ThreatQuotient

ThreatQ Investigations User Guide

Version 4.1.0

October 12, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Overview

ThreatQ Investigations is seeded as part of the ThreatQ platform. The versioning assigned to this PDF, 4.1.0, 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.

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.

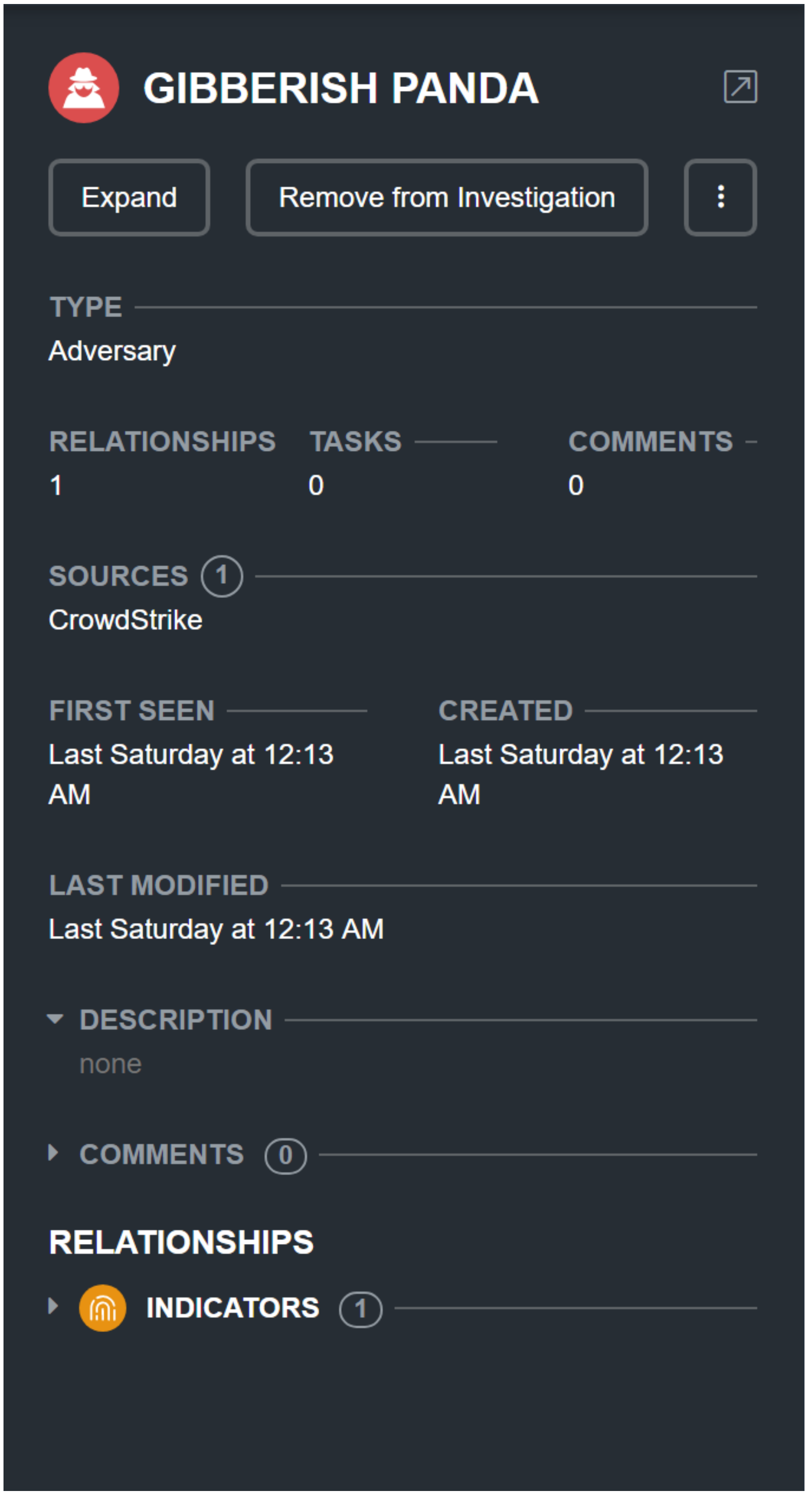
The evidence board allows you to:

- 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.

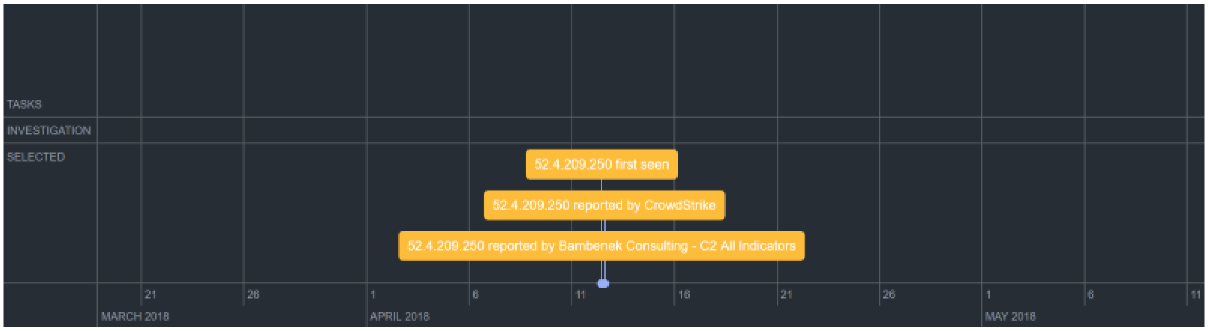


The action panel allows you to:

- 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.



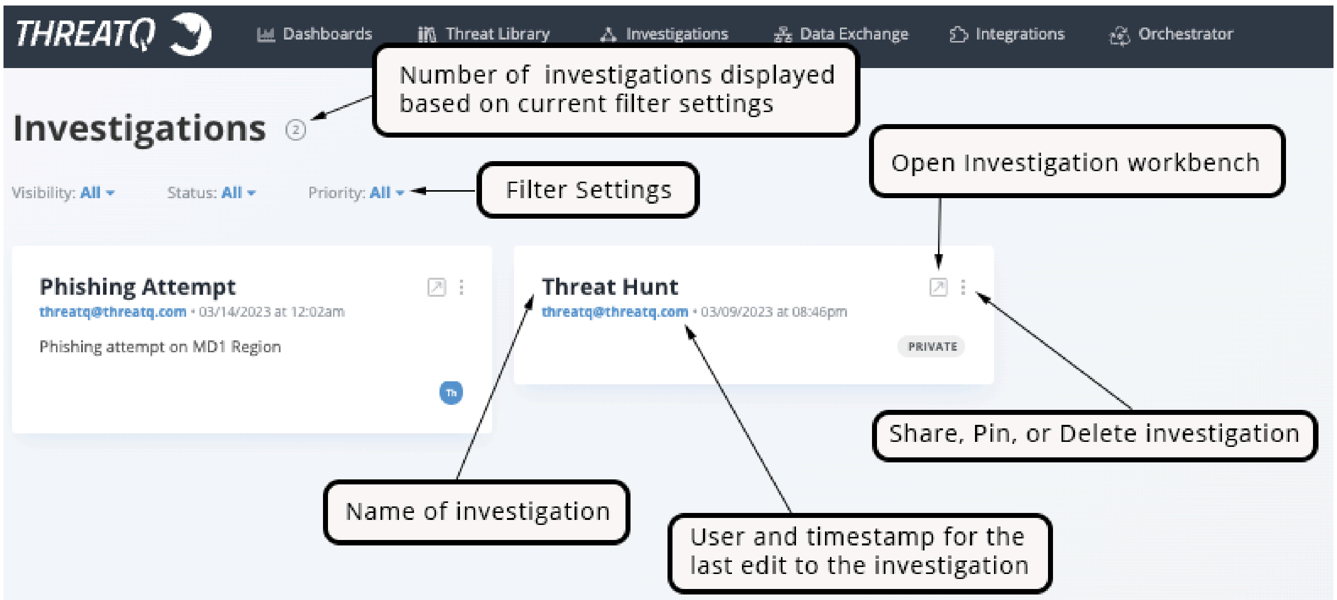
You can view:

- 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

About the Investigations Page

Investigations begins with the Investigations page. You can access the Investigations page by clicking on the Investigations link located in the top menu of the ThreatQ platform.



Visibility Filter

The Visibility filter allows you to filter your investigations by the sharing status of each investigation.

VISIBILITY OPTION	DESCRIPTION
All (default)	This option displays all investigations, private and shared.
Private	This option displays investigations you have created and that have not been shared with other users. These investigations will also have a **Private** tag located to the bottom-right of the investigation card.
Shared	This option displays investigations that you have shared with others or have been shared with you.

Status Filter

The Status filter allows you to filter your view by **Open** and **Closed** investigations.

Priority Filter

The Priority filter allows you to filter your investigations by the set priority. Options include:

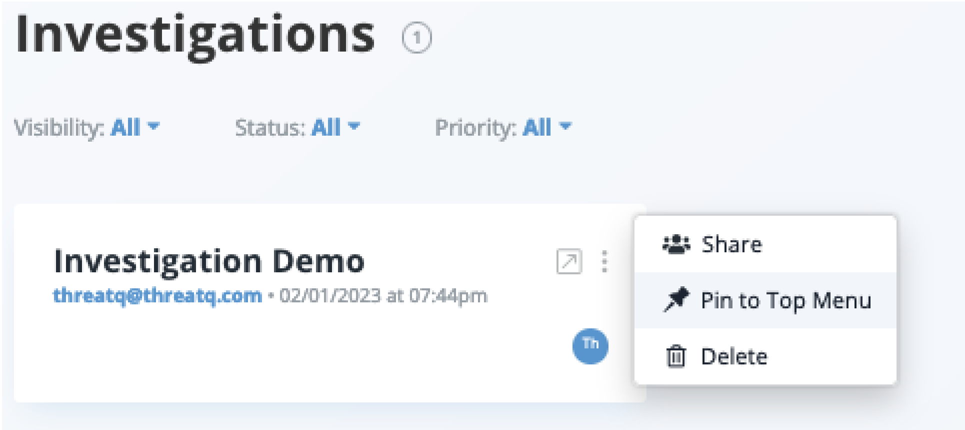
- All (default)
- Normal
- Escalated

> Priority designations should respect your organization's SOP.

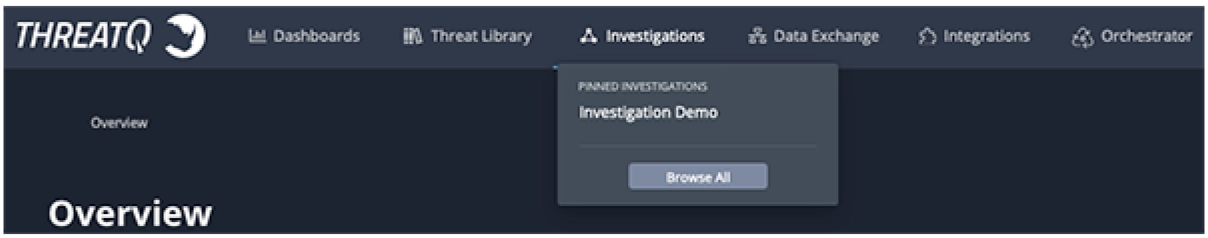
Pinning an Investigation

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.   You can repeat the same steps to unpin an investigation.

1. 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 Investigation will now appear under the Investigations menu.



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.

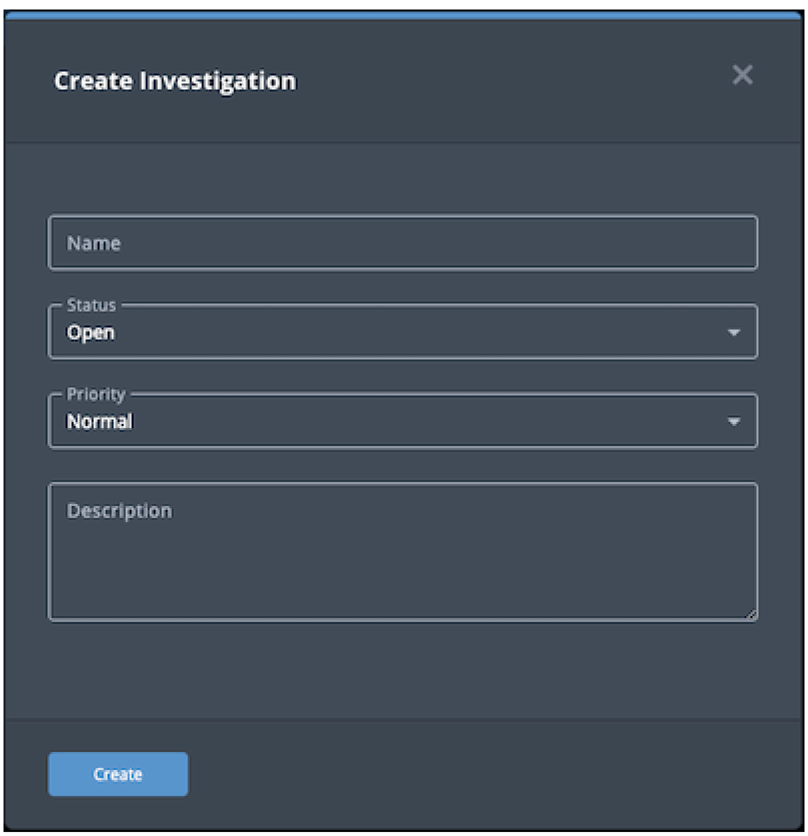
You can also pin an investigation from the Evidence Board.

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.



2. Populate the Create Investigation window as follows:

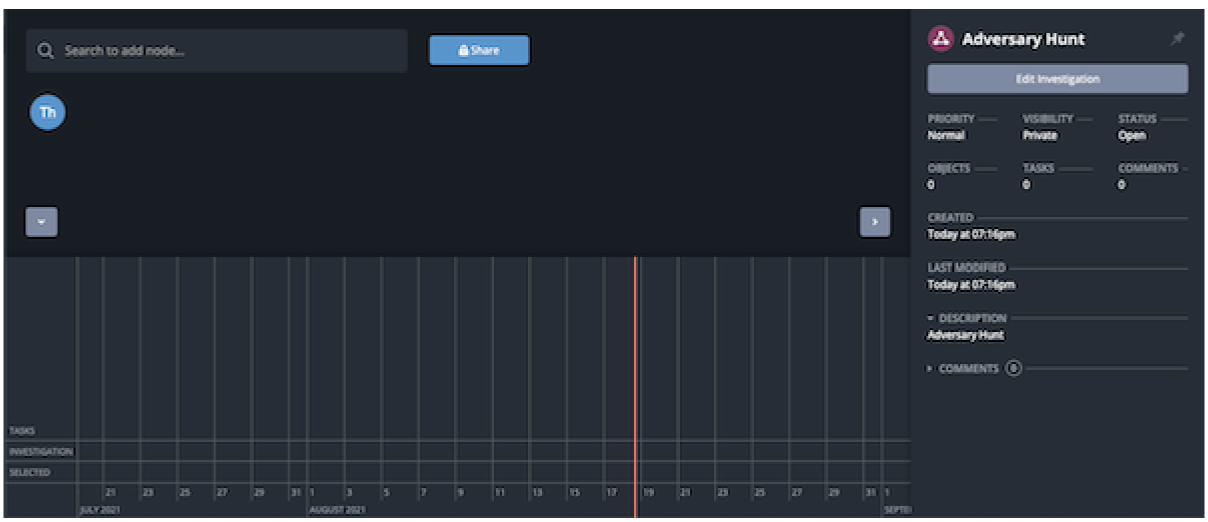
- Type a **Name** for the investigation.
- Select a **Status**:
  - **Open** - Open investigations appear as normal on the Investigations page.
  - **Closed** - Closed investigations appear greyed out on the Investigations page.
- Select a **Priority**:

  > 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.



Sharing Investigations

You can share an investigation you have created with one or more users as well as set their permission level for the investigation.

Sharing Permission Levels

You can set permission levels for individual users within your organization as well as assign all users to the Viewer role. Options include:

PERMISSION LEVEL	DESCRIPTION	NOTES
Viewer (Can View)	User can view the investigation.	You can use the Everybody option to assign the Viewer role to all users.
Editor (Can Edit)	User can view and edit the investigation.	While you can assign multiple users to the Editor role, this must be performed one user at a time. You also cannot assign all users (Everybody group) to the Editor role.
Owner (Make Owner)	Owner User can view, edit, close, and share the investigation with others.	There can only be one owner for an investigation. If you assign another user as the owner of your investigation, your permissions will automatically be updated to Editor.

Sharing Status Icon

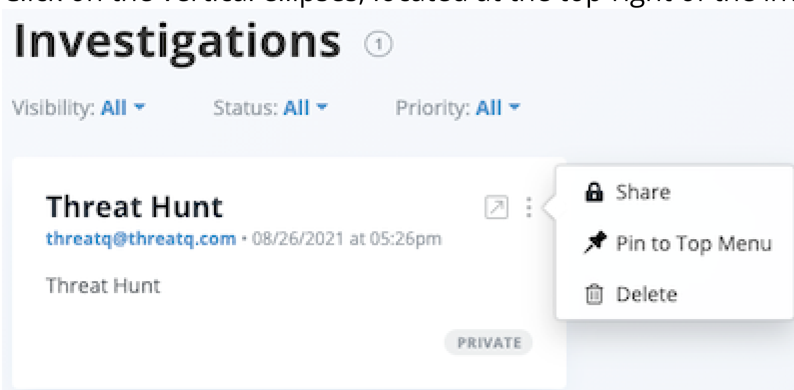
The Share(d) button displayed depends on your permission level and the sharing status of the investigation.

PERMISSION LEVEL	SHARED WITH OTHERS?	SHARE(D) BUTTON
Owner	No	

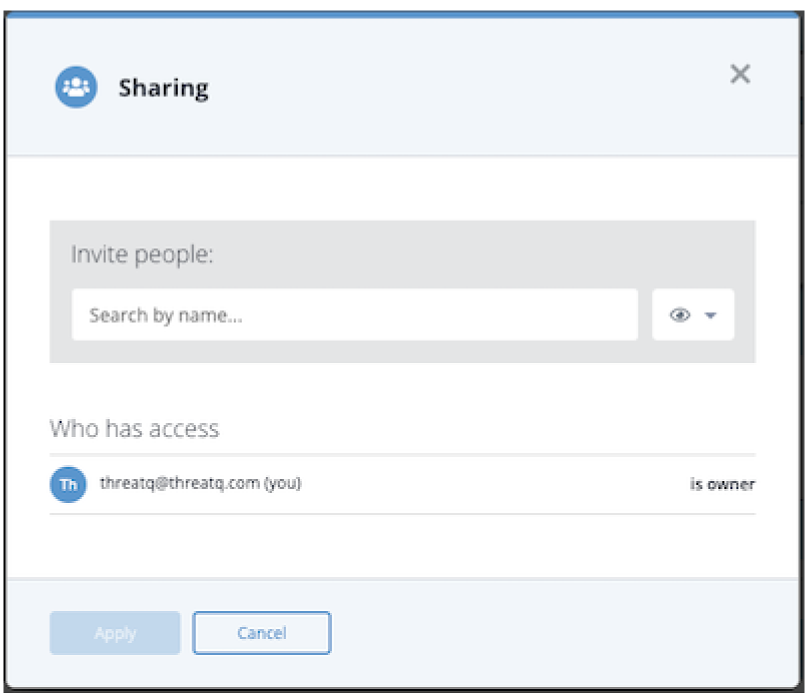
Owner, Editor	Yes	Share
Viewer	Yes	Shared

Sharing an Investigation from the Investigations Landing Page

1. Navigate to the Investigations landing page and locate the investigation you intend to share.
2. Click on the vertical ellipses, located at the top-right of the investigation card, and select **Share**.



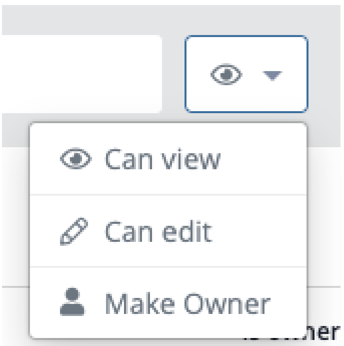
The Sharing window allows you to select the user to which you want to grant access.



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.

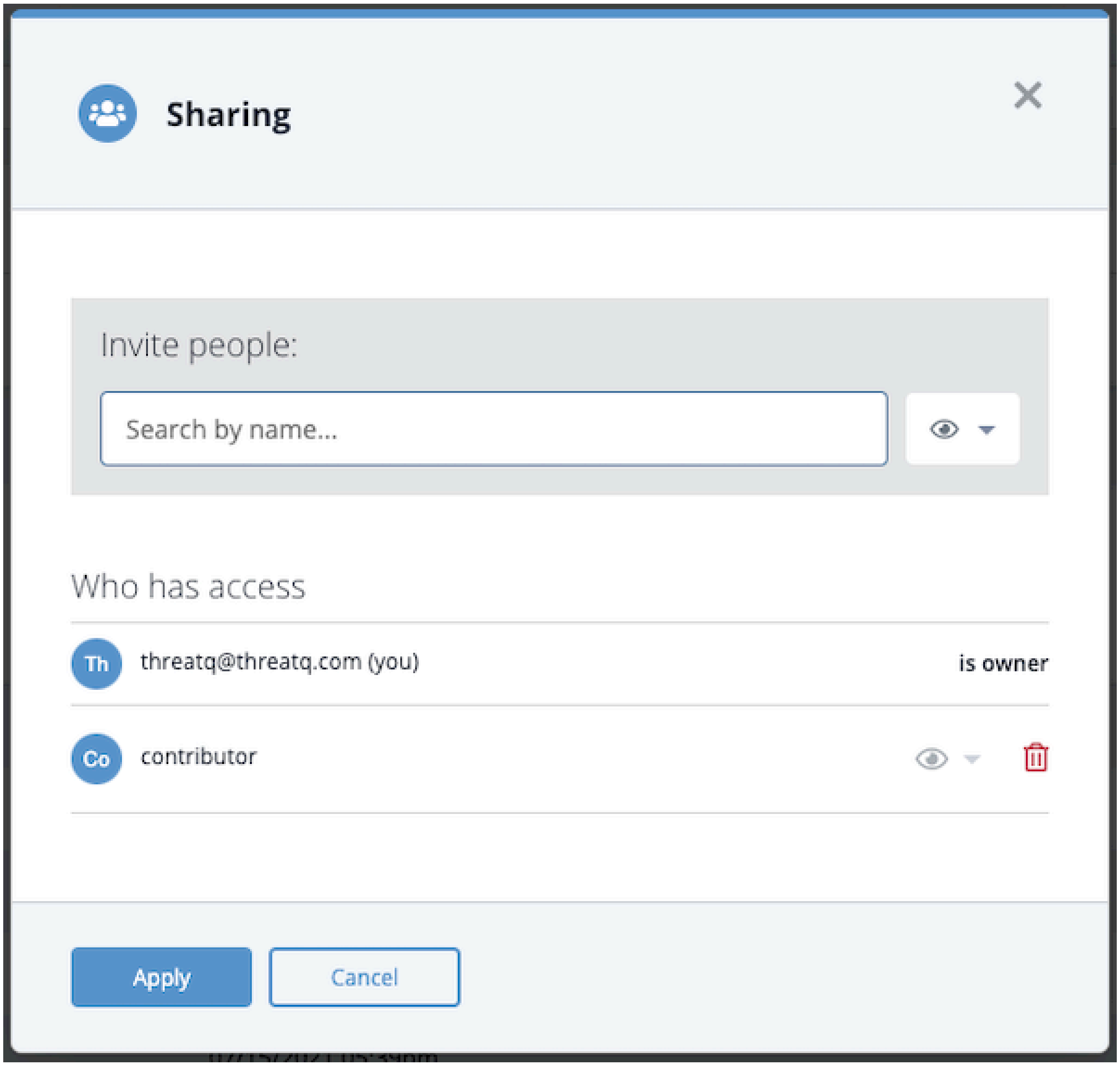
If you assign owner permissions to another user, your permissions automatically change to editor-level.



4. Use the search field to locate and select the user you intend to share the investigation with.

You can also use the **Everybody (Public)** option. This option grants view-only access to all users.

The user is now listed in the **Who has access** list.

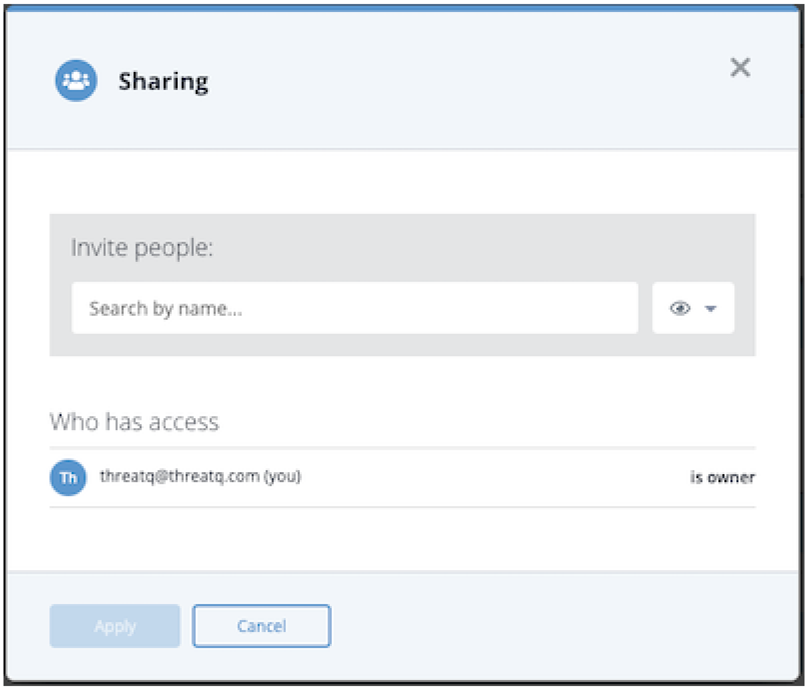


5. Click the **Apply** button to save the user's permission level.

Sharing an Investigation from the Evidence Board

1. Open an investigation and click on the **Share** button, located to the right of the search, on the Evidence Board.

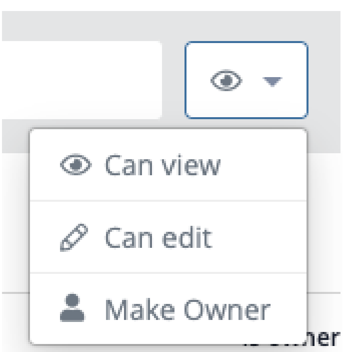
   The Sharing window will open.



2. 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.

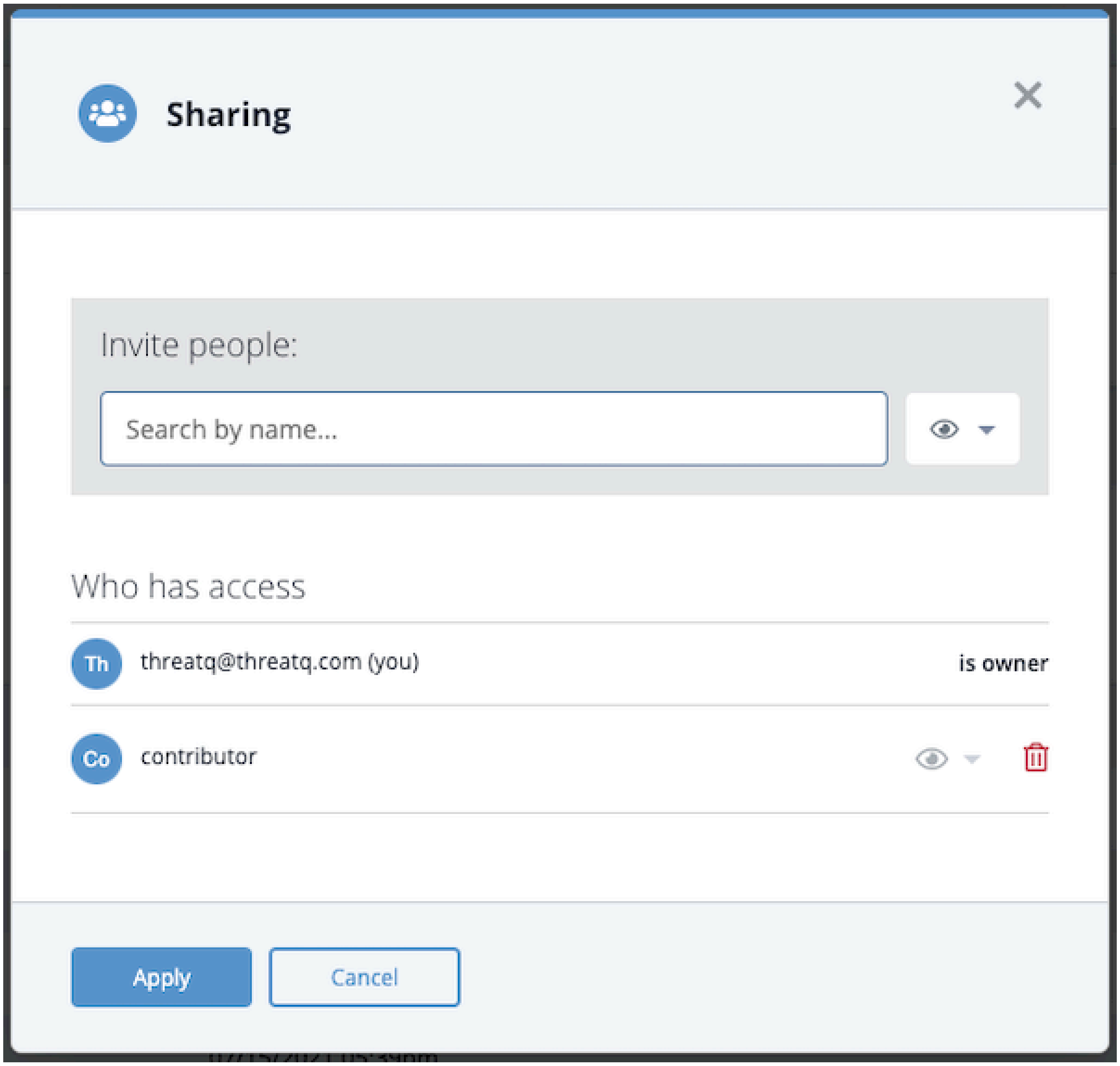
> If you assign owner permissions to another user, your permissions automatically change to editor-level.



3. Use the search field to locate and select the user you intend to share the investigation with.

> You can also use the **Everybody (Public)** option. This option grants view-only access to all users.

The user is now listed in the **Who has access** list.



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

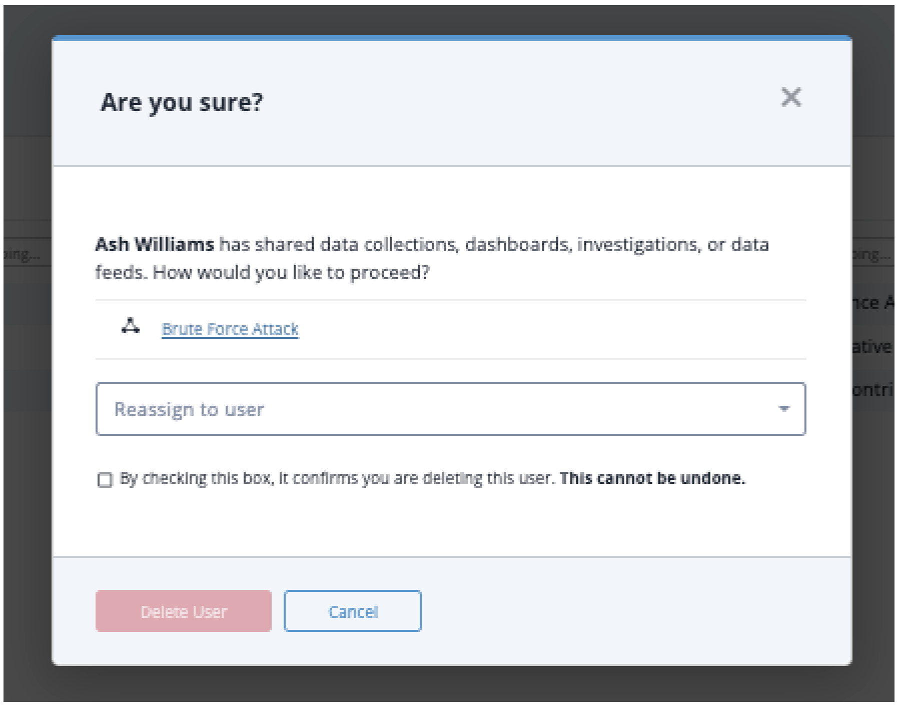
Unsharing an Investigation

You can remove an individual's access if you are the owner of an investigation.

1. Access the Sharing window from either the investigation's landing page card or from the Evidence Board.
2. Locate the user to remove under the **How has Access** section and click on the red trashcan located in the right column.
3. Click on **Apply** to save your sharing settings.

Reassigning Ownership when Deleting an Investigation Owner

In the event where an investigation owner's account is deleted from the ThreatQ platform, the administrator performing the delete will alerted that the account selected for deletion is the owner of one or more investigations, data feeds, and data collections. The adminstrator will be prompted to reassign ownership to another user before proceeding with the account deletion.



Deleting an Investigation

Deleting an investigation removes it from the Investigations page and also from your system. Take care in selecting this option as it cannot be undone.

> Only the owner of an investigation can delete it.

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**.

About Exploratory Data Points

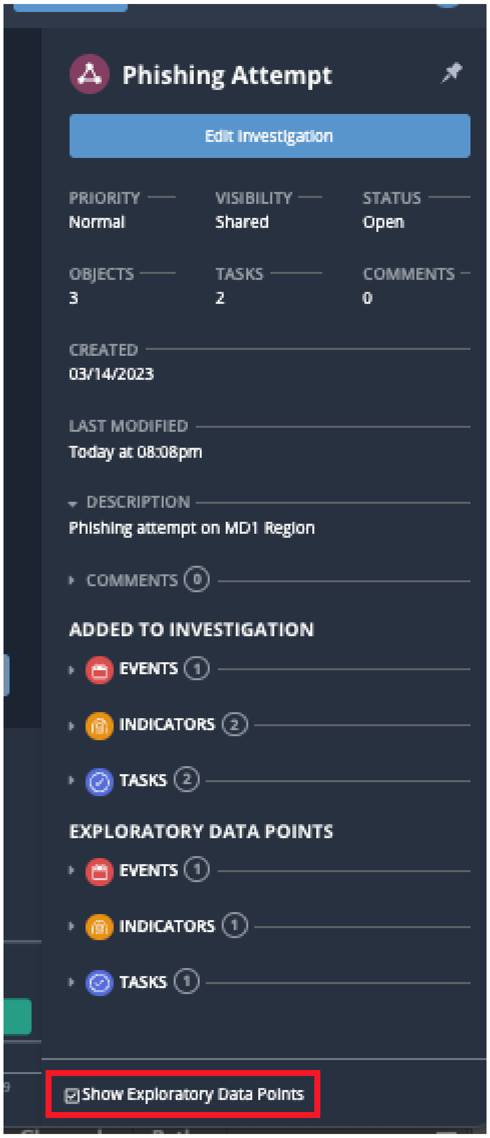
Exploratory Data Points are object nodes that have not been committed to an investigation. These nodes can be an individual object you have added to your investigation or related to another object in the investigation.

All objects begin as Exploratory Data Points until they have been committed to the investigation. Objects can be committed to an investigation by right-clicking on the object's node and selecting **Commit to Investigation**.

Showing/Hiding Exploratory Data Points for an Investigation

This option sets the visibility configuration for the entire investigation. You will not be able to show uncommitted object nodes on the Evidence Board if this option is not selected.

1. Click on any empty space on the Evidence Board to load the Investigation in the Action Panel.
2. Scroll to the bottom of the Action Panel and check/uncheck the **Show Exploratory Data Points** option.


Phishing Attempt
Edit Investigation
PRIORITY
Normal
VISIBILITY
Shared
STATUS
Open
OBJECTS
3
TASKS
2
COMMENTS
0
CREATED
03/14/2023
LAST MODIFIED
Today at 08:08pm
DESCRIPTION
Phishing attempt on MD1 Region
COMMENTS 0
ADDED TO INVESTIGATION
EVENTS 1
INDICATORS 2
TASKS 2
EXPLORATORY DATA POINTS
EVENTS 1
INDICATORS 1
TASKS 1
Show Exploratory Data Points

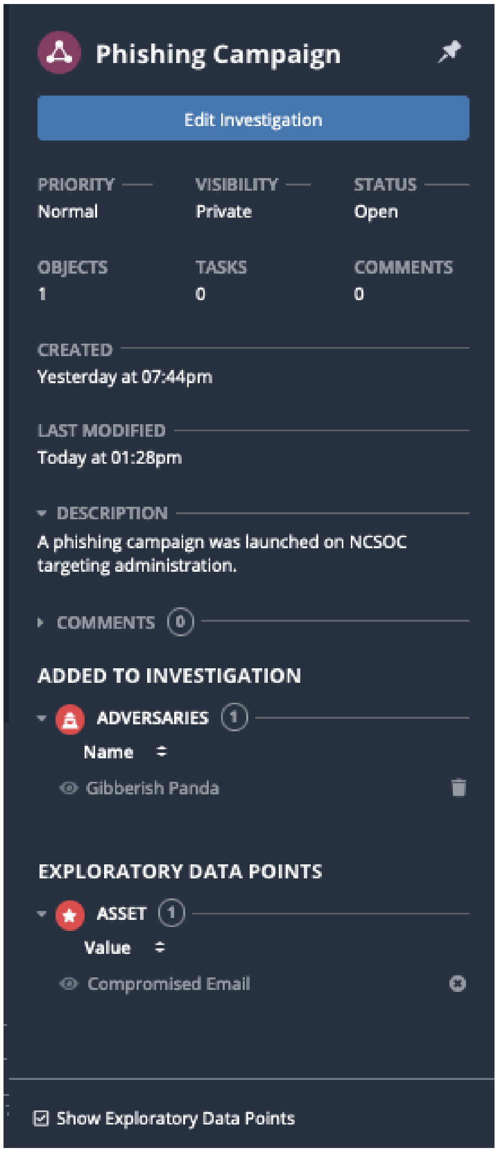
Action Panel

About the Action Panel

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.

Viewing Investigation Details

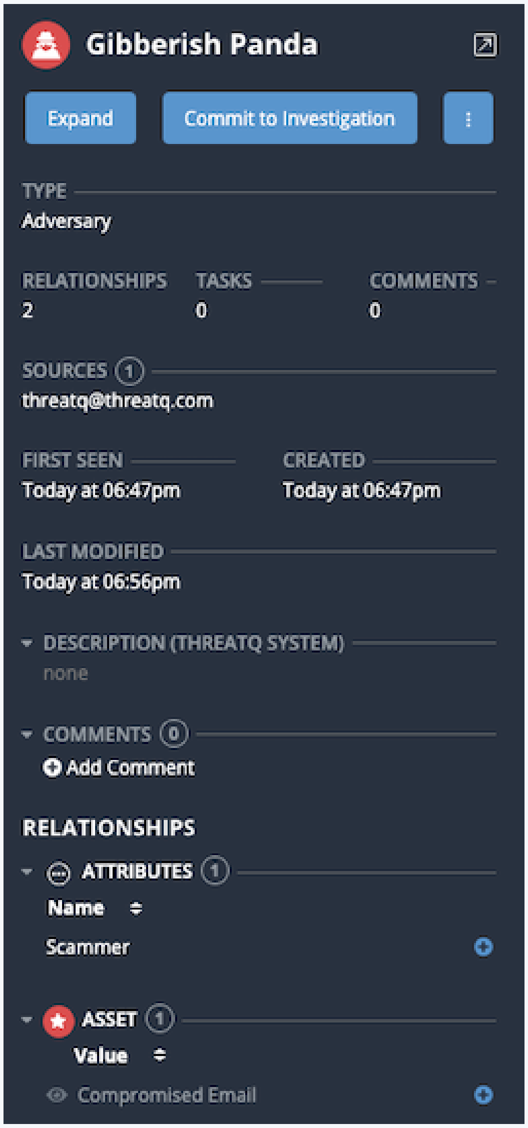
The investigation's details are displayed in the Action Panel when an investigation is initially loaded. You can view the following:



SCREENSHOT	FIELD	DESCRIPTION
	Investigation Details	You can view the investigation's details at the top of the Action Panel. This includes the Priority, Visibility settings, investigation Status, number of objects associated with the investigation
	Created	The date and time the investigation was created.
	Last Modified	The date and time of when the investigation was last modified.
	Description	The description of the investigation.
	Comments	Displays any comments that have been added to the investigation.
	Added to the Investigation	Displays all objects that have been added to the investigation.
	Exploratory Data Points	Threat objects and related objects that have not been committed to the investigation.
	Show Exploratory Data Points	Allows you to toggle the visibility of related object nodes. Objects that have not been committed to an investigation will appear under this heading.

Viewing an Object's Details

Clicking on an object's node on the evidence board will load the object's details in the action panel.

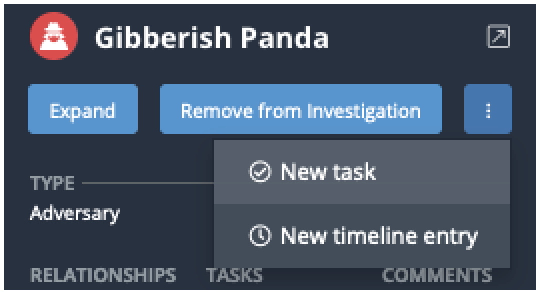


SCREENSHOT	FIELD	DESCRIPTION
		Opens the highlighted object's details page in a new tab.
	Expand	Displays all attributes and objects associated with the object on the evidence board.
	Remove from Investigation	Removes the selected object from the investigation.
	Type	Displays the type of object, the number of related objects, the number of tasks assigned to the object and the number of comments.
	Sources	The sources for the object.
	First Seen	The time and date of when object first appeared in the investigation.
	Created	The date and time when the object was first created in the ThreatQ platform.
	Last Modified	The date and time of when the object was last modified on the ThreatQ platform.
	Description (ThreatQ System)	The ThreatQ System description of the object if available. If not, this field lists a value of none. The ThreatQ System description is pulled from the Descriptions Pane in the object's details page. This field displays the object's description as a string value. It does not include any formatting such as tables.
	Comments	Displays any comments associated with the object. This information is pulled from the object's details.
	Added to the Investigation	Displays all objects that have been added to the investigation.
	Relationships	Displays all attributes and objects related to the selected object.

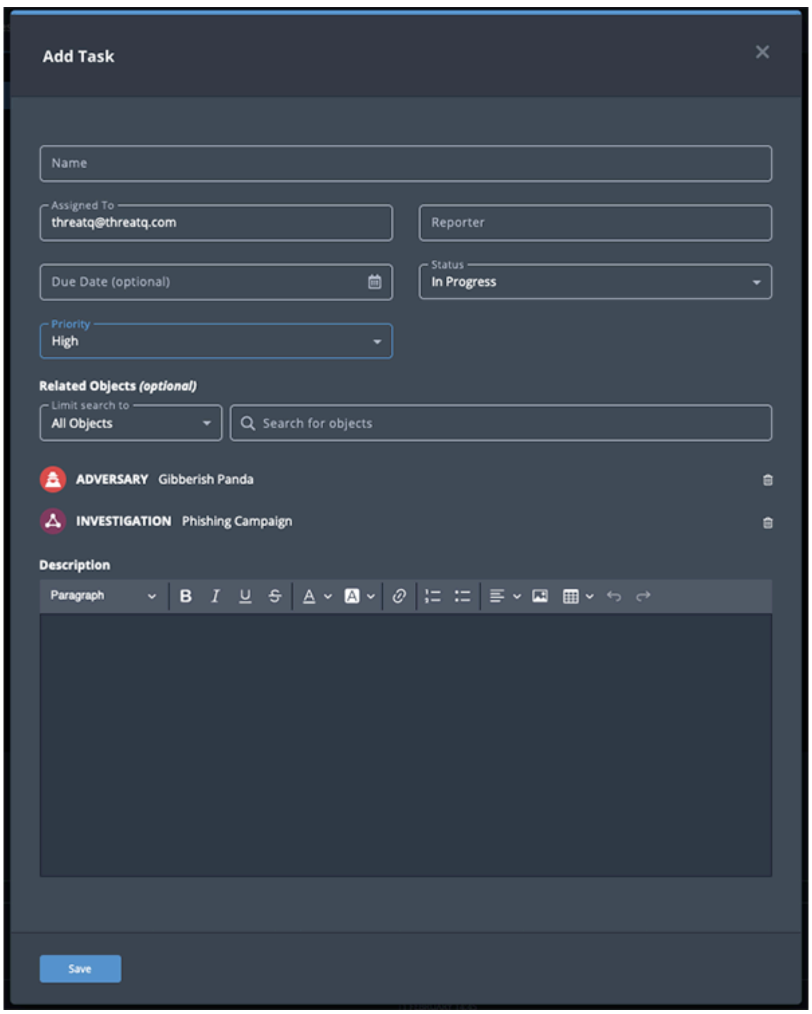
Creating a New Task for an Object

You can assign a new task for a highlighted object from the action panel.

1. Click in the vertical ellipsis and select **New Task**.



The Add Task dialog box will open.



2. Complete the following fields:

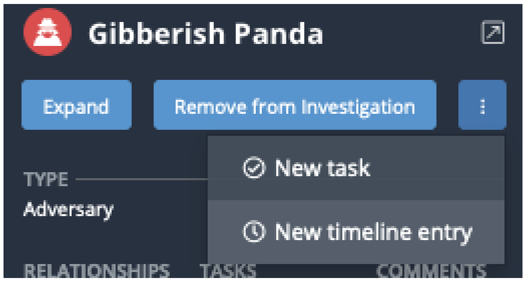
FIELD	DESCRIPTION
Name	The name of the task.
Assigned To	The ThreatQ user assigned the task.
Reported	The ThreatQ user that created task.
Due Date	The optional due date to complete the task.
Status	The status of the task. Options include: ○ To Do ○ In Progress ○ Review ○ Done
Priority	The priority of the task. Options include: ○ Low ○ Medium ○ High
Related Objects	The object, related objects, and investigations associated with the task.
Description	The description of the task.

3. Click **Save** to create the task.
4. Right-click on the new task's node and select **Commit to Investigation**.

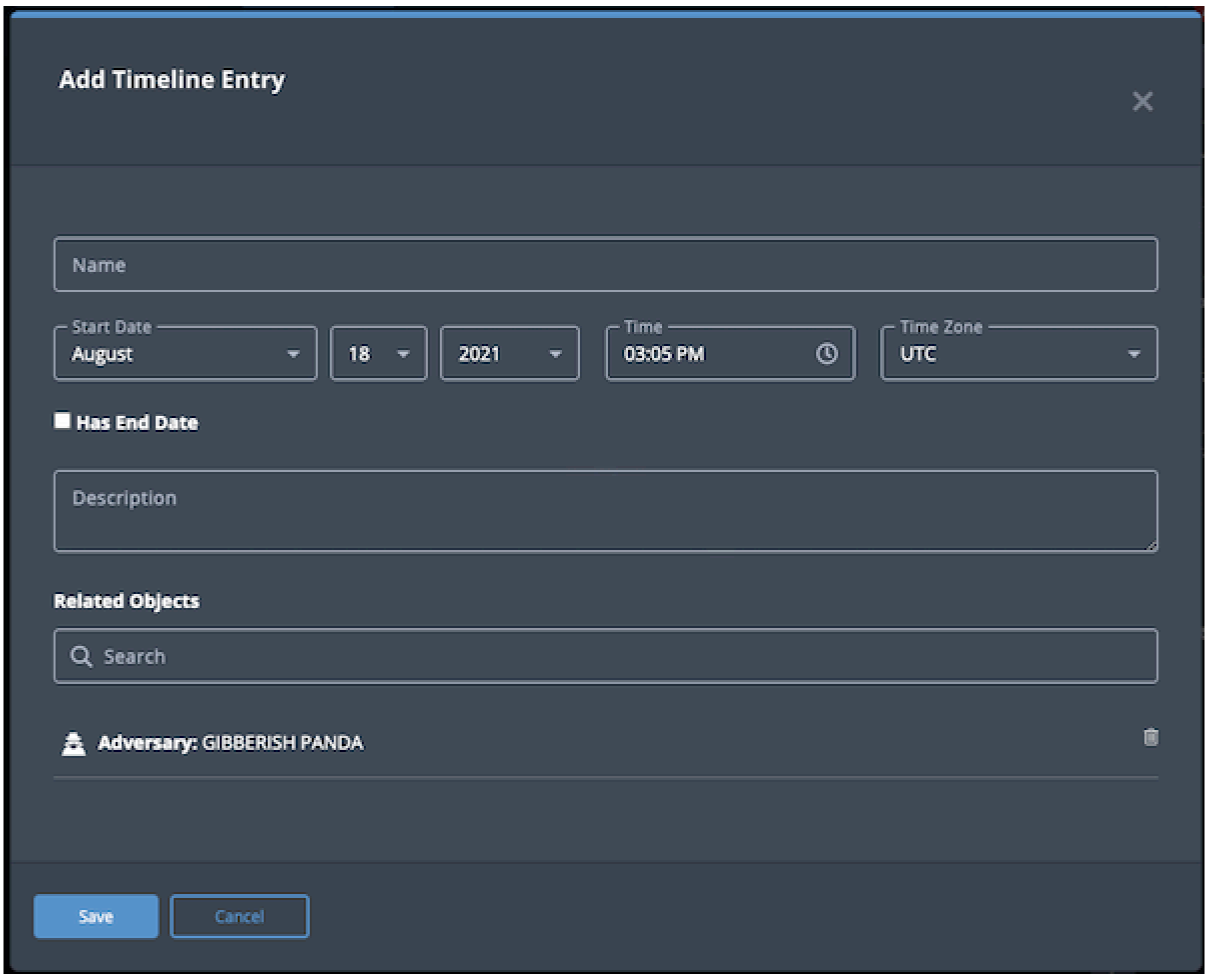
Creating a New Timeline Entry for an Object

You can assign a new timeline entry for a highlighted object from the action panel.

1. Click in the vertical ellipsis and select **New Timeline Entry**.



The Add Timeline Entry dialog box will open.



2. Complete the following fields:

FIELD	DESCRIPTION
Name	The name of the timeline entry.
Start Date	Select the month, day, year, time and time zone for the timeline entry.
Has an End Date	Optional - enable if the entry has an end date.
End Date	Select the month, day, year, time and time zone for the timeline entry. These fields will only appear if you have selected the **Has an End Date** field.
Description	The description of the timeline entry.
Related Objects	The object, related objects, and investigations associated with the entry.

3. Click **Save** to create the new timeline entry.

Previewing an Object

You can open a preview tab for investigation objects and related objects from the Action Panel. From the preview tab, you can perform the the same actions that are available from the object's details page including:

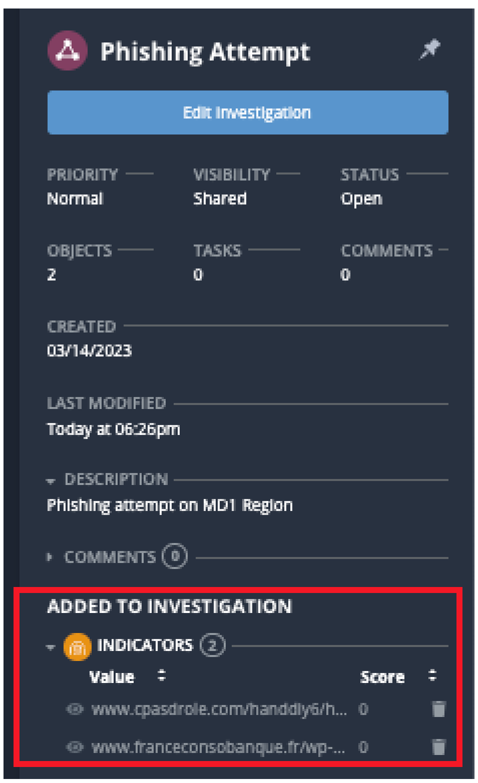
- Update Expiration (Indicators Only)
- Update Score (Indicators Only)
- Update object Status (Indicator Only)
- Add Attributes, Sources, Tags etc.

Additionally, you can run operations against the previewed object.

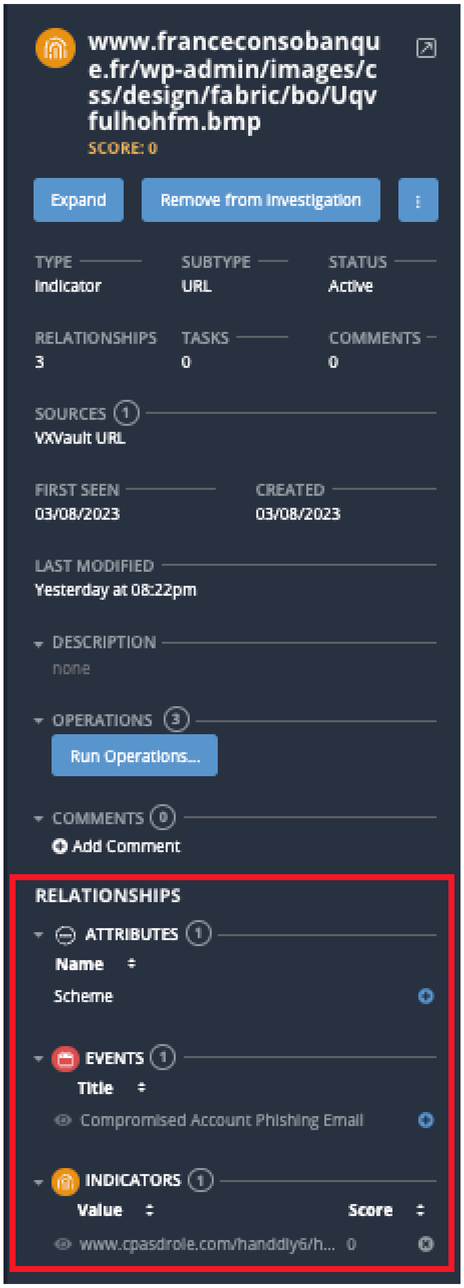
Opening an Object in the Preview Tab

The steps for previewing an investigation or related object differ only in terms of which object you select on the Evidence Board.

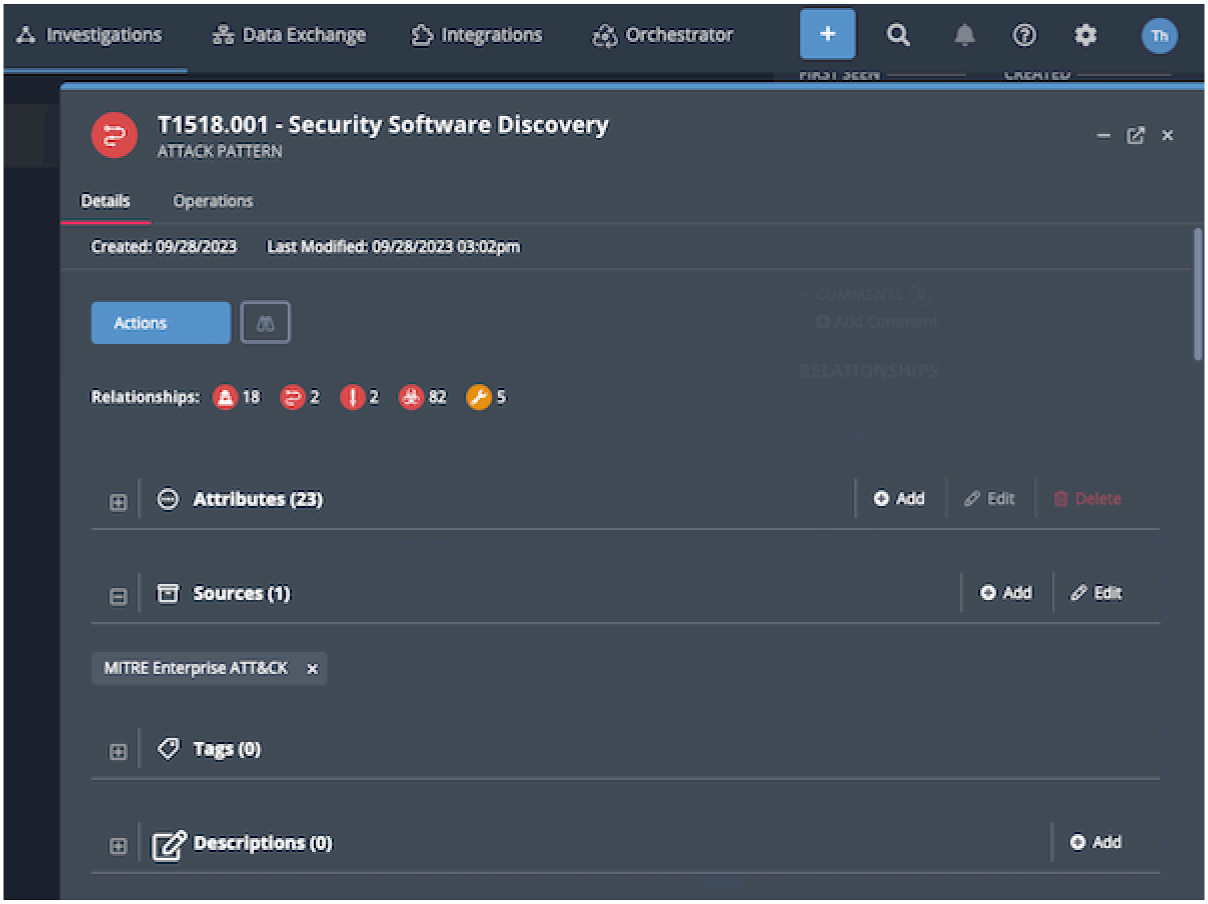
- If the investigation itself is loaded in the Action Panel, you will see an Added to Investigations section at the bottom of the panel.



- If an object node is selected, you will see a Relationships section listed at the bottom.



1. To view the preview panel, click the Preview icon  located to the left of the object name.



2. Review and/or update the object's details as needed. You can also run an operation to pull further context for the object using the Operations tab located at the top of the window.

Running an Operation from the Action Panel

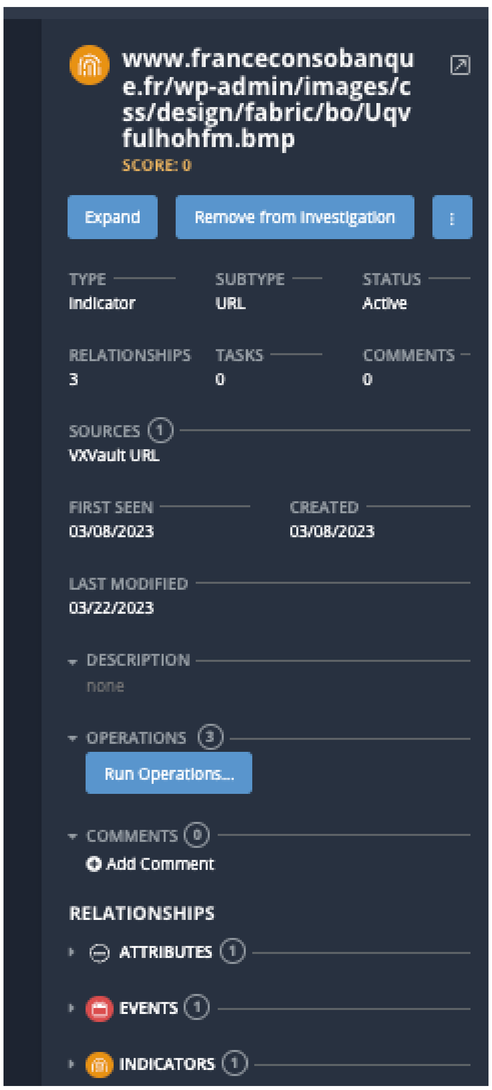
You can run an action against an object in your investigation from the Action Panel. You can also run operations against related objects from the Preview window.

> You must have an enabled operation that is compatible with the object type in order for the Operations heading to load in the Action Panel for the object.

Running an Operation against an Object

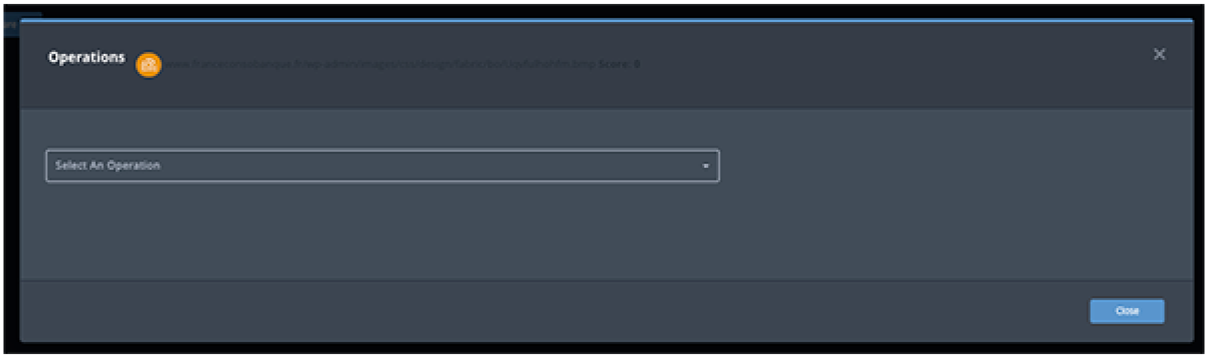
1. Click on the object's node on the Evidence Board.

   The object's details will load in the Action Panel

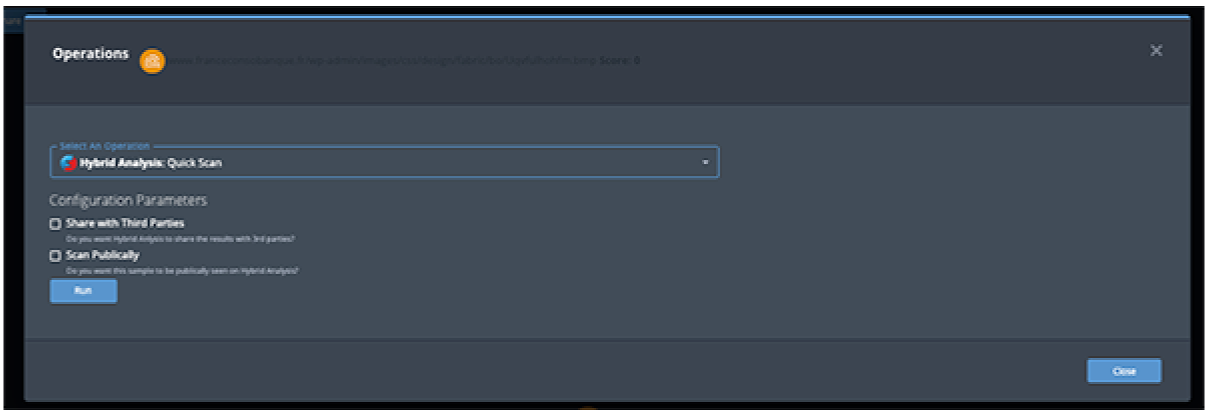


2. Click on the **Run Operations...** option under the Operations heading.

The Operation window will open.



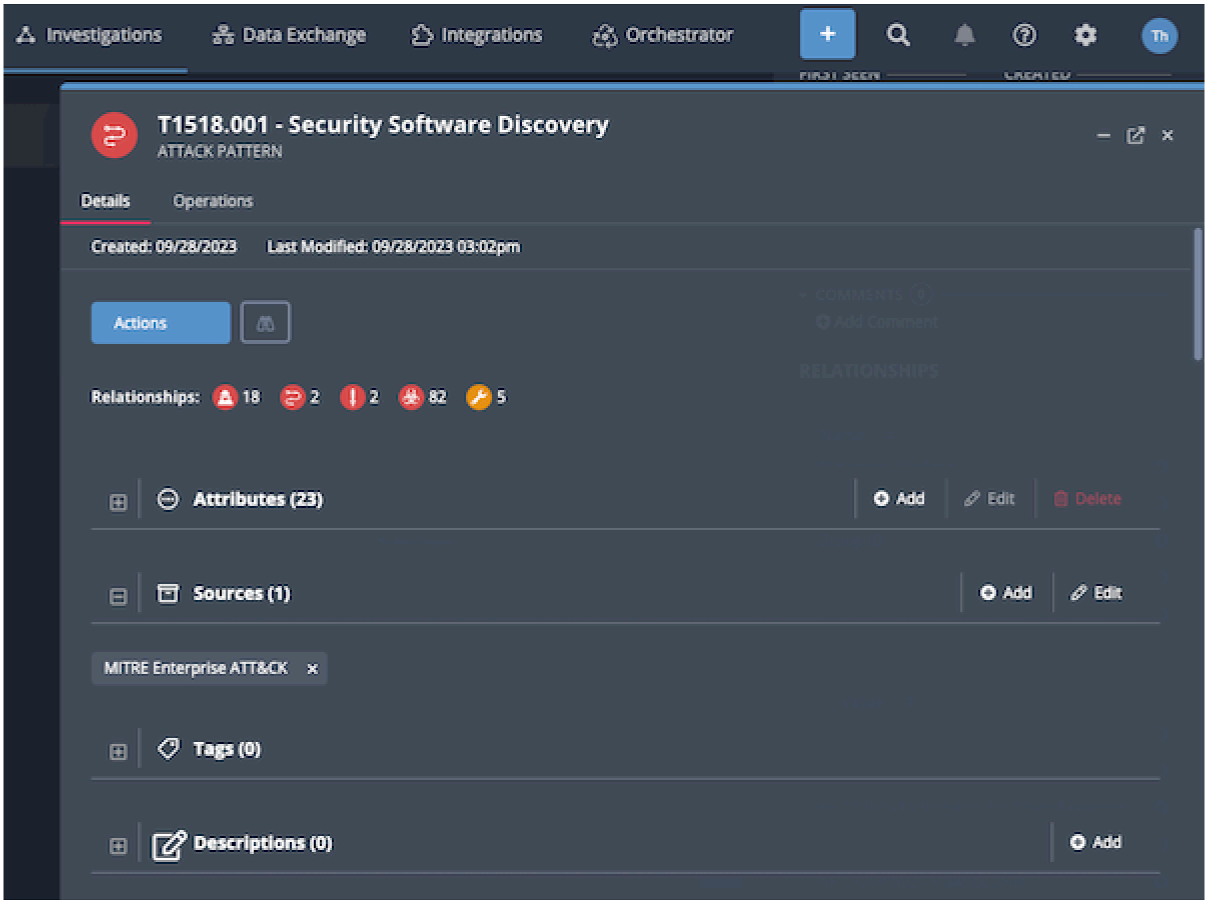
3. Select the operation to run using the dropdown provided.
4. Set your configuration parameters, if offered by the operation, and click on **Run**.



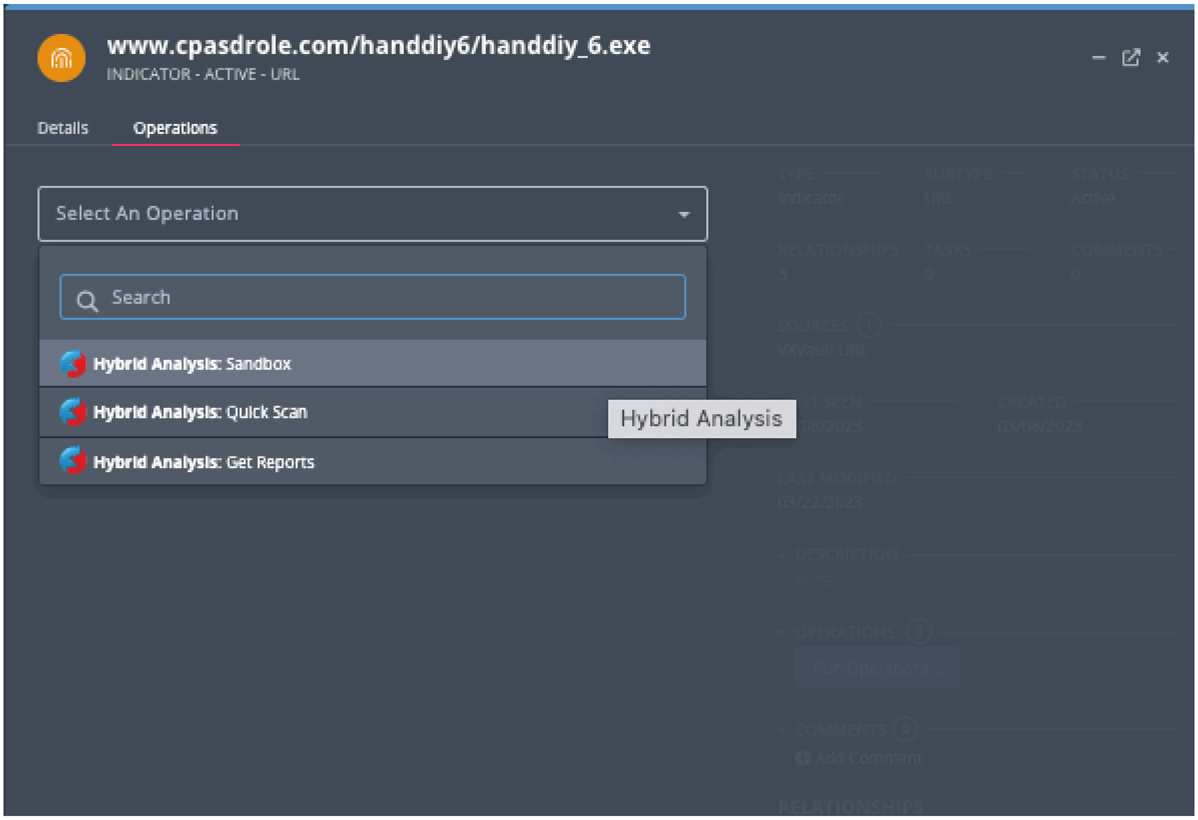
Running an Operation against a Related Object

1. Click on the object's node on the Evidence Board to load its details in the Action Panel.
2. Locate the object under the Relationships heading and click on the Preview icon.

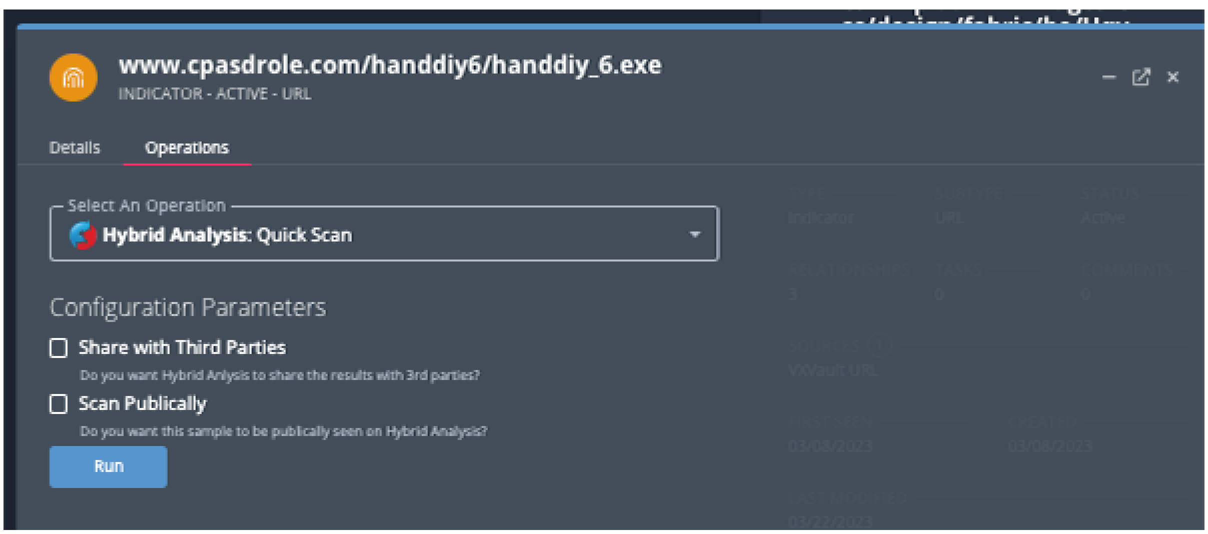
   The Preview window will open.



3. Click on the **Operations** tab located at the top of the window.
4. Use the dropdown menu provided to select the operation to run.



5. Set your configuration parameters, if offered by the operation, and click on **Run**.



Showing/Hiding Object Relationships

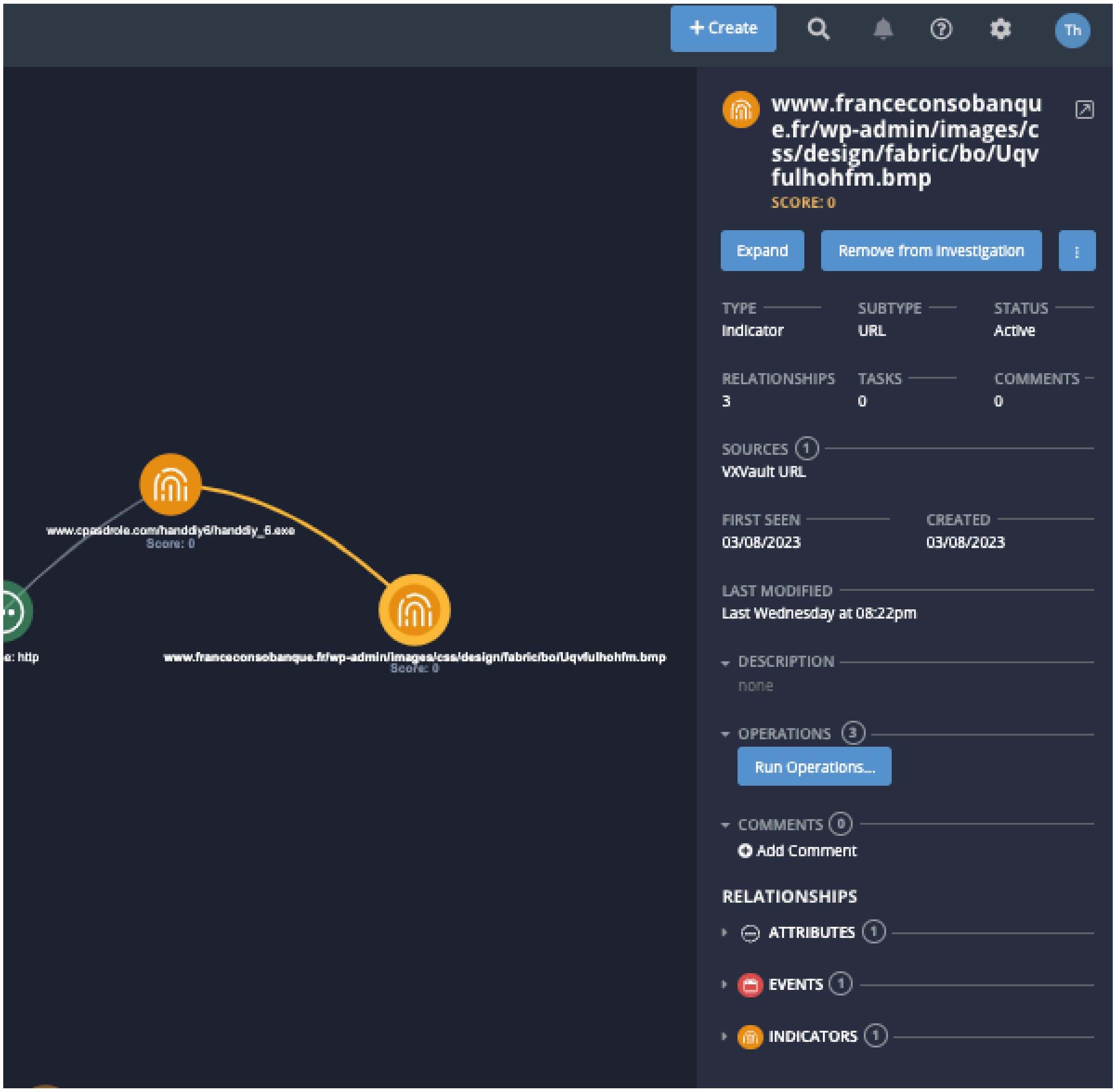
You can expand and hide an object's relationships, both committed and uncommitted, on the Evidence from the Action Panel. This allows you to create a better visual representation of your investigation as well as hide related objects that add little value to the investigation.

> Uncommitted related object nodes will only appear on the Evidence Board if you have enabled Exploratory Data Points.

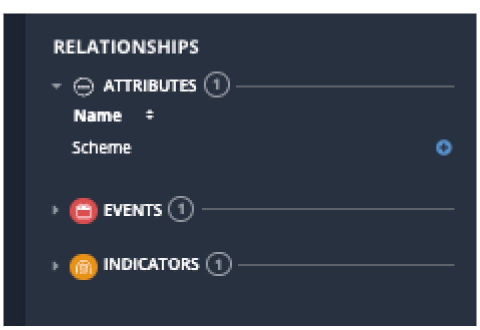
Show a Specific Object Relationship for an Object

1. Click on the object's node on the Evidence Board to load its details in the Action Panel.

   The Relationships section will be loaded at the bottom of the panel and will be categorized by object type.



2. Expand the Relationships categories and locate the object to display on the Evidence Board.



3. Click on the plus icon located to the right of the related object name.

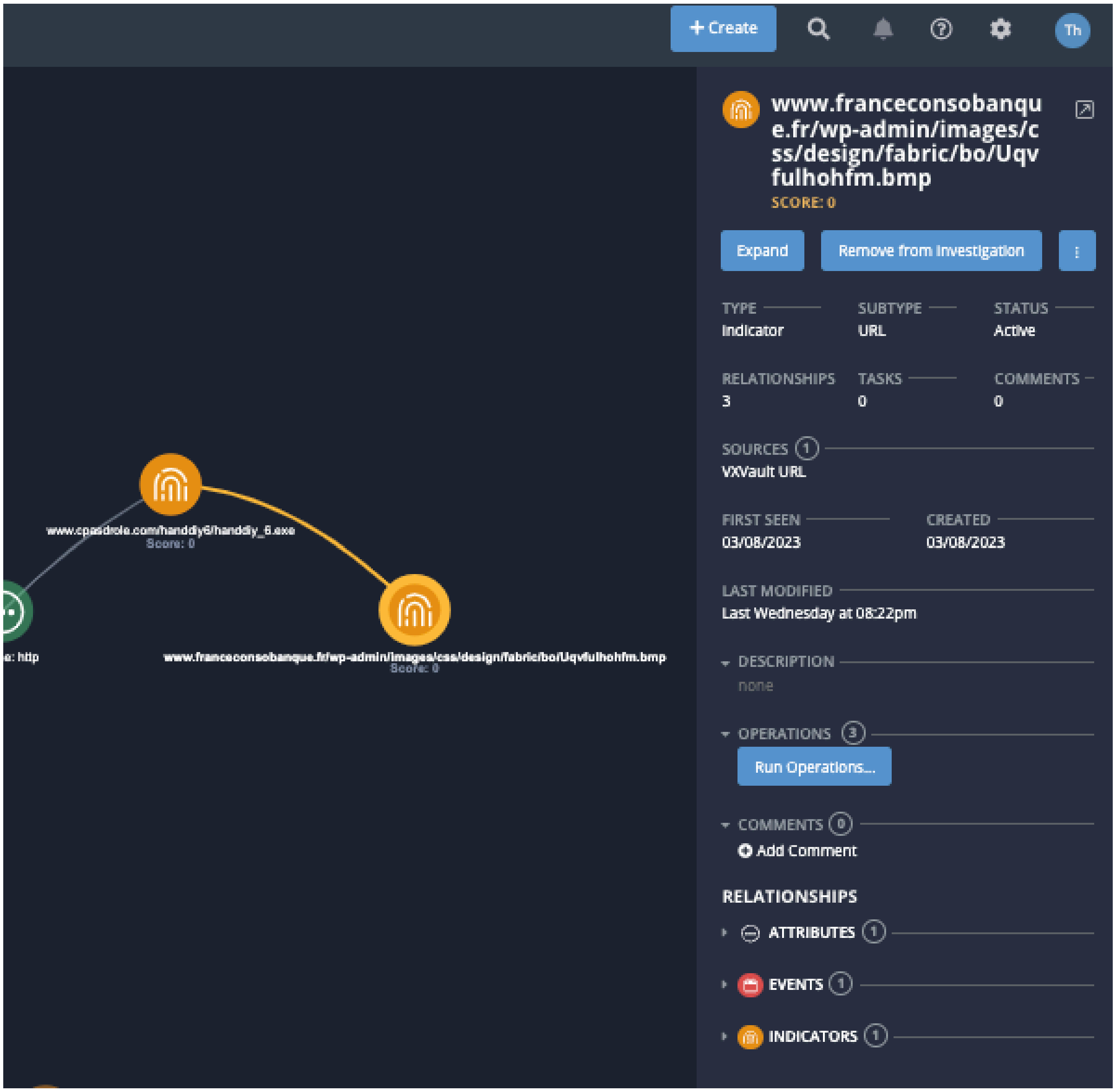
   The object's node will appear on the Evidence Board with visible data line connecting it to the original object.

4. Right-click on the related object and select **Commit to Investigation** to add the object to the investigation.

Show all Object Relationships for an Object

1. Click on the object's node on the Evidence Board to load its details in the Action Panel.

   The Relationships section will be loaded at the bottom of the panel and will be categorized by object type.



2. Click on the **Expand** button located towards the top of the panel.

   All related object nodes will appear on the Evidence Board with visible data lines connecting them to the original object.

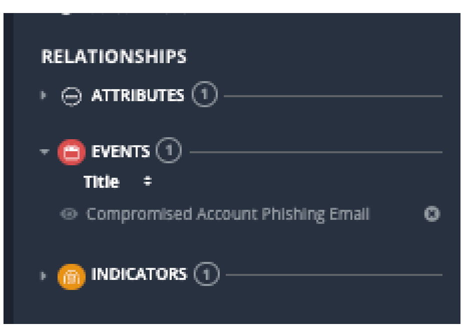
3. Right-click on any related object and select **Commit to Investigation** to add the object to the investigation.

Hide an Object Relationship

Hiding an Object Relationship remove the object's node from the Evidence Board and does not remove it from the parent object or the investigation.

1. Click on the object that the related object is attached to on the Evidence Board.

2. Locate the object under the Relationships section of the Action Panel.



3. Click on the **X** icon next to the object name to remove it's node from the Evidence Board.

   The related object's node will be removed from the Evidence Board.


www.franceconsobanque.fr/wp-admin/images/css/design/fabric/bo/Uqvfulhohfm.bmp
Score: 0
Scheme: https

Evidence Board

About the Evidence Board

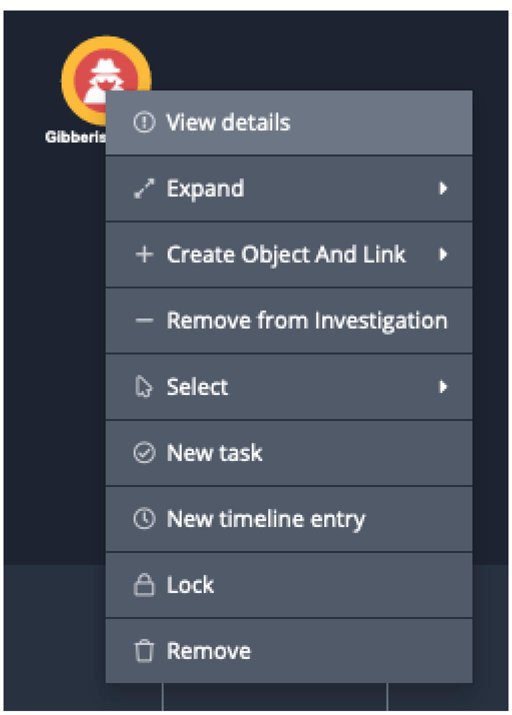
The evidence board is where most of the interaction takes place in an investigation. The evidence board allows you to add ThreatQ objects, such as Indicators and Adversaries to the investigation, represented as graphical nodes. The evidence board interacts with the other two components of an investigation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

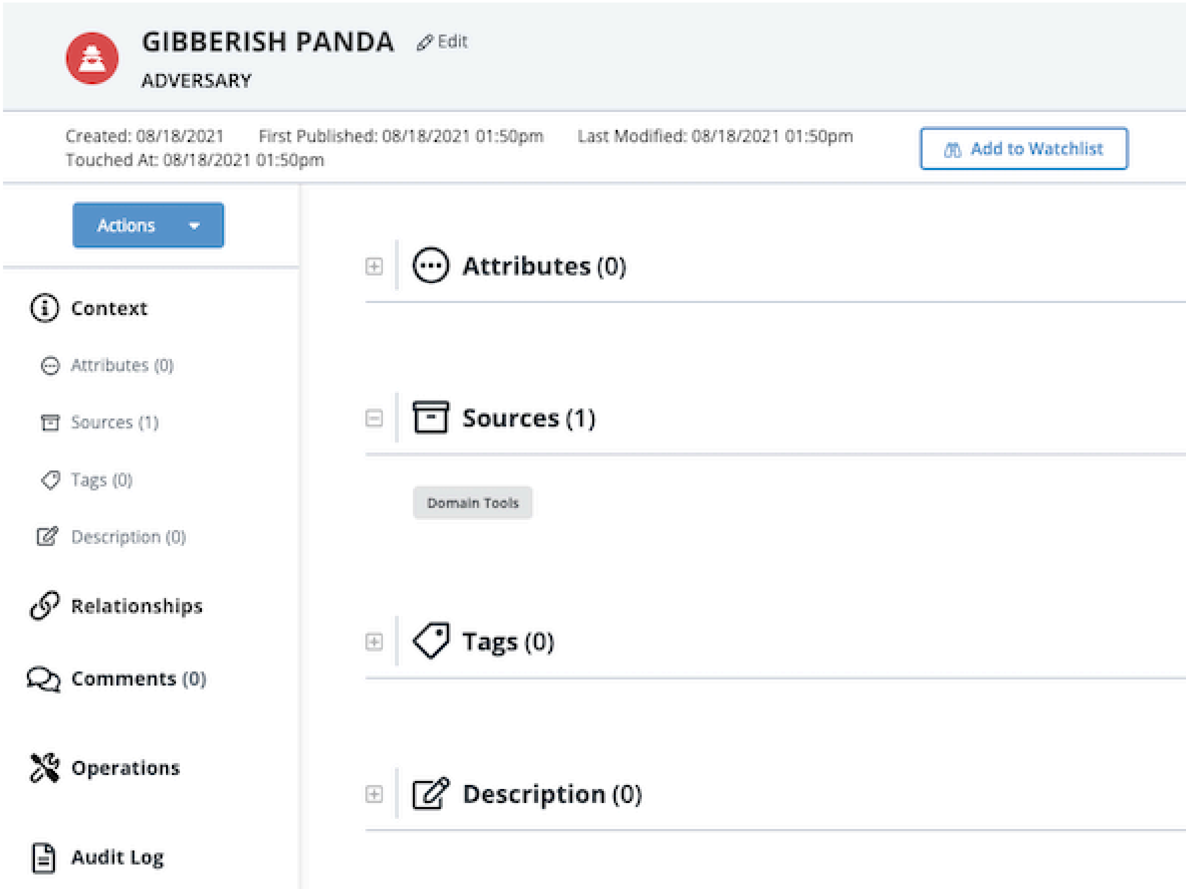
Accessing an Object's Details Page on the Evidence Board

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


GIBBERISH PANDA
Edit
ADVERSARY
Created: 08/18/2021
First Published: 08/18/2021 01:50pm
Last Modified: 08/18/2021 01:50pm
Touched At: 08/18/2021 01:50pm
Add to Watchlist
Actions
Context
Attributes (0)
Sources (1)
Tags (0)
Description (0)
Relationships
Comments (0)
Operations
Audit Log
Attributes (0)
Sources (1)
Domain Tools
Tags (0)
Description (0)

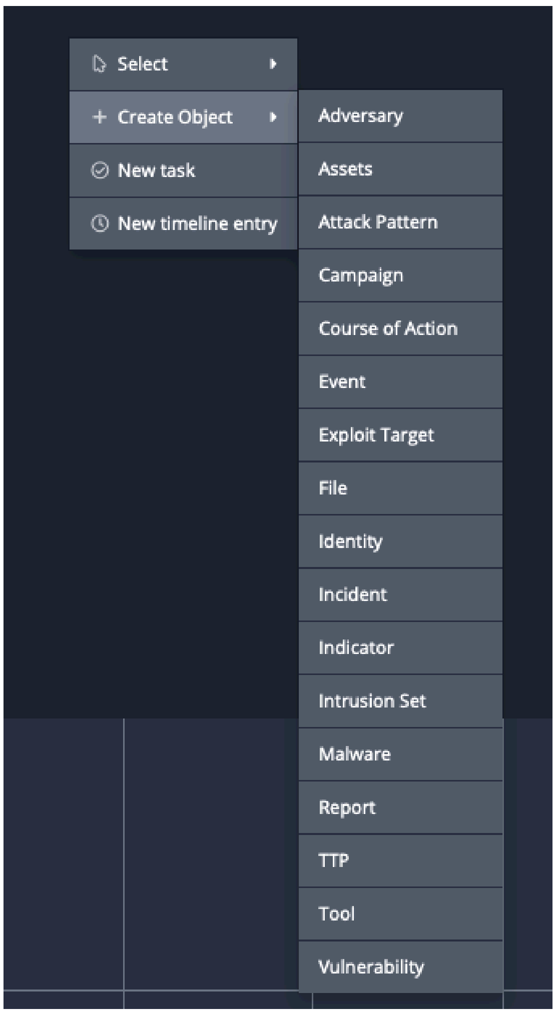
Adding/Removing an Object

You can create a new threat object or add an existing threat object to the Evidence Board. You can also remove an object from the investigation.

Creating a New Threat Object

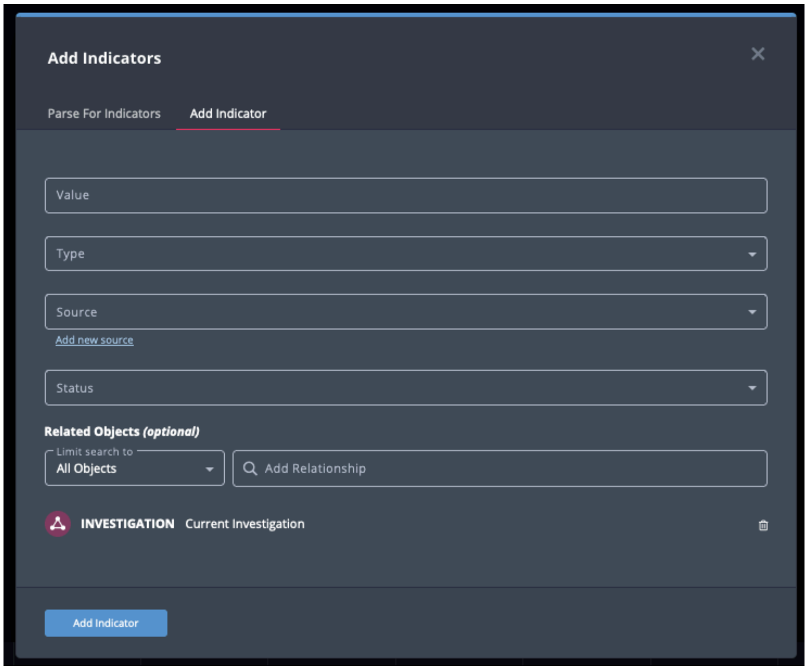
When you create a new object from the evidence board, it is automatically added to your current investigation.

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 <object>** button to save your entry.

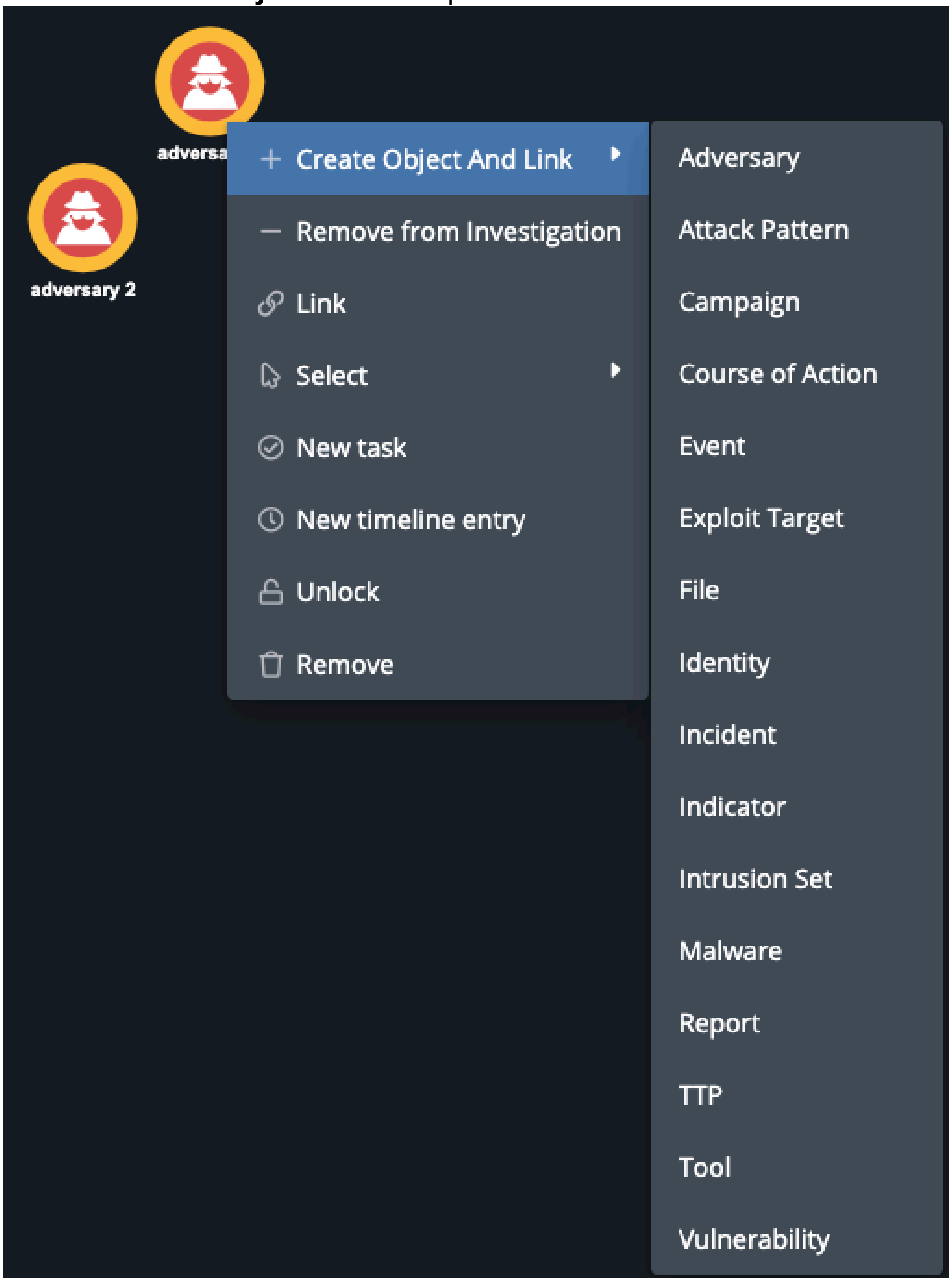
   The new object is added to your current investigation and is viewable by other users that the investigation has been shared with.

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 on one of the nodes.

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.

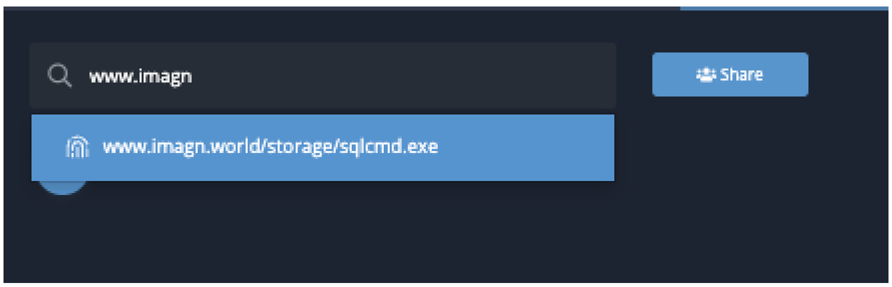
4. Click the **Add *<object type>*** button to save the new object and add it to the evidence board. The object will be linked to all the objects listed in the Related Objects section.

Adding an Existing Threat Object to an Investigation

The steps in this section relate to adding an object to an investigation with TQI. You can also add an object to an investigation from the object's details page. See the Object Details topic for more details.

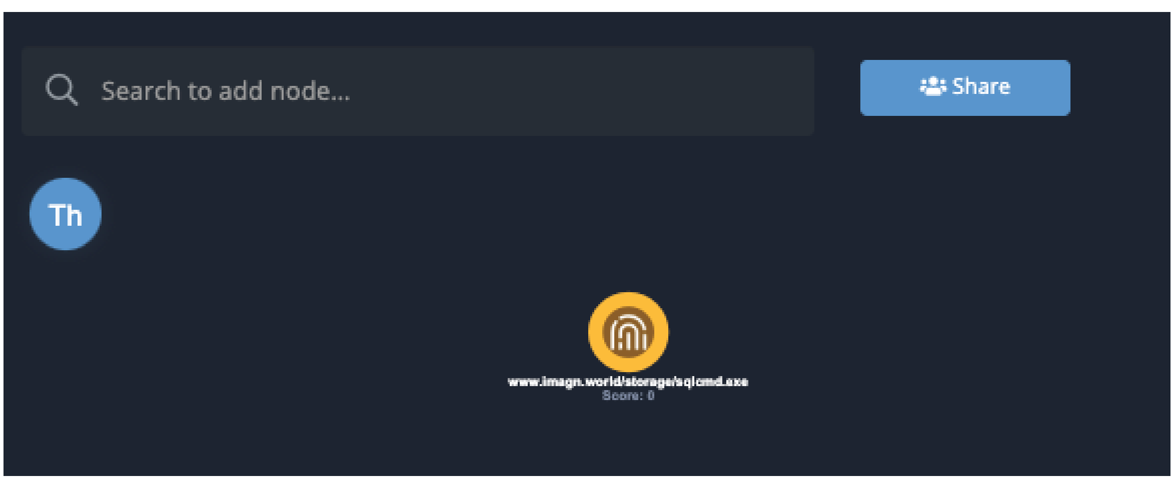
When you add an object to the evidence board, it becomes available for further examination. However, it **does not** immediately become a part of the current investigation. You must explicitly **commit** the object to the investigation. Until you do so, only you can view the object in the investigation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

1. Use the Evidence Board search menu to locate the object to add to the investigation.

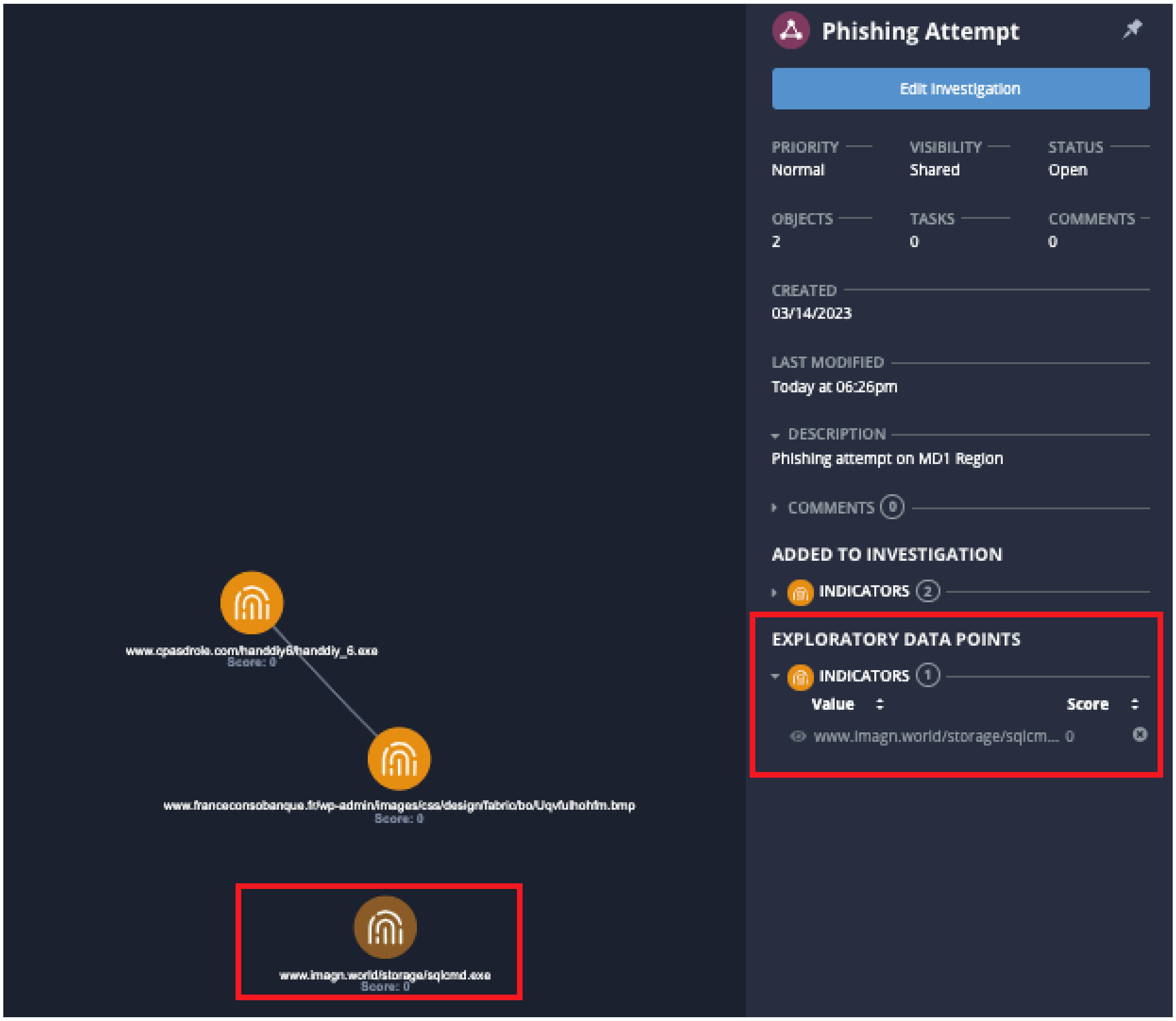


You can also add an object to an investigation from its details page by clicking on the **Actions** dropdown and selecting **Add to Investigation**.

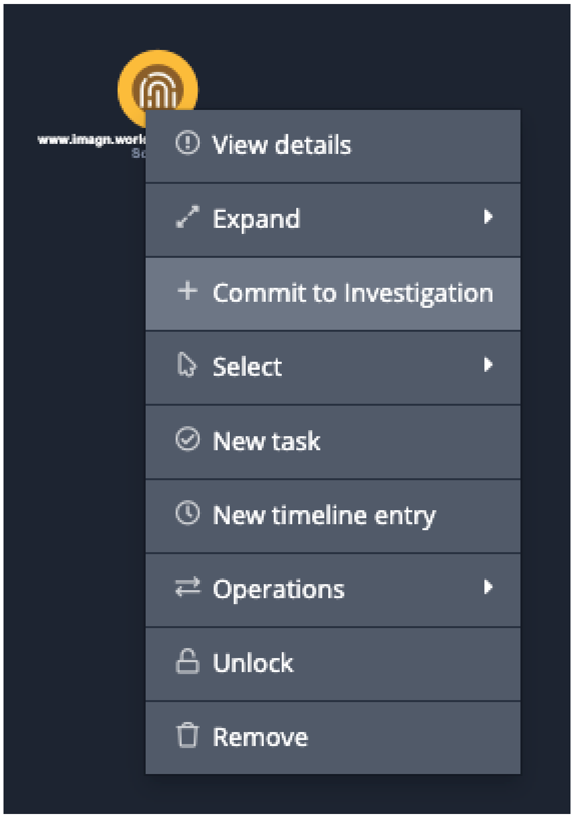
2. On the evidence board, select and highlight the node that represents the object you want to manage.



At this point, the object node slightly darker than the other nodes and will appear as a Exploratory Data Point in the Action Panel. Other users will not be able to see this object in the invested until you have committed it.



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



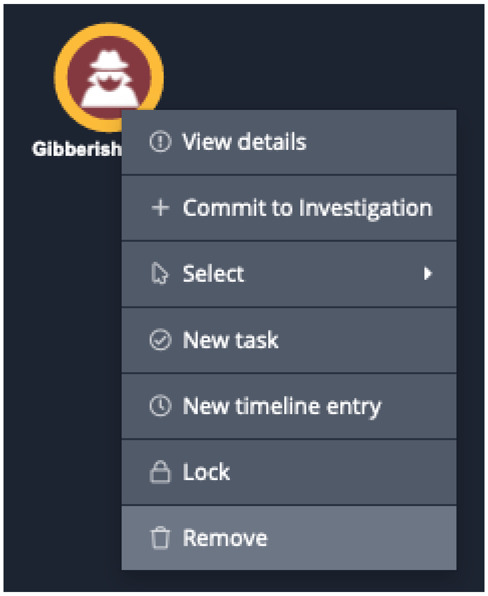
The object will now be committed to the investigation and can be viewed by other users that the investigation has been shared with.

Removing an Object from the Investigation

Removing 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**.



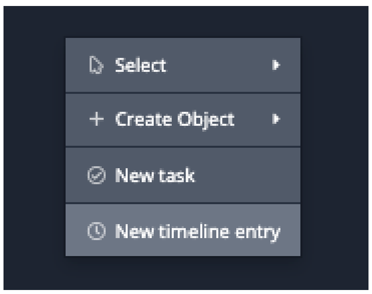
Adding a New Timeline Entry

You can add independent timeline entries and timelines associated with an object in an investigation.

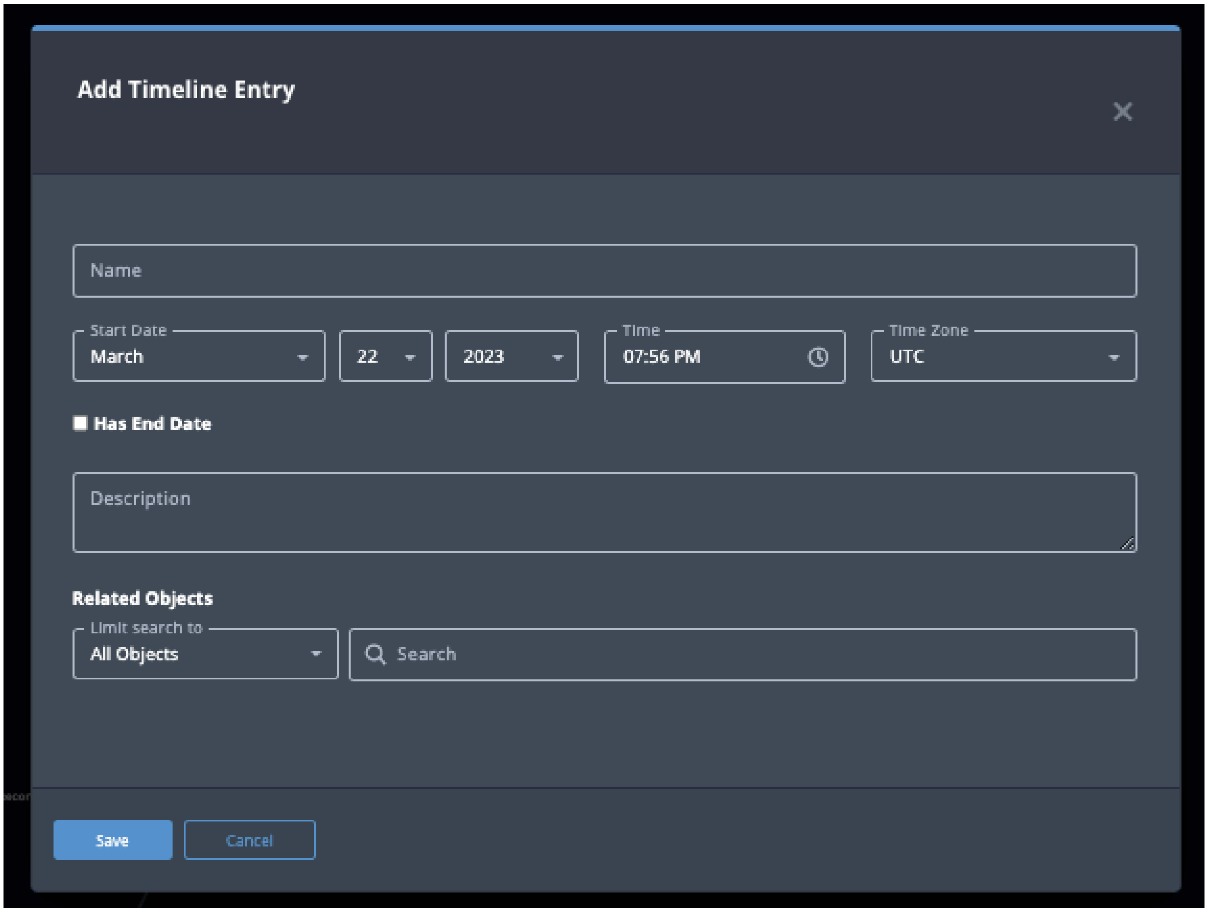
Adding a New Timeline Entry to the Investigation

You can add new timeline entries to an investigation independent of an object.

1. Right-click on an empty space on the evidence board and select the **New Timeline Entry** option.

   The Add Timeline Entry form loads.



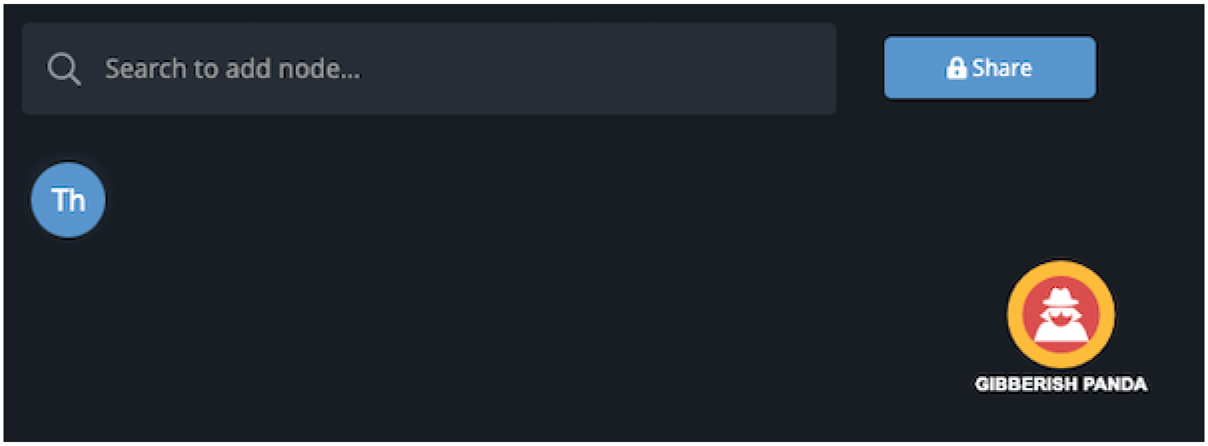
2. Complete the timeline form fields and click on **Save**.

   The new timeline entry will appear in the timeline.

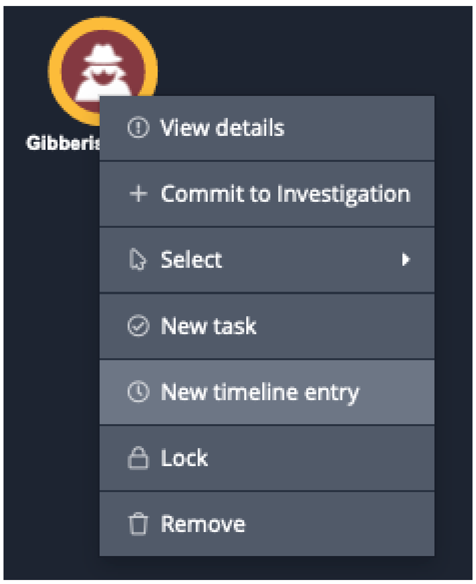
Adding a New Timeline Entry to an Investigation Object

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.

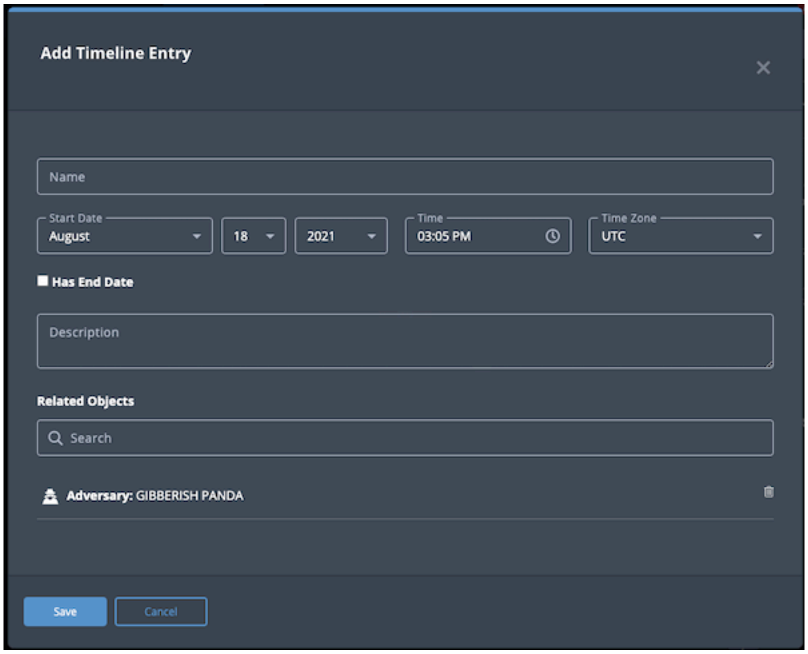
1. On the evidence board, select and highlight the node that represents the object for which you want to enter a timeline entry.



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



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



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.

Creating a New Task

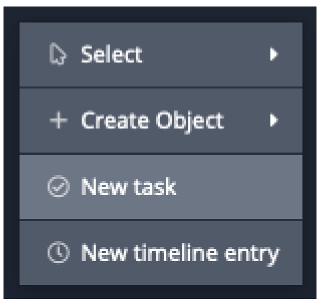
You can create and assign new tasks to an investigation or to an object that is part of an investigation.

Creating a New Task for an Investigation

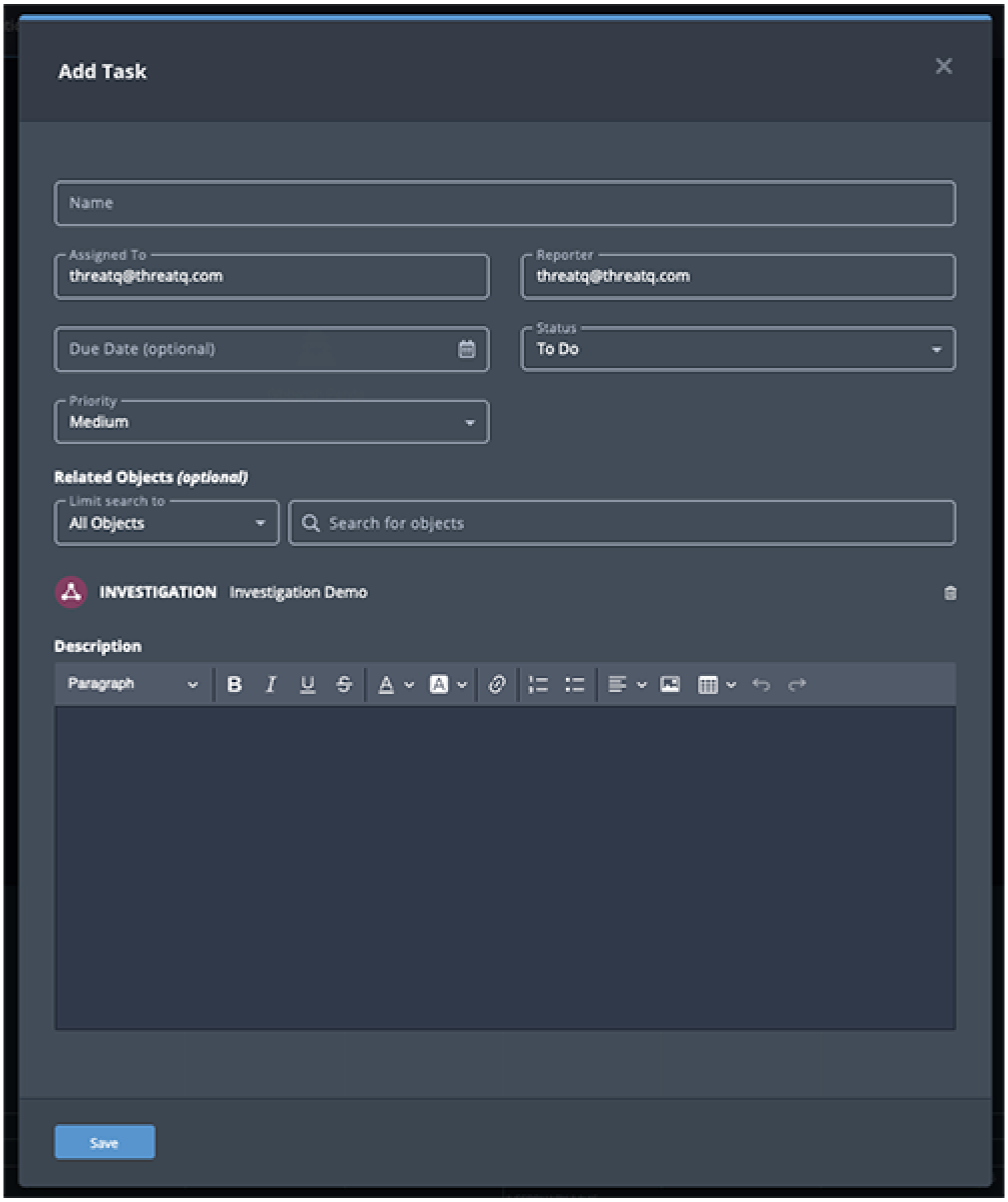
ThreatQ allows you to create and assign tasks to yourself or other users in the platform. You can also use tasks in ThreatQ Investigations. When you assign a new task, you can add contextual information and correlate with Indicators , Events , Adversaries , Signatures , and Files .

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.

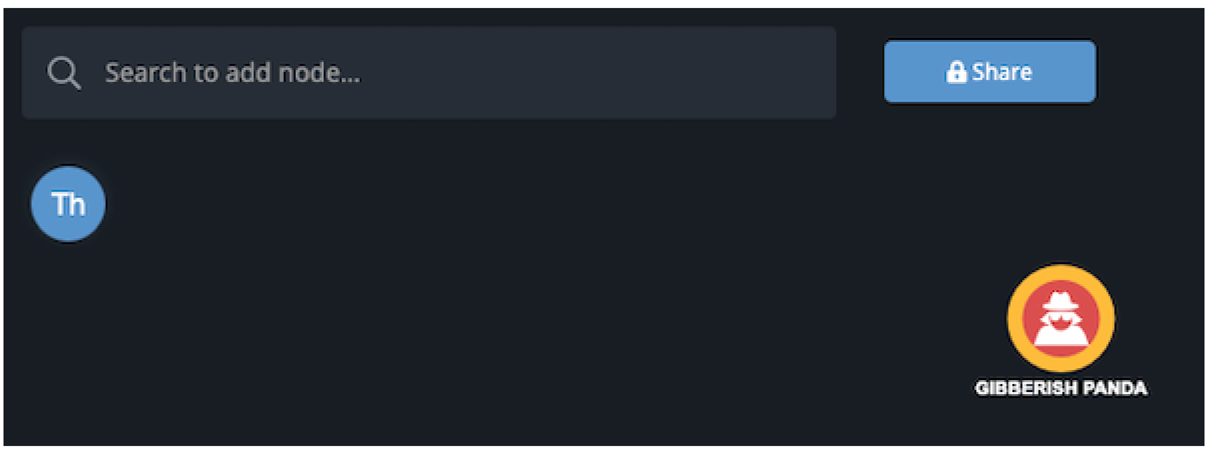
Creating a New Task Related to an Object

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.

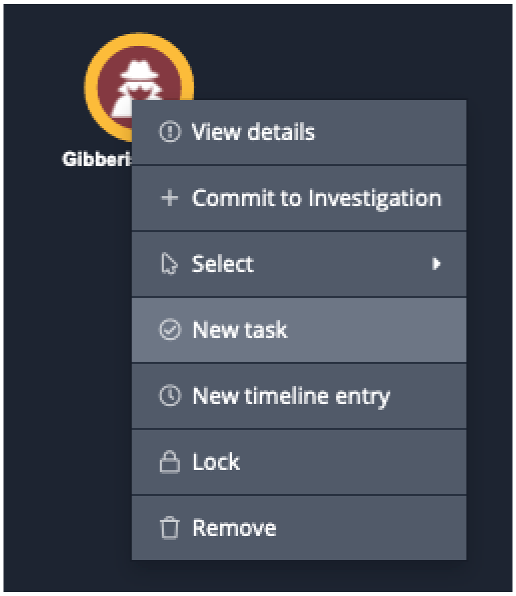
> If an investigation owner or editor create a task for user who does not have access to the investigation, the user can access the task via Threat Library. However, he cannot view the investigation unless an owner or editor shares the investigation with him. In the Threat Library detail page, the Owner 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 on the object 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.

Linking/Unlinking Objects

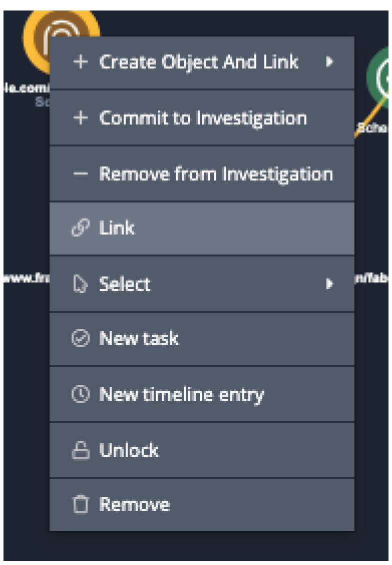
Linking two object nodes on the Evidence Board creates a visible connection on the evidence board and relates the objects to each other in the Action Panel.

Linking Two Objects

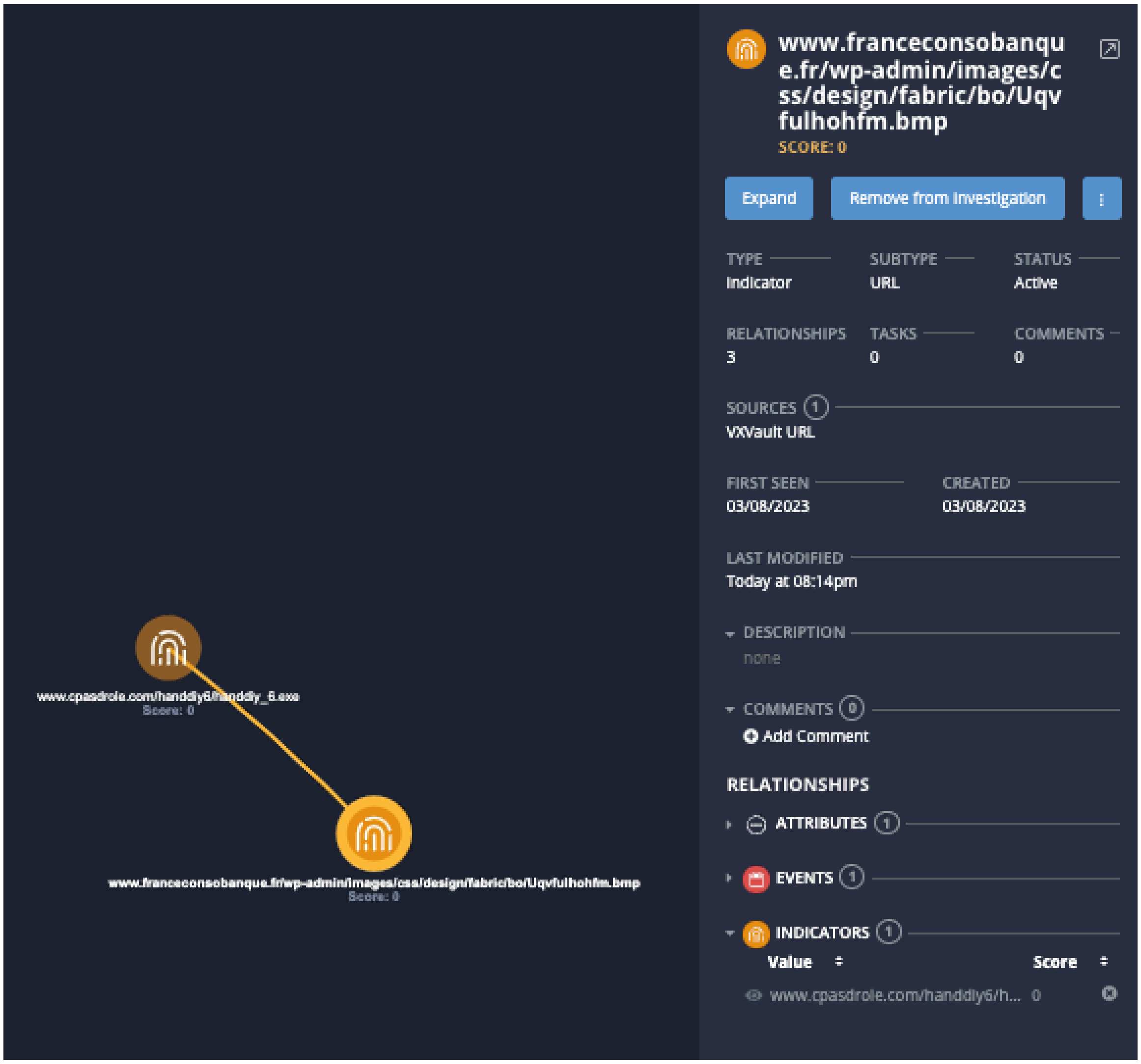
You can link two objects in an investigation. Linking an object will add it as a relationship to object in the Action Panel.

1. Select two object nodes on the evidence board.

2. Right-click on one of the highlighted objects and select **Link** from the dropdown menu.



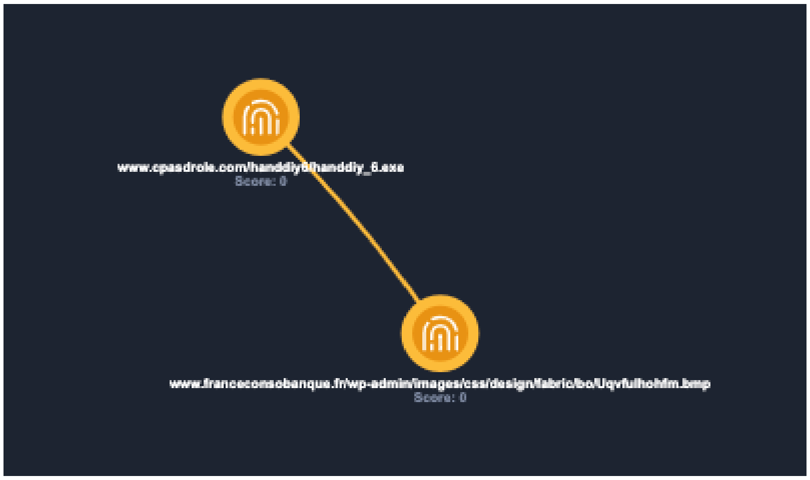
The objects will now be linked and physical graph line will appear connecting the objects. The linked object will also appear as relationships in the Action Panel.



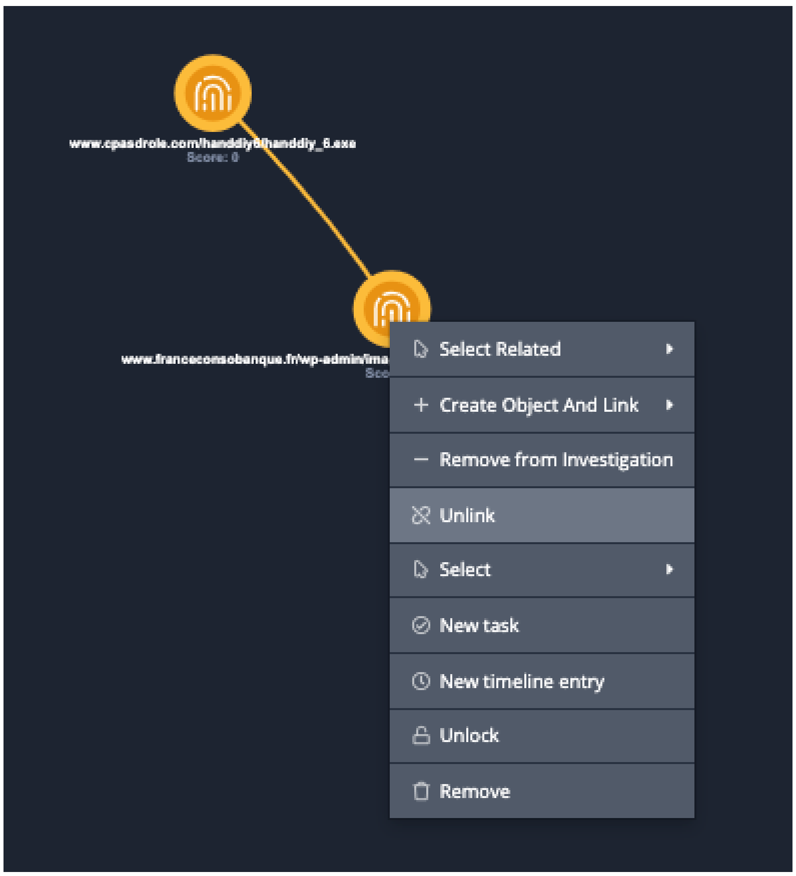
Unlinking an Object

You can unlink two linked objects. This will remove the objects from their relationships section of the Action Panel.

1. Select both linked object nodes on the Evidence Board.



2. Right-click on the node and select **Unlink** from the dropdown menu.



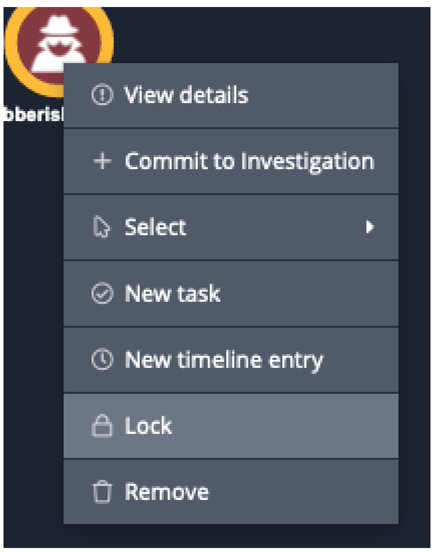
Locking/Unlocking an Object

You can lock and unlock an object to 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.

> The steps below can be used to lock and unlock an object on the evidence board.

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

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



3. Optionally, if you want to unlock the object, right-click on it and select **Unlock**.

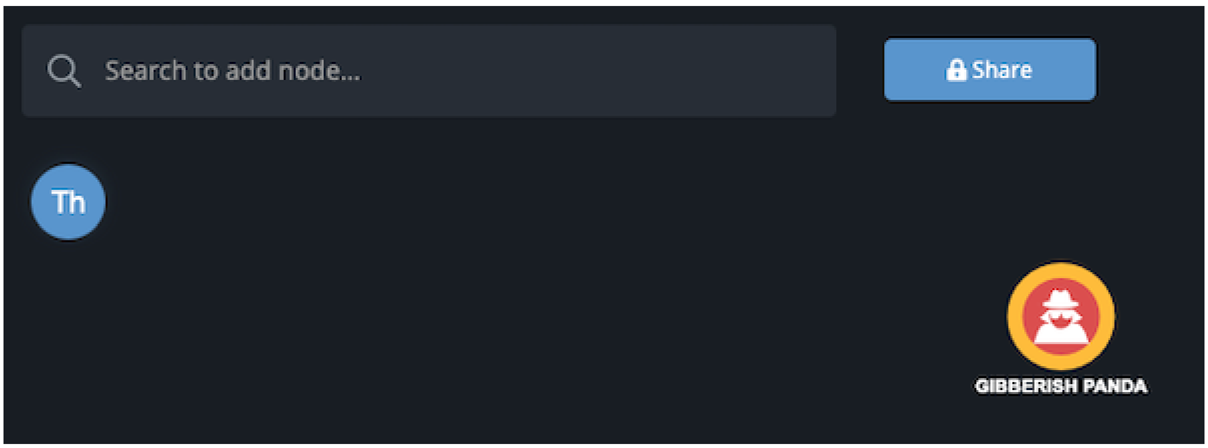
Object Relationships Visibility Options

You can expand and hide an object's relationships on the Evidence Board.

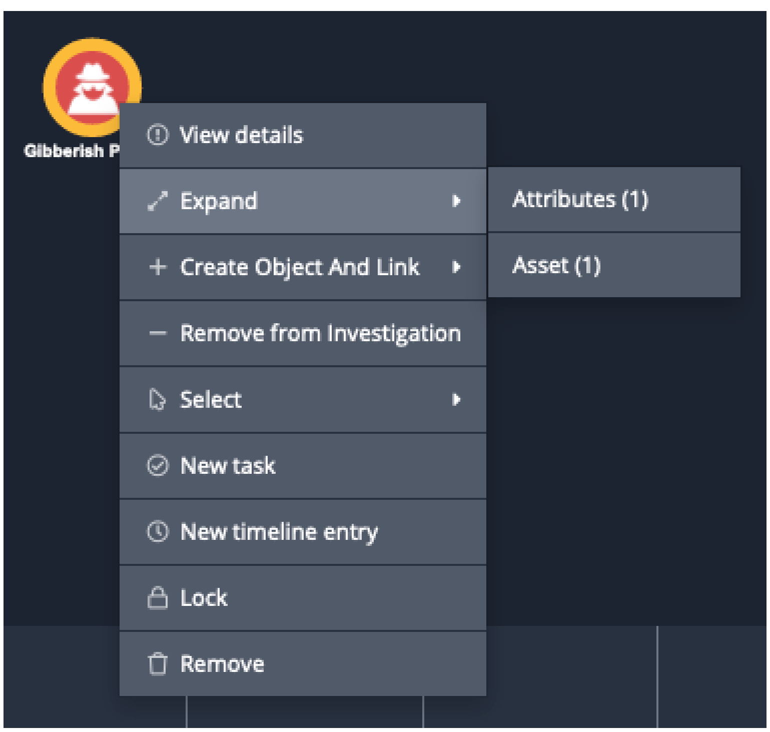
Viewing an Object's Relationships on the Evidence Board

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.

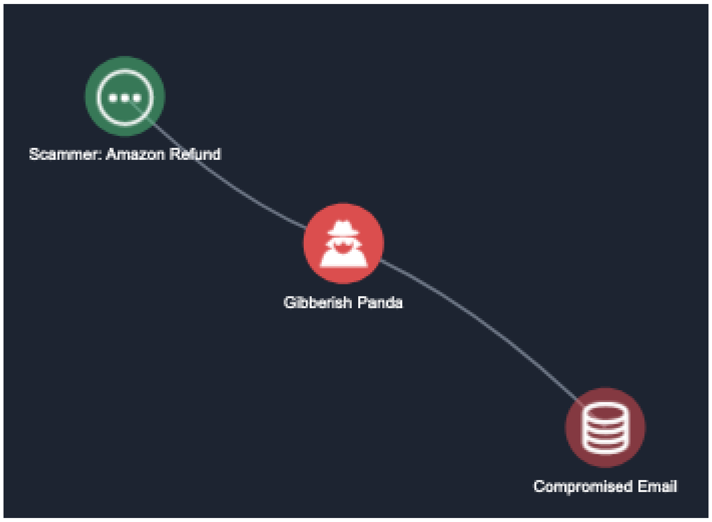
1. On the evidence board, select and highlight the node that represents the object you want to manage.



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



The node view expands to include related objects and attributes.



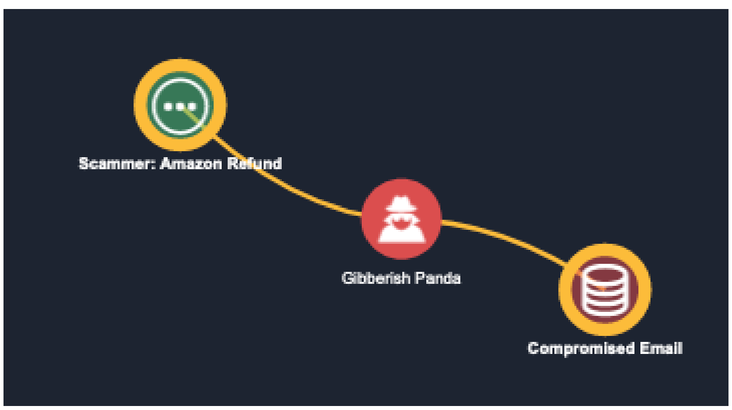
Hiding an Object's Relationships on the Evidence Board

You can hide an object's relationships on the evidence board. This does not delete the related objects and attributes from the object or investigation.

The following steps outline two methods to hide the related objects and attributes.

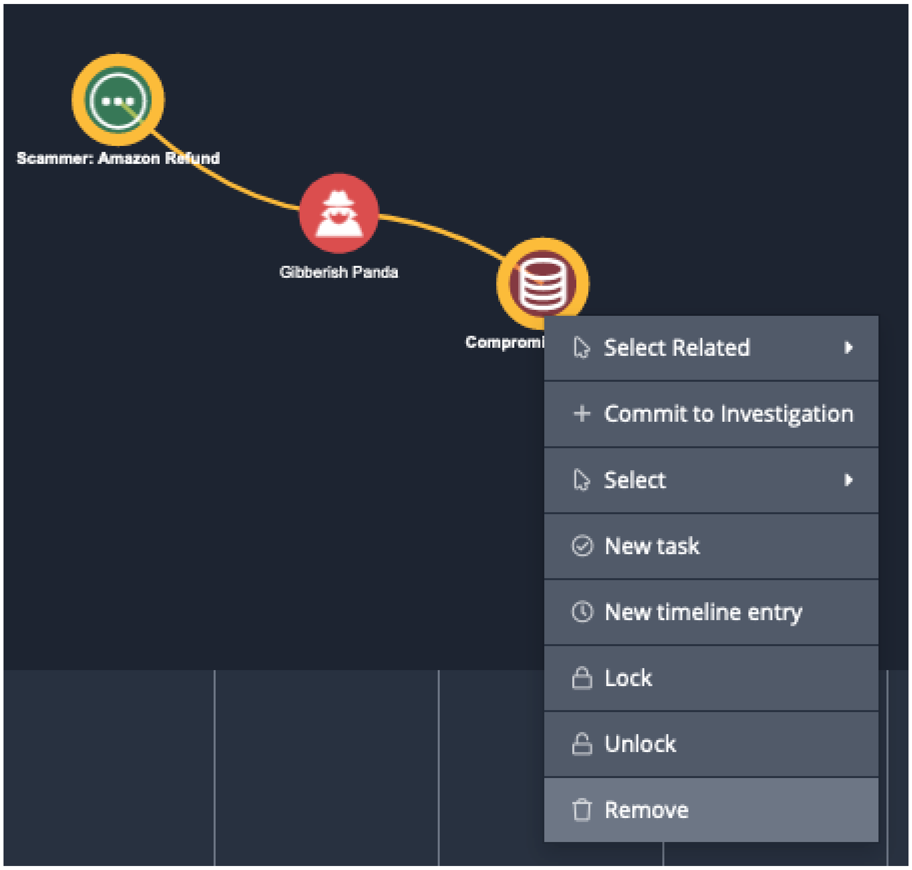
Right-Click Menu

1. Click on the relation object's node on the evidence board.



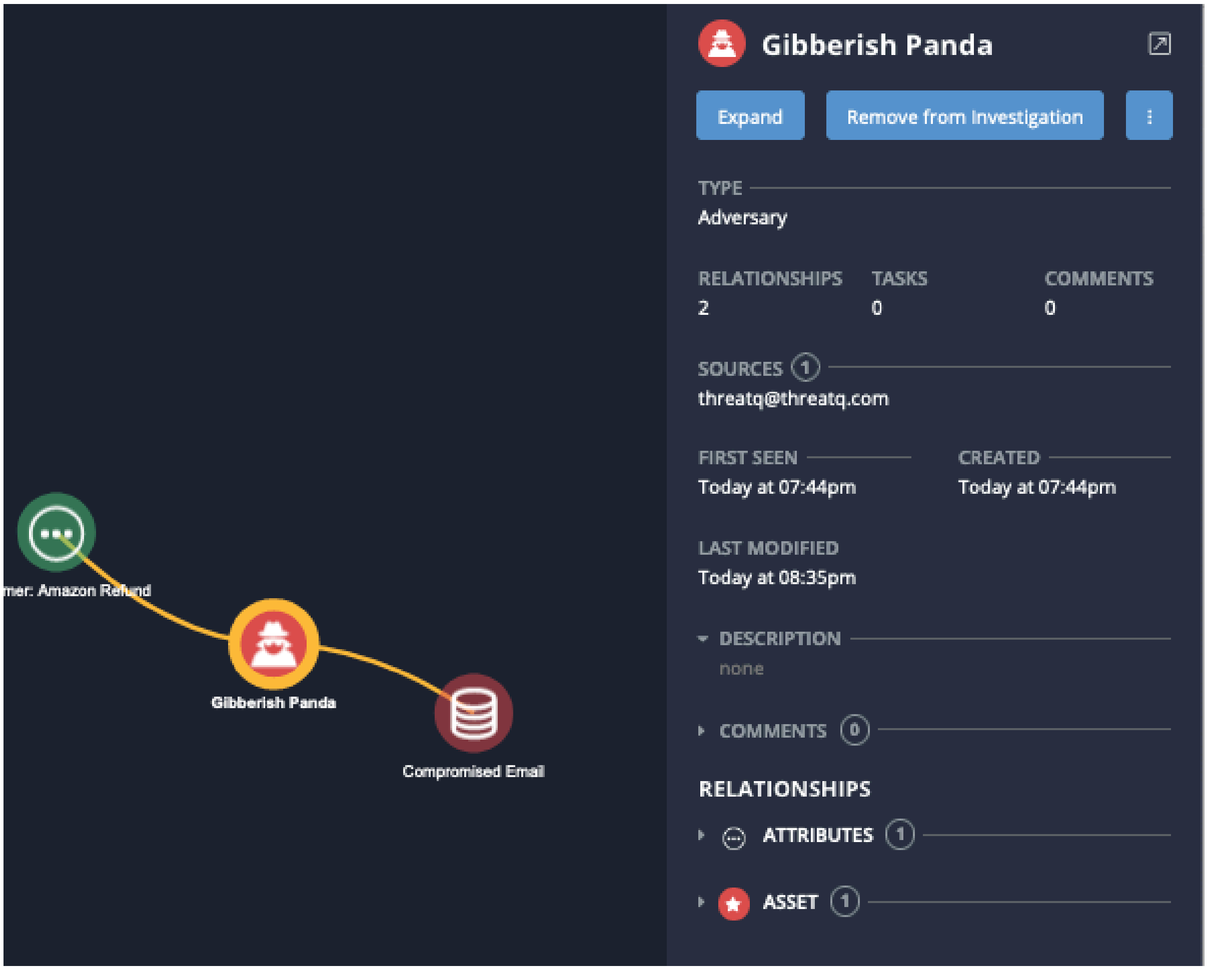
> You can select multiple node holding down the **Ctrl** key and clicking on the related nodes you want to hide.

2. Right click on the node and select **Remove**.

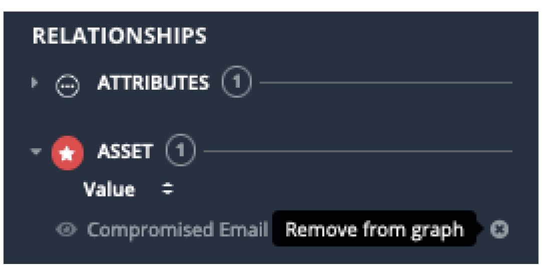


Investigation Object Details Menu

1. Click on the parent object node for the related objects and attributes.



2. Click on the **X** icon next to each object under the **Relationships** heading in the right pane window.



Timeline

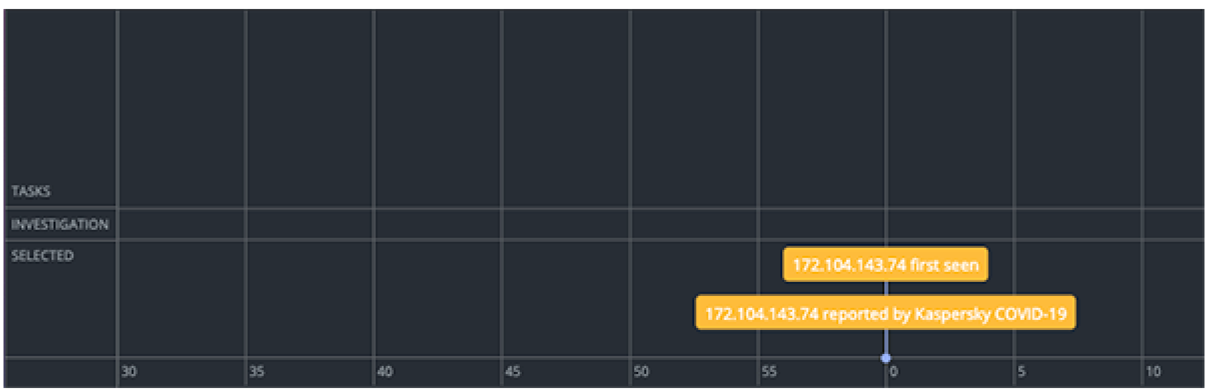
About the Timeline

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.

Timeline Rows

The Timeline displays entries in one of three row cateogories:

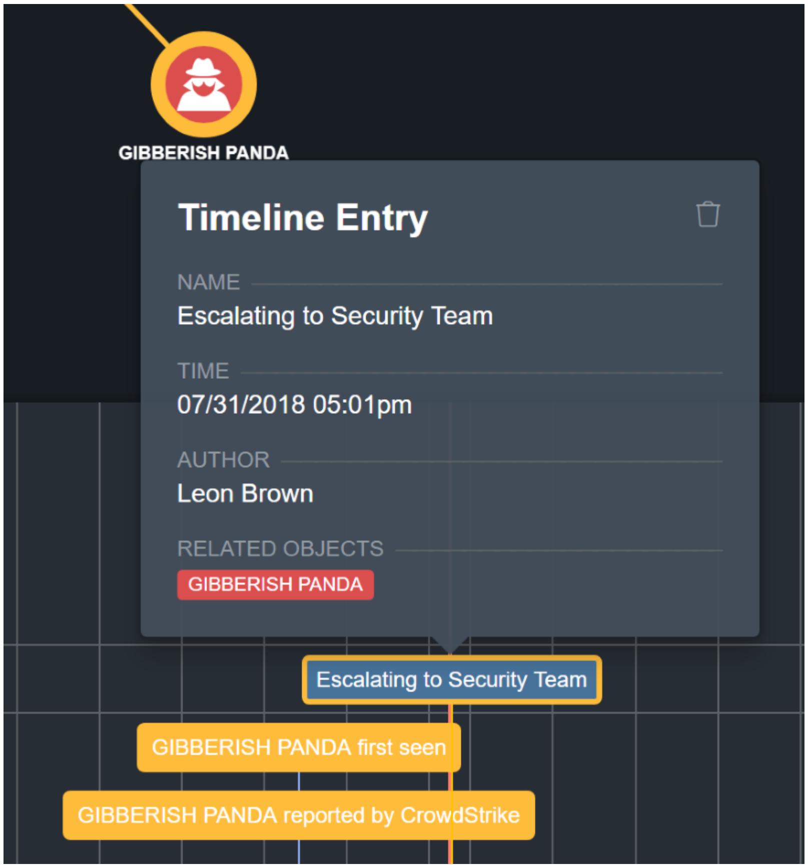
- **Tasks** - displays the task and extends to the due date on the timeline (if supplied).
- **Investigation** - displays timeline entries, both automatically generated and manually added.
- **Selected** - plots on the Timeline when the selected system object was first seen/reported by a threat intelligence source.



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.



Deleting an TimeLine Entry Summary

You can delete Timeline Entries that you by clicking on the entry within the timeline and clicking on the delete icon.

> You can delete entries for the **Tasks** and **Investigation** timeline rows but not from the **Selected** row.

Change Log

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

- **Version 4.0.0**
  - Complete rewrite of guide.