from the **Analysis Layers** dropdown. This capability highlights the techniques exclusively used by the remaining Groups, streamlining your focus on their activities. Simultaneously, techniques employed by the deselected Groups are grayed out, ensuring effortless comparisons without removing the deselected Groups from the view.



Deselecting Groups highlights techniques used by the remaining Groups

Technique Prevalence View

In ThreatConnect 7.3, we launch a powerful new feature that enables you to create dynamic heat maps displaying the prevalence of each ATT&CK technique used by various Groups. This functionality is achieved through meticulous calculations based on the percentage of Groups employing these techniques.

In an ATT&CK view, you'll find the option to toggle the **Threat Group Comparison** dropdown to **Technique Prevalence**. **Technique Prevalence** view displays the prevalence of the techniques for all selected Groups with respect to the entire pool of Groups in the view. Identification of prevalent techniques is essential for effective threat management and making informed strategic decisions. Prioritizing highly prevalent techniques empowers your organization to strengthen its defenses where it matters most.

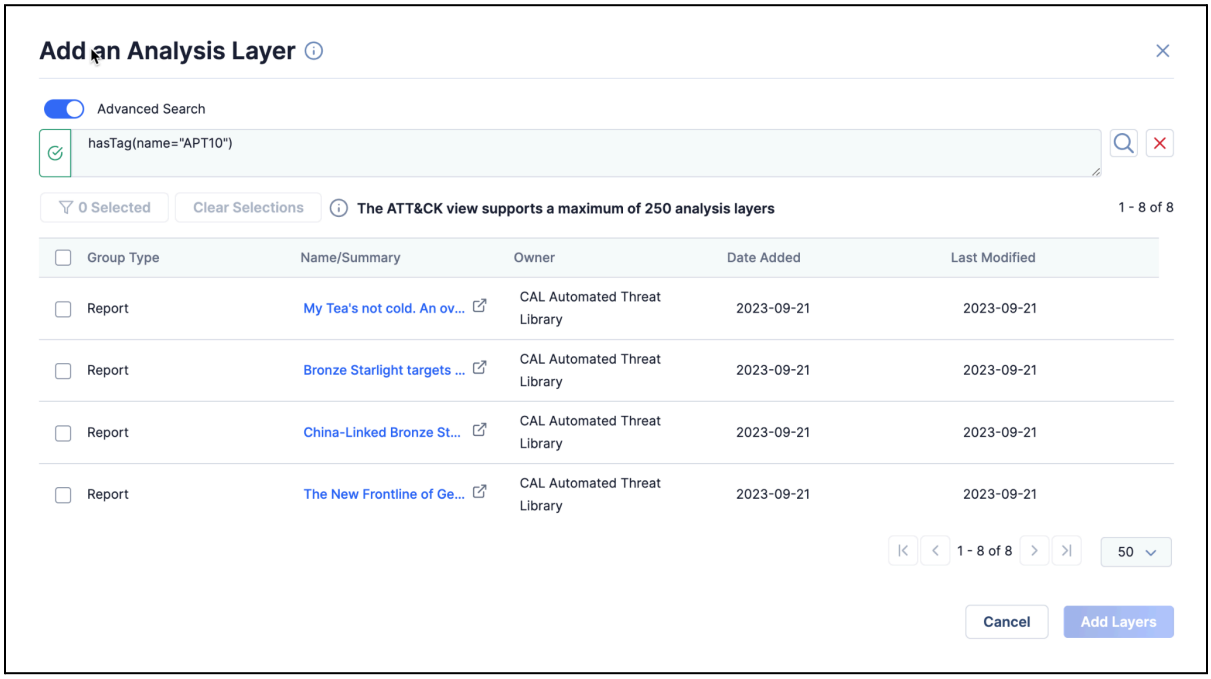
Our user-friendly color-coded heat map in the **Technique Prevalence** view simplifies your analysis by using color to represent how prevalent each technique is compared with the other techniques shown in the view. There are four possible colors, representing each quartile of prevalence [**75% - 100% (Highest)**, **50% - 74% (High)**, **25% - 49% (Moderate)**, and **Less than 1% - 24% (Lowest)**], and a legend for these colors is displayed in the **Analysis Layers** dropdown. (Once again, we recommend that you check out this view in light and dark mode to see which you like better!) This approach supports focused threat analysis, allowing you to spotlight and thoroughly investigate techniques employed by your selected threat groups.

Technique Prevalence *view helps you focus on the most commonly used techniques of the selected Groups*

Advanced Group Filtering

In version 7.2 of ThreatConnect, the ATT&CK Visualizer provided only basic filtering options for Group selection, such as owner and Group type. In version 7.3, we introduce advanced Group search capabilities with TQL to give you even more flexibility and precision so you can truly focus your analyses on your Groups of interest. Being able to use TQL to narrow down

your search for Groups to add as analysis layers to an ATT&CK view is especially useful when dealing with extensive datasets or intricate investigations.

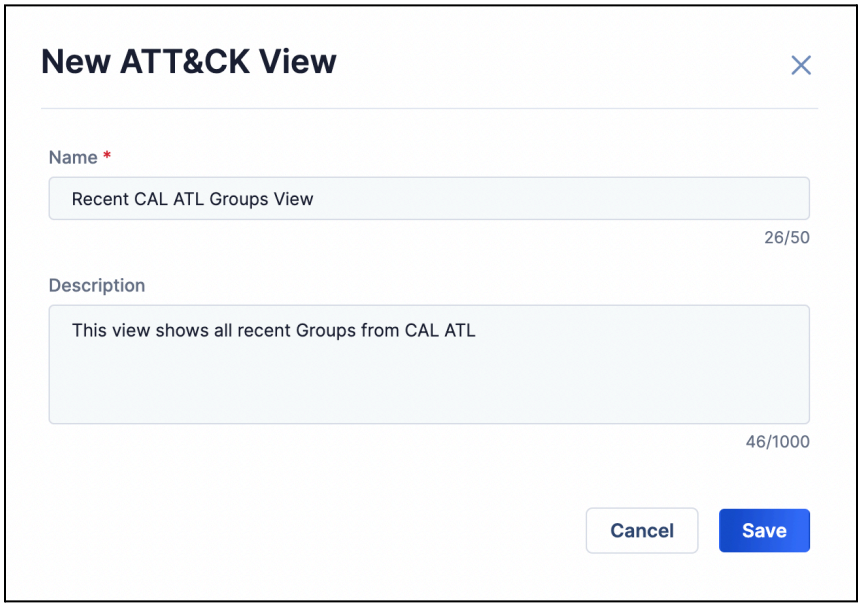


Use TQL to search for Groups more precisely and efficiently

Save ATT&CK Views

You can now easily save your ATT&CK views, save copies of your views for ongoing work, save changes to existing views, switch between views, delete views you no longer need, and close views.

Once you create an ATT&CK view, you can name and save it by clicking the **Save View** button at the upper right. All saved ATT&CK views are accessible from the main **ATT&CK** screen that is displayed when you click **ATT&CK** on the top navigation bar. When working in a view that you have already named and saved, you can click the **Save** button at the upper right to view a dropdown with options to save your changes to the existing view or create a new copy of the view with those changes. In addition, you can search for saved ATT&CK views by name directly from the **ATT&CK** screen, as well as edit metadata for a view, save a copy of the view, and delete the view..These enhancements to the ATT&CK Visualizer provide you with greater flexibility and enable you to streamline your experience when analyzing and customizing ATT&CK views.

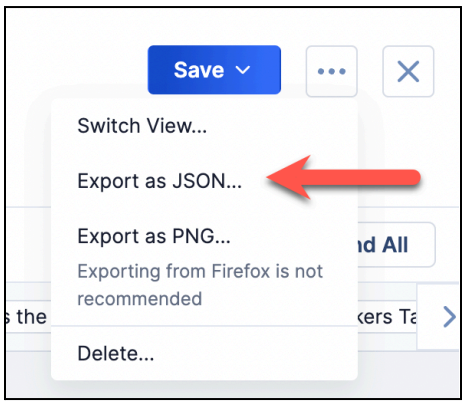


Save your ATT&CK views for future viewing, analysis, and updates

Read Only Users can also take advantage of some of the ATT&CK Visualizer functionality. They can view saved ATT&CK views and build new ones by adding Groups to a view, but they cannot save or modify any views.

Export ATT&CK Views as JSON Files

In addition to being able to save the ATT&CK views you create, you can now export your views as JSON files, enabling you to easily share them with colleagues, team members, and other stakeholders, who can then import and view them via their own ThreatConnect accounts. This capability promotes collaboration and knowledge sharing.



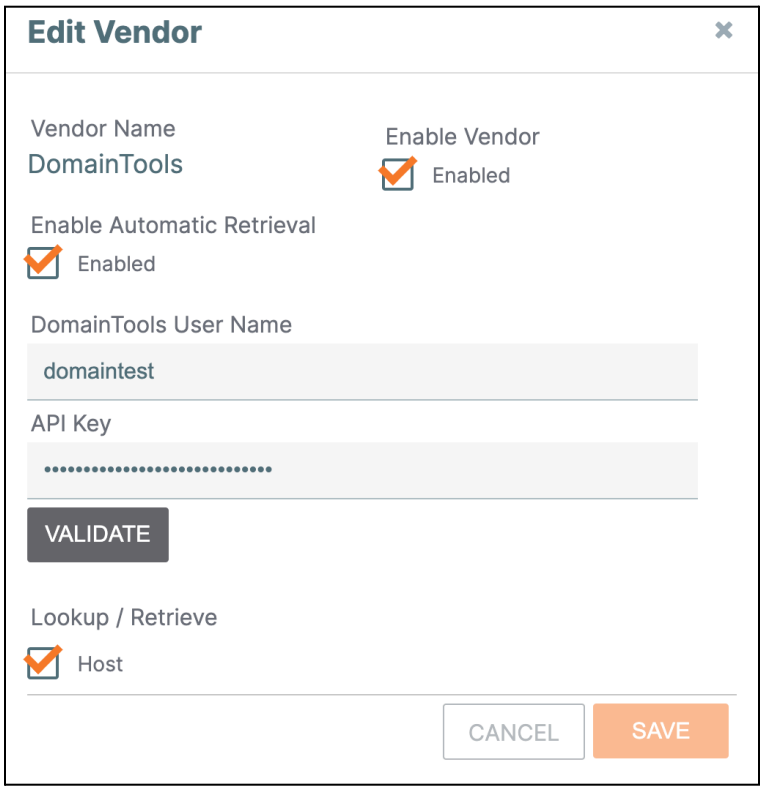
Export ATT&CK views as JSON files for easy sharing and collaboration

Built-In Enrichment

DomainTools Enrichment

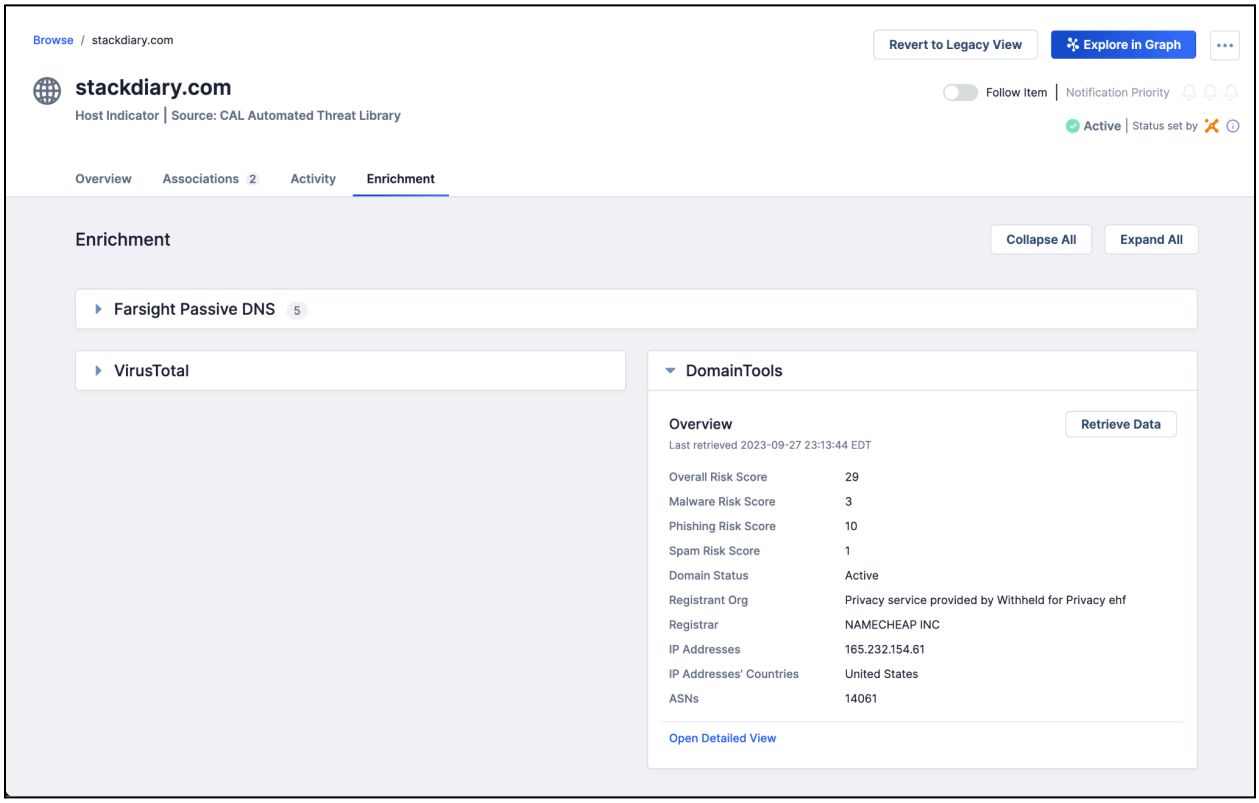
We are excited to introduce another powerful built-in enrichment feature in our 7.3 release, this time powered by DomainTools®. This easy-to-use integration allows you to apply the DomainTools deep domain insights directly within ThreatConnect, providing you with a more complete perspective on potential 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 DomainTools username and API key to the **Enrichment Tools** section of the **Indicators** tab of **System Settings**, validating these parameters, and then selecting the **Host** Indicator type.



*Configure the DomainTools enrichment in **System Settings***

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



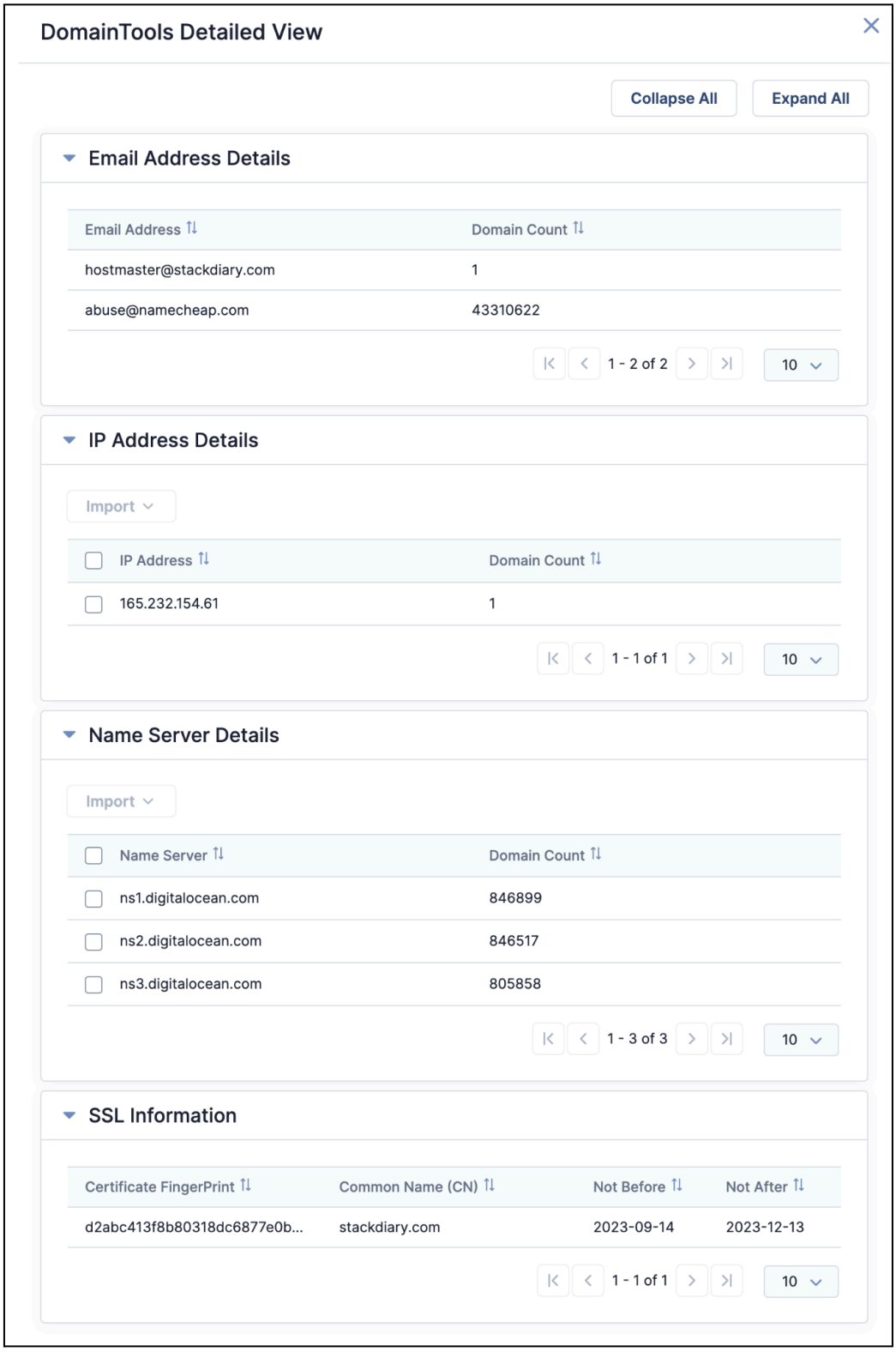
*View DomainTools enrichment data on the **Enrichment** tab of a Host Indicator's **Details** screen*

When you navigate to a Host Indicator's **Enrichment** tab for the first time, information from DomainTools is pulled and cached. Every time you revisit the **Enrichment** tab for the Indicator, cached data will be displayed until a new DomainTools lookup is made after the caching time limit expires. To get the latest enrichment data from DomainTools before the caching time limit expires, you can always click the **Retrieve Data** button on the **DomainTools** card.

To delve further into the information DomainTools has about a Host, click the **Open Detailed View** link at the lower left of the **DomainTools** card. This will open the **DomainTools Detailed View** drawer, where you can view comprehensive details about what DomainTools knows about the Host Indicator.

The **DomainTools Detailed View** drawer can display the following types of information, depending on availability for the particular Indicator:

- **Email Address Details**: This card displays the email addresses connected to the domain under investigation and provides a count of other domains associated with each email address.
- **IP Address Details**: This card displays the IP addresses associated with the domain under investigation and provides a count of other domains linked to each IP address.
- **Name Server Details**: This card displays the name servers associated with the domain under investigation and provides a count of other domains linked to each name server.
- **SSL Information**: This card displays information about the SSL certificate linked to the domain under investigation, including certificate fingerprint, common name (CN), and dates establishing the time window during which the certificate is valid.

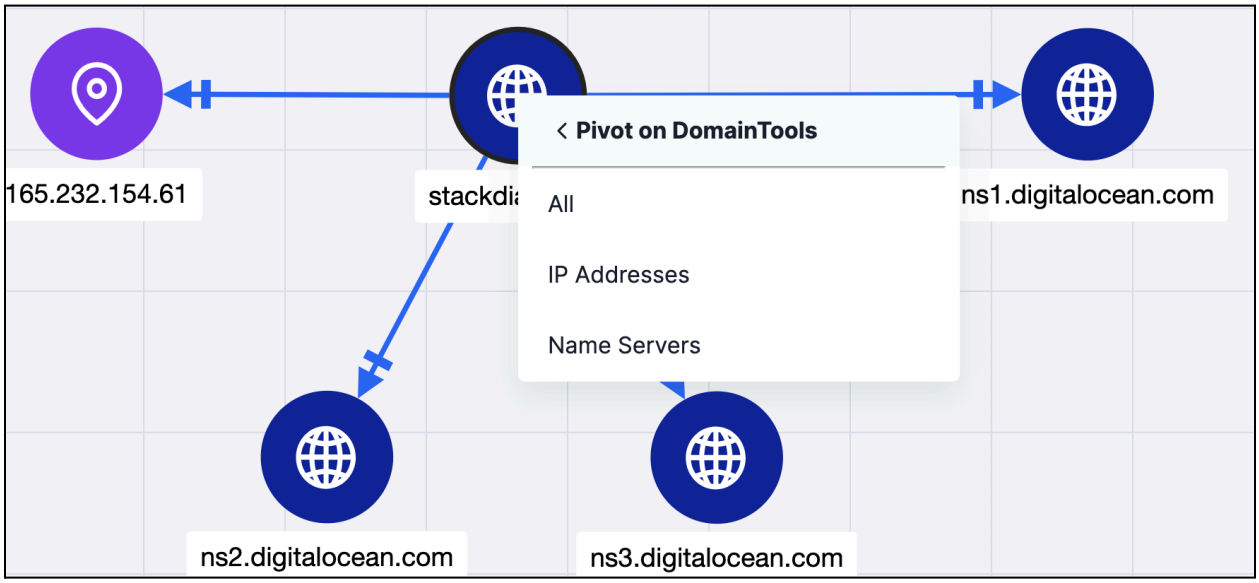


*The **DomainTools Detailed View** drawer provides information DomainTools has on a Host Indicator*

Having these detailed insights empowers you to

- detect potential shared ownership or bulk domain registration practices,
- identify possible suspicious activities tied to domains,
- deepen your understanding and enhance the depth of domain investigations,
- validate certificate authenticity by comparing fingerprints,
- identify potential security risks if a certificate fingerprint matches known malicious sources, and
- verify the intended domain for an SSL certificate, safeguarding against potential misuse like impersonation or phishing.

The relationships identified through the DomainTools enrichment can also be visualized in Threat Graph.



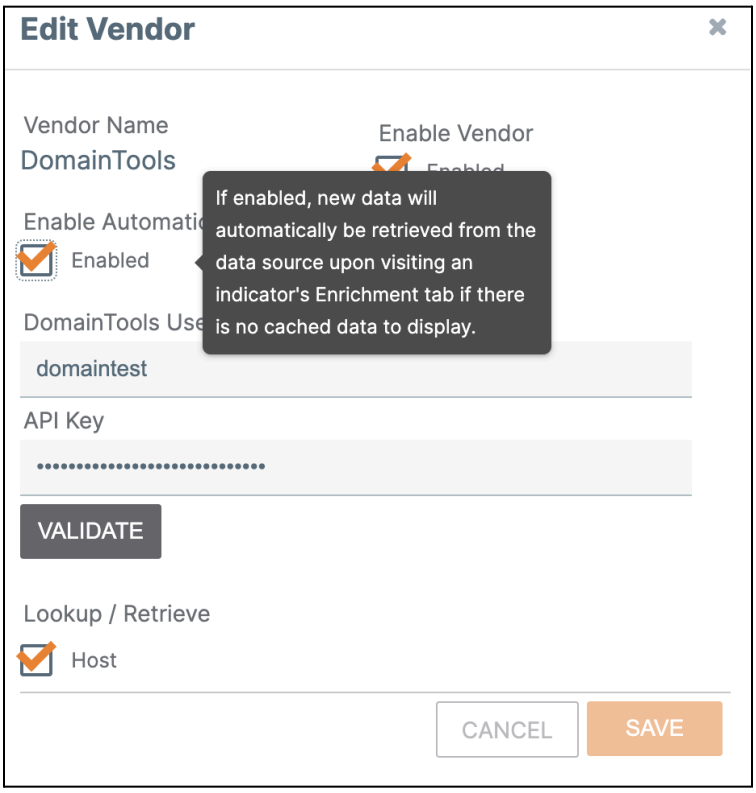
Pivoting on DomainTools enrichment data in Threat Graph gives you insight into an Indicator's IP addresses and name servers

We have also made the DomainTools enrichment data points available in the UI accessible via the v3 API. This allows you to leverage the existing `/v3/indicators/enrich` and `/v3/indicators/{id or summary}/enrich` v3 API endpoints to enrich Indicators with DomainTools automatically, eliminating the need to navigate to the **Enrichment** tab in the UI and making the enrichment process more efficient and streamlined.

Enhanced Control Over Enrichment Tool Lookups

In this update, we've enhanced System Administrator autonomy over the automatic lookup capabilities of all of our currently available enrichment tools: VirusTotal™, Shodan®, urlscan.io, Farsight Security® Passive DNS, and DomainTools.

System Administrators can now enable or disable automatic lookups for each enrichment tool in the tool's configuration in **System Settings > Indicators > Enrichment Tools**. Automatic lookups are activated by default. Disabling them prevents information from the enrichment tool from being automatically downloaded when a user accesses the **Enrichment** tab for an Indicator of the type(s) covered by the service. In this case, users would have to click the **Retrieve Data** button to initiate enrichment. Once obtained, enrichment data are cached per the time limit established in the system settings and remain accessible until expiration. This added flexibility empowers System Administrators to control the enrichment process, offering them discretion on when and how to employ the built-in enrichment functionalities and thereby making the enrichment process more flexible and user centric.



*Enable or disable automatic enrichment in **System Settings***

Improvements

Enrichment

- The urlscan.io enrichment functionality has been expanded as follows:
    - The **URLScan Detailed** view drawer, accessible from the **Enrichment** tab of the new **Details** screen for URL Indicators, has two new cards: **Certs Details**, which provides certificate details for all of the URL's current SSL certificates, and **Links to Domains**, which displays a list of links present on the URL that lead to other domains or external websites. The Indicators displayed on the **Links to Domains** card may be imported into ThreatConnect and associated to a new or existing Group.
    - You can now pivot on urlscan.io enrichment data in Threat Graph for URL Indicators. Available pivot types are **IP Address** and **Links to Domains**.

System Settings

- The following new system settings were added:
    - **intelReqResultsRefreshExecutionTime**: This setting determines the system time at which the Intelligence Requirement results refresh monitor will poll ThreatConnect and the ThreatConnect Global Intelligence Dataset for new local and global results, respectively, for IR keyword queries.
    - **intelReqResultsRefreshMonitorEnabled**: This setting turns the Intelligence Requirement results refresh monitor on or off. If this setting is turned off, results will not be retrieved automatically for IR keyword queries. In this scenario, you must click the **Retrieve Results** button on the **Overview** tab of an IR's **Details** screen to manually retrieve the most recent results for the IR's keyword query.
    - **thirdPartyEnrichmentAPILimit**: This setting determines the maximum number of Indicators API users can enrich in a single request to the `/v3/indicators/enrich` ThreatConnect v3 API endpoint.

API & Under the Hood

- All date-time fields and query parameters in the v3 API now support ISO 8601 format.

- The following date-time fields are now supported on the Indicators and Groups v3 API endpoints and the Batch V2 API: `firstSeen`, `lastSeen`, `externalDateCreated`, `externalDateExpires`, and `externalDateLastModified`. Users can include these fields in the request body for requests made to the Indicators and Groups v3 API endpoints and in a JSON file uploaded to the Batch V2 API. They can also return these fields in API responses and filter results with corresponding TQL parameters when using the v3 API.
- The `/v3/indicators/enrich` endpoint now allows users to define Indicators in the request body by using each Indicator's `id` or a combination of each Indicator's `type`, `summary`, and, if not in the user's Organization, `ownerName`. This endpoint will also return enrichment data for enriched Indicators and more verbose error logging when an error occurs with the request.
- The Playbooks v2 API endpoints now accept a Playbook's ID or Group XID when targeting a specific Playbook in a request.
- When using the Batch V2 API, you can now specify whether to pin Attributes to the **Attributes** card of an object's **Details** screen via the `pinned` field. This field accepts a Boolean value.

Bug Fixes

Threat Intelligence

- MITRE ATT&CK sub-technique T1036.002 was missing from the ATT&CK Visualizer. It has now been added.
- 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.
- An issue causing TQL queries using **hasIndicator()** containing references to certain Indicator values to return an error has been resolved.
- Some minor UI enhancements were made on the **Associations** tab of the new **Details** screen to ensure that the terms used in the tables' column headers match the terms used in the column selectors.

Playbooks

- An issue causing Playbooks that have just been activated not to execute because the Playbook's Trigger is experiencing a delay in becoming active has been resolved.

Workflow

- In ThreatConnect version 7.2.1, potential Case associations had to be enabled for at least one of your Communities or Sources in order for potential associations to be suggested for Cases in your Organization. This issue has been resolved. You no longer need to enable potential Case associations in a Community or Source to receive suggested potential associations for Cases in your Organization.
- Code refactoring was incorporated to enable performance improvements for potential associations for Workflow Cases.

API & Under the Hood

- 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.

- The `/v2/indicators/observed` endpoint in the v2 API was erroneously returning the last time the API user observed any Indicator, not the specific Indicator entered in the query. This issue has been fixed.
- An issue causing errors to occur in MySQL® queries, particularly COUNT queries, was resolved.
- An issue preventing SAML authentication events from emitting an audit log has been fixed.

Dependencies & Library Changes

- ThreatConnect is now running OpenSearch® version 2.6.0.

Maintenance Releases Changelog

2023-12-13 7.3.3 [Latest]

Bug Fixes

- An issue causing database lookup failures in the V2 Batch API when handling large numbers of Group associations was fixed.
- An issue causing the index lists in the Datastore Explorer in the Playbook Designer to overrun the dark background when viewing ThreatConnect in dark mode has been resolved.
- An issue causing IP geolocation services to fail for all Address Indicators if an invalid Address Indicator is entered into the system was resolved.
- An issue causing the search bar in the **Results** section of the **Keyword Tracking & Results** card on the **Details** screen for IRs to be case sensitive was resolved.
- An issue causing checkboxes that have been selected in certain Playbook App configurations to revert to an unselected state after the configuration has been saved was fixed.
- An issue preventing file hashes from being able to be merged on the **File Hash Details** card of a File Indicator's **Details** screen was fixed.
- An issue causing an error when trying to create IRs with large ID numbers on certain ThreatConnect instances has been resolved.
- After adding default key/value entries in the **install.json** file in a Playbook App configuration, switching the action and then returning to the previous action would result in an error and the added entries being removed from the table. This issue has been resolved.
- When using the v3 API to upload a document file to a Report Group and the Report's XID is used as its identifier, the file type and size were being deleted. In addition, Report Groups created through the v3 API were unable to have document files uploaded to them. These issues have been corrected.
- An issue preventing the **Search** drawer from opening from the **System Settings** screen has been fixed.
- When a user's system role is changed, the user's Community and Source permissions are set to the default permissions that their Organization has in those owners. An

issue that was preventing some of these permissions from changing, resulting in the user being unable to access some of their Communities and Sources, was resolved.

2023-11-21 7.3.2-M1121R

Bug Fixes

- When using the v3 API to upload a document file to a Report Group and the Report's XID is used as its identifier, the file type and size were being deleted. In addition, Report Groups created through the v3 API were unable to have document files uploaded to them. These issues have been corrected.

2023-11-15 7.3.2

Bug Fixes

- An issue causing certain multiselect dropdowns for Playbook Apps to erroneously display selected items when the App is edited for the first time was resolved.
- An issue causing continuous requests to occur and cause latency when viewing Playbook executions was fixed.
- An issue causing an error to occur when using the v3 API to update Security Labels in Group Attributes has been resolved.
- An issue causing selections made in the Doc Analysis Import feature to reset when the section in which the selections were made is hidden was fixed.
- The **TC - Search Refresh** App is now exempt from the time limit set by the **appsRuntimeKillMinutes** system setting.
- An issue causing the App Builder not to pass Python® proxy flags correctly was fixed.
- IR results will no longer refresh after details that do not affect the results (e.g., **Subtype**, **Category**) are updated.
- An issue causing the **Category** field for an IR to clear when updating other fields on the **Details** card of the **Details** screen for an IR was fixed.
- An issue causing the **Import as Playbook** option on the **Templates** screen for Playbooks to be available to Read Only Users has been fixed.

- An issue causing an error to occur when creating a dashboard **Query** card that sorts on **Matched** with a **Display Type** of **Datatable** and a **Query By** selection of **Intelligence Requirement Results** has been resolved.
- An issue preventing labels and numerical data on treemap charts added to reports from being included in PDF exports of the reports was fixed.
- An issue causing duplicate results to be displayed by TQL queries that return large amounts of data over multiple pages was resolved.
- An issue preventing the **tc.log** from rolling over was fixed.
- An issue causing dates instead of Group types to be displayed on the *y*-axis of **Heat Map** cards in imported dashboards was resolved.
- Changes to Indicator Status will now be displayed on the **Activity** tab of the Indicator's **Details** screen.
- An issue causing the text of a selected saved query not to be displayed in the **Advanced Query** field of the **Query** step when creating or editing a query card for a dashboard was fixed.

2023-10-27 7.3.1-M1027R

Bug Fixes

- An issue causing Tags containing uppercase letters to not be included in imports via the batch API has been resolved.

2023-10-26 7.3.1-M1026R

Bug Fixes

- An issue causing the App Builder not to pass Python proxy flags correctly was fixed.
- An issue causing the **Category** field for an IR to clear when updating other fields on the **Details** card of the **Details** screen for an IR was fixed.
- An issue preventing the **tc.log** from rolling over was fixed.

2023-10-18 7.3.1

Bug Fixes

- A change was added to the proxy flags to enable the App Builder to run in an environment with a proxy server.
- An issue causing Groups added one at a time, or the first Group when adding multiple Groups at a time, as an analysis layer to an ATT&CK view to be displayed in the same color until the view is saved has been resolved.
- An issue preventing Apps deleted in the App Builder UI from being deleted on the file system was fixed.
- An issue causing incorrect data to populate on the **MTTD Average** and **MTTR Average** Cases Metric dashboard cards for instances running ThreatConnect on PostgreSQL® was fixed.
- An issue causing an error to occur when duplicating a Workflow containing an automated Task was fixed.
- The `/v3/intelRequirements/results` endpoint now supports archiving a result, associating a result to an IR object, and marking a result as a false positive. This endpoint also supports the creation of new data when associating global results to an IR, and additional permission checks have been added to ensure data integrity and security are maintained when updating IR results.
- An issue causing the download of Playbook execution logs to time out after 5 minutes was resolved.
- An issue causing latency when copying a Group from a Community or Source to an Organization was fixed.