ThreatConnect® Release Notes

Software Version 7.12

January 15, 2026

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

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

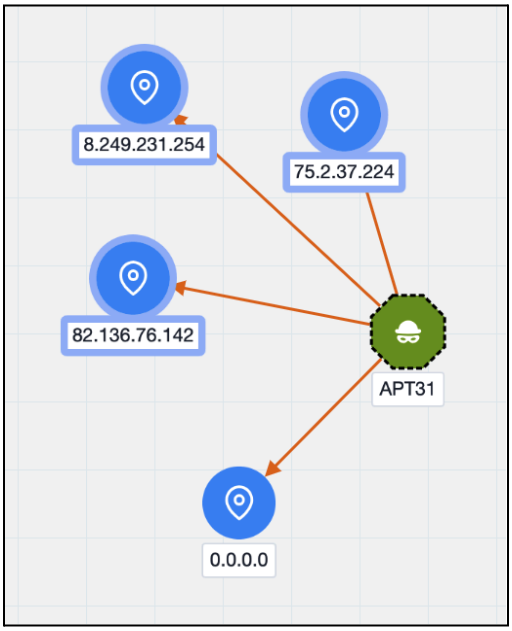
Table of Contents

New Features and Functionality

Threat Graph: Bulk Pivots and Enrichment

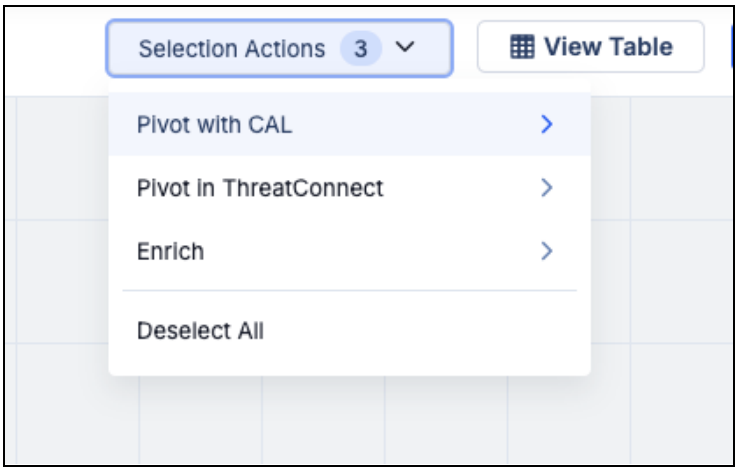
In version 7.12 of ThreatConnect, you can now **select multiple nodes in Threat Graph and pivot on or enrich those nodes in a single operation**. Being able to quickly expand your visible dataset allows you to spend more time evaluating the related information—which can include associated objects in your ThreatConnect owners, relationships that exist in CAL™, and data from supported third-party enrichment services—and less time clicking.

To select multiple nodes, hold down the **Shift** or **Command** key on your keyboard and click on each node you want to select.



Selected nodes in Threat Graph are highlighted

After selecting a set of nodes, choose an option from the **Selection Actions** dropdown at the upper right of the graph.



*The **Selection Actions** menu provides available pivot and enrichment options*

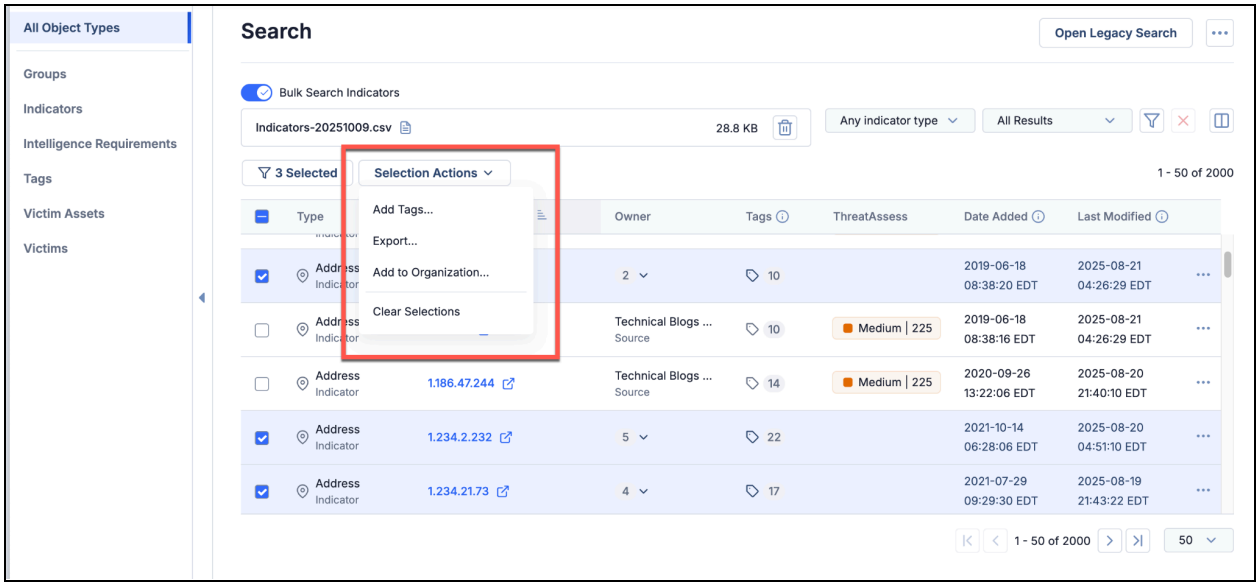
Only options that apply to at least one of the selected nodes will be provided in the **Selection Actions** menu. Available relationship types and enrichment options will vary between objects, and not all pivot and enrichment options will yield results. The results that are displayed after running a pivot or enrichment operation depend on the available data in your ThreatConnect owners, data present in CAL, or data provided by a third-party enrichment service.

Bulk Indicator Search: Bulk Actions on Consolidated Indicators

As you examine and investigate Indicators in a bulk Indicator search of an uploaded file, you can now select consolidated rows of deduplicated Indicators and **take any of the following bulk actions** available in the **Selection Actions** dropdown on those Indicators:

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

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



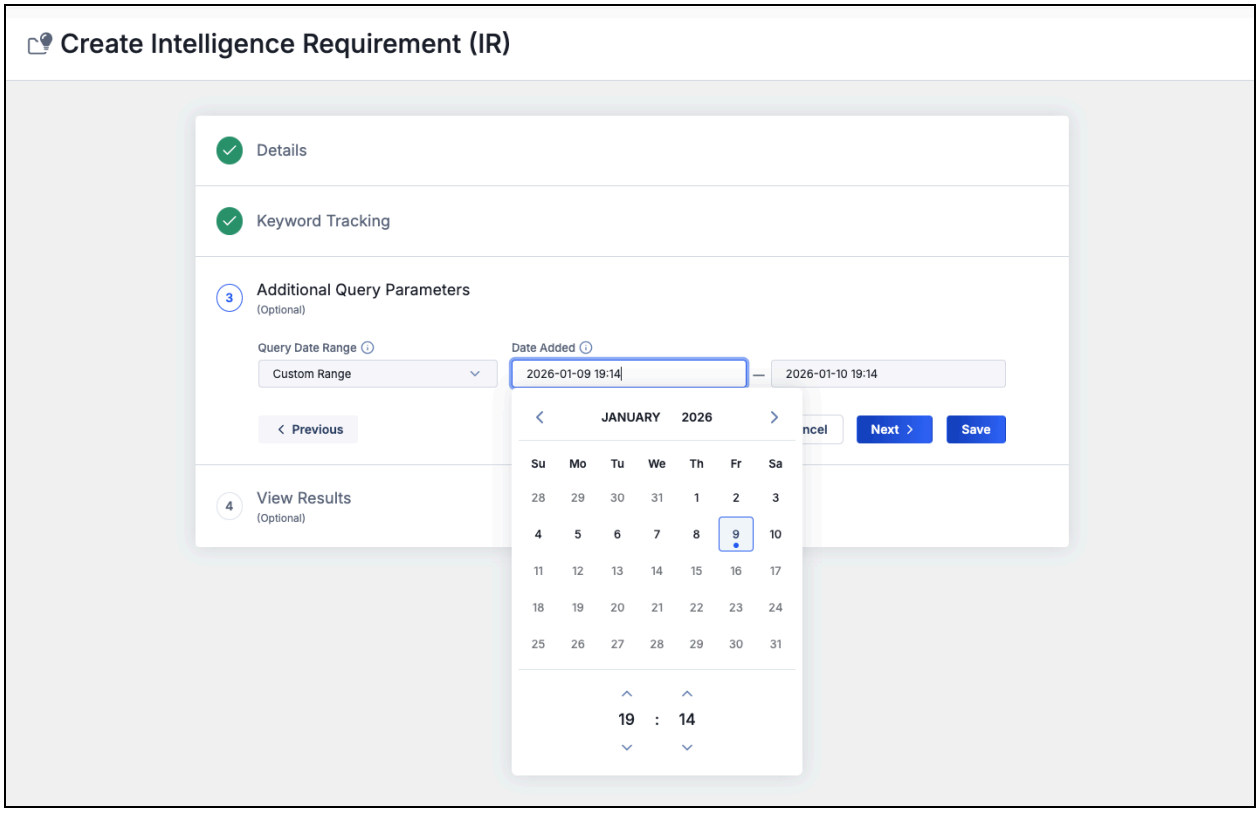
Take bulk actions on deduplicated Indicators in your ThreatConnect owners identified in an uploaded file

Intelligence Requirements: Query Date Range

It is best practice for threat intelligence teams to review their intelligence and collection requirements on a regular interval to ensure they are focused on the intelligence that is most valuable to their organization. To help you more effectively follow this best practice while using the ThreatConnect Intelligence Requirements (IR) feature, the 7.12 release lets you **configure your IR keyword queries to return only information added to ThreatConnect within a defined time frame**. By specifying that only results with **Date Added** or **External Date Added** values within your defined query date range should be returned, you reduce the likelihood that historical data matching an IR will surface in your IR results list.

Define Query Date Range

You can define a query date range for an IR in the new **Additional Query Parameters** step when creating a new IR or in the new **Additional Query Parameters** card on an existing IR's **Details** screen. For new IRs, you can define a custom range or select from four pre-configured ranges (**Today**, **Next 7 Days**, **Next 30 Days**, or **Next 60 Days**). For existing IRs, you can define a custom range, including time specified to the minute.



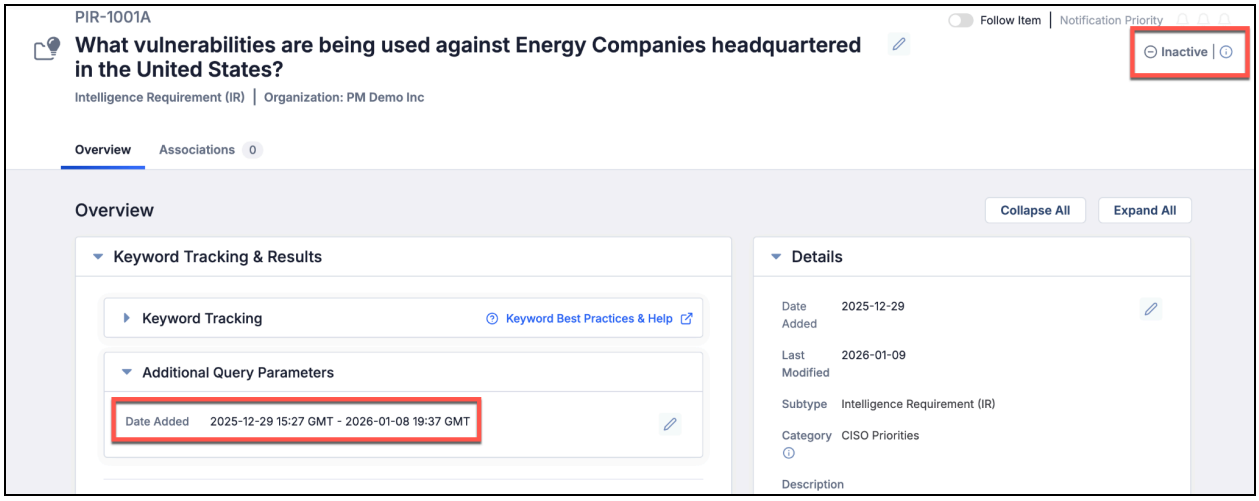
Define a query date range when creating a new IR

Query date ranges are optional. In addition, existing Intelligence Requirements will not have date ranges applied unless you choose to add those parameters on the IR's **Details** screen.

If you leave the start or end date empty when configuring a query date range, the monitor that powers the IR will return data based on the single defined parameter. For example, if you set only a start date for **Date Added**, then the monitor will return results matching the query that have a **Date Added** or **External Date Added** value after the defined start date. If you set only an end date for **Date Added**, then the monitor will return results matching the query between the time the ThreatConnect instance was set up through the defined end date.

IR Status

IRs now have a status, which is displayed at the upper right of their **Details** screen. If the current date and time are before the end date of the IR's query date range, the IR's status is set to **active**, indicating that it is currently retrieving results or will retrieve results after its start date is reached. Once the end date for an IR's query date range is reached, the IR's status is set to **inactive**, indicating that it is no longer retrieving results.



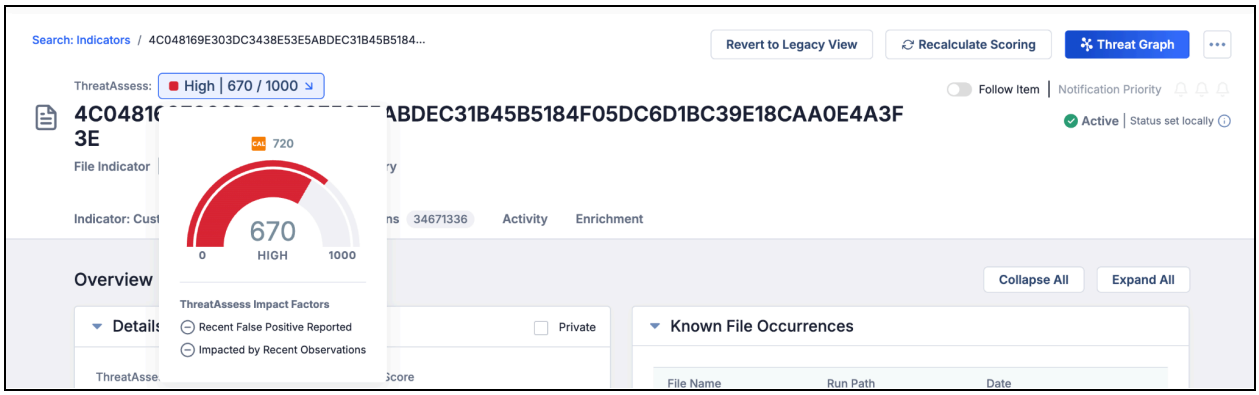
*IRs are set to inactive once the current date and time match the end of the **Date Added** range (i.e., the query date range)*

If you want to activate an inactive IR, you can remove the **Date Added** range in the **Additional Query Parameters** card on the IR's **Details** screen. Alternatively, to set an IR to active and retrieve results added to ThreatConnect between the time the IR was set to inactive and the current time, simply update the end date of the range to a future date and time that includes the time period when the IR was inactive.

Indicator Score Displays

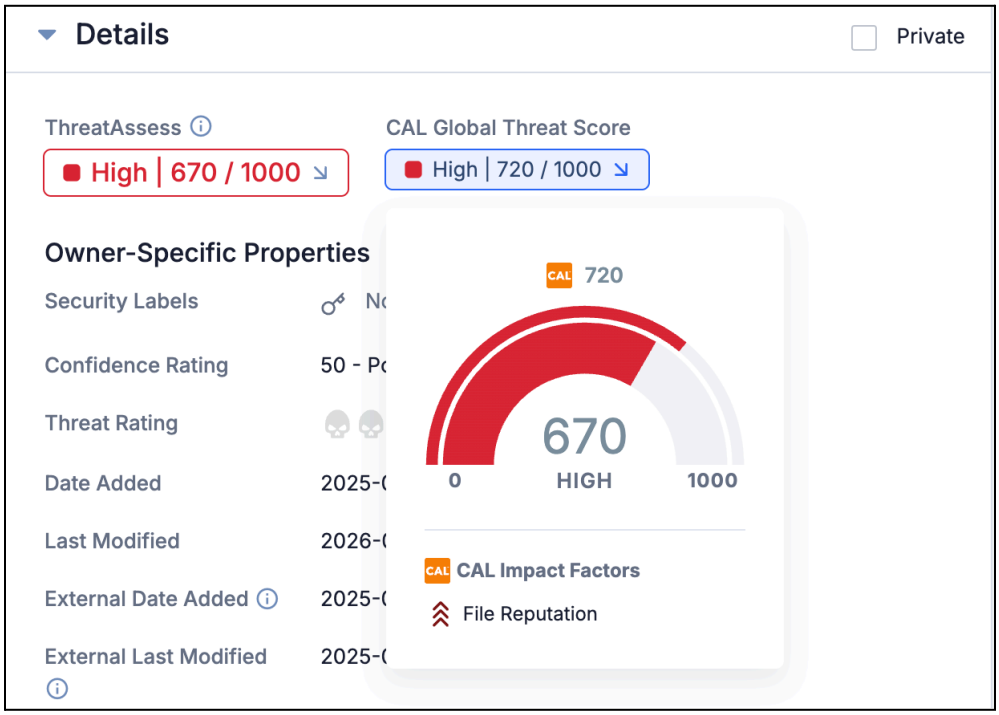
The past several ThreatConnect releases have included a variety of UI updates intended to highlight contextual data to help you get to action faster. Similarly, the 7.12 release includes one small, but impactful, **change to how and where Indicator scores are displayed** in ThreatConnect.

You can now see an Indicator's ThreatAssess score at the upper left of the Indicator's **Details** screen. If you click the ThreatAssess score, you can see the ThreatAssess impact factors contributing to the score, as well as the Indicator's CAL score (now called the **CAL Global Threat Score**) at the top of the scoring graphic.



*View an Indicator's ThreatAssess score at the top of its **Details** screen*

Both scores are still available on the **Details** card. If you click a score, you can see the impact factors contributing to it.



*View an Indicator's ThreatAssess and CAL Global Threat Score and the contributing impact factors on the **Details** card*

This update was driven by customer feedback about making better use of space on the Indicator **Details** screen. Please continue to share feedback with us via your Customer Success Representative or our Customer Feedback Portal.

Improvements

Threat Intelligence

- AI insights containing Live Brief and Intel Agent data from Dataminr Pulse Alerts are now available for Event Groups imported into ThreatConnect from version 2.0.*x* of the **Dataminr Pulse Alerts Engine** App:
    - AI insights from Dataminr Pulse Alerts display on the **Details** screen for relevant Events in Sources to which a feed for version 2.0.*x* of the **Dataminr Pulse Alerts Engine** App is deployed.
    - When retrieving Event Groups with the v3 API, if you assign the `fields` query parameter a value of `insights` in the API request, the API response will return the AI summary in the `insights` field and the AI provider (Dataminr) in the `aiProvider` field.
    - You can use the following TQL parameters to filter Event Groups imported from the **Dataminr Pulse Alerts Engine** App by their AI insights:
        - `insights`: Filters Events Groups based on the contents of their AI insights.
        - `aiProvider`: Filters Event Groups based on the provider of their AI insights.
- TQL now supports the `hasThreatActorProfile()` nested query parameter for filtering on data in Threat Actor Profiles. You can use the following parameters in nested queries for Threat Actor Profiles: `deprecated`, `mitre_id`, `mitre_link`, `externalDateAdded`, and `externalLastModified`.
- Threat Actor Profiles and the unified view for Vulnerability Groups are now available in the **Details** drawer.
- The layout of the **Details** card on an Indicator's **Details** screen now adjusts dynamically based on the card width in order to optimize the available space.

Dashboards

- You can now query by Intelligence Requirements on dashboard Query cards.
- You can now configure Indicator Metric cards for Email Subject and Hashtag Indicator types by selecting **Email Subject** or **Hashtag**, respectively, from the **Metric Types** dropdown.

Threat Graph

- The following improvements were made to the undo/redo feature:
    - You can now apply the **Undo** and **Redo** buttons in Threat Graph to layout changes, including selection of layout options (Cola, CoSE-Bilkent, etc.) and manual movement of nodes (individual or multiselected) around a graph.
    - The limit on the number of actions you can undo or redo has been raised from 10 to 50.

Reporting

- When saving a new report template in the Reporting feature, the character limit for the template's **Name** field is now 500.
- The **Group Associations** and **Indicator Associations** tables in reports now include hyperlinks on the object names in the **Name** column, providing quick access to each object's **Details** screen in ThreatConnect.
- When creating a custom report from a Group template, you can now select whether to open the report in a new tab or the current tab.

ATT&CK

- The ATT&CK Tag **Approximate Match** conversion rule now converts formats supported by CrowdStrike® in addition to the previously supported formats for MITRE ATT&CK®.

Permissions

- Only users with a System role of Administrator, Operations Administrator, or Super User or an Organization role of Organization Administrator can edit their own logout interval on the **My Account** screen. This permission setting was updated for enhanced security and administrative control.

Apps & Services

- The **Automation & Feeds** dropdown on the top navigation bar now has a **Jobs** option that provides quick access to the **Jobs** screen, which provides the functionality

previously located on the **Apps** tab of the **Organization Settings** screen, including management of Job Apps and generation of App Delivery Tokens and API Developer Tokens.

- On the **Services** screen, the **Details** drawer for a Feed API Service now has an **Organization** field that displays the Organization that owns the Source to which that Feed API Service is deployed. You can use this information to differentiate between Feed API Services deployed for the same App, particularly to ensure that you are viewing or editing the expected Service.
- When updating Apps with custom Attribute Types, you no longer need to upload JavaScript® Object Notation (JSON) files containing the updated Attribute Types. Instead, the Attribute Types will be updated automatically on the System level when you upgrade the App on the **TC Exchange™ Settings** screen.

System Settings

- The **aiSummaryEnabled** system setting has been updated to function as follows:
  - If the **aiSummaryEnabled** checkbox is selected, AI insights will automatically be provided by participating feeds to relevant Group objects, and you will be able to generate AI summaries for relevant Group objects on the **AI insights** card on the **Details** screen.
  - If the **aiSummaryEnabled** checkbox is cleared, AI insights will automatically be provided by participating feeds to relevant Group objects, but you will not be able to generate AI summaries on the Group **Details** screen.

API & Under the Hood

- The following endpoints have been added to the v3 API:
  - `/v3/posts`: Allows you to create, retrieve, and delete posts (Notes).
  - `/v3/posts/reply`: Allows you to create and delete post (Note) replies.
- When using the `/v3/intelRequirements` v3 API endpoint to create or update IRs, you can now configure the following fields:
  - `earliestTimestamp`: The start date in an IR query date range.
  - `latestTimestamp`: The end date in an IR query date range.
- When using the V2 Batch API to create or update Event Groups, you can now assign values to the following fields:

    - `insights`: *<String>* An AI-generated summary of the Event that displays on the **AI insights** card on the Event's **Details** screen.
    - `aiProvider`: *<String>* The source of the AI-generated summary provided for the Event. If a value is assigned to `insights`, you must assign a value to this field.
- Security improvements were made to session timeout protocol. When a user logs out of their ThreatConnect instance, they are now immediately redirected to the login page.

Bug Fixes

Dashboards

- Dashboard cards and other areas of that platform querying for Cases by Group association were not returning Cases with associated Groups in Communities and Sources. This issue was fixed.

Threat Intelligence

- An issue preventing the display of AI insights for Reports in the **CAL Automated Threat Library** Source was resolved.
- An issue causing an error to occur in ThreatAssess when analyzing an Indicator that exists only in an owner with a **Credibility/Weight** of **0** was fixed.
- An issue causing performance lags when loading areas of the **Details** screen for Groups was fixed.

Apps & Services

- An issue preventing Job Apps from being configured for Environment Servers on certain ThreatConnect instances was resolved.

Playbooks

- Playbooks with caching enabled in their Trigger were not capturing cache metrics. This issue was corrected.

API & Under the Hood

- An issue preventing Attributes created via the v3 API from being returned by v3 API GET requests was fixed.
- When sending a PUT request to the v3 API to update an Indicator, if you used the Indicator's summary to identify it, there was a possibility that the request would update copies of the Indicator in owners other than the intended one or that the operation would result in an error. This issue has been corrected.

Dependencies & Library Changes

- There are no new dependencies or library changes for ThreatConnect version 7.12.0.

Maintenance Releases Changelog

2026-01-22 7.12.0-0122R [Latest]

Improvements

- Performance improvements were made for GET requests to the v3 API for Security Labels attached to Indicators, Indicator Attributes, Groups, and Group Attributes.