IBM Resilient

resilient

Incident Response Platform

USER GUIDE v29

Resilient Incident Response Platform User Guide

Platform Version	Publication	Notes
29.0	October 2017	Initial publication.

Table of Contents

1. Introduction

The Resilient Incident Response Platform is a purpose built tool for the unique requirements of consistently and efficiently managing computer-related security incidents or the breach of personally identifiable information.

This guide provides you with a detailed description of the Resilient platform and its various features and functions that you use when responding to incidents.

If you are an administrator and you require information about dynamic playbooks or system administration, see the *Resilient Incident Response Platform Master Administrator Guide*.

2. Concepts You Need to Know

The Resilient Incident Response Platform is, essentially, a central hub for incident responses. It is customizable so that it can be tailored to meet the needs of your company or organization. Therefore, how you interact with the Resilient platform is dependent on these customizations.

This guide focuses on the incident response aspect of the Resilient platform. The following sections provide a description of the basic concepts you should know to interact effectively with the Resilient platform when responding to incidents.

2.1. Incidents and Objects

An *incident* is an event in which data or a system may possibly be compromised. The Resilient platform allows these incidents to be entered by Resilient users or systems integrated with the Resilient platform. You can then monitor the status from the start to the resolution of the incident.

An incident within the Resilient platform can contain the following objects:

- Task. A unit of work to be accomplished by a user, device or process. The Resilient platform handles some tasks automatically. What is more relevant is that you can be assigned tasks to accomplish manually and mark them as complete when done. Incident owners can track the progress of the various tasks.
- Note. Text added to an incident or task for clarification or additional information.
- Attachment. A file uploaded and attached to an incident or task.
- Artifact. Data that supports or relates to the incident. The Resilient platform organizes artifacts by type, such as file name, MAC address, suspicious URL, MD5 and SHA1 file hashes, and more. An artifact can also have an attachment, such as an email, log file, or malware sample.

In addition to objects, an incident can utilize one or more workflows. A *workflow* is a predefined set of activities that can perform a complex set of instructions. With the proper permission, you can view the status of an incident’s workflows and, if necessary, terminate a workflow.

2.2. Dynamic Playbook

Your organization designs and implements the set of rules, conditions, business logic and tasks used to respond to an incident. This set is referred to as a *dynamic playbook*. These playbooks provide the Resilient platform the means to update the response to an incident automatically as the input changes or the incident progresses.

You do not see dynamic playbooks directly, but you see its results. The dynamic playbook determines which information is available to you, which tasks are assigned to you, and which actions you can take on any particular incident. As the incident changes, so can the assigned tasks and actions.

2.3. Your Role

Your administrator defines your role, which determines how you interact with incidents. For example, an observer role could allow you to view incident information but not change it, while an incident creator can enter and manage incidents. You may be able to access all incidents or just specific incidents.

The following lists some of the actions you may be able to take on incidents, depending on your role.

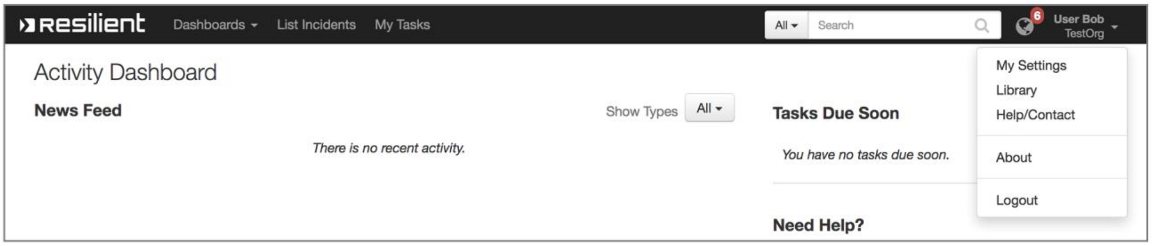
- Create an incident.
- Generate reports on one or more incidents.
- Check the status of the incident.
- Edit incident information and monitor the tasks.
- Perform tasks as assigned.
- Close an incident.
- Delete an incident.
- Perform other actions configured by your administrator. These actions are accessible through the **Actions** button in the incident page, or a **[…]** button near an object.

3. Getting Started

You access the Resilient platform from a web browser. Your administrator provides you with the URL and login information.

Before you log in, make sure that you are using a supported web browser, which is the current release or one release back of each of the following browsers: Chrome, Firefox, Safari and Internet Explorer.

At any time, you can access the documentation and Support information by clicking your user name in the right corner and selecting **Help/Contact** in the drop-down menu. There is also a link to the documentation and Support on the Activity Dashboard page, which is the home page when you log in.



There is no recent activity.

You have no tasks due soon.

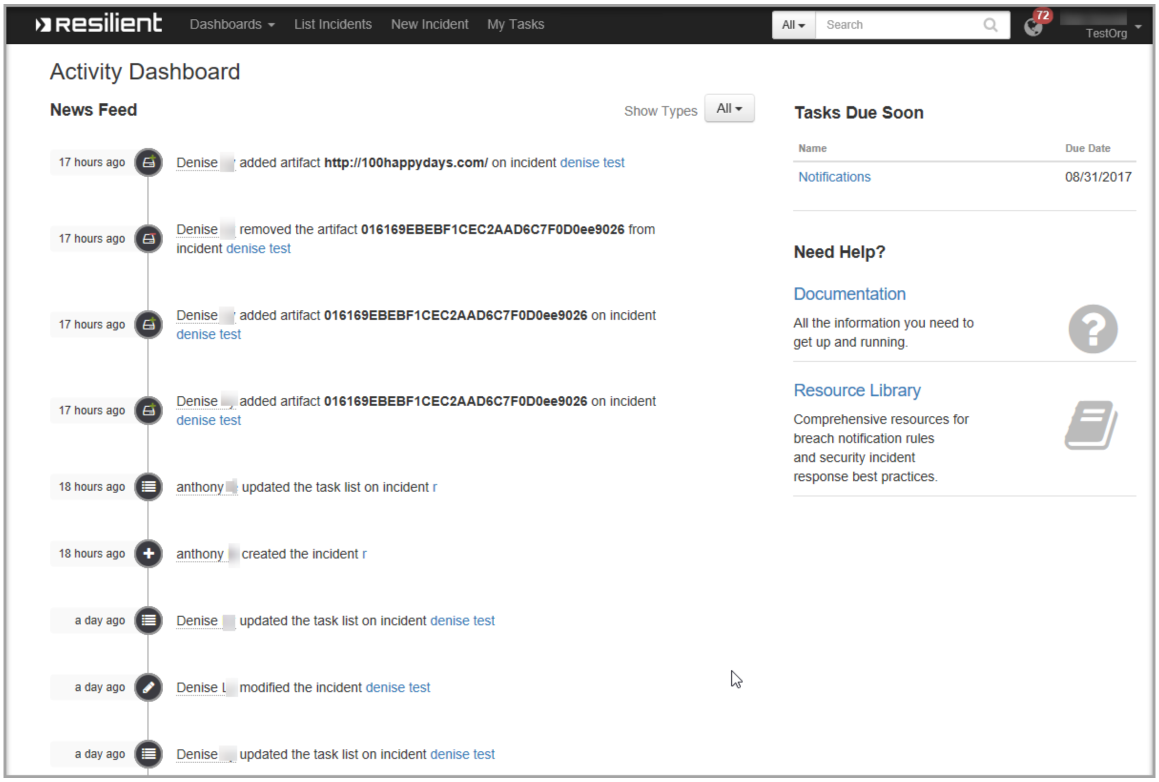
3.1. Activity Dashboard

The Activity Dashboard is the default page when you log in. It contains the following:

- **Newsfeed**: Provides up-to-the-minute activity updates for all incidents for which you are a member. To view specific actions only in the newsfeed, click the **Show Types** drop-down menu. In addition, each incident may also have a Newsfeed tab that shows only the activities for that incident.
- **Tasks Due Soon**: Displays tasks assigned to you that are due within the next 7 days. Click the task to go directly to that task and incident.

  TIP: Click on **My Tasks** in the menu bar to see all of your tasks.

Here is an example of an Activity Dashboard.



Activity Dashboard

News Feed

Show Types All ▾

17 hours ago Denise [redacted] added artifact **http://100happydays.com/** on incident denise test

17 hours ago Denise [redacted] removed the artifact **016169EBEBF1CEC2AAD6C7F0D0ee9026** from incident denise test

17 hours ago Denise [redacted] added artifact **016169EBEBF1CEC2AAD6C7F0D0ee9026** on incident denise test

17 hours ago Denise [redacted] added artifact **016169EBEBF1CEC2AAD6C7F0D0ee9026** on incident denise test

18 hours ago anthony [redacted] updated the task list on incident r

18 hours ago anthony [redacted] created the incident r

a day ago Denise [redacted] updated the task list on incident denise test

a day ago Denise L[redacted] modified the incident denise test

a day ago Denise [redacted] updated the task list on incident denise test

Tasks Due Soon

Name	Due Date
Notifications	08/31/2017

Need Help?

Documentation

All the information you need to get up and running.

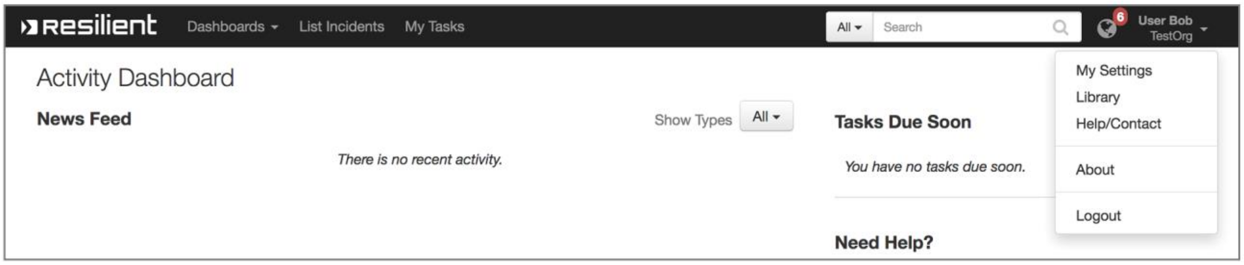
Resource Library

Comprehensive resources for breach notification rules and security incident response best practices.

You can access the Activity Dashboard anytime by clicking the **Dashboards** menu and selecting **Activity Dashboard**. There is another type of dashboard called Analytics, which is described in Analytics Dashboard.

3.2. My Settings

You can edit your personal settings by clicking the arrow in the upper right corner of the page near your name and then selecting **My Settings**.



There is no recent activity.

You have no tasks due soon.

In the My Settings page, you can access the following:

- My Profile

  Allows you to update basic profile information such as name, title, and phone numbers. Click **Edit** then make the desired changes and select **Save**.

- Notifications

  You can receive a notification when an activity occurs that involves you, such as being assigned a task or incident. Each notification on the Notifications page has an information icon, which you can hover over for details.

  For each notification, you can choose to be notified by email, alert icon in the Resilient toolbar, both or neither, by clicking the checkbox next to the appropriate icon. You do not receive notifications for actions that you instigate; for example, you do not receive Task Closed notifications for tasks that you close.

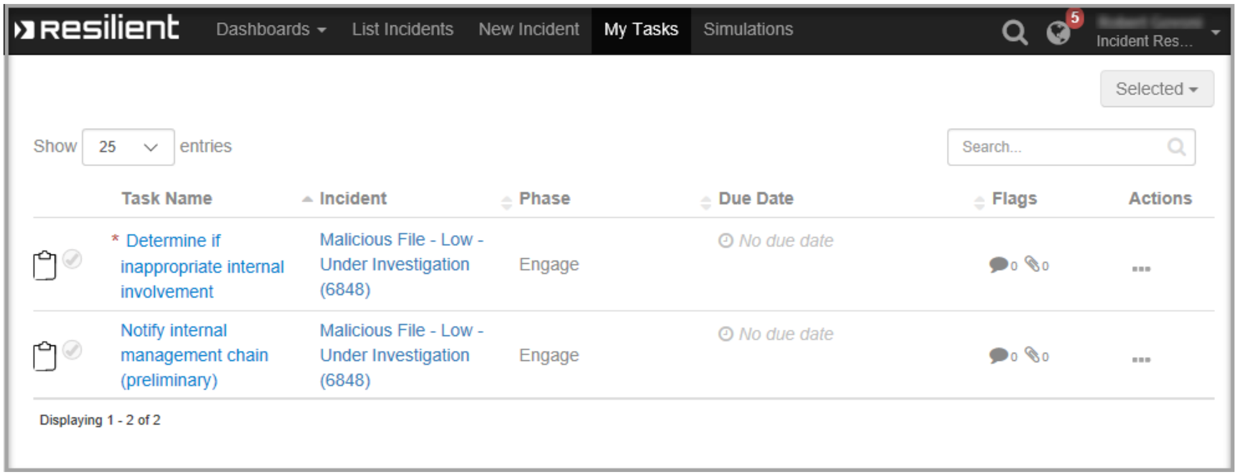
  If you choose to be notified by the alert icon in the Resilient toolbar, you will see a number by the globe icon next to the left of your username whenever there are available notifications. The previous screenshot shows 6 notifications. You can click on the globe icon to review the notifications.

- Change Password

  This feature allows you to change your password.

3.3. My Tasks

You can view the tasks of each incident. You can also view a list of tasks assigned to you, regardless of incident, by clicking **My Tasks** in the menu bar. You can then click the task name for details, the incident name to go to the incident, modify the due date, add notes and attachments, and perform actions. See the Tasks section in this guide for details on managing tasks.



	Task Name	Incident	Phase	Due Date	Flags	Actions
	* Determine if inappropriate internal involvement	Malicious File - Low - Under Investigation (6848)	Engage	No due date	0 0	...
	Notify internal management chain (preliminary)	Malicious File - Low - Under Investigation (6848)	Engage	No due date	0 0	...

Displaying 1 - 2 of 2

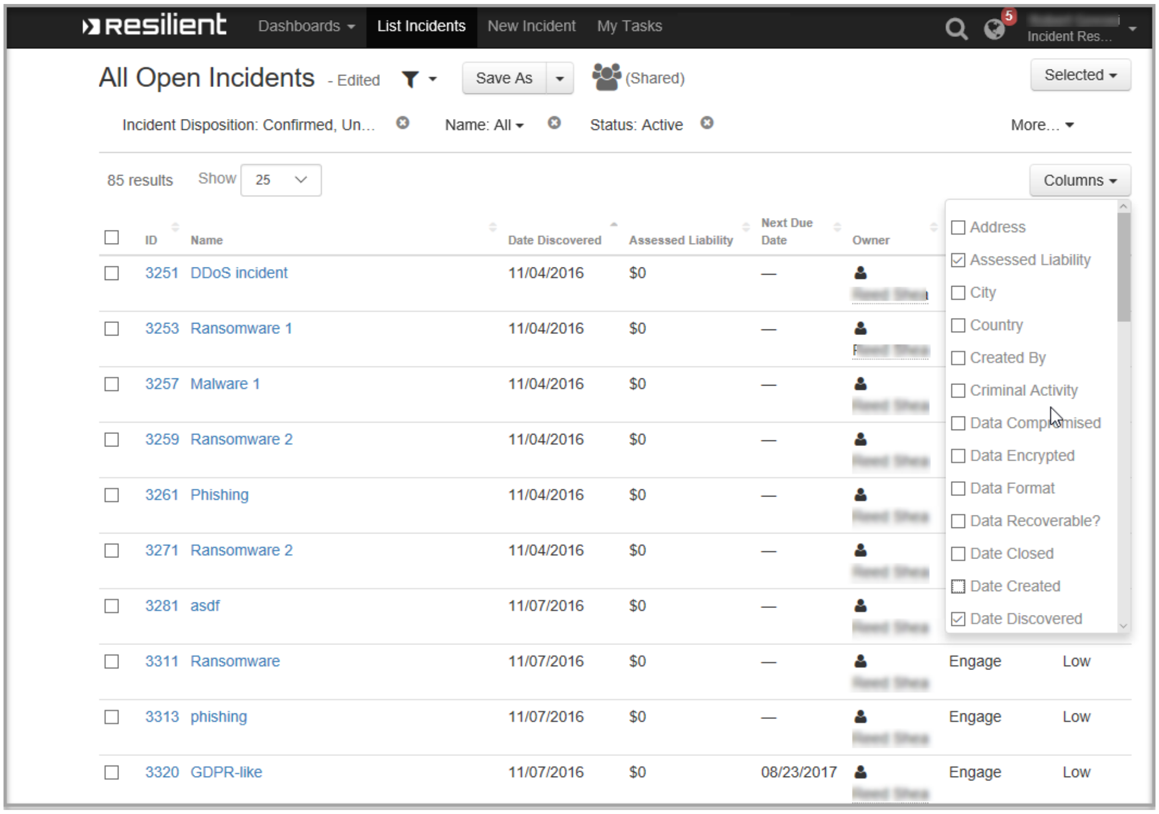
4. Observing Incidents

Click **List Incidents** in the menu bar to display all incidents. Click an incident name to view its details.

4.1. List of Incidents

The List Incidents page displays those incidents that you have permission to view. This page provides an overview of the incidents; however, you determine which information is shown by selecting the columns. To do this, click the **Columns** button on the right then check the columns you wish to view and uncheck those you wish to hide. You can also drag the columns left or right to reorganize the information.

The following is an example of a List of Incidents page with the Columns button selected.



All Open Incidents - Edited

Incident Disposition: Confirmed, Un… Name: All Status: Active

85 results Show 25

☐	ID	Name	Date Discovered	Assessed Liability	Next Due Date	Owner		
☐	3251	DDoS incident	11/04/2016	$0	—	[redacted]		
☐	3253	Ransomware 1	11/04/2016	$0	—	[redacted]		
☐	3257	Malware 1	11/04/2016	$0	—	[redacted]		
☐	3259	Ransomware 2	11/04/2016	$0	—	[redacted]		
☐	3261	Phishing	11/04/2016	$0	—	[redacted]		
☐	3271	Ransomware 2	11/04/2016	$0	—	[redacted]		
☐	3281	asdf	11/07/2016	$0	—	[redacted]		
☐	3311	Ransomware	11/07/2016	$0	—	[redacted]	Engage	Low
☐	3313	phishing	11/07/2016	$0	—	[redacted]	Engage	Low
☐	3320	GDPR-like	11/07/2016	$0	08/23/2017	[redacted]	Engage	Low

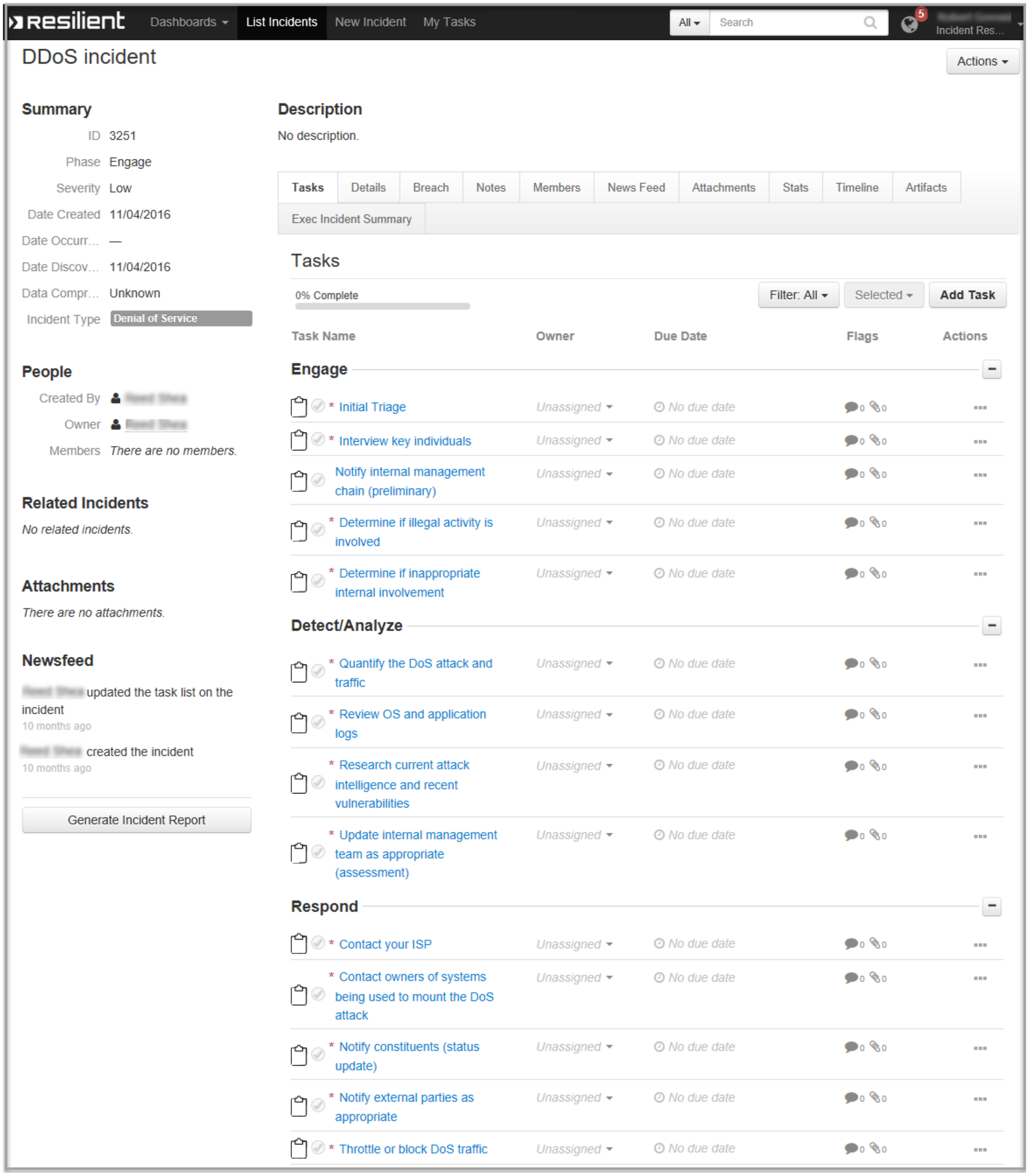
- ☐ Address
- ☑ Assessed Liability
- ☐ City
- ☐ Country
- ☐ Created By
- ☐ Criminal Activity
- ☐ Data Compromised
- ☐ Data Encrypted
- ☐ Data Format
- ☐ Data Recoverable?
- ☐ Date Closed
- ☐ Date Created
- ☑ Date Discovered

4.2. Individual Incident

The information shown for each incident can vary. The basic layout for an incident is that general information is shown on the left, in a section of the page called Summary Section.

The Resilient platform organizes the detailed incident information into various tabs. Your administrator defines and customizes these tabs. Some tabs may be conditional and appear only when one or more given conditions occur.

The following screenshot is an example of an incident page.



DDoS incident

Summary

ID	3251
Phase	Engage
Severity	Low
Date Created	11/04/2016
Date Occurr...	—
Date Discov...	11/04/2016
Data Compr...	Unknown
Incident Type	Denial of Service

People

Created By	[redacted]
Owner	[redacted]
Members	*There are no members.*

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

[redacted] updated the task list on the incident
10 months ago

[redacted] created the incident
10 months ago

Description

No description.

Tasks

0% Complete

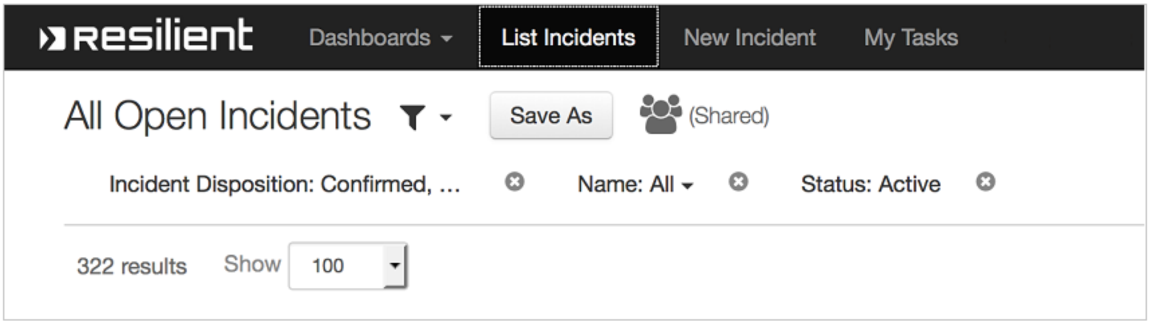
Task Name	Owner	Due Date	Flags	Actions
Engage				
* Initial Triage	Unassigned	No due date	0 0	⋯
* Interview key individuals	Unassigned	No due date	0 0	⋯
Notify internal management chain (preliminary)	Unassigned	No due date	0 0	⋯
* Determine if illegal activity is involved	Unassigned	No due date	0 0	⋯
* Determine if inappropriate internal involvement	Unassigned	No due date	0 0	⋯
Detect/Analyze				
* Quantify the DoS attack and traffic	Unassigned	No due date	0 0	⋯
* Review OS and application logs	Unassigned	No due date	0 0	⋯
* Research current attack intelligence and recent vulnerabilities	Unassigned	No due date	0 0	⋯
* Update internal management team as appropriate (assessment)	Unassigned	No due date	0 0	⋯
Respond				
* Contact your ISP	Unassigned	No due date	0 0	⋯
* Contact owners of systems being used to mount the DoS attack	Unassigned	No due date	0 0	⋯
* Notify constituents (status update)	Unassigned	No due date	0 0	⋯
* Notify external parties as appropriate	Unassigned	No due date	0 0	⋯
* Throttle or block DoS traffic	Unassigned	No due date	0 0	⋯

4.3. Filters

The Incidents page can contain a very large number of incidents. To better navigate this page, you can use various filters, as well as create your own.

Filters are persistent. Therefore, when you click **List Incidents** in the menu bar to display the Incidents page, you see the results matching the last filter used. The name at the upper left corner of the page is the name of the filter. For example, the following screenshot shows the All Open Incidents filter. This filter lists all the open incidents by searching for these properties:

- Disposition = Confirmed or Unconfirmed
- Name = All (equivalent to no filtering by name)
- Status = Active



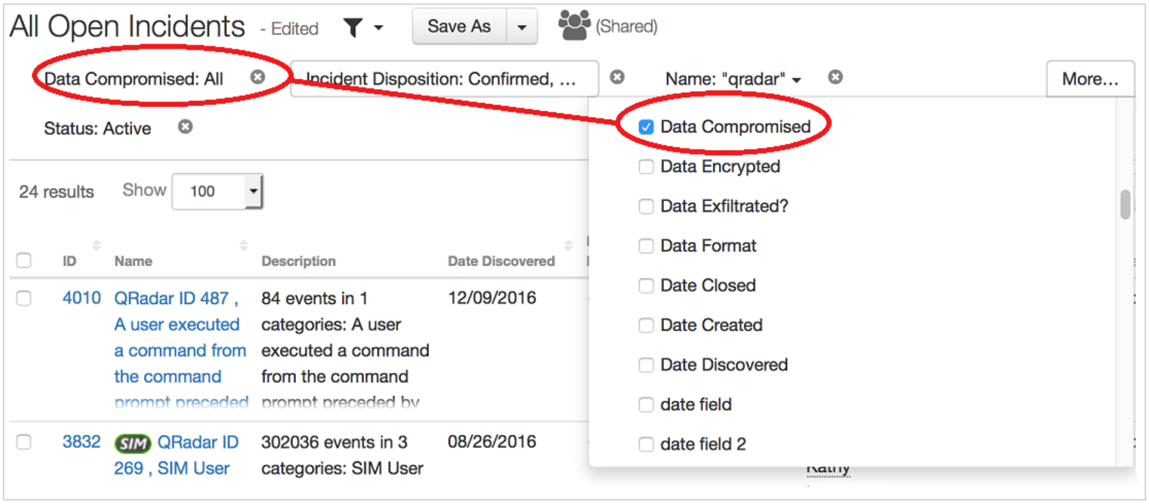
All Open Incidents ▼ ▾

Incident Disposition: Confirmed, … ⊗ Name: All ▾ ⊗ Status: Active ⊗

322 results Show 100

You can choose a different filter by clicking the down arrow next to the filter icon (▼ ▾).

You can further filter the incident list by searching for fields with a specific value. Click the **More** button. Select the fields you wish to use in your filter. As you click the checkbox next to a field, it appears with the other fields. The following example shows the Data Compromised field selected.



All Open Incidents - Edited ▼ ▾

Data Compromised: All ⊗ Incident Disposition: Confirmed, … ⊗ Name: "qradar" ▾ ⊗

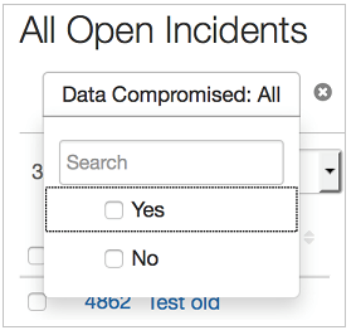
Status: Active ⊗

24 results Show 100

☑ Data Compromised
□ Data Encrypted
□ Data Exfiltrated?
□ Data Format
□ Date Closed
□ Date Created
□ Date Discovered
□ date field
□ date field 2

□	ID	Name	Description	Date Discovered
□	4010	QRadar ID 487 , A user executed a command from the command prompt preceded	84 events in 1 categories: A user executed a command from the command prompt preceded by	12/09/2016
□	3832	SIM QRadar ID 269 , SIM User	302036 events in 3 categories: SIM User	08/26/2016

You can then click on the field and choose or enter a value, depending on the field.



All Open Incidents

Data Compromised: All

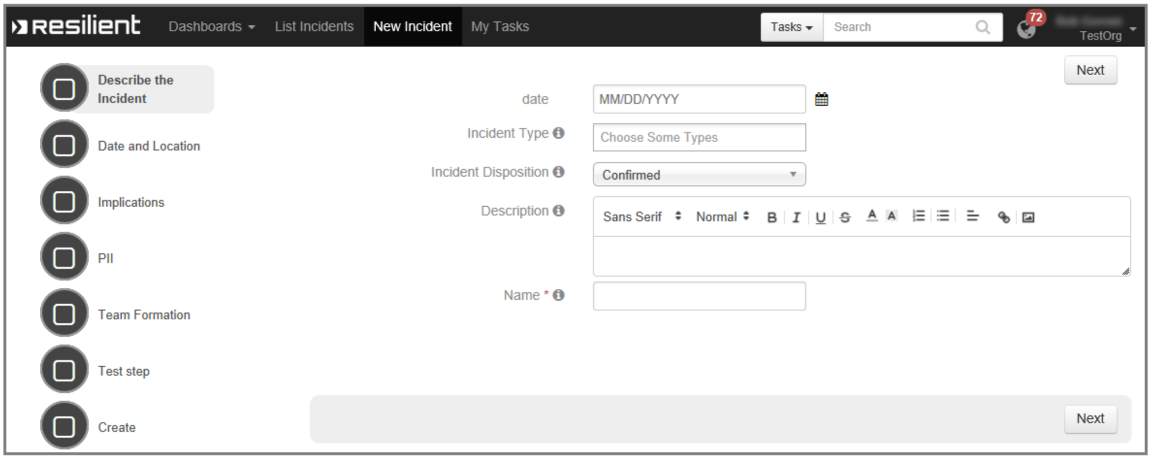
To remove a field from the filter, click the **x** next to the field.

If you wish to reuse your filter settings, click the **Save As button**. Enter a name and description for your filter. Choose **Private** (default) or **Shared**, which allows other users to select and use your filter.

If making changes to a filter, you can discard your changes by clicking the arrow next to the **Save As** button then selecting **Discard Changes** from the menu.

5. Creating an Incident

To report a new incident, click **New Incident** in the menu bar. This starts a wizard that guides you through entering the incident details and reviewing the recommended actions based on those specifics, as well as forming an incident response team. The following figure shows an example of the first page.



date: MM/DD/YYYY

Incident Type: Choose Some Types

Incident Disposition: Confirmed

Description:

Name *:

Some answers may cause additional steps to appear in the wizard. For example, indicating that Personally Identifiable Information (PII) has been compromised causes the system to add steps. These steps allow you to provide additional specific information and, in the case of compromised PII data, allow you to select those regulators that should be notified. Your answers assist the Resilient platform to properly assess the incident and generate an appropriate playbook.

6. Managing Incidents

How you manage an incident depends on your role, the nature of the incident, and the dynamic playbook in place. The tasks involved with managing an incident include the following:

- Add or update incident details.
- In the case of PII data, update breach information.
- Perform the tasks assigned to you.
- Add, edit or remove notes.
- Add or remove attachments.
- Add or remove artifacts.
- Implement pre-defined actions and check their status.
- Add information to data tables. If configured, interact with other security tools from data tables.

If you are an incident owner or a member, you may be able to add and assign tasks, and create custom tasks.

You can manage incidents individually by clicking **List Incidents** in the menu bar to display all incidents then clicking an incident name to view its details. You can also perform some functions on multiple incidents simultaneously in the List Incidents page by clicking the checkboxes next to those incidents then clicking the **Selected** button and choosing a function.

➢ **NOTE**: Depending on your role and the configuration of the Resilient platform, you may not be able to access all the tabs and features listed in this guide.

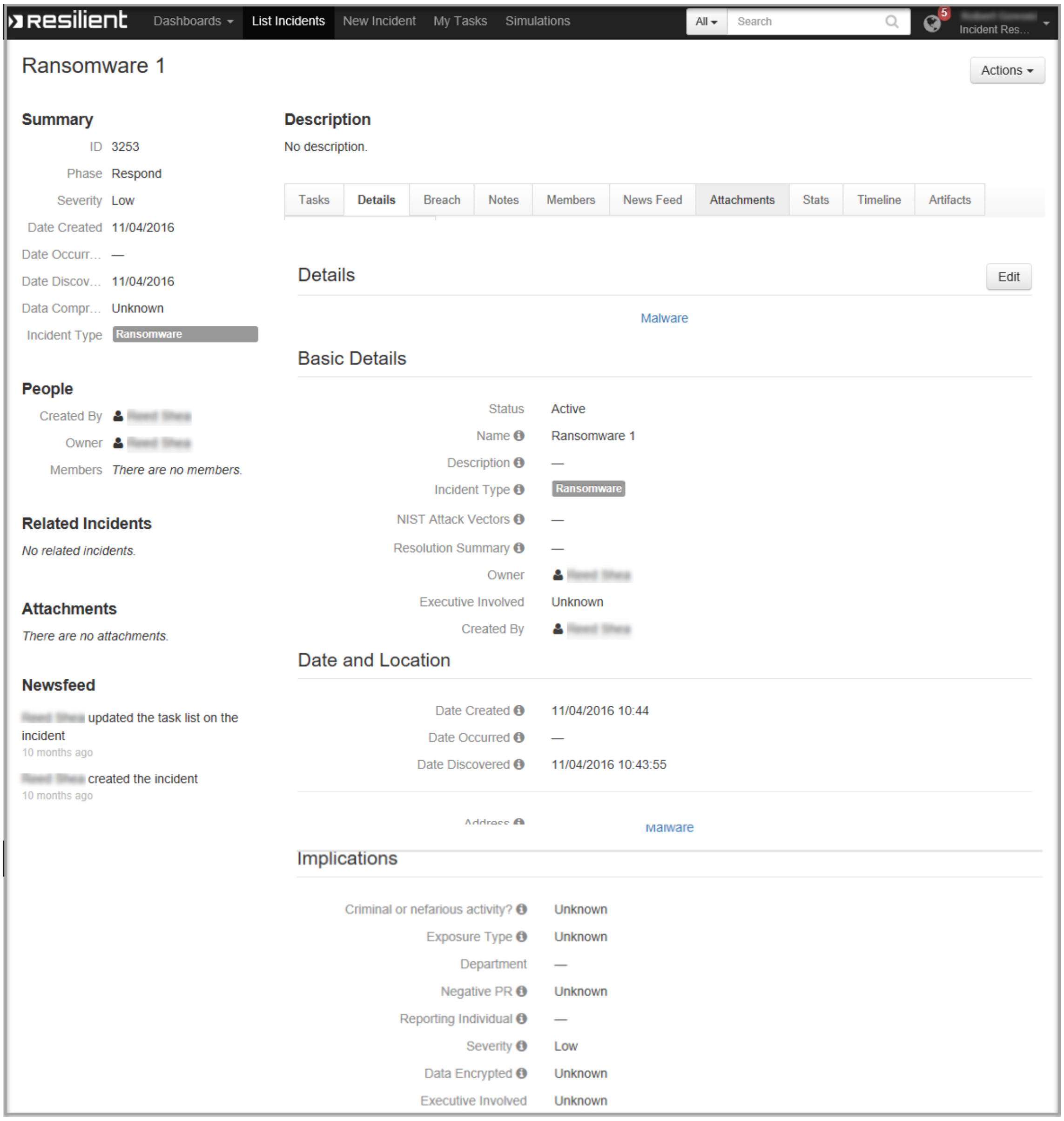
6.1. Incident Details

As details about an incident emerge, you can update the information. Typically, you update the information in the incident’s **Details** tab. For Personally Identifiable Information (PII) data, you update the information in the **Breach** tab. Depending on the dynamic playbook, the tabs may not be present, renamed, or in a different order than shown in the sample screenshots in this guide.

To modify information, go to the **Details** tab and click the **Edit** button then edit the various fields as required. Changes may cause additional tasks to be added to the playbook.

If you change a field regarding PII data, such as changing Exposure Type in the example from Unknown to Yes, make sure to review the **Breach** tab to enter additional required information. If you change an “Unknown” to “Yes,” you can update the details from within the task that instructs you to investigate if data has been compromised.

The following is an example of a **Details** tab.



Ransomware 1

Summary

ID	3253
Phase	Respond
Severity	Low
Date Created	11/04/2016
Date Occurr...	—
Date Discov...	11/04/2016
Data Compr...	Unknown
Incident Type	Ransomware

People

Created By	[redacted]
Owner	[redacted]
Members	*There are no members.*

Related Incidents

No related incidents.

Attachments

There are no attachments.

Newsfeed

[redacted] updated the task list on the incident
10 months ago

[redacted] created the incident
10 months ago

Description

No description.

Details

Malware

Basic Details

Status	Active
Name	Ransomware 1
Description	—
Incident Type	Ransomware
NIST Attack Vectors	—
Resolution Summary	—
Owner	[redacted]
Executive Involved	Unknown
Created By	[redacted]

Date and Location

Date Created	11/04/2016 10:44
Date Occurred	—
Date Discovered	11/04/2016 10:43:55
Address	

Malware

Implications

Criminal or nefarious activity?	Unknown
Exposure Type	Unknown
Department	—
Negative PR	Unknown
Reporting Individual	—
Severity	Low
Data Encrypted	Unknown
Executive Involved	Unknown

6.2. Breach

If the incident involves Personally Identifiable Information (PII) data, additional information is required under the **Breach** tab of the incident. Additional details such as types of data involved, number of records, and applicable jurisdictions are required. For EMEA, AsiaPac, and Latin America jurisdictions, it is important to read each tooltip in order to determine applicability to the incident.

Entering these details allows the system to generate an assessment, which provides a summary of the reporting and notification requirements. The summary also provides a liability estimate of what could be imposed by authorities in the form of fines for not completing the required notifications.

To modify breach information, go to the **Breach** tab and click the **Edit** button then edit the various fields as required.

The Resilient platform maintains a database of breach notification statutes (laws passed by a legislature and signed into law), regulations (laws made by agencies), trade organization bulletins, and guidance documents, including penalties where applicable. You can review the statutes in the Resource Library, which you access by clicking on your username in the upper right hand corner of the page and selecting **Library** from the drop-down menu. There is also a link to the Resource Library on the Activity Dashboard. Select the desired jurisdiction or regulator to view the relevant text of the document. Hyperlinks to the full source documents are also included. The Library is organized into sections. Access to each section is dependent on your organization’s subscription.

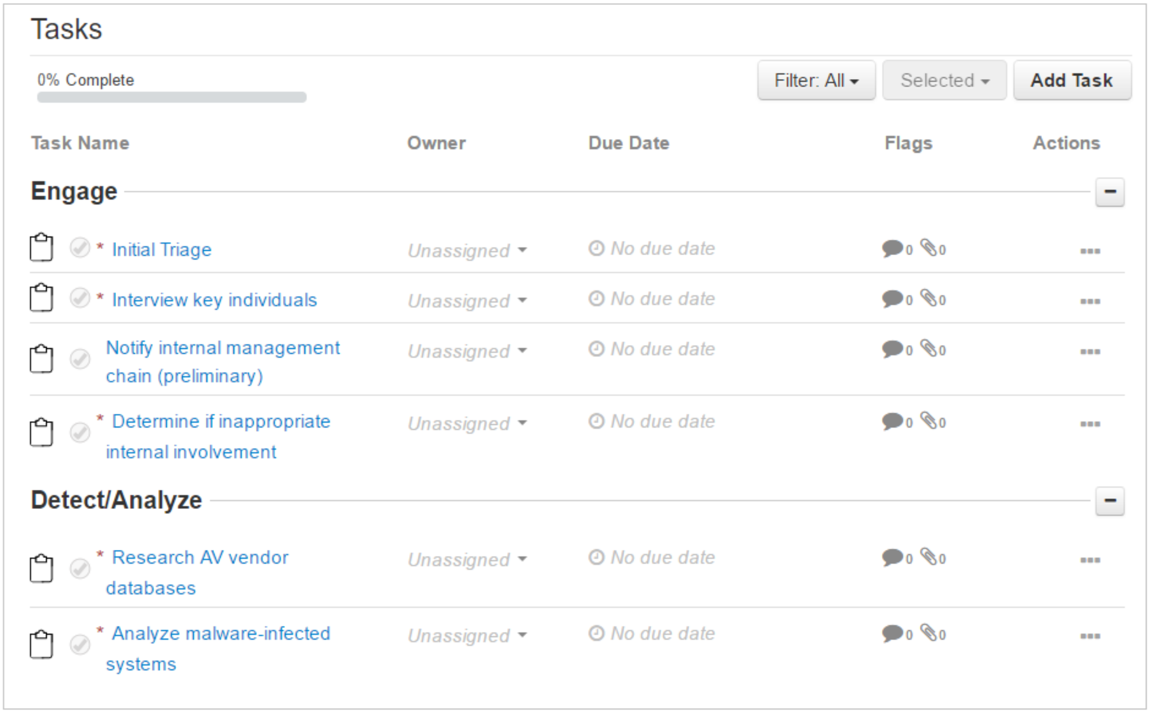
6.3. Tasks

You can access tasks as follows:

- The activity dashboard lists those tasks assigned to you that are due soon. Click a task to go to that task's page.
- Click **My Tasks** in the menu bar to see a list of all the tasks assigned to you, regardless of incident. Click a task to go to that task's page.
- Open an incident from the List Incidents page then click the **Tasks** tab to see all the tasks for that incident. Click a task to go to that task's page.

6.3.1. Tasks Tab

The **Tasks** tab in an individual incident allows you to view and manage all the tasks for the incident you selected. The tab organizes the tasks by phase, which you can expand or collapse. The following is an example of the tasks table.



Tasks

0% Complete

Task Name	Owner	Due Date	Flags	Actions
Engage				
* Initial Triage	Unassigned ▾	No due date	0 0	...
* Interview key individuals	Unassigned ▾	No due date	0 0	...
Notify internal management chain (preliminary)	Unassigned ▾	No due date	0 0	...
* Determine if inappropriate internal involvement	Unassigned ▾	No due date	0 0	...
Detect/Analyze				
* Research AV vendor databases	Unassigned ▾	No due date	0 0	...
* Analyze malware-infected systems	Unassigned ▾	No due date	0 0	...

For each task, you can access the following information, from left to right:

- Hover over the clipboard icon to see if the task is system generated or user added.
- If the circle and checkmark icon is green, the task is completed; otherwise, it is incomplete. You can click the icon to mark a task as completed.
- Hover over the task name to see its instructions.
- Owner column. Click the down arrow to select an owner, if unassigned, or reassign the task. The drop-down lists only those users or groups who are members of the incident. When you save your changes, the assignees receive a notification.
- Due Date column. Click the date to change or assign a due date.
- Flags column, notes icon. Shows the number of notes added to the task. Click the icon to open the task and view or add notes.
- Flags column, attachments icon. Shows the number of attachments added to the task. Click the icon to open the task and view or add attachments.
- Actions column. Click the **[…]** button to see the available actions for the task. Click the action to perform it.

Also in the Tasks tab, you can perform the following:

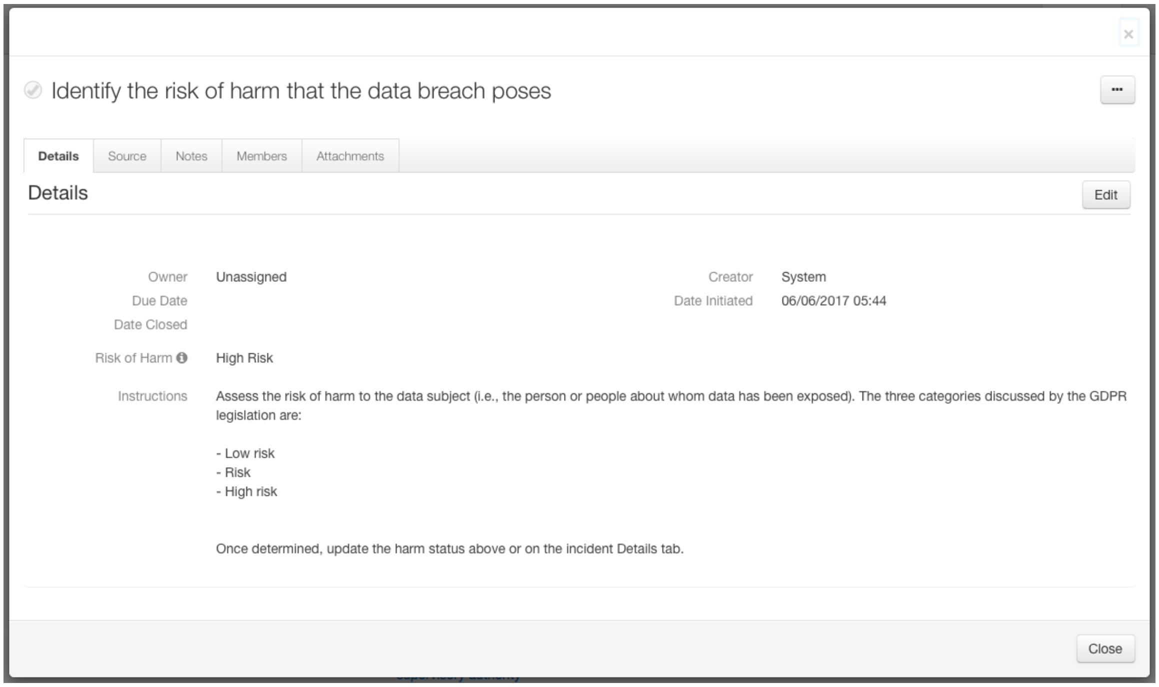
- Perform an action on multiple tasks. Select the tasks then click the **Selected** button and choose the action. To select multiple tasks, click on the clipboard icon of one task then hold the Shift or Ctrl key (Windows), or Command key (Mac) and click the clipboard icon of the other tasks.
- Create custom tasks, which are additional tasks beyond the ones generated by the playbook. Click the **Add Task** button, enter the appropriate information in the dialog and click **Create**. This adds the custom task to the playbook, where you can assign it to a user for completion.

6.3.2. Individual Task

When viewing an individual task, there are also tabs to view the source of the task, record notes, and upload attachments. In the Members tab of the task, you can mark a task as Private if you consider the task as sensitive and do not wish it to be viewed by the incident team in general. The owner of the incident and members of the task can view a private task.

You can also mark the task as completed by clicking the **Mark Task Complete** button. Marking a task complete not only informs the incident owner that the task is done, but also allows the Resilient platform to implement the next step in the dynamic playbook.

The following is an example of an individual task.



Identify the risk of harm that the data breach poses

Details

Owner: Unassigned
Due Date:
Date Closed:
Creator: System
Date Initiated: 06/06/2017 05:44

Risk of Harm: High Risk

Instructions: Assess the risk of harm to the data subject (i.e., the person or people about whom data has been exposed). The three categories discussed by the GDPR legislation are:

- Low risk
- Risk
- High risk

Once determined, update the harm status above or on the incident Details tab.

6.4. Notes

To add a note or a comment to be shared with other members of the incident team, go to the **Notes** tab (at incident or task level). Type your comment in the text box and click **Post**. This posts the note on incident team members' Activity Dashboard. With the appropriate permission, you can edit or delete notes by selecting the appropriate option on the **Notes** tab.

To direct a note to a specific incident member, place your cursor in the text box and type the "@" symbol, and a list of all the organization's users appears. Select the appropriate user(s) and continue entering the note. When complete, click **Post**; the users you selected receive a notification directing them to log in and view it.

6.5. Attachments

If the feature is available, you can upload attachments related to the incident. You can upload attachments to the incident or individual task. To attach a file, open the appropriate incident or task then select the **Attachments** tab. Click **Upload File** and select the file you wish to attach. Note the maximum file size is 25 MB. You can delete attachments from the incident or task by clicking the **Delete** button next to the appropriate file.

6.6. Timeline

The Timeline tab features a robust timeline display that can be set to display days, weeks, and months. Additionally, you can add milestones to call out important events within the timeline. To add a milestone, click the **New Milestone** button. Here you can add a date, title, and description of your milestone.

6.7. Artifacts

An artifact is data that supports or relates to the incident. The tab organizes artifacts by type, such as file name, MAC address, suspicious URL, MD5 and SHA1 file hashes, and more. An artifact can also have an attachment, such as an email, log file, and malware sample.

➢ **NOTE**: Any IPv4 addresses encoded in an IPv6 format are displayed in the IPv4 format. True IPv6 addresses are displayed in IPv6 format.

6.7.1. Artifacts Tab

The Artifacts tab lists all the artifacts added to this incident and allows you to add, edit, and perform actions on artifacts. If the list is long, you can filter by artifact type.

You add artifacts by clicking the **Add Artifact** button, selecting the type of artifact then entering information such as the type, an attachment if prompted, and a description of the artifact including how it relates to the incident. For some artifact types, you can enter multiple values; for example, email addresses. Make sure to separate multiple values by a comma, space or new line.

You can perform actions on each artifact listed in the Artifacts tab by clicking the **[…]** button. The available actions depend on the type of artifact. For example, if there is an artifact with a type of IP address artifact, you can click **[…]** and run a “Search LDAP” action in the menu to search your Active Directory for more information about the address.

➢ **NOTE**: The Details tab displays geolocation data for the ip address artifact type if your organization has enabled this feature. The Details tab displays Whois information for the DNS name artifact type when you click the **Load** button.

6.7.2. Tabular Display

The Artifacts tab allows you to display the artifacts in a tabular format or visually as a graph.

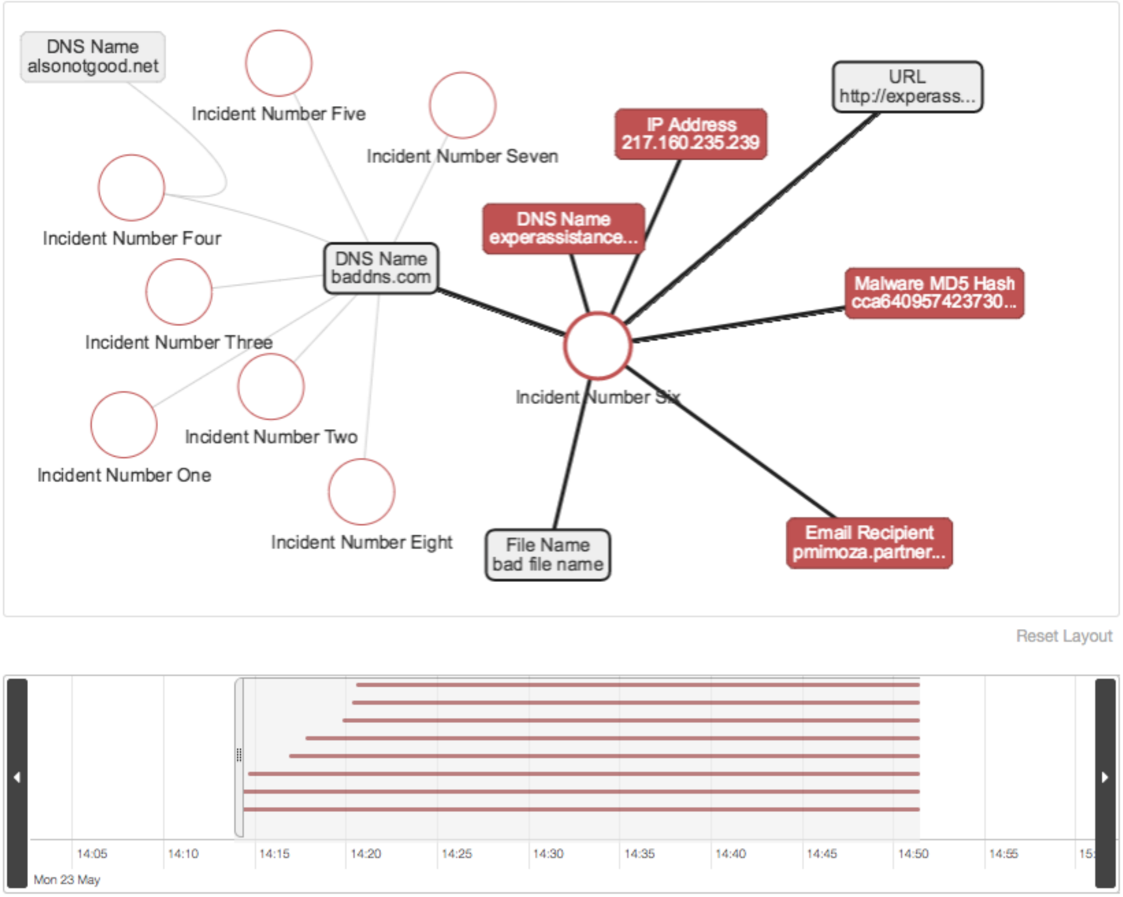
In the table, you can click on the artifact value for additional information. You access actions by clicking the **[…]** button. If the Resilient Security module is enabled for your organization, the Resilient platform examines supported file types for matches with threat intelligence feeds. If a match is found, a red exclamation point is displayed next to the artifact. You can click on these artifact matches to display further information, if available.

6.7.3. Graph Display

The graph displays the incident as a circular node with each artifact as a block attached to the node. Here are the actions you can take in the graph:

- Drag the artifacts to rearrange them so you can better show the relationship to each other.
- Hover over the incident node or the artifact to display its details and the Action button.
- If the Security module is enabled, the Resilient platform examines supported file types for matches with threat intelligence feeds. If a match is found, the artifact is highlighted in red.
- Click within the graph area then use the mouse wheel to resize the graph.
- If any artifact is also associated with another incident, the graph shows that incident as a separate circular node. You can click on each node to focus on that incident and its artifacts.
- Use the timeline at the bottom of the graph to limit the view to a specific length of time. If you have multiple incidents in the graph, a red horizontal line at the top of the timeline represents each incident. Hover over each line to display the incident name.

The following is an example of a graph with multiple incidents. One artifact is associated with eight incidents. All eight are shown in the graph as circles and as red lines in the timeline.



6.8. Actions

Your administrator and the dynamic playbook define the actions that you can perform on an incident or task.

You can select an action to take as follows:

- For multiple incidents, go to the List Incidents page and click the checkbox on the desired incidents then click the **Selected** button and choose the action to take.
- For an individual incident, click the Actions button on the incident's page.
- For a task, click the [**…**] button in a Task page.

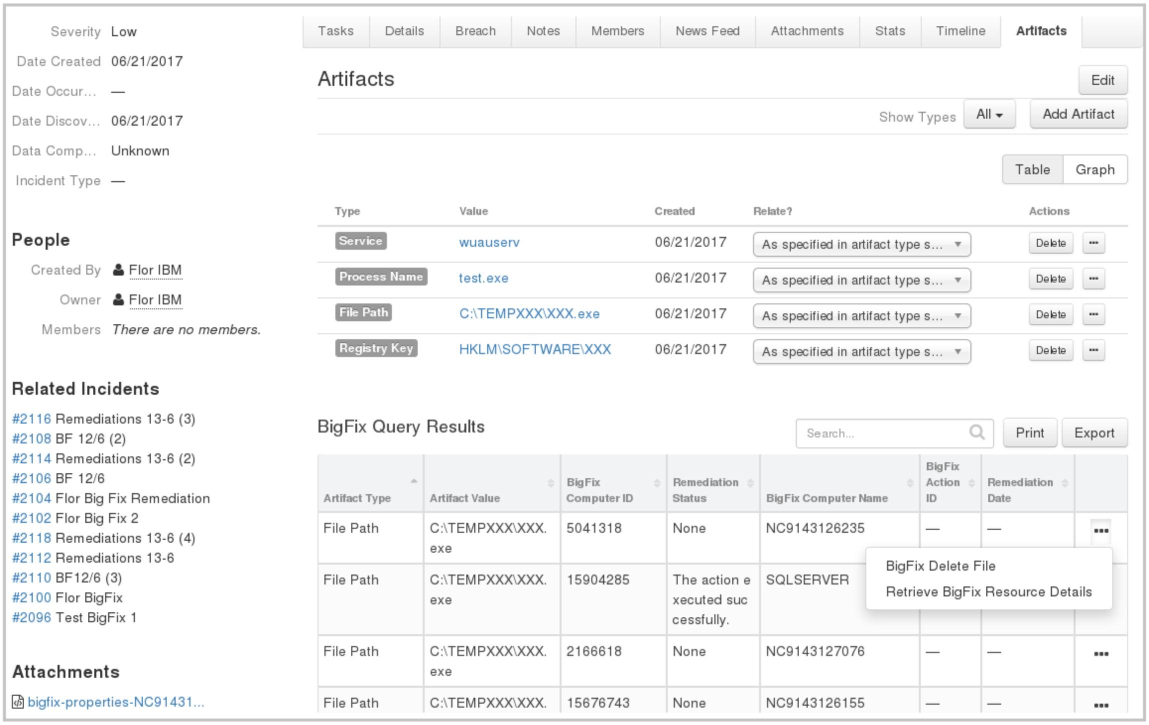
You can also select **Action Status** from the Actions button to view the status of the various actions.

6.9. Data Tables

Data tables are used to organize information in a tabular format, using rows and columns, and can be found in the various tabs of the incident. Typically, you can add information to these tables.

The Resilient platform can integrate with various Security Information and Event Management (SIEM) products so that incident information can be escalated into the Resilient platform to simplify and streamline the process of escalating and managing incidents. Depending on the level of integration, you can interact with these products directly from the Resilient platform interface. If your Resilient platform is configured with such a tool, the table may be populated with data from that tool, and you may be able to send commands to that tool.

The following example shows an integration with IBM BigFix. In the data table, you can access two actions available for the top row, BigFix Delete File and Retrieve BigFix Resource Details.



Severity	Low
Date Created	06/21/2017
Date Occur…	—
Date Discov…	06/21/2017
Data Comp…	Unknown
Incident Type	—

People

Created By	Flor IBM
Owner	Flor IBM
Members	*There are no members.*

Related Incidents

#2116 Remediations 13-6 (3)
#2108 BF 12/6 (2)
#2114 Remediations 13-6 (2)
#2106 BF 12/6
#2104 Flor Big Fix Remediation
#2102 Flor Big Fix 2
#2118 Remediations 13-6 (4)
#2112 Remediations 13-6
#2110 BF12/6 (3)
#2100 Flor BigFix
#2096 Test BigFix 1

Attachments

bigfix-properties-NC91431...

Artifacts

Type	Value	Created	Relate?	Actions
Service	wuauserv	06/21/2017	As specified in artifact type s…	Delete ···
Process Name	test.exe	06/21/2017	As specified in artifact type s…	Delete ···
File Path	C:\TEMPXXX\XXX.exe	06/21/2017	As specified in artifact type s…	Delete ···
Registry Key	HKLM\SOFTWARE\XXX	06/21/2017	As specified in artifact type s…	Delete ···

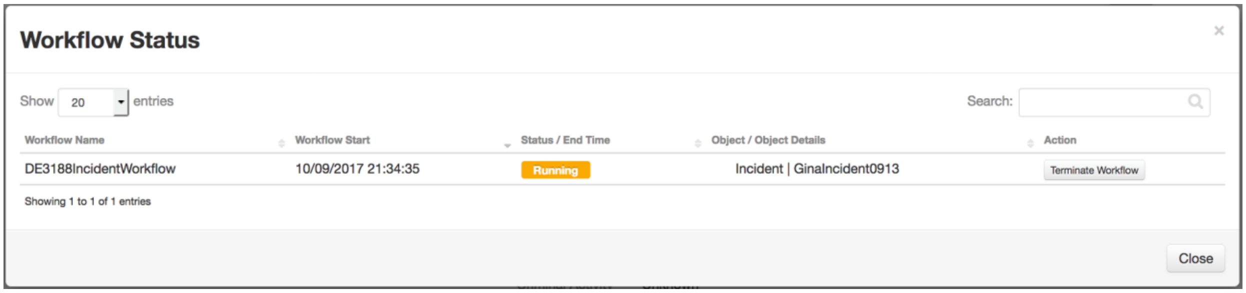
BigFix Query Results

Artifact Type	Artifact Value	BigFix Computer ID	Remediation Status	BigFix Computer Name	BigFix Action ID	Remediation Date	
File Path	C:\TEMPXXX\XXX.exe	5041318	None	NC9143126235	—	—	•••
File Path	C:\TEMPXXX\XXX.exe	15904285	The action executed successfully.	SQLSERVER			
File Path	C:\TEMPXXX\XXX.exe	2166618	None	NC9143127076	—	—	•••
File Path	C:\TEMPXXX\XXX.	15676743	None	NC9143126155	—	—	•••

6.10. Workflows

Invoked by an action, a *workflow* is a predefined set of activities that can perform a complex set of instructions. Once started, a workflow executes all its activities until it reaches its conclusion.

If you have permission, you can view the status of an incident's workflows. From within the incident page, click the **Actions** button then select **Workflow Status** near the bottom of the drop-down menu. This opens the Workflow Status window, as shown in the following example.



Workflow Status

Workflow Name	Workflow Start	Status / End Time	Object / Object Details	Action
DE3188IncidentWorkflow	10/09/2017 21:34:35	Running	Incident | GinaIncident0913	Terminate Workflow

Showing 1 to 1 of 1 entries

The status of a workflow can be Running, Completed, Suspended or Terminated.

A Suspended workflow can occur when the incident closes before the workflow completes. Reopening an incident resumes the workflow. You can permanently terminate a workflow if it is suspended and you do not plan to reopen the incident. You can also terminate a workflow if you find that it does not complete in an expected amount of time and is preventing the completion of the incident. Normally, you should not terminate a workflow in an open incident.

When terminating a workflow, you have the option to add a reason for terminating the workflow. This text displays as a popup when a user hovers over the workflow status.

Multiple objects in the same incident can invoke the same workflow, which causes multiple instances of the workflow to appear in the status table. To understand which object caused each workflow, hover over the Object/Object Details in the workflow row for additional information, such as the specific row in a data table that launched the workflow.

6.11. Managing the Incident Team

As an incident owner, you can add or remove members of an incident team. To access the incident team, open the appropriate incident, click the **Members** tab then select **Edit**. Click the drop-down menu and select the user name or group that you wish to add. The user or group appears under the list of members. To remove a team member or group, click **Remove** next to the name.

6.12. Closing an Incident

Once users complete all the tasks for an incident, you can close it. If there are any empty fields that are required to close the incident, you are prompted to enter the data. If closing multiple incidents, you are also prompted to fill in any empty, required fields. In this case, the value you enter goes to the same field in every incident, except those fields that already have data.

To close an incident, click the **Actions** button then select **Close Incident** near the bottom of the drop-down menu.

To close one or more incidents from the Incidents page, select the incidents, click the **Selected** button then click **Close Incidents**.

6.13. Deleting an Incident

If you have the permission, you can delete incidents. When you delete an incident, it is permanently deleted from the Resilient platform. Typically, you should close an incident instead of deleting it.

When you delete an incident, the incident's attachments, such as tasks and artifacts, are deleted, and all mention of the incident is removed from the news feed and system notification. Deleting an incident does not generate a system notification, but users can receive email notifications.

To delete an incident, click the **Actions** button then select **Delete Incident** near the bottom of the drop-down menu.

To delete one or more incidents from the Incidents page, select the incidents, click the **Selected** button then click **Delete Incidents**.

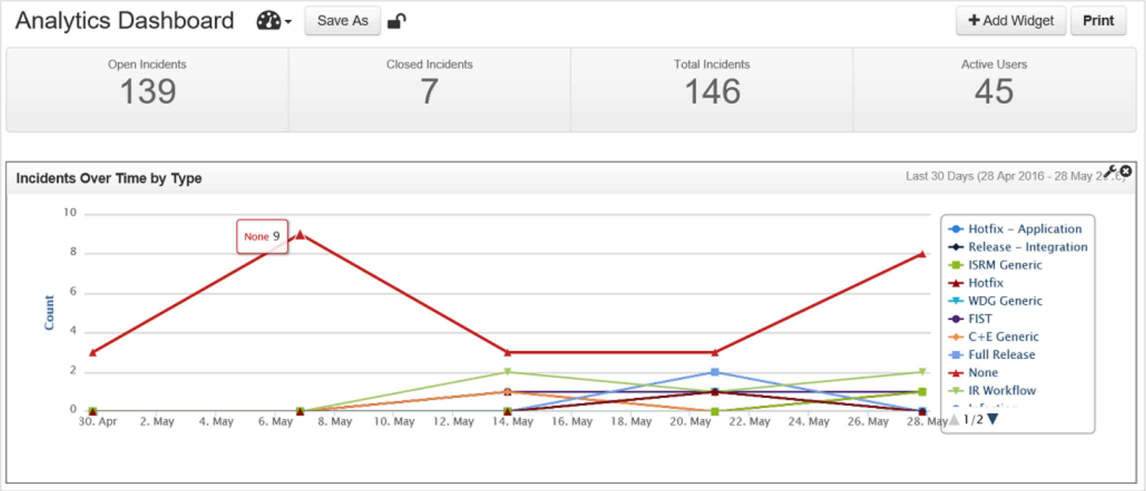
The Resilient platform logs all instances of deleted incidents.

7. Reports and Analysis

The Resilient platform allows you to view statistical information with the Analytics dashboard, and generate reports on one or more incidents.

7.1. Analytics Dashboard

The Analytics Dashboard displays various charts and graphs for viewing statistical information, dependent upon your access and permission level. The following is an example of an analytics dashboard with only one widget.



Open Incidents	Closed Incidents	Total Incidents	Active Users
139	7	146	45

When you first open the Analytics Dashboard, the default dashboard displays. There can be various, customized analytic dashboards that you can choose to display by clicking the selector icon (▾). Click **Print** to access a printable version of the dashboard.

In each table and chart, you can click on the various elements for more information. In addition, you can click on each item in the chart's legend to display or remove that item from the chart.

7.1.1. Customizing the Analytics Dashboard

The Analytics Dashboard provides a selection of predefined widgets, such as pivot tables and charts, which you can place on the dashboard.

To add a widget, click **Add Widget** in the upper right hand corner of the dashboard then drag and drop the widget to the desired location on the page.

To configure an existing widget, hover over the widget and select the wrench icon in the top right corner to expose the widget's configuration dialog. Select the configuration options, such as a date range, that you wish to implement then click **Save**. Those widgets that you cannot customize do not have the wrench icon.

To remove a widget from the dashboard, hover over the widget and select the X icon in the top right corner.

To save your changes, you can create a new analytics dashboard. Click the **Save As** button on the dashboard then enter any name you choose, a brief description and whether to share it or not. If you click **Public** as the Sharing option, other users can select and view your dashboard. To discard your changes, click the arrow next to **Save As** and click **Discard Changes**.

7.1.2. Managing Analytics Dashboards

You can edit and delete the various analytic dashboards by clicking the selector icon (⏲▾) and choosing **Manage Dashboards**. On the management page, you can also view the contact information of each dashboard owner by hovering over the owner's name.

7.2. Generating an Incident Report

You can generate a report on a single incident or multiple incidents, using a standard template or customizing the report to meet your needs.

To generate a report, perform the following:

1. Click **List Incidents** in the menu bar.
2. In the List Incidents page, select one or more incidents that you wish to have in the report by checking the checkbox next to each incident.
3. Click the **Selected** button in the upper right corner. This gives you a drop-down list.
4. Choose one of the following options:
    - **Export to Excel (All Data)**. This option generates an Excel spreadsheet with all data available for the incident, regardless of the columns shown in the List Incidents page. The system generates the report then prompts you to download the file.
    - **Export to Excel (Visible Columns)**. This option generates an Excel spreadsheet with only data shown in the columns in the List Incidents page. The system generates the report then prompts you to download the file.
    - **Generate Printable**. You have the option to select a predefined report template or select **Customize** to build your own report.
5. If you selected **Generate Printable** then clicked the **Customize** link to generate a custom report, perform the following in the Build a Report page:
    a. Select the sections that you wish to appear in the report by checking the appropriate boxes.

    b. Review the sections checked by default to determine if you wish to have them in the report.

    c. In the preview on the right side of the screen, you can choose to reorder the sections by dragging and dropping each section.

    d. Optionally, you can create a new report template based on your selections. Simply, enter a name for your template in Create Template section and click **Create**. Alternatively, you can overwrite one of your custom templates by selecting it from the drop-down in the Edit Template section, and click the **Save** button.

    e. When done, click **Print**. The system generates the report then presents a Print window.

To modify an existing template, select **Generate Printable** then click the Customize link as described previously. In the Edit Template section of the Build a Report page (lower left side), select the appropriate template from the drop-down menu and click **Load**. Modify the sections and ordering as desired then click **Save**.

➢ **NOTE**: You can also generate a report when viewing an existing incident. Click the **Generate Incident Report** button on the lower left side of the incident page. This provides the same functions as the Generate Printable option.

8. Navigation

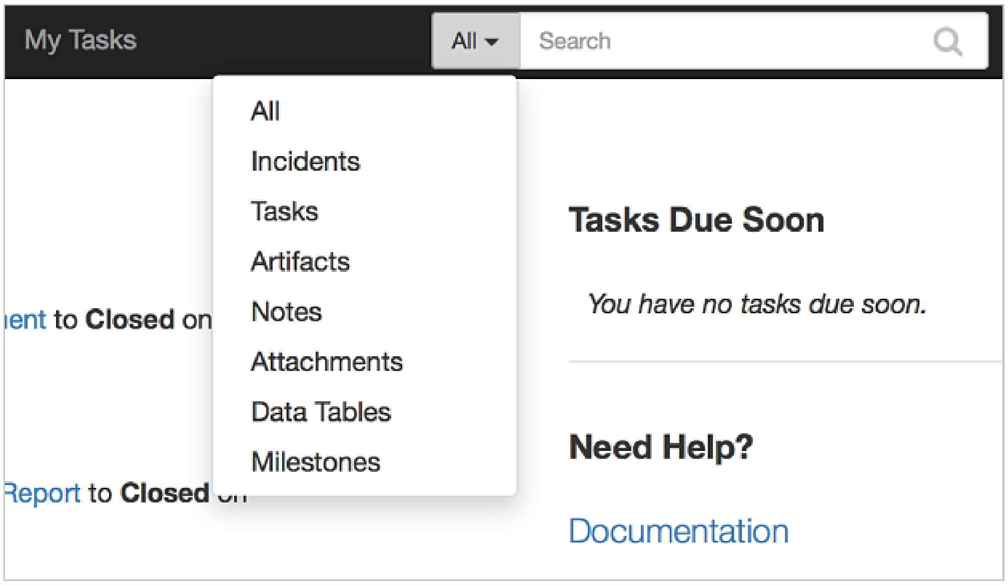
The Resilient platform provides a robust search function, as well as the ability to filter the information on the various pages.

The Search function in the Resilient toolbar, which appears on every page, allows you to search for a keyword or phrase in any or all object types. The Search function supports the following:

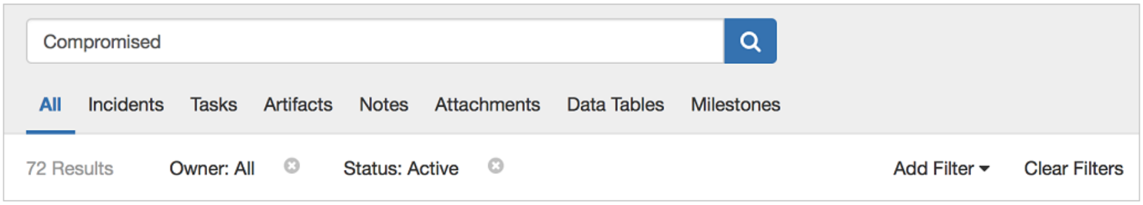
- Wildcards (*), which you can use in any location in your entry.
- Tilde (~) at the end of your entry performs an approximate search, also called a fuzzy search, which returns strings matching your entry exactly, with one character extra, and with one character different from your entry.
- Phrases when enclosed in quotes.

The Search function is not case sensitive.

By default, the function searches for your entry in every object type. The example screenshot below shows the default, **All**. To narrow your search to a specific object type, click the arrow and select the type.

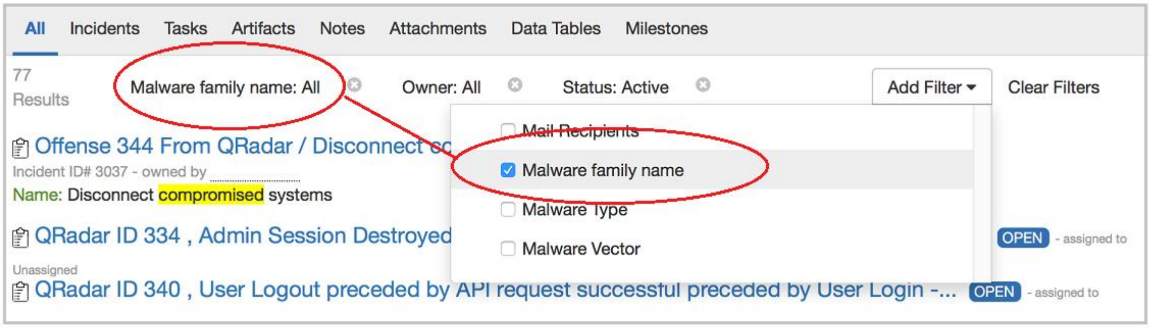


Alternately, on the Search results page, you can use the tabs to filter by object type.



On the Search results page, each result starts with an icon that represents the object type. Hover over the icon to see a definition of the object type.

The Search results page allows you to add filters that can further narrow your results. The previous screenshot shows the default filters, Owner (set to All) and Status (set to Active). To add filters, click **Add Filter** then select the filters you wish to use. As you click the checkbox next to a filter, it appears with the other filters. The following example shows Malware family name selected.



All Incidents Tasks Artifacts Notes Attachments Data Tables Milestones

77 Results

Malware family name: All ⊗ Owner: All ⊗ Status: Active ⊗ Add Filter ▾ Clear Filters

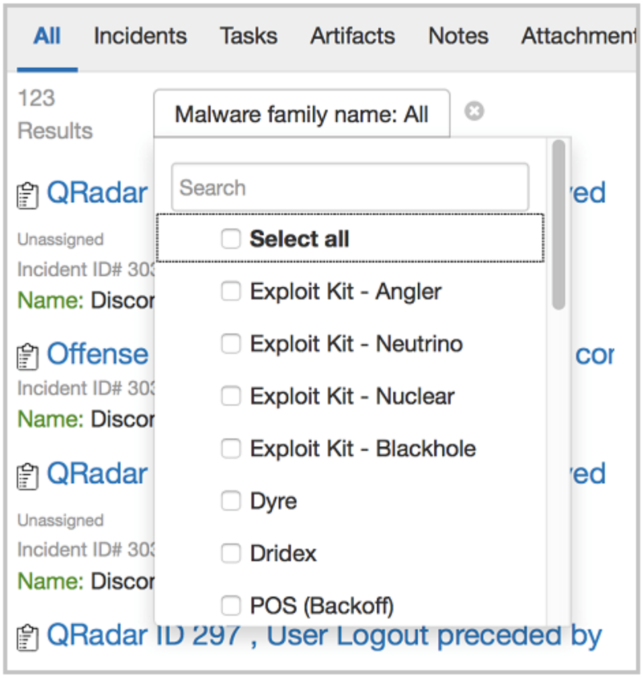
□ Mail Recipients
☑ Malware family name
□ Malware Type
□ Malware Vector

Offense 344 From QRadar / Disconnect co
Incident ID# 3037 - owned by
Name: Disconnect compromised systems

QRadar ID 334 , Admin Session Destroyed
Unassigned
OPEN - assigned to

QRadar ID 340 , User Logout preceded by API request successful preceded by User Login -... OPEN - assigned to

You can then click on the filter and choose or enter a value, depending on the filter.



All Incidents Tasks Artifacts Notes Attachment

123 Results

Malware family name: All ⊗

Search

□ **Select all**
□ Exploit Kit - Angler
□ Exploit Kit - Neutrino
□ Exploit Kit - Nuclear
□ Exploit Kit - Blackhole
□ Dyre
□ Dridex
□ POS (Backoff)

QRadar ... ed
Unassigned
Incident ID# 303
Name: Discor

Offense ... cor
Incident ID# 303
Name: Discor

QRadar ... ed
Unassigned
Incident ID# 303
Name: Discor

QRadar ID 297 , User Logout preceded by

To remove a filter, click the **x**. To remove all filters, click **Clear Filters**.

You can use the Search field within the results page to perform a new search while preserving your previous search results. Simply use the browser's back button to return to your previous search.