MARCH 2021

Threat Intelligence Data Exchange Feature

Usability Test Findings & Recommendations

Bella Jones
UX / UI Designer

Context and Impact

This usability assessment was conducted right as an internal MVP build became available and just before the initial General Audience (GA) release was scheduled to roll out.

As lead designer on the project, I believed there were key usability issues that needed to be addressed in order to maximize user adoption of the new feature.

Because of the timing of these usability findings and recommendation, we were able to include key UI enhancements that hugely impacted not only the user experience but also the customer sales POC (proof of concept) experience, helping to generate more sales leads and new customers than originally anticipated.

Usability Testing Process and Key Findings

Across the usability sessions, we most frequently received feedback about the below areas of the platform experience.

	Key Observations				
Platform Experience	**Recognition rather than Recall**	**Match b/w System and Real World**	**Error Prevention**	**Visibility of System Status**	**Prioritized Improvements**
ONBOARDING EXPERIENCE	Users could not clearly identify the first steps needed to set up.	Help language was unclear and did not fully guide user or introduce key terms.	Connection bundle generation allowed user to click create multiple times for same client.	User was looking for toast messages to confirm their set up steps.	Clarify the set up workflow by implementing an **onboarding wizard** that will guide users through the process. (Delivered in **MS1**)
INFORMATION HIERARCHY	Key information was hidden in tabs that required multiple clicks.	Language for some buttons did not match the assumed or intended action.	Naming and labeling caused some confusion.	Activity log information was dispersed in hidden tabs.	**Consolidate sidebar information** into the same view, rather than in tabs. Relabel certain buttons and add help text for more clarity. (Delivered in **MS1**)
STATUS AND ERROR MESSAGING	User did not intuitively observe status messages in the activity log. Error messages are non-existent or not prevalent.	The action word in status messages in the activity logs were buried in the subheader text.	Adequate error prevention in most forms and deletion workflows. Minor tweaks needed.	User expected more confirmation toast messages for actions they were taking.	**Consolidate and relabel activity log messages for release**. (Delivered in **MS1**) Address additional improvements to performance and error messaging in **MS2**.
DATA FEED CONTROLS	Lack of top-level information about the contents of an incoming feed.	N/A	Lack of ability to opt out of an incoming feed and to control the status assignments raised concerns.	Lack of clear status messages when feed transfers were successfully made. User did not intuitively see these in the activity log.	Prioritize enabling **Opt-in/Opt-out** Feed Subscription model and Subscriber **Status Override** as part of **MS2**.

Design Revisions

The sessions revealed a clear need for more guidance on getting started, so we designed an onboarding wizard to help clarify the process.

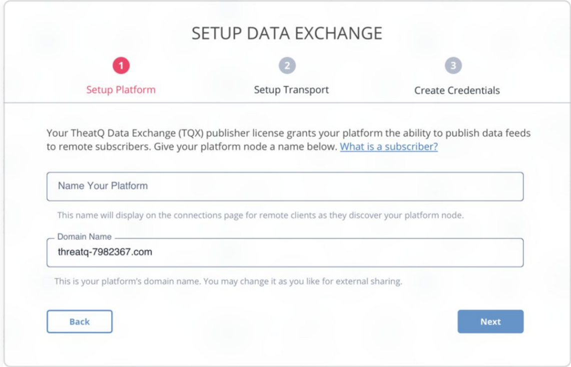
Prioritized Improvements

Clarify the set up workflow by implementing an onboarding wizard that will guide users through the process.

Consolidate sidebar information into the same view, rather than in tabs. Relabel certain buttons and add help text for more clarity.

Consolidate and relabel activity log messages for release in MS1. Address additional improvements to performance and error messaging in MS2.

Prioritize enabling Opt-in/Opt-out Feed Subscription model and Subscriber Status Override as part of MS2.



SETUP DATA EXCHANGE

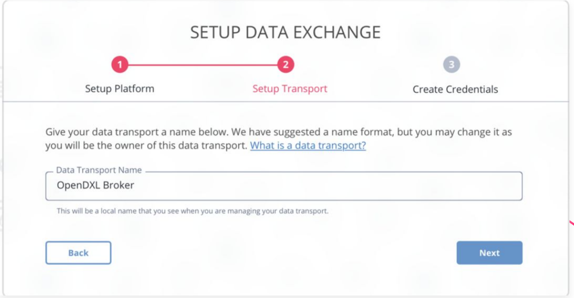
Your TheatQ Data Exchange (TQX) publisher license grants your platform the ability to publish data feeds to remote subscribers. Give your platform node a name below. What is a subscriber?

Name Your Platform

This name will display on the connections page for remote clients as they discover your platform node.

Domain Name: threatq-7982367.com

This is your platform's domain name. You may change it as you like for external sharing.

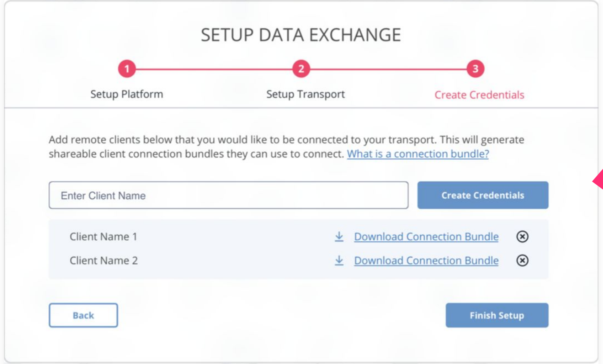


SETUP DATA EXCHANGE

Give your data transport a name below. We have suggested a name format, but you may change it as you will be the owner of this data transport. What is a data transport?

Data Transport Name: OpenDXL Broker

This will be a local name that you see when you are managing your data transport.



SETUP DATA EXCHANGE

Add remote clients below that you would like to be connected to your transport. This will generate shareable client connection bundles they can use to connect. What is a connection bundle?

Enter Client Name

Client Name 1 — Download Connection Bundle

Client Name 2 — Download Connection Bundle

Design Revisions

Observing the users' pain points regarding the information hierarchy in the sidebar helped us improve its language and organization.

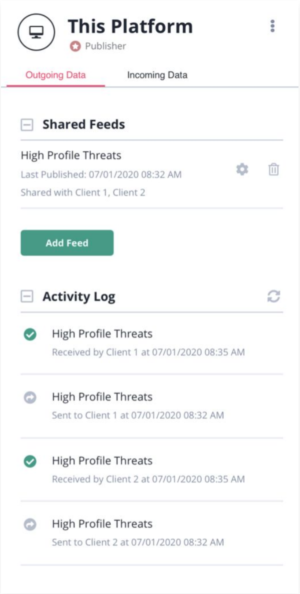
Prioritized Improvements

Clarify the set up workflow by implementing an onboarding wizard that will guide users through the process.

Consolidate sidebar information into the same view, rather than in tabs. Relabel certain buttons and add help text for more clarity.

Consolidate and relabel activity log messages for release in MS1. Address additional improvements to performance and error messaging in MS2.

Prioritize enabling Opt-in/Opt-out Feed Subscription model and Subscriber Status Override as part of MS1.5.



This Platform
Publisher

Outgoing Data | Incoming Data

Shared Feeds

High Profile Threats
Last Published: 07/01/2020 08:32 AM
Shared with Client 1, Client 2

Activity Log

High Profile Threats
Received by Client 1 at 07/01/2020 08:35 AM

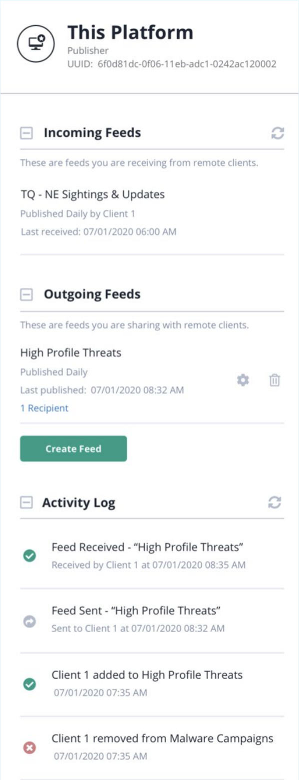
High Profile Threats
Sent to Client 1 at 07/01/2020 08:32 AM

High Profile Threats
Received by Client 2 at 07/01/2020 08:35 AM

High Profile Threats
Sent to Client 2 at 07/01/2020 08:32 AM

Before

- Incoming Data information is hidden in tab
- Activity log information is dispersed between the tabs
- Language in activity log messages do not clearly indicate the action occurring
- User thought "Add Feed" would subscribe them to a feed



This Platform
Publisher
UUID: 6f0d81dc-0f06-11eb-adc1-0242ac120002

Incoming Feeds

These are feeds you are receiving from remote clients.

TQ - NE Sightings & Updates
Published Daily by Client 1
Last received: 07/01/2020 06:00 AM

Outgoing Feeds

These are feeds you are sharing with remote clients.

High Profile Threats
Published Daily
Last published: 07/01/2020 08:32 AM
1 Recipient

Activity Log

Feed Received - "High Profile Threats"
Received by Client 1 at 07/01/2020 08:35 AM

Feed Sent - "High Profile Threats"
Sent to Client 1 at 07/01/2020 08:32 AM

Client 1 added to High Profile Threats
07/01/2020 07:35 AM

Client 1 removed from Malware Campaigns
07/01/2020 07:35 AM

After

- User can now see both incoming and outgoing data in same view
- Activity log information is consolidated
- Language in activity log messages is clearer
- Button relabeled "Create Feed" to more better represent the system action

Design Revisions

Many users did not intuitively utilize the activity log, many expected messages confirming successful completion of an action.

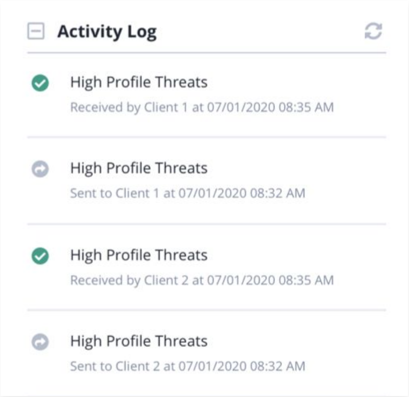
Prioritized Improvements

Clarify the set up workflow by implementing an onboarding wizard that will guide users through the process.

Consolidate sidebar information into the same view, rather than in tabs. Relabel certain buttons and add help text for more clarity.

Consolidate and relabel activity log messages for release in MS1. Address additional improvements to performance and error messaging in MS2.

Prioritize enabling Opt-in/Opt-out Feed Subscription model and Subscriber Status Override as part of MS2.



Activity Log

High Profile Threats
Received by Client 1 at 07/01/2020 08:35 AM

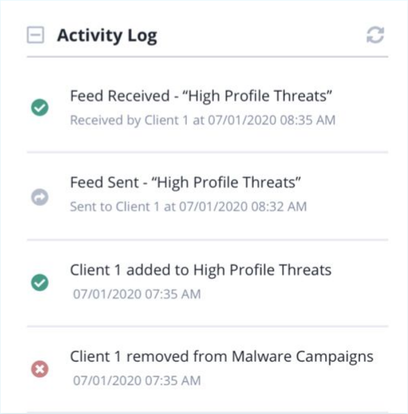
High Profile Threats
Sent to Client 1 at 07/01/2020 08:32 AM

High Profile Threats
Received by Client 2 at 07/01/2020 08:35 AM

High Profile Threats
Sent to Client 2 at 07/01/2020 08:32 AM

Before

- Language in activity log messages do not clearly indicate the action occurring
- Users expected more messaging



Activity Log

Feed Received - “High Profile Threats”
Received by Client 1 at 07/01/2020 08:35 AM

Feed Sent - “High Profile Threats”
Sent to Client 1 at 07/01/2020 08:32 AM

Client 1 added to High Profile Threats
07/01/2020 07:35 AM

Client 1 removed from Malware Campaigns
07/01/2020 07:35 AM

After

- “Feed Received” and “Feed Sent” pulled up into log entry header
- New messages added confirming the action of adding or removing recipients

Longer-term recommended fix: Add more confirmation status messaging and feed-based activity logs on the Edit Feed pages.

Design Revisions

Multiple internal SMEs emphasized the importance of customers having better recipient feed control over subscription and ingestion.

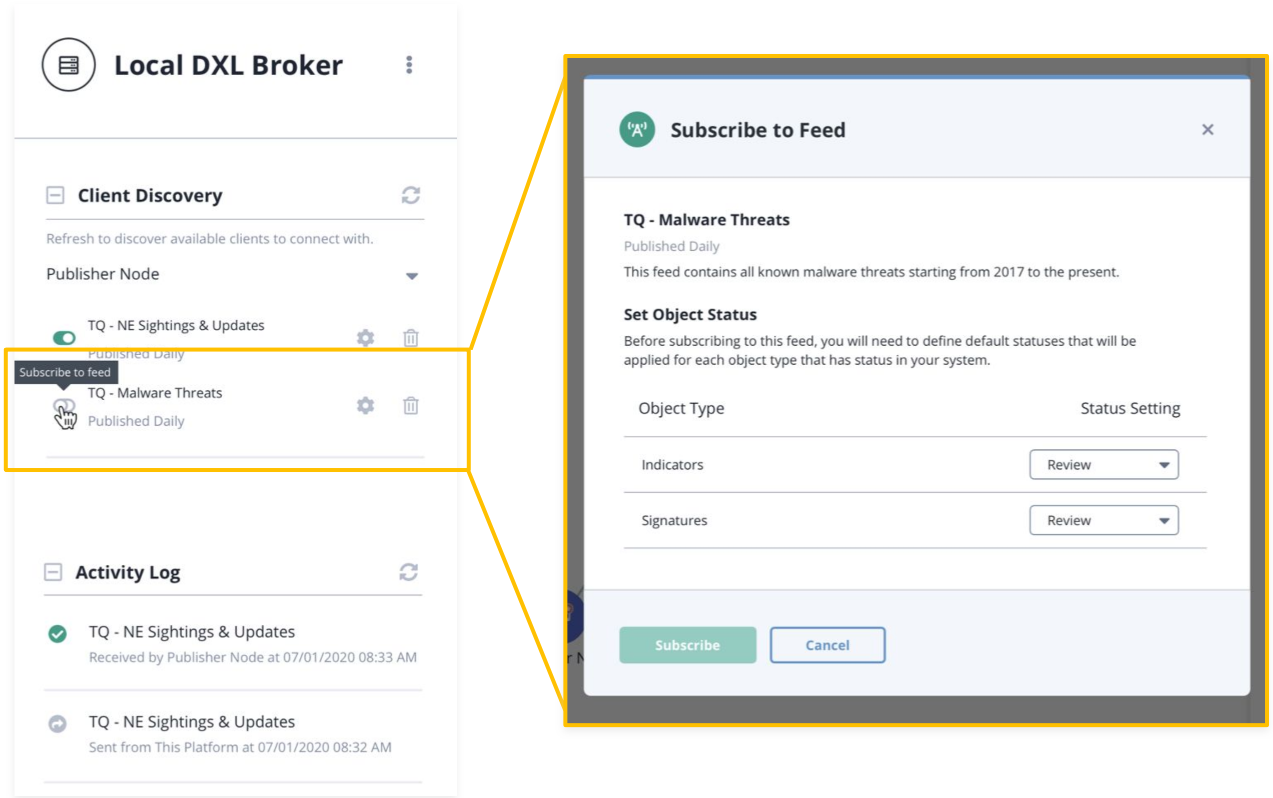
Prioritized Improvements

Clarify the set up workflow by implementing an onboarding wizard that will guide users through the process.

Consolidate sidebar information into the same view, rather than in tabs. Relabel certain buttons and add help text for more clarity.

Consolidate and relabel activity log messages for release. Address additional improvements to performance and error messaging in MS2.

Prioritize enabling Opt-in/Opt-out Feed Subscription model and Subscriber Status Override as part of MS2.



Local DXL Broker

Client Discovery

Refresh to discover available clients to connect with.

Publisher Node

TQ - NE Sightings & Updates
Published Daily

Subscribe to feed

TQ - Malware Threats
Published Daily

Activity Log

TQ - NE Sightings & Updates
Received by Publisher Node at 07/01/2020 08:33 AM

TQ - NE Sightings & Updates
Sent from This Platform at 07/01/2020 08:32 AM

Subscribe to Feed

TQ - Malware Threats
Published Daily
This feed contains all known malware threats starting from 2017 to the present.

Set Object Status
Before subscribing to this feed, you will need to define default statuses that will be applied for each object type that has status in your system.

Object Type	Status Setting
Indicators	Review
Signatures	Review

Quotes from Participants

After design revisions were made, we conducted a second round of usability testing with a wider pool of participants, some of them repeats from the first round of sessions. These were some of the things they had to say about the improvements.

“The interface feels super sleek.”

“Leaps and bounds forward from the last version I saw”

“That [onboarding wizard] was easy!”

Future Recommendations and Potential Pain Points

Although we were able to pivot quickly to make impactful usability improvements, we also uncovered larger usability issues that will need to be addressed as part of the feature roadmap.

ADDITIONAL USER GUIDANCE

- Context-setting introduction screen to explain bigger picture and purpose that this feature serves to their organization during the setup wizard process

SYSTEM STATUS & ERROR MESSAGING

- Positive reinforcement and workflow conclusion by making it clear that “it’s working”.
- Clear messages or alerts when the system encounters an error, prompting the user to take an action to remediate the issue.

FEED MANAGEMENT & AUDITING

- Show more feed health and analytics information such as number of objects ingested.
- Enable users to pull audit logs of activity on a per feed basis.
- Enable users to view data segments of ingested packages by feed.