Resilient Incident Response Platform

USER GUIDE v26

Published: June 2016

https://www.resilientsystems.com

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 Resilient users with an introduction to the system's user interface and workflow for entering and managing incidents, and the tasks associated with an incident management plan.

The Resilient Incident Response Platform is comprised of a Privacy Module and a Security IR Module. Access to certain areas of the product is dependent upon your organization's subscription.

1.1. Supported Browsers

The Resilient user interface is a single-page JavaScript application. As such, it relies on certain functionality of the web browser to provide a rich and clean user experience. In order to enjoy the optimal experience you should use a modern supported web browser. Supported web browsers include the current release and one release back of each of the following browsers: Chrome, Firefox, Safari and Internet Explorer.

2. Dashboards

There are two dashboard views available to each user, the Activity Analytics Dashboard. Click the **Dashboard** tab, and then select the desired view.

2.1. Activity Dashboard

The Activity Dashboard is the default page when you log in.

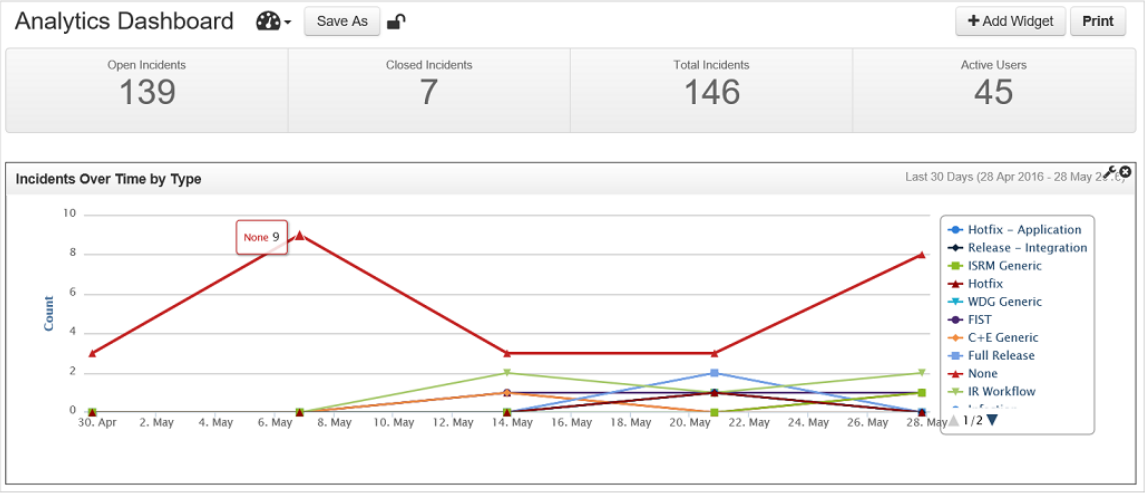
It contains the following:

- **Newsfeed**: Provides up-to-the-minute activity updates for all incidents for which you are a member. To view only specific actions in the newsfeed, click the **Show Types** drop-down menu.
- **Tasks Due Soon**: Displays tasks assigned to you that are due within the next 7 days.

This page also has links to documentation and the Resource Library (click for more information).

2.2. 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.



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.

2.2.1. 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 and configure a widget, perform the following:

1. Click **Add Widget** in the upper right hand corner of the dashboard to add the widget to the dashboard immediately.
2. Drag and drop the widget to the desired location on the page.
3. To configure a 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**.

   NOTE: 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**.

2.2.2. 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 email address of each dashboard owner by hovering over the owner's name.

3. Understanding Incidents

Resilient users can create incidents. Systems integrated with the Resilient platform can also create incidents within the platform. The Incidents list page, which is accessible by clicking **List Incidents** in the menu bar, displays all incidents.

Each incident can contain significant information. The Resilient platform organizes this information into various tabs. By default, the tabs include Tasks, Details Breach, Attachments, Artifacts and more. However, your administrator can add or hide tabs and customize each tab. Some tabs may be conditional and appear only under one or more given conditions.

The following lists the actions you can take on incidents:

- Create an incident.
- Generate reports on one or more incidents.
- Check the status of the incident.
- Close an incident.
- As an incident owner, you can edit incident information and the response plan.
- Others custom actions configured by your administrator. These actions are accessible through the **Action** button in the incident page (across all tabs), or a […] button near an object, such as a task.

When viewing incidents, you can filter the list based on various combinations of field settings. Click the **More** button to select the fields that you wish to include in the filtering criteria. To save selected filter settings for future use, click **Filters** then **Save As** then assign a name to the filter set. To re-use a saved filter, click **Filters** then select the named filter that you wish to use.

➢ **NOTE**: Many of the text fields allow you to add formatting options using industry-standard toolbars.

4. Creating an Incident

To report a new incident, click **New Incident** in the menu bar. This starts the 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.

If you select Yes to indicate that Personally Identifiable Information (PII) has been compromised, additional data fields become enabled and additional detail will be required in order for the system to properly assess the incident and generate an appropriate response plan.

If you enable HIPAA as a Regulator and you indicate that personal information is involved in the incident, there is an additional step in the wizard. This step is a Risk Assessment based on the HIPAA requirements where covered entities (and business associates, where applicable) assess the probability that a breach has occurred and maintain documentation of that assessment.

5. Generating an Incident Report

You can generate a report on a single incident or multiple incidents, using a standard temple 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.
3. Click the **Reports** button in the upper left 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 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 that are 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 dropdown 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, click the Customize link as described previously. In the Edit Template section of the Build a Report page, 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.

6. Managing Incidents

You can manage incidents by assigning and completing tasks, creating custom tasks, adding or updating incident information, adding attachments and artifacts, and selecting a predefined action.

The **Action** button in the incident page (accessible regardless of the selected tab) applies to the incident. You can also take actions on individual tasks.

To change the details of an incident, visit either the **Details** or **Breach** tab of the incident, depending on what information needs to be modified.

- **NOTE**: If you change a "No" answer to "Yes" regarding the exposure of Personally Identifiable Information, additional tasks are added to the incident response plan. You should visit the **Breach** tab to enter additional required information.
- **NOTE**: If you change from "Unknown" to "Yes", you can update the details from within the task that instructs you to investigate if data has been compromised.

Once all tasks are completed for an incident, you can close it by clicking the **Close Incident** button.

Depending on the conditions configured by the Master Administrator, there may be a number of tabs for the incident. The following sections describe the standard tabs, which may or may not be visible for the incident.

- **NOTE**: Many of the text fields allow you to add formatting options using industry-standard toolbars.

6.1. Tasks

The **Tasks** tab allows you to view all tasks for incidents of which you are a member. Click on a task name to view its details. When viewing a task, there are also tabs to view the source of the task, record notes, and upload attachments (if this feature is enabled for your organization). Only the incident owner and administrators can perform specific features, such as editing tasks.

The tab organizes the tasks by phase, which you can expand or collapse. Hover over the task icon to see various properties, such as system-generated or user-added. You can also hover over the task name to see its instructions. A green check mark means the task is complete.

To assign a task, click the drop-down in the Owner column and select a user name. The drop-down lists only those users or groups who are members of the incident. When you save your changes, the assignees receive an email notification.

To change or assign a due date, click the date under Due Date column.

You can perform the same action, such as setting a due date, for multiple tasks. Select the tasks then click the **Selected** button and choose the action.

You can create custom tasks, which are additional tasks beyond the ones generated by the application, by clicking the **Add Task** button. Enter the appropriate information in the dialog and click **Create**. This creates the custom task and adds it to the existing incident response plan, where you can assign it to a user for completion. The Master Administrator can also create automatic tasks to be applied to all incident response plans, as described in the "Phases & Tasks" section of the Master Administrator Guide.

If you consider that a task is sensitive and should not be viewed by the incident team in general, you can mark the task as Private. To perform this operation, you must be an administrator, incident owner, or task owner.

You mark a task as completed by clicking the circle and checkmark icon. When green, the task is completed. If you opened an individual task, click the **Mark Task Completed** button.

6.2. Breach

If the incident involves 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 tool tip 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.

6.3. 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) and click **Add a Note**. Type your comment in the text box and click **Post**. This posts the note on incident team members' Activity Dashboard. Notes can be edited or deleted by Administrators, Incident Owners, or Incident Creators 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.

6.4. Incident Members

To add or remove members of an incident team, open the appropriate incident and click the **Members** tab then select **Edit**. Click the dropdown menu and select the user name or group that you wish to add then click **Add**. The user or group appears on the right under **Current Members** once they have been successfully added. To remove a team member or group, click **Remove** next to their name.

6.5. Attachments

The Resilient platform supports the uploading of attachments related to the incident. This feature must be enabled by the master administrator for your organization. Attachments may be added at the incident or the individual task level. 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, milestones can be added 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. You can find the Timeline tab in any open incident.

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.

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.

You can perform actions on each artifact. The available actions depend on the type of artifact; for example, you can select an IP address artifact then use the Search LDAP action 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.

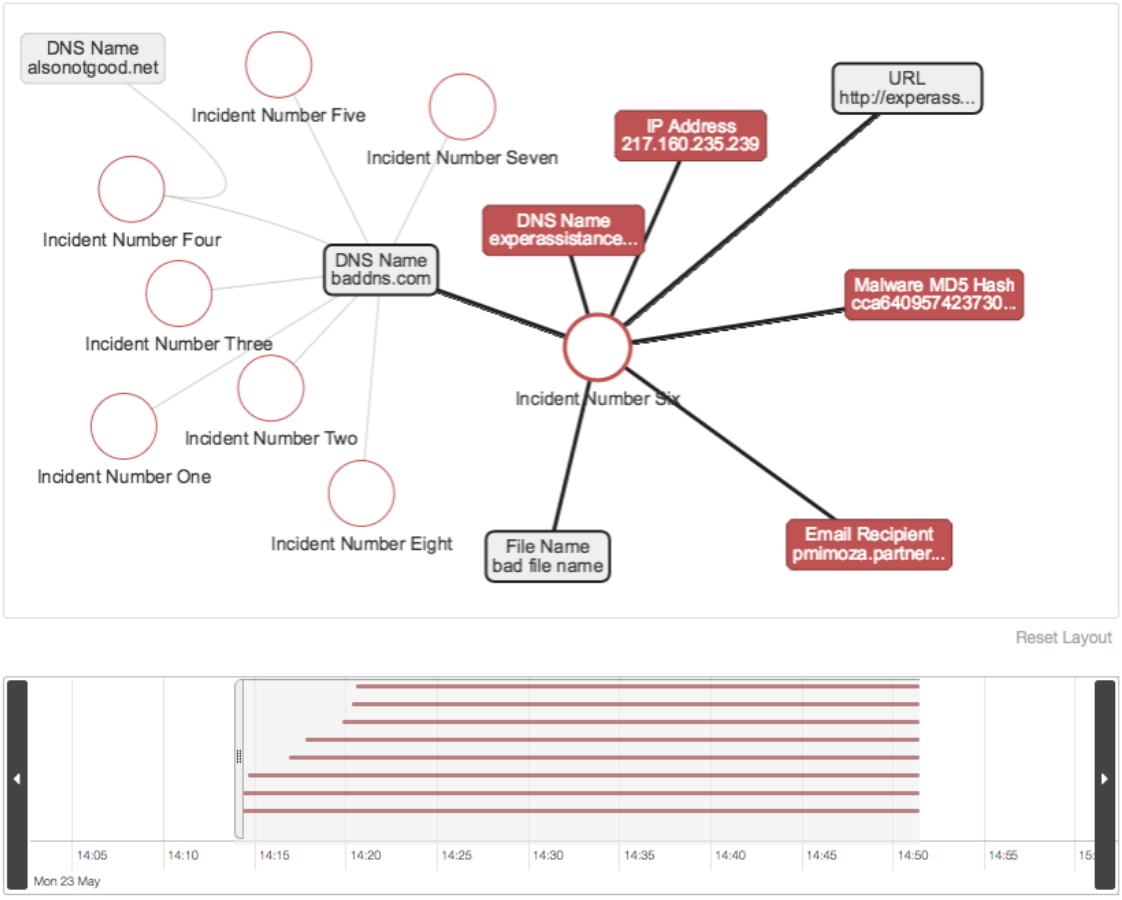
The Artifacts tab allows you to display the artifacts in a tabular format or visually as a graph.

In the table, you can click on the artifact value for additional information. You access actions by clicking the **[…]** button. If the Security module is enabled, 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.

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.



7. Simulations – Simulated Scenarios and Risk Assessments

Administrators have the ability to run simulations, which are hypothetical circumstances that can help your team to understand the impact of data loss situations and to rehearse the response process. There are two types of activities available on the **Simulations** tab:

- Simulated Scenarios – Full functionality incident creation, marked in the tool as a simulated situation rather than an actual occurrence.
- Simulated Risk Assessments - Unrecorded, unlogged assessments based on limited situation parameters for data breaches involving PII.

To run a simulated scenario, click the **More** tab and select **Simulations**. Click **Start New Scenario** and complete the incident entry wizard. To close an active simulated incident, click the **Close Incident** button within the appropriate incident. Simulated scenarios are distinguished within the system by a special icon; however, the process of working with simulated items is identical to working with a real situation that your organization tracks using the Resilient platform.

Simulated risk assessments allow you to test the implications of a data breach situation without keeping it in your organization's record. The wizard collects basic information about a hypothetical data breach event, and ends with an assessment that includes a summary of the recommended steps to be taken as well as the estimated fine liability.

8. Other Tools

8.1. Documentation and Support

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 on the Activity Dashboard.

8.2. Resource Library

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.

To access the Library, click on your user name in the upper right hand corner of the page, and select **Library** from the dropdown 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.

8.3. My Settings

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

- 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

  This feature allows you to update your personal preferences for receiving notifications about various actions that occur in the system. For each action listed, select the radio button next to the method of preferred notification, either through email or through the small globe icon in the Resilient UI, or both. Hover over the small "I" icon for a brief explanation of each action.

- Change Password

  You can change your Resilient password by entering your current password, your new password, and then clicking **Change Password**.

8.4. Notifications

Notifications show activity that specifically involves you, such as tasks or incidents being assigned to you. There is an alert icon for notifications on the tool bar at the top of the page, to the left of your username, which displays the number of your notifications. Click on the icon to review notifications. Some notifications send an email to your address

Notification options can be customized by accessing the Notifications section under My Settings. My Settings is available by clicking your username. For each alert, you can choose whether to be notified via email, in-product notifications, or neither. Note that notifications are suppressed for actions that you instigate; for example, you do not receive Task Closed notifications for tasks that you close.

8.5. Search

The product contains a search functionality that spans open and closed incidents, tasks, and comments. Enter a word or phrase into the **Search** field on the toolbar and click **Enter**. You can filter search results by making an additional selection on the left side of the search results page.