ThreatConnect® Release Notes

Software Version 7.4

January 10, 2024

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

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

Table of Contents

New Features and Functionality

ATT&CK Visualizer Version 3

In our latest release of ATT&CK® Visualizer, we're thrilled to unveil three impactful features designed to elevate your organization's security posture:

1. **Map Your Security Coverage for Techniques and Sub-techniques**: You can gain a comprehensive understanding of your security landscape by visualizing your coverage for each MITRE ATT&CK® technique and its sub-techniques. This feature enables you to evaluate the strengths and weaknesses for the specific techniques you're concerned about, while also helping you identify security gaps by overlaying any ATT&CK view with your existing coverage. This feature is a powerful tool for enhancing your defense strategies with precision.
2. **Identify Alike Threat Actor Groups**: You can make threat analysis more targeted and efficient by quickly identifying Groups using similar techniques and sub-techniques. This focused approach helps you find similar threat groups, keeping you ahead of potential threats.
3. **Import MITRE ATT&CK Navigator JSON Files**: This feature enables you to import JSON files for views built in the MITRE ATT&CK Navigator into the ThreatConnect ATT&CK Visualizer. By using ThreatConnect as a centralized platform for ATT&CK views, your security teams will be able to collaborate more effectively. Imported ATT&CK views also provide native support for **Technique Prevalence** and **Security Coverage**, simplifying the analysis and management of the imported data in the ThreatConnect ATT&CK Visualizer.

Map Your Security Coverage for Techniques and Sub-techniques

In ThreatConnect 7.4, we introduce a powerful feature that gives Organization Administrators the ability to map their Organization's security coverage in our ATT&CK Visualizer. Once an Organization Administrator has assigned levels of coverage across techniques and sub-techniques, you can seamlessly overlay the security coverage map onto any ATT&CK view, allowing you to identify which techniques are covered and which ones may need attention. This visualization will help you strategically enhance your defense strategies,

ensuring solid coverage for the techniques that are most critical to your organization's security.

Let's break down the process of assigning and visualizing security coverage into two straightforward steps.

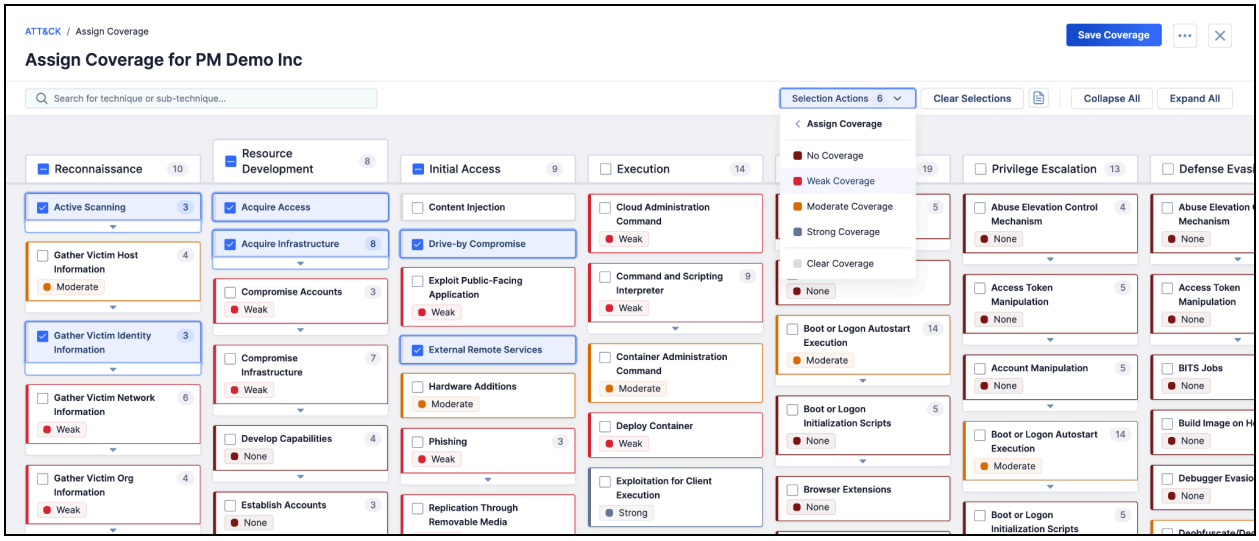
Step 1: Assign Security Coverage

Important: Only Organization Administrators can assign security coverage in the ATT&CK Visualizer. Other users may utilize their Organization's security coverage by overlaying it on their ATT&CK views.

To assign security coverage for your Organization, click **ATT&CK** on the top navigation bar to view the **ATT&CK** landing page. Then click the **Assign Coverage** button at the upper right, which will direct you to the **Assign Coverage** screen for your Organization. This screen displays all ATT&CK techniques and sub-techniques. To assign security coverage for one or more techniques, simply select the techniques, click the **Selection Actions** dropdown, select **Assign Coverage**, and choose the coverage level that best describes the techniques' security strength in your Organization:

- **Strong Coverage** if your organization's security defenses are well equipped to detect, mitigate, and respond effectively to the techniques
- **Moderate Coverage** if your organization has a reasonable amount of coverage of the techniques
- **Weak Coverage** if your organization is equipped to provide only limited coverage for the techniques
- **No coverage** if your organization's security defenses are not addressing or detecting the techniques

Each coverage level is shown in its own color, effectively giving you a heat map of security coverage across all techniques and sub-techniques in your Organization.

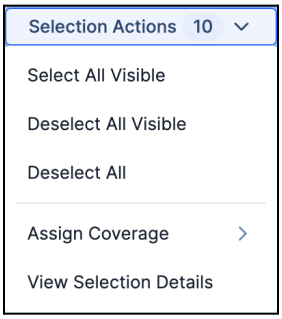


Assign security coverage for techniques and sub-techniques in your Organization

To quickly locate and assign coverage to a specific technique or sub-technique, use the search bar at the upper left to isolate the view to techniques that match your entered text.

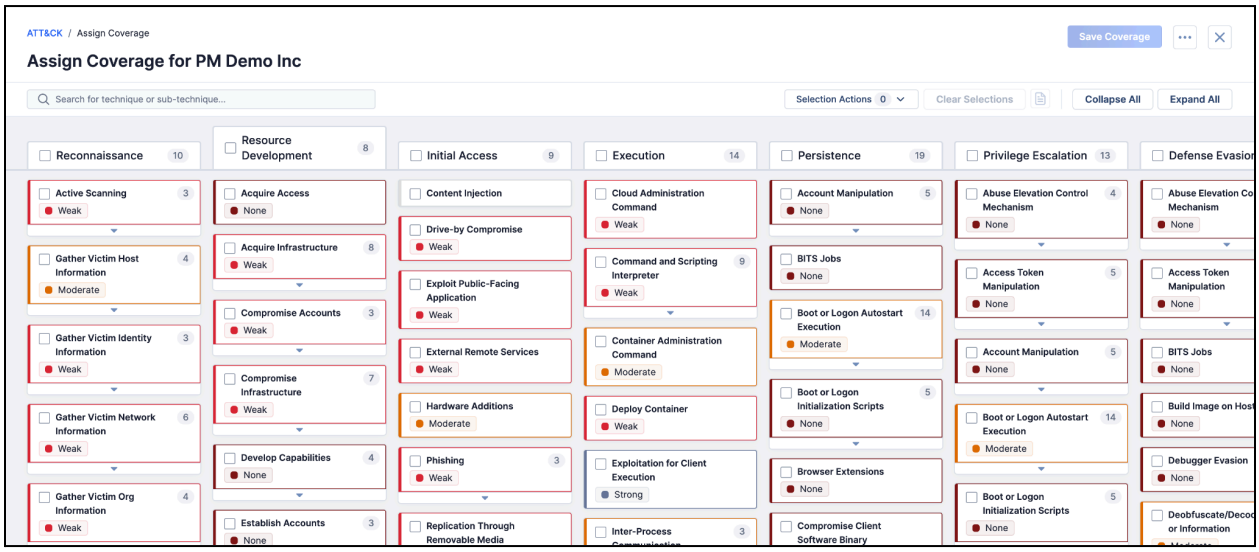
The **Selection Actions** menu provides several other handy options:

- **Select All Visible** lets you select all the techniques and sub-techniques currently visible (i.e., not collapsed) on your screen, including items that are scrolled off to the side, top, or bottom.
- **Deselect All Visible** clears selections among the visible (i.e., not collapsed) techniques and sub-techniques, including items that are scrolled off to the side, top, or bottom.
- **Deselect All** removes selections for all techniques and sub-techniques, giving you a fresh slate to work with.
- **View Selection Details** opens a drawer with details of all selected techniques and sub-techniques.



Selection options for assigning security coverage

If you do not have coverage details for a particular technique, you can choose to leave it without any assigned coverage. This ensures that your coverage assignments remain accurate and relevant. After you have mapped all of your coverage, click the **Save Coverage** button at the upper right to apply your coverage assignments in the ATT&CK Visualizer for read-only viewing for all users in your Organization.

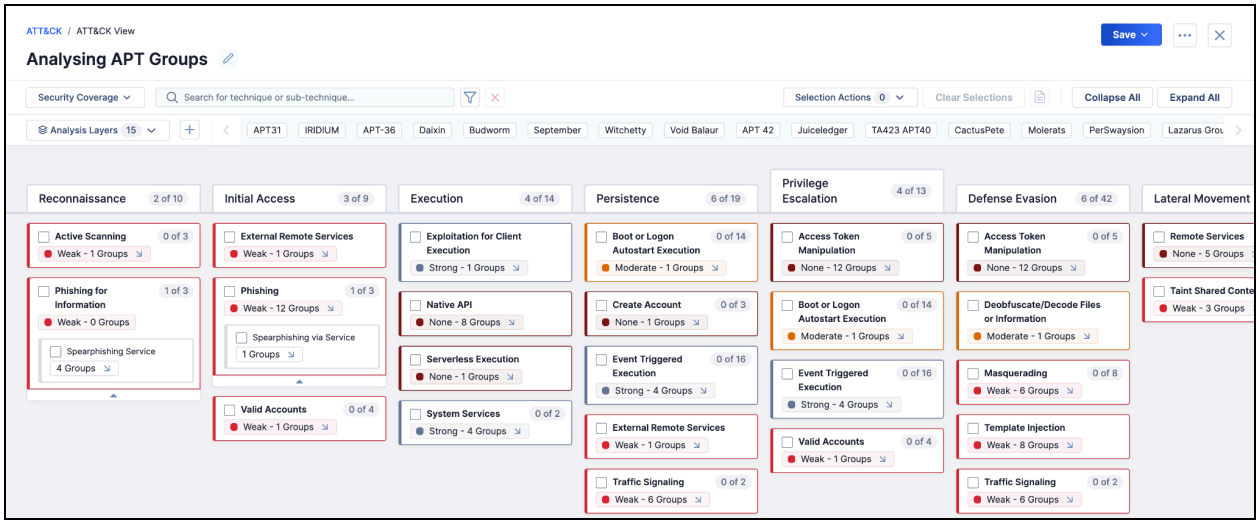


Sample security coverage assignments in ATT&CK Visualizer

Step 2: Visualize Coverage and Identify Gaps

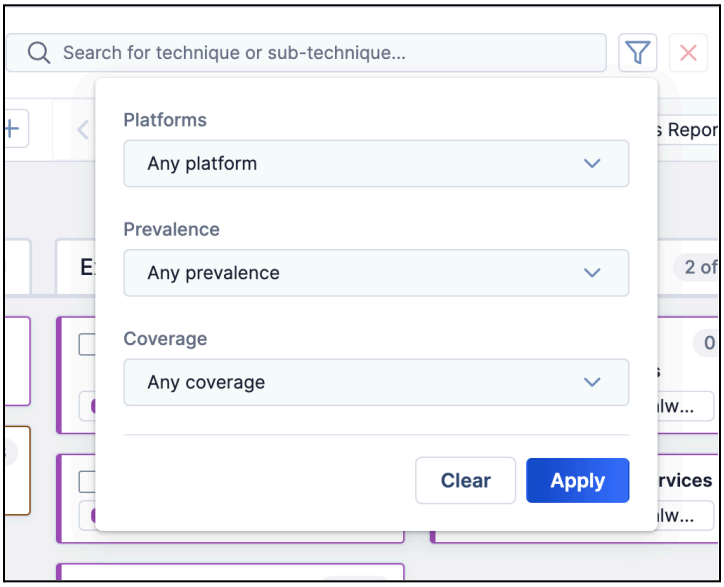
Once you have successfully assigned security coverage in your Organization, it's time to evaluate the effectiveness of your Organization's security measures. To begin, click the **+ Create ATT&CK View** button and choose **Standard View**. Once the new ATT&CK view is displayed, toggle the **Threat Group Comparison** dropdown to **Security Coverage**. Then add analysis layers to build the ATT&CK view. Once you have added all threat groups that are of interest to your analysis, this view will provide you with a detailed breakdown of your Organization's coverage for each technique, including the number of Groups actively utilizing each technique. You can also click on the field containing the number of Groups for a particular technique to view the Groups' names.

Just like on the **Assign Coverage** screen, the coverage levels are color coded, allowing you to view a heat map of the security coverage across techniques, sub-techniques, and all of your added analysis layers (Groups). You can view a legend for the color assignments in the **Analysis Layers** dropdown.



Overlay security coverage on an ATT&CK view to identify techniques and Groups with weak or no coverage

We also offer powerful new filtering options to further enhance your analysis. In ThreatConnect 7.4, you can filter your ATT&CK view data based on platform, security coverage, and technique prevalence. This feature enables you to tailor your view and focus on the specific information that matters most to your organization's security assessment. You can also take advantage of this filter option to pinpoint techniques that are highly prevalent, but have weak or no coverage, enabling you to focus your efforts on strengthening your defenses for these specific techniques.



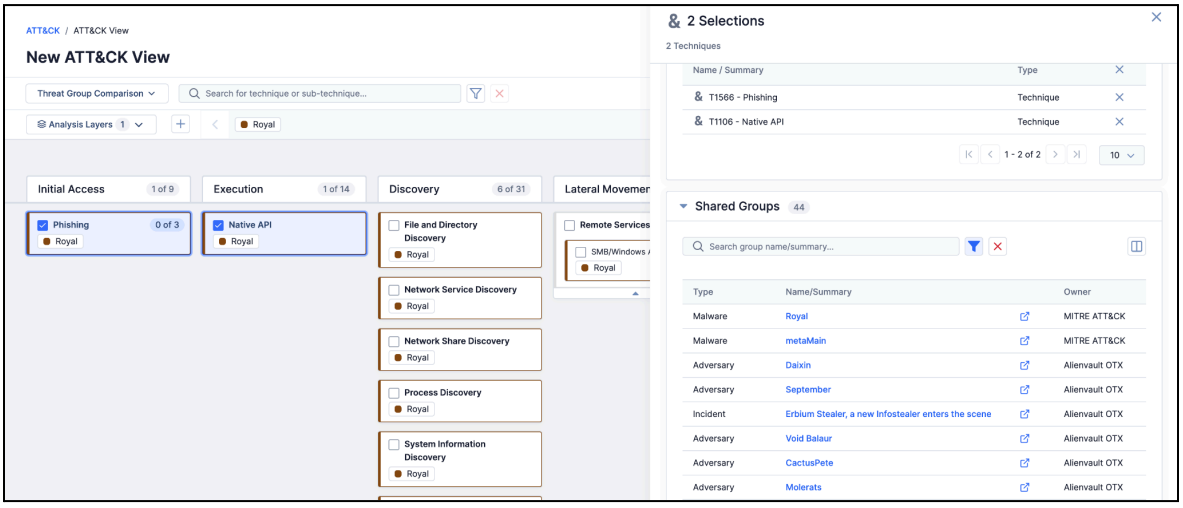
Filter by platform, prevalence, and coverage to more accurately target the areas where your organization can strengthen its defenses

Identify Alike Threat Actor Groups

In this release, we introduce a valuable feature within the ATT&CK Visualizer that allows you to identify threat groups that share similar techniques. In previous releases, we offered **ATT&CK Technique** and **ATT&CK Sub-technique** drawers containing details on shared Groups for an individual technique or sub-technique (that is, Groups across all of the ThreatConnect owners to which you have access that contain an ATT&CK Tag representing that technique or sub-technique). In ThreatConnect 7.4, you can select multiple techniques and sub-techniques to open your analysis to Groups using specific combinations of techniques and view a **Selection Details** drawer containing a list of all selected techniques and a list of all of the shared Groups.

Imagine that you are investigating a particular threat group, and you notice it uses a set of techniques. If you're curious about other threat groups that employ the same set of techniques, all you have to do is select all the relevant techniques in the ATT&CK Visualizer and view the **Selection Details** drawer. You will then be able to view all threat groups in your owners that employ those techniques.

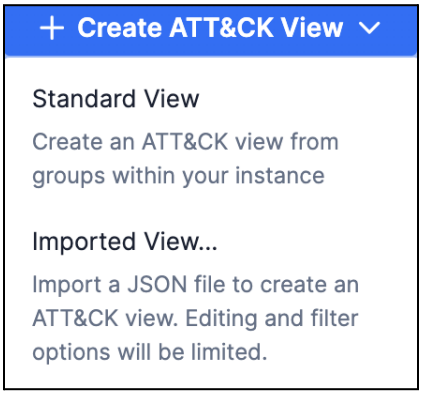
This feature not only simplifies your analysis, but also empowers you to make more informed decisions by uncovering the full scope of threat actor groups utilizing a specific set of techniques. With the ability to easily create technique combinations and derive comprehensive threat group insights, this version of the ThreatConnect ATT&CK Visualizer enhances your threat intelligence capabilities, ensuring you stay one step ahead in the ever-evolving landscape of cybersecurity.



Identify similar threat groups by selecting a set of techniques and subtechniques

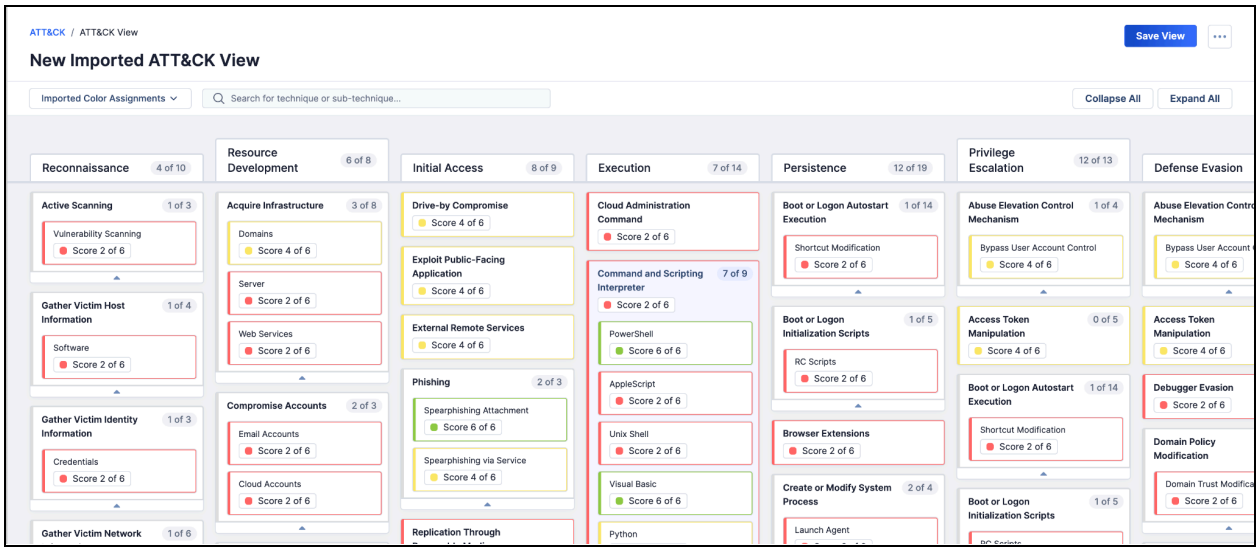
Import MITRE ATT&CK Navigator JSON Files

Finally, we are thrilled to introduce the ability to import external MITRE ATT&CK Navigator views into our platform. This capability empowers you to seamlessly integrate external threat intelligence within our system and provides a centralized location for collaboration.
Now that you can import external views, we have renamed the native ATT&CK views built using the Groups in ThreatConnect as standard views. Views imported as JSON files from the MITRE ATT&CK Navigator are called imported views. To import a view, first ensure that you have downloaded a JSON file from the MITRE ATT&CK Navigator. Then click **+ Create ATT&CK View** at the upper right of the **ATT&CK** screen, select **Imported View…**, and choose the JSON file to import.



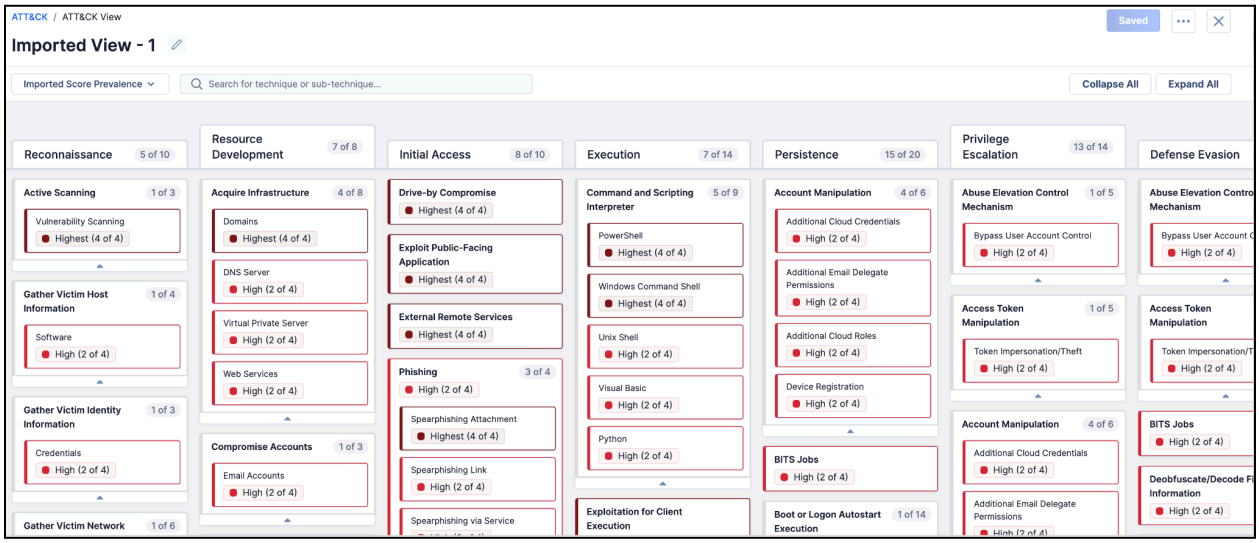
*Select **Imported View…** to import a JSON file from MITRE ATT&CK Navigator*

Imported views include the same color selections and technique scores as in the MITRE ATT&CK Navigator. To see this information, keep the default selection of **Imported Color Assignments** in the dropdown at the upper left of the ATT&CK Visualizer. This functionality allows you to easily bring externally created views into ThreatConnect, saving you time and effort by leveraging the work you have already done in the MITRE ATT&CK Navigator.



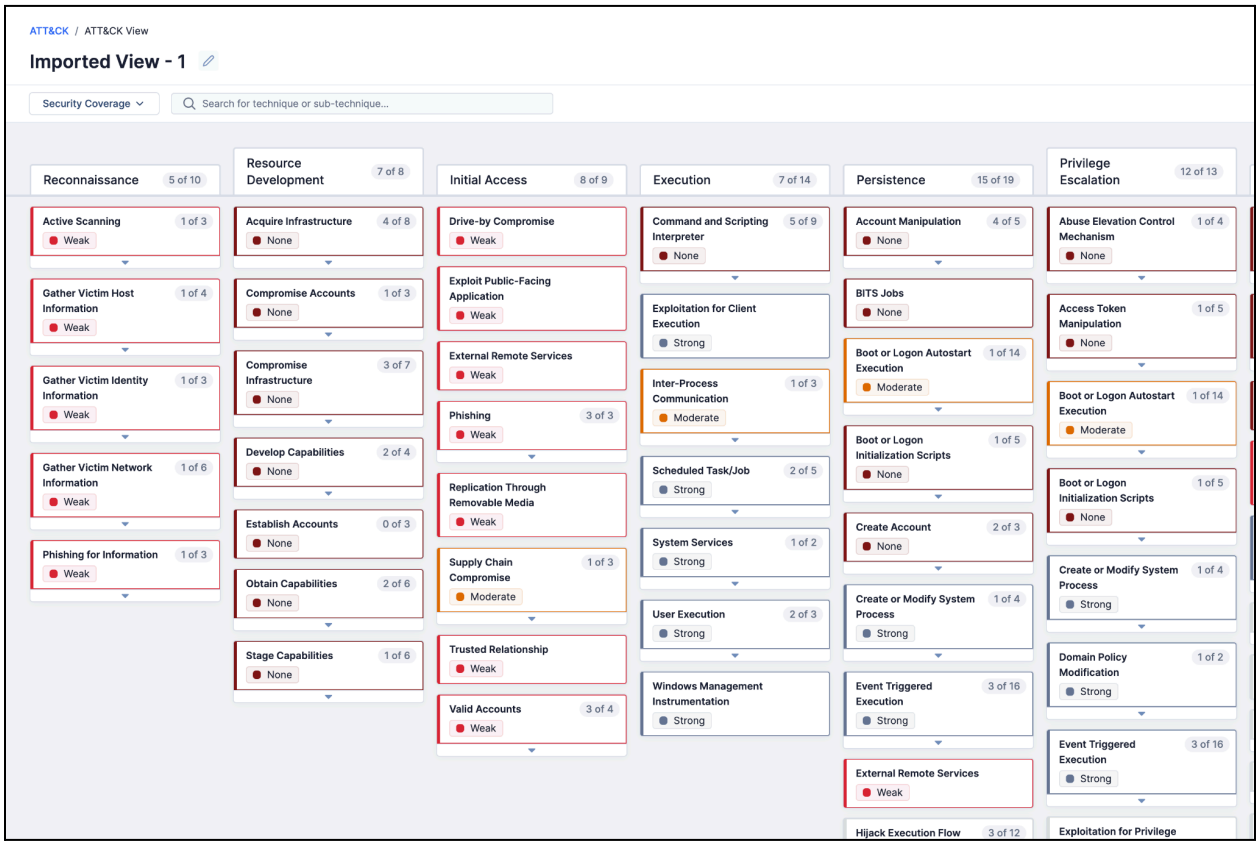
Imported view in ATT&CK Visualizer, showing MITRE ATT&CK Navigator color selections

Furthermore, our imported view also enables you to see the range of scores assigned to techniques in the ATT&CK view, as well as your Organization's security coverage across each technique. To see the score range associated with each technique that has been assigned a score in an imported view, select **Imported Score Prevalence** from the dropdown at the upper left. This view will help you identify the score range in which each technique's assigned score falls, providing you with crucial information for improving your defense strategies.



View score prevalence for imported ATT&CK views

Alternatively, you can select **Security Coverage** from the dropdown to evaluate each technique's security coverage, giving you the information you need to optimize your organization's cybersecurity strategy.



View security coverage for imported ATT&CK views

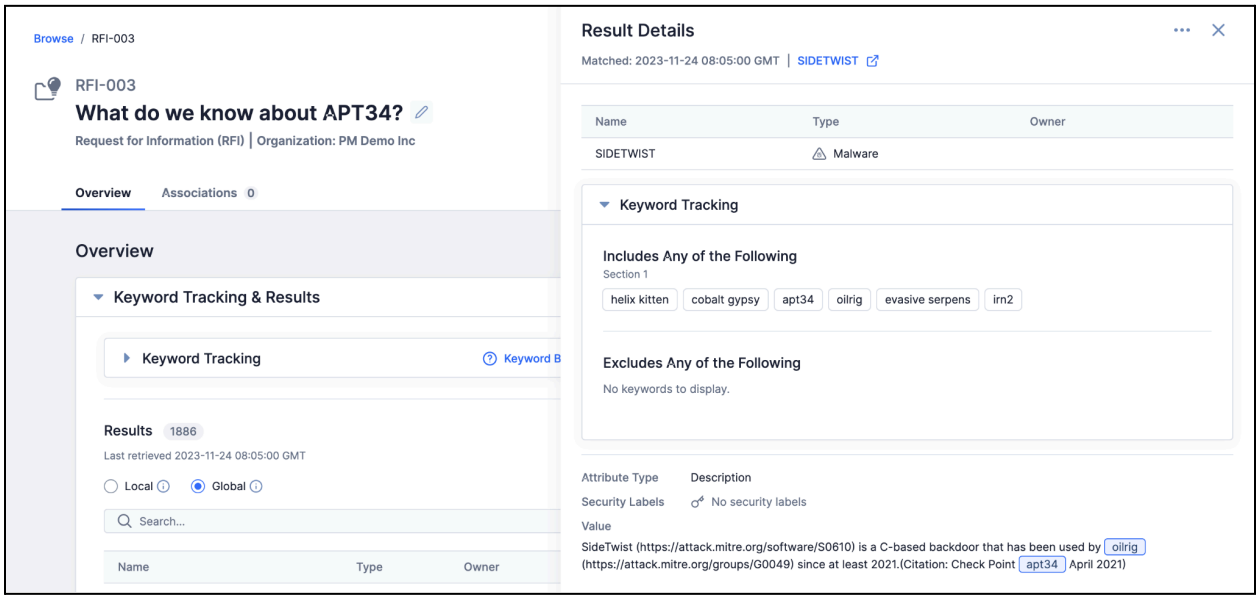
You can also save imported views for future reference. Saved imported views can be easily accessed from the **ATT&CK** screen on the **Imported Views** tab.

Just like with standard ATT&CK views, you can switch between imported views, export the views as a JSON or PNG file, and delete views you no longer need by clicking on the **Options** ••• menu at the upper right.

Intelligence Requirements Version 2

Keyword Query Exact Matches

In ThreatConnect version 7.3, we introduced our market-changing Intelligence Requirement (IR) capability. This feature allows you not only to capture your requirements in a central location, but also to automatically identify information that is likely related to your requirements. Version 2 of Intelligence Requirements builds upon the foundation set in version 1, adding the ability to quickly see the fields (e.g., part of the name of a Workflow Case) or exact information (e.g., text in a name or in a Description Attribute of an Indicator or Group) that matched an IR keyword query.



*Keyword matches are highlighted in the **Result Details** drawer*

The matched information is highlighted in the new **Result Details** drawer, which can be viewed from the **Details** screen for an IR and in step 3 (**View Results**) when creating an IR, showing you exactly where each matching keyword was found. This update removes the need to dig for exactly what matched your keywords to determine whether a result is accurate. Our goal is to enable you to spend more time analyzing and taking action on what is important and less time verifying the accuracy of the matches ThreatConnect provides.

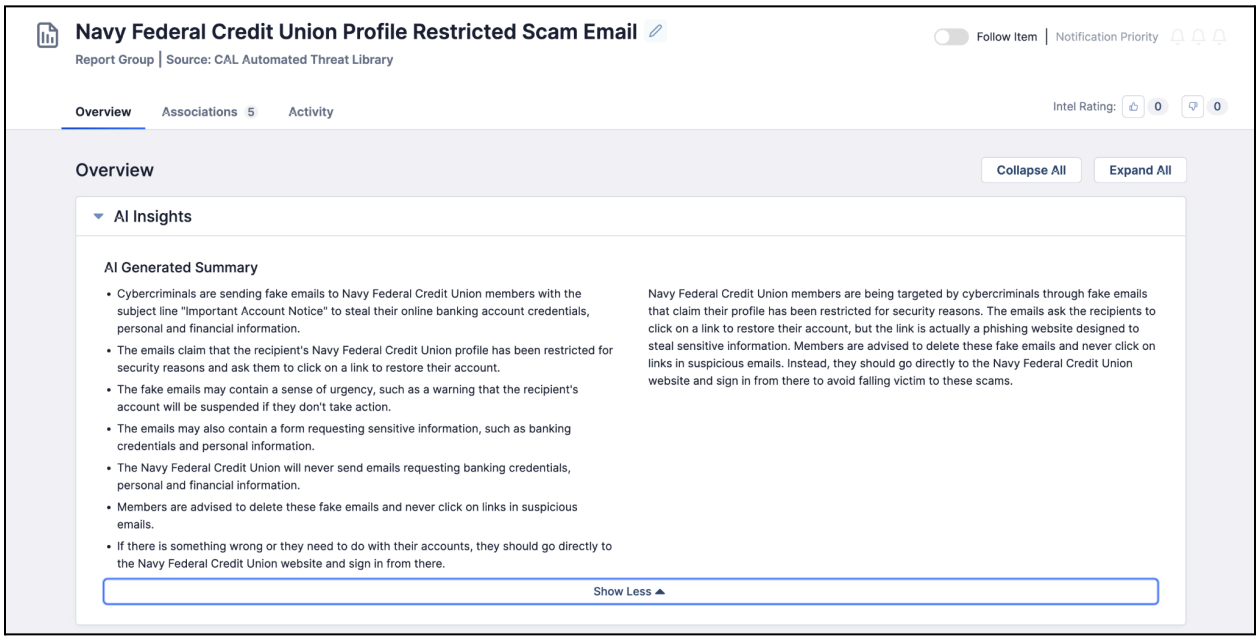
Finally, in addition to the **Result Details** drawer, you will find that we added a couple of "creature comforts" to IRs in 7.4. First, the **Get Suggestions** button now provides suggestions for industry-related words and phrases to make sure that you are able to cover

all of your bases when looking for information relevant to a particular industry. Second, associations to IRs are now shown in a new **Intelligence Requirements** card on the **Associations** tab of the **Details** screen for Groups and Indicators.

AI Insights Version 1

AI-Generated Summaries in the CAL Automated Threat Library

With the availability of generative AI technology, ThreatConnect is looking at ways we can leverage this technology in the platform for the benefit of our customers. Our first foray into AI is part of the 7.4 release of ThreatConnect, which includes AI-generated summaries for Report Groups in the CAL™ Automated Threat Library (ATL) Source.



***AI Insights** give you a quick way to understand if a Report in the CAL ATL is relevant*

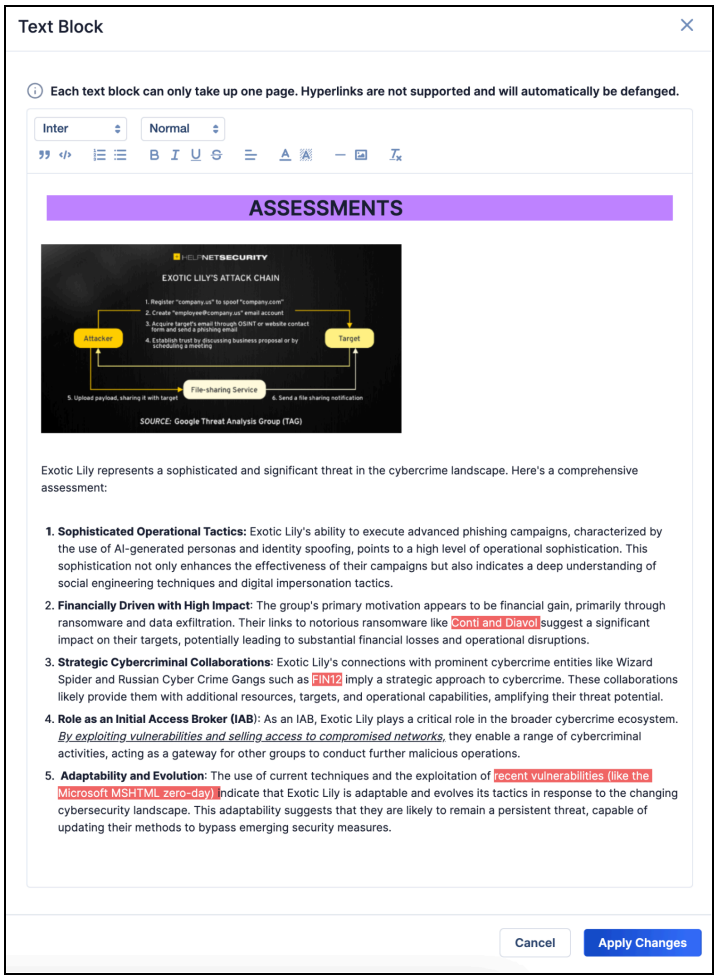
This feature provides a short, easy-to-understand set of bullet points that summarize the high points of the report or blog and a summary of the report itself. With this feature, you can get a high-level understanding of the contents of the report and quickly decide whether that report needs more analysis or attention or if it's not relevant to your organization.

New Text Editor for Reports

We are excited to introduce a powerful new text editor in our Reporting **Text Block** section that enhances your report creation experience. This innovative text editor comes equipped with a host of key features to make your reporting tasks more efficient and user friendly. You can access this new text editor in the **Report Editor** section under **Basic Elements** → **Text Block**.

Some of the key features of the new text editor are as follows:

- **Rich Text Formatting**: The new text editor provides an intuitive rich text formatting experience. You can apply formatting such as bold, italics, underlines, and more to your text with just a few clicks.
- **Inline Image Support**: You can enhance your reports by directly inserting images into them, making your reports more visually appealing and informative.
- **Text Highlighting**: You can make key information pop with text highlighting, enabling you to emphasize critical points in your reports.
- **Text Alignment**: The new text editor offers text alignment options, ensuring your content looks polished and well structured.
- **Font Color Customization**: You can add a personal touch to your documents by customizing font colors to match your branding or preferences.
- **Font Selection**: You can choose from a range of fonts to find the perfect style for your documents.
- **Improved Text Formatting**: You can now structure your reports with support for six heading levels and normal text, ensuring clarity and organization.



*Create visually appealing reports using the new **Text Block** editor*

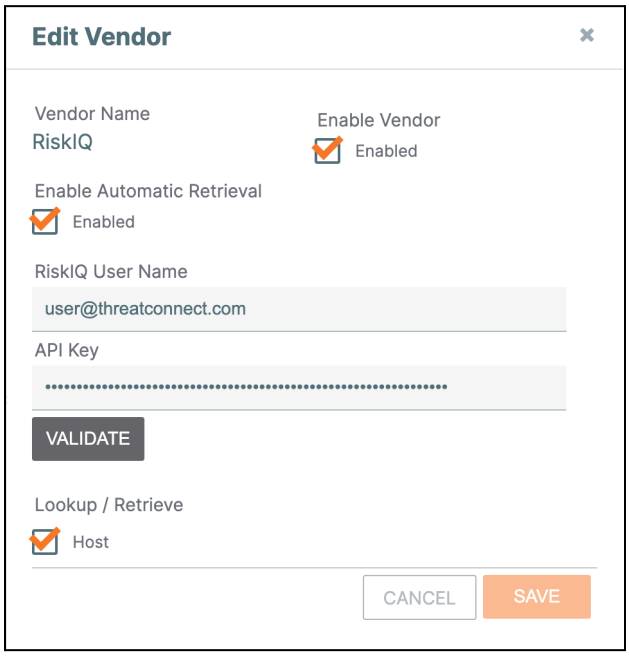
With these key features, the new text editor enables you to craft visually appealing, well-structured, and informative reports, while incorporating your branding for a personalized touch. We believe that these enhancements will significantly improve your report creation process, allowing you to create more impactful and visually engaging reports.

Built-In Enrichment

RiskIQ Enrichment

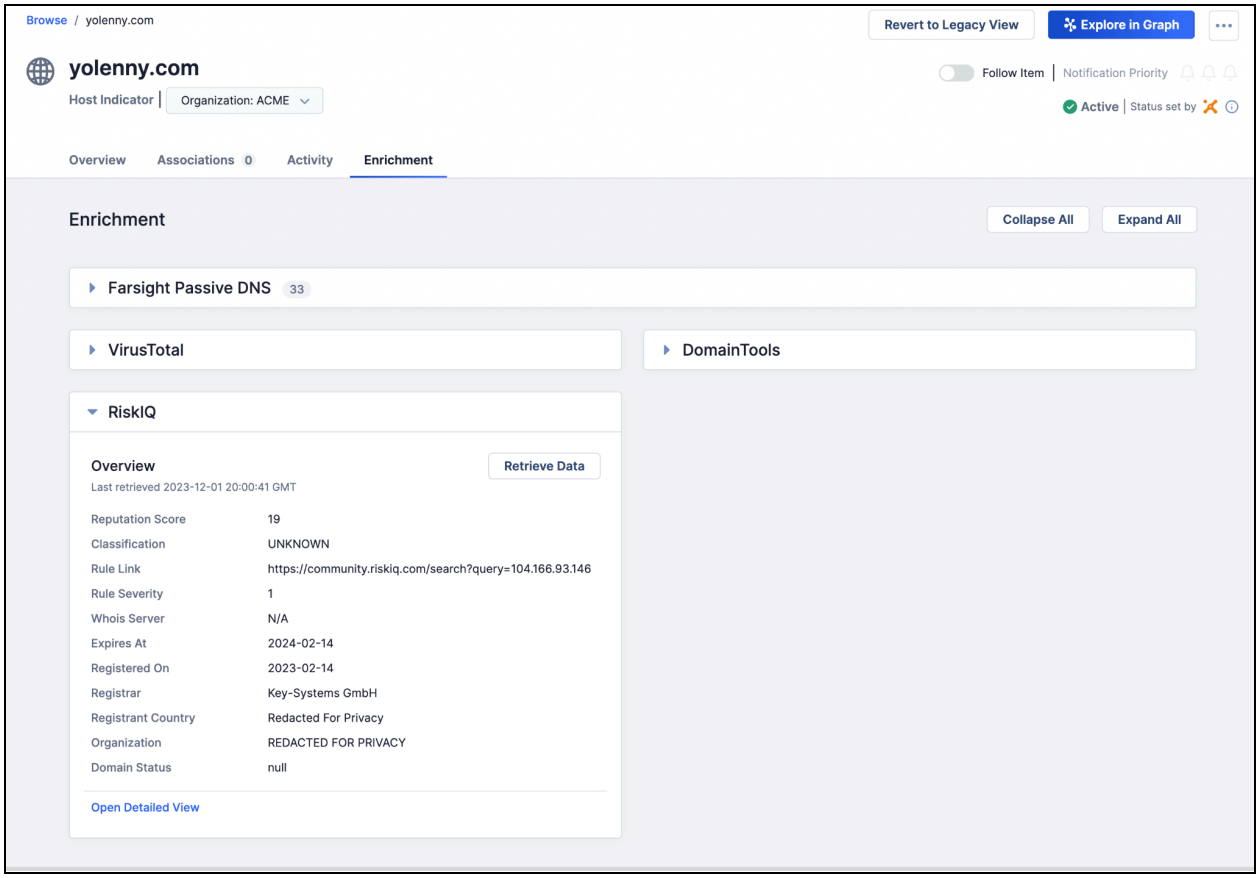
We're thrilled to unveil a robust new enrichment tool in our 7.4 update, powered by RiskIQ®. With this integration, you can leverage RiskIQ's host insights directly within ThreatConnect, providing you with essential information for evaluating potential dangers linked to a domain.

System Administrators can enable this built-in enrichment by adding their RiskIQ 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 RiskIQ 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 RiskIQ 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 RiskIQ is pulled and cached. Every time you revisit the **Enrichment** tab for the Indicator, cached data will be displayed until a new RiskIQ lookup is made after the caching time limit expires. To get the latest enrichment data from RiskIQ before the caching time limit expires, you can always click the **Retrieve Data** button on the **RiskIQ** card.

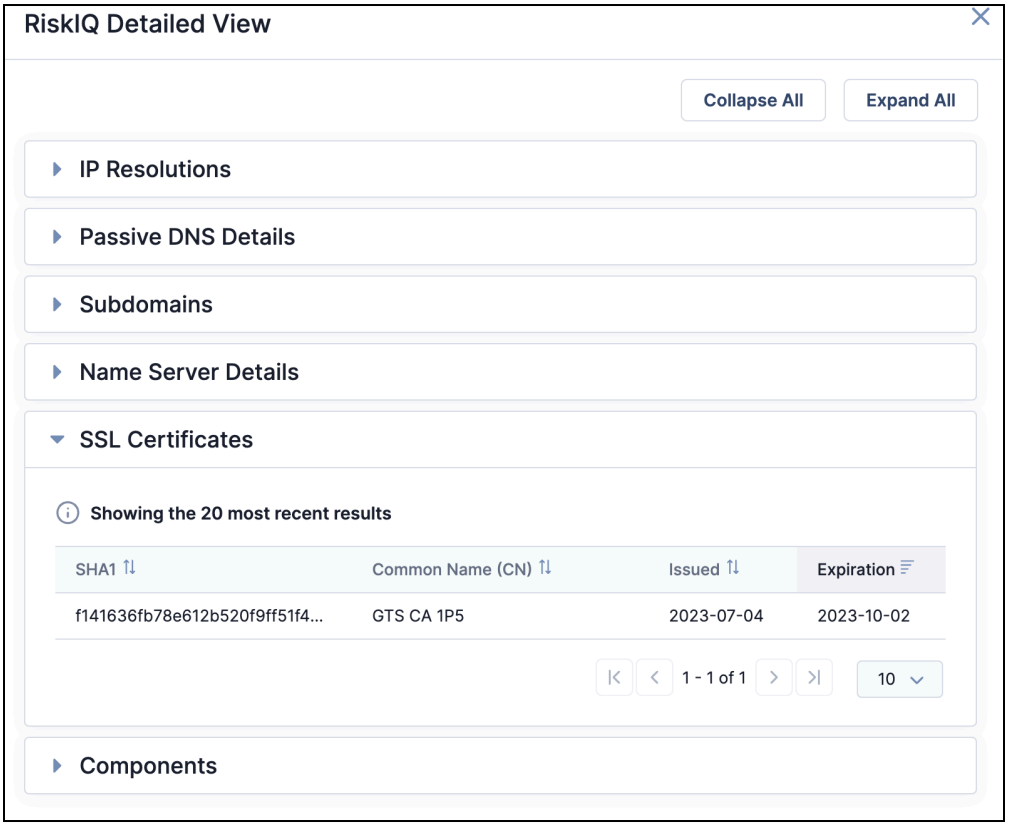
To delve further into the information RiskIQ has about a Host, click the **Open Detailed View** link at the lower left of the **RiskIQ** card. This will open the **RiskIQ Detailed View** drawer, where you can view comprehensive details about what RiskIQ knows about the Host Indicator.

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

- **IP Resolutions**: This card displays the IP addresses to which the investigated domain resolves and provides information regarding their initial and most recent sightings.
- **Passive DNS Details**: This card provides information about historical DNS data related to specific domains.This information helps in identifying patterns of malicious

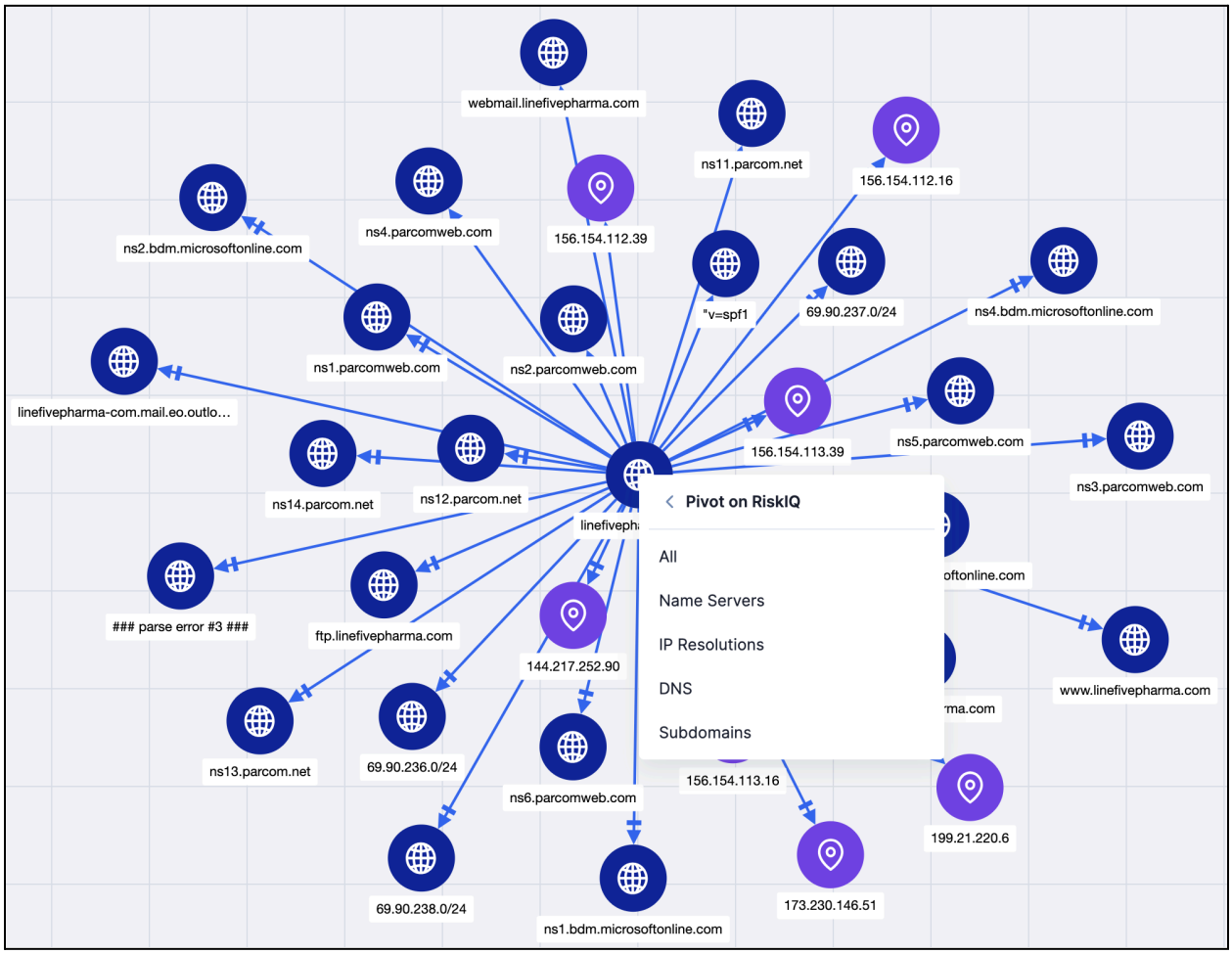
behavior, tracking the evolution of threats, and understanding the infrastructure used by cybercriminals.

- **Subdomains**: This card displays the subdomains associated with the domain under investigation, helping to identify all publicly accessible subdomains and assess potential entry points for attackers.
- **Name Server Details**: This card displays the domain's associated name servers, helping you gain insights into hosting providers and providing you with a comprehensive view of the domain's ecosystem.
- **SSL Certificates**: This card displays information about the SSL certificates linked to the domain, including SHA-1, common name (CN), and dates establishing the time window during which the certificate is valid.
- **Articles**: This card displays articles associated with the domain, offering a historical perspective on the domain's behavior, affiliations, and any prior occurrences or inquiries related to it.
- **Components**: This card displays the components associated with the domain and provides information on the components' type, version, and first- and last-seen dates.



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

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



Pivoting on RiskIQ enrichment data in Threat Graph gives you insight into an Indicator's Name Servers, IP Resolutions, DNS, and Subdomains

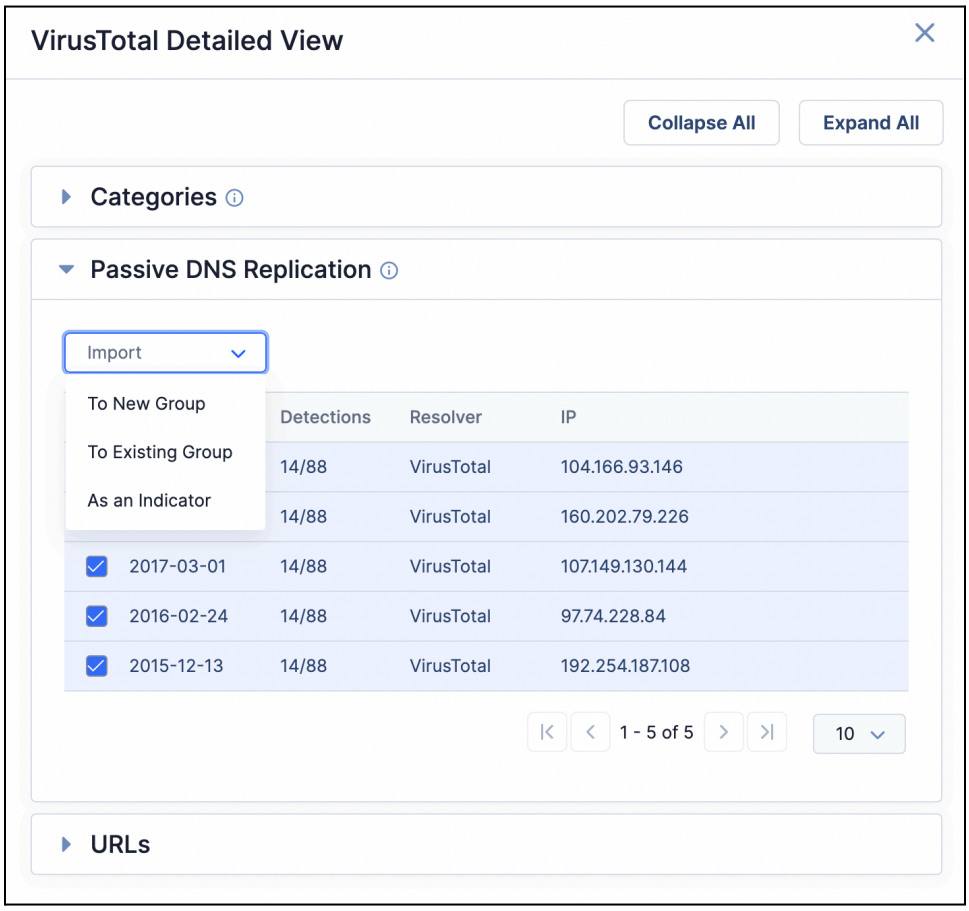
We have also made the RiskIQ enrichment data points available in the UI accessible via the v3 API. This allows you to leverage the existing `/v3/indicators/enrich` and `/v3/indicators/{id or summary}/enrich` v3 API endpoints to enrich Indicators with RiskIQ automatically, eliminating the need to navigate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

Built-In Enrichment Import Functionality Enhancement

Over the past several releases, we have continually enhanced our platform by incorporating information from leading enrichment vendors such as VirusTotal™, Shodan®, urlscan.io, DomainTools®, and now RiskIQ. These vendors provide valuable information about associated

Indicators related to the parent Indicators under investigation, which is accessible in the **Detailed View** drawer for each enrichment vendor.

In previous releases, you had the option to import these Indicators into a Group that was then associated to the parent Indicator. However, this arrangement did not provide the ability to directly associate related Indicators with the parent Indicator. In this release, we are introducing a new capability that allows you to import these Indicators as direct associations to the parent Indicator. You can now import relationship information from VirusTotal, Shodan, urlscan.io, DomainTools, and RiskIQ into ThreatConnect by selecting the Indicators from the vendor's **Detailed View** window on the **Enrichment** tab and then choosing to import them via the **As an Indicator** option in order to bring them in as direct associations to the parent Indicator.



Import and associate related Indicators to the Indicator under investigation

Improvements

Threat Intelligence

- A new Signature Group type was added: STIX Pattern.
- A new **CAL™ - Quad9 Observed Attempted Resolutions** section has been added to the **DNS Resolutions** card on the **Details** screen for Address and Host Indicators, showing location and count information for computers that attempted to access suspicious domains captured by Quad9® infrastructure within the last 90 days.
- Formatting improvements were made to the **Attributes** card on the new **Details** screen, with all fields expanded when you first navigate to the **Details** screen.

Intelligence Requirements

- When creating an IR or viewing an IR's **Details** screen, the **Excludes** section of the **Keyword Tracking** section now says "Excludes Any of the Following" instead of "Excludes All of the Following." As such, OR logic is now being used between keywords instead of AND logic in the "Excludes" part of the resulting query.

Playbooks

- A new **Intel Requirement** Trigger type for Playbooks was added, enabling you to Trigger Playbooks based on actions for IRs. In addition, UserAction Triggers now have an **Intel Requirement** type, enabling you to run Playbooks on demand from the **Details** screen for an IR.

System Settings

- The following new system settings were added:
    - **playbooksDbCredentialsEnabled**: This setting determines whether a username and password are required to interact with the Playbooks database on Redis®. If **playbooksDbUsername** and **playbooksDbPassword** both have values, ThreatConnect will use them to authenticate to the Playbooks Redis database.

  - **potentialAssociationMode**: This setting enables System Administrators to configure how potential associations are suggested on their ThreatConnect instance. The setting provides a dropdown with three options:
    - **Matched**: Potential associations will be based on matching Artifacts to Indicators on your ThreatConnect instance.
    - **Associated**: Potential associations will be based on second-degree associations to objects on your ThreatConnect instance.
    - **Both**: Potential associations will be based on matching Artifacts to Indicators on your ThreatConnect instance AND on second-degree associations to objects on your ThreatConnect instance.
  - **v3ApiTurboMode**: This setting activates a performance-improved algorithm for fetching large numbers of certain types of child objects (e.g., Attributes, Tags, associations, etc.) within the context of a v3 API request. You can enable this setting for threat intelligence only, Workflow only, or both.
  - **v3ApiTurboModeBatchSize**: This setting determines the number of unique child items fetched per batch within a turbo-enabled lookup.
  - **v3ApiTurboModeExemptionLimit**: This setting determines the maximum number of child items per batch for which turbo lookups will be performed. Turbo lookups for child items that exceed this limit will be skipped and performed separately. This setting may be disabled by setting its value to -1.
- The **Configuration / Organization** category has been removed from **System Settings → Info → System Health**.

Notifications

- Previously, the **Notifications Center** was displaying notifications regarding updates to the TC Exchange™ catalog for all users. Now, those notifications will be displayed only for System Administrators.

Search and Analyze

- In the **Search** drawer, strings containing one or more periods (**.**) or an at-sign (**@**) character will be treated as a single search term. As such, the search results will return only matches to the entire string.

Workflow

- The Workflow **Cases** screen now auto-refreshes to provide near-real-time updates made by other users in your Organization.

API & Under the Hood

- Performance upgrades for batching linked data were made to the v3 API.
- The `/v3/indicators/enrich` endpoint now supports enriching Indicators with data retrieved from RiskIQ.
- When using the `/v3/groups` endpoint, API users can assign the `fields` query parameter a value of `insights` to return AI insights for Report Groups in the CAL Automated Threat Library (ATL) Source.
- The `/v3/tags` endpoint has been updated to allow API users with an Organization role of Organization Administrator to assign security coverage to ATT&CK Tags.
- When creating a batch job with the V2 Batch API, you can now assign the `attributeWriteType` field a value of `Singleton` to have the batch job replace existing Attributes added to an Indicator or Group only if the incoming data include Attributes with the same Attribute Type(s) as the existing Attributes. Otherwise, existing Attributes added to an Indicator or Group will remain unchanged.

Bug Fixes

Dashboards

- An issue causing dates instead of Group types to be displayed on the *y*-axis of **Heat Map** cards in dashboards was resolved.

Threat Graph

- The styling of the **Selected** button and the **Selected Actions** menu in the Threat Graph **Details** drawer was improved to provide more intuitive functionality.

Intelligence Requirements

- Attributes, associations, Security Labels, and other data were not being displayed on the **Details** drawer for IR results. This issue has been corrected.

Playbooks

- An issue causing Playbooks configured to execute automatically upon creation of a Workflow Case to execute twice was fixed.

API & Under the Hood

- An issue causing duplicate Indicators to be included in the `customAssociations` object when retrieving an Indicator's custom associations with the v3 API was fixed.
- An issue causing a Group's Attributes and associations to be deleted when using the v3 API to associate a Victim Asset to the Group has been fixed.

Dependencies & Library Changes

For instances running ThreatConnect version 7.2.0 or later, it is recommended that signed certificates be used in place of self-signed certificates. This change is related to Python® 3.11 and Java® functionality, because some vendors of plugins used in Playbooks and other Apps that interact with ThreatConnect may have more stringent requirements for security measures.

Maintenance Releases Changelog

2024-02-07 7.4.1 [Latest]

Improvements

- Two new configuration options were added to the **Data** tab of the **Contribute to Community/Source** window:
    - **Limit Depth**: Selecting the **Yes** option enables you to set a limit for the number of association levels copied during the contribute operation.
    - **Max Depth**: Enter the maximum number of association levels to be copied during the contribute operation. An entry of **1** indicates that only the primary Group and Groups directly associated to it will be contributed.
- A new system setting, **userMaxSessions**, was added. This setting, which has a default value of **2**, determines how many simultaneous browser sessions a user may have at one time. This setting resolves an issue that was causing out-of-memory errors due to multiple user sessions being created and remaining active when users close and re-open browsers running ThreatConnect.
- Trace logging was added to the search cluster health check.
- On instances with a proxy configured in the system settings, Playbook App logs using the TRACE log level were exposing user credentials. These credentials will now be obfuscated.

Bug Fixes

- API users with an Organization role of Organization Administrator were able to use the v3 API to create users with a System role of Operations Administrator. This issue was corrected.
- An issue causing an error to occur when clicking in the **Name** column for an IR category in **System Settings > Categories** was resolved.
- An issue causing an error when opening a new tab with the **Details** screen for an object whose owner has parentheses in its name was fixed.
- An issue causing mismatched file hashes uploaded via batch import to have incorrect **CommonIndicator** records was fixed. All affected data have been repaired.

- When editing an IR, selecting the **Reset All Archived and False Results** checkbox was causing the IR's results list, including all associated results, to reset. This issue has been fixed.
- When creating or editing a user through the **/v3/security/users** endpoint, the **logoutIntervalMinutes** field's value will default to 30 if you do not provide a value for this field in the body of your POST or PUT request.
- An issue causing unstructured Indicator imports to fail when a URL in the data set contains commas has been fixed.
- Adding an association between a Group and an IR and then contributing the Group to a Community or Source was resulting in corrupt data showing up in the data logs and preventing the IR from being re-created after being deleted if the contributed copy still exists. This issue has been resolved.
- An issue causing an error to occur when downloading published Groups was fixed.
- When uploading a new Attribute Type into ThreatConnect, Validation Rule updates included in the JSON file for the Attribute Type were being ignored unless at least one Attribute Type using the Validation Rule was also updated. This issue has been corrected.
- An issue causing an error to occur on the ContentPackService component when starting up the **tc-mon** server was resolved.
- An issue causing SAML-enabled ThreatConnect instances to redirect to favicon.ico upon first login has been resolved.