NOVEMBER 2021

Role Based Access Control Feature Design Plan

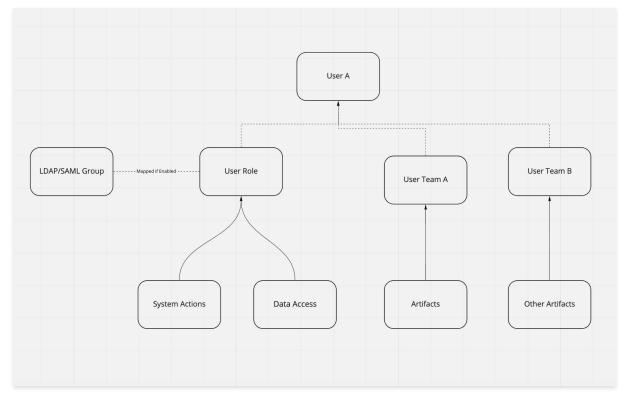
Bella Jones UX / UI Designer

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

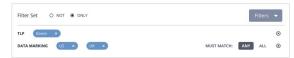
Custom Roles: Action Controls + Data Access Permissions

- 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

Role	Role Name					
	ns Permissions					
Below	are the permissions associated with the selected role.					
0	Administrative Functions					
	✓ Create and Manage Exports					
	Manage Server Administration					
	Manage System Configurations					
	OAuth Management					
	User Management					
•	Object Management					
	Data Management					
0						

Data Access Permissions

Users in this role are only permitted to see data based on the following criteria.



Role Assignment

Save

Search users below to assign them to this role. If a user has an existing role, it will be replaced with this role.

Reassign
Reassign
Reassign
Reassign

High Fidelity Designs

Custom Roles: Action Controls + Data Access Permissions

Jsers in this role are only permitted to see data based on the	ne following criteria.
Filter Set O NOT ONLY	Filters 🔫
TLP Green ×	®
DATA MARKING US × UK ×	MUST MATCH: ANY ALL ③

- 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

Data Con	Data Controls					
Data Markings	Indicator Expiration	Scoring	TLP	Whitelisted Indicators		

Data Markings

Disabled 💽 Enabled

Data markings can be used to apply restrictions, permissions, and other guidance for how data can be accessed and shared. Utilize this page to configure your data markings and then apply them to custom roles on the User Managment page to control access to data in ThreatQ. How it works.

Data Marking	Filters			
Q. Start typing				
Confidential Clearance	Select a Filter	SOURCE VirtusTotal X	۲	View All Filters
Declassified	Select a Filter	SOURCE Domain Tools x	۲	View All Filters
Secret Clearance	Select a Filter	WITH ATTRIBUTE Country/Spain x	۲	View All Filters
United Kingdom Office	Select a Filter	WITH ATTRIBUTE Country UK x	۲	View All Filters
United States Office	Select a Filter 🗸	SOURCE Emerging Threats ×	8	View All Filters
	Source			
	Тад			
	With Attribute			

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

Team	n Name			
Tear	n Mer	nbers		
View a	and mar	nage members of this team below. Use the s	search bar to add new members.	
Q :	Search to	ə add		
G	A T	om Ashoff	Role: SOC Manager	创
0	c J	oseph Crawford	Role: Network Analyst	۵
6	к	Dave Krasik	Role: Network Analyst	Û
		ssignment team will be granted access to the following Data Collections (1)	artifacts.	Remove
Users	on this I	team will be granted access to the following		Remove
Users	on this i	team will be granted access to the following Data Collections (1)	O Add	Remove
Users	on this i	team will be granted access to the following Data Collections (1) NAME ©	O Add	
Users	on this t	Data Collections (1) NAME € Q. Start typing	Add Owner +	J.com
Users	In this to the second sec	Data Collections (1) NAME © C Storres 8 and Above	Add OWNER = Q. Start typing admin@threatq	į.com
Users	on this 1	team will be granted access to the following Data Collections (1) NAME © G Start typing IOCs Scores 8 and Above Adversary Campaigns 2020	Add OWNER = Q Start (yppig_ admin@threatq admin@threatq	į.com
Users I	on this 1	team will be granted access to the following Data Collections (1) NAME C Start typing IOCs Scores 8 and Above Adversary Campaigns 2020 Open Flagged Network Tasks	Add OWNER 0 C Start typing admin@threatq admin@threatq admin@threatq	ı.com ı.com
Users I		team will be granted access to the following Data Collections (1) NAME © C. Stort typing IOCs Scores 8 and Above Adversary Campaigns 2020 Open Flagged Network Tasks Dashboards (1)	Add	ı.com ı.com
Users I		team will be granted access to the following Data Collections (1) NAME e Q. Start Typing IOCs Scores 8 and Above Adversary Campaigns 2020 Open Flagged Network Tasks Dashboards (1) NAME e	Add	µ.com µ.com µ.com

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

Threat Library Bob's Data Coll											
Q Search for keywords											
Filter Set 1 🔲 NOT									Filters	-	•
CREATED AT Before 05/27/2021 03	:04am ×										۲
Add Another Filter Set						Limit by TLP:	🗹 Red	🗹 Amber 🛛 🗹	Green 🗹 W	hite 🗹 Not !	Spe
Micators (42,816)							œ	Manage Colu	imns 💌	Actions	
QUICK FILTERS Type • St	atus 👻 Score 👻	Expiration 👻									
QUICK FILTERS Type + St	atus ¥ Score ¥	Expiration • DATE CREATED •	LAST MODIFIED \$	STATUS \$	SCORE ©	EXPIRATION	DATE	TAGS			
			LAST MODIFIED 0 10/12/2021 04:41pm	status • Active	score ¢	EXPIRATION	DATE	TAGS			
VALUE \$	туре С	DATE CREATED				EXPIRATION	DATE	TAGS			
value ≎ @ 223.87.178.49	TYPE ©	DATE CREATED •	10/12/2021 04:41pm	Active	0	EXPIRATION	DATE	TAGS			
VALUE © 223.87.178.49 © 223.247.149.130	TYPE + IP Address IP Address	DATE CREATED	10/12/2021 04:41pm 10/12/2021 04:41pm	Active Active	0	EXPIRATION	DATE	TAGS			
 value ● 223.87.178.49 223.247.149.130 223.18.153.172 	TYPE IP Address IP Address IP Address	DATE CREATED	10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm	Active Active Active	0 0 0	EXPIRATION	DATE	TAGS			
VALUE • • 223.87.178.49 • 223.277.140.130 • 223.18.153.172 • 223.17.92.145	IP Address IP Address IP Address IP Address	DATE CREATED 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm	10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm	Active Active Active Active	0	EXPIRATION	DATE	TAGS			
VALUE * V23.37.178.49 223.247.149.130 223.247.149.130 223.18.153.172 Que 223.11.52.145 223.11.52.0.05	TYPE C IP Address IP Address IP Address IP Address IP Address	DATE CREATED	10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm	Active Active Active Active Active		EXPIRATION	I DATE	TAGS			
value •	1797E C IP Address IP Address IP Address IP Address IP Address IP Address	DATE CREATED	10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm	Active Active Active Active Active Active	0 0 0 0 0	EXPIRATION	DATE	TAGS			
VALUE P VALUE	TYPE © IP Address IP Address IP Address IP Address IP Address IP Address	DAT CILATO	10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm 10/12/2021 04:41pm	Active Active Active Active Active Active	0 0 0 0 0	EXPIRATION	DATE	TAGS			

Design Commit Complete

Project Docs / 2	021 Projects	🖉 😋 🏠 🧿 🆻 🔒 Share 🚥	Fig. 3 - Data Access Permissions Application M	atrix:			
RBAC De	sign Commit		User's Data Access Permission	Item	Scenario		Behavior
	d by Bob Ricca dated: 8 minutes ago by Bella Jones - 1dt. 10 people viewed		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 Attribute B that has a TLP=Red	h an Attribute A that has TLP=Green and an	Use 1 is able to view Object A and Attribute A, but unable to view Attribute B
Overview					User 1 is attempting to view an Object A with Source B that has a TLP=Red	h a Source A that has TLP=Green and a	User 1 is unable to view Object A and Source A, but unable to view Source B
This design docu	ment describes a project to deliver role based access control (RBAC) to Threa ther view certain types of data or take actions on that data).	tQ. This project includes the ability for TQ admins to control transactions based on user role (Ex.			User 1 is attempting to view an Object A with relationship to an Object B that has a source		User 1 is able to view Object A, but will not be able to see the relationship to Object B or access Object B
We have some ve	ry limited and infrequently used custom RBAC-like capabilities that are impler	nented through the CLI and manual config file edits, however based on POCs and additional customer is is of particular importance in the federal space, where RBAC, TLP, and data markings are more			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
	is to satisfy the production requirements of some key customer prospects. It is standard practices.	is is of particular importance in the rederal space, where KokC, TLP, and data markings are more			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
High Level Us	se Cases	Delivery 1: Custom Roles to include Action Permissions and I	Data Access Control			lection A, which has objects with ONLY	User 1 can be added, but upon sharing/assigning, User 2 will get notification message stating:
	want to be able to do:	The existing default roles in the TQ Platform will remain available and permissions will be uner	litable :				"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?"
TLP and or data in my	ss Control - I want to be able to restrict user access to data within TQ usin custom markings so that I can have proper separation of privileges to cert system that is more sensitive than other data. At the same time, I still want of access and collaboration across various user types.	Maintenance Administrative					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
a. Singl b. Singl	e company with different types of users - E.g. US and International based e-tenancy MSSP with multiple companies who can access a global TQ - E. mer A and Customer B can access a common set of MSSP-shared data.	Primary Contributor Read-Only					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.
	trol - I want to restrict access to certain actions within TQ based on user	For each custom role created, Maintenance and Admin Users will be able to				lection B, which has objects with s 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
that I can m	Nes - I want to be able to create additional custom roles within the TQ UI so nore granularly control RBAC.	Name the role Grant or Deny Action Permissions				lection C, which contains objects	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
	ng Groups - I want to be able to create buckets of users for the purposes facts such as investigations, dashboards, or data collections.	Grant or Deny Data Access Permissions Manage which users are assigned to the role				C, which contains <u>both</u> 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 TLPRRed
Concepts & 1	Terminology	Creating a Custom Role	Role Page - Create Role			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:
Term	Definition						"User 1 may not have the permissions to be able to see all of the data in this dashboard, do you wish to proceed?"
User Role	A user's role defines what permissions the user has to perform actions in the system or access data (at the	 When the user clicks "Create Role" they will see a page with a form with the following sections in this order: 	User Management		Crears liois		If User 1 views Dashboard A, the widget that is populated by Data Collection A will display an empty state with a message stating:
		 "Role Name" Text Input User will be able to name this custom role 	denormal and and see				"You do not have permission to view this data." Once added. User 1 will appear with a "limited access" badge on the Team page
		Action Permissions User will be able to set permissions for what actions the user can take in th	Create Role Page - Initial Landing e				
		platform Data Access Permissions 	THREATQ 🕥 tot Salidounity 🗈 Thread Library 🔺 Investigations	n Guta Exchange 🖒 Integrations 🖒 Automation	🗕 🕹 🖉 🤹 🕹 🖗		
		 User will be able to set permissions for what data the user can see in the platform 	< Create Role				
		Role Assignment					

() integrations

 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.