NOVEMBER 2021

Role Based Access Control

Feature Design Plan

Bella Jones

UX / UI Designer

Key Use Cases

As an administrative user, I want to be able to do the following:

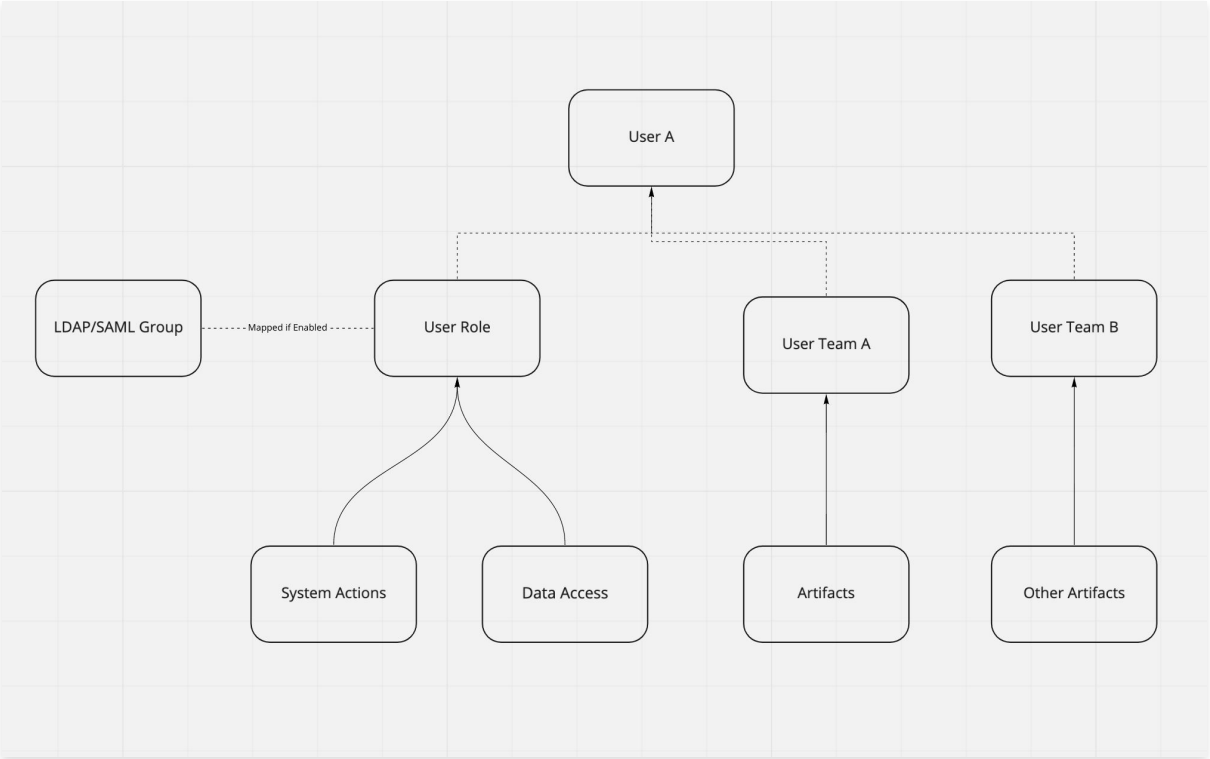
1. **Data Access Control** - I want to be able to restrict user access to data within TQ using TLP and or custom markings so that I can have proper separation of privileges to certain data in my system that is more sensitive than other data. At the same time, I still want to allow ease of access and collaboration across various user types.

2. **Action Control** - I want to restrict access to certain actions within TQ based on user roles.

3. **Custom Roles** - I want to be able to create additional custom roles within the TQ UI so that I can more granularly control RBAC.

4. **Custom User Groups** - I want to be able to create buckets of users for the purposes of sharing artifacts such as investigations, dashboards, or data collections.

Building a Conceptual Framework



RBAC Conceptual Framework

- Users can only possess a single Role at a time
- Users can be members of more than one Team at a time
- Teams can contain multiple users with differing Roles
- If the system has LDAP or SAML enabled, Admins will be able to map those User Groups to TQ Roles

Defining Key Concepts & Terminology

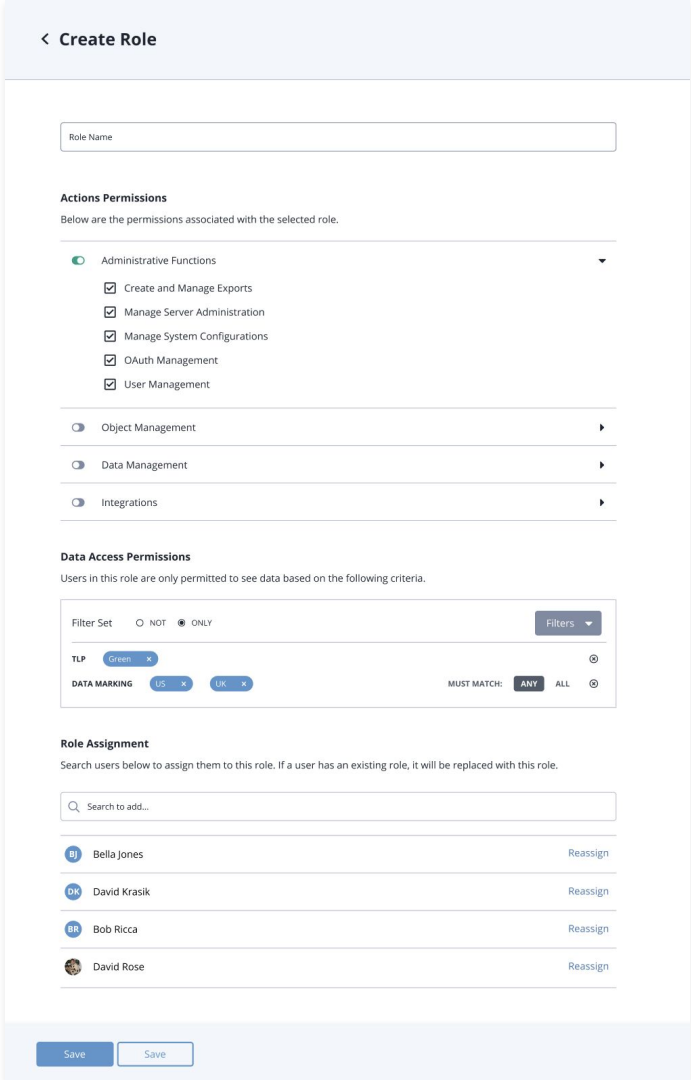
Term	Definition
User Role	A user's role defines what permissions the user has to perform actions in the system or access data (at the object level) in the system. A user can only have a single Role in the system at a time.
User Team	A bucket of users assembled for the purposes of sharing artifacts such as dashboards, investigations, and data collections. A user can be a part of multiple Teams in the system.
Artifact	A "filtered view" of data, such as a dashboard, data collection, or investigation.
Actions Permissions	The various actions that a user is permitted to take in the system, as defined by their role.
Data Access Permissions	The object-level data that a user is permitted to see in the system, as defined by their role.
Data Marking	A custom data characteristic that can be used to define a user's Data Access Permissions. It's designation on object data will be configurable in a similar way to TLP, but will be an object-level characteristic, rather than granular.

High Fidelity Designs

Custom Roles: Action Controls + Data Access Permissions

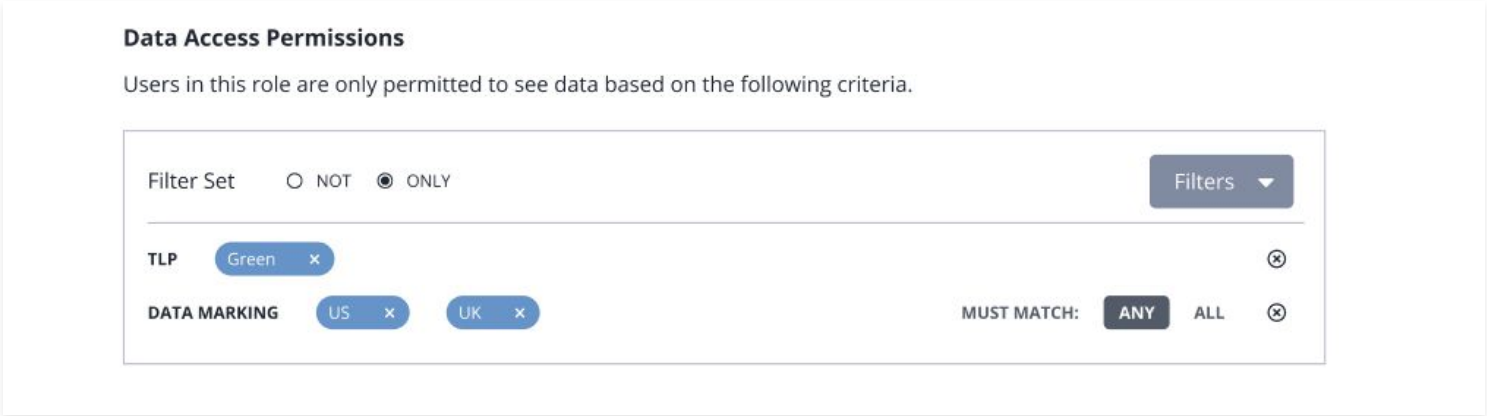
- Admins can create custom user Roles defined by Action permissions and Data Access permissions

- Action Permissions are categorized so that users can enable an entire category or have more granular controls for each



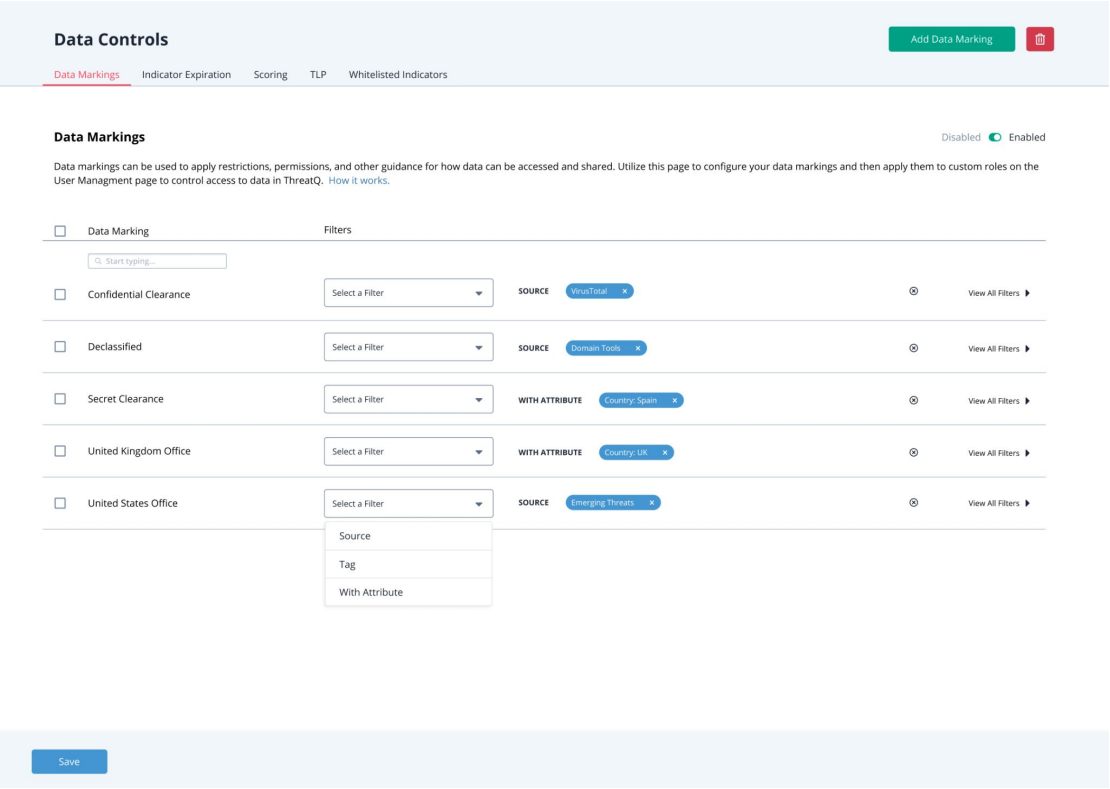
High Fidelity Designs

Custom Roles: Action Controls + Data Access Permissions



- Data Access Permissions will allow users to manage access to data based on TLP, Object Type, or Data Markings
- Users can define permissions to the data as either restrictive (NOT) or permissive (ONLY)

High Fidelity Designs



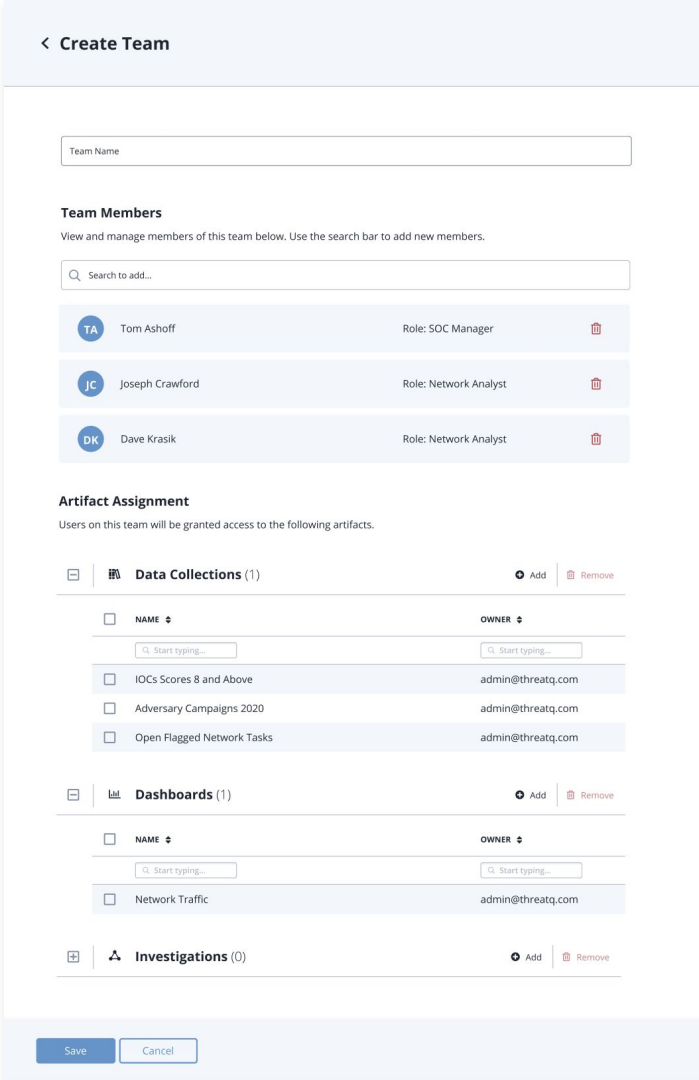
Managing Data Markings

- Custom data markings will be Object-level designations
- Admins users will be able to configure these much like TLP
- Users can assign by Source, Tag, or Attribute
- These markings will enable sharing with users based on geographic region, clearance level, or any other criteria the customer needs to use for grouping data access

High Fidelity Designs

Custom Teams: Artifact Assignment & Sharing

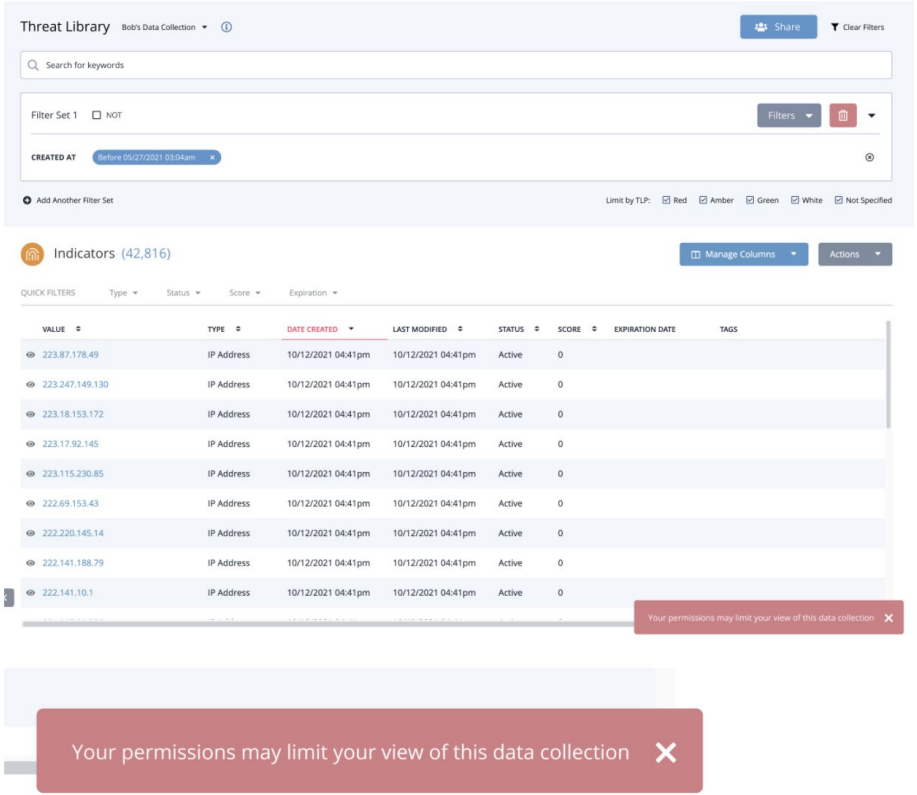
- Admins can create user Teams, or “buckets of users” for sharing and assigning artifacts such as investigations, dashboards, and data collections
- Users with differing Roles can belong to the same Team
- If a user’s Role permissions prevent them from seeing some or all of the data in an artifact:
  - The artifact can still be shared with/assigned to them
  - When they go to view it, the data that returns will be filtered according to that user’s Data Access permissions



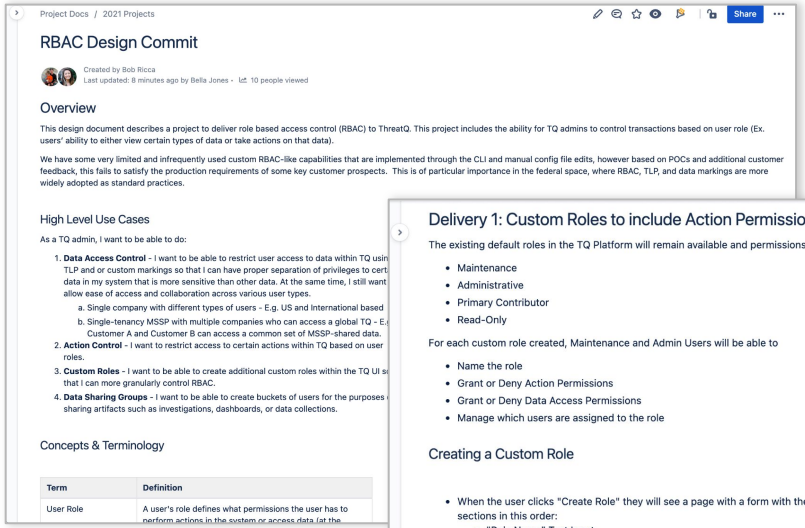
High Fidelity Designs

Role Permissions Application

- Users will not be prevented from seeing artifacts themselves, rather their permissions will apply when they try to view the data within an artifact
- For example, if a user attempts to view a data collection and their role permissions prevent them from viewing some or all of the data in the collection, then they will see a message notifying them of this limitation



Design Commit Complete



Project Docs / 2021 Projects

Share

RBAC Design Commit

Created by Bob Ricca
Last updated: 8 minutes ago by Bella Jones • 10 people viewed

Overview

This design document describes a project to deliver role based access control (RBAC) to ThreatQ. This project includes the ability for TQ admins to control transactions based on user role (Ex. users' ability to either view certain types of data or take actions on that data).

We have some very limited and infrequently used custom RBAC-like capabilities that are implemented through the CLI and manual config file edits, however based on POCs and additional customer feedback, this fails to satisfy the production requirements of some key customer prospects. This is of particular importance in the federal space, where RBAC, TLP, and data markings are more widely adopted as standard practices.

High Level Use Cases

As a TQ admin, I want to be able to do:

1. **Data Access Control** - I want to be able to restrict user access to data within TQ usin
   TLP and or custom markings so that I can have proper separation of privileges to cert
   data in my system that is more sensitive than other data. At the same time, I still want
   allow ease of access and collaboration across various user types.
   a. Single company with different types of users - E.g. US and International based
   b. Single-tenancy MSSP with multiple companies who can access a global TQ - E.
      Customer A and Customer B can access a common set of MSSP-shared data.
2. **Action Control** - I want to restrict access to certain actions within TQ based on user roles.
3. **Custom Roles** - I want to be able to create additional custom roles within the TQ UI s
   that I can more granularly control RBAC.
4. **Data Sharing Groups** - I want to be able to create buckets of users for the purposes
   sharing artifacts such as investigations, dashboards, or data collections.

Concepts & Terminology

Term	Definition
User Role	A user's role defines what permissions the user has to perform actions in the system or access data (at the

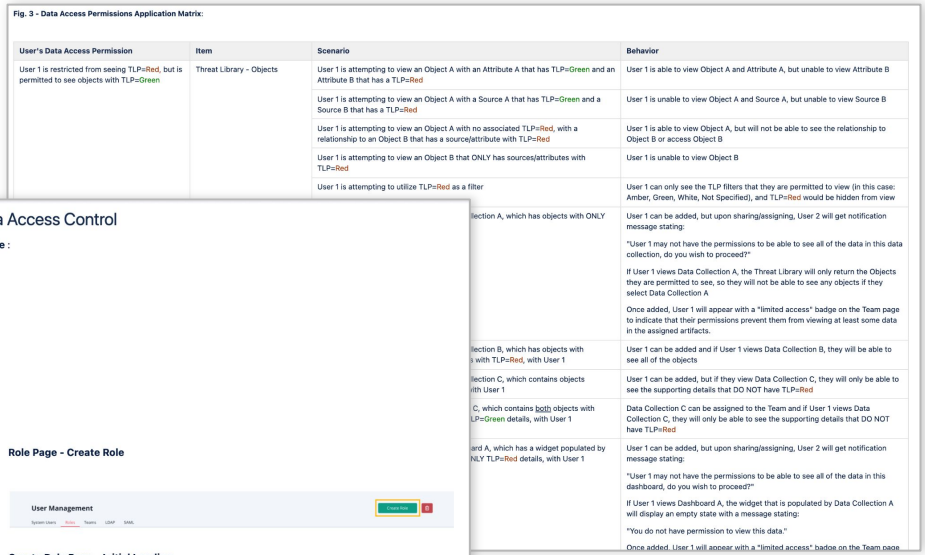
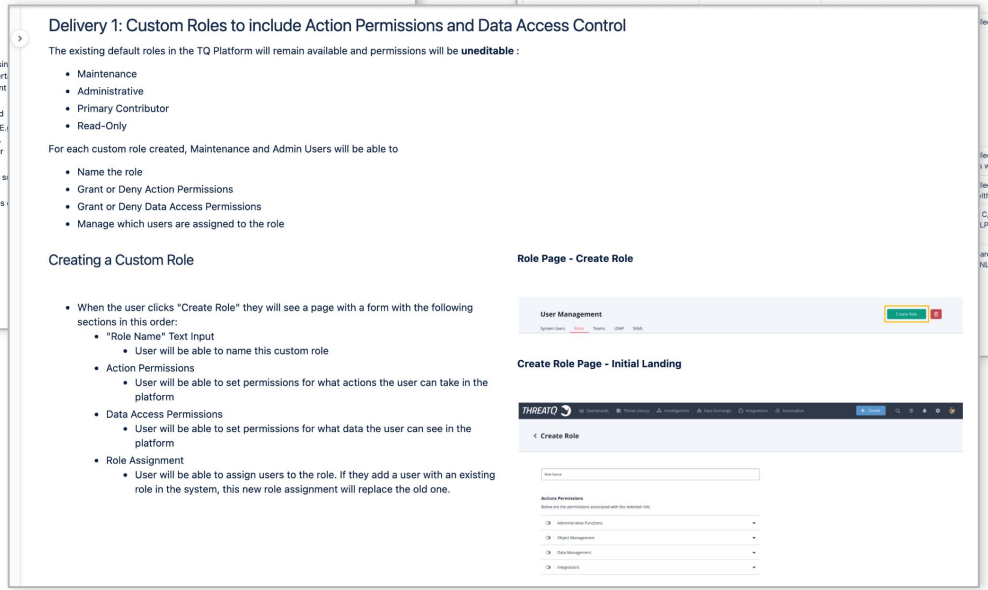


Fig. 3 - Data Access Permissions Application Matrix:

User's Data Access Permission	Item	Scenario	Behavior
User 1 is restricted from seeing TLP=Red, but is permitted to see objects with TLP=Green	Threat Library - Objects	User 1 is attempting to view an Object A with an Attribute A that has TLP=Green and an Attribute B that has a TLP=Red	User 1 is able to view Object A and Attribute A, but unable to view Attribute B
		User 1 is attempting to view an Object A with a Source A that has TLP=Green and a Source B that has a TLP=Red	User 1 is unable to view Object A and Source A, but unable to view Source B
		User 1 is attempting to view an Object A with no associated TLP=Red, with a relationship to an Object B that has a source/attribute with TLP=Red	User 1 is able to view Object A, but will not be able to see the relationship to Object B or access Object B
		User 1 is attempting to view an Object B that ONLY has sources/attributes with TLP=Red	User 1 is unable to view Object B
		User 1 is attempting to utilize TLP=Red as a filter	User 1 can only see the TLP filters that they are permitted to view (in this case: Amber, Green, White, Not Specified), and TLP=Red would be hidden from view
		lection A, which has objects with ONLY	User 1 can be added, but upon sharing/assigning, User 2 will get notification message stating: "User 1 may not have the permissions to be able to see all of the data in this data collection, do you wish to proceed?" If User 1 views Data Collection A, the Threat Library will only return the Objects they are permitted to see, so they will not be able to see any objects if they select Data Collection A Once added, User 1 will appear with a "limited access" badge on the Team page to indicate that their permissions prevent them from viewing at least some data in the assigned artifacts.
		lection B, which has objects with with TLP=Red, with User 1	User 1 can be added and if User 1 views Data Collection B, they will be able to see all of the objects
		lection C, which contains objects ith User 1	User 1 can be added, but if they view Data Collection C, they will only be able to see the supporting details that DO NOT have TLP=Red
		C, which contains both objects with LP=Green details, with User 1	Data Collection C can be assigned to the Team and if User 1 views Data Collection C, they will only be able to see the supporting details that DO NOT have TLP=Red
		ard A, which has a widget populated by NLY TLP=Red details, with User 1	User 1 can be added, but upon sharing/assigning, User 2 will get notification message stating: "User 1 may not have the permissions to be able to see all of the data in this dashboard, do you wish to proceed?" If User 1 views Dashboard A, the widget that is populated by Data Collection A will display an empty state with a message stating: "You do not have permission to view this data." Once added, User 1 will appear with a "limited access" badge on the Team page



Delivery 1: Custom Roles to include Action Permissions and Data Access Control

The existing default roles in the TQ Platform will remain available and permissions will be **uneditable** :

- Maintenance
- Administrative
- Primary Contributor
- Read-Only

For each custom role created, Maintenance and Admin Users will be able to

- Name the role
- Grant or Deny Action Permissions
- Grant or Deny Data Access Permissions
- Manage which users are assigned to the role

Creating a Custom Role

- When the user clicks "Create Role" they will see a page with a form with the following sections in this order:
  - "Role Name" Text Input
    - User will be able to name this custom role
  - Action Permissions
    - User will be able to set permissions for what actions the user can take in the platform
  - Data Access Permissions
    - User will be able to set permissions for what data the user can see in the platform
  - Role Assignment
    - User will be able to assign users to the role. If they add a user with an existing role in the system, this new role assignment will replace the old one.

Role Page - Create Role

Create Role Page - Initial Landing