

ThreatQuotient



ThreatQ User Guide

Version 2.4.0

September 01, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
About TQI Versioning	4
About ThreatQ Investigations	5
Concept.....	5
Evidence Board	5
Action Panel	6
Timeline	8
Getting Started with Investigations	9
Starting an Investigation.....	9
Managing Investigations.....	11
Filtering Investigations.....	12
Continuing an Investigation	13
Sharing an Investigation	14
Pinning an Investigation	16
Deleting an Investigation.....	17
Editing an Investigation.....	18
Action Panel Overview.....	19
Managing Threat Intelligence Data from the Action Panel	20
Evidence Board	22
Adding Threat Intelligence Data to the Evidence Board	22
Adding a Task to an Investigation.....	24
Managing Threat Intelligence Data on the Evidence Board	26
Accessing an Object's Details Page from the Evidence Board	28
Viewing an Object's Relationships on the Evidence Board	29
Adding an Object to an Investigation.....	31
Adding a New Task Related to an Object.....	32
Adding a New Timeline Entry Related to the Object	34
Locking and Unlocking an Object on the Evidence Board.....	37
Creating an Object from the Evidence Board	38
Deleting an Object from the Evidence Board	38
Selecting Multiple Objects on the Evidence Board.....	39
Creating and Linking a New Object	40
Sharing an Investigation	41
Using the Timeline	44
Timeline Overview	44
Adding a Timeline Entry.....	44
Viewing a Timeline Entry Summary.....	45

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2021 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

About TQI Versioning

ThreatQ Investigations is seeded as part of the ThreatQ platform. The versioning assigned to this PDF, 2.4.0, is for documentation-tracking purposes only and does not indicate a separate ThreatQ Investigations version.

About ThreatQ Investigations

ThreatQ Investigations is a cybersecurity situation room that enables collaborative threat analysis, investigation, and coordinated response. Investigations is built upon a collaborative investigation interface that aggregates all information on screen with a focus on the evidence board, which displays threat intelligence data as icons.

ThreatQ Investigations is built on top of the ThreatQ threat intelligence platform and allows for capturing, learning, and the sharing of knowledge. This results in a single visual representation of the complete investigation at hand, who did what and when, based on a shared understanding of all components of the investigation: threat data, evidence, and users.

Concept

The following describes the components of an investigation and how it can be used to drive an incident response.

Evidence Board

The evidence board provides a visual representation of the threat intelligence data you are currently investigating.



The evidence board allows you to:

- Fuse together threat data and user actions to more quickly determine the right actions to take.
- Accelerate investigation, analysis, and understanding of threats in order to update your defensive posture proactively.
- Drive down mean time to detect (MTTD) and mean time to respond (MTTR).

Action Panel

Using the action panel, incident handlers, malware researchers, SOC analysts, and investigation leads gain more control, and are able to take the right steps at the right time.

 **GIBBERISH PANDA** 

Expand

Remove from Investigation



TYPE

Adversary

RELATIONSHIPS

1

TASKS

0

COMMENTS

0

SOURCES

1

CrowdStrike

FIRST SEEN

Last Saturday at 12:13 AM

CREATED

Last Saturday at 12:13 AM

LAST MODIFIED

Last Saturday at 12:13 AM

▼ DESCRIPTION

none

► COMMENTS

0

RELATIONSHIPS

►  INDICATORS

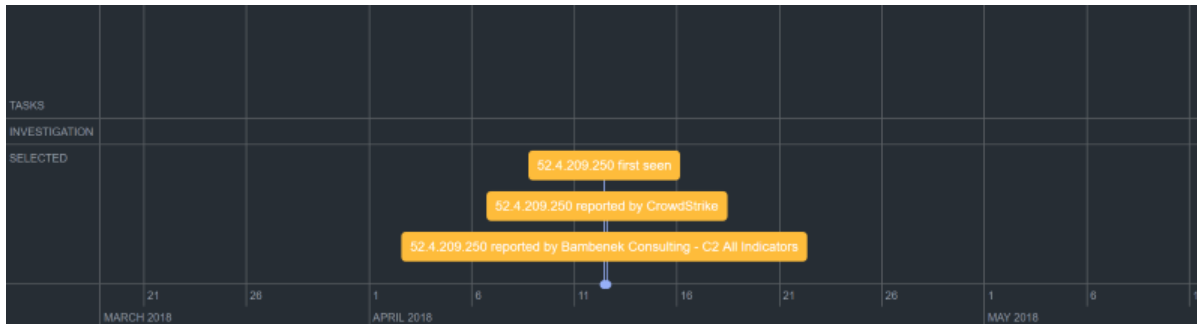
1

The action panel allows you to:

- See how the work of others impacts and extends your own.
- View a summary of any aspect of the evidence board that currently has mouse focus.

Timeline

You can build incident, adversary, and campaign timelines to accelerate understanding of threat intelligence data. The timeline portion of an investigation allows you to visualize how the investigation began and understand how the response unfolded.



You can view:

- When indicators, events, adversaries, files, signatures, and so on were discovered and included in the Threat Library.
- Any assigned and closed tasks.
- Who was working on what aspect of the investigation and when.

Getting Started with Investigations

Managing investigations begins with the Investigations page. You can create one or more investigations and this page serves as your access point. On the Investigations page, you can:

- View all the investigations you created or investigations another user shared with you.
- Create and delete investigations.
- View a date and time stamp for the last person who updated an investigation.
- Manage current investigations.

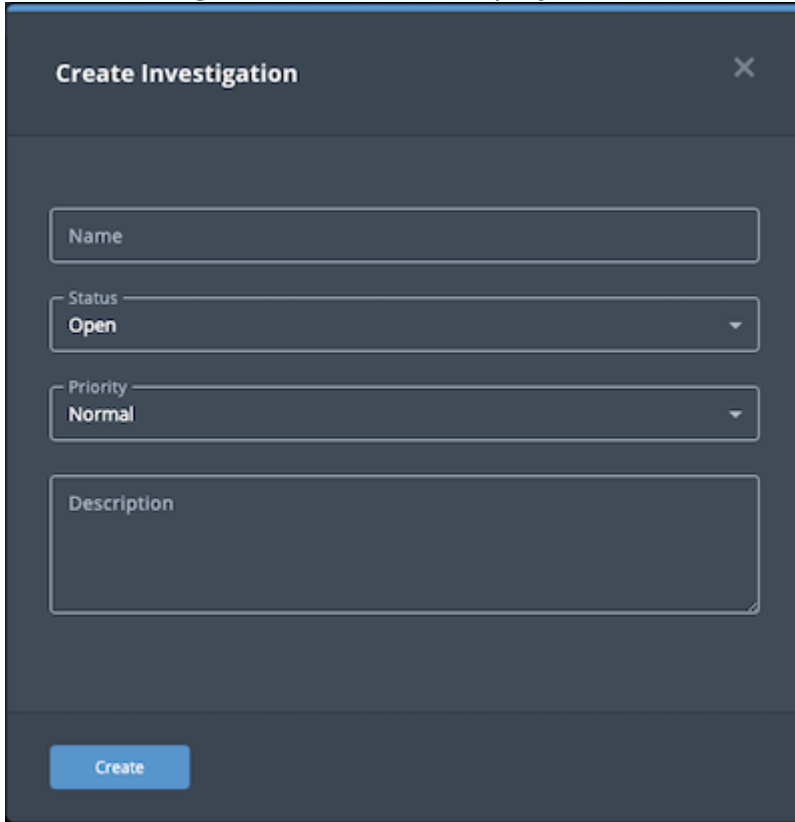
As you create or enter an investigation, the system navigates you to the investigations workbench, which is comprised of the evidence board, action panel, and timeline. You will learn how to interact with these components later in this user guide.

Starting an Investigation

1. Select one of the following options:

PATH	USE WHEN...
Investigations menu > Start your first investigation button	This is your first investigation
Threat Library Actions menu > Start Investigation	You want to add the current object to a new investigation
Investigations page > Create Investigation button	General use.
Top Navigation bar > Create button	General use.

The Create Investigation window is displayed.

A screenshot of the 'Create Investigation' window. The window has a dark grey header with the title 'Create Investigation' and a close button (X). Below the header, there are four input fields: 'Name' (a text box), 'Status' (a dropdown menu with 'Open' selected), 'Priority' (a dropdown menu with 'Normal' selected), and 'Description' (a larger text box). At the bottom of the window is a blue button labeled 'Create'.

2. Populate the Create Investigation window as follows:

- Type a **Name** for the investigation.
- Select a **Status**:
 - **Open** - Open investigations appear as normal on the Investigations page.
 - **Closed** - Closed investigations appear greyed out on the Investigations page.
- Select a **Priority**:



What is normal or escalated depends upon your organization.

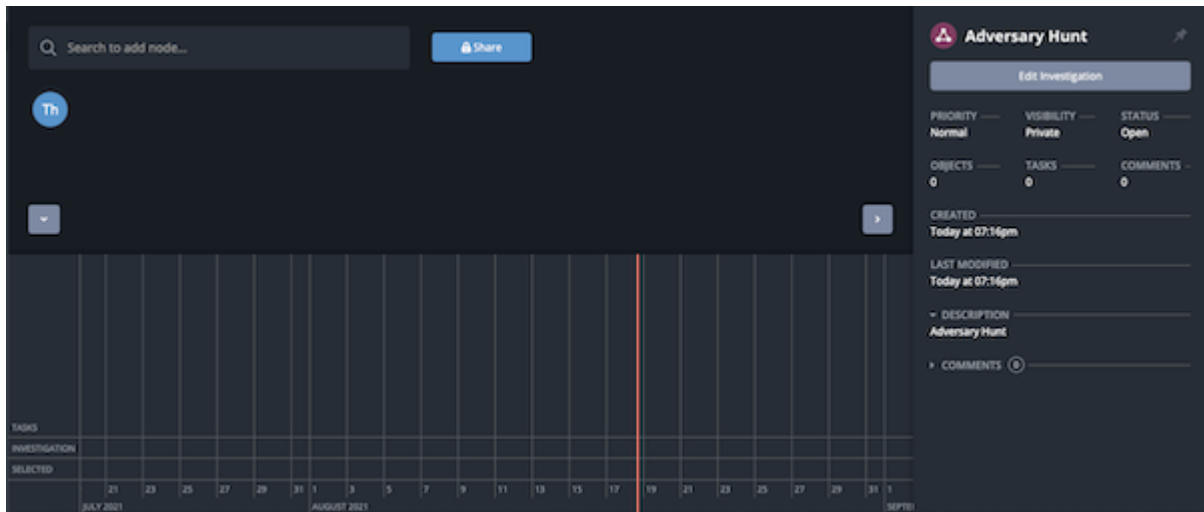
- **Normal**
- **Escalated**
- Optionally, type a **Description** for the investigation.

3. Click **Create**.

The investigation workbench appears.



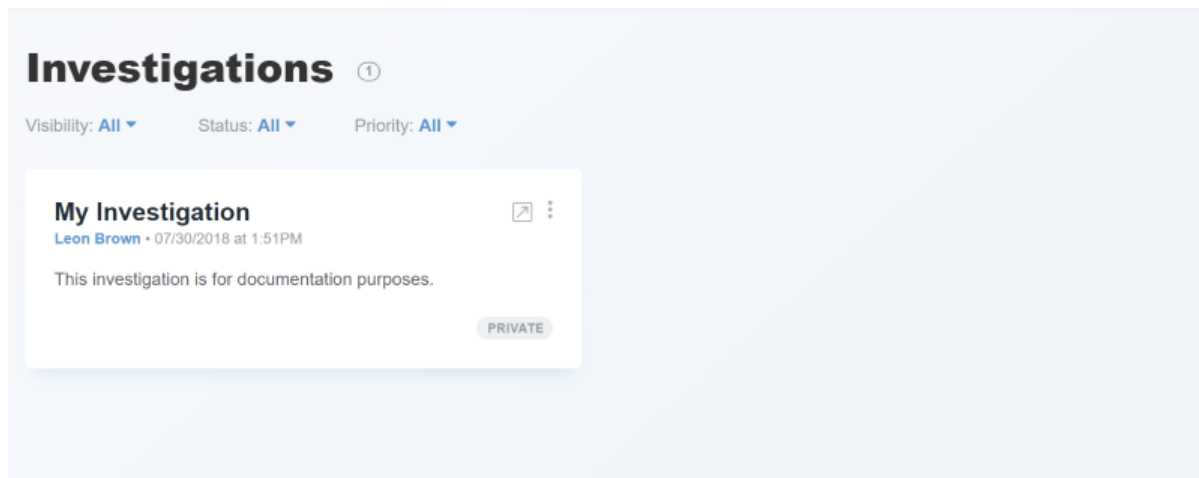
If you created this investigation via the Threat Library Actions menu, the associated object is automatically added to the investigation and displayed on the evidence board.



Managing Investigations

After an investigation is created, you can manage it on the Investigations page.

1. From the **Investigations** menu, click the **Browse All** button.



2. The following table describes the actions you can take to manage your investigations on the Investigations page.

TO	YOU CAN
Create a new investigation	See Starting an Investigation .

TO	YOU CAN
Filter the investigations displayed	See Filtering Investigations .
Continue an investigation	Select the investigation title; see Continuing an Investigation .
Share an investigation	See Sharing an Investigation .
Pin an investigation	See Pinning an Investigation .
Delete an investigation	Click the vertical ellipsis menu and select Delete ; see Deleting an Investigation .
Edit an investigation	See Editing an Investigation .

Filtering Investigations

To manage the investigations displayed on the Investigations page, you can apply filters.

1. Click the **Investigations** menu and select one of the following options:

- Click a pinned investigation to access it directly.
- Click the **Browse All** button to access the Investigations page.



If you have not pinned any investigations, clicking the **Investigations** menu takes you directly to the Investigations page.

2. Use the following filters to customized your view of the Investigations page:

FILTER	OPTIONS
Visibility	◦ All ◦ Private

	◦ Shared
Status	◦ All ◦ Open ◦ Closed
Priority	◦ All ◦ Normal ◦ Escalated

Continuing an Investigation

To return to an investigation after working in another area of ThreatQ, complete the following steps:

1. Click the **Investigations** menu and select one of the following options:

- Click a pinned investigation to access it directly.
- Click the **Browse All** button to access the Investigations page.



If you have not pinned any investigations, clicking the **Investigations** menu takes you directly to the Investigations page.

2. From, the Investigations page, click the name of the investigation you want to continue. The investigation workbench is displayed.



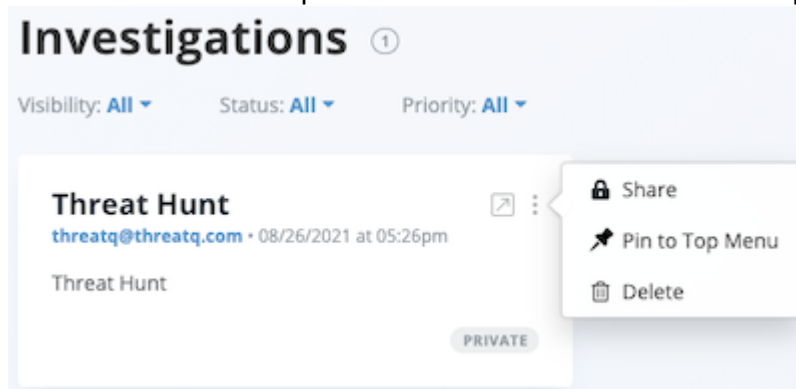
Sharing an Investigation

Owners and editors have the option to share an investigation with other users as well as update or remove their sharing permissions. In addition, the Share(d) button displayed depends on your permission level and the sharing status of the data collection.

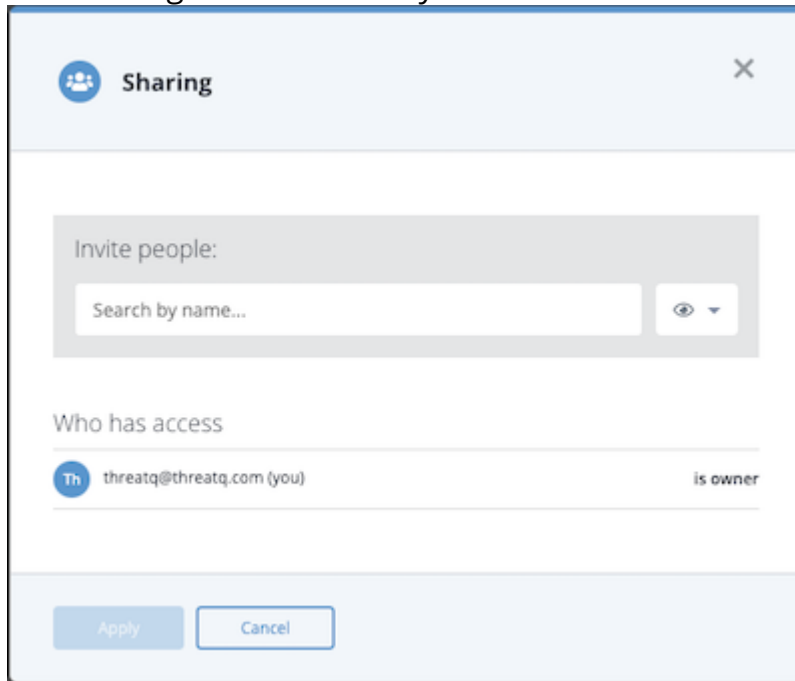
PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON
Owner	No	
Owner, Editor	Yes	
Viewer	Yes	

You can share an investigation from the Investigations page or the evidence board of the investigation. See the Sharing topic for more information on the permissions you can assign to each investigation.

1. From the Investigations page, locate the investigation you want to share.
2. Click the vertical ellipsis menu and select the **Share** option.



The Sharing window allows you to select the user to which you want to grant access.



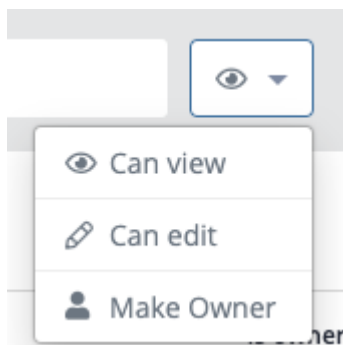
3. Click the arrow next to the  icon to select the user's permission level.



If you are granting access to all users, you must select the **Can View** option. You can only assign editing permission to individual users, not to all users.

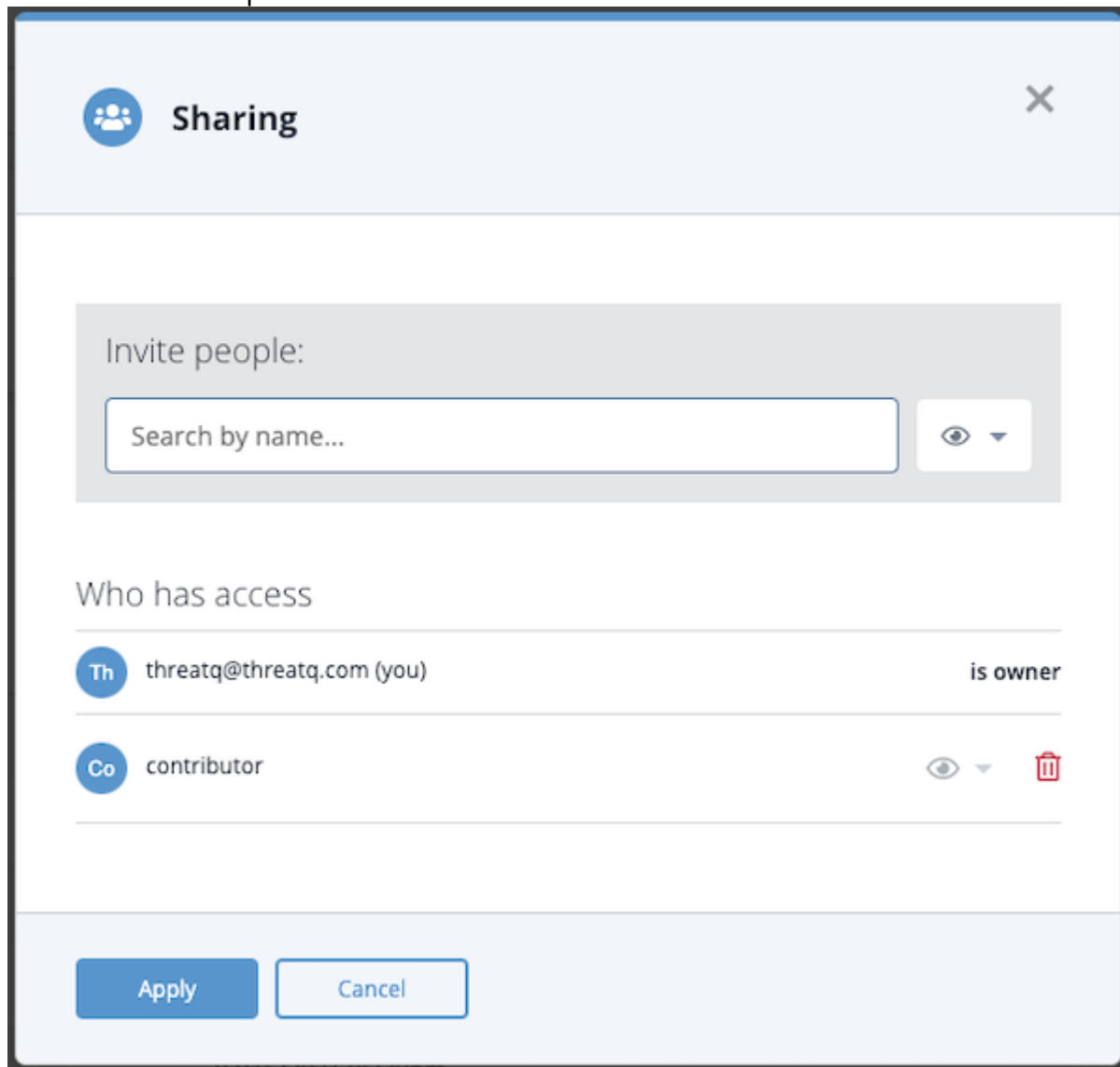


If you assign owner permissions to another user, your permissions automatically change to editor-level.



4. Use the search field to locate and select the user name or the **Everybody (Public)** option. This option grants view-only access to all users. The user is now listed in the Who has access list. From this listing, you can change or

delete the user's permissions.



5. Click the Apply button to save the user's permission level.

Pinning an Investigation

You can create a Favorites list of frequently accessed investigations by pinning them to the Investigations menu. These shortcuts allow you to bypass the Investigations page and go directly to the investigation's evidence board.

Method 1 - Investigations Page

1. From the Investigations page, locate the investigation you want to pin to the Investigations menu.

2. Click the vertical ellipsis menu and select the **Pin to Top Menu** option.
The Pinned Investigations section of the Investigations menu now displays a link to the investigation.



Investigation names on the Investigations menu are truncated at thirty characters. In addition, if you add more than ten investigations to the menu, a scroll bar allows you to browse the list.

3. To remove the pinned investigation, you can click the vertical ellipsis menu and select the **Unpin from Top Menu** option.

Method 2 - Action Panel

From an investigation's action panel, you can click the thumbtack icon  to the right of the investigation name to pin or unpin the investigation.

Deleting an Investigation

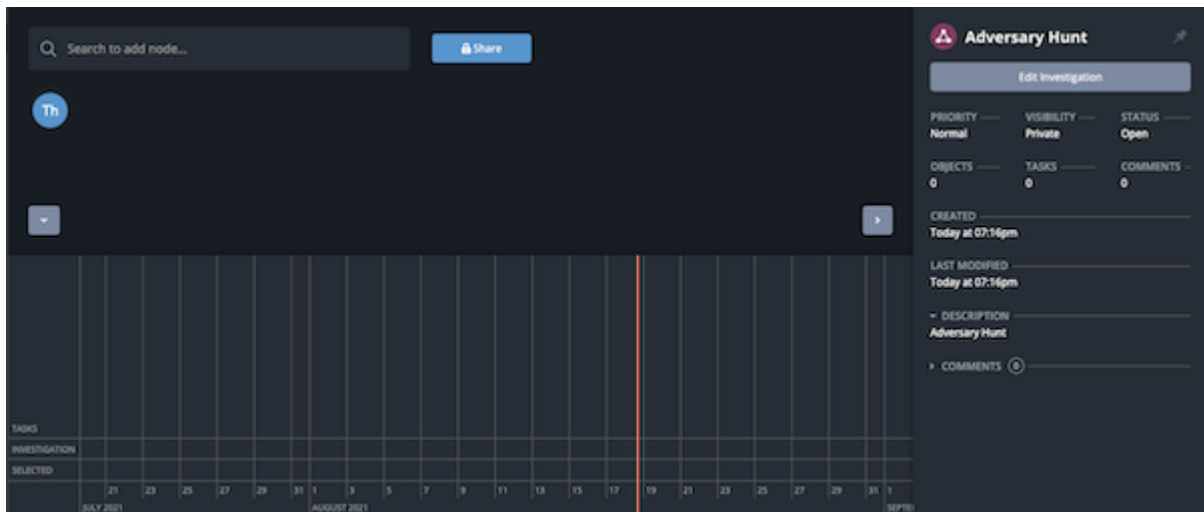
Only the owner of an investigation can delete it. Deleting an investigation removes it from the Investigations page and also from your system. Take care in selecting this option.

1. From the Investigations page, locate the investigation you want to delete.
2. Click the vertical ellipsis menu and select **Delete**.
The **Are You Sure?** window prompts you to confirm the deletion.
3. Click **Delete Investigation**.

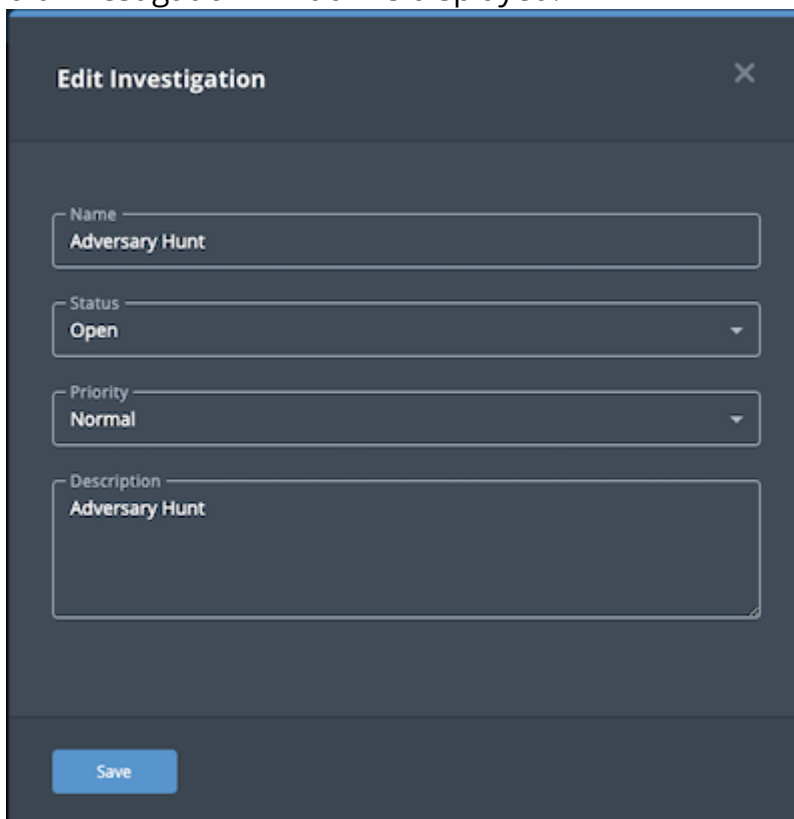
Editing an Investigation

To edit the original parameters for an existing investigation, complete the following steps:

1. From the investigation's evidence board, verify that none of the investigation nodes have focus.



2. In the action panel, click the **Edit Investigation** button.
The Edit Investigation window is displayed.



3. Enter your changes.
4. Click the **Save** button.

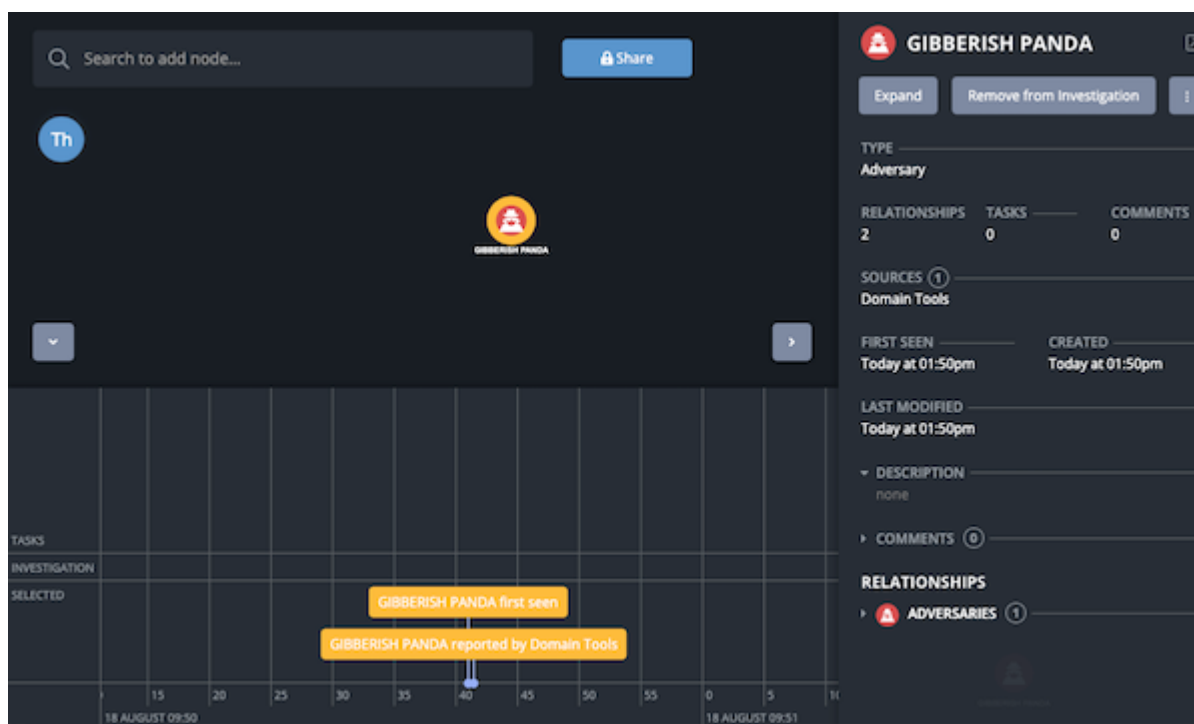
Action Panel Overview

As you create an investigation and add objects to that investigation, these items are also reflected in the action panel. The action panel provides an overview of an item on the evidence board that currently has mouse focus. Depending on the item being summarized, you can also interact with and edit an object on the evidence board, and create timeline entries.

Managing Threat Intelligence Data from the Action Panel

After an object is added to the evidence board, you can manage some aspects of the object from the action panel.

1. On the evidence board, select and highlight the node that represents the object you want to manage.



2. The following table describes the actions you can take to manage your object from the action panel.

TO	YOU CAN
View the object's details page	Click the open in new tab icon beside the name of the object. For more information about object details pages, see the Object Details topic in the ThreatQ Platform guide.
View the object's relationships on the evidence board	Click Expand ; see Viewing an Object's Relationships on the Evidence Board .

TO	YOU CAN
Add the highlighted object to the investigation	Click Commit to Investigation ; see Adding an Object to an Investigation .
Add a new task related to the object	Click the vertical ellipsis menu and select New Task ; see Adding a New Task Related to an Object .
Add a new timeline entry related to the object	Click the vertical ellipsis menu and select New Timeline Entry ; see Adding a New Timeline Entry Related to the Object .
Pin an investigation	See Pinning an Investigation .

Evidence Board

The evidence board is where most of the interaction takes place in an investigation. The evidence board allows you to add ThreatQ objects, such as Indicators and Adversaries to the investigation, represented as graphical nodes. The evidence board interacts with the other two components of an investigation workbench, the action panel and the timeline.

As you add objects to the evidence board, relevant information about that object is automatically included on the timeline. If you select to highlight a node on the evidence board, the action panel displays a summary relevant to that node. These summaries can range from as broad as the overall investigation to as granular as an attribute related to an object.

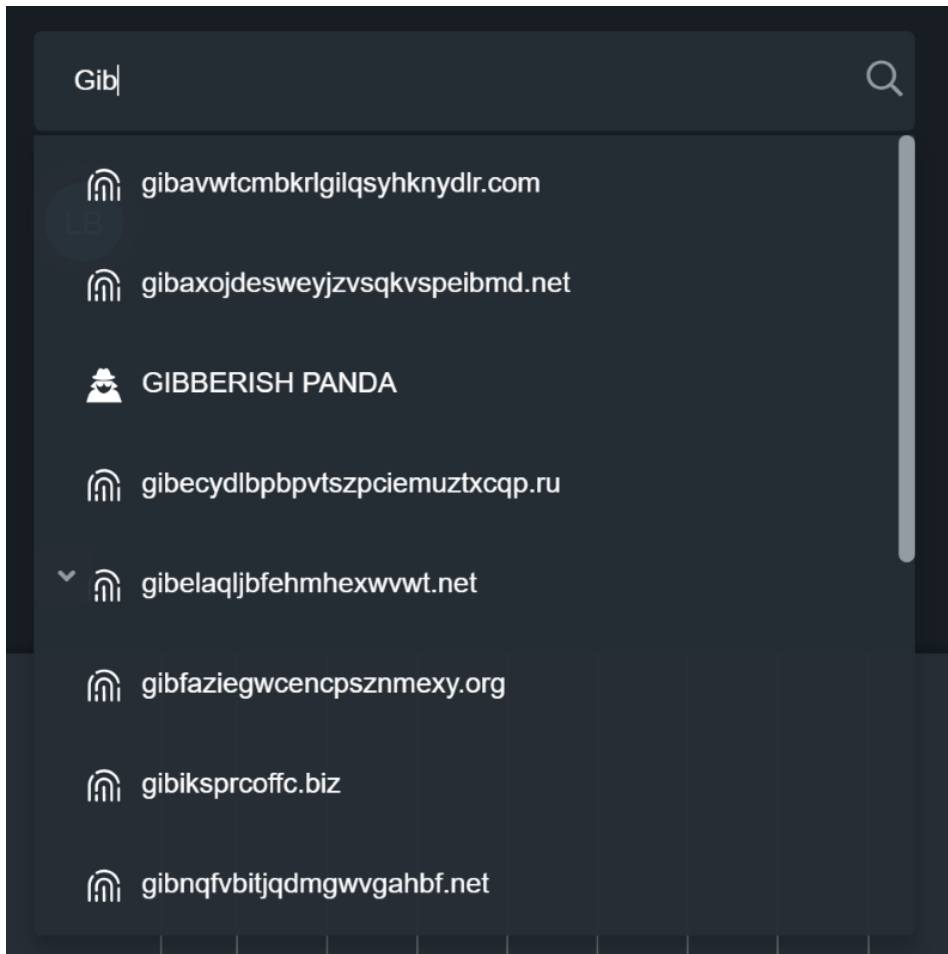
Adding Threat Intelligence Data to the Evidence Board

To begin an investigation, you must add threat intelligence data to the investigation workbench to explore and research. ThreatQ objects, such as indicators, adversaries, files, signatures, and events appear on the evidence board as nodes.



When you add an object to the evidence board, it becomes available for further examination. However, it does not immediately become a part of the current investigation. You must explicitly assign the object to the investigation. For more information, see [Adding an Object to an Investigation](#).

1. On the evidence board in the upper left corner, enter your search criteria to search the Threat Library for threat intelligence data.



If you enter an object name that is not found, you can click the Create link to add the new object. Then, select the object type you want to create from the drop-down list.

2. When you discover your object, mouse over and select it.
The object appears as a node highlighted on the evidence board.



Relevant information about the object, such as when it was first seen and where it originated appears on the timeline. With the object highlighted as the focal point, a summary appears in the action panel.

Adding a Task to an Investigation

ThreatQ allows you to create and assign tasks to yourself or other users in the platform. You can also use tasks in ThreatQ Investigations. When you assign a new task, you can add contextual information and correlate with Indicators, Events, Adversaries, Signatures, and Files.

For more information about Tasks, see the ThreatQ Platform documentation.

1. Right-click on an empty portion of the evidence board and select **New Task**. The Add Task dialog box opens.
2. Enter a task **Name**.
3. Enter the assignee's email address in the **Assigned To** field.
4. Optionally, use the date picker to select a **Due Date**.
5. Select one of the following statuses:
 - To Do
 - In Progress
 - Review
 - Done

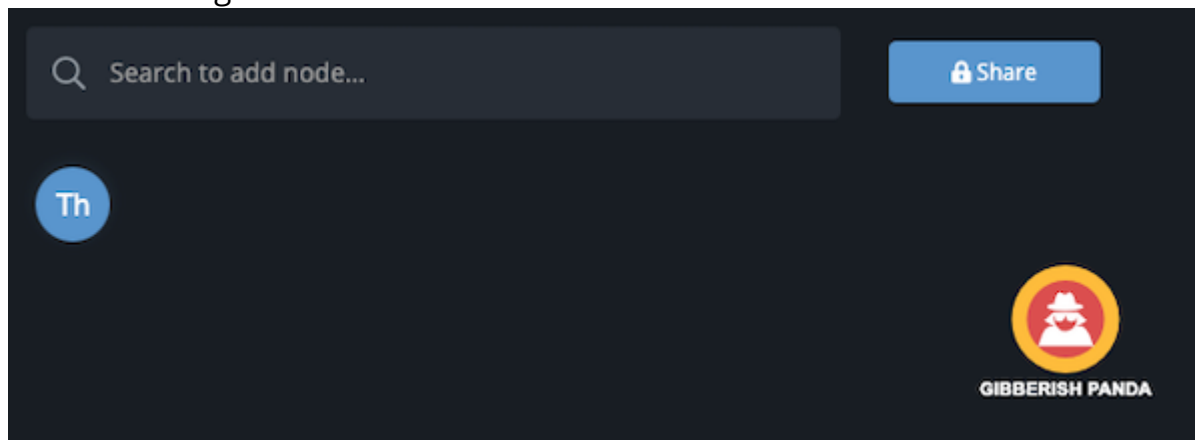
7. Select one of the following task priorities:
 - Low
 - Medium
 - High
8. Optionally, enter any **Associated Objects**.
9. Enter a **Description** for the task.
10. Click **Save**.

The task is added to the evidence board and the timeline.

Managing Threat Intelligence Data on the Evidence Board

After an object is added to the investigation workbench, you can manage it on the evidence board.

1. On the evidence board, select and highlight the node that represents the object you want to manage.



2. The following table describes the actions you can take to manage your object on the evidence board.

TO	YOU CAN
View the object's details page	Right-click the node and select View Details ; see Accessing an Object's Details Page from the Evidence Board .
View the object's relationships on the evidence board	Right-click the node and select Expand ; see Viewing an Object's Relationships on the Evidence Board .
Add the highlighted object to the investigation	Right-click the node and select Commit to Investigation ; see Adding an Object to an Investigation .
Select objects	Right-click the node and click Select . From this option, you can select all the objects on the Evidence Board or

TO	YOU CAN
	all objects of a specific type, such as all adversaries or all attack patterns.
Add a new task related to the object	Right-click the node and select New Task ; see Adding a New Task Related to an Object .
Add a new timeline entry related to the object	Right-click the node and select New Timeline Entry ; see Adding a New Timeline Entry Related to the Object .
Unlock or lock an object	Right-click the node and select Unlock or Lock ; see Locking and Unlocking an Object on the Evidence Board .
Delete an object from the evidence board	Right-click the node and select Remove ; see Deleting an Object from the Evidence Board .
Create an object	Right-click any location on the Evidence board and select Create Object ; see Creating an Object from the Evidence Board .
Share an investigation	Click the Share button; see Sharing an Investigation .

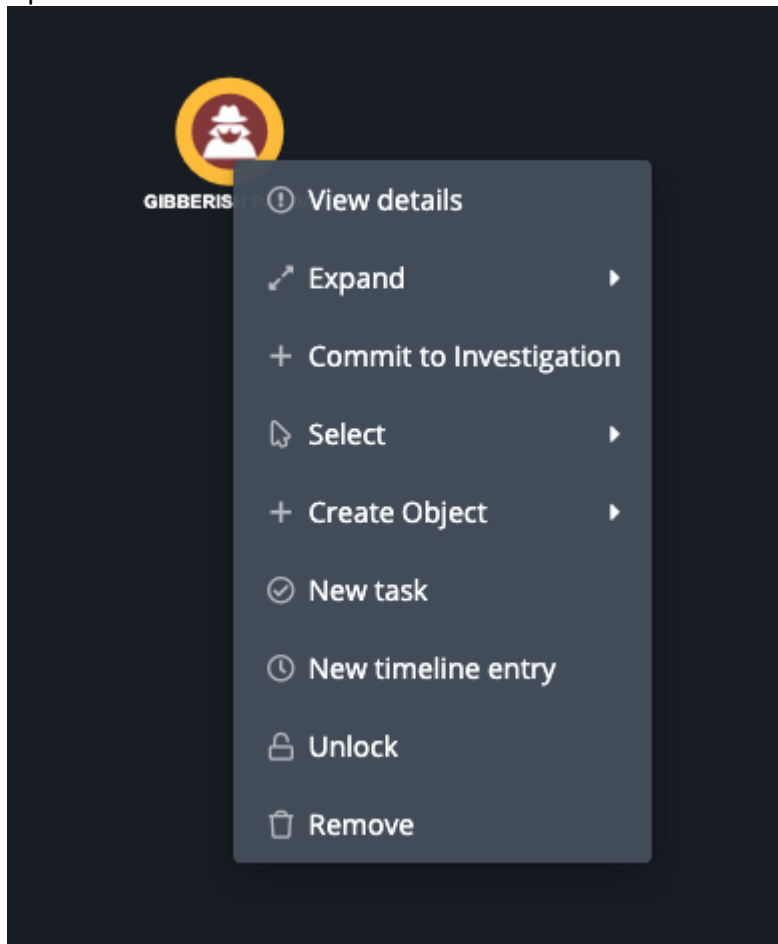
3. After you add an object to an investigation, the following additional options are available from the right-click menu:

TO	YOU CAN
Create a new object and link it to another	Right-click the node and select Create Object And Link ; see Creating and Linking a New Object
Remove an object from the investigation	Right-click the node and select Remove from Investigation . When you remove an object from an investigation. It remains displayed on the Evidence Board until you delete it; see Deleting an Object from the Evidence Board .

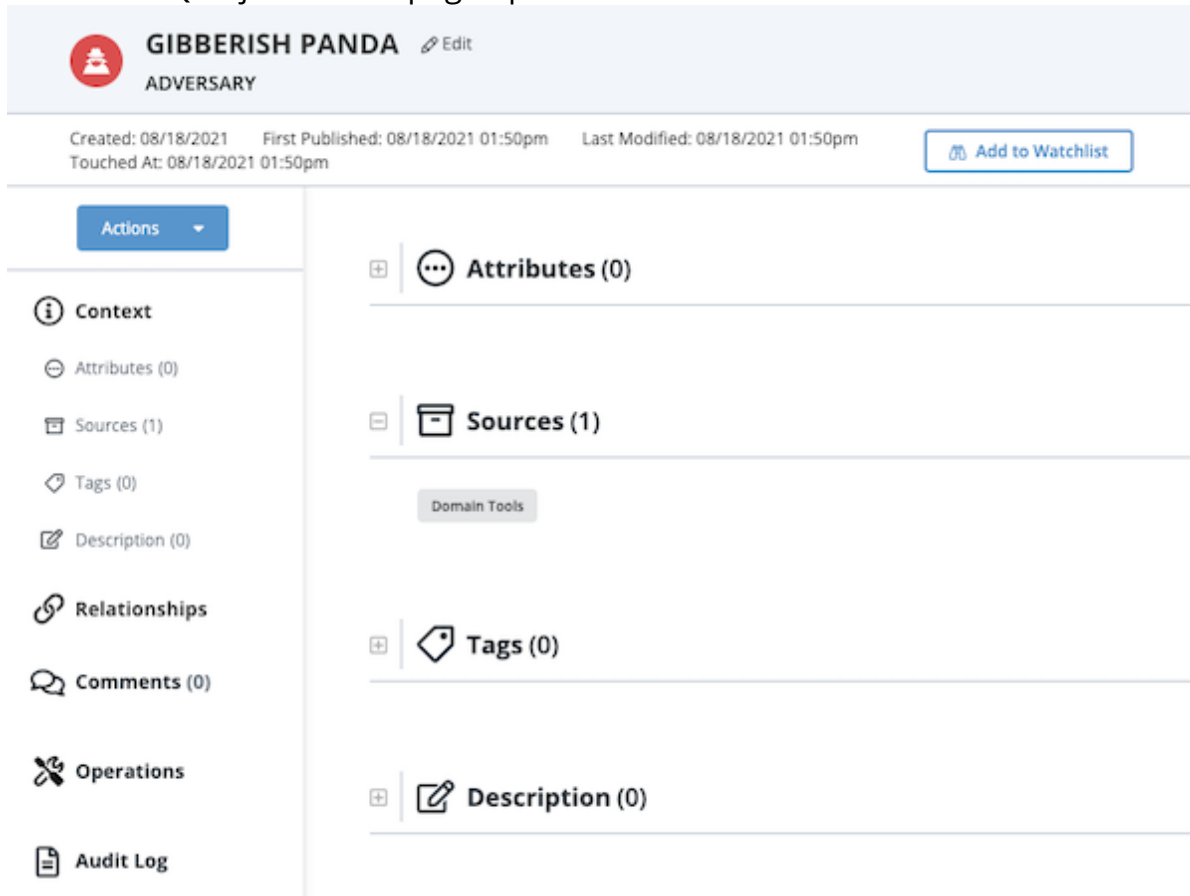
Accessing an Object's Details Page from the Evidence Board

You can select an object on the evidence board and launch its object details page in ThreatQ for further investigation. For more information about ThreatQ objects, see the ThreatQ Platform documentation.

1. On the evidence board, right-click the node you want to view and select the **View Details** option.



The ThreatQ object details page opens in a new browser tab

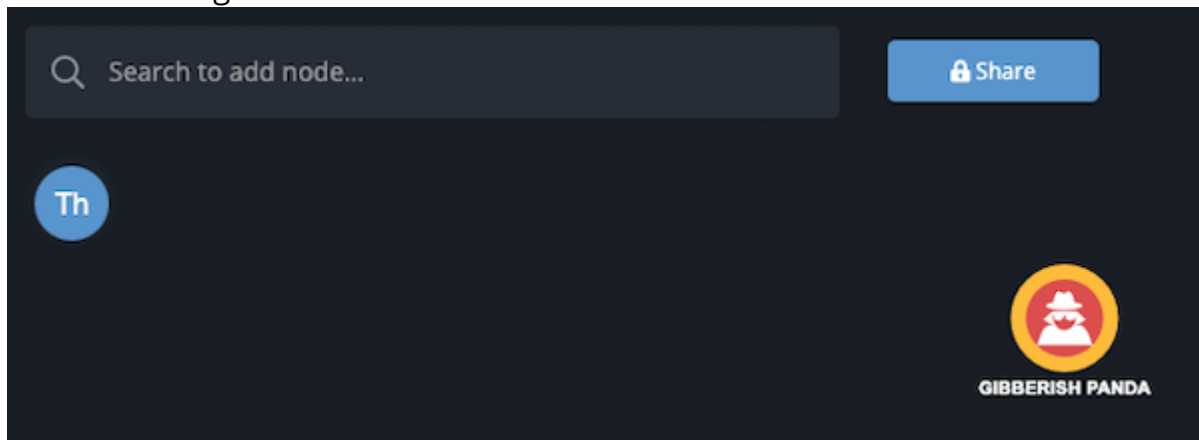


The screenshot shows the ThreatQ object details page for an adversary named "GIBBERISH PANDA". The page has a light blue header with the object name and an "Edit" link. Below the header, it displays metadata: "Created: 08/18/2021", "First Published: 08/18/2021 01:50pm", "Last Modified: 08/18/2021 01:50pm", and "Touched At: 08/18/2021 01:50pm". There is an "Add to Watchlist" button. A left sidebar contains a list of sections: Context, Attributes (0), Sources (1), Tags (0), Description (0), Relationships, Comments (0), Operations, and Audit Log. The main content area shows expandable sections for Attributes (0), Sources (1), Tags (0), and Description (0). The Sources section is expanded, showing a "Domain Tools" button.

Viewing an Object's Relationships on the Evidence Board

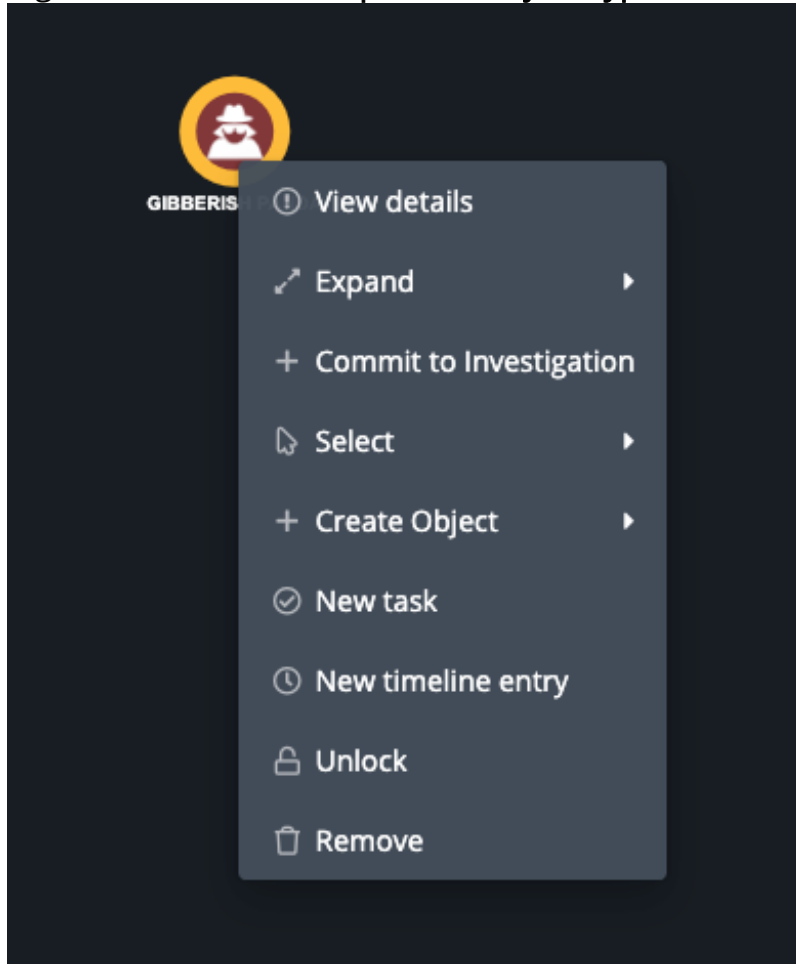
After you add an object to the evidence board, you can view the object's relationships to other nodes, such as attributes and related indicators.

1. On the evidence board, select and highlight the node that represents the object you want to manage.

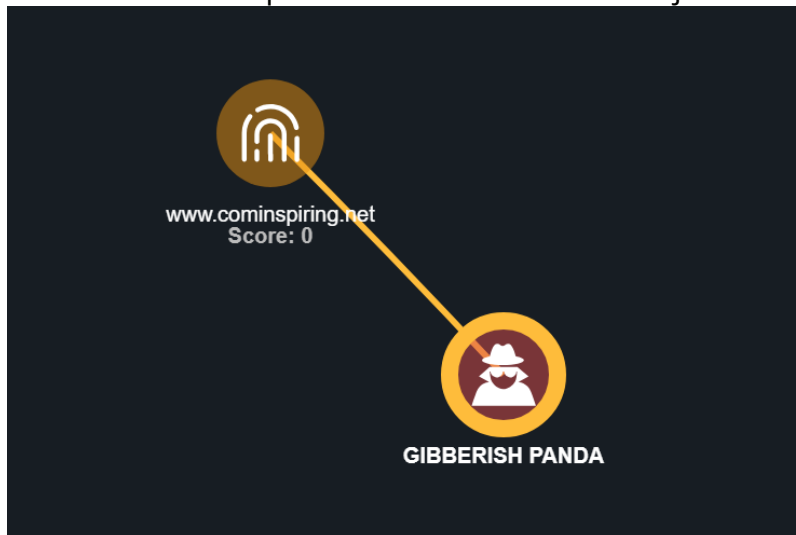


The screenshot shows the Evidence Board interface. At the top, there is a search bar with the placeholder text "Search to add node..." and a "Share" button. Below the search bar, there is a blue circular node with the letters "Th". In the bottom right corner, there is a circular logo with a red and yellow design, and the text "GIBBERISH PANDA" below it.

2. Right-click and select **Expand** > <Object Type> or Attributes.



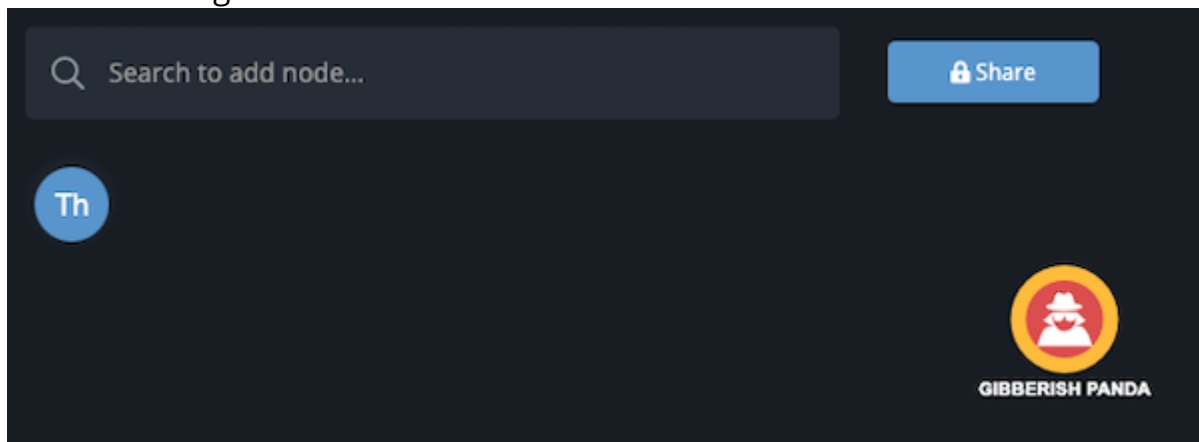
The node view expands to include related objects and attributes.



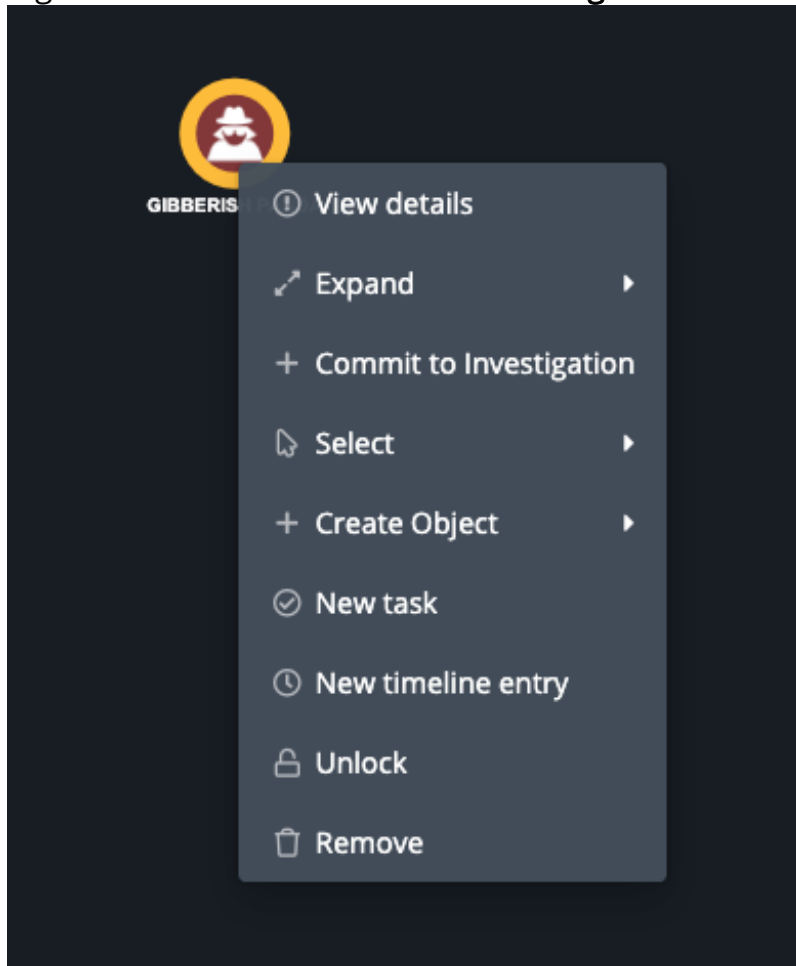
Adding an Object to an Investigation

When you add an object to the evidence board, it becomes available for further examination. However, it does not immediately become a part of the current investigation. You must explicitly assign the object to the investigation. Until you do so, only you can view the object in the investigation workbench, regardless of the investigation's visibility settings. After you add the object to the investigation, other ThreatQ users can view your work if the investigation is *shared*.

1. On the evidence board, select and highlight the node that represents the object you want to manage.



2. Right-click and select **Commit to Investigation**.



3. Optionally, you can remove the object from the investigation by right-clicking and selecting **Remove from Investigation**.

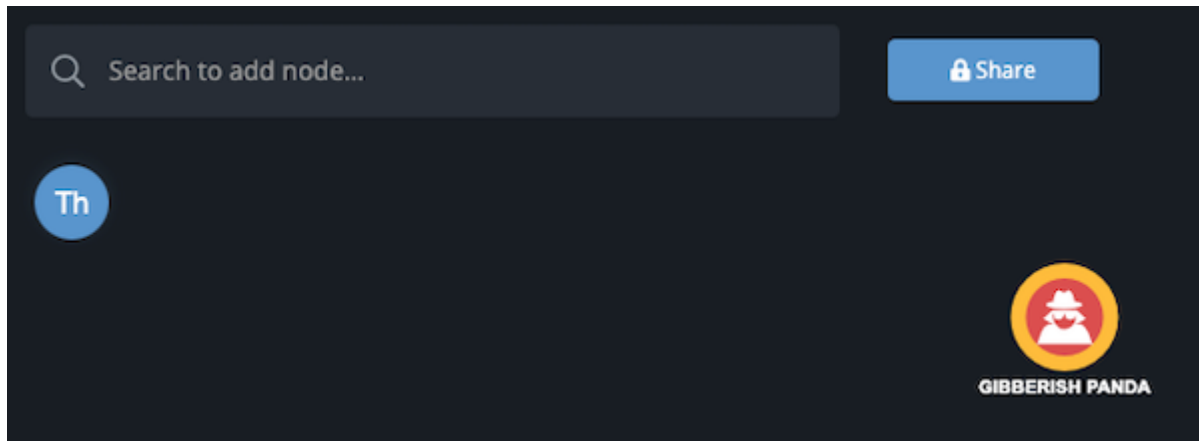
Adding a New Task Related to an Object

ThreatQ allows you to create and assign tasks to yourself or other users in the platform. You can also use tasks in ThreatQ Investigations. When you assign a new task related to an object on the evidence board, you are automatically adding contextual information and correlating the task with the selected object.

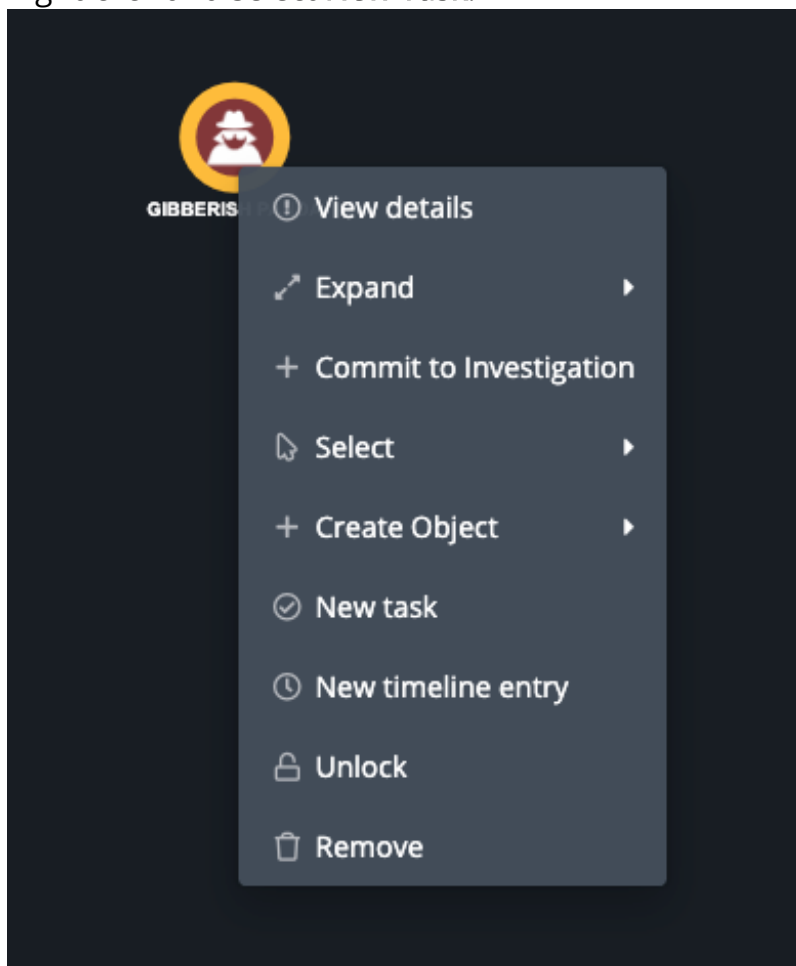
If an investigation owner or editor create a task for user who does not have access to the investigation, the user can access the task via Threat Library. However, he cannot view the investigation unless an owner or editor shares the investigation with him. In the Threat Library detail page, the Owner column lists the name of the investigation user so that the user can request access if needed.

For more information about Tasks, see the Tasks topic.

1. On the evidence board, select and highlight the node that represents the object you want to create a task for.



2. Right-click and select **New Task**.



The Add Task dialog box opens.

3. Populate the following fields:

FIELD NAME	DESCRIPTION
------------	-------------

Name	Enter the task name.
Assigned To	Enter the assignee's email address.
Reporter	Enter the email address of the reporter.
Due Date	Use the date picker to select a due date.
Status	Select a status for the task.
Priority	Select a priority for the task.
Related Objects	Use the search field to locate and add associated objects.
Description	Enter a brief description of the task.

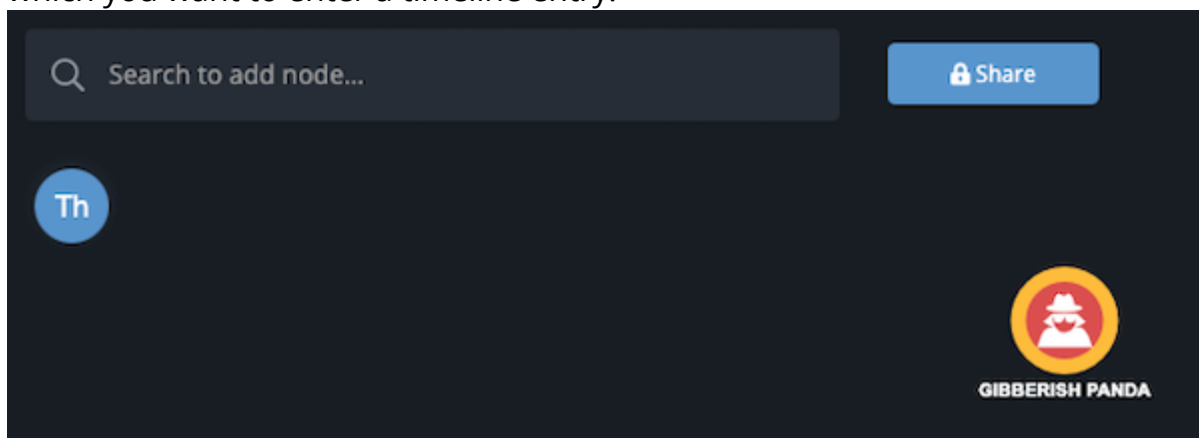
4. Click **Save**.

The task is added to the evidence board and the timeline.

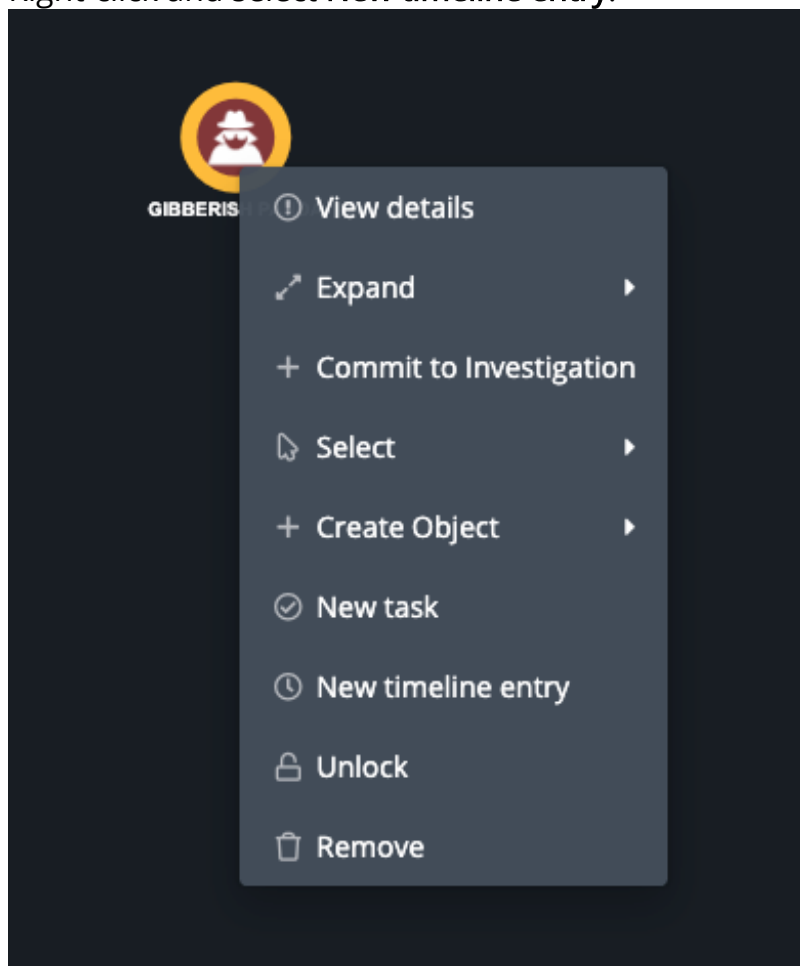
Adding a New Timeline Entry Related to the Object

When you add an object to the evidence board, some relevant attributes are included on the timeline. In addition, you can manually add timeline entries related to the object to use as milestones in the investigation. You can also add a timeline entry independent of a object; see [Adding a Timeline Entry](#).

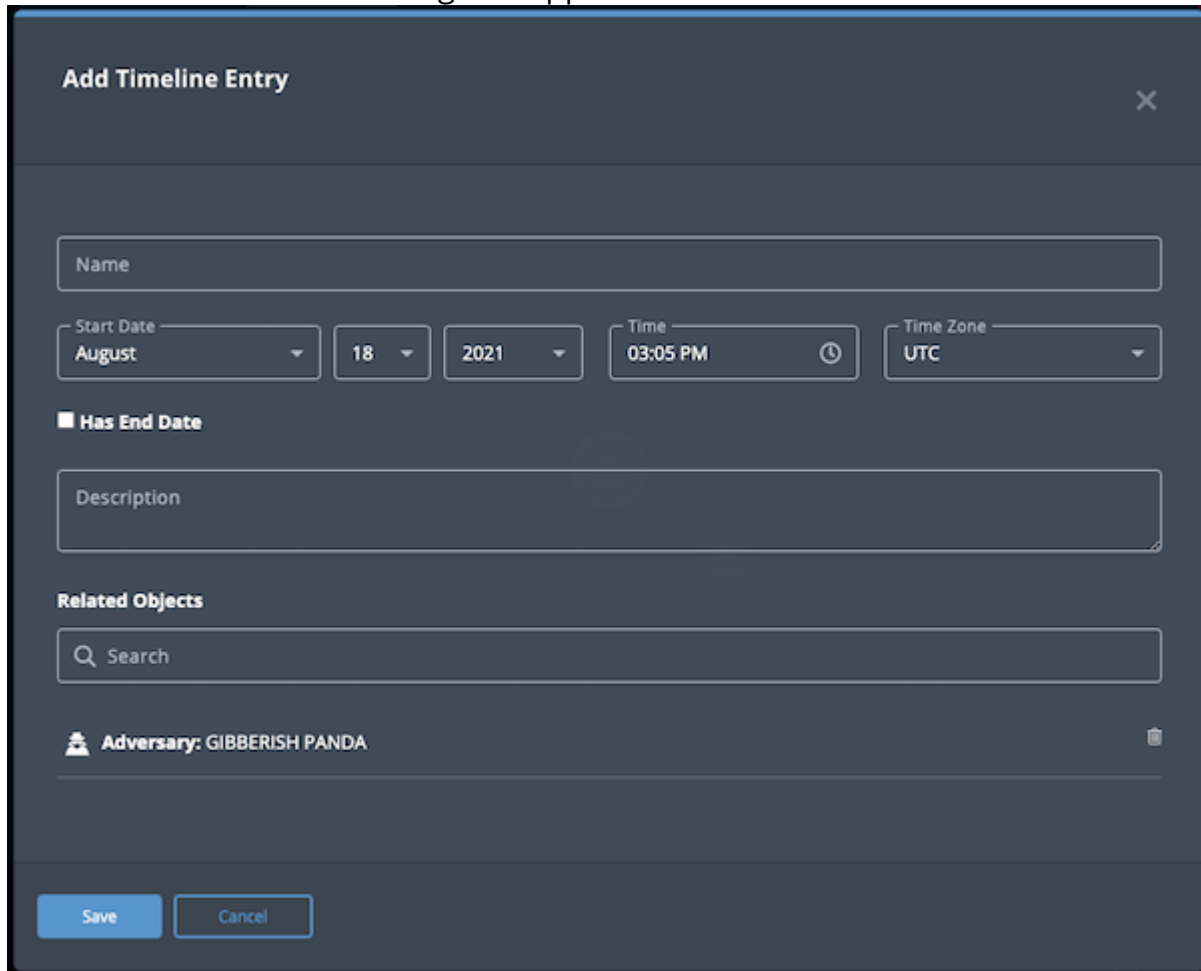
1. On the evidence board, select and highlight the node that represents the object for which you want to enter a timeline entry.



2. Right-click and select **New timeline entry**.



The **Add Timeline Event** dialog box appears.



Add Timeline Entry [Close]

Name

Start Date: August 18 2021 Time: 03:05 PM [Clock Icon] Time Zone: UTC

☒ Has End Date

Description

Related Objects

Search

Adversary: GIBBERISH PANDA [Trash Icon]

Save Cancel

3. Add the following information about the event:

- **Name**
- **Start Date, Time, and Time Zone**
- **End Date, Time, and Time Zone** - Check the **Has End Date** checkbox to access and populate these fields.
- **Description**
- **Related Objects**

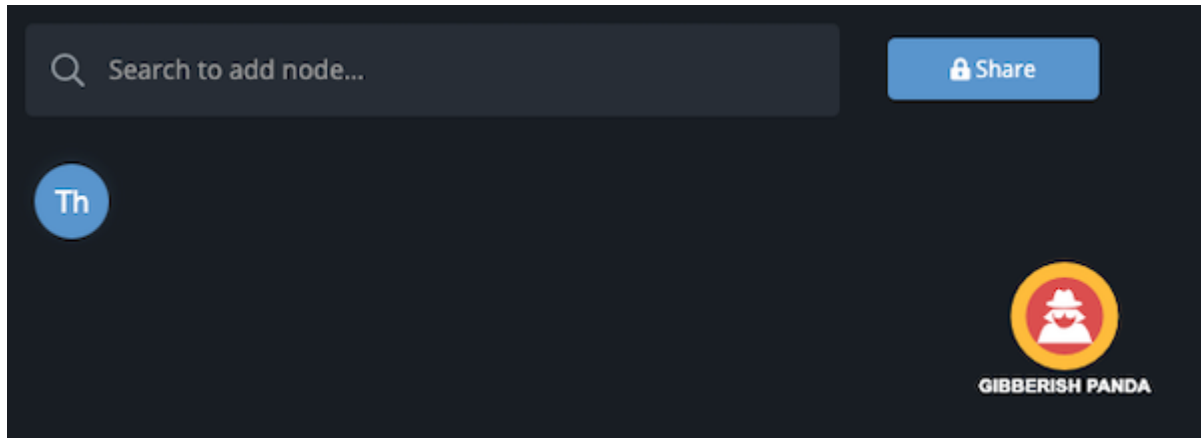
4. Click **Save**.

The new entry is displayed on the timeline.

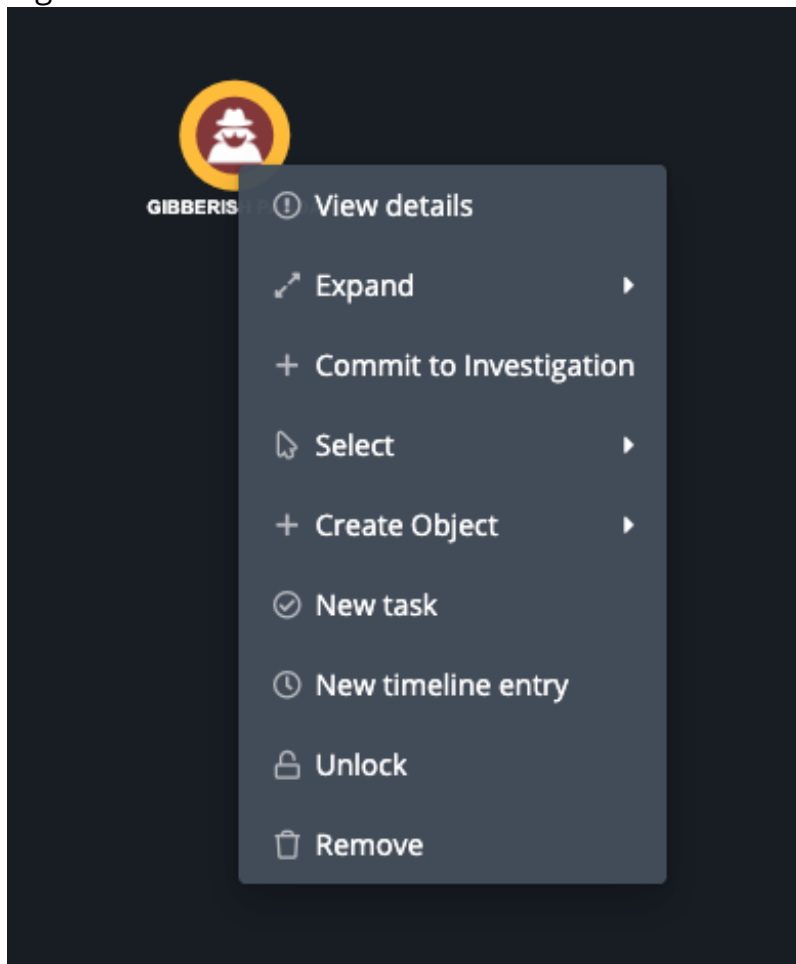
Locking and Unlocking an Object on the Evidence Board

When an object is locked on the evidence board, it is anchored to its current location and does not move when you click and drag a related attribute or object.

1. On the evidence board, select and highlight the node that represents the object you want to unlock.



2. Right-click and select **Unlock**.



3. Optionally, if you want to lock the object, right-click and select **Lock**.

Creating an Object from the Evidence Board

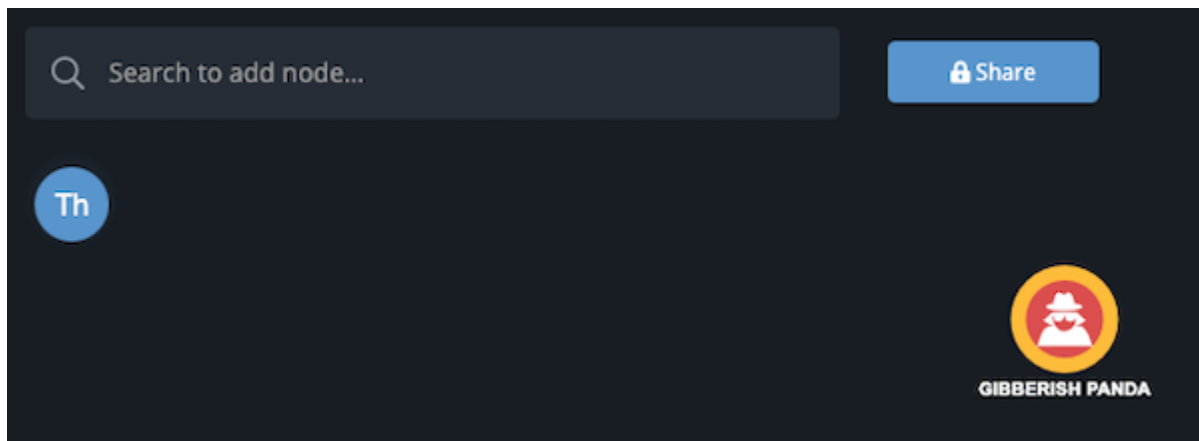
When you create a new object from the evidence board, it is automatically added to your current investigation.

1. Right-click the evidence board and select the **Create Object** option.
 2. Click the object type you want to create.
 3. Populate the corresponding object creation form.
 4. Click the Add button to save your entry.
- The new object is added to your current investigation.

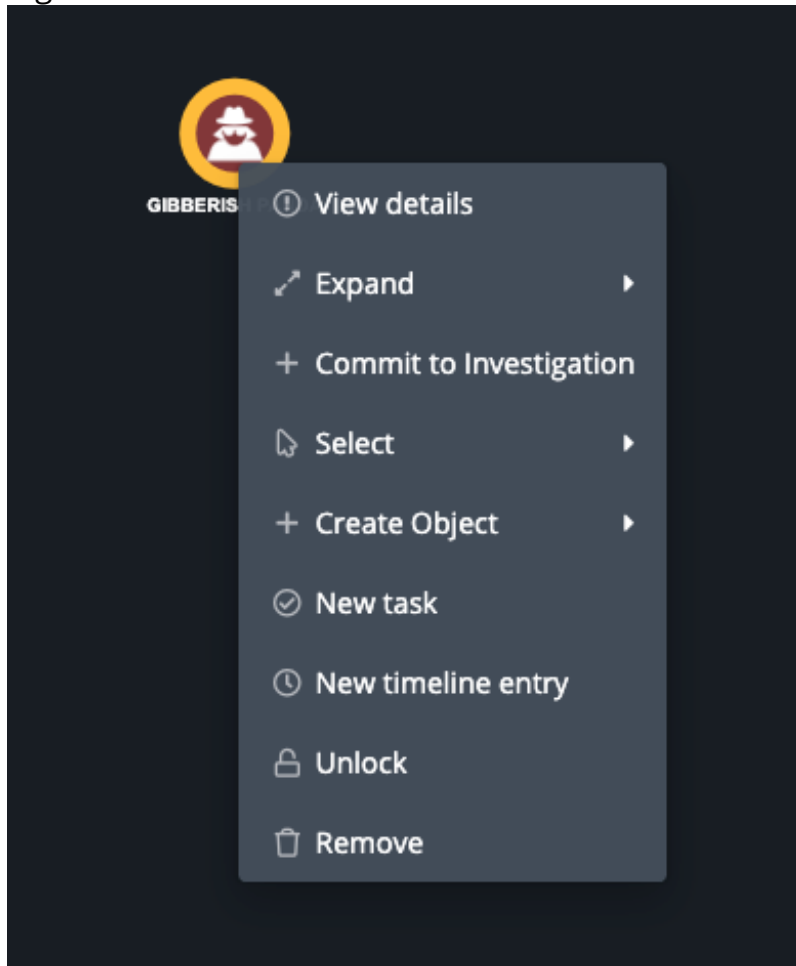
Deleting an Object from the Evidence Board

Deleting an object removes it from the evidence board and your investigation, but not from the ThreatQ platform.

1. On the evidence board, select and highlight the node that represents the object you want to remove.



2. Right-click and select **Remove**.



Selecting Multiple Objects on the Evidence Board

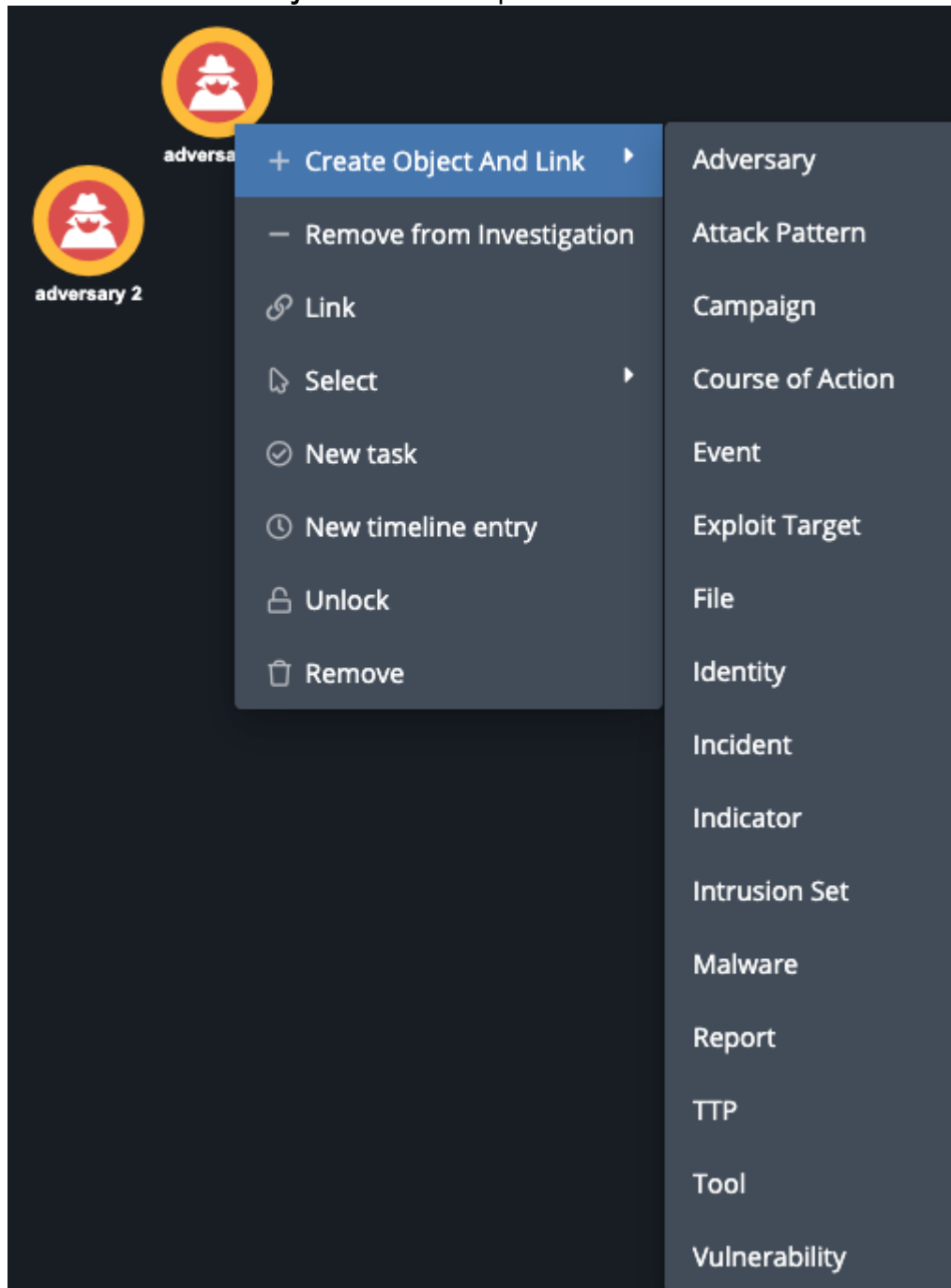
You can select multiple objects and apply changes to all objects at once. To multi-select objects, you can right-click and drag a selector box around the objects or press command (mac) or control (windows) and select the objects.

1. On the evidence board, press and hold command (mac) or control (windows), right-click and drag a selector box around the desired objects, then release the keyboard and mouse button.
The selected objects are highlighted on the evidence board.
2. Right-click and complete the available tasks as desired in [Managing Threat Intelligence Data on the Evidence Board](#).

Creating and Linking a New Object

The **Create Object And Link** option allows you to create a new object and link it to object(s) on the evidence board.

1. From the evidence board, select one or more nodes and right-click.
2. Select the **Create Object And Link** option.



3. From the object type list, select the type of object , such as an Adversary or Attack Pattern, you want to create.

The add form for the object type is displayed. The Related Objects section lists all the

nodes you selected in step 1. To remove a related object, click the trashcan icon next to the node.

4. Click the **Add <object type>** button to save the new object and add it to the evidence board. The object is linked to all the objects listed in the Related Objects section.

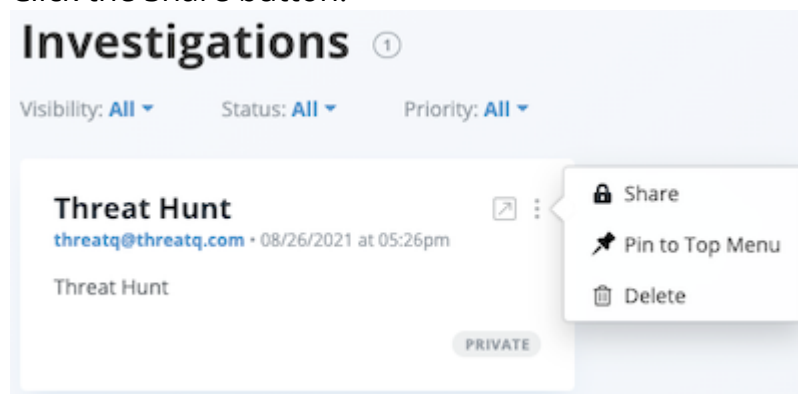
Sharing an Investigation

Owners and editors have the option to share an investigation with other users as well as update or remove their sharing permissions. In addition, the Share(d) button displayed depends on your permission level and the sharing status of the data collection.

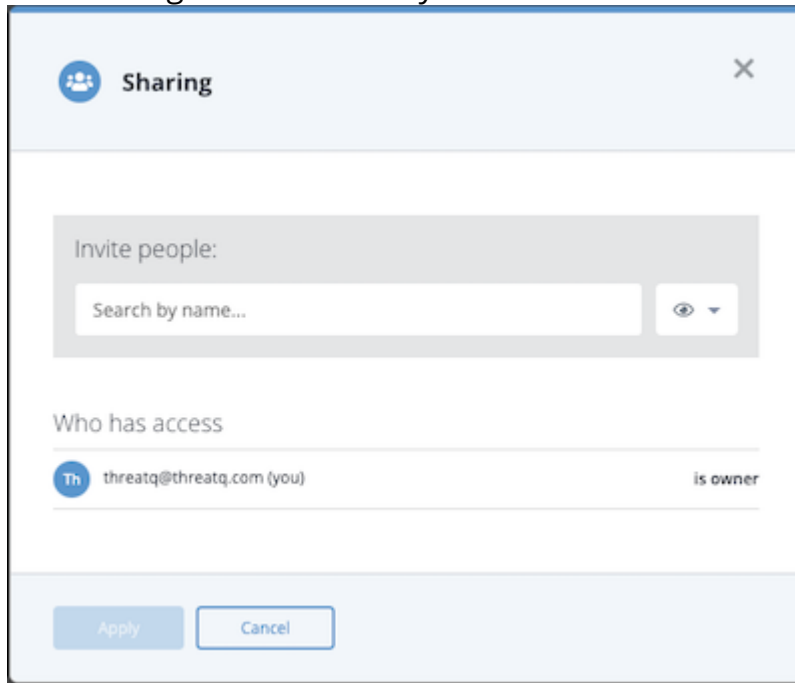
PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON
Owner	No	
Owner, Editor	Yes	
Viewer	Yes	

You can share an investigation from the Investigations page or the evidence board of the investigation. See the Sharing topic for more information on the user and group-level permissions you can assign to each investigation.

1. Access the evidence board of the investigation you want to share.
2. Click the Share button.



The Sharing window allows you to select the user to which you want to grant access.



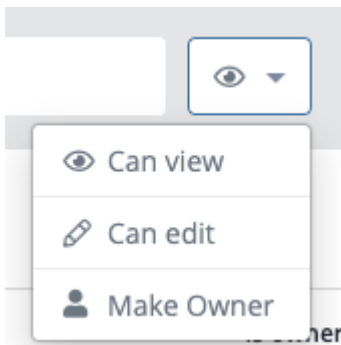
3. Click the arrow next to the  icon to select the user's permission level.



If you are granting access to all users, you must select the **Can View** option. You can only assign editing permission to individual users, not to all users.

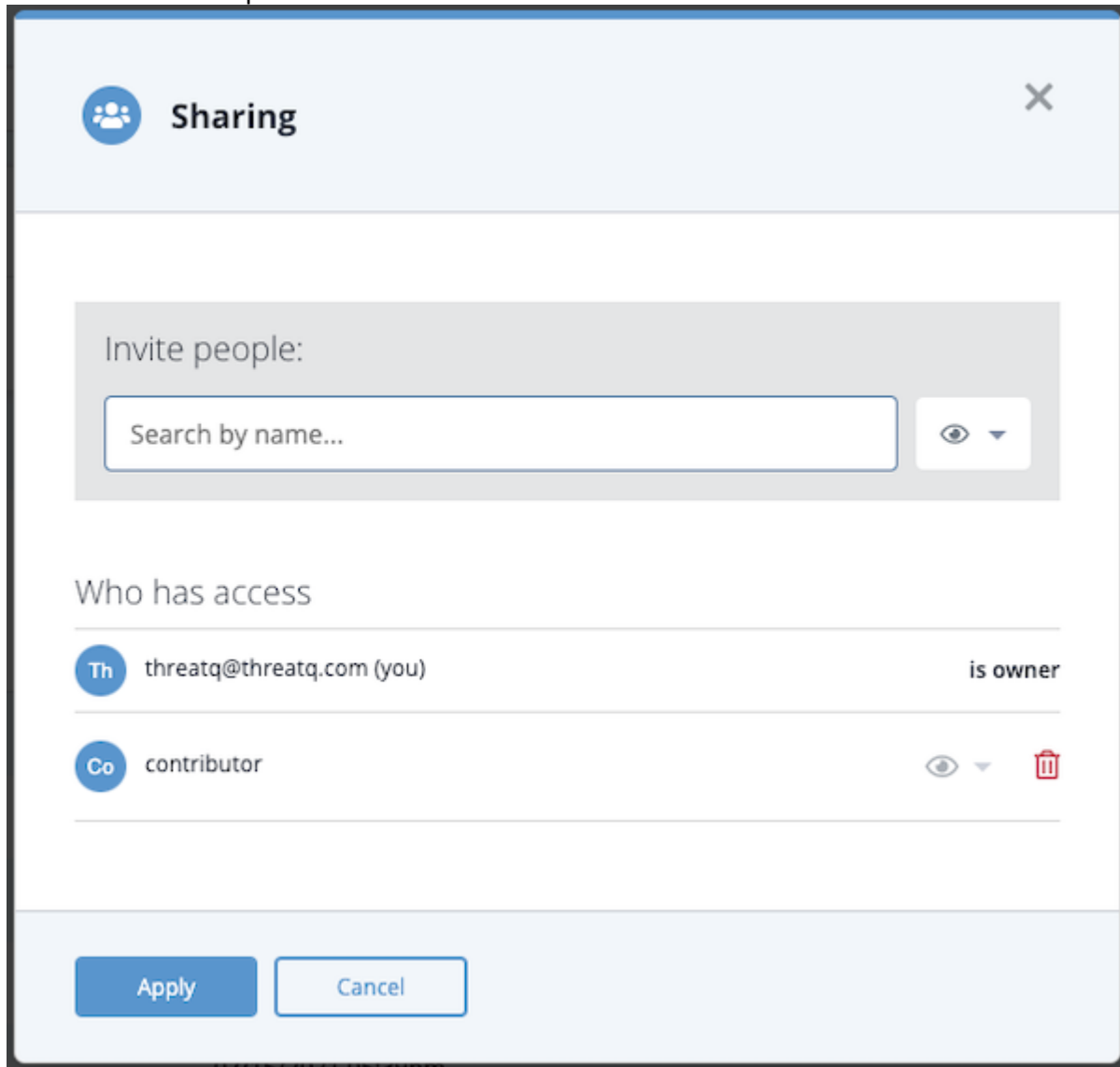


If you assign owner permissions to another user, your permissions automatically change to editor-level.



4. Use the search field to locate and select the user name or the **Everybody (Public)** option. This option grants view-only access to all users. The user is now listed in the Who has access list. From this listing, you can change or

delete the user's permissions.



The image shows a 'Sharing' dialog box with a light blue header and a close button (X) in the top right corner. Below the header is a section titled 'Invite people:' containing a search input field with the placeholder text 'Search by name...' and a button with an eye icon and a dropdown arrow. Below this is a section titled 'Who has access' which lists two users: 'threatq@threatq.com (you)' with the role 'is owner' and 'contributor' with a role dropdown (eye icon) and a delete button (trash icon). At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

5. Click the Apply button to save the user's permission level.

Using the Timeline

The following describes how to use the timeline in an investigation.

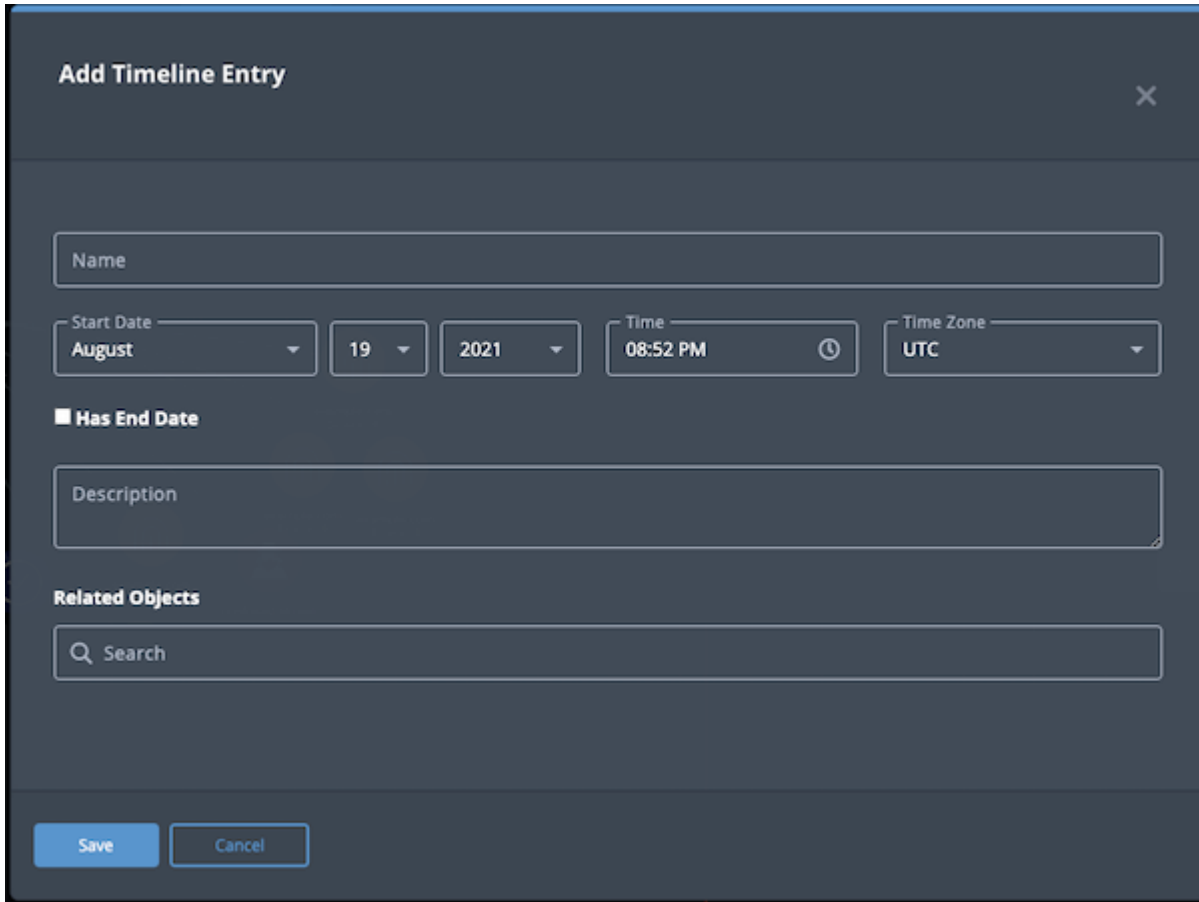
Timeline Overview

The timeline provides a view of milestones and tasks within an investigation. Most timeline events are auto generated, such as when ThreatQ first encountered an object and how the threat intelligence data was discovered, for example, via feed. When you create a task, it is also added to the timeline. Finally, you can create a timeline event associated with or independent of an object.

Adding a Timeline Entry

When you add an object to the evidence board, some relevant attributes are included on the timeline. You can also manually add timeline entries to use as milestones in the investigation.

1. Right-click an empty portion of the evidence board.
2. Select the **New Timeline Entry** option.
The **Add Timeline Event** window is displayed.



Add Timeline Entry ×

Name

Start Date: August 19 2021 Time: 08:52 PM Time Zone: UTC

☐ Has End Date

Description

Related Objects

Q Search

Save Cancel

3. Add the following information about the event:

- **Name**
- **Start Date, Time, and Time Zone**
- **End Date, Time, and Time Zone** - Check the **Has End Date** checkbox to access and populate these fields.
- **Description**
- **Related Objects**

4. Click **Save**.

A new entry appears on the timeline.

Viewing a Timeline Entry Summary

After an item is added to the timeline, you can view a summary of that item in the investigation workbench. Some of these panels allow you to perform actions, such as launching an object's details page and deleting a task.

1. From the investigation workbench, select an item on the timeline.
2. Double-click the item to open the summary panel.



GIBBERISH PANDA

Timeline Entry

🗑️

NAME _____

Escalating to Security Team

TIME _____

07/31/2018 05:01pm

AUTHOR _____

Leon Brown

RELATED OBJECTS _____

GIBBERISH PANDA

Escalating to Security Team

GIBBERISH PANDA first seen

GIBBERISH PANDA reported by CrowdStrike