ThreatConnect® Release Notes

Software Version 7.1

April 12, 2023

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

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

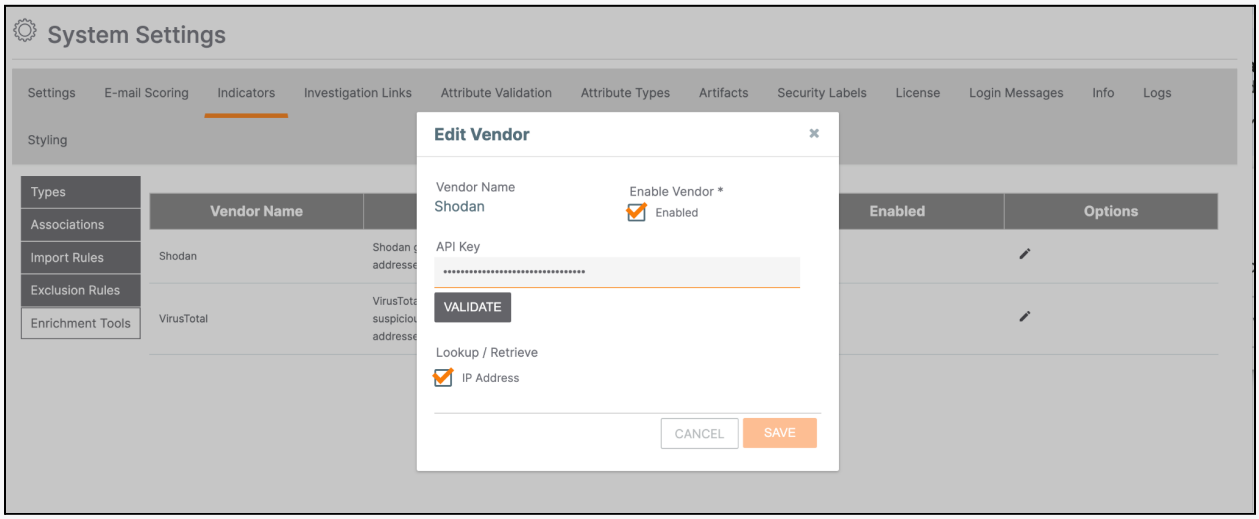
Table of Contents

New Features and Functionality

Built-In Enrichment: Shodan

In version 7.0 of ThreatConnect, we introduced built-in enrichment with VirusTotal™, allowing users to obtain consolidated views of enrichment on IOCs without the need for Playbooks or manual searches on additional websites.[1] In ThreatConnect 7.1, we are excited to announce the addition of built-in enrichment with Shodan®.[2] This powerful search engine provides detailed information about vulnerabilities and enriches IP addresses with actionable intelligence for threat investigations and other security operations. With this new feature, users can remove false positives and obtain a more complete picture of their investigations, making ThreatConnect 7.1 an even more powerful tool for threat intelligence.

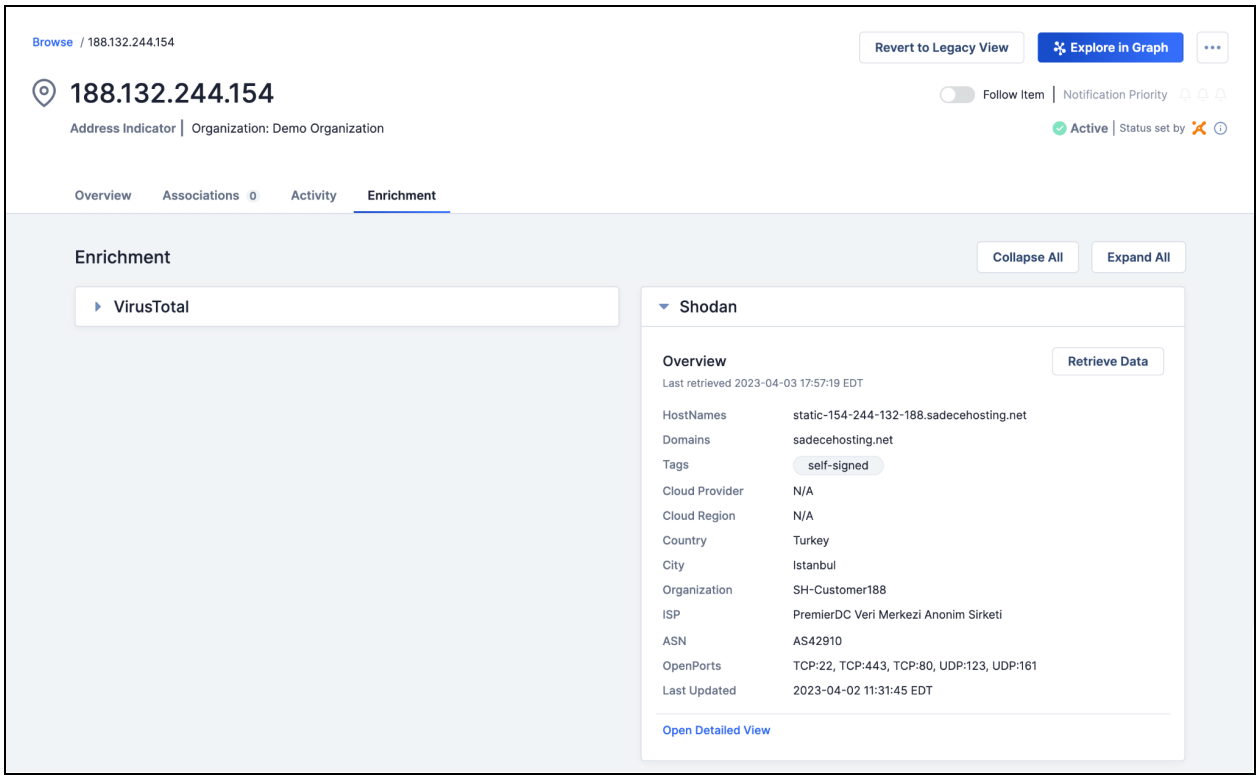
System Administrators can enable built-in enrichment by adding their Shodan API key to the **Enrichment Tools** section of the **Indicators** tab of **System Settings** and then selecting the **IP Address** Indicator type.



*Configure Shodan enrichment in **System Settings***

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

[1] VirusTotal™ is a trademark of Google, Inc.
[2] Shodan® is a registered trademark of Shodan.



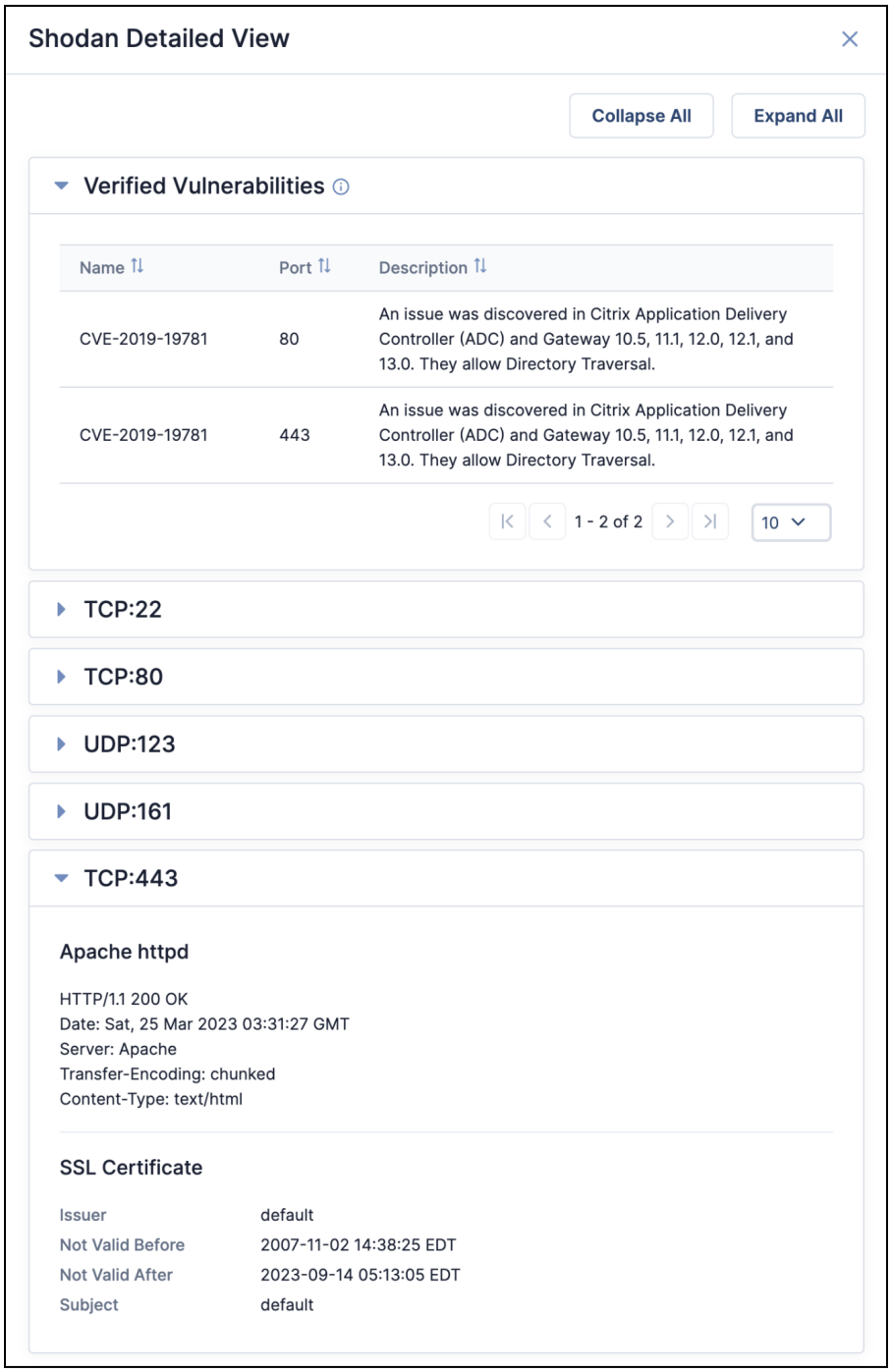
*Shodan data are provided on the **Enrichment** tab of an Indicator's **Details** screen*

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

To take a deeper dive into the information Shodan knows about an Indicator, click the **Open Detailed View** link at the bottom of the **Shodan** card to open the **Shodan Detailed View** drawer, which offers comprehensive information about IP addresses for your research requirements. The following details are included:

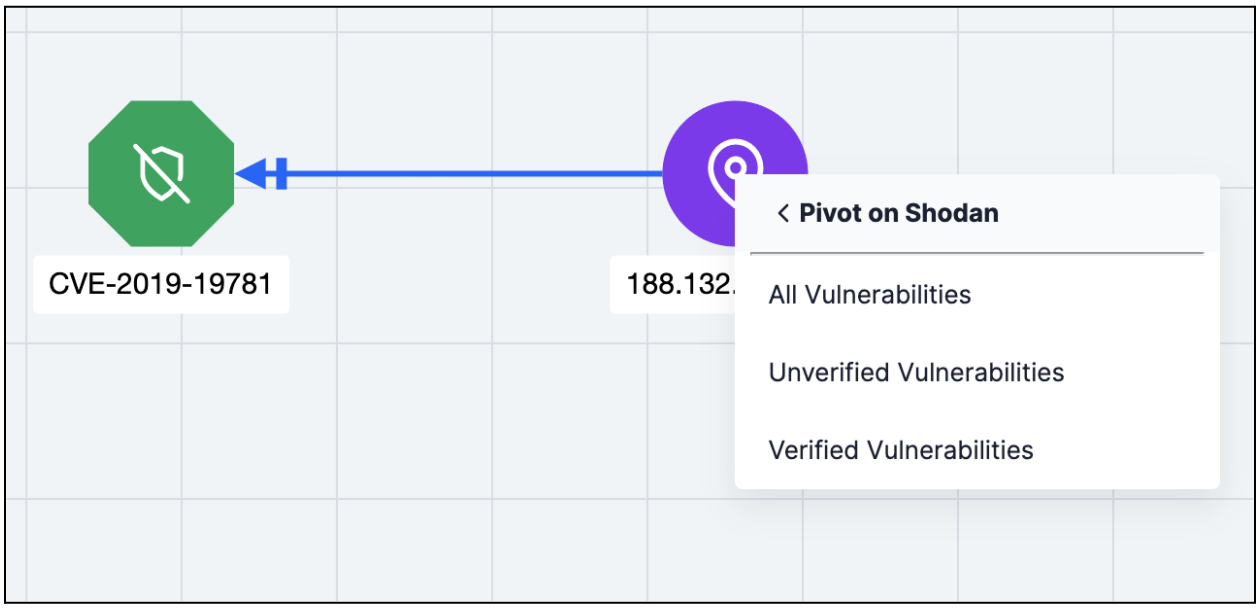
- **Ports, Protocols, and Associated Certificates**: The **Shodan Detailed View** displays information on all open ports and their corresponding protocols, allowing you to delve deeper into the target infrastructure. Additionally, the view contains certificate details for SSL/TLS-enabled services. This kind of data is invaluable for detecting misconfigurations, expired certificates, or weak cryptographic algorithms that could present potential security risks.

- **Verified and Unverified Vulnerabilities**: The **Shodan Detailed View** showcases both verified and unverified vulnerabilities. This feature aids security researchers in identifying potential threats and adopting appropriate measures to reduce risks.



*The **Shodan Detailed View** provides detailed enrichment information for Address Indicators*

These relationships can also be visualized in Threat Graph.

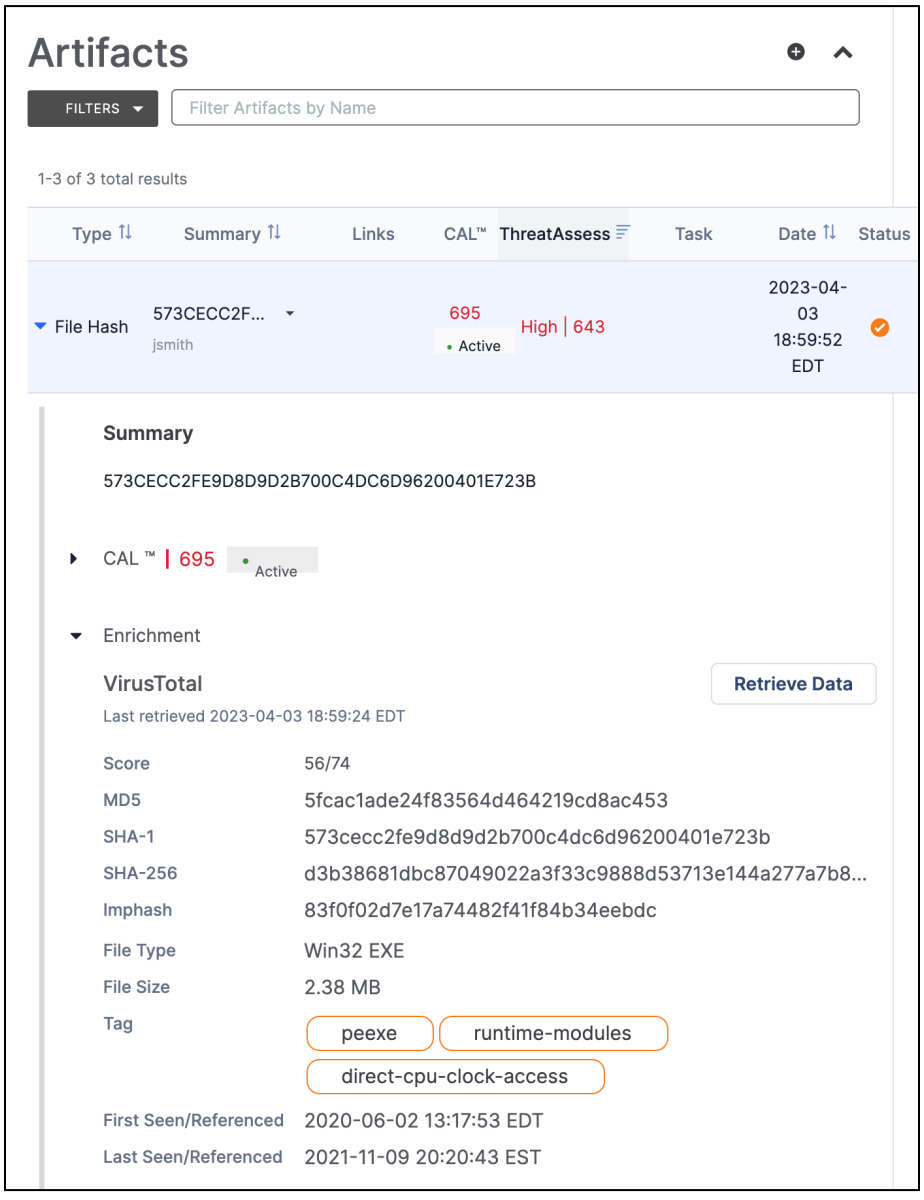


Pivoting on Shodan enrichment data in Threat Graph gives you insight into an Indicator's vulnerabilities

We have also made the Shodan enrichment data points available in the UI accessible via the v3 API. In addition, you can take advantage of a new v3 API endpoint to enrich Indicators with Shodan automatically. This feature eliminates the need to navigate to the **Enrichment** tab in the UI, making the enrichment process more efficient and streamlined.

Built-In Enrichment: VirusTotal Enhancements

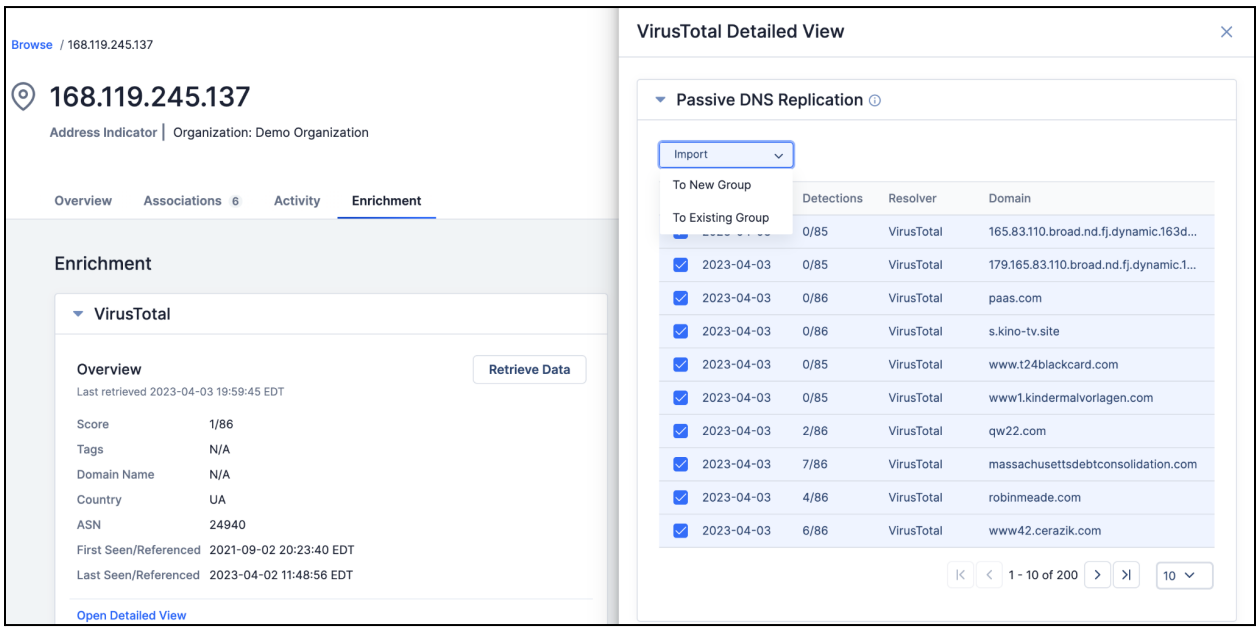
In ThreatConnect 7.1, you can take advantage of built-in enrichment with VirusTotal in Workflow Cases. This enhancement enables you to obtain a detailed overview of what VirusTotal knows about your Address, File, Host, and URL Artifacts.



VirusTotal enrichment is provided for Artifacts in a Workflow Case

You can also use a new v3 API endpoint to enrich Indicators with VirusTotal automatically. This feature eliminates the need to navigate to the **Enrichment** tab in the UI, making the enrichment process more efficient and streamlined.

In addition, you now can import VirusTotal relationship information into ThreatConnect by selecting Indicators from the **VirusTotal Detailed View** on the **Enrichment** tab and then selecting whether to associate them to a new or existing Group upon import. This functionality provides a deeper understanding of the relationships between Indicators and allows you to quickly import suspicious Indicators into ThreatConnect for further investigation.



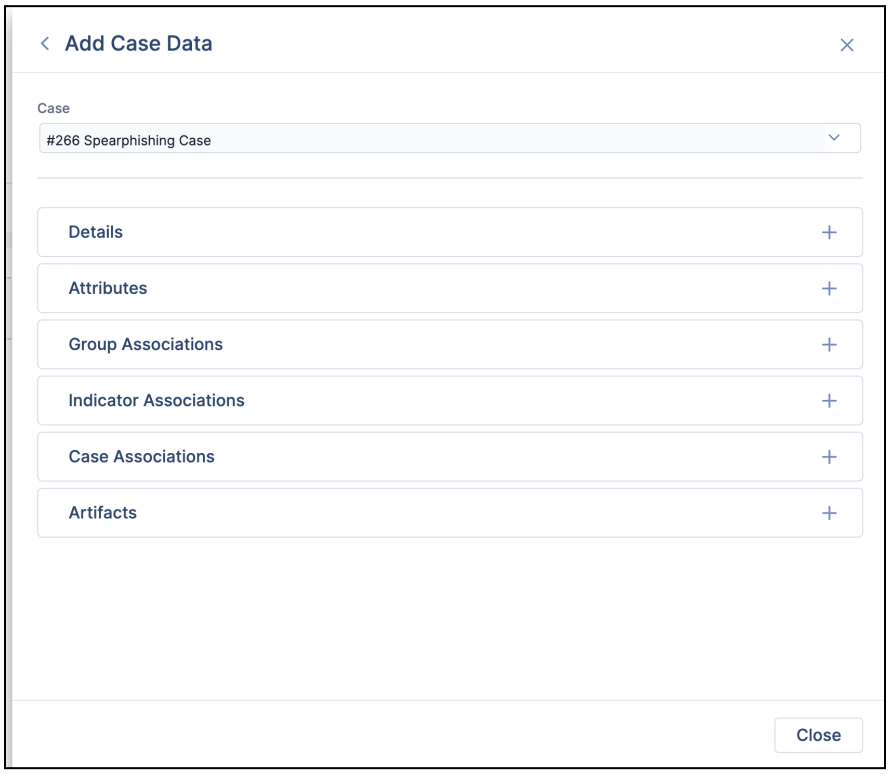
Import VirusTotal relationship Indicators into ThreatConnect

Reporting Version 2

Our second iteration of reporting includes several new features designed to give you greater flexibility in how you organize and analyze your data. In ThreatConnect 7.1, you can now add information about Workflow Cases into your reports. You can even include information about multiple Cases and multiple Groups in the same report. Finally, we have made the process of creating reports more intuitive and user friendly by adding the ability to create reports directly from the **Reporting** screen.

Case Reports

You can now create reports directly from a Workflow Case and add Case-related information such as Case Details; Attributes; Artifacts; and Indicator, Group, and Case Associations into your reports.You can build custom charts using saved ThreatConnect Query Language (TQL) queries or TQL queries you build on the fly to add to your report. Metrics charts, including system metrics, user metrics, Case metrics, and Playbook metrics, are also available.

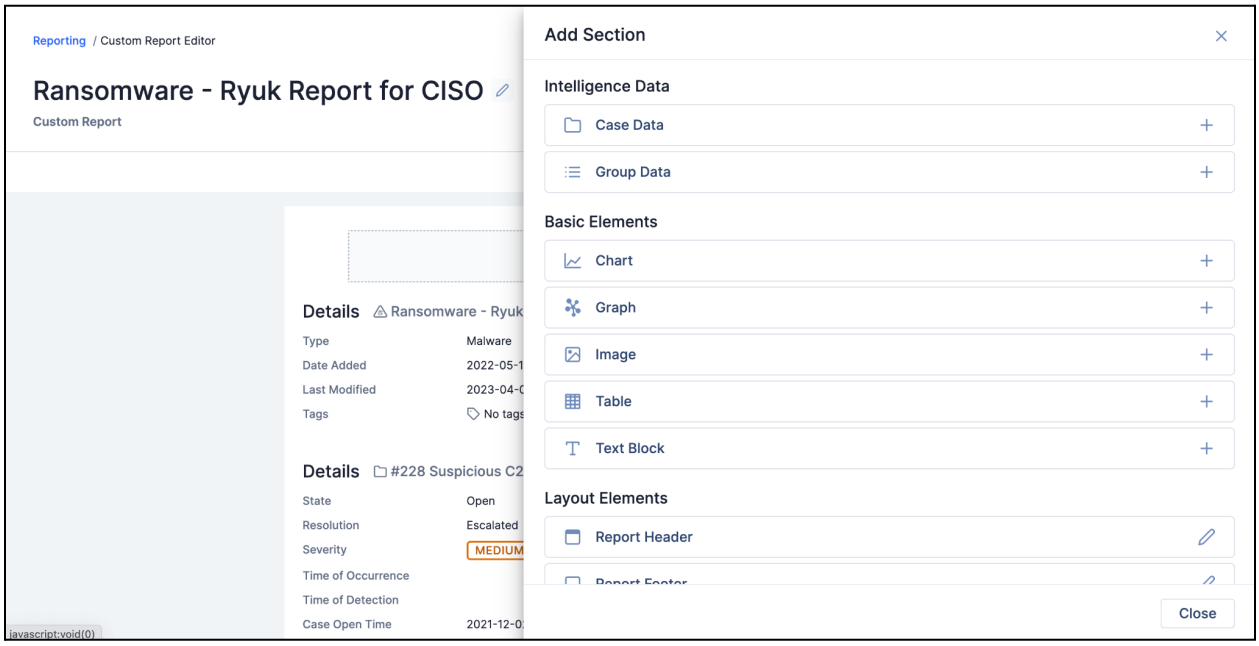


Generate reports with information about Workflow Cases

Multi-Group and Multi-Case Reports

With ThreatConnect 7.1, our reporting functionality has been updated to include support for adding information from multiple Cases and Groups to a single report. This new feature will enable you to streamline your investigations and organize your data more efficiently than ever before.

Furthermore, the ability to add information from multiple Cases and Groups enables you to generate more comprehensive reports. By incorporating data from multiple Groups and Cases into a single report, you can provide a more complete picture of your findings, which can help to inform decision making and drive business outcomes.

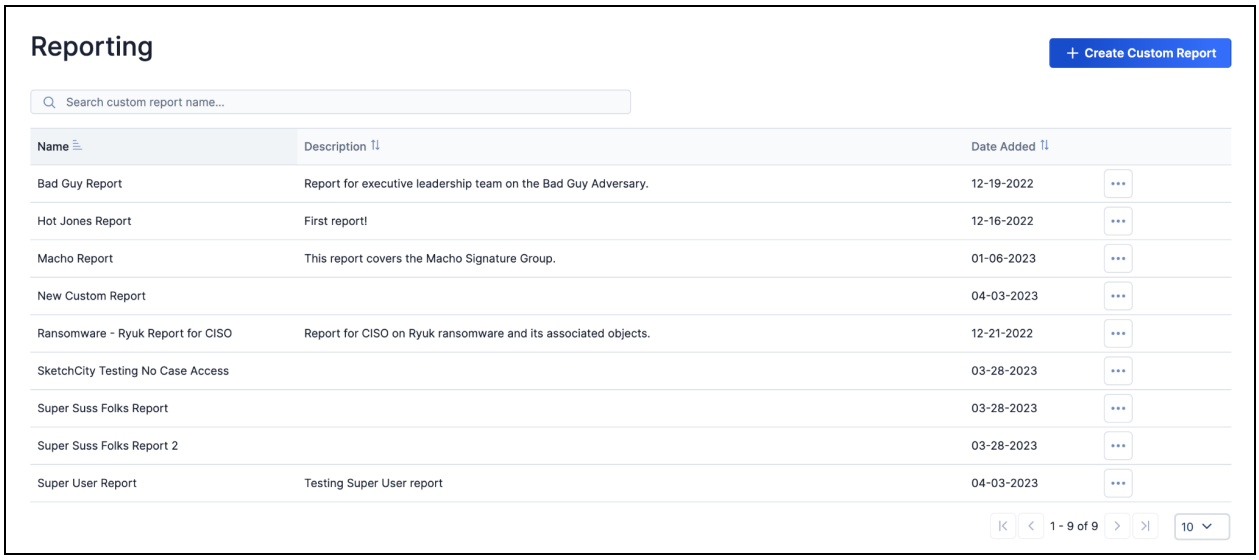


Generate reports with multiple Cases and Groups

Create Reports from the Reporting Screen

In ThreatConnect 7.1, you have the ability to create generic reports about any investigation without specifically involving any particular Case or Group. This new feature allows you to generate generic reports on any investigation quickly and easily, without the need to create and manage a Case or Group.

With the ability to create generic reports, you can now easily analyze and report on data from any investigation, regardless of whether it is associated with a particular Case or Group. This new capability will give you greater flexibility and control over your reporting workflows.



*Generate generic reports from the **Reporting** screen*

Details Screen Updates

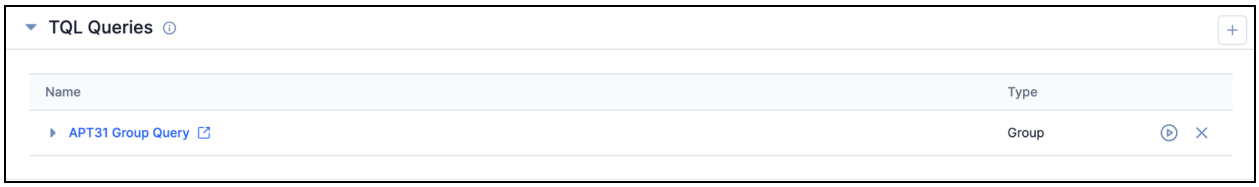
In ThreatConnect 7.0, we released the first version of our updated **Details** screen. The goal of this new view is to streamline one of the main areas of the platform and make it easier for users to sift through Attributes to find what they were looking for and make decisions faster. In ThreatConnect 7.1, we are continuing with that effort by adding a couple of key new features to the new view of the **Details** screen: **TQL Auto Associate** and **Pinned Association Attributes**.

TQL Auto Associate

TQL Auto Associate enables you to assign up to two TQL queries to a Group—for example, one query that looks for Indicators and one query that looks for Groups. When these queries are run, they create associations between the Group and objects returned by the queries that are not associated to the Group.

*Select a Group Query or Indicator Query on the **TQL Queries** card on the **Associations** tab of the **Details** screen*

Once you select or create a query to use for associations, you will have the option to run the query on demand or allow it to run automatically on a schedule, typically every night, depending on how your System Administrator has configured the feature. When the query runs, any new items in your Organization (if you do not have cross-owner associations turned on) and your Communities and Sources (if you do have cross-owner associations turned on) will be automatically associated with the Group to which you assigned the query.



*The **Play** button on the right can be used to run the query on demand*

This feature can be used to build a Threat Library or a Threat Actor Profile more efficiently. It can also be used to populate any new information related to a Campaign or other object that you are actively working on. As mentioned previously, the monitor runs nightly, so that when you log in each day, you have a full set of new information to work with, and you don't have to dig through everything you have to find that information.

Pinned Association Attributes

Another update we made on the **Details** screen in ThreatConnect 7.1 is the addition of the **Pinned Association Attributes** card on the **Overview** tab. Previously, to view Attributes of Groups associated to the object whose **Details** screen you are viewing, you had to navigate to the **Associations** tab, find the associated object you wanted to access, and then click on that object and view its **Details** screen.

With this release, you can have an Organization Administrator configure specific Attributes as Association Attributes, which will allow these Attributes to be displayed on the **Overview** tab of the **Details** screen for all Group objects of a specific type that are associated to the object.

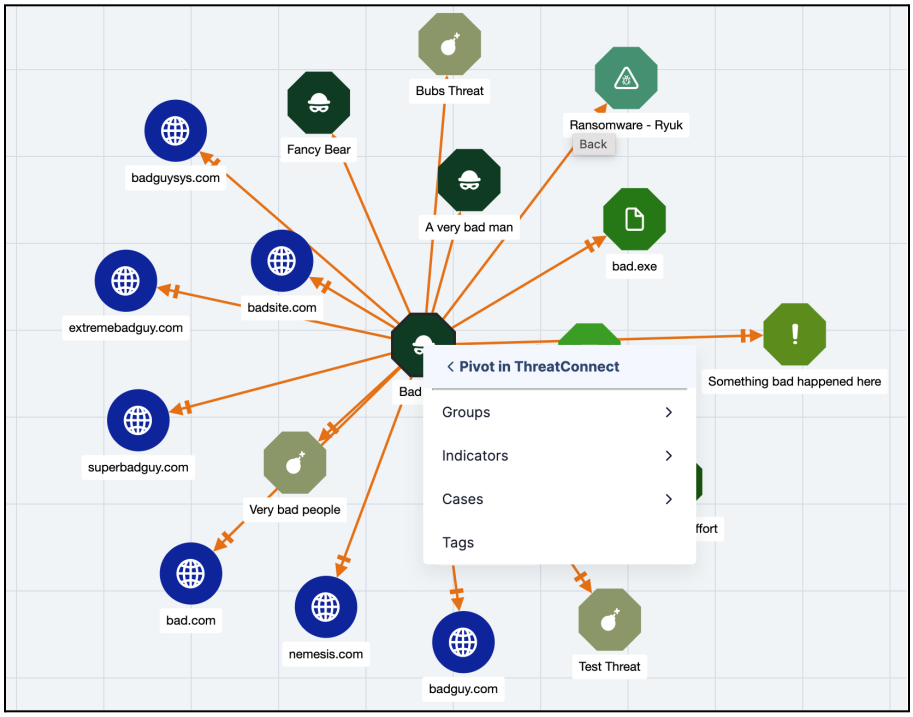
For example, if you are investigating an Email Address that is associated with an Intrusion Set in your Organization, you will be able to see the Description Attribute for the Intrusion Set right on the **Overview** tab of the **Details** screen for the Email Address without having to access the Intrusion Set's **Details** screen (provided that your Organization Administrator has configured the Description Attribute for Intrusion Sets as an Associated Attribute). This new functionality will enable you to get context on associated objects directly from an object's **Details** screen without having to click through associations individually.

Threat Graph Improvements

Over the past year and a half, we have been incrementally updating our Threat Graph feature to add functionality and new features that can be leveraged to do link analysis and allow you to pivot within your ThreatConnect dataset to find new, actionable information. In ThreatConnect 7.1, we have added two exciting new enhancements to Threat Graph: pivoting on Tags and the ability to run Playbooks on Indicators.

Tags in Threat Graph

In this version of ThreatConnect, you will now be able to pivot on Tags in Threat Graph. This functionality was previously available only in the associations graph on the legacy **Details** screen. With this new capability, you can now pivot from a Tag to see what is known about the Tag, and you can pivot to Tags (i.e., you can select a node and ask ThreatConnect to tell you what Tags are applied to that object). This functionality is especially useful because Tags can exist across owners and across objects in your Organization and on your instance, and many ThreatConnect users leverage Tags for key processes related to MITRE ATT&CK® and managing intelligence requirements, among others.[3]

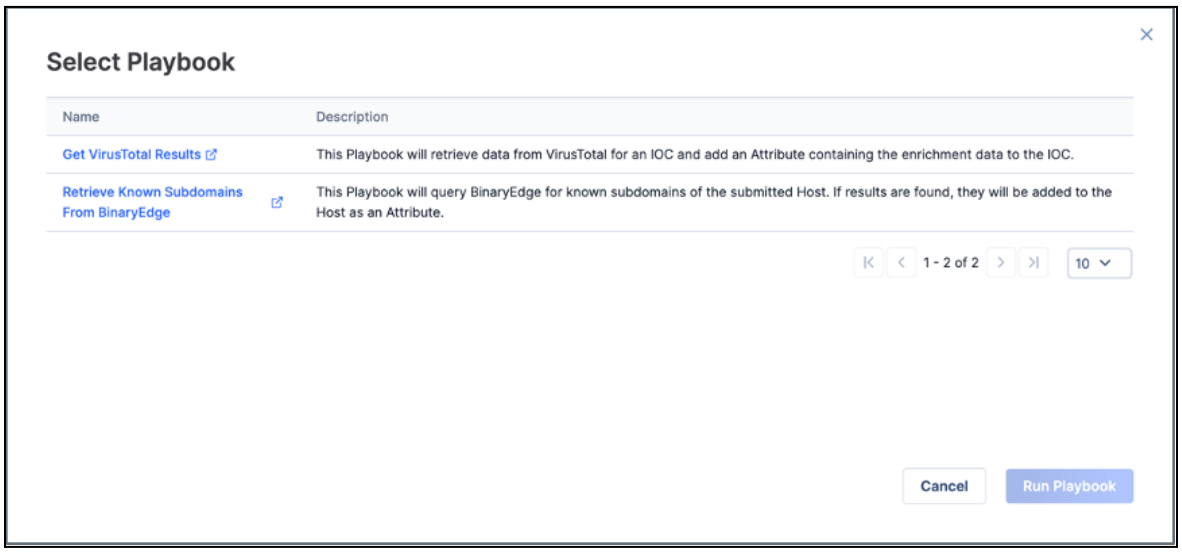


You can now pivot on Tags in Threat Graph

[3] MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.

Run Playbooks on Indicators from Threat Graph

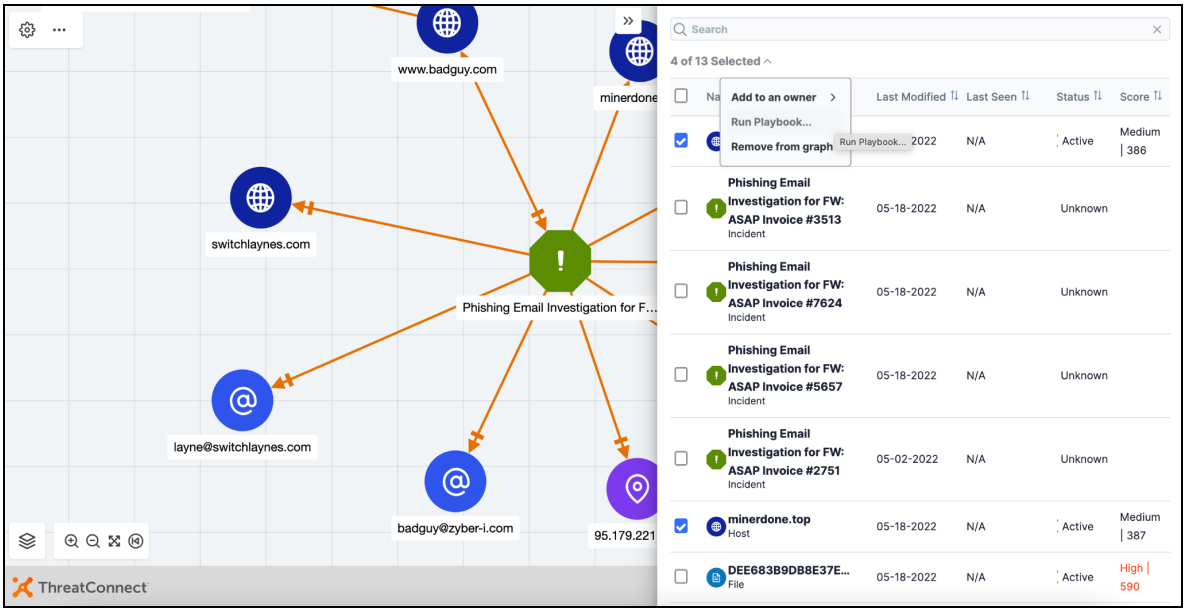
The ability to run Playbooks from Threat Graph is one of the most requested features we've discussed with customers since we began the process of revamping Threat Graph. In ThreatConnect version 7.1, the first version of this functionality is finally available. While using Threat Graph, you can now leverage the same UserAction Trigger Playbooks that you run on the **Details** screen. All you need to do is click on an Indicator node in the Graph and select the **Run Playbook…** option from the menu. You will then see the **Select Playbook** window.



Select a Playbook to run from the Threat Graph

Select a Playbook to run by clicking on its **Description**, and then click the **Run Playbook** button.

In addition to running Playbooks on individual Indicators, you can select multiple Indicators from the **Details** table in Threat Graph and run a UserAction Playbook on all of those Indicators at once, eliminating the need to visit the **Details** screen for each Indicator individually and run the Playbook. This functionality allows you to run Playbooks on multiple Indicators with fewer clicks and fewer page loads.



*Run a Playbook on multiple Indicators with fewer clicks from the **Details** table in Threat Graph*

Improvements

Dashboards

- When creating a dashboard query card with a **Datatable** display type that is querying by Cases, you now have more column options to select from, including **Case ID**, **Assignee**, **Status**, **ThreatAssess**, **CAL Score**, **Remaining Tasks**, **Created By**, **Created Date**, and **Closed Date**. In addition, the **Created Date** and **Closed Date** columns display timestamps rather than just dates.

Threat Intelligence

- The following TQL query parameters are now available, including in the v3 API:
  - `associatedGroupSource`: Use this parameter to filter results based on the method used to create an association to a Group.
  - `associatedIndicatorSource`: Use this parameter to filter results based on the method used to create an association to an Indicator.
- **CAL Impact Factors** were added to the **ThreatAssess & CAL** area of the **Details** card on the **Overview** tab of the new **Details** screen, providing context on the Indicator's CAL score.
- The **Expand All** and **Collapse All** buttons on the new **Details** screen now respectively expand and collapse all cards and sections within cards.

Attributes

- A default Source Attribute was added to the **Details** card on the **Overview** tab of the new **Details** screen for Indicators and Groups.

Playbooks

- For all Group, Indicator, Case, Track, and Victim Playbook Trigger types, a **Select All** option was added in the Trigger configuration for selecting all owners at once.

Workflow

- Super Users can now assign Workflows, Cases, and Tasks in all Organizations, not just their home Organization, to themselves.

System Settings

- The following new system settings were added:
    - **appsPythonhome311**: This setting holds the path to the Python 3.11.*x* binary.
    - **tqlAssociationExecutionTime**: This setting determines the time at which the TQL Association Monitor will execute the TQL Association Process, which runs once per day. When the TQL Associations Process runs, each TQL query belonging to a Group is executed and the results are associated to the Group.
    - **tqlAssociationMonitorEnabled**: This setting turns the TQL Association Monitor on or off. If this setting is turned off, TQL queries added to Groups will not run automatically and must be run manually by a user.
    - **tqlAssociationMonitorInterval**: This setting determines the frequency, in minutes, at which the TQL Association Monitor will check to see if the TQL Association Process, which runs once per day, should be executed.
    - **tqlAssociationTotalAssignable**: This setting determines the maximum number of TQL queries that can be assigned and used for TQL associations on the ThreatConnect instance.

API & Under the Hood

- Support for the **`lastUpdated`** field for Case objects has been added to the v3 API.
- The v2 Batch API now supports the creation of Group-to-Indicator associations in addition to Indicator-to-Group and Group-to-Group associations.
- Playbook server names are no longer being overwritten as **tc-job** during upgrades.
- The session ID entropy for ThreatConnect was increased to 128 bits.

Bug Fixes

Threat Intelligence

- When creating a new Campaign, Event, or Incident Group from an account using dark mode, an issue was causing dates in the calendar selector for the **First Seen** (Campaign) and **Event Date** (Event and Incident) fields not to be visible or selectable. This issue has been resolved.
- Starting with ThreatConnect 7.0, if a file hash conflict occurred when contributing a Group to a Community or Source, the user would be returned to the **Sharing** tab of the Group's **Details** screen instead of being shown an error message describing the file hash conflict. This error message has now been restored.
- An issue causing Tag auto-completion to be case sensitive has been fixed. When you enter a Tag, you will be presented with possible matches to existing Tags regardless of the case of the existing Tags and of the case of the Tag you are entering.

Reporting

- In the **Add Text Block** section for a report, you will now see a disclaimer about how hyperlinks are not supported and will automatically be defanged. This disclaimer is intended to serve as a reminder that there is no way to create functioning hyperlinks in this section of the report.
- An issue preventing custom Indicators associated to Groups from being included in reports was fixed.

Attributes

- An issue causing HTML image and hyperlink tags to render as clickable strings in Attributes using Markdown has been addressed. The new **Details** screen will render images and sanitize hyperlinks, and the legacy **Details** screen will output the HTML as an unclickable string.
- An issue causing the user who created an Attribute for an Indicator or Group always to be listed as the user who last modified the Attribute, even if another user has made changes to the Attribute, has been fixed.

Playbooks

- An issue preventing query parameters for WebHook Triggers from being reordered or deleted has been resolved.
- An issue causing an error to occur when attempting to import a new version of a Playbook from the Playbook's execution graph or from the Playbooks' table entry on the **Playbooks** screen has been resolved.

Jobs & Apps

- An issue preventing Jobs from deploying via **TC Exchange™ Settings** when the maximum number of allowed API users is allocated was resolved.[4]

System Settings

- An issue causing test emails sent by System Administrators to fail to send when multiple email addresses separated by commas were entered as the recipient has been fixed.

API & Under the Hood

- The character limit for the **`fileName`** endpoint for Documents and Reports was raised to 255 in both the v2 and v3 API.
- An issue causing extensive memory usage to occur on some instances has been resolved.
- For the **`/v2/indicators`**, **`/v2/groups`**, and **`/v2/tasks`** API endpoints, the **`communityOrSource`** and **`additionalOwners`** fields will now be included in API responses only when **`?includes=additional`** is appended to the end of the request URL. Previously, these fields were being included in the default response for each endpoint automatically.
- An issue causing **`GET`** requests to **`/v3/security/users`** not to return a full set of details to API users was fixed.

[4] TC Exchange™ is a trademark of ThreatConnect, Inc.

Dependencies & Library Changes

- Python® 3.11 is now supported for App executions only. Support for using Python 3.11 to build Apps will be available in a future version of ThreatConnect.[5]

[5] Python® is a registered trademark of Python Software Foundation.

Maintenance Releases Changelog

2023-09-21 7.1.3-M0921R [Latest]

Bug Fixes

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

2023-08-08 7.1.3-M0808R

Improvements

- The following new system setting was added:
    - **playbookSessionPurgeTimeoutSeconds**: This setting determines the number of delay seconds after which a Playbook session is purged.

2023-06-27 7.1.3

Bug Fixes

- An issue causing instance instability when parsing files that have very large numbers of Indicators has been resolved.
- An issue preventing Playbooks from executing for Indicators in Threat Graph 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.
- An issue causing out-of-memory errors to occur when using the v2 API to get the number of associated Indicators for an object has been resolved.
- 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 Attribute Descriptions to be truncated in the **Report Editor** and PDF preview for a Report was resolved.

- An issue causing some Markdown tables on the **Attributes** card of the new **Details** screen to be cut off was fixed.
- 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 some Markdown tables in the **Attributes** section of the **Details** drawer on the **Browse** screen to be cut off was fixed.
- An issue causing an error when using the **Update Global Variable** App in Playbook Components was fixed.
- An issue causing potentially associated Cases not to be displayed on the **Associations** tab of the **Details** screen for some Groups was fixed.

2023-06-08 7.1.1e

Bug Fixes

- A performance enhancement was implemented for Indicator counts.

2023-05-31 7.1.2

Improvements

- The following information was added to **INFO**-level Playbook log entries: Playbook Name, Start Time, Session ID, Group XID, Playbook Log Level, Version.

Bug Fixes

- An issue causing Markdown not to be rendered properly for read-only custom Attributes on the new **Details** screen was fixed.
- An issue causing Markdown tables to overflow and not be readable in their entirety for custom Attributes on the new **Details** screen has been fixed.
- An issue causing certain Attributes that have a custom Attribute Type not to be editable on the new **Details** screen was resolved.
- An issue preventing Feed Deployer App Services from automatically starting up after restart of a ThreatConnect instance was fixed.

- An issue causing the **Create TAXII User** button not to be available even though the limit on the number of TAXII™ users has not been reached has been resolved.[6]
- Benign Amazon S3™ errors are now being logged at the **TRACE** level instead of the **ERROR** level.[7]
- The **Attributes** card on the new **Details** screen for objects with large numbers of Attributes was not paginating the Attributes, preventing some of the Attributes from being displayed and being searchable. This issue has been corrected.
- An issue causing Playbook execution delays was fixed.

2023-05-19 7.1.1d

Bug Fixes

- An issue causing an out-of-memory error to occur when using the v2 API to retrieve Indicators by a Tag that is assigned to a very large number of Indicators was fixed

2023-05-08 7.1.1c

Bug Fixes

- A memory leak caused by completed Playbooks with Components or Iterators not clearing from internal collections was fixed.
- Raw HTML responses from Playbook UserAction Triggers were being encoded and displayed incorrectly in tooltips on the **Playbooks** card of the new **Details** screen. These responses are now being decoded and displayed properly.

2023-05-04 7.1.1

Improvements

- ActiveMQ® Cipher Suite configuration can now be enabled, allowing you to determine which cipher suites are used in the encryption of ActiveMQ messages in ThreatConnect.[8]

[6] TAXII™ is a trademark of The MITRE Corporation.
[7] Amazon S3™ is a trademark of Amazon Technologies, Inc.
[8] ActiveMQ® is a registered trademark of Apache Software Foundation.

- In the configuration for User Metric dashboard cards, there is now an **Hourly** option in the **Group By** menu.
- When creating or editing a Community or Source in **Account Settings**, you can now enable or disable the ability for users to change Indicator Status. If this option is disabled, then all Indicators imported during a structured Indicator import will automatically be given a status of active.

Bug Fixes

- The new **Details** screen is no longer available for Task Group objects. These objects may now be viewed only on the legacy **Details** screen.
- An issue preventing Playbook Components from displaying input fields when editing Apps has been resolved.
- An issue causing HTML tags to be displayed in plain text instead of being rendered in tooltip responses for UserAction Playbooks on the new **Details** screen was resolved.
- An issue preventing Super Users from importing Playbooks into Organizations other than their home Organization has been resolved.
- An issue causing discrepancies in Workflow Case creation counts for a particular day has been resolved.
- An issue preventing Super Users from using the Unstructured Indicator Import feature to import Indicators into an Organization other than the Super User's home Organization has been resolved.
- An issue causing the Structured Indicator Import functionality to ignore values in the **Active** column of the CSV file for new Indicators was fixed.
- Indicator searches on the **Browse** screen have been adjusted to ensure that only active Indicators are returned by default.
- An issue causing counts for some Group types to be incorrect on dashboard cards has been resolved.
- An issue preventing pagination from occurring in API responses returned from the **`/v3/indicators/deleted`** endpoint has been fixed.
- An issue causing an error to occur when using the v3 API to edit a File Indicator that contains a File Occurrence was fixed.
- Performance improvements were made to improve latency issues with potential associations for Workflow Cases.
- An issue causing problems with saving Artifacts in a new Workflow Case was fixed.

2023-04-20 7.1.0b

Bug Fixes

- An issue causing memory leaks leading to out-of-memory errors to occur when using Playbooks containing Delay Operators or Apps that have a Retry Flag has been resolved.

2023-04-12 7.1.0a

Bug Fixes

- An intermittent issue causing database deadlocks and system instability under certain conditions has been resolved.
- An issue causing Job Apps not to process the value of Organization variables of the FILE type as input has been fixed.