Version: 6.5

5 April 2022

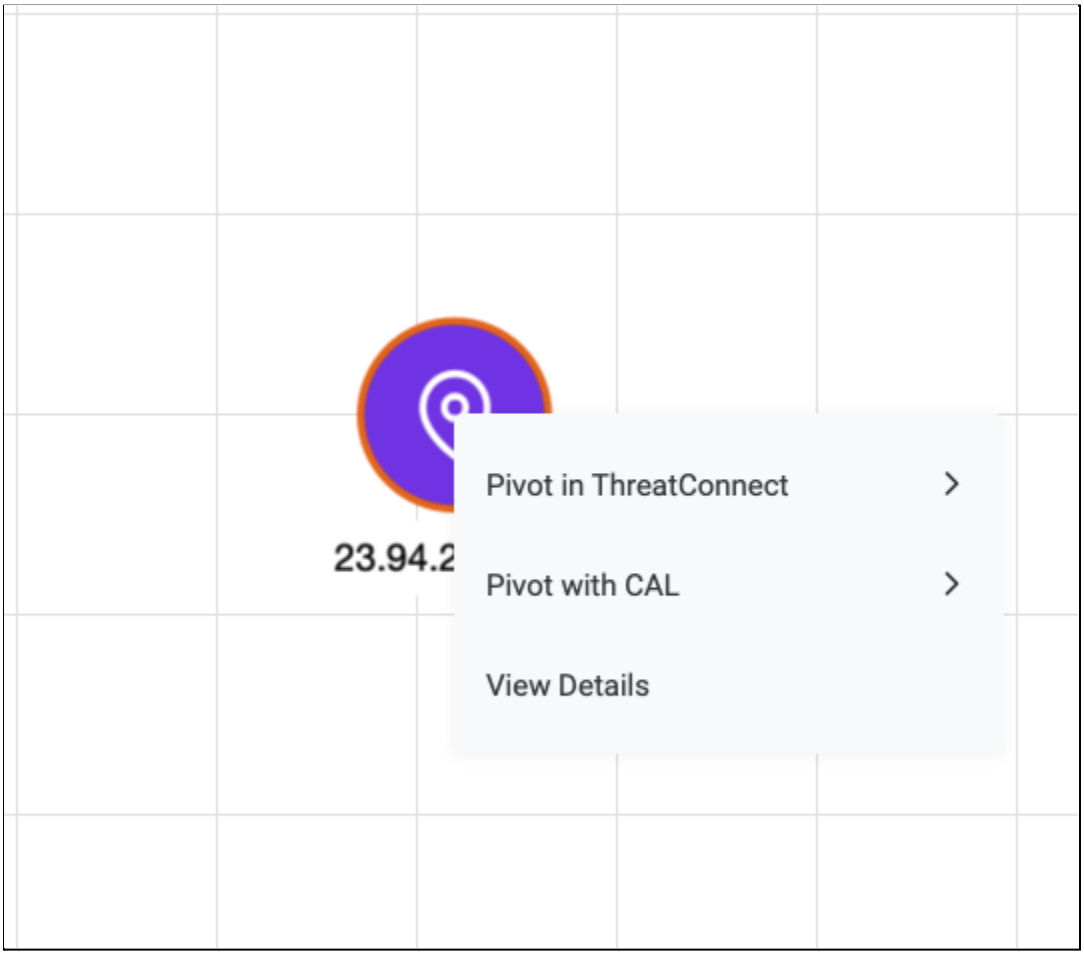
ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | **F:** +1.703.229.4489
www.ThreatConnect.com

New Features and Functionality

Graph View Improvements - Phase 2

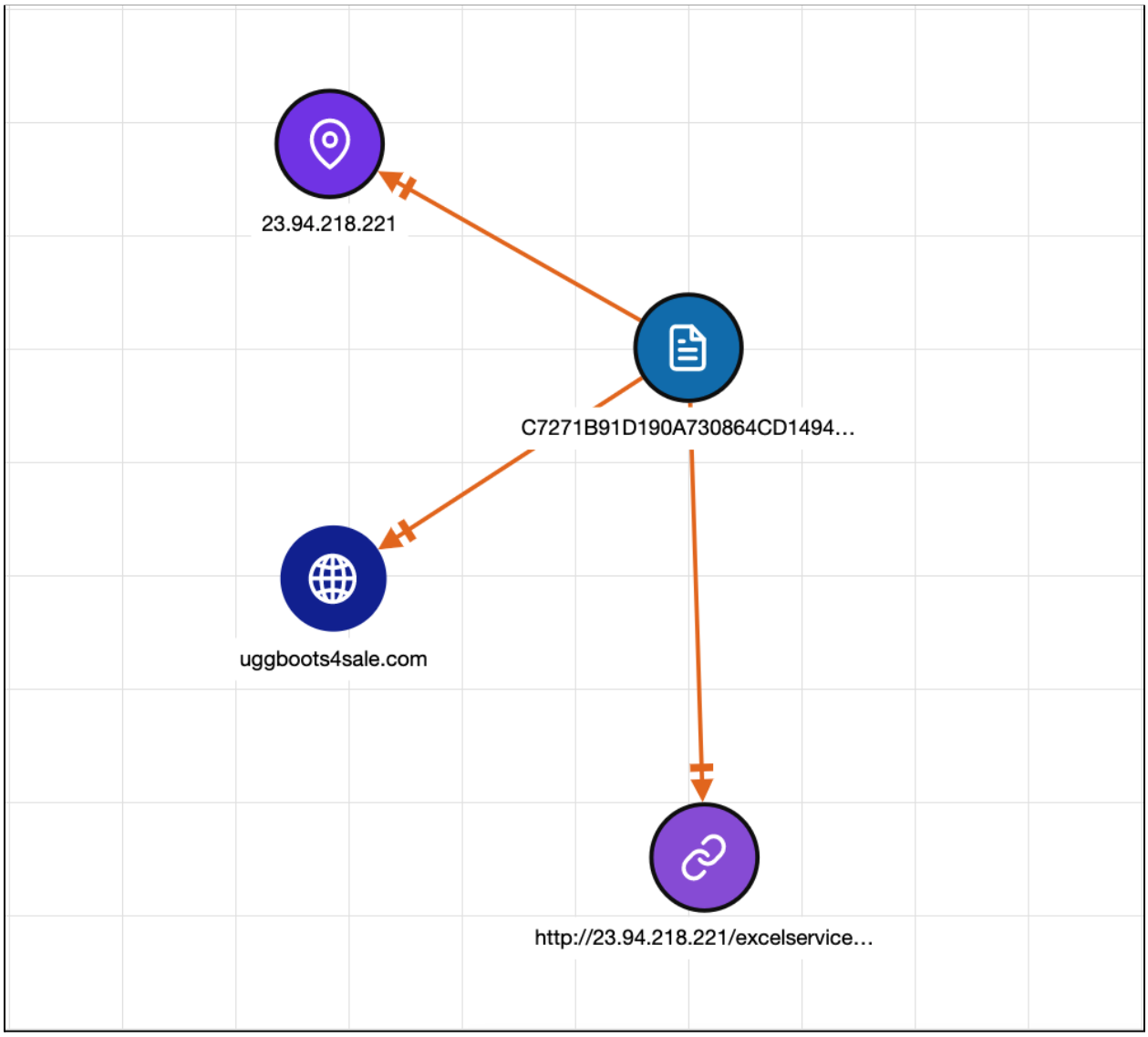
In ThreatConnect 6.5, we expand upon the foundations we built in Phase 1 of the graph view improvements released in ThreatConnect 6.4. In Phase 2, users can pivot on Indicator-to-Indicator relationships (sometimes referred to as custom relationships) that exist in their ThreatConnect instance, as well as Indicator-to-Indicator relationships that exist in the ThreatConnect Collective Analytics Layer (CAL™).[1]



Pivot in ThreatConnect and explore the CAL dataset in the same graph

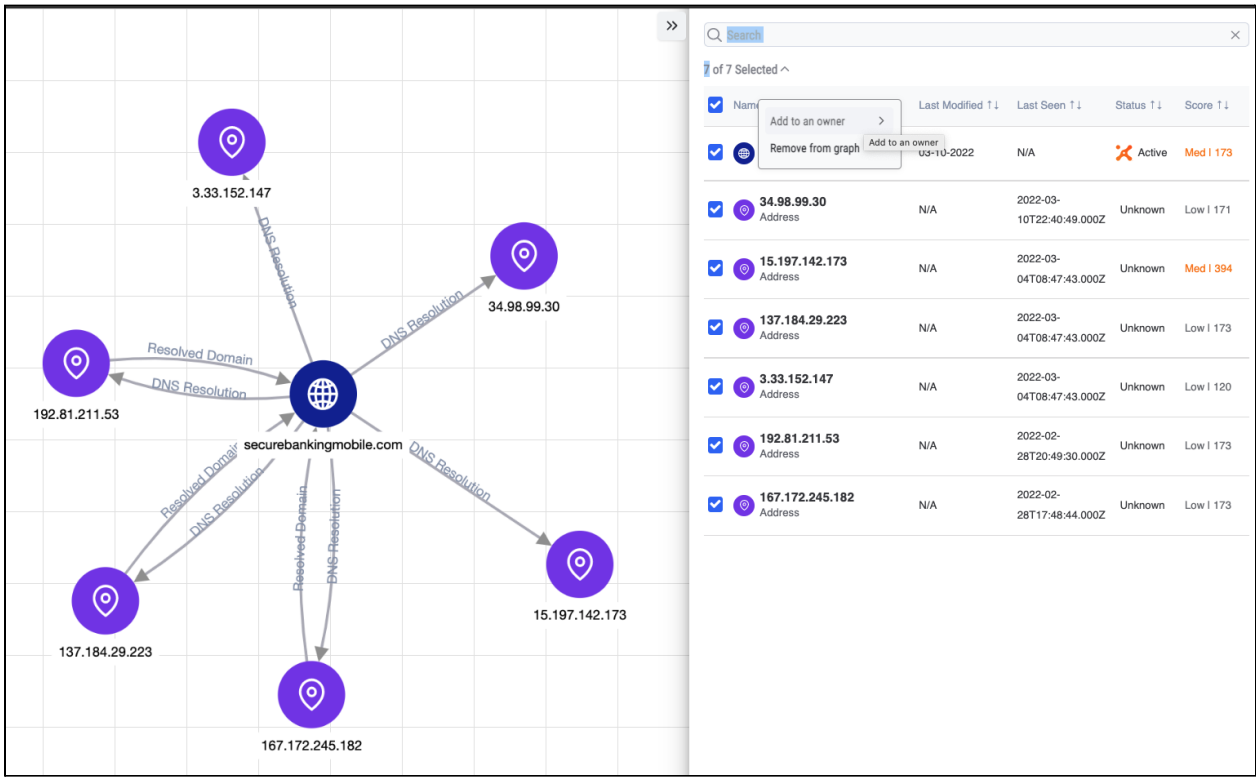
Also in this phase, users can pivot in multiple owners on the same graph to see Indicator-to-Indicator associations that may exist across different owners and CAL.

[1] CAL™ is a trademark of ThreatConnect, Inc.



Black borders on nodes indicate that the Indicator exists in multiple owners and shows that the user is viewing information from multiple owners in the graph

Then, after building out a graph, users can save the Indicators discovered during their pivoting, view a **Details** drawer with additional information about Indicators that exist in their Organization, and remove nodes from the graph via the new table. The ability to save Indicators is especially notable, as it can be used to save information found when pivoting in the CAL dataset.



Import Indicators from the graph

There are a few things that are important to note. First, this set of features is Phase 2 of graph view improvements in ThreatConnect. There will be at least 3 phases of these updates, and the legacy graph will continue to be available on the **Details** screens of Groups and Indicators until we fully replicate all available functionality in the new graph. Second, this version of the graph view allows users to pivot only on Indicator-to-Indicator relationships. Users will not be able to pivot on Indicator-to-Group-to-Indicator relationships in this phase. Because of this, users may observe associations in the **Associations** card on an Indicator's **Details** screen, but not have any pivot results in the new graph. This lack of results is due to the lack of direct Indicator-to-Indicator relationships for the Indicator being investigated. This limitation will be addressed in Phase 3 of this initiative.

Last Modified Date Timestamp on Groups

With ThreatConnect 6.5, users will now be able to see when Groups were last modified. This timestamp has been available on Indicators for a while, but it is now available on Group objects as well. This feature was requested by multiple customers and will help users make sure they are working with the most up-to- date Group information.

The Last Modified date timestamp on Groups is available in ThreatConnect 6.5

The Last Modified date timestamp appears on the Group's **Details** screen, the Group's **Details** drawer, and the table on the **Browse** screen. The field is also available as a filter in ThreatConnect Query Language (TQL).

Fusion API - Defined Link Support in V3 API

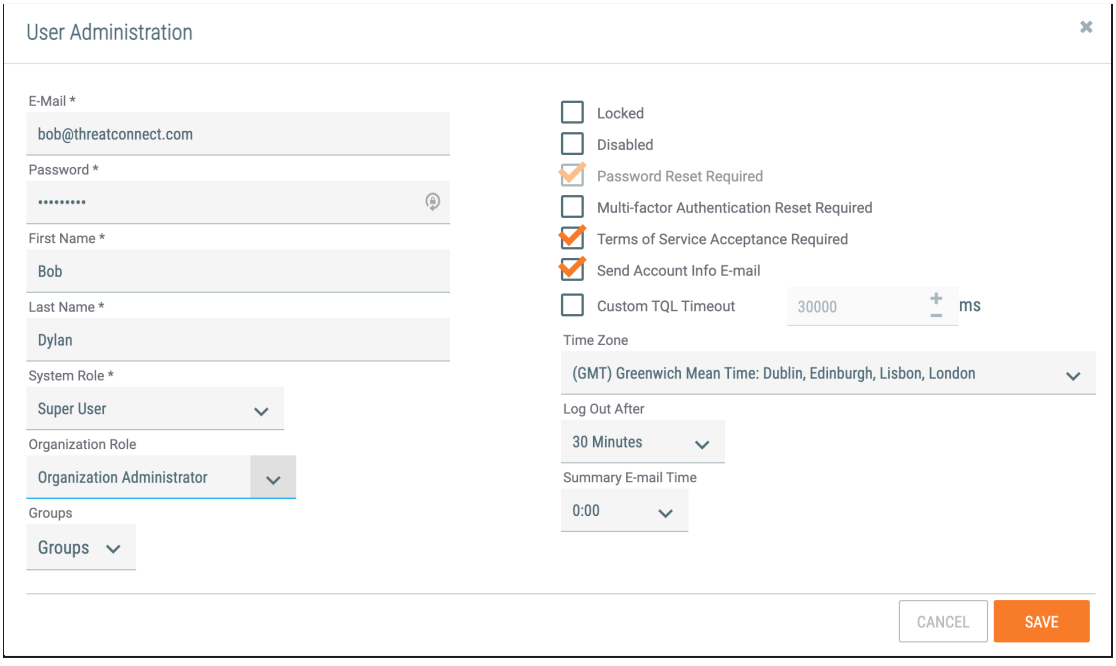
Version 3 of the ThreatConnect API was released alongside Workflow in ThreatConnect 6.0. Since that time, we have worked to iterate on the API by adding support for intelligence objects in 6.4. This new update to the V3 API will enable users to link intelligence from the Threat Intelligence Platform (TIP) side of ThreatConnect to Cases in Workflow, and vice versa. This capability will allow users to automate the establishment of direct associations between intelligence and Cases in the platform, making that process less manual and less time consuming.

Multitenant Superuser

In version 6.5 of ThreatConnect, we are releasing the new Super User System role, which will enable users on multitenant instances to easily view and manage all of their customers' data without the excessive logistical burden of logging in and out of different user accounts. Super Users on multitenant instances can complete investigations for one customer and then, without changing to a different login, work an investigation for another customer, all while ensuring that the underlying customer data never co-mingle. Super Users also have the ability to view intelligence across multitenant instances to identify common patterns and resolutions.

Only users with the permission to select System roles when creating users (that is, users who have a System role of Administrator or Operations Administrator) can create Super User accounts. Super User accounts do not have any access or permissions at the System level, and their Organization role is automatically set to Organization Administrator and cannot be changed.

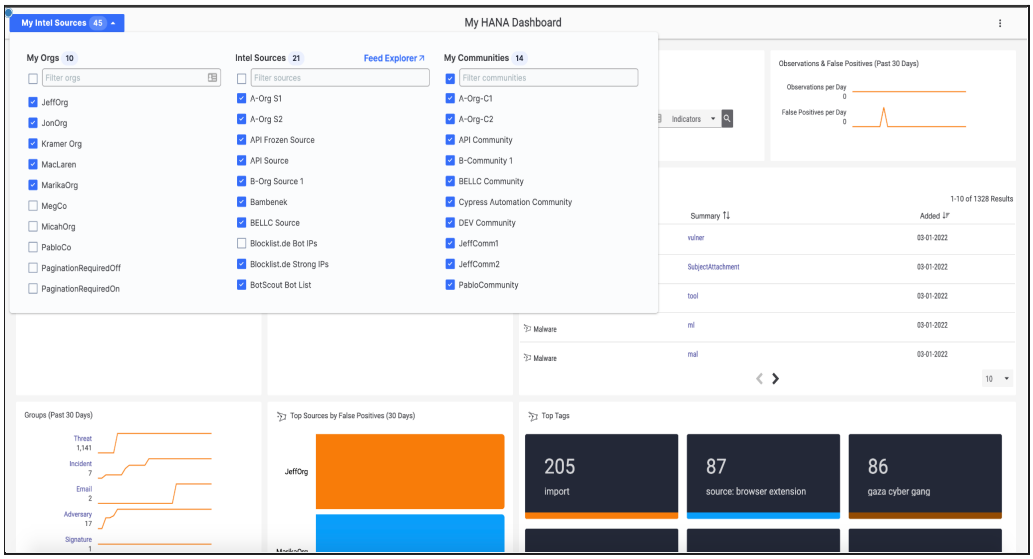
The Organization Administrator permissions of the Super User apply to all Organizations on their ThreatConnect instance. In this release, Super Users cannot be limited to have visibility only to specific Organizations.



The Super User System role is automatically paired with the Organization Administrator Organization role

Super User - Dashboard

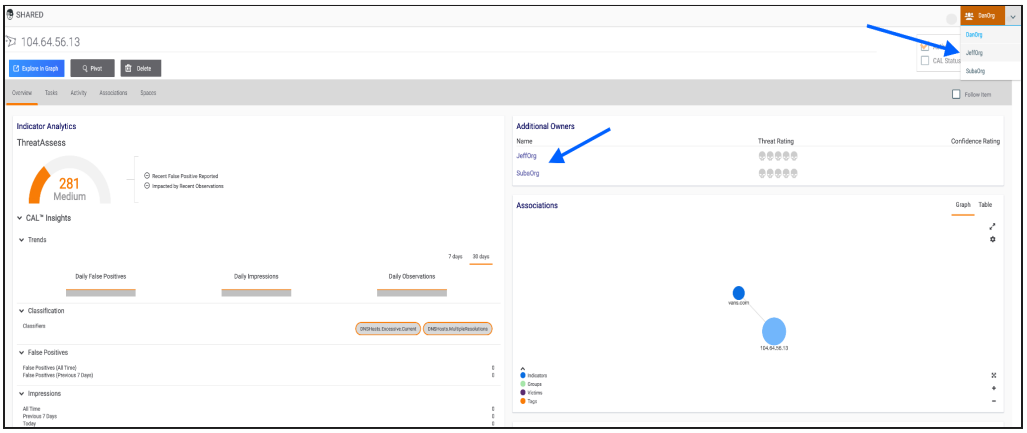
Super Users can have full visibility across customer environments by creating dashboards to view data for one or more customers at once. This capability enables Super Users to track metrics for Cases, manage intel, take action on threat intelligence, and understand relationships and trends impacting all of their customers.



Super Users can create dashboards to track Case metrics and intelligence trends across all of their customers

Super User - Explore Intel across Customers

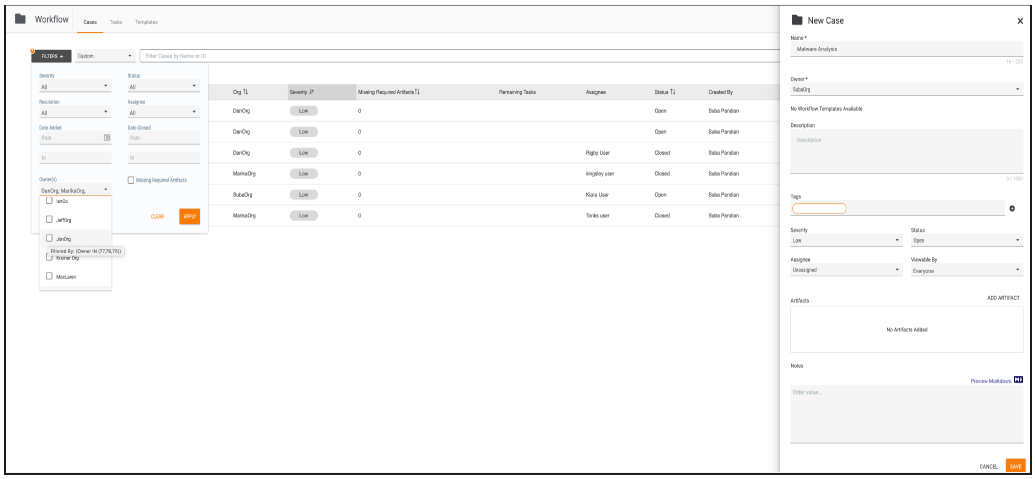
Because Super Users can see all threat intelligence in all Organizations on their ThreatConnect instance, they have the ability to understand and correlate intel across customers and make quicker and more informed decisions. Super Users can gather relevant context specific to each customer by a simple switch between the customer Organizations.



*Super Users can see all Organizations that own a piece of threat intel in the **Additional Owners** card on the **Details** screen*

Super User - Workflow and Playbooks

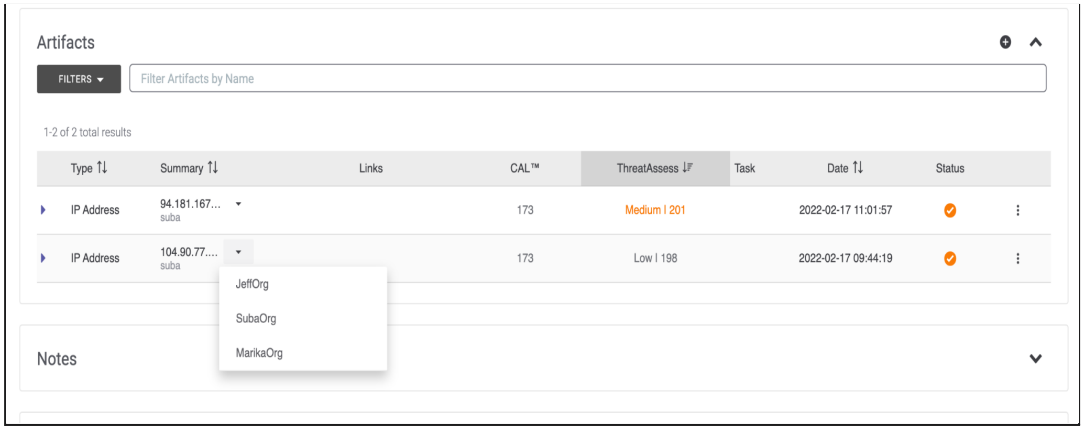
Super Users can view, create, and manage Cases and Playbooks across their customers' Organizations. They can also create Workflow Templates and Playbooks and share them across different customers, greatly streamlining the way in which case management and orchestration processes are shared across tenants in an multitenant instance.



Super Users can view all Workflow Cases across the owners they select

Super Users investigating a Case also have the ability to view related intelligence of Indicators of Compromise across their customers' Organizations. For Super Users, the **Artifacts** card in a Case will show all owners, including other Organizations on the ThreatConnect instance, for each Artifact. This ability to

track Case Artifacts across Organizations can help analysts to coordinate responses on an attack across their customers.



Super Users can view all Organizations that contain an Artifact

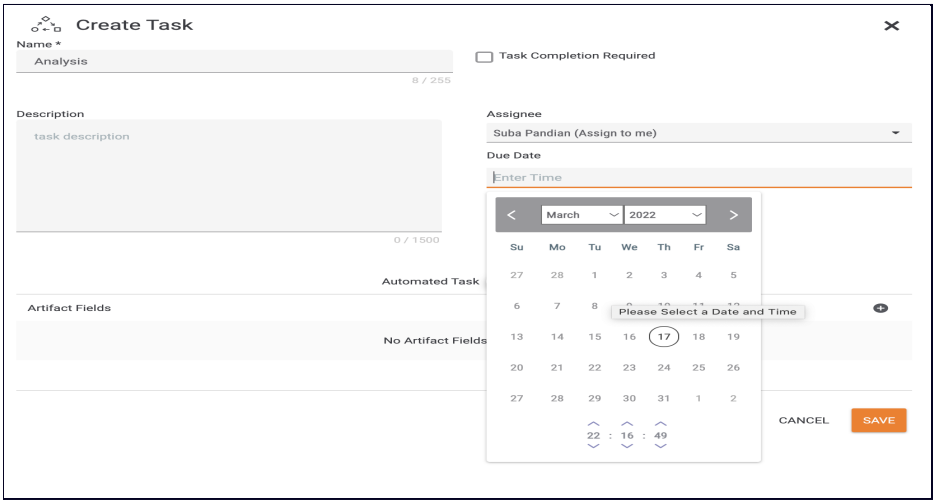
Workflow Analysts Efficiency Metric

The **Top 10 Case Closing Analyst** efficiency metric displays the 10 users who closed the most Cases in the past 30 days on an easy-to-read dashboard card. This information can help team leads and managers measure and track the individual performance of analysts, discover skill gaps, identify outstanding analysts, and acknowledge analyst contributions.

*The **Top 10 Case Closing Analyst** card displays the number of Cases closed and who closed the most Cases over the past 30 days*

Workflow - Granular Task Due Dates

The due dates for Workflow Tasks can now be tracked down to the minute, enabling teams to track Tasks more accurately and manage expectations around their turnaround time.



The due dates for Workflow Tasks can be scheduled down to the minute

Improvements

In addition to the brand new features listed above, we've made a number of improvements to the features users already know and love.

Playbooks

- When a Service App fails to activate, an error message is displayed on the **Services** tab of the **Playbooks** screen. The message includes the date and time when the Service failed to start and a summary of why it failed to start, which is retrieved from the corresponding log files.
- The following output variables have been added to the Workflow Trigger: **#tc.wf.username**, **#tc.wf.firstname**, **#tc.wf.lastname**. These variables enable tracking of the user triggering the Workflow Playbook.
- The following output variable has been added to the Mailbox Trigger: **#trg.mbox.raw**. This variable contains the raw email contents received by the Trigger.
- WebHook and UserAction Triggers have a new **Timeout** field that allows you to configure a custom timeout length for the Trigger.
- App Developers can now enable and configure retry logic for specific actions in the App Builder.

Threat Intelligence

- An **Exact matches** checkbox has been added to the **FILTERS** area of the **Browse** screen to enable searches for specific content (versus "contains" searches in the Summary).
- In the **Intel Sources** section of **MY INTEL SOURCES**, the **ThreatConnect Intelligence** and **Technical Blogs and Reports** sources are no longer highlighted at the top of the list, but rather appear in alphabetical order within the rest of the list.
- The character limit for the description of an Indicator when performing an unstructured Indicator import has been increased.

Workflow

- The table on the **Tasks** screen now displays a sortable column with the number of missing required Artifacts for each Task.
- On the **Cases** screen, the total number of missing required Artifacts for all Tasks in each Case can be viewed on the card for each Case (card view) or as a sortable column in the table (table view). The **FILTERS** selector also has a new checkbox, **Missing Required Artifacts**, that, when selected, returns only Cases that are missing required Artifacts.
- It is now easy to add Attributes to a Workflow Template via a "Click to add another attribute." link located under the most recently added Attribute.

- When importing a Template with embedded Workflow Playbooks containing Organization- or user-level variables, those variables will automatically be created in your Organization, and you will be prompted to enter values for them upon import of the Template.

Dashboards

- **Top 10 Case Closing Analyst,** a new Metric card found in the **Cases** subsection, displays a chart showing the ten analysts who have closed the most Workflow Cases in the past 30 days, along with the number of Cases they have closed..

System Settings

- Enabling a new system setting, **syslogIncludePlaybookExecution**, causes Playbook and Playbook App execution logs to be sent to the configured Syslog host.
- A new system setting, **mailConnectionTimeout**, enables System Administrators to configure a custom timeout length for the Mailbox Trigger in Playbooks.
- A new system setting, **apiIndicatorObservationLimit**, enables System Administrators to configure the maximum number of observed Indicators that can be returned at a time from the v2 API.
- Eight existing system settings were renamed and given an updated description to account for the change from Elasticsearch® to OpenSearch® in ThreatConnect version 6.4:[2]

Old Name	New Name	New Description
logToElasticSearch	logToSearchCluster	Turn on or off logging to the search cluster
elasticSearchUrl	searchUrl	The URL for the search server
elasticSearchEnabled	searchEnabled	Turns on or off support for search
esBackupHour	searchBackupHour	Hour of the day when the search backup should run
xpackSecurityEnabled	searchSecurityEnabled	Turn on/off security for the search cluster on your system
xpackAdminUsername	searchAdminUsername	The search admin username
xpackAdminPassword	searchAdminPassword	The search admin password
elasticSearchCluster	searchCluster	The search cluster name. Must match the one specified in the search cluster configuration

[2] Elasticsearch® is a registered trademark of Elasticsearch BV.
OpenSearch® is a registered trademark of Amazon Web Services.

API & Under the Hood

- An upgrade to log4j 2.17.1 was implemented.
- Two new branches have been added to the Management API: one that allows you to retrieve a list of users currently logged into the ThreatConnect instance and another that allows you to retrieve information about Playbook Environment services on the instance.
- Two new query parameters have been added to the Management API: one that allows you to specify the instance you want to retrieve information for and another that allows you to specify the worker count when updating the Playbook worker count for the ThreatConnect instance.
- Additional fields will be returned when retrieving Java virtual machine (JVM) statistics and a list of actively running Playbooks via the Management API.
- When retrieving Indicator observations using the v2 API, the API response will now include the total number of observations and the date and time of the last observation for each Indicator.
- When retrieving Indicator observations using the v2 API, the maximum number of Indicators returned has been increased from 10 to 20,000. System Administrators can adjust this limit via a new **apiIndicatorObservationLimit** system setting, if desired.

Bug Fixes

Playbooks

- An issue causing Playbook Apps to fail to retrieve Organization variables when using the **runtimeVariables** feature and running on an Environment has been resolved.
- A problem causing the **#gbl.username.runas** variable to return a Playbook's creator rather than the **Run As** user has been corrected.

Threat Intelligence

- An issue causing the **Associations** card on the **Details** screen to experience long or infinite load times has been fixed.
- When non-encoded TQL queries are entered, an error message specifying that the problem is a non-encoded URI will be returned rather than the more generic "Unauthorized Response" error.
- Searches for terms existing in very large Document Groups were causing no results to be returned, even if the terms existed in other intelligence objects as well. This problem has been fixed.

Workflow

- Long Case Attribute values such as email bodies are no longer causing overlap and inability to scroll when viewed on the **Attributes** card in a Workflow Case in an Organization where Markdown has not been enabled.
- When adding an Attribute that accepts input via select-one radio buttons to a Case, the list of radio-button options was collapsed, showing multiple items on one line and running over into the **Source** field. This issue has been remediated.

Dashboards

- A problem was fixed that was causing cards with the **Upvotes** and **Downvotes** column to show thumbs-up and thumbs-down icons, respectively, instead of vote counts.

API & Under the Hood

- An issue causing the ThreatConnect installer not to function without Internet has been corrected.

Dependencies & Library Changes

- There are no dependencies & library changes in ThreatConnect 6.5.

Maintenance Releases Changelog

There have been no patch releases at this time. 6.5 is the latest version.