



# **Security Incident Response Module**

## **Step-by-Step Tutorial**

Document Version: 01.00.02 | December 2018

Rsam © 2018. All rights reserved

[Privacy Policy](#) | [Terms of Service](#)

# Contents

About Rsam Tutorials .....	3
Rsam Sandbox Environment .....	4
Sign-In Page.....	4
Rsam Security Incident Response .....	5
Overview .....	5
Security Incident Response Workflows .....	5
Event Workflow .....	6
Incident Workflow.....	7
User Accounts .....	8
High-Level Steps .....	9
Step-by-Step Configuration .....	10
Step 1: Creating an Event .....	10
Step 2: Reviewing the Event .....	12
Step 3: Creating a Task .....	13
Step 4: Creating a Playbook Rule.....	14
Step 5: Responding to an Incident Escalated from the Event .....	17
Step 6: Working with Tasks.....	21
Step 7: Investigating the Incident .....	23
Appendix 1: Email Notifications and Offline Decision Making .....	25
Setting up Email Addresses .....	25
Offline Decision Making .....	26
Appendix 2: Rsam Documentation .....	27
SIRP Module Baseline Configuration Guide .....	27
Online Help .....	27

## About Rsam Tutorials

---

The Rsam module step-by-step tutorials are designed to help you learn about a specific Rsam module and to gain basic familiarity with the user interface. The Rsam platform is highly configurable and is capable of handling both simple and comprehensive applications. The step-by-step tutorials and Rsam sandboxes, however, are specifically designed to quickly deliver a user experience without requiring further training. Each step-by-step tutorial walks you through common, out-of-the-box functionality within a given Rsam module, allowing you to get immediate hands-on familiarity with the module.

# Rsam Sandbox Environment

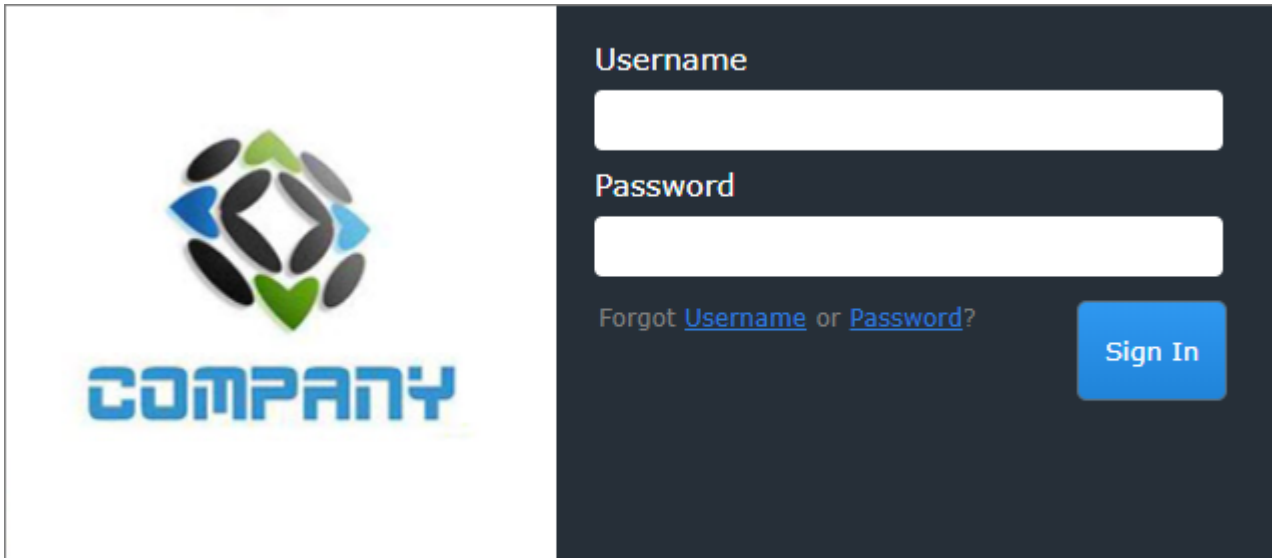
---

Rsam module step-by-step tutorials are designed to work with the out-of-the-box Rsam configuration. You may follow this tutorial using an Rsam Sandbox environment or using your own instance of Rsam that you already own. If you are using this tutorial with an Rsam Sandbox environment, the URL to access your Rsam sandbox is delivered through an email. Otherwise, you may contact your Rsam Administrator for the URL to access your Rsam instance.

If you are using an Rsam sandbox environment, you should have provided Rsam with your organization's internet facing IP address. To find this information, open a browser and connect to an IP discovery site such as [www.whatismyip.com](http://www.whatismyip.com), or contact your organization's Network Administrator for assistance. You may also contact your Rsam Customer Representative with any questions.

## Sign-In Page

Tutorials leverage pre-defined accounts that require manual authentication. While your organization may intend to use SSO authentication, Rsam sandbox environments require manual authentication through the Rsam Sign-In page so that you can easily toggle between various sample accounts used throughout the tutorial.



Like most elements in Rsam, the Sign-In page can be configured in a number of ways. Different authentication options such as user self-registration, integration with customer user directories (such as Active Directory), or integration with Single Sign-On products, such as Shibboleth, can be applied. You can also embed your own branding and logo on the Sign-In page.

# Rsam Security Incident Response

## Overview

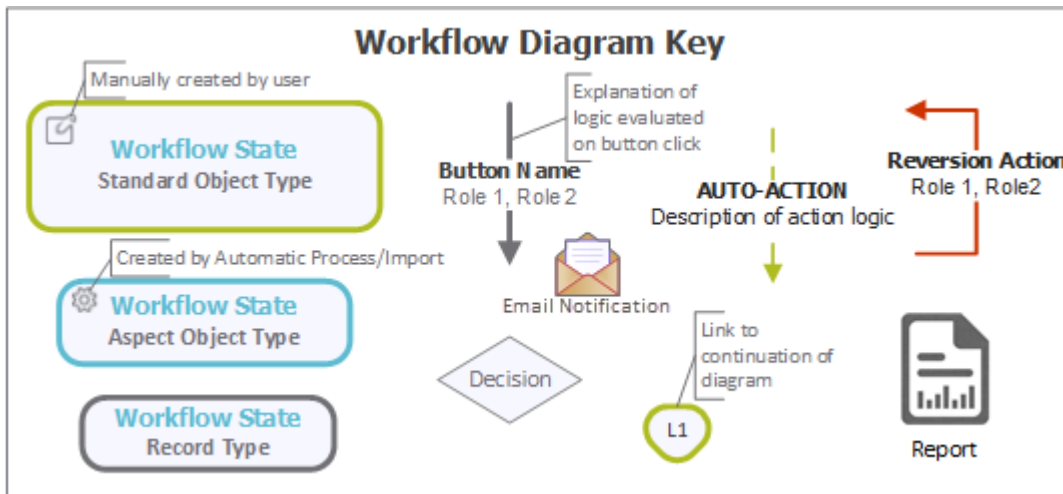
The Rsam Security Incident Response (SIRP) module allows you to manage events reported in your organization. With this module, you review the events and escalate only those events to incidents that impact your organization. The events escalated to incidents are managed and closed using the playbook rules and tasks.

## Security Incident Response Workflows

This section covers the following diagrams that illustrate the workflows in the Security Incident Response module:

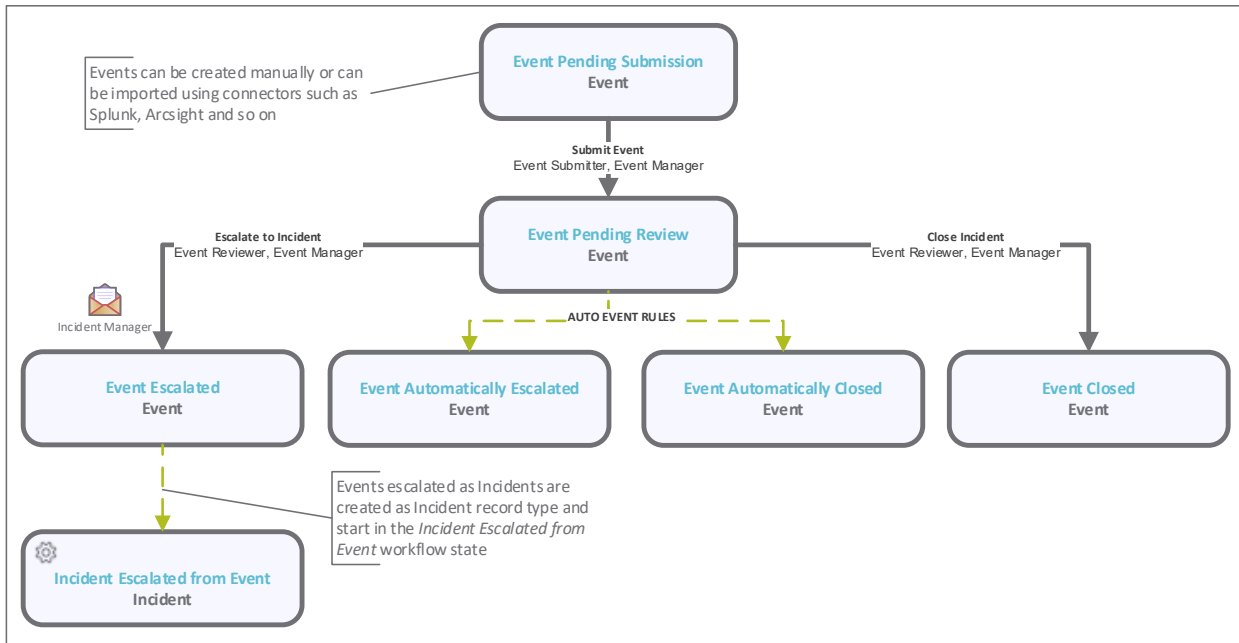
- Event
- Incident
- Task

Before proceeding to the specific workflows, it is recommended that you familiarize yourself with the following Rsam workflow diagram key.



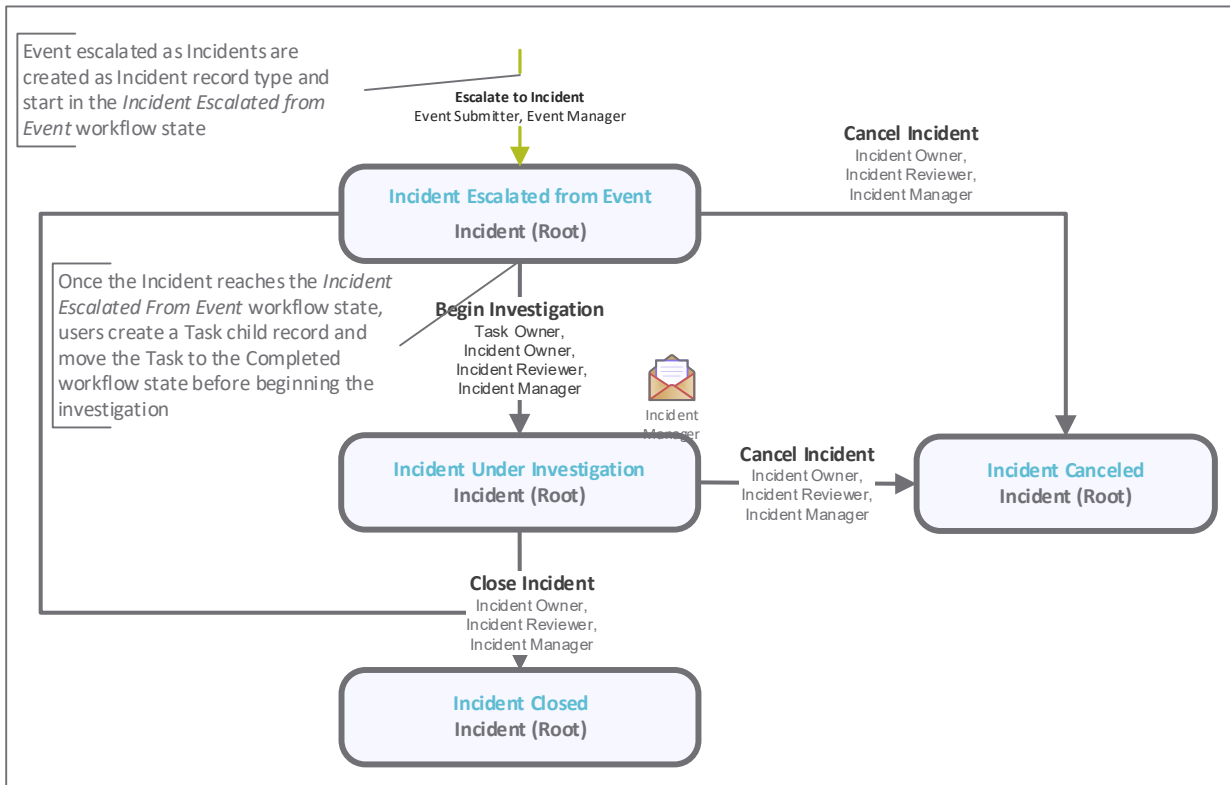
## Event Workflow

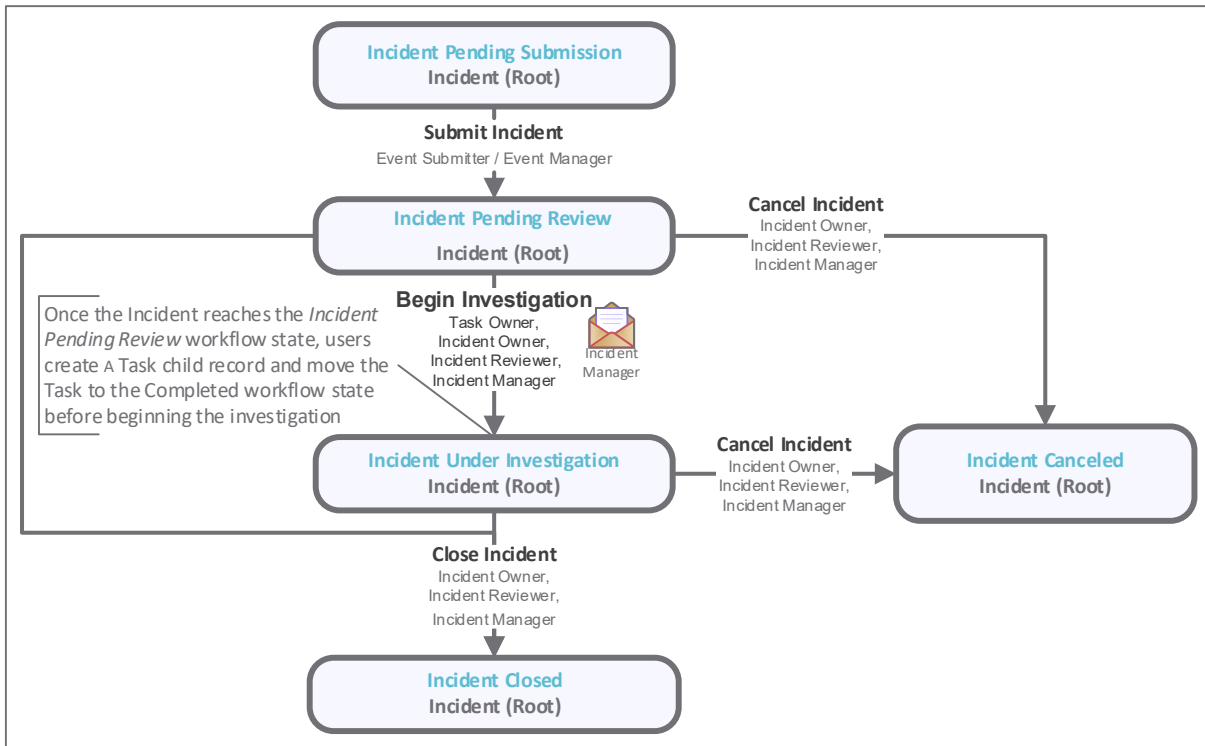
The following diagram depicts the out-of-the-box Event workflow.



## Incident Workflow

The following diagrams depict the out-of-the-box Incident workflow.





**Notes:**

- This tutorial explains the workflow starting in the Incident Escalated from Event state.
- You may create as many variations to this pre-defined workflow configuration as desired to lessen or increase the number of steps and to match your specific business processes.

## User Accounts

User accounts are required for the individuals that are authorized to access a specific Rsam module. The Rsam sandbox for Security Incident Response module comes with pre-populated sample accounts that include the user accounts mentioned in the following table.

**Note:** Sample users for each of these roles are optionally provided with the baseline module installation package.

Account ID	User	Business Responsibilities
<b>r_sirp_event_manager</b>	SIRP Event Manager	This user is responsible for overall administration of events, therefore, has the ability to create, submit, edit, and delete events. In addition, this user can manage event escalation rules.
<b>r_sirp_event_reviewer</b>	SIRP Event Reviewer	This user is responsible for reviewing events. The events are either escalated to incidents or closed directly.



Account ID	User	Business Responsibilities
<b>r_sirp_incident_manager</b>	SIRP Incident Manager	This user is responsible for creating tasks and playbook rules. Before submitting incidents for investigation, the SIRP Incident Manager user builds the task list.
<b>r_sirp_incident_reviewer</b>	SIRP Incident Reviewer	This user is responsible for investigating incidents.
<b>r_sirp_task_owner</b>	SIRP Task Owner	This user has the ability to work on the tasks associated with incidents. However, this user has read-only permission on incidents that includes tasks for which they are the owners.

The default password for all accounts in the Rsam Security Incident Response sandbox is *password*. Individual users may change their password once authenticated. Users with administrator permissions may also reset the password of other users.

## High-Level Steps

The following is a high-level list of the steps described in this tutorial.

Step	User	Description
<b>Step 1: Creating an Event</b>	SIRP Event Manager	In this step, the <i>SIRP Event Manager</i> creates an event.
<b>Step 2: Reviewing the Event</b>	SIRP Event Reviewer	In this step, the <i>SIRP Event Reviewer</i> reviews the event and escalates the event to incident.
<b>Step 3: Creating a Task</b>	SIRP Incident Manager	In this step, the <i>SIRP Incident Manager</i> creates a task.
<b>Step 4: Creating a Playbook Rule</b>	SIRP Incident Manager	In this step, the <i>SIRP Incident Manager</i> creates a playbook rule and assigns the task to the playbook rule.
<b>Step 5: Responding to an Incident Escalated from the Event</b>	SIRP Incident Manager	In this step, the <i>SIRP Incident Manager</i> builds the task and submits the incident to the SIRP Incident Reviewer user for investigation.
<b>Step 6: Working with Tasks</b>	SIRP Task Owner	In this step, the <i>SIRP Task Owner</i> works on the tasks associated with the incident.
<b>Step 7: Investigating the Incident</b>	SIRP Incident Reviewer	In this step, the <i>SIRP Incident Reviewer</i> works on all the tasks associated with the incident, then closes all the tasks, and then finally closes the incident.

# Step-by-Step Configuration

This section contains the workflow steps we will follow in this tutorial. The path covered in this tutorial will walk you through the steps to create an event, escalate the event to incident, create a task and playbook rule, respond to the incident, and investigate the incident. This path was chosen as it is a common path to follow, though you are welcome to explore other paths as well.

From this point forward, we will provide the steps that are required to complete this tutorial. Before you begin to practice each step, consider the following underlying capabilities:

- a. Practicing each step requires a different user account as mentioned in the [High-Level Steps](#) section. However, you may execute all the steps with the *SIRP Incident Manager* credentials in one session if desired.
- b. Workflow state transitions involve sending email notifications to users in the workflow. If you want to ensure that your workflow users receive the notifications while practicing the steps, please see the [Setting up Email Addresses](#) section of the Appendix A, later in this tutorial.

## Step 1: Creating an Event

In this step, you will log in to Rsam as the *SIRP Event Manager* to create an event manually.

**Note:** Instead of creating events manually, you can also import events from 3rd party Security Information and Event Management (SIEM) software products, such as Splunk, ArcSight and QRadar.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Security Incident Response module.
2. Sign in as the *SIRP Event Manager* user. Enter **Username** as *r\_sirp\_event\_manager* and **Password** as *password*.
3. From within the navigation panel at the left-hand side, navigate to **Security Incident Response > SIRP Management Team Home**.



The SIRP Management Team Home page appears.

- Under **Self Registration**, click **Submit a new Event record**.



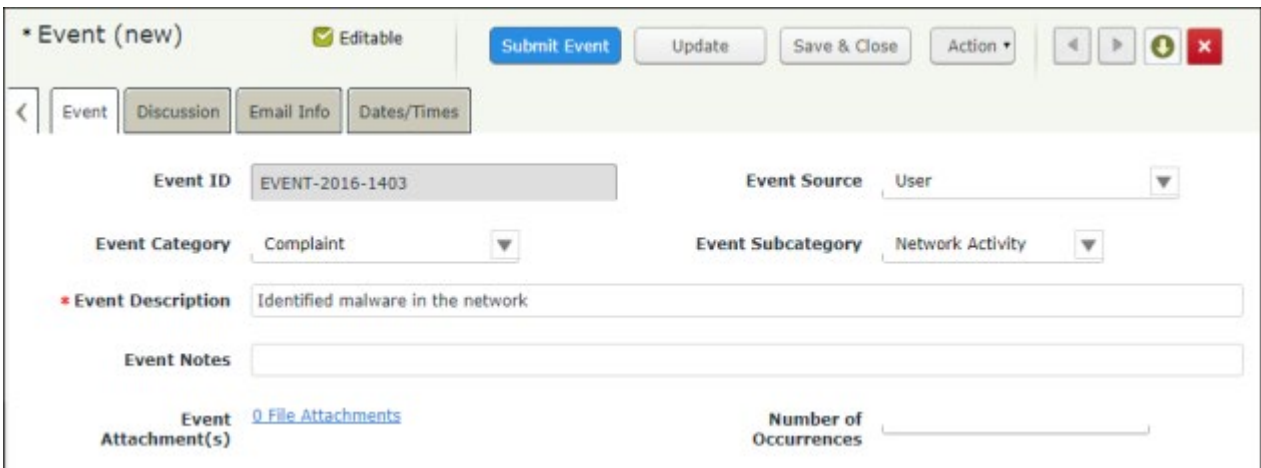
The page displaying the event category types appears.

- In the **Information** column of the **SIRP Event Library** category, click **Select**.

Select from the list below				
Name	Type	Entity	State	Category
SIRP Event Library	SOAR Data	Rsam Libraries	N/A	<a href="#">Select</a>
SIRP Incident Library	SOAR Data	Rsam Libraries	N/A	<a href="#">Select</a>
TVM Data	SOAR Data	Threat and Vulnerability Management	N/A	<a href="#">Select</a>

The **Event (new)** record opens with the **Event** tab selected.

- Complete the **Event Source**, **Event Category**, **Event Subcategory**, **Event Description** attributes, and any other attributes that are necessary to your business requirement.

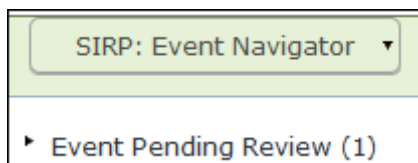


- Click **Submit Event**.
- Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.  
You have been successfully logged out from the Rsam Security Incident Response module.

## Step 2: Reviewing the Event

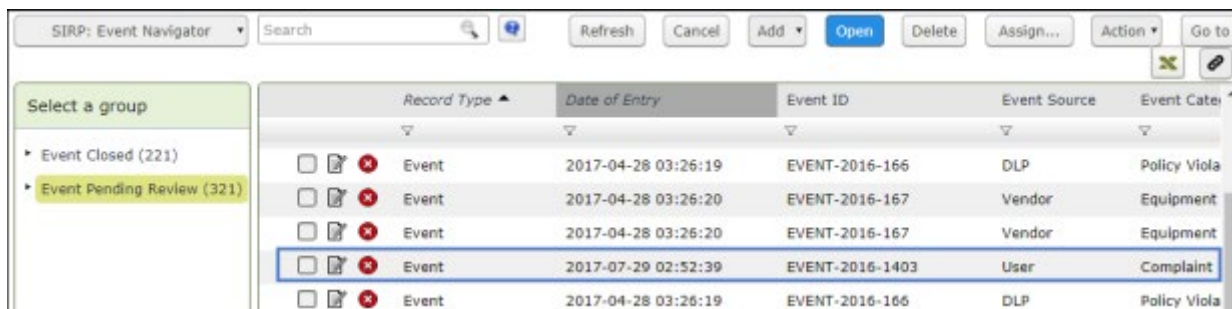
In this step, you will log in to Rsam as the *SIRP Event Reviewer* to review the event and escalate the event as incident.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Security Incident Response module.
2. Sign in as the *SIRP Event Reviewer* user. Enter **Username** as *r\_sirp\_event\_reviewer* and **Password** as *password*.
3. From within the navigation panel at the left-hand side, navigate to **Security Incident Response > Events Navigator**.  
The **Event Navigator** home page appears.
4. With **SIRP: Event Navigator** selected, click **Event Pending Review**.



The events in the **Event Pending Review** state appear.

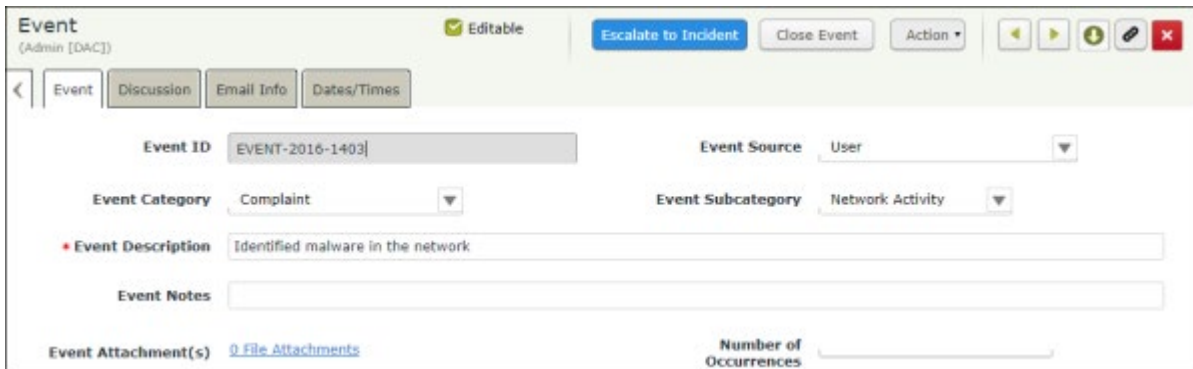
5. Locate the event record.
6. Double-click the event record.



Record Type	Date of Entry	Event ID	Event Source	Event Category
Event	2017-04-28 03:26:19	EVENT-2016-166	DLP	Policy Viola
Event	2017-04-28 03:26:20	EVENT-2016-167	Vendor	Equipment
Event	2017-04-28 03:26:20	EVENT-2016-167	Vendor	Equipment
Event	2017-07-29 02:52:39	EVENT-2016-1403	User	Complaint
Event	2017-04-28 03:26:19	EVENT-2016-166	DLP	Policy Viola

The **Event** record opens with the **Event** tab selected.

7. Click **Escalate to Incident**.



8. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.  
You have been successfully logged out from the Rsam Security Incident Response module.

## Step 3: Creating a Task

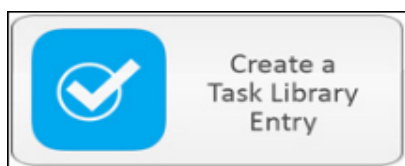
In this step, you will log in to Rsam as the *SIRP Incident Manager* to create a task.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Security Incident Response module.
2. Sign in as the *SIRP Incident Manager*. Enter **Username** as *r\_sirp\_incident\_manager* and **Password** as *password*.
3. From within the navigation panel at the left-hand side, navigate to **Security Incident Response > Task Library Management**.



The **Task Library** home page appears.

4. Click the **Create a Task Library Entry** image.



The **Library Task (new)** record opens with the **Library Task (new)** tab selected.

- Complete the **Task Order**, **Task Type**, and **Task Name** attributes, and set the **Task Assigned To** attribute to *r\_sirp\_task\_owner*. You may also complete other attributes, as necessary.



- Click **Save & Close**.  
A new task is created.

## Step 4: Creating a Playbook Rule

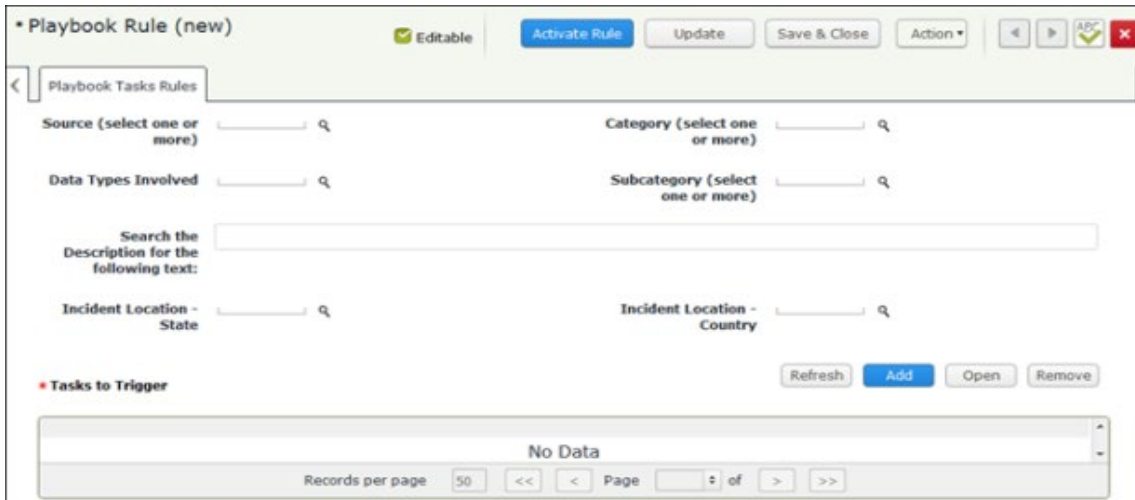
In this step, by staying signed in to Rsam as the *SIRP Incident Manager*, you will create a playbook rule and assign the task created in [Step 3: Creating a Task](#) to the playbook rule. At the end, you will activate the playbook rule.

- From within the navigation panel on the left-hand side, navigate to **Security Incident Response > Playbook Rules Management**.
- Click the **Create a new Playbook Rule** image.




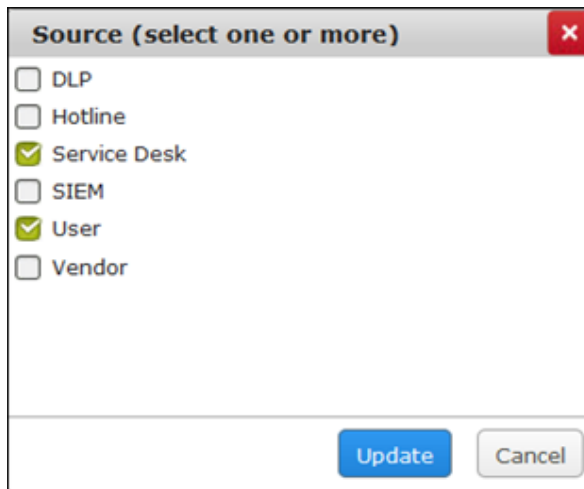
The **Playbook Rule (new)** opens with the **Playbook Tasks Rules** tab selected.

3. Enter a name in the **Playbook Rule Name** attribute.




4. Set the **Source (select one or more)** attribute.

- a. Click the  icon associated with the **Source (select one or more)** attribute. The **Source (select one or more)** dialog appears.
- b. Select the check box for required sources.

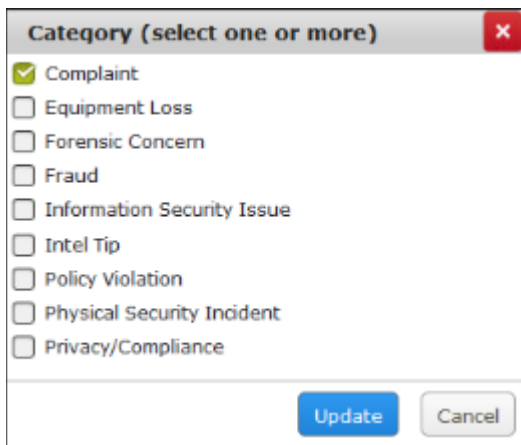


- c. Click **Update**.

5. Set the **Category (select one or more)** attribute.

- a. Click the  icon associated with the **Category (select one or more)** attribute. The **Category (select one or more)** dialog appears.

- b. Select the check box for desired categories.



**Category (select one or more)**


- Complaint
- Equipment Loss
- Forensic Concern
- Fraud
- Information Security Issue
- Intel Tip
- Policy Violation
- Physical Security Incident
- Privacy/Compliance

Update Cancel

- c. Click **Update**.

The **Category (select one or more)** attribute is set.

6. Set the **Subcategory (select one or more)** attribute.

- a. Click the  icon associated with the Subcategory (select one or more) attribute.  
The **Subcategory (select one or more)** dialog appears.

- b. Select the check box for desired subcategories.



**Subcategory (select one or more)**

- Insider Threat
- Intrusion
- Malware
- Misconduct
- Network Activity
- Phishing
- Social Engineering
- Theft - Data
- Theft - Hardware

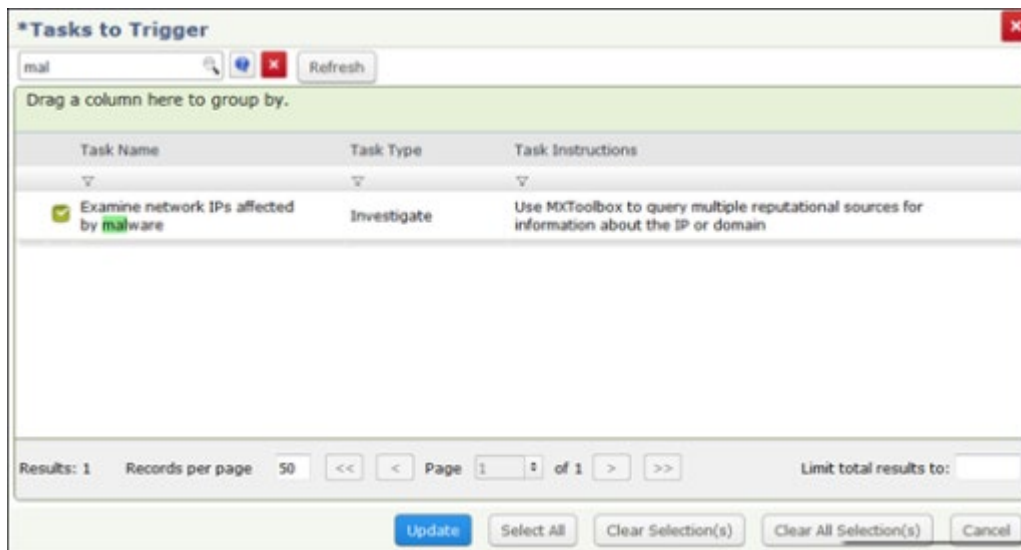
Update Cancel

- c. Click **Update**.

The **Subcategory (select one or more)** attribute is set.



7. Add the tasks you want to trigger.
  - a. Click **Add** along the **Tasks to Trigger**.  
The **Tasks to Trigger** dialog appears.
  - b. Select the check box for desired tasks and select the task created in [Step 3: Creating a Task](#).



- c. Click **Update**.  
The task is added and appears under **Tasks to Trigger**.
8. Click **Activate Rule**.  
A new playbook rule is created and is in the active state.

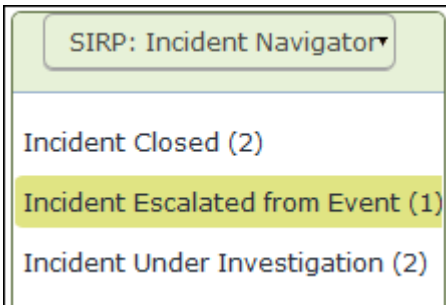
**Note:** Clicking **Save & Close** will put the playbook rule in the deactivated state.

## Step 5: Responding to an Incident Escalated from the Event

In this step, by staying signed in to Rsam as the *SIRP Incident Manager*, you will respond to an incident escalated from the event. During this process, you will build the task list. Later, you will assign an owner to each task and submit the incident for investigation.

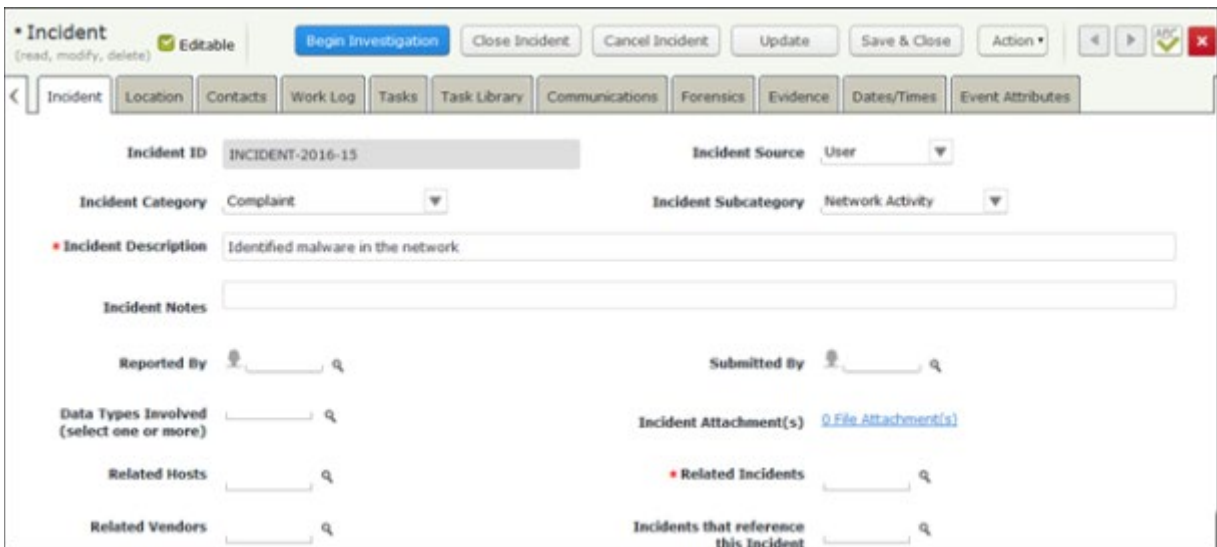
1. From within the navigation panel on the left-hand side, navigate to **Security Incident Response > Incident Response Navigator**.  
The Incident Response Navigator home page appears.

- From within the Incident Response Navigator home page, click **Incident Escalated from Event**.



The incidents escalated from events appear.

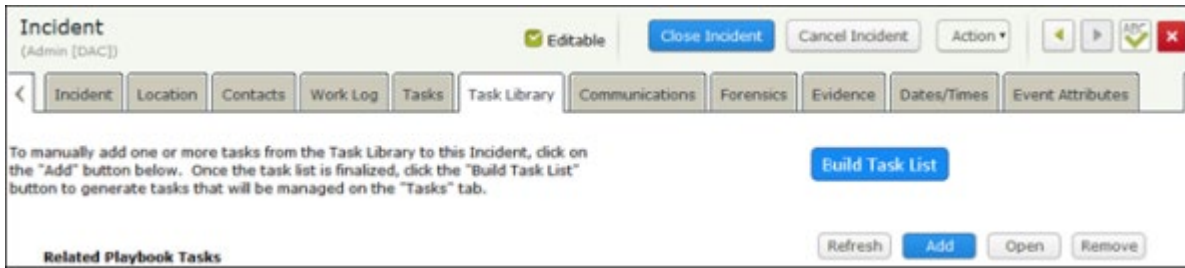
- Locate the incident.
  - Double-click the incident.
- The **Incident** record opens with the **Incident** tab selected.
- Complete all the required attributes, and any additional attributes that are necessary to you.



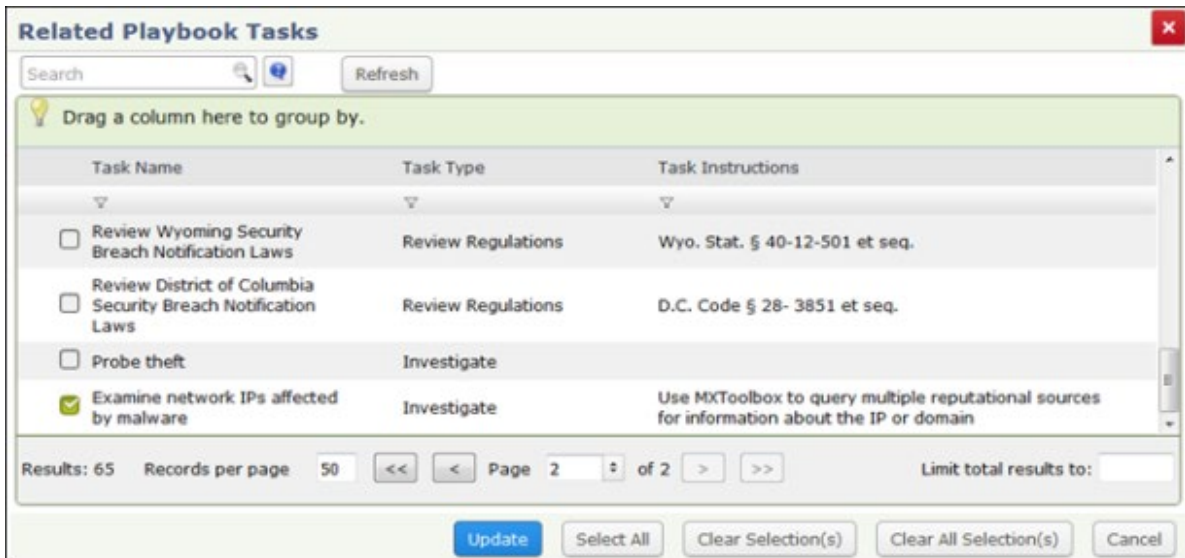
- Click the **Location** tab, and then complete all the attributes as necessary.



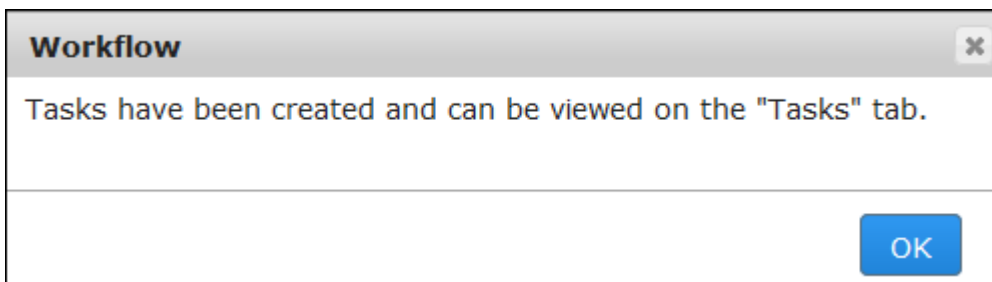
- Click the **Task Library** tab.



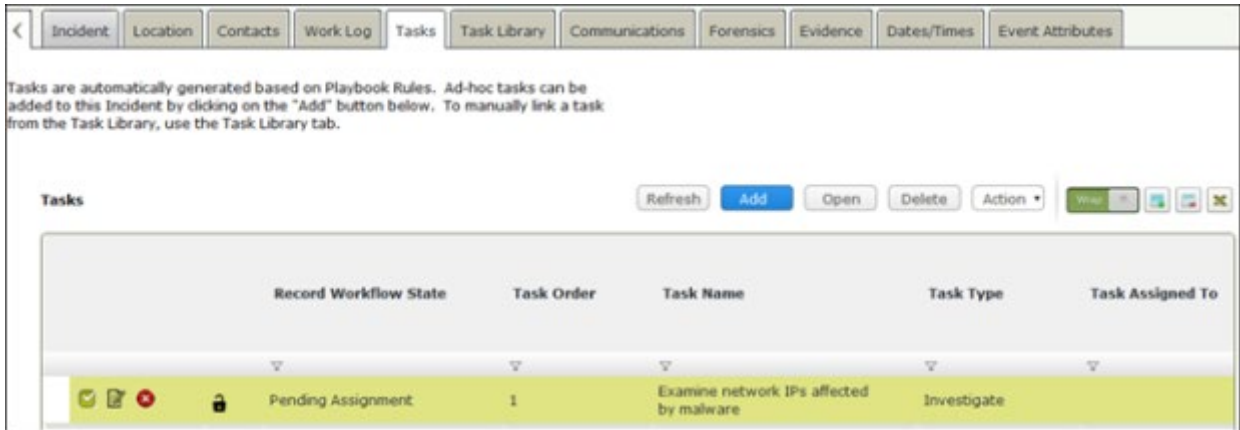
- Click **Add** along the **Related Playbook Tasks**.  
The **Related Playbook Tasks** dialog appears.
- Search for the task created in [Step 3: Creating a Task](#) and select the check box for the task.



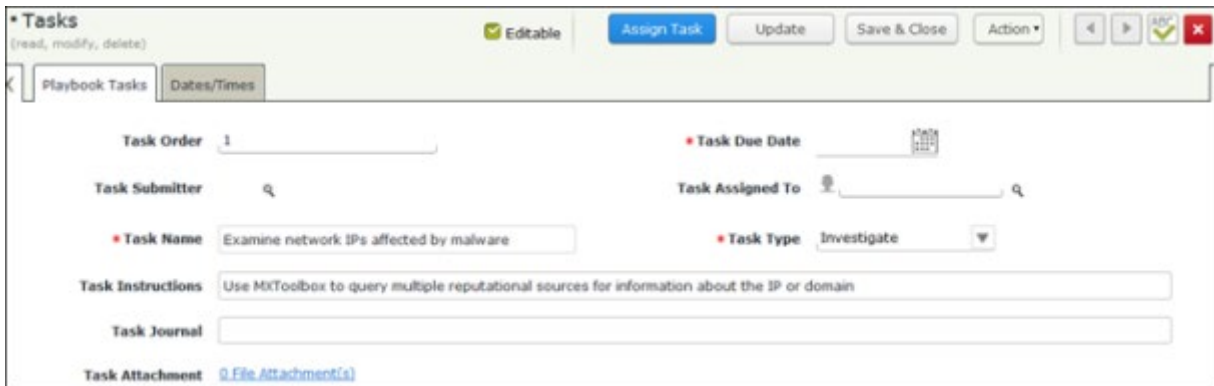
- Click **Update**.  
The task is added to the incident.
- Click **Build Task List**.
- In the message that appears indicating that the tasks are created and appear on the **Tasks** tab, click **OK**.



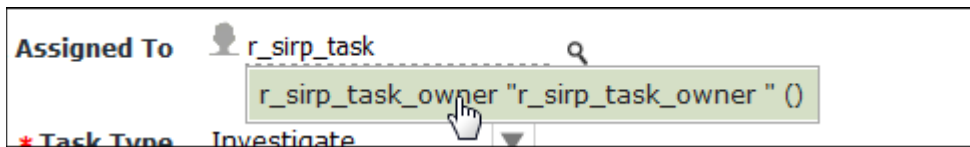
The tasks enter the **Pending Assignment** state and appear on the **Tasks** tab.



13. Double-click the task.  
The **Tasks** record opens with the **Playbook Tasks** tab selected.
14. Complete the **Task Due Date** attribute.



15. Set the **Task Assigned To** attribute to *r\_sirp\_task\_owner*.
  - a. Enter *r\_sirp\_task\_owner* in the **Task Assigned To** attribute. A list of users matching the criteria appear.
  - b. In the user list, select *r\_sirp\_task\_owner* "r\_sirp\_task\_owner" ().



The **Task Assigned To** attribute is set to *r\_sirp\_task\_owner*.

16. Complete other attributes as necessary.

17. Click **Assign Task**.  
The task enters the **Assigned** state.
18. Click **Begin Investigation**.  
The incident enters the **Incident Under Investigation** state.

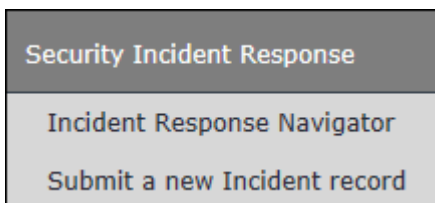
**Note:** If you have defined Playbook Rules, the tasks are linked automatically to incidents as children when the criteria is met.

19. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.  
You have been successfully logged out from the Rsam Security Incident Response module.

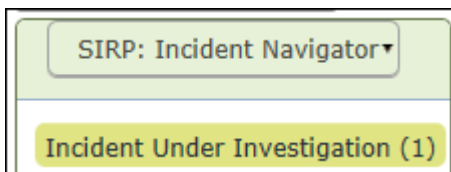
## Step 6: Working with Tasks

In this step, you will log in to Rsam as the *SIRP Task Owner* to work on the tasks associated with the incident. You will want to create tasks manually when there are no Playbook Rules that link the tasks to incidents.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Security Incident Response module.
2. Sign in as the *SIRP Task Owner* user. Enter **Username** as *r\_sirp\_task\_owner* and **Password** as *password*.
3. From within the navigation panel at the left-hand side, navigate to **Security Incident Response > Incident Response Navigator**.



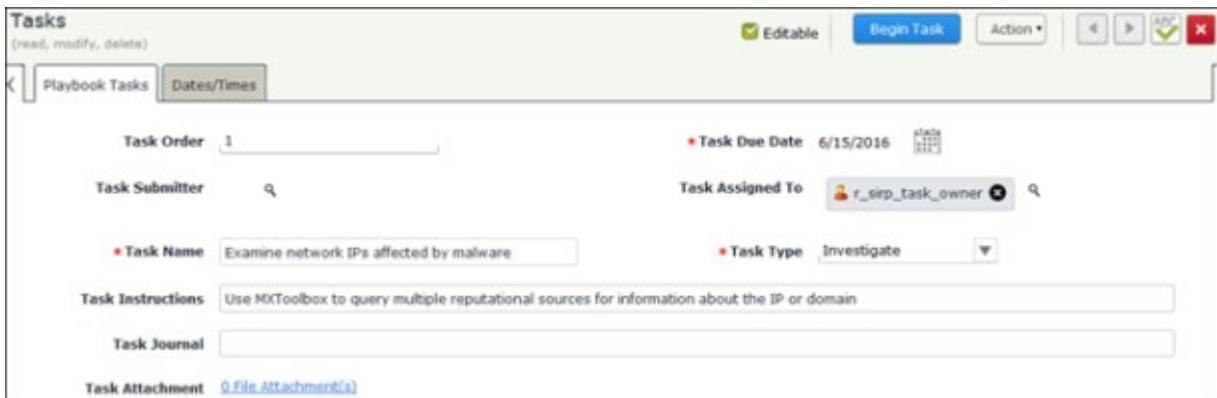
4. From within the **Incident Response Navigator**, click **Incident Under Investigation**.



The incidents in the *Incident Under Investigation* state appear.

5. Locate the incident.

6. Double-click the incident.  
The **Incident** record opens with the **Incident** tab selected.
7. Click the **Tasks** tab.
8. Double-click the task.  
The **Tasks** record opens with the **Playbook Tasks** tab selected.
9. Click **Begin Task**.



The task enters the **In Progress** state.

4. Click **Close Task**.



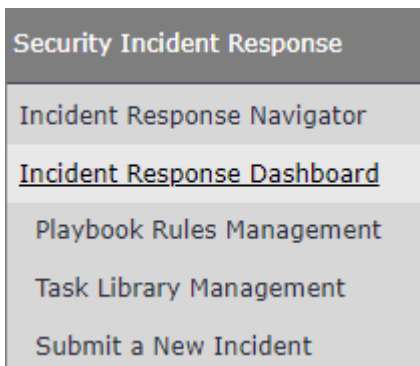
The task enters the **Completed** state.

10. Repeat steps 8 through 10 to close other tasks, if available.
11. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.  
You have been successfully logged out from the Rsam Security Incident Response module.

## Step 7: Investigating the Incident

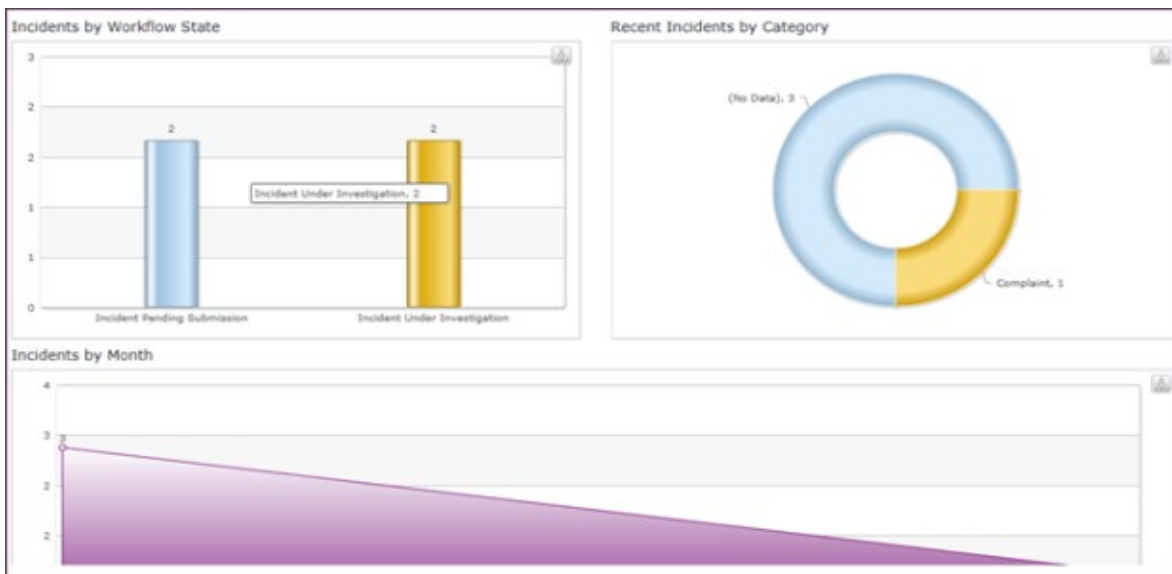
In this step, you will log in to Rsam as the *SIRP Incident Reviewer* to review the closed tasks associated with the incident. You will close the incident if all the closed tasks are found satisfactory.

1. Open an Rsam supported browser and enter the URL of the Rsam instance containing the Security Incident Response module.
2. Sign in as the *SIRP Incident Reviewer*. Enter **Username** as `r_sirp_incident_reviewer` and **Password** as `password`.
3. From within the navigation panel at the left-hand side, navigate to **Security Incident Response > Incident Response Dashboard**.



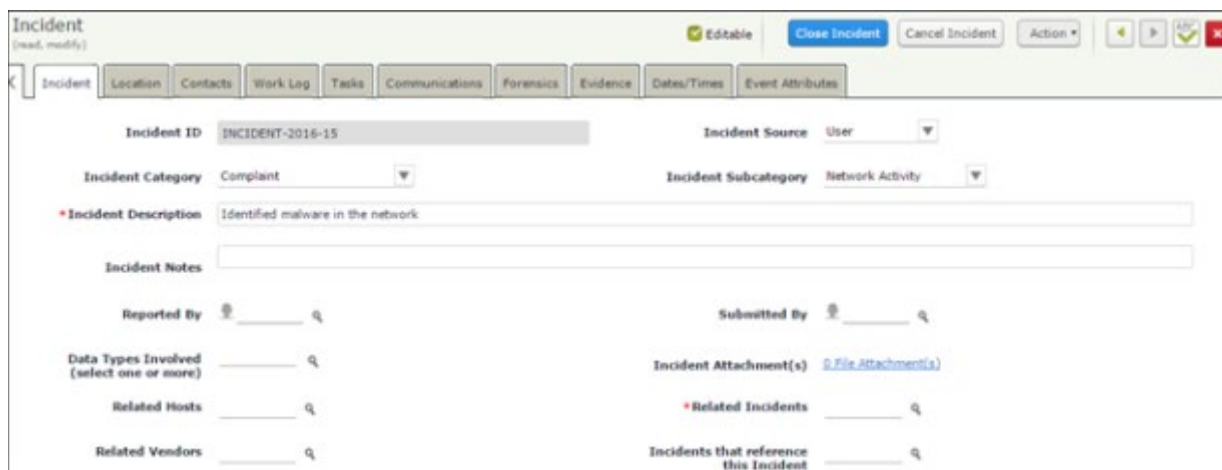
The Incident Response Dashboard home page appears.

4. From within the **Incidents by Work State** chart, click on the bar representing the **Incident Under Investigation** state.



The **SIRP module Incidents by Workflow State** chart opens with incident records.

5. Click **Incident Under Investigation**.  
The incident records in the **Incident Under Investigation** state appear.
6. Locate the incident you want to investigate and close.
7. Double-click the incident.  
The **Incident** record opens with the **Incident** tab selected.
8. Click the **Tasks** tab, open the tasks, and review all the associated tasks.
9. Click **Close Incident**.



The screenshot shows the 'Incident' record form in the R-sam Security Incident Response module. The form is titled 'Incident' and includes a 'read, modify' status. The incident ID is 'INCIDENT-2016-15'. The incident source is 'User' and the incident category is 'Complaint'. The incident subcategory is 'Network Activity'. The incident description is 'Identified malware in the network'. The form includes fields for 'Reported By', 'Submitted By', 'Data Types Involved (select one or more)', 'Related Hosts', 'Related Vendors', 'Incident Attachment(s)', 'Related Incidents', and 'Incidents that reference this Incident'. The 'Close Incident' button is visible in the top right corner.

The incident enters the **Incident Closed** state.

10. Hover the cursor over the username at the right-hand corner and select **Logout** from the options that appear.  
You have been successfully logged out from the Rsam Security Incident Response module.

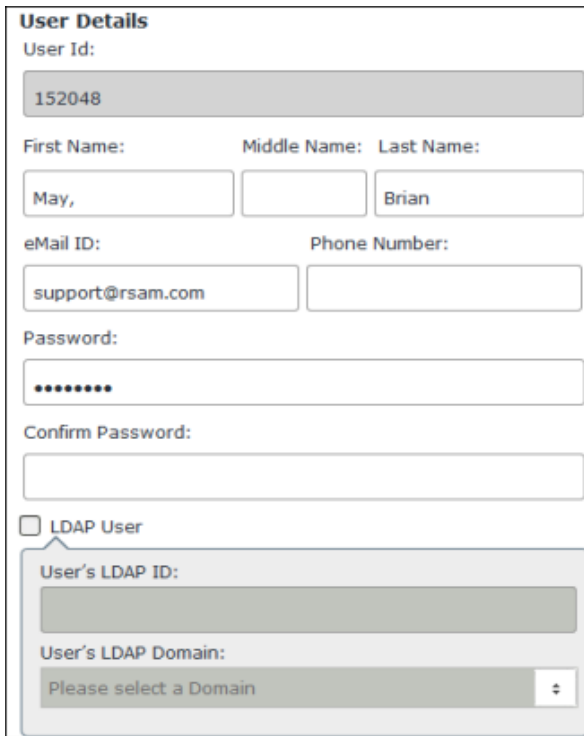


# Appendix 1: Email Notifications and Offline Decision Making

## Setting up Email Addresses

This module is configured to send automated email notifications at specific points in the workflow. In a production system, email addresses are usually gathered automatically using an LDAP server or a directory service. However, the email addresses in your Rsam instance can be manually provided for testing purposes. To manually provide the email addresses, perform the following steps:

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the Security Incident Response Module module.
2. Sign in as *r\_admin* user. Enter **Username** as *r\_admin* and **Password** as *password*.
3. Navigate to **Manage > Users/Groups**.
4. Double-click a user row to open the details.
5. Provide an email address in the **eMail ID** attribute.



**User Details**

User Id:  
152048

First Name: Middle Name: Last Name:  
May, Brian

eMail ID: Phone Number:  
support@rsam.com

Password:  
\*\*\*\*\*

Confirm Password:

LDAP User

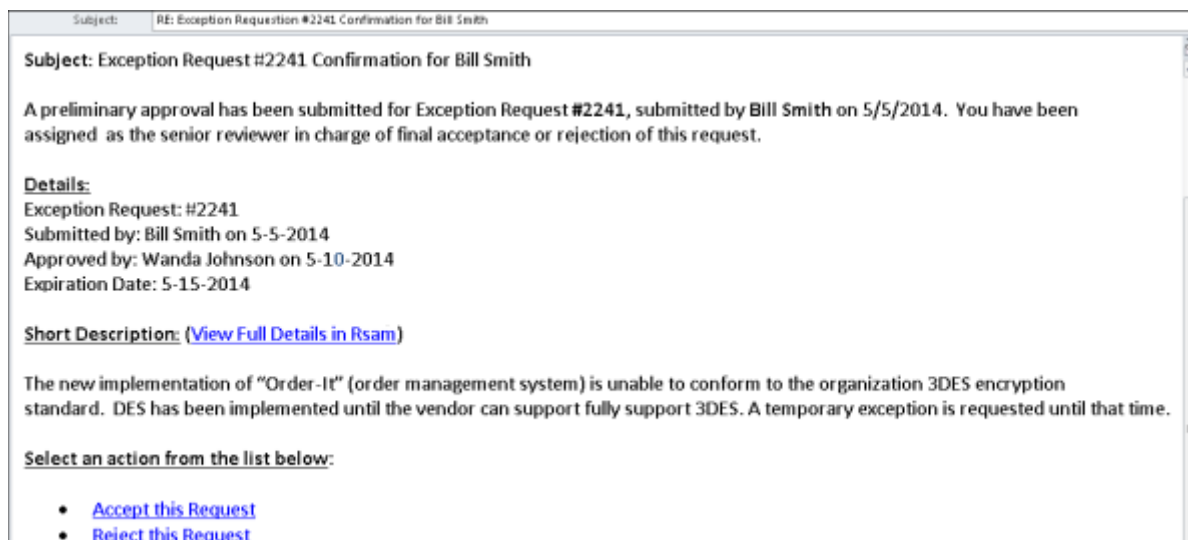
User's LDAP ID:  
User's LDAP Domain:  
Please select a Domain

6. Click **OK**.  
The email address of the user account is saved.

## Offline Decision Making

Rsam email notifications are configurable including what notification should be sent, what users or roles will receive the notifications, and the content in the notifications.

Offline Decision Making is a powerful and popular feature of Rsam. It provides the Rsam platform directly to the users to perform workflow actions without connecting to the Rsam module. The following image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Offline Decision Making actions.



## Appendix 2: Rsam Documentation

### SIRP Module Baseline Configuration Guide

To learn more about the pre-configurations in the Security Incident Response Module, refer the *Security Incident Response Module Baseline Configuration Guide*. You should have received the *Security Incident Response Module Baseline Configuration Guide* along with the Security Incident Response Module sandbox. If not, please contact your Rsam Customer Representative to obtain an electronic copy of the *Security Incident Response Module Baseline Configuration Guide*.

### Online Help

This tutorial provides the step-by-step instructions for the Rsam Security Incident Response Module module. To get familiar with the specific Rsam features used in this configuration, refer the *Rsam End-User Help*, *Rsam Administrator Help*, or both. The Online help you can access depends on your user permissions. To access the Online Help, perform the following steps:

1. Sign in to your Rsam instance. For example, sign in as *Example Administrator* user. Provide the **Username** as *r\_admin* and **Password** as *password*.
2. Hover the cursor over **Help** and select an Online help from the menu that appears. Depending on your user permissions, you will be able to access the Rsam End-User Help, Rsam Administrator Help, Step-by-Step Tutorials, or all.

The following image shows the *Rsam Administrator Help*, opened from the *Example Administrator* user account.

