ThreatConnect®
Super User Guide

Software Version 7.0

Technical Guide

January 18, 2023

10026-04 EN Rev. A

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

Overview

A Super User account in ThreatConnect enables users on multitenant instances to easily view and manage all of their customers' data from a single user account. Super Users do not have any access or permissions at the System level, but do have full data-level, administrative, and configuration permission at the Organization level for all Organizations on the ThreatConnect instance. Super Users may view, create, edit, and delete data (dashboards, posts, threat intelligence, Workflow, and Playbooks) in all Organizations on the ThreatConnect instance. They also can administrate and configure all Organizations, including creating, deleting, and updating user accounts and adding, modifying, and deleting Organization-level variables, metrics, Attribute Types, Indicator exclusion lists, and Security Labels.

This guide covers all of the functionalities specific to your Super User account. It discusses all the areas of ThreatConnect in which you can access and modify data in all Organizations on your instance and the administrative and configuration functions available to you for those Organizations.

Managing Data in All Organizations as a Super User

Your Super User account belongs to one Organization (your "home Organization"), but you can view, manage, and modify dashboard, posts, threat intelligence, Workflow, and Playbooks information in all Organizations on your ThreatConnect instance.

Dashboard

As a Super User, you can determine which Organizations' data you want to view on the **Dashboard** screen. You can also configure dashboard cards to show data from selected Organizations and, for query cards, enter ThreatConnect Query Language (TQL) queries to search for objects belonging to multiple Organizations.

The Dashboard Screen

The **My Intel Sources** selector on the **Dashboard** screen will display a **My Orgs** list from which you can select the Organizations whose data you want to view (Figure 1).

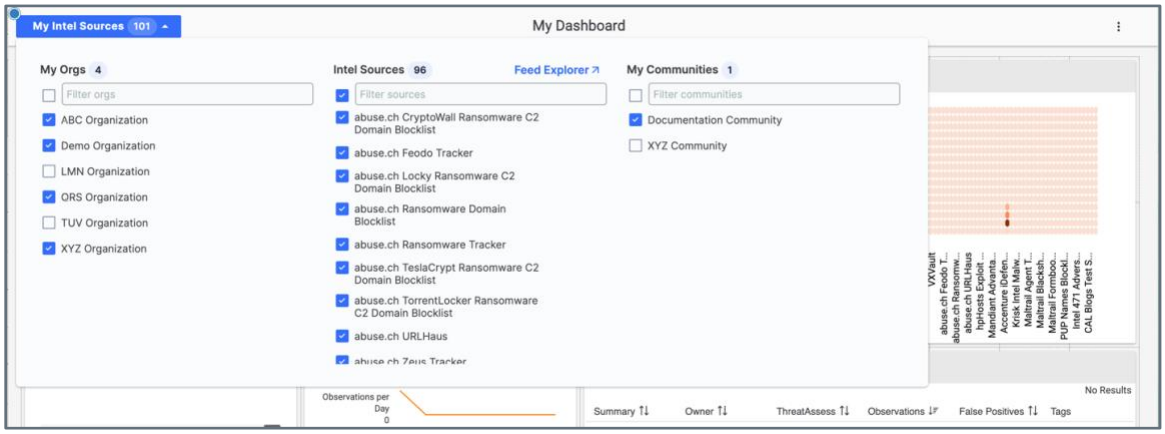

Figure 1

Dashboard Card Configuration

When configuring Metric and Query dashboard cards, you can use the **My Orgs** list to select Organizations whose data you want to include on the card (Figure 2).

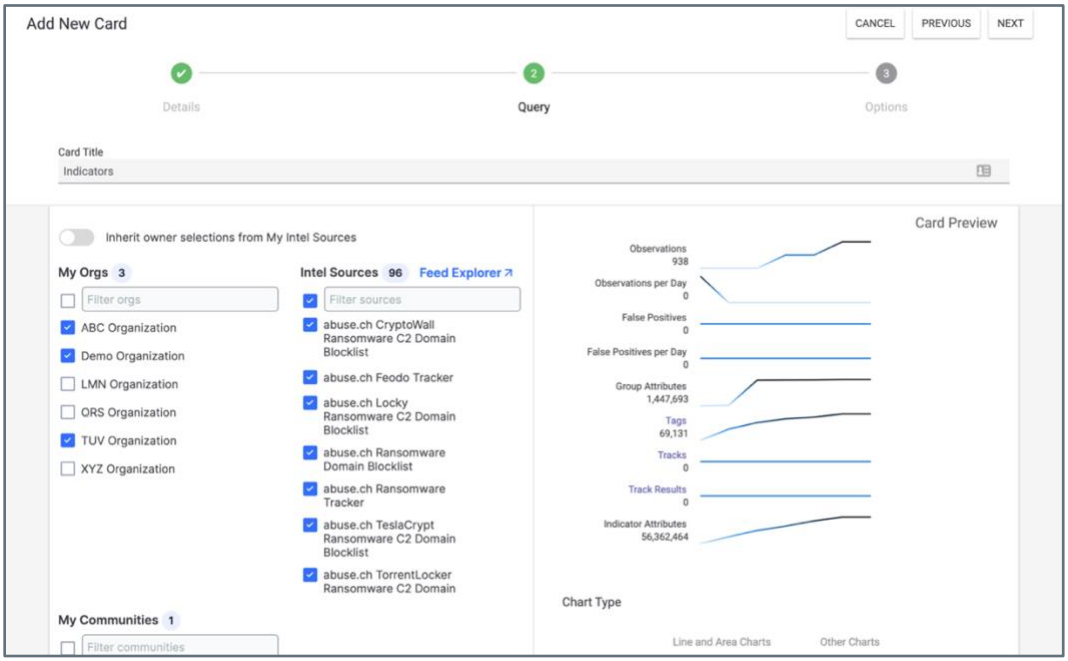

Figure 2

TQL Queries

When configuring Query dashboard cards, you can enter a TQL string to search for objects belonging to multiple Organizations in the **Advanced Query** field. See the "Query for Objects Belonging to Multiple Owners" section of *Constructing Query Expressions* for more information.

Posts

For a Super User, the **My Org** section of the **Posts** screen will display all Organizations on your ThreatConnect instance (Figure 3).

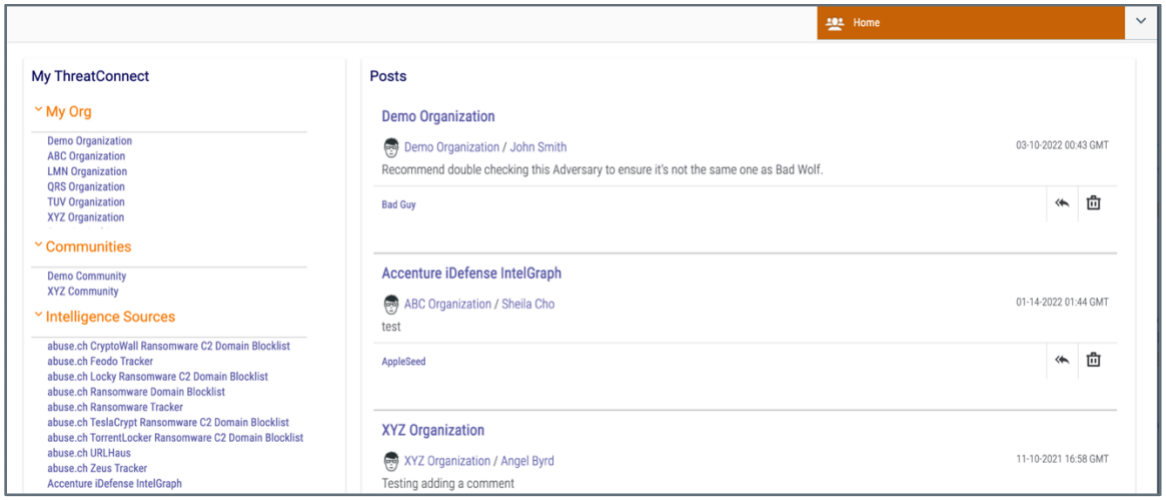

Figure 3

By default, the screen will display posts from your home Organization, and the name of your home Organization will be at the top of the **My Org** list. To view posts in another Organization, click on that Organization's name in the list. You can also use the selector at the top right of the screen to navigate to the **Posts** screen for another Organization.

Threat Intelligence

As a Super User, you can view, create, import, filter, search for, modify, and delete threat intelligence in all Organizations on your ThreatConnect instance.

Browse

The **My Intel Sources** selector on the **Browse** screen will display a **My Orgs** list from which you can select the Organizations whose data you want to view (Figure 4).

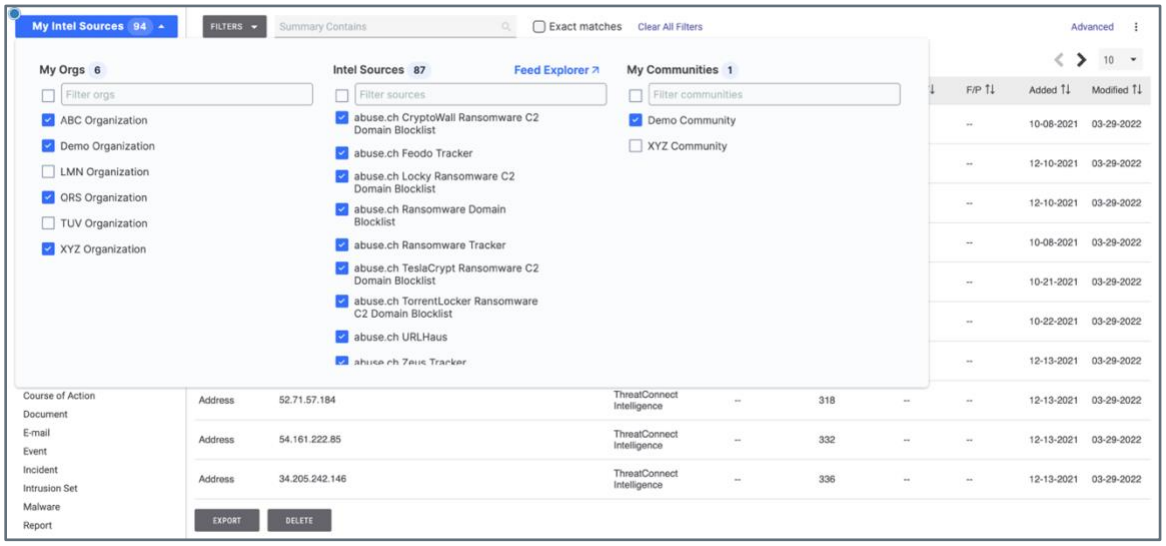

Figure 4

Create

When using the **Create** option on the top navigation bar to add an object (Indicator, Group, Track, or Victim) to ThreatConnect, you can select any Organization on the ThreatConnect instance from the **Owner** menu (Figure 5).

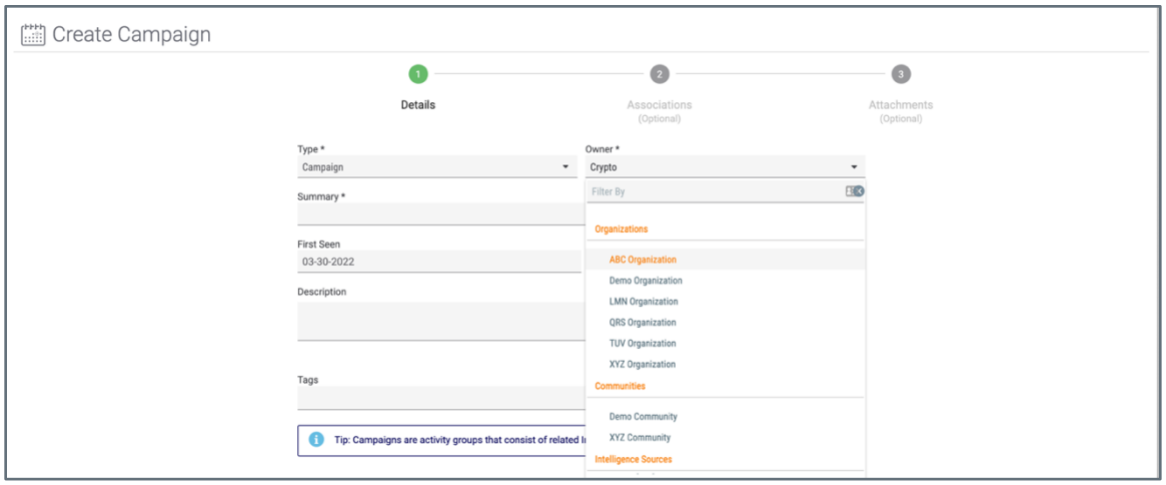

Figure 5

Import

When using the **Import** option on the top navigation bar to import objects (Email import, structured Indicator import, unstructured Indicator import, or Signature import), you can select any Organization on the ThreatConnect instance from the **Owner** menu (Figure 6).

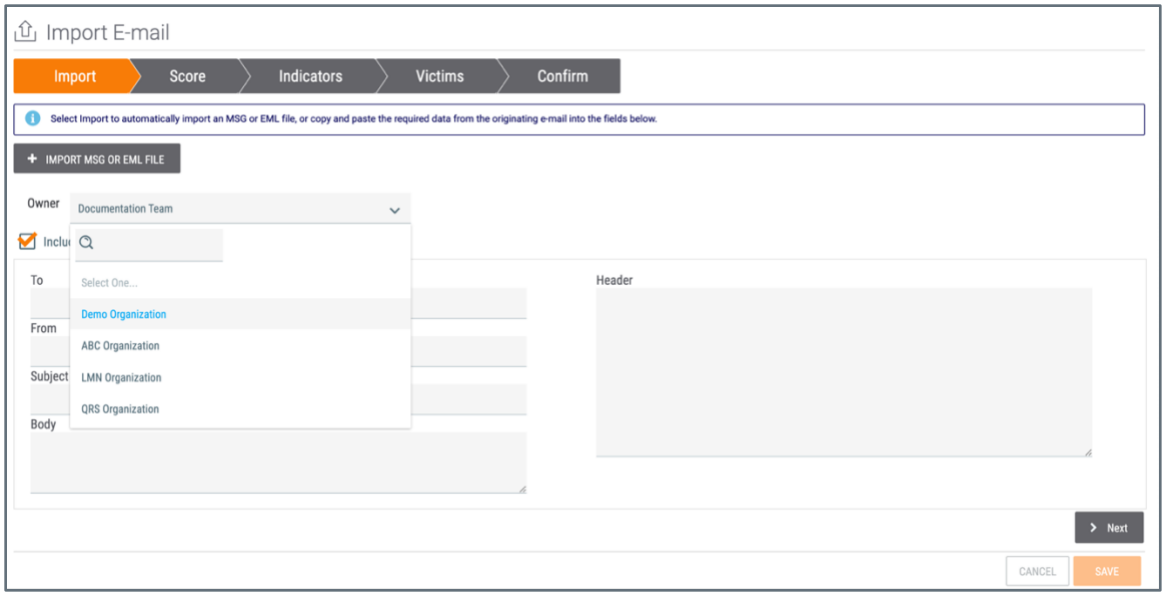

Figure 6

Search and Analyze

The **OWNERS** selector in the **Search** drawer will display a **My Orgs** list from which you can select the Organizations in which to search for data (Figure 7).

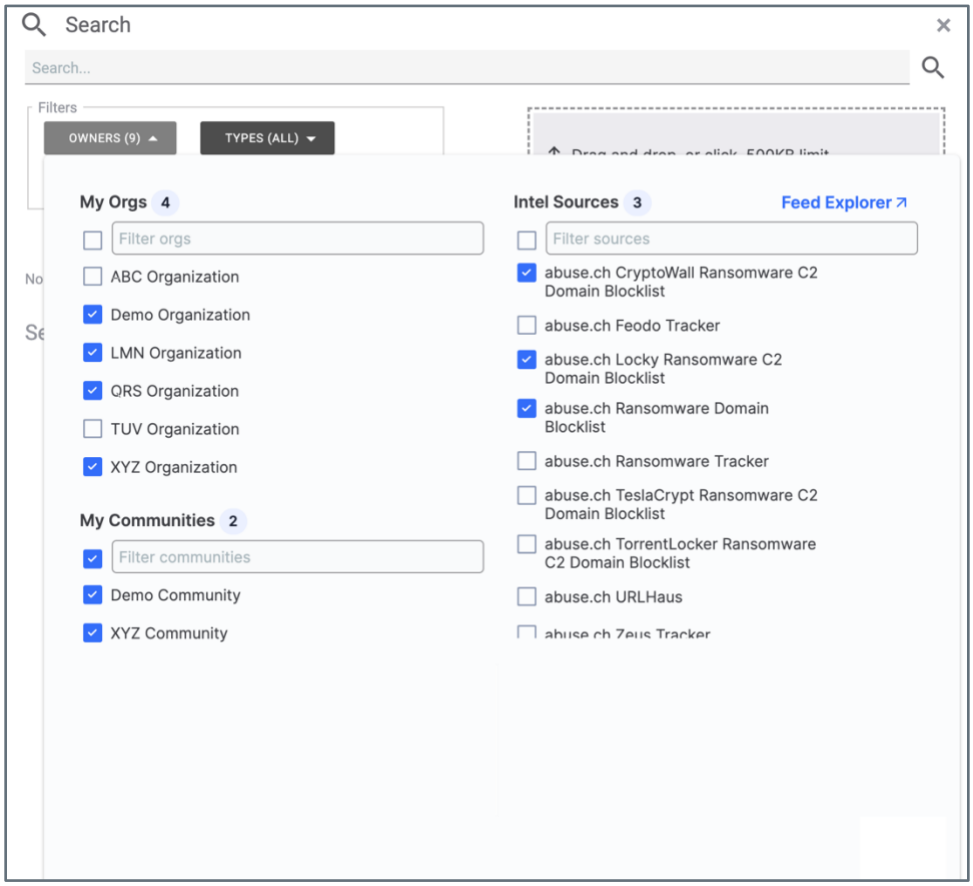

Figure 7

You can also add objects found during searches to any Organization on your instance (Figure 8).

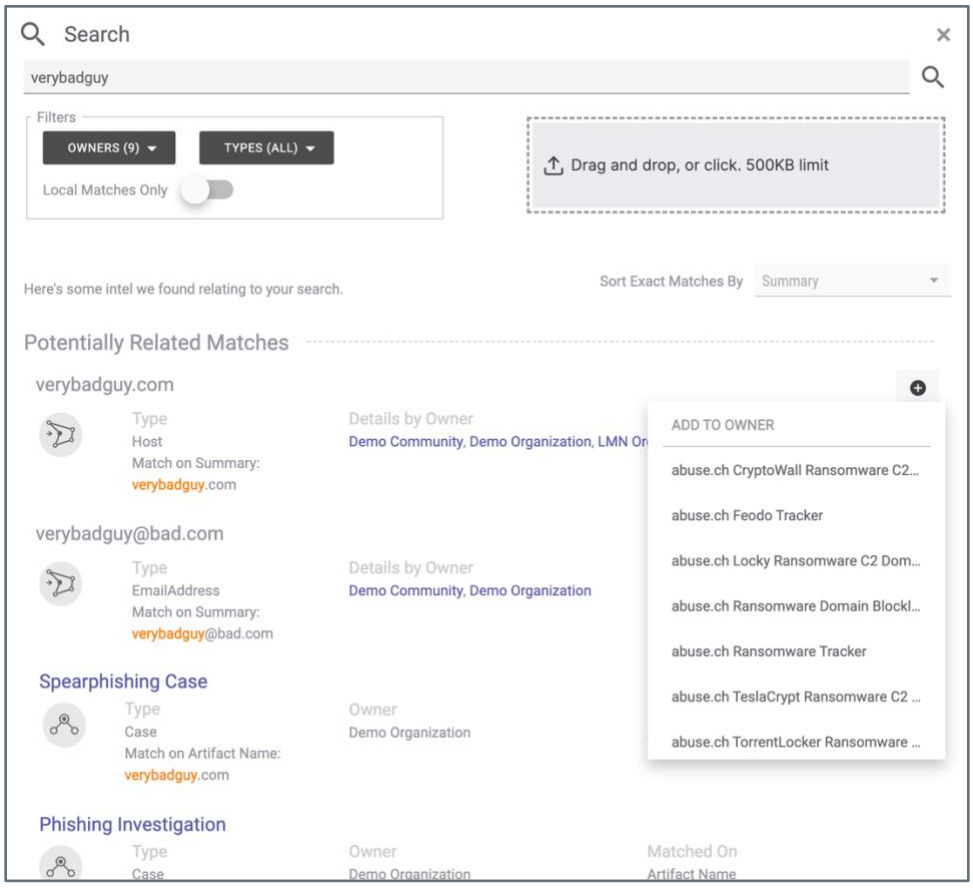

Figure 8

Note: The **ADD TO OWNER** dropdown lists all owners in alphabetical order. It does not separate them by owner type (Organization, Community, and Source). Scroll down to find the owner to which you want to add an object found during a search.

The Details Screen

In addition to Communities and Sources, the **Owners & Feeds** card on the new **Details** screen (Figure 9) and the **Additional Owners** card on the legacy **Details** screen (Figure 10) for an object will list all of the other Organizations that own the object. Click on the name of an Organization to view the object within that Organization.

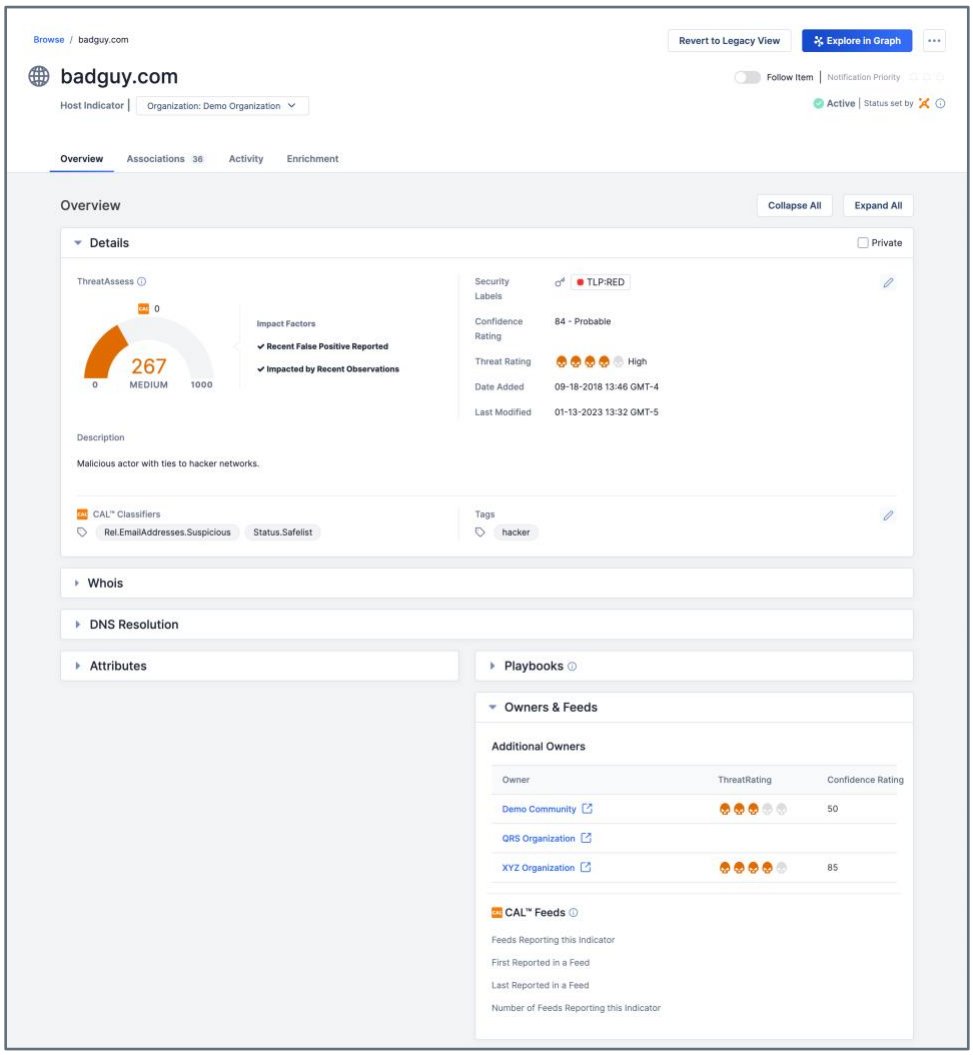

Figure 9

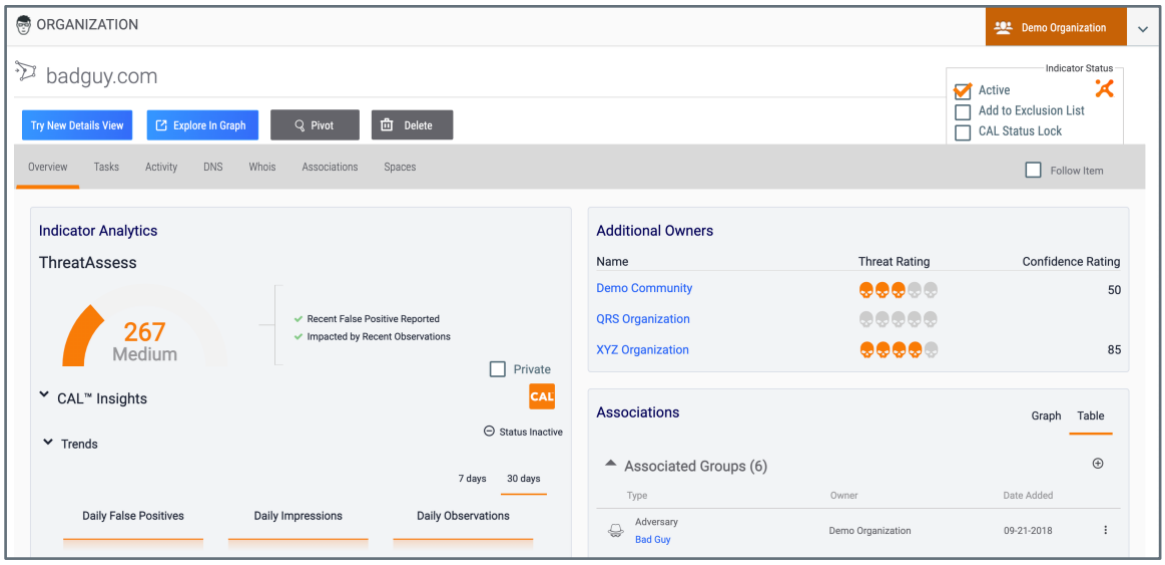

Figure 10

On the new **Details** screen, you can also use the dropdown at the top left of the header section to select the owners in which to view the object. On the legacy **Details** screen, you can also use the selector at the upper-right corner of the screen to choose owners in which to view the object. When viewing the object in an Organization other than your home Organization on the legacy **Details** screen, the label at the upper-left corner of the screen will be **SHARED** instead of **ORGANIZATION**.

Cross-Owner Associations

If cross-owner associations are enabled on your ThreatConnect instance, you can view and create associations between objects in the Organizations on your instance and between those in the Communities and Sources to which you have access. In other words, in addition to being able to create associations between objects in your home Organization, Communities, and Sources, you can create associations between objects in the Organizations on your instance (i.e., Organization-to-Organization associations) and associations between objects in any Organization on your instance and the Communities and Sources to which you have access.

Threat Graph

When viewing the Threat Graph for an object that exists in multiple Organizations on your instance, you can use the **Pivot in ThreatConnect** option to explore the object's associations in each Organization.

ThreatConnect Query Language

You can write TQL queries that search for objects existing in multiple Organizations on your instance. See the "Query for Objects Belonging to Multiple Owners" section of *Constructing Query Expressions* for more information.

ThreatConnect Browser Extension

When selecting sources for the ThreatConnect Browser Extension to scan for potential Indicators and Groups, you can select multiple Organizations on your instance (Figure 11).

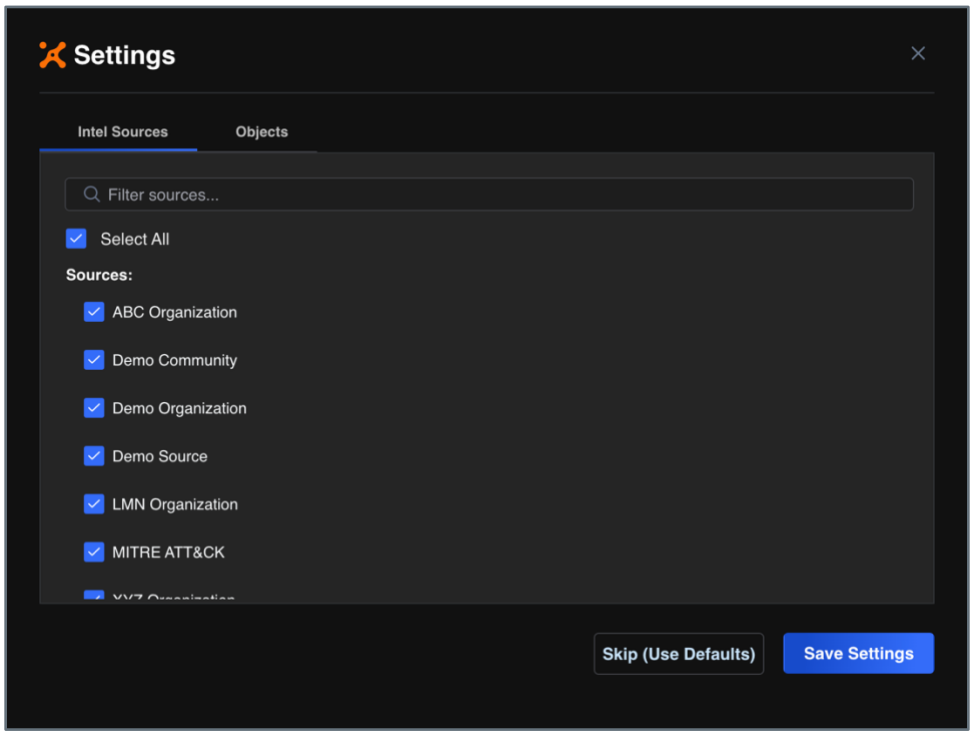

Figure 11

The Browser Extension will indicate when a scan finds objects that are known to exist in multiple Organizations on your instance (Figure 12).

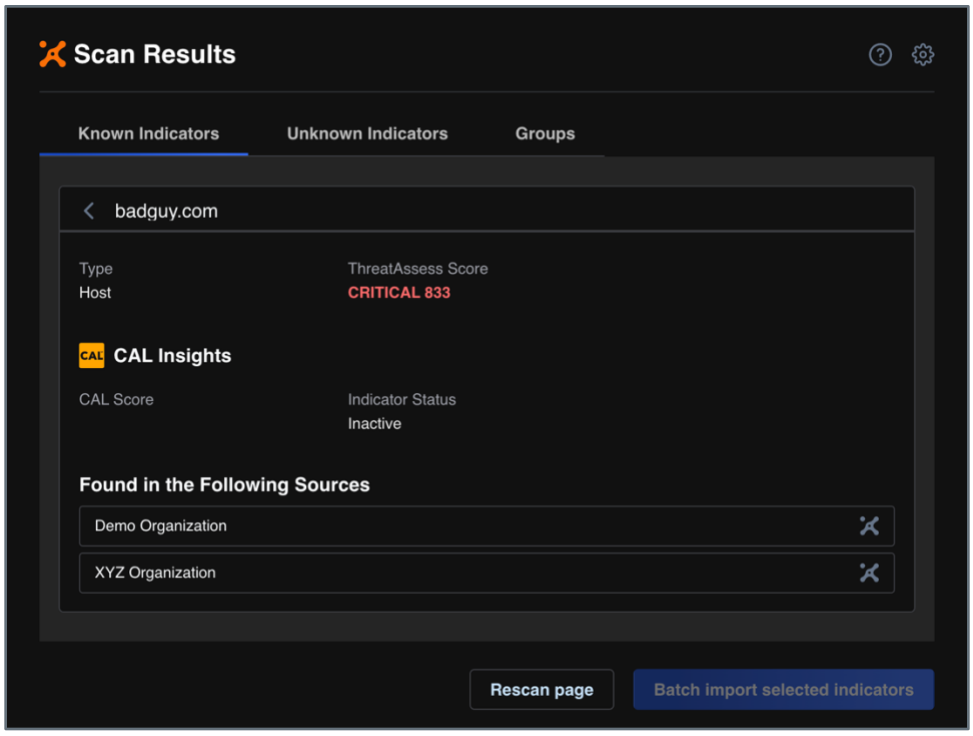

Figure 12

When importing scanned Indicators into ThreatConnect, you can select any Organization on your ThreatConnect instance as the destination owner (Figure 13).

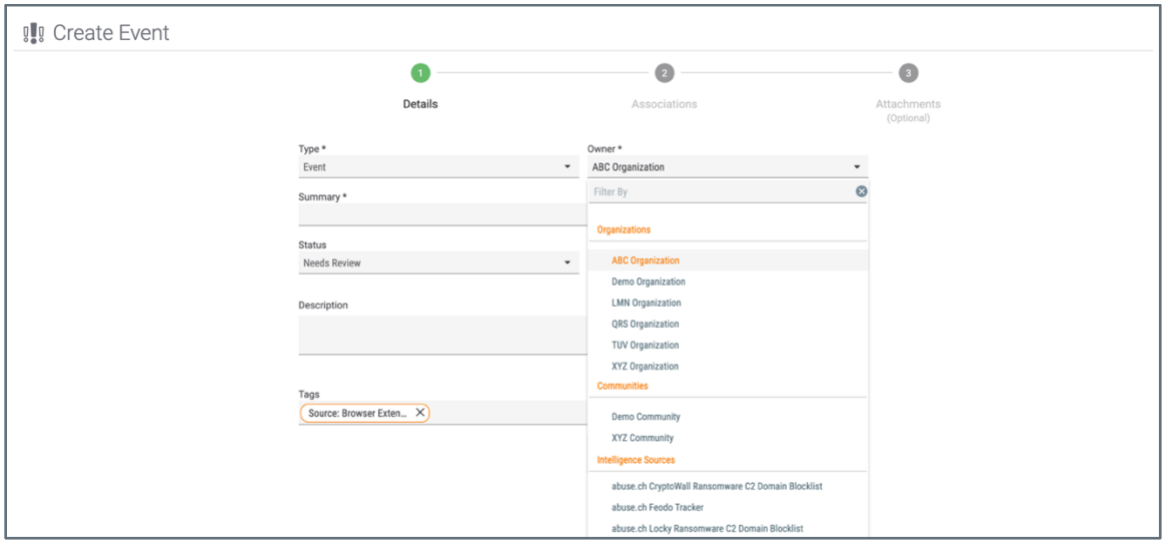

Figure 13

Workflow

As a Super User, you can view, create, modify, assign, and delete Workflow Tasks, Workflows, Templates, and Cases in all Organizations on your ThreatConnect instance.

Workflow Tasks

The Workflow **Tasks** screen will display all Tasks in all Cases in all Organizations on your instance, with the **Org** column indicating the Organization to which each Task belongs (Figure 14).

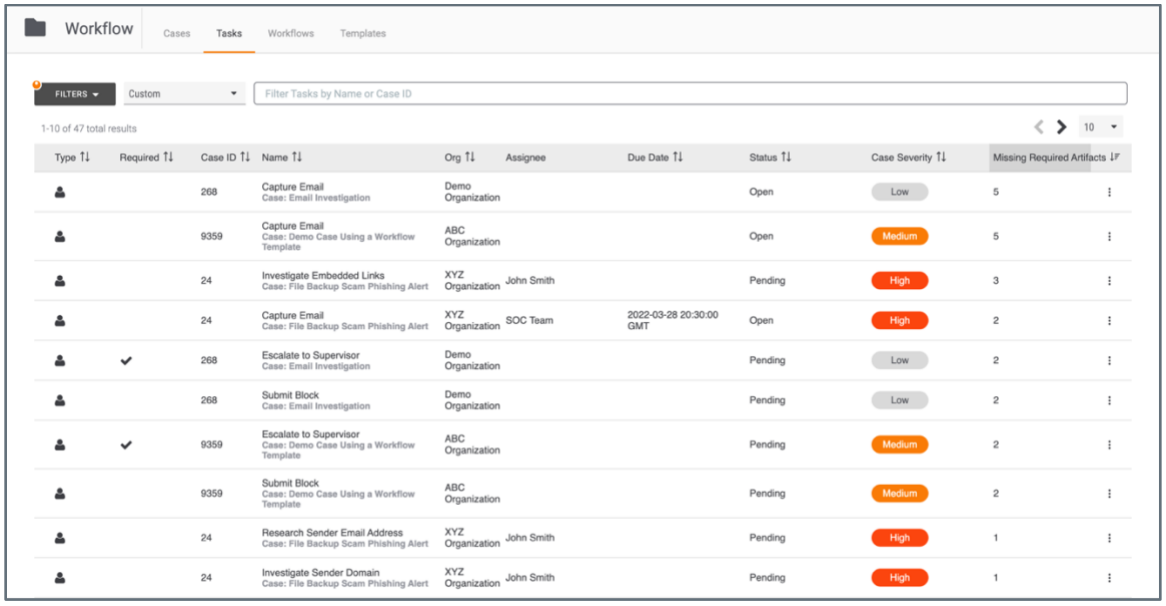

Figure 14

You can use the **Owner(s)** dropdown menu in the **FILTERS** selector to select the Organizations you want to include in the **Tasks** table (Figure 15).

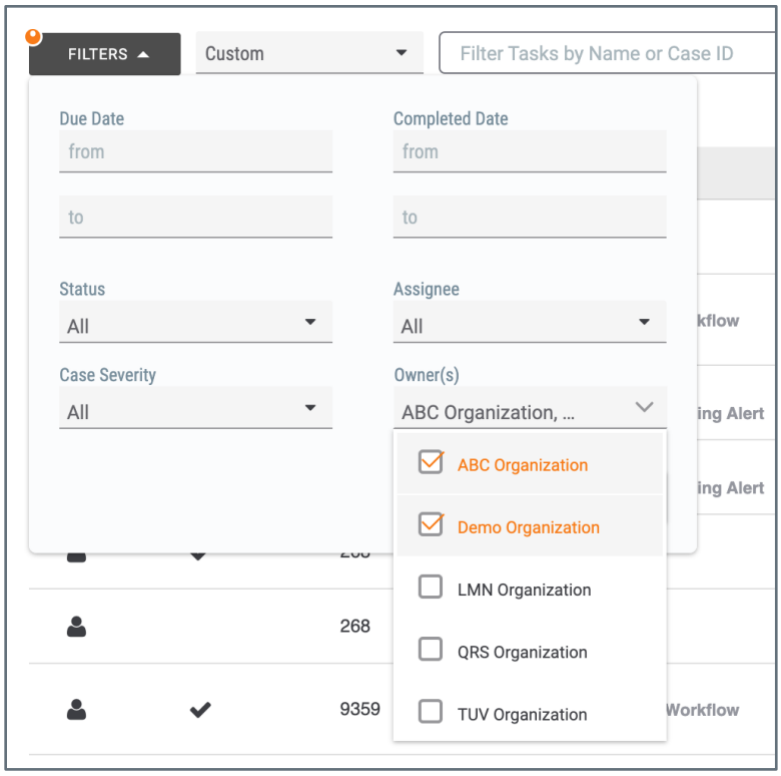

Figure 15

Note: If the Tasks table is blank when you first use your Super User account to access the **Tasks** screen, this may be because there are no Organizations selected in the **Owner(s)** menu. Selecting at least one Organization will cause the table to populate (as long as the selected owners contain at least one Case with at least one Task in it).

You can select an assignee for any Task in any Case, but the assignee must belong to the Organization that owns the Case.

Workflows

The Workflows Screen

The **Workflows** screen will display all Workflows in all Organizations on your instance, with the text at the top left of each Workflow card indicating the Organization to which the Workflow belongs (Figure 16).

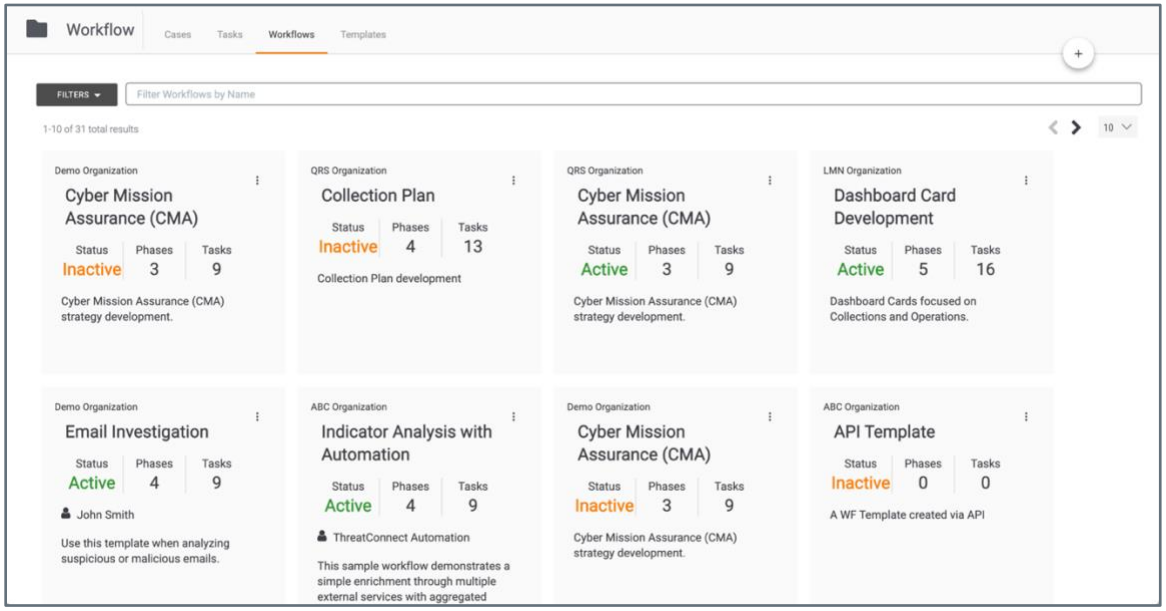

Figure 16

You can use the **Owner(s)** dropdown menu in the **FILTERS** selector to select the Organizations you want to include in the **Workflows** table (Figure 17).

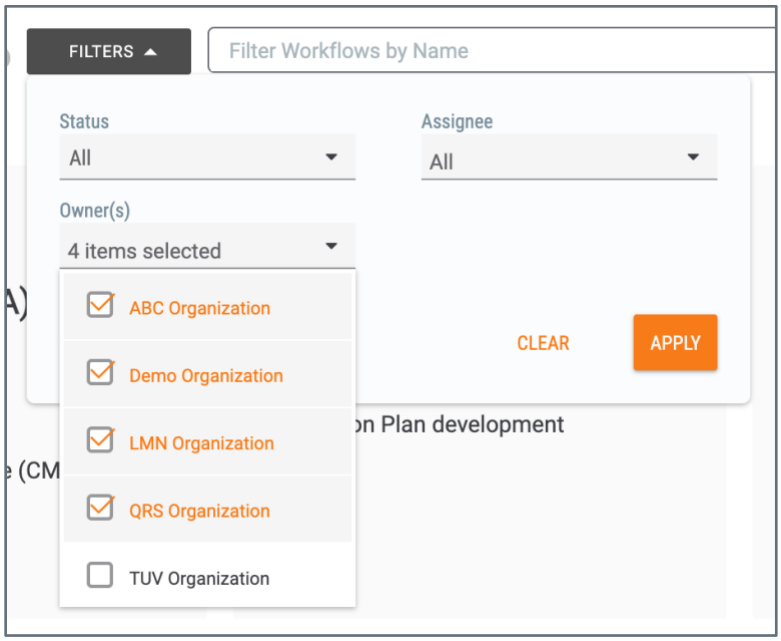

Figure 17

Note: If the **Workflows** table is blank when you first use your Super User account to access the Workflows screen, this may be because there are no Organizations selected in the **Owner(s)** menu. Selecting at least one Organization will cause the table to populate (as long as the selected owners contain at least one Workflow).

Creating a Workflow

When creating a new Workflow, you must select the Organization that will own the Workflow (Figure 18).

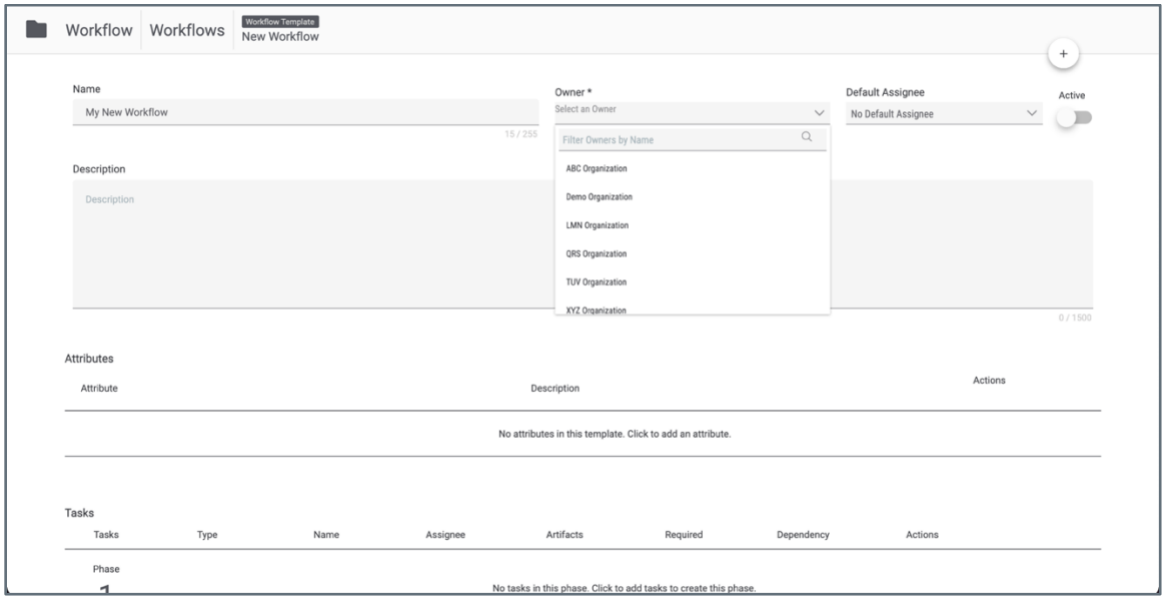

Figure 18

Note: The **Default Assignee** menu will not populate until you select an owner, because the default assignee must belong to the Organization that owns the Workflow. Similarly, when you assign a Task in the Workflow, the **Default Assignee** dropdown menu will list only users who are in the Organization that owns the Workflow.

Importing a Workflow

When importing a Workflow, you must select the Organization that will own the Workflow (Figure 19).

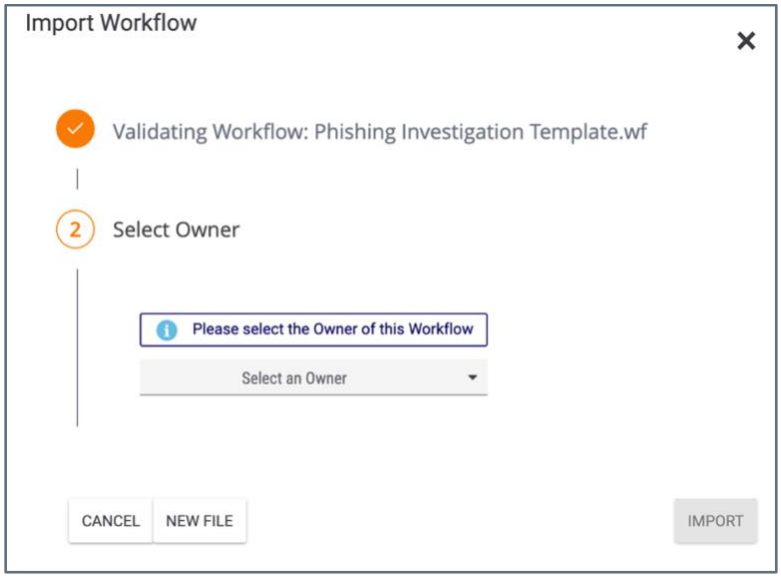

Figure 19

Note: In addition to the **Validating Workflow** and **Select Owner** steps, you may see steps labeled **Variables** or **Missing Apps**. See the "Importing a Workflow" section of *The Workflows Screen* for more information.

Sharing a Workflow across Organizations

As a Super User, you can easily share Workflows across Organizations. On the **Workflows** screen, select the **Duplicate** option from the vertical ellipsis menu for a Workflow. Enter a name for the Workflow, and then select the destination Organization from the **Select Owner** menu (Figure 20).

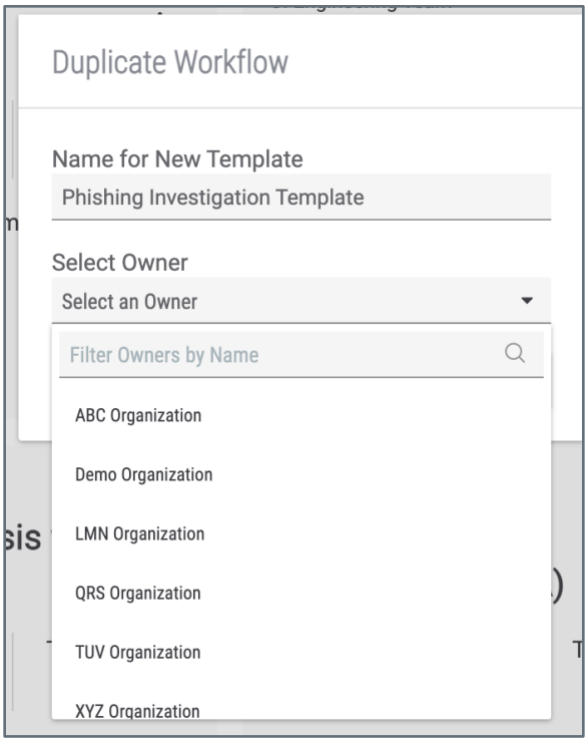

Figure 20

Workflow Templates

The Templates Screen

The **Templates** screen will display all System-level and TC Exchange™ Templates that you can copy to an Organization as a Workflow. To view TC Exchange Templates, toggle the **TC Exchange Templates** slider on, as in Figure 21. Toggling this slider off will display all Templates installed at the System level in your ThreatConnect instance.

Copying a Template to an Organization

When copying a System-level or TC Exchange Template to an Organization as a Workflow, you must select the destination Organization (Figure 21).

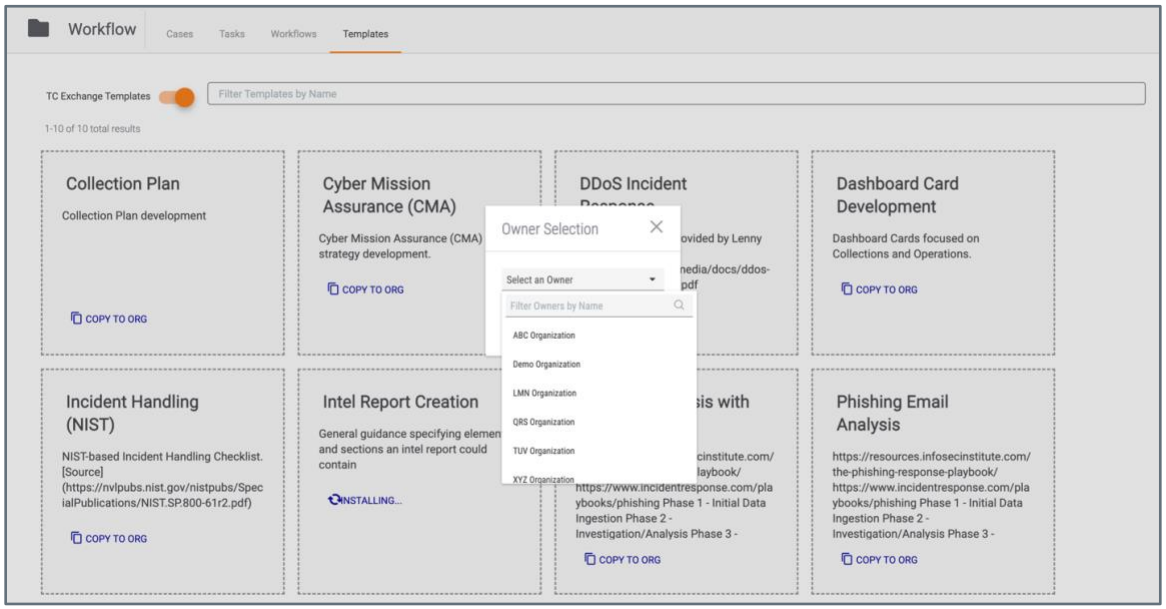

Figure 21

Workflow Cases

The Cases Screen

The Workflow **Cases** screen will display all Cases in all Organizations on your instance, with the **Org** column indicating the Organization to which each Case belongs (Figure 22).

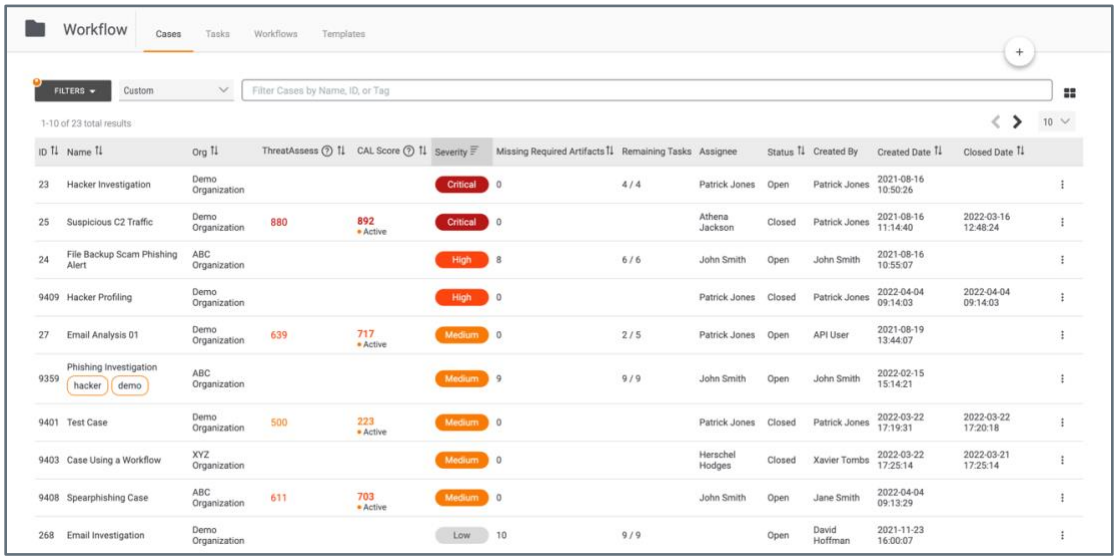

Figure 22

In card view, the Organization that owns the Case is displayed at the top of the Case's card (Figure 23).

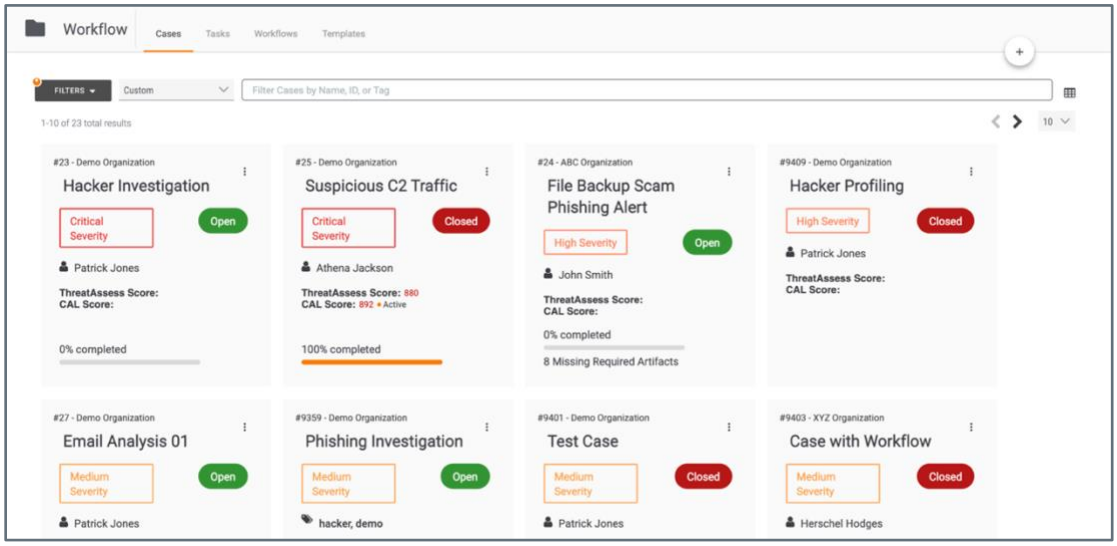

Figure 23

You can use the **Owner(s)** dropdown menu in the **FILTERS** selector to select the Organizations you want to include in the **Cases** table (Figure 24).

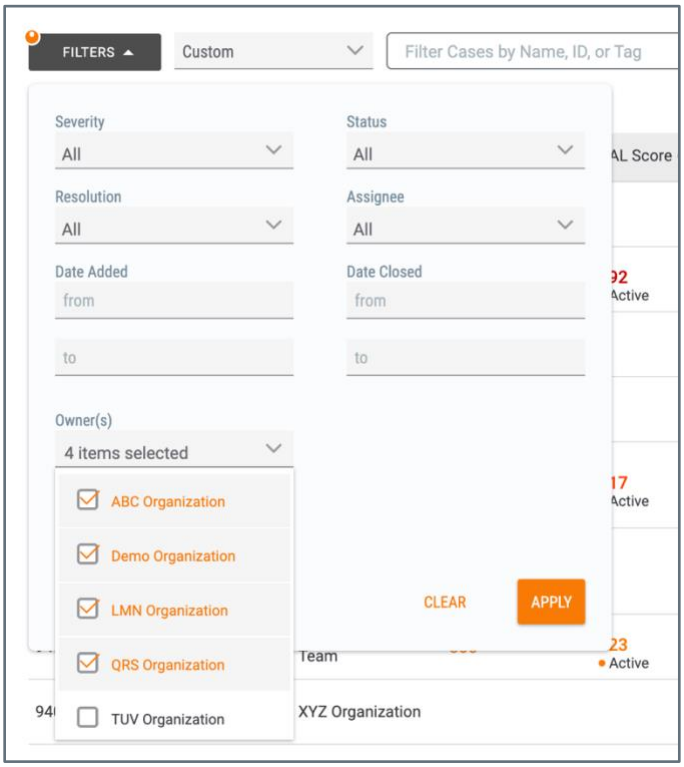

Figure 24

Note: If the **Cases** screen is blank when you first use your Super User account to access the **Cases** screen, this may be because there are no Organizations selected in the **Owner(s)** menu. Selecting at least one Organization will cause the screen to populate (as long as the selected owners contain at least one Case).

Creating a Case

When creating a new Case, you must select the Organization that will own the Case (Figure 25).

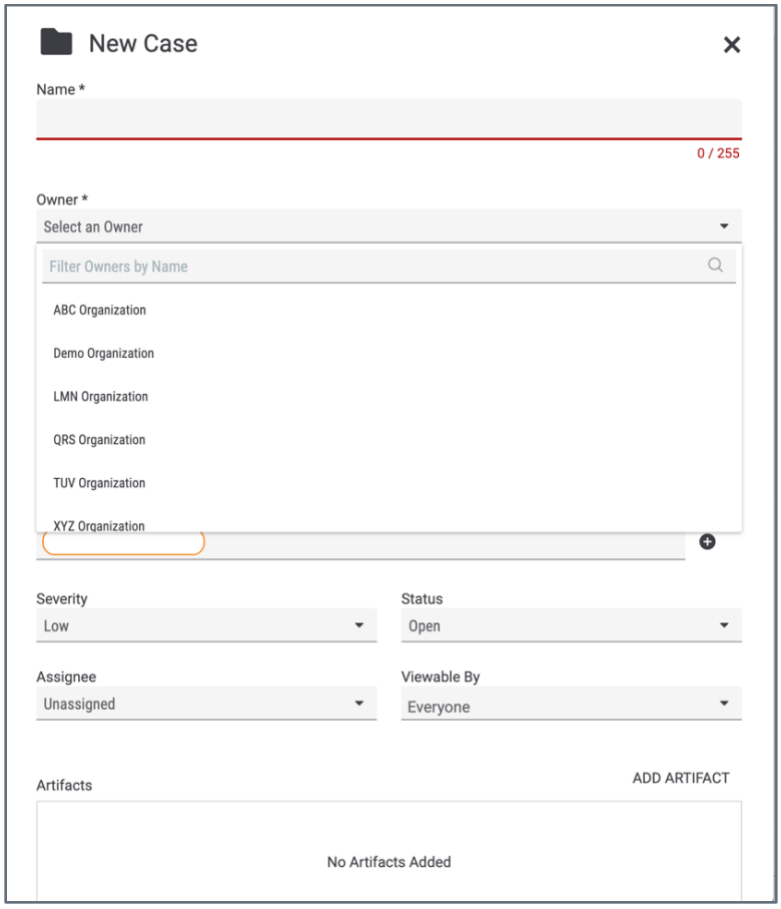

Figure 25

Note: The **Assignee** menu will not populate with any options besides **Unassigned** until you select an owner, because the assignee must belong to the Organization that owns the Case. Similarly, when you assign a Task in the Case, the **Assignee** dropdown menu will list only users who are in the Organization that owns the Case.

Viewing a Case

When you view a Case, you will see the Organization that owns the Case at the top left of the screen (Figure 26).

Figure 26

Viewing Artifact Owners

If an Artifact that is a ThreatConnect Indicator type exists in multiple Organizations on your instance, you can view the Organizations in the dropdown list in the **Summary** column (Figure 27).

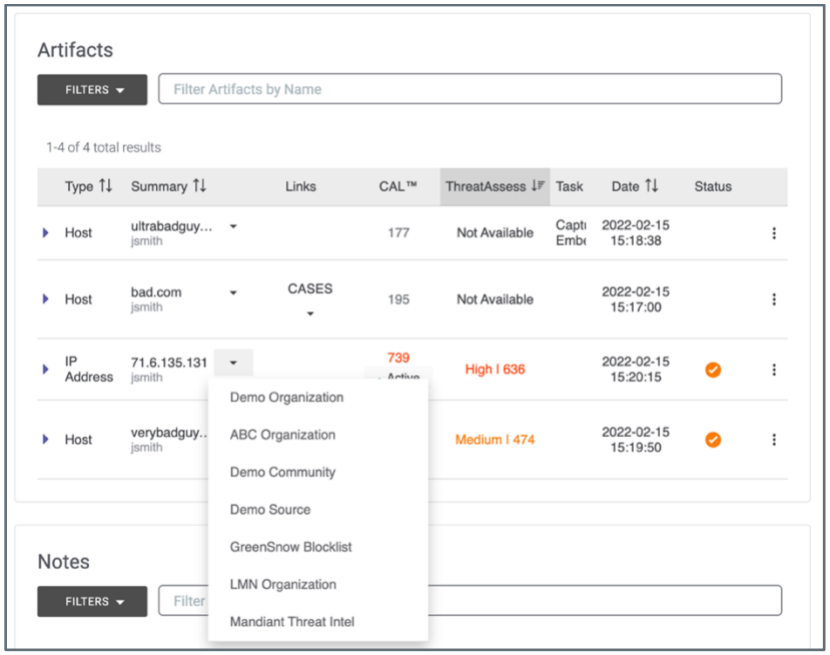

Figure 27

Click on an Organization's name in the list to view the **Details** drawer for the Indicator in that Organization.

Note: If an Artifact that is a ThreatConnect Indicator type exists in multiple owners, including multiple Organizations, only the Indicator in your home Organization and the copies in Communities and Sources for which potential Case associations are enabled will be suggested as potential associations for the Case being viewed.

Playbooks

For a Super User, the **Playbooks** screen will display all Playbooks in all Organizations on your instance, with the **Organization** column indicating the Organization to which each Playbook belongs (Figure 28).

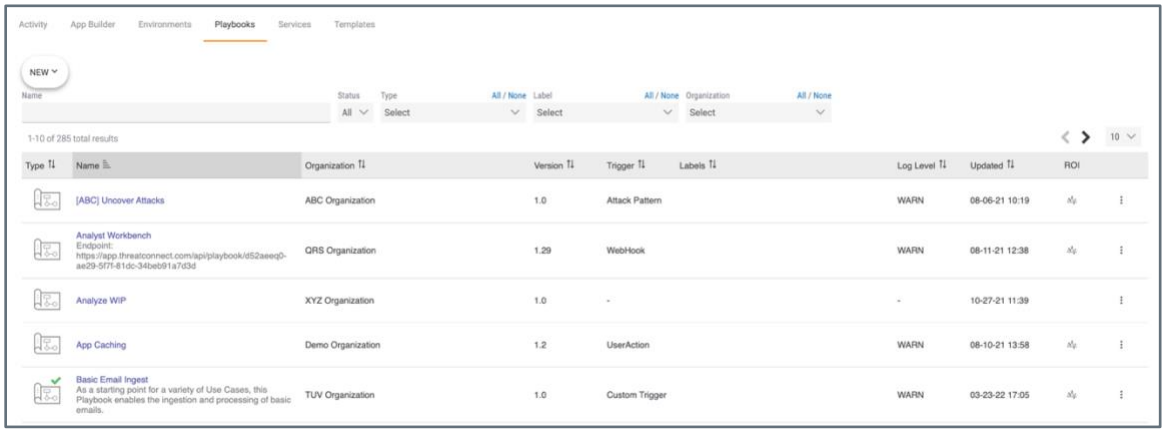

Figure 28

You can use the **Organization** dropdown menu along the top of the screen to select the Organizations you want to include in the **Playbooks** table (Figure 29).

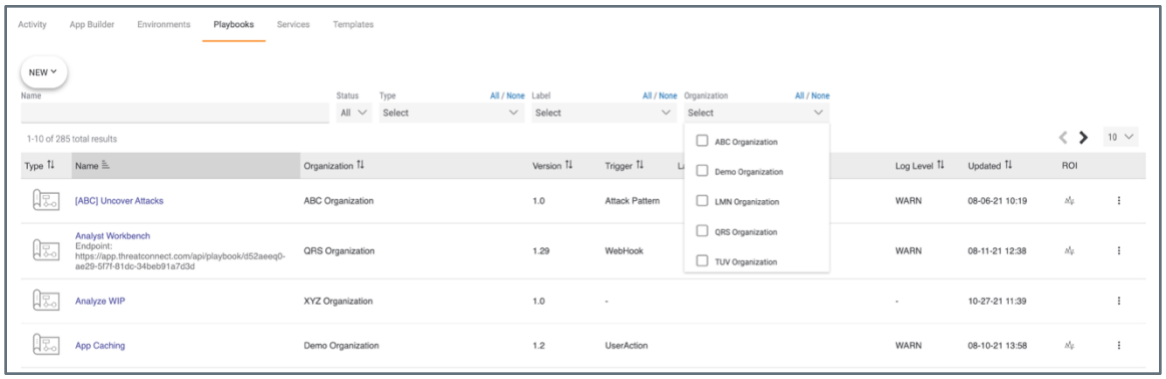

Figure 29

Creating a Playbook

When creating a new Playbook (including a Playbook Component or Workflow Playbook), you must select the Organization that will own the Playbook (Figure 30).

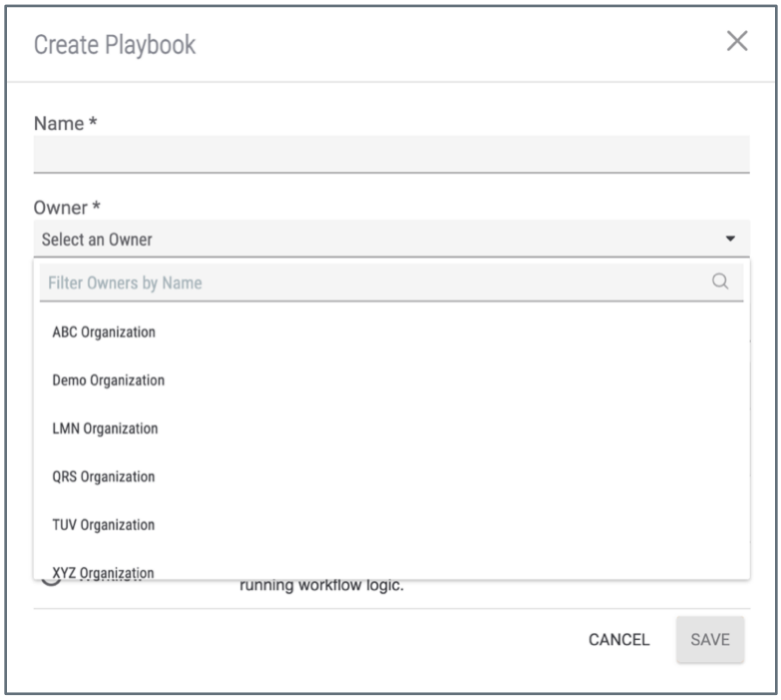

Figure 30

Importing a Playbook

When importing a Playbook, you must select the Organization that will own the Playbook (Figure 31).

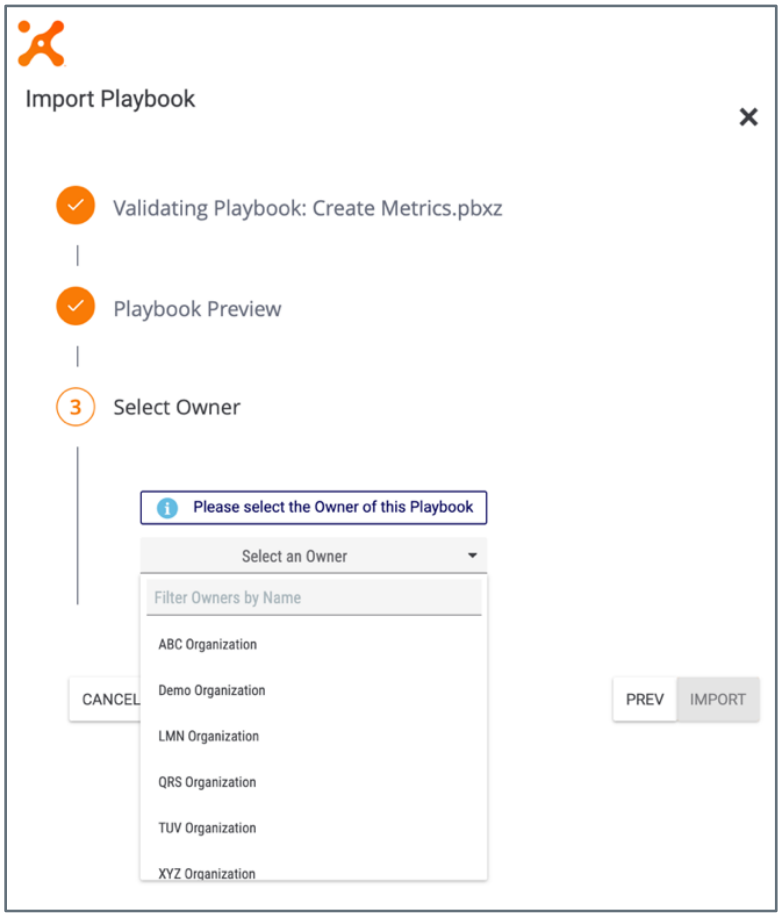

Figure 31

You can easily share a Playbook from one Organization to another by exporting the Playbook, or by generating a Share Token, and then immediately importing it into another Organization.

Viewing a Playbook

When you view a Playbook, you will see the Organization that owns the Playbook at the upper-right corner of the **Playbook Designer** (Figure 32).

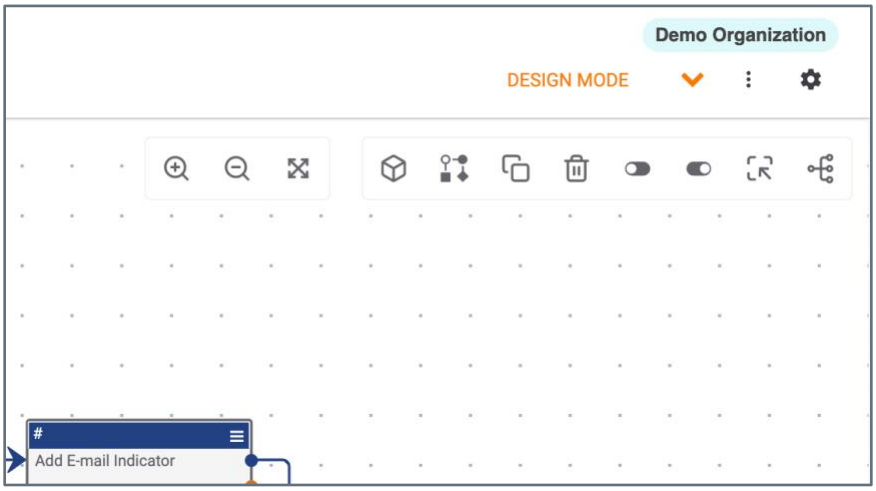

Figure 32

When you are working in a Playbook, the features of that Playbook will be specific to the Organization that owns the Playbook. For example, only the Apps that are available for use in the owning Organization will be available to the Playbook. Similarly, when using the **Run As** App menu option or the Playbook settings menu option to run an App or Playbook, respectively, as a different user, only users in the owning Organization will be available in those menus.

Playbook Templates

When importing a Playbook Template as a Playbook, you must select the Organization that will own the Playbook (Figure 33).

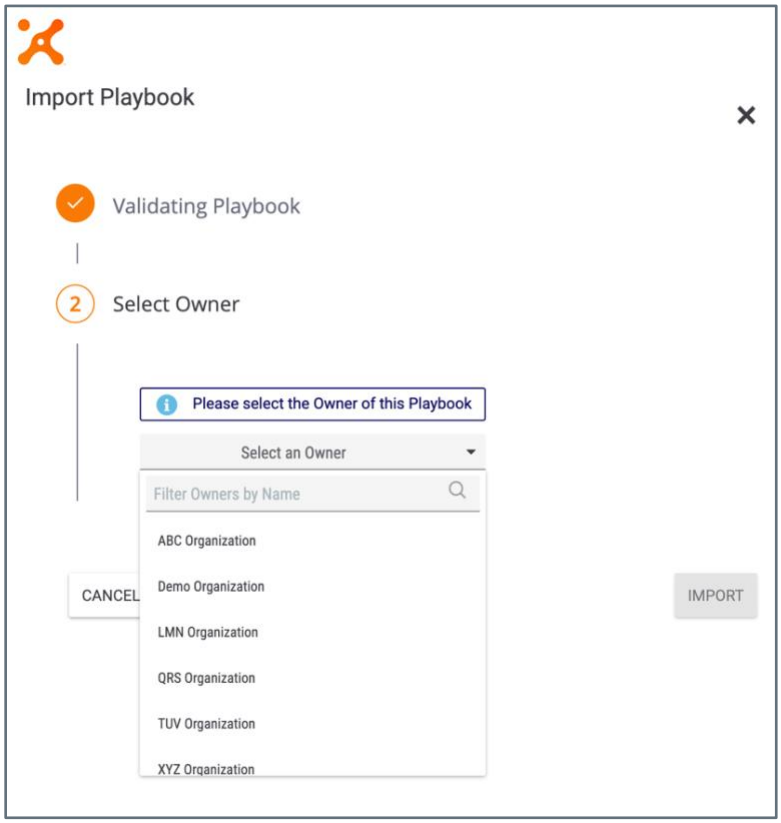

Figure 33

Administration and Configuration of All Organizations

Your Super User account has a System role of Super User and an Organization role of Organization Administrator. This combination of roles means that you are an Organization Administrator for every Organization on your ThreatConnect instance, allowing you to view, modify, and manage the **Organization Settings** and **Organization Config** screens for all Organizations. See *ThreatConnect Organization Administration Guide* for more information on the functionalities and permissions available to Organization Administrators.

Organization Settings

Viewing Organization Settings

When you click the **Org Settings** option in the **Settings** menu, the **Membership** tab of the **Organization Settings** screen for your home Organization will be displayed (Figure 34).

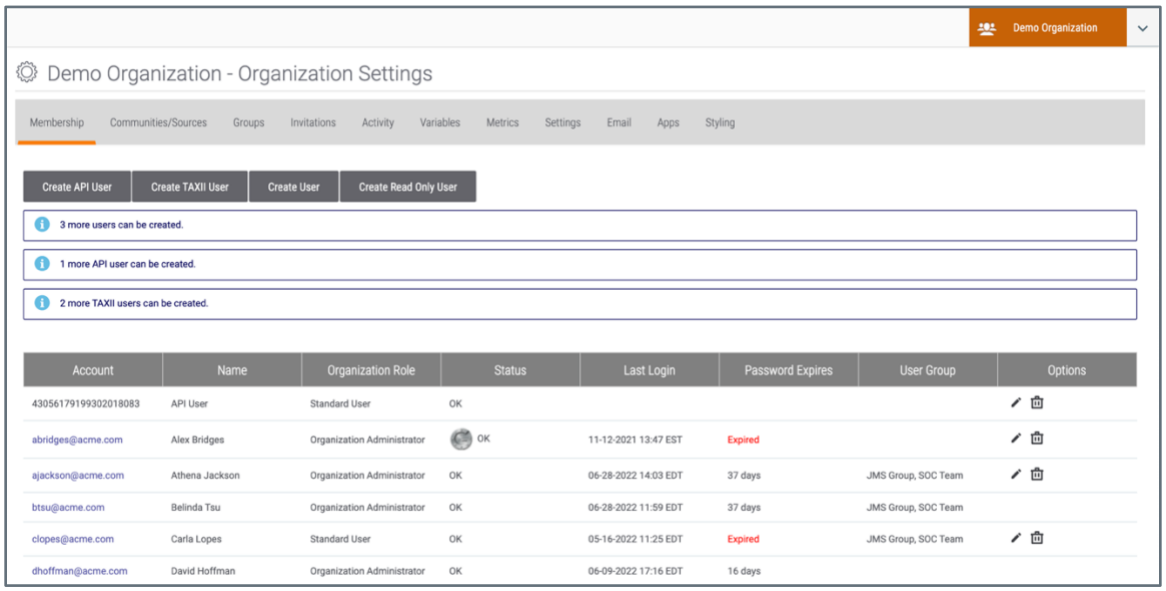

Figure 34

You have full access to all tabs of this screen for every Organization on your instance. To view this screen for a different Organization, choose the desired Organization from the selector at the upper-right corner of the screen.

Managing User Accounts

When creating a user account, the System role for the account will automatically be **User**, and you will not have a menu to select a different System role, nor will you be able to view user System roles in the table on the **Membership** tab of the **Organization Settings** screen. You also will not be able to modify or delete users with a System role that is higher than yours.

Organization Activity

The **Activity** tab of the **Organization Settings** screen logs all user activity in an Organization. When you perform an activity (e.g., create an Indicator) in an Organization other than your home Organization, other members of that will not see your name as part of the log entry. Instead, the activity will be attributed to your Organization (e.g., **Host bad.com was created by Demo Organization**).

Organization Configuration

When you click the **Org Config** option in the **Settings** menu, the **Attribute Types** tab of the **Organization Config** screen for your home Organization will be displayed (Figure 35).

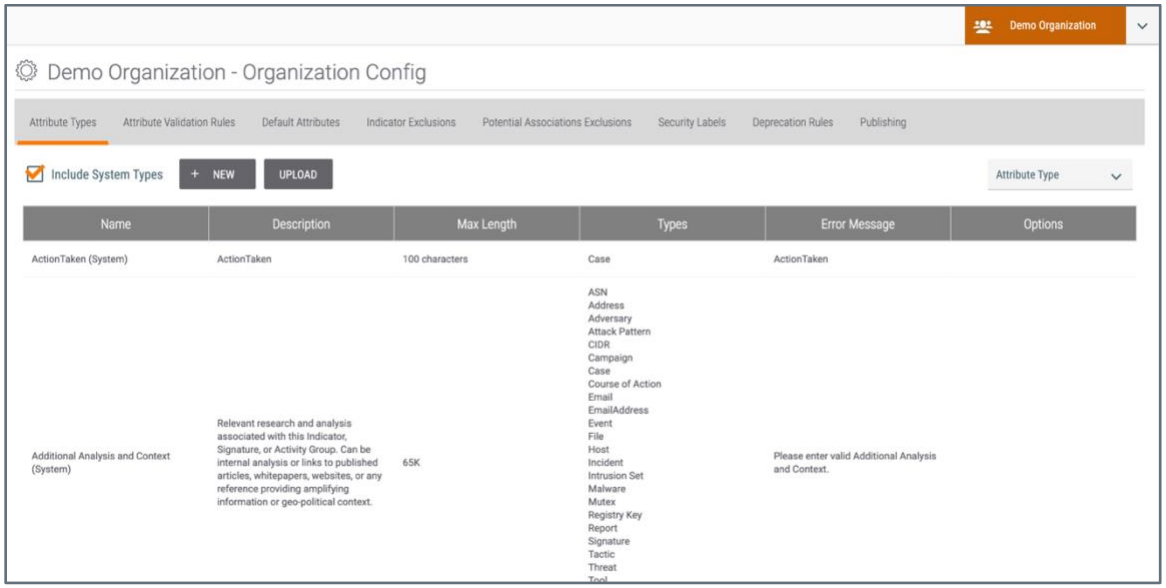

Figure 35

You have full access to all tabs of this screen for every Organization on your instance. To view this screen for a different Organization, choose the desired Organization from the selector at the upper-right corner of the screen.