

ThreatQ Investigations User Guide

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 © 2018 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.

Last Updated: Tuesday, July 31, 2018

Contents

ThreatQ Investigations User Guide	1
Warning and Disclaimer	2
Contents	4
Introduction	6
ThreatQ Investigations Introduction	6
Concept Overview	6
Evidence Board	7
Action Panel	7
Timeline	8
Investigations Management	10
Investigations Overview	10
Starting an Investigation	10
Managing Investigations	13
Filtering Investigations	14
Continuing an Investigation	15
Changing the Visibility of an Investigation	16
Deleting an Investigation	17
Editing an Investigation	17

Evidence Board	22
Evidence Board Overview	22
Adding Threat Intelligence Data to the Evidence Board	22
Managing Threat Intelligence Data on the Evidence Board	24
Accessing an Object's Details Page from the Evidence Board	26
Viewing an Object's Relationships on the Evidence Board	28
Adding an Object to an Investigation	30
Adding a New Task Related to an Object	31
Adding a New Timeline Entry Related to the Object	33
Locking and Unlocking an Object on the Evidence Board	35
Deleting an Object from the Evidence Board	36
Selecting Multiple Objects on the Evidence Board	37
Adding a Task to an Investigation	38
Action Panel	40
Action Panel Overview	40
Managing Threat Intelligence Data from the Action Panel	40
Timeline	43
Timeline Overview	43
Adding a Timeline Entry	43
Viewing a Timeline Entry Summary	44

Introduction

The following provides an introduction to ThreatQ Investigations.

- [ThreatQ Investigations Introduction](#)
- [Concept Overview](#)

ThreatQ Investigations Introduction

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 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 Overview

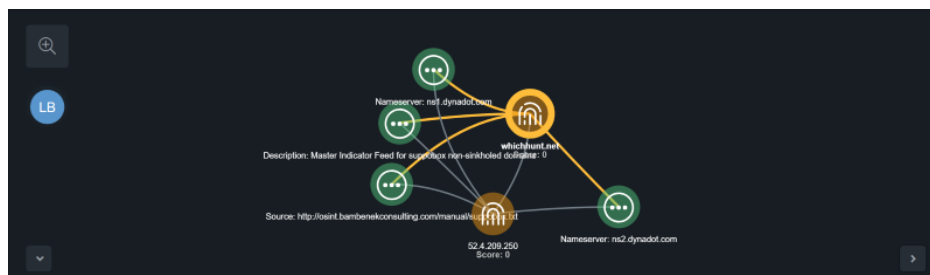
The following describes the components of an investigation and how it can be used to drive an incident response.

- [Evidence Board](#)
- [Action Panel](#)
- [Timeline](#)

Evidence Board

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

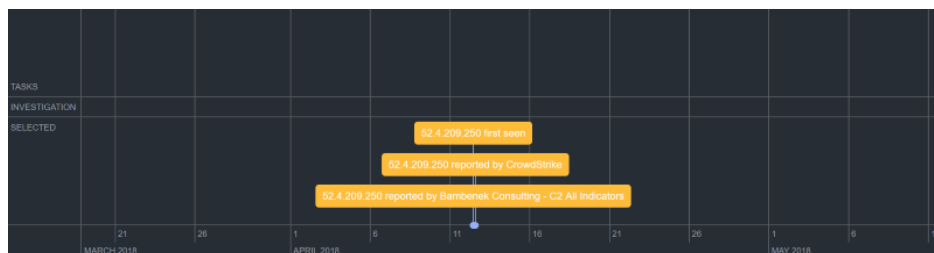
- See how the work of others impacts and extends your own.
- View a summary of any aspect of the evidence board that currently has mouse focus.

The screenshot displays the ThreatQ interface for an adversary named "GIBBERISH PANDA". At the top, there is a red circular icon with a white silhouette of a person wearing a hat. Below the icon, the name "GIBBERISH PANDA" is displayed in white. To the right of the name is a small square icon with a white arrow pointing up and to the right. Below the name, there are three buttons: "Expand", "Remove from Investigation", and a button with three vertical dots. Below the buttons, there are three sections: "TYPE" with the value "Adversary", "RELATIONSHIPS" with the value "1", and "TASKS" with the value "0". Below these sections, there is a "COMMENTS" section with the value "0". Below the "COMMENTS" section, there is a "SOURCES" section with a circled "1" and the value "CrowdStrike". Below the "SOURCES" section, there are two sections: "FIRST SEEN" with the value "Last Saturday at 12:13 AM" and "CREATED" with the value "Last Saturday at 12:13 AM". Below these sections, there is a "LAST MODIFIED" section with the value "Last Saturday at 12:13 AM". Below the "LAST MODIFIED" section, there is a "DESCRIPTION" section with a downward arrow and the value "none". Below the "DESCRIPTION" section, there is a "COMMENTS" section with a rightward arrow, the text "COMMENTS", a circled "0", and a horizontal line. Below the "COMMENTS" section, there is a "RELATIONSHIPS" section with a rightward arrow, a yellow circular icon with a white silhouette of a person wearing a hat, the text "INDICATORS", a circled "1", and a horizontal line.

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.



Investigations Management

The following describes how to create and manage investigations:

- [Investigations Overview](#)
- [Starting an Investigation](#)
- [Managing Investigations](#)

Investigations Overview

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 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; see [Managing 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.

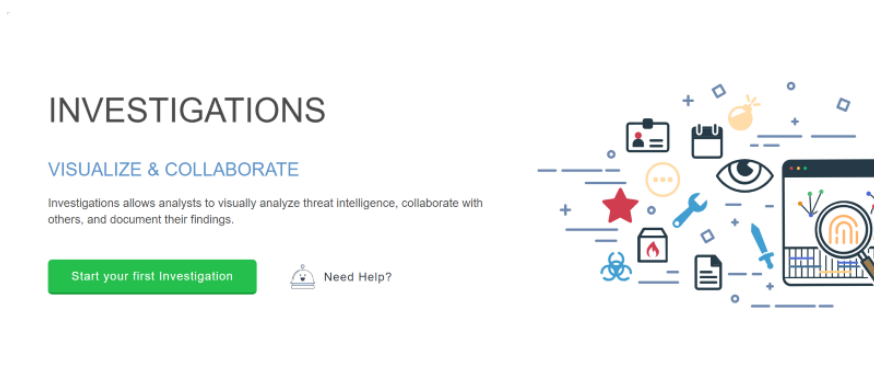
Starting an Investigation

To start your first investigation or start a new investigation, complete the following steps:

Procedure:

1. From the main menu, select one of the following options:

- **Investigations**, if this is your first investigation
- or **Create > Investigation**



2. If this is your first investigation, click **Start your first investigation**.

CREATE INVESTIGATION

×

Name

Status

Open

▼

Priority

Normal

▼

Visibility

Private

▼

Description

Create

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



What's normal and escalated depends upon your organization.

6. Select a **Visibility**:
 - **Private** - Only you can view and work with the investigation.
 - **Shared** - All ThreatQ users in your organization can view and work with the investigation.
7. Optionally, type a **Description** for the investigation.
8. Click **Create**.

The investigation workbench appears.

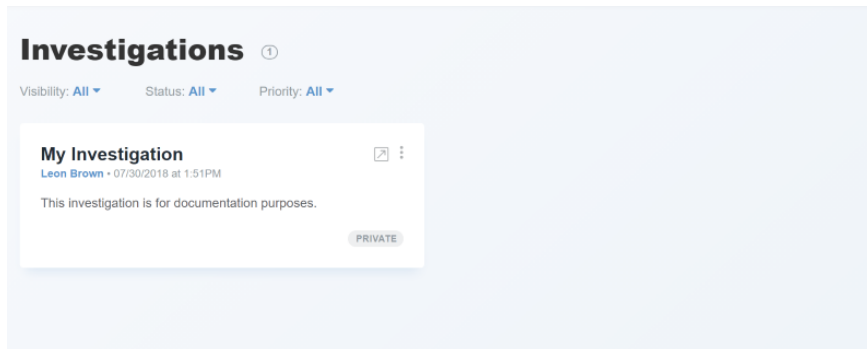


Managing Investigations

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

Procedure:

1. From the main menu, select **Investigations**.



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	Select one of the following options: <ul style="list-style-type: none">• Start your first investigation• Create > Investigation See Starting an Investigation .
Filter which investigations are viewed	See Filtering Investigations .
Continue an investigation	Select the investigation title; see Continuing an Investigation .

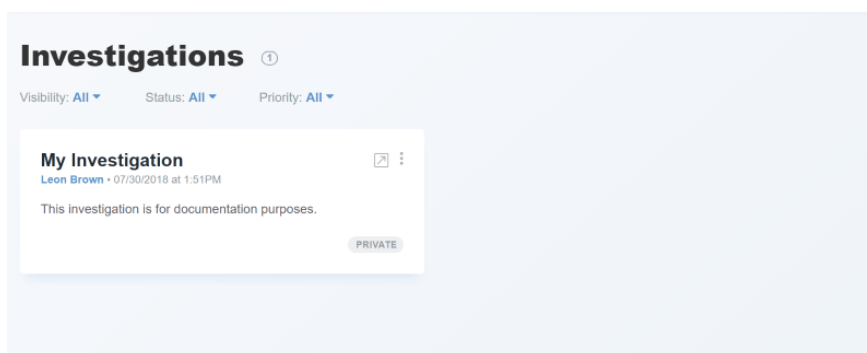
To	You can
Make an investigation private or shared	<p>Click the vertical ellipsis menu and select one of the following options:</p> <ul style="list-style-type: none">• Make Private• Make Shared <p>See Changing the Visibility of an Investigation.</p>
Delete an investigation	<p>Click the vertical ellipsis menu and select Delete; see Deleting an Investigation.</p>

Filtering Investigations

To manage the number of investigations viewed from the Investigations page, you can apply filters to view investigations based on specific criteria.

Procedure:

1. From the main menu, select **Investigations**.



2. Optionally, for **Visibility**, select one of the following filtering criteria:
 - **All**
 - **Private**

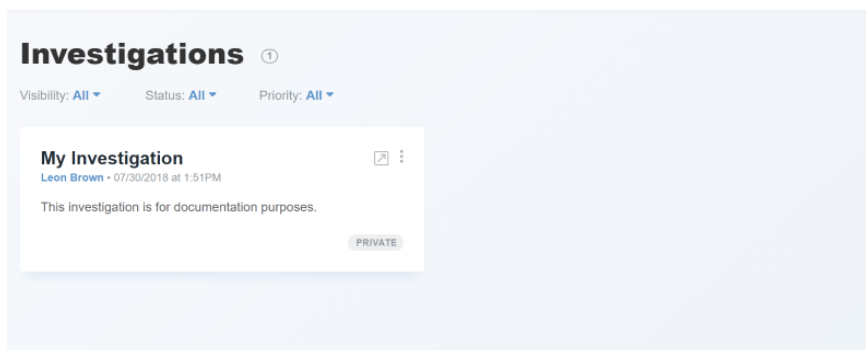
- **Shared**
3. Optionally, for **Status**, select one of the following filtering criteria:
 - **All**
 - **Open**
 - **Closed**
 4. Optionally, for **Priority**, select one of the following filtering criteria:
 - **All**
 - **Normal**
 - **Escalated**

Continuing an Investigation

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

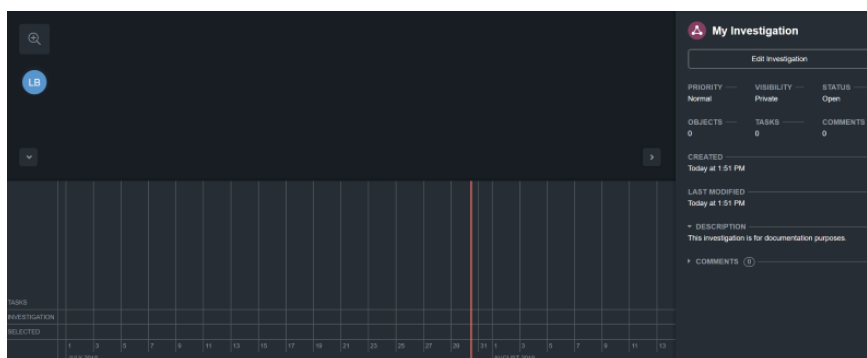
Procedure:

1. From the main menu, select **Investigations**.



2. Click the name of the investigation you want to continue.

The investigation workbench appears.

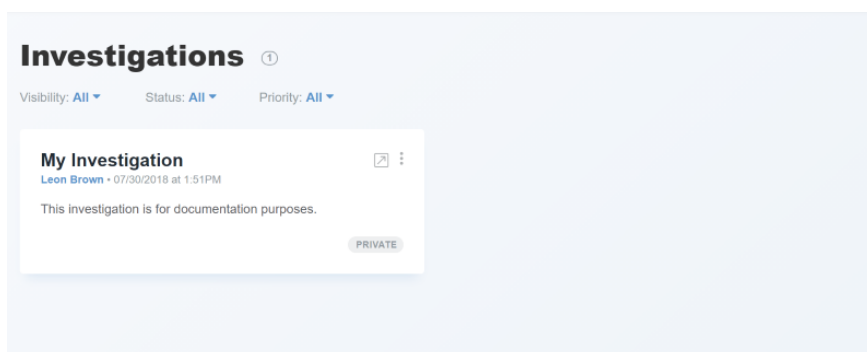


Changing the Visibility of an Investigation

You can change the visibility of an investigation from the Investigation page. As desired, you can decide whether an investigation is visible only to you or shared with everyone in your organization.

Procedure:

1. From the main menu, select **Investigations**.



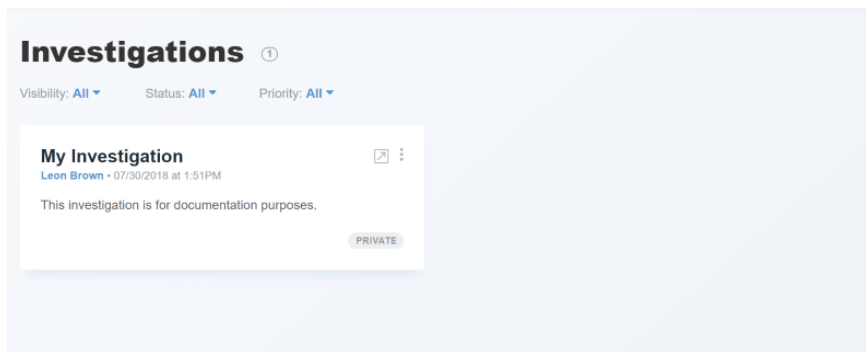
2. Select the investigation you want to edit.
3. Click the vertical ellipsis menu and select one of the following options:
 - **Make Private**
 - **Make Shared**

Deleting an Investigation

Deleting an investigation removes it from the Investigations page, but also from your system. Take care in selecting this option.

Procedure:

1. From the main menu, select **Investigations**.



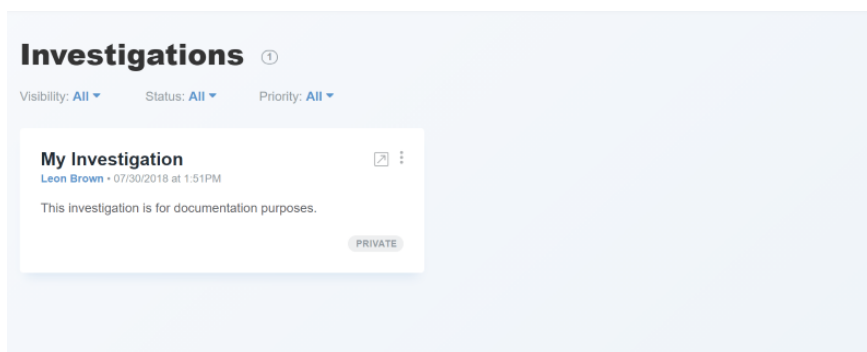
2. Click the name of the investigation you want to edit.
3. Click the vertical ellipsis menu and select **Delete**.
4. Click **Delete Investigation**.

Editing an Investigation

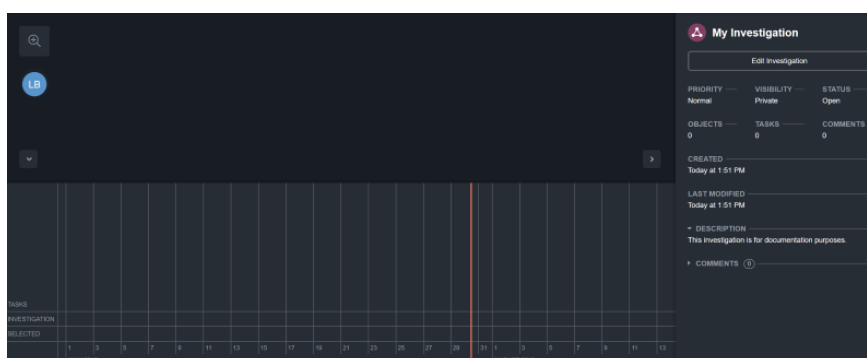
To edit the original parameters for an existing investigation, complete the following steps:

Procedure:


1. From the main menu, select **Investigations**.



2. Click the name of the investigation you want to edit.



3. Make sure that no nodes have the mouse focus and that you are viewing the action panel for the investigation.

 **My Investigation**

Edit Investigation

PRIORITY —
Normal

VISIBILITY —
Private

STATUS —
Open

OBJECTS —
0

TASKS —
0

COMMENTS —
0

CREATED —
Today at 1:51 PM

LAST MODIFIED —
Today at 1:51 PM

▼ DESCRIPTION —
This investigation is for documentation purposes.

▶ COMMENTS 0 —

4. In the action panel, click **Edit Investigation**.

EDIT INVESTIGATION ×

Name

Status

Open ▼

Priority

Normal ▼

Visibility

Private ▼

Description

This investigation is for documentation purposes.

Save

5. Optionally, edit the **Name** for the investigation.
6. Optionally, select a new **Status**:
 - **Open** - Open investigations appear as normal on the Investigations page.
 - **Closed** - Closed investigations appear greyed out on the Investigations page.
7. Optionally, select a new **Priority**:
 - **Normal**
 - **Escalated**



What's normal and escalated depends upon your organization.

8. Optionally, change the **Visibility**:
 - **Private** - Only you can view and work with the investigation.
 - **Shared** - All ThreatQ users in your organization can view and work with the investigation.
9. Optionally, edit the **Description** for the investigation.
10. Click **Save**.

Evidence Board

The following describes how to use the evidence board in an investigation.

- [Evidence Board Overview](#)
- [Adding Threat Intelligence Data to the Evidence Board](#)
- [Managing Threat Intelligence Data on the Evidence Board](#)
- [Adding a Task to an Investigation](#)

Evidence Board Overview

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, adversaries, and so on to the investigation, represented as a graphical node. 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



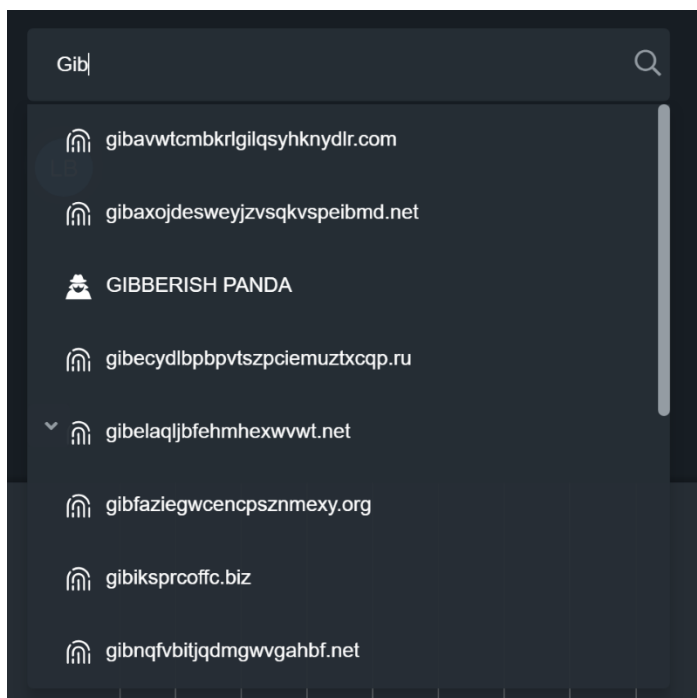
investigation. For more information, see [Adding an Object to an Investigation](#).

Procedure:

1. On the evidence board in the upper left corner, click the **Search** icon.

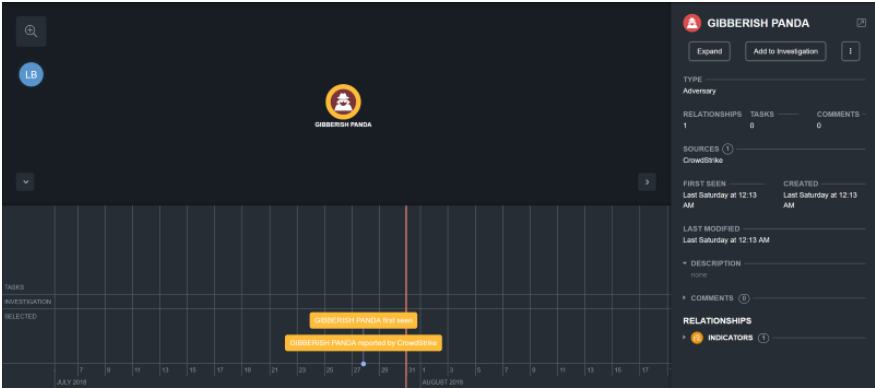


2. Enter criteria to search the Threat Library for threat intelligence data.



3. When you discover your object, mouse over it 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.

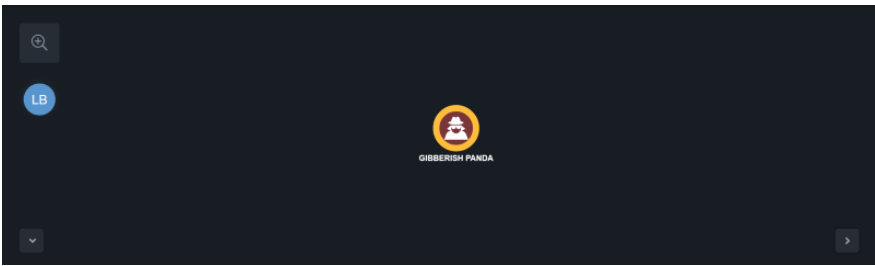
With the object highlighted as the focal point, a summary appears in the action panel.

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.

Procedure:

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 on 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 on the node and select Expand ; see Viewing an Object's Relationships on the Evidence Board .
Add the highlighted object to the investigation	Right-click on the node and select Add to Investigation ; see Adding an Object to an Investigation .
Add a new task related to the object	Right-click on 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 on the

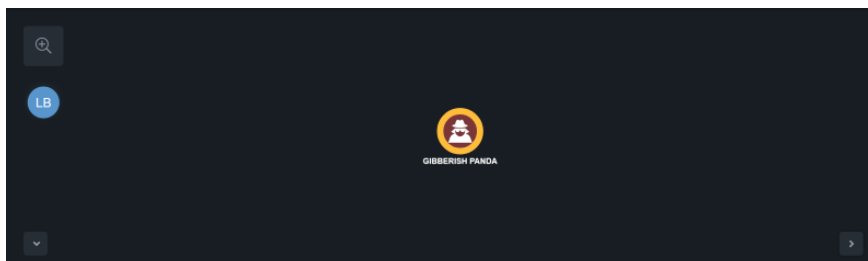
To	You can
	node and select New Timeline Entry ; see Adding a New Timeline Entry Related to the Object .
Unlock or lock an object	Right-click on the node and select Unlock or Lock ; see Locking and Unlocking an Object on the Evidence Board .
Delete an object from the evidence board	Right-click on the node and select Delete ; see Deleting an Object from the Evidence Board .

Accessing an Object's Details Page from the Evidence Board

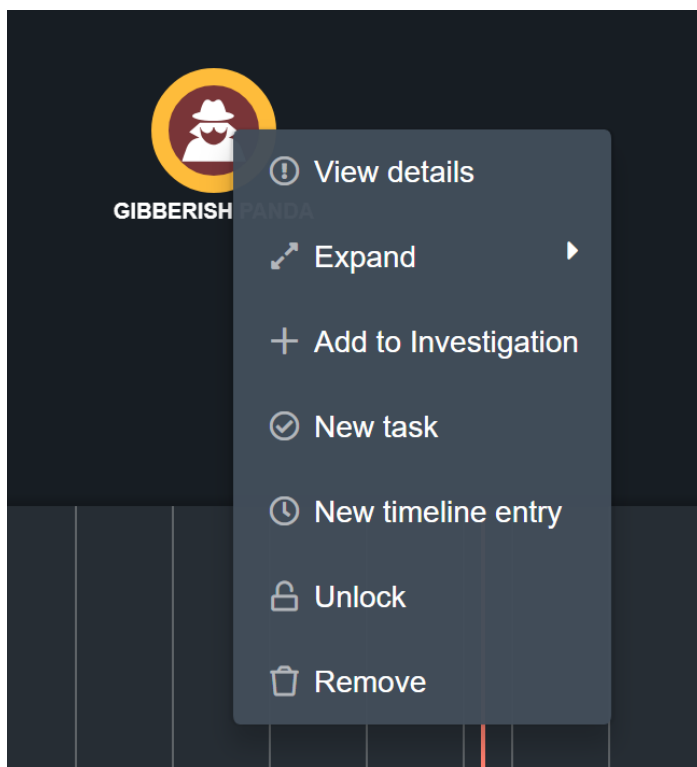
You can select an object on the evidence board and launch its object details page in ThreatQ for further investigation. For more information about ThreatQ objects, see the [ThreatQ User Guide](#).

Procedure:

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



2. Right-click and select **View Details**.



The ThreatQ object details page opens in a new browser tab.

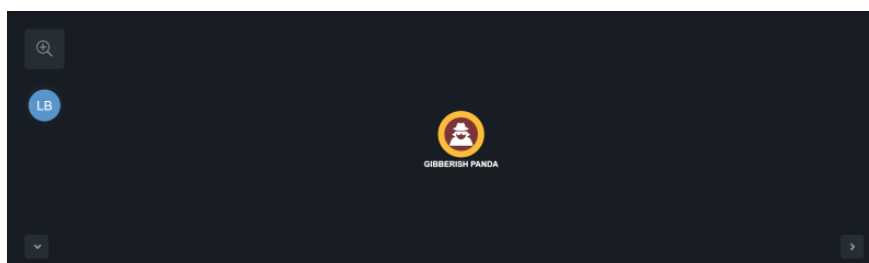


Viewing an Object's Relationships on the Evidence Board

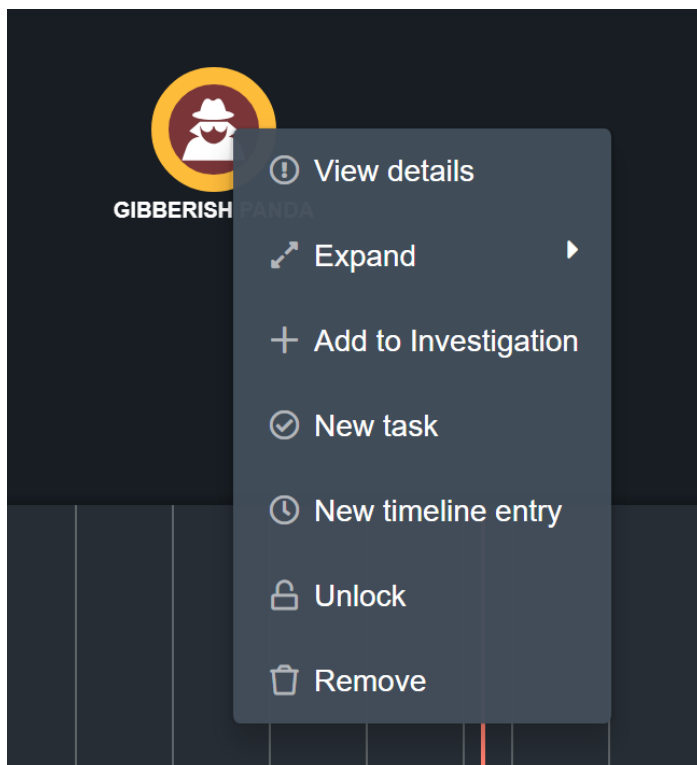
After you add an object to the evidence board, you can select to view the object's relationships as nodes, such as attributes and related indicators. You can then expand the view for related objects, as well.

Procedure:

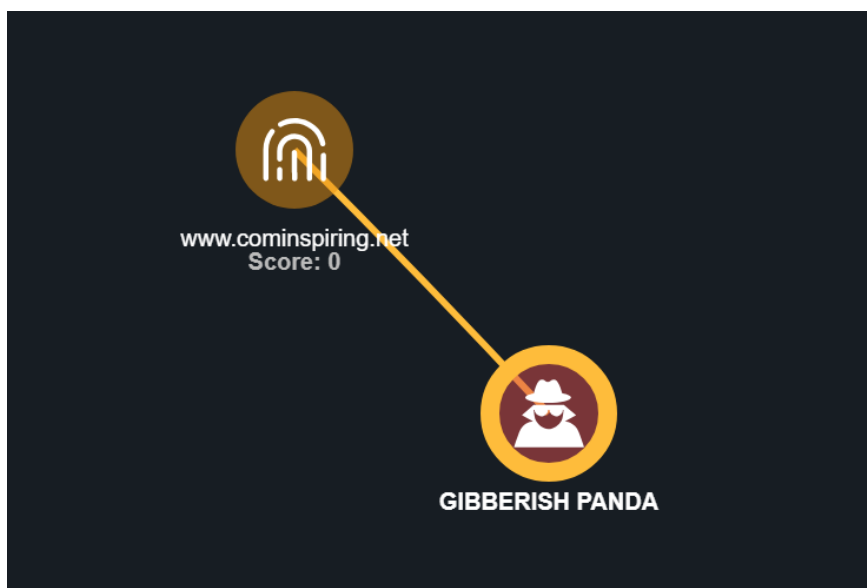
1. On the evidence board, select and highlight the node that represents the object you want to manage.



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



The node view expands to include related objects and attributes.

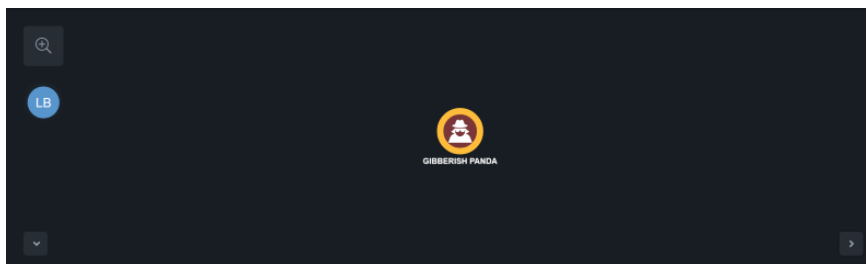


Adding an Object to an Investigation

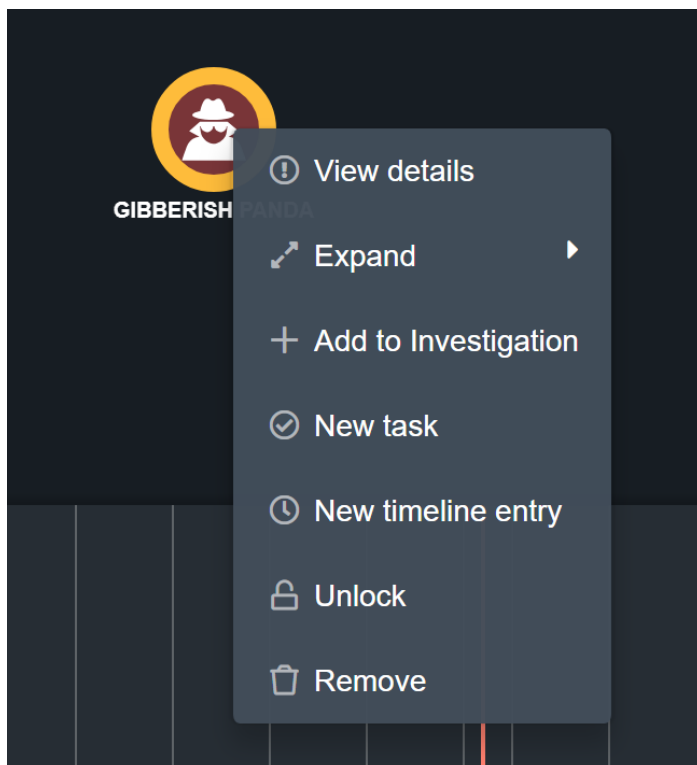
When you add an object to the evidence board, it becomes available for further examination. However, it does not immediately become a part of the current investigation. You must explicitly assign the object to the investigation. Until you do so, only you will be able to view the object in the investigation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

Procedure:

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



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



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

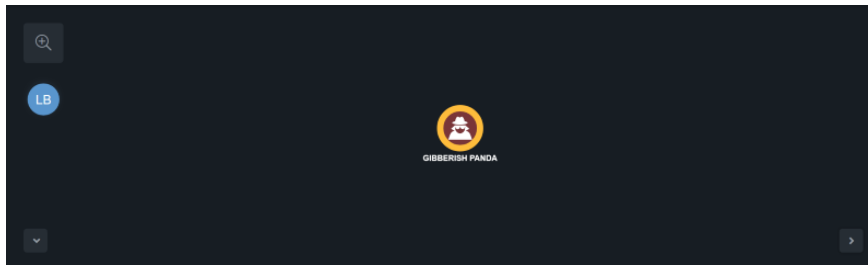
Adding a New Task Related to an Object

ThreatQ allows you to create and assign tasks to yourself or other users in the platform. You can also utilize 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.

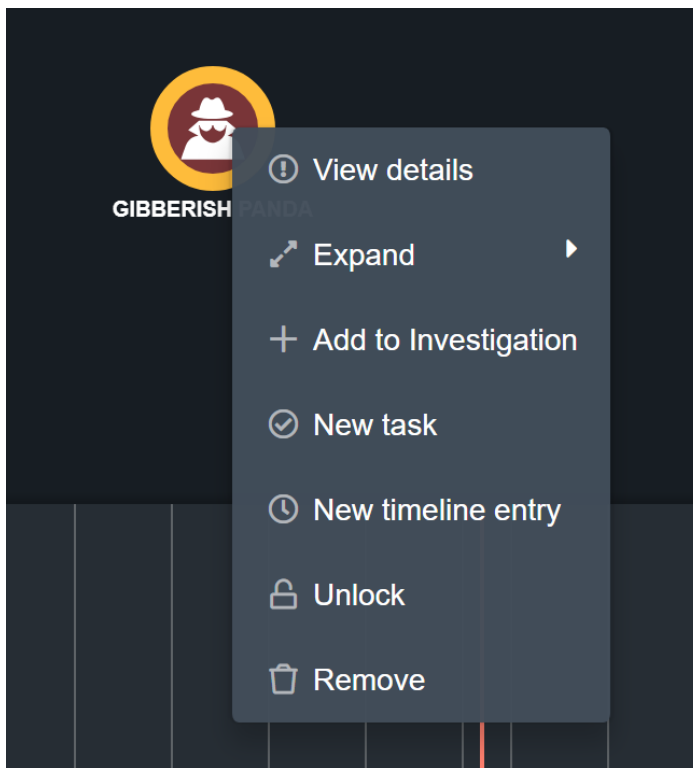
For more information about Tasks, see the [ThreatQ User Guide](#).

Procedure:

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. Enter a task **Name**.
4. Enter the assignee's email address in the **Assigned To** field.
5. Optionally, use the date picker to select a **Due Date**.

6. 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**.

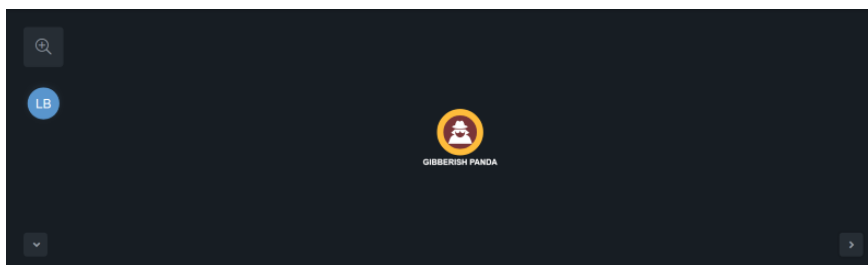
The task is added to the evidence board and the timeline.

Adding a New Timeline Entry Related to the Object

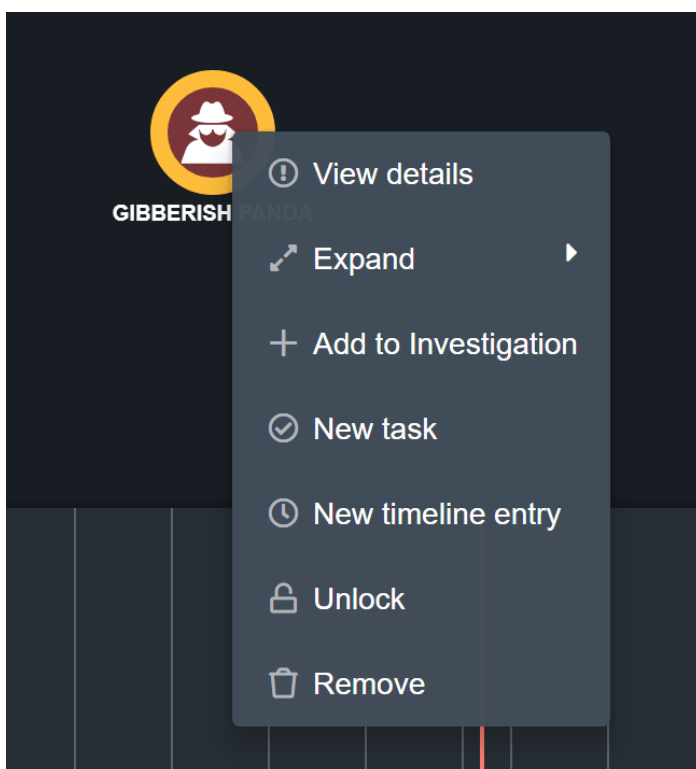
When you add an object to the evidence board, some relevant attributes are included on the timeline. You can also manually add timeline entries related to the object to use as milestones in the investigation. You can also add a timeline entry independent of a object; see [Adding a Timeline Entry](#).

Procedure:

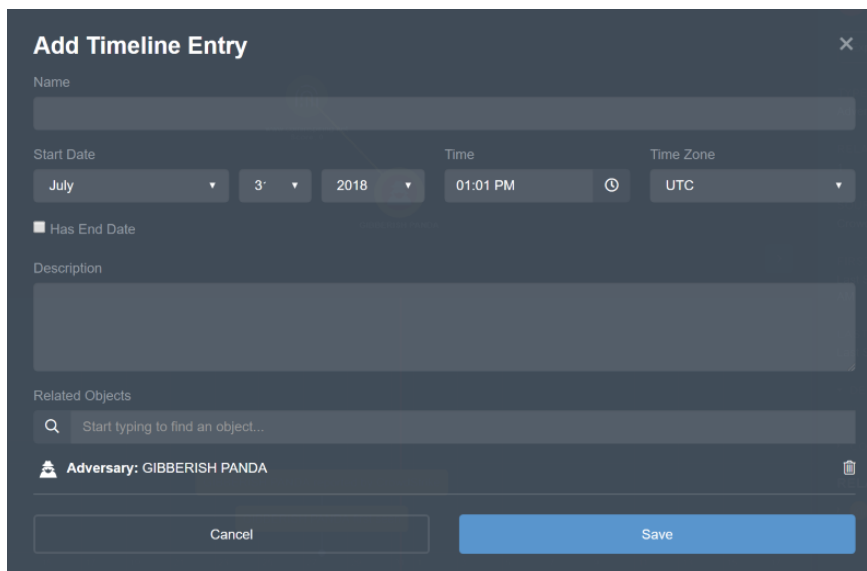
1. On the evidence board, select and highlight the node that represents the object for which you want to enter a timeline entry.



2. Right-click and select **New Timeline Entry**.



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



3. Enter a **Name** for the entry.
4. Enter a **Start Date**, **Time**, and **Time Zone**.
5. Optionally, select if the entry has an end date. If selected, enter an **End Date**, **Time**, and **Time Zone**.
6. Enter a **Description** for the timeline entry.
7. Optionally, enter any **Related Objects**.
8. Click **Save**.

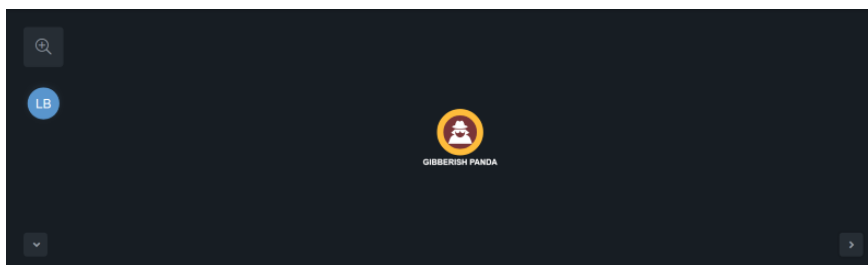
A new entry appears in the timeline.

Locking and Unlocking an Object on the Evidence Board

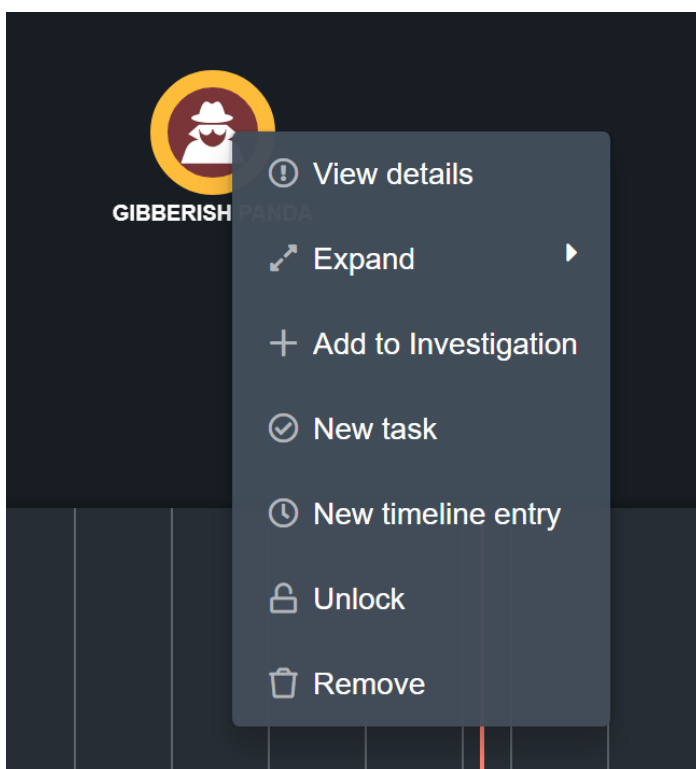
When an object is locked on the evidence board, it will not move when you click and drag a related attribute or object.

Procedure:

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



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



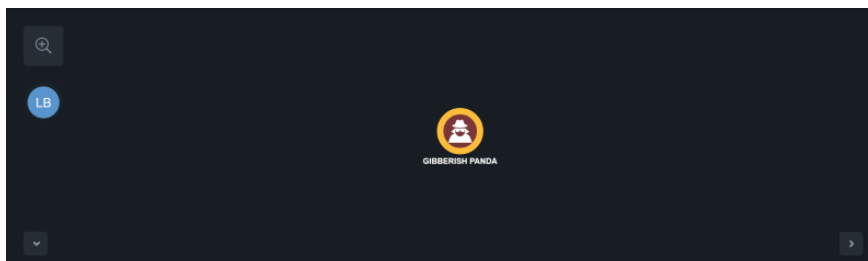
3. Optionally, if you want to lock the object, right-click and select **Lock**.

Deleting an Object from the Evidence Board

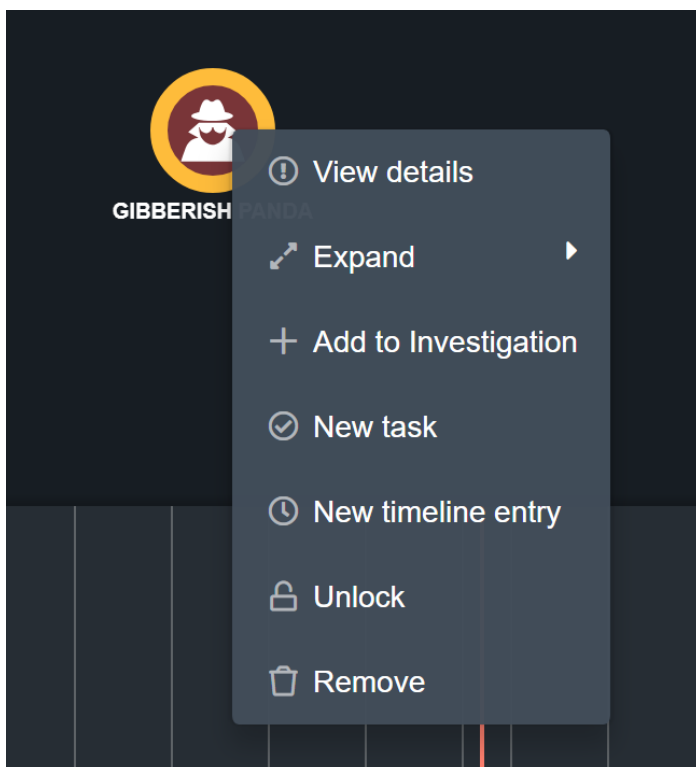
Deleting an object removes it from the evidence board and your investigation, but not from the ThreatQ platform. Take care in selecting this option.

Procedure:

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



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



3. Click **Delete**.

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.

Procedure:

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](#).

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 utilize 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 User Guide](#).

Procedure:

1. Right-click on an empty portion of the evidence board.
2. Right-click and select **New Task**.

The Add Task dialog box opens.

3. Enter a task **Name**.
4. Enter the assignee's email address in the **Assigned To** field.
5. Optionally, use the date picker to select a **Due Date**.

6. 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.

Action Panel

The following describes how to use the action panel in an investigation.

- [Action Panel Overview](#)
- [Managing Threat Intelligence Data from the Action Panel](#)

Action Panel Overview

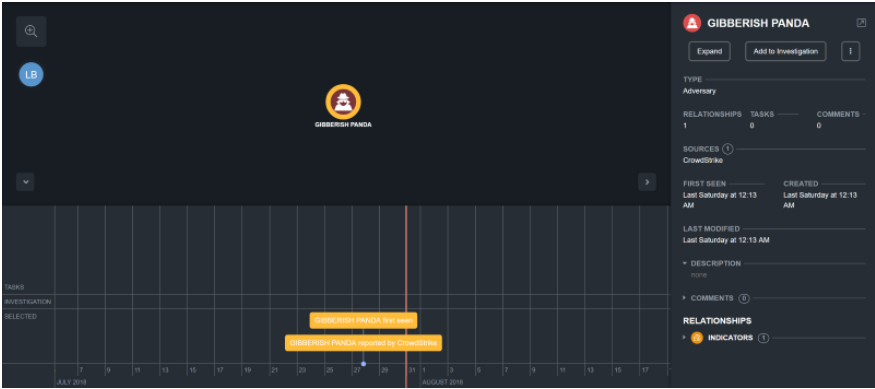
As you create an investigation and add objects to that investigation, these items are also reflected in the action panel. The action panel provides an overview of an item on the evidence board that currently has mouse focus. Depending on the item being summarized, you can also interact with and edit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

Procedure:

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 ThreatQ User Guide .
View the object's relationships on the evidence board	Click Expand ; see Viewing an Object's Relationships on the Evidence Board .
Add the highlighted object to the investigation	Click Add to Invest- igation ; see Adding an Object to an Invest- igation .

To	You can
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 .

Timeline

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

- [Timeline Overview](#)
- [Adding a Timeline Entry](#)
- [Viewing a Timeline Entry Summary](#)

Timeline Overview

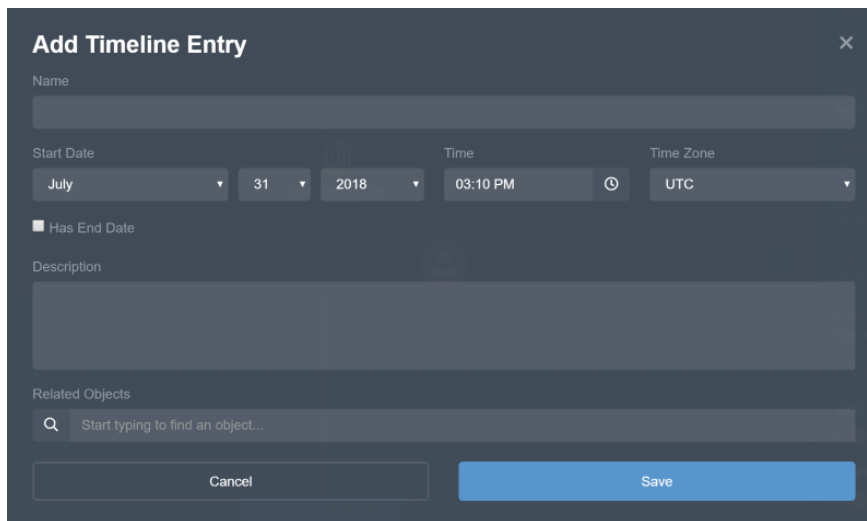
The timeline provides a view of milestones and tasks within an investigation. Most timeline events are auto generated, such as when ThreatQ first encountered an object and how the threat intelligence data was discovered, for example, via feed. When you create a task, it is also added to the timeline.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

Procedure:

1. Right-click on an empty portion of the evidence board.
2. Right-click and select **New Timeline Entry**.

The image shows a dark-themed dialog box titled "Add Timeline Entry" with a close button (X) in the top right corner. It contains several input fields: a "Name" field at the top; "Start Date" with a dropdown menu showing "July", a day dropdown showing "31", and a year dropdown showing "2018"; a "Time" field showing "03:10 PM" with a clock icon; and a "Time Zone" dropdown menu showing "UTC". Below these is a checkbox labeled "Has End Date". There is a large "Description" text area. At the bottom, there is a "Related Objects" section with a search bar containing the placeholder text "Start typing to find an object...". At the very bottom are two buttons: "Cancel" and "Save".

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

3. Enter a **Name** for the entry.
4. Enter a **Start Date**, **Time**, and **Time Zone**.
5. Optionally, select if the entry has an end date. If selected, enter an **End Date**, **Time**, and **Time Zone**.
6. Enter a **Description** for the timeline entry.
7. Optionally, enter any **Related Objects**.
8. 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.

Procedure:

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

