SOAR-Threat & Vulnerability Management Module

Step-by-Step Tutorial

Document Version: 01.00.02 | December 2018

Contents

About Rsam Tutorials 3

Rsam Sandbox Environment 4

Sign-In Page 4

Rsam SOAR-Threat & Vulnerability Management 5

Overview 5

SOAR - Vulnerability Management Workflow 5

User Accounts 7

High-Level Steps 7

Step-by-Step Procedure 8

Step 1: Verifying Vulnerability Records 8

Step 2: Selecting the False-Positive Action Plan 9

Step 3: Approving the False-Positive Action Plan 12

Appendix 1: Email Notifications and Offline Decision Making 14

Setting up Email Addresses 14

Offline Decision Making 15

Appendix 2: User Assignment Options 16

Appendix 3: Rsam Documentation 17

SOAR-TVM Module Baseline Configuration Guide 17

Online Help 17

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.

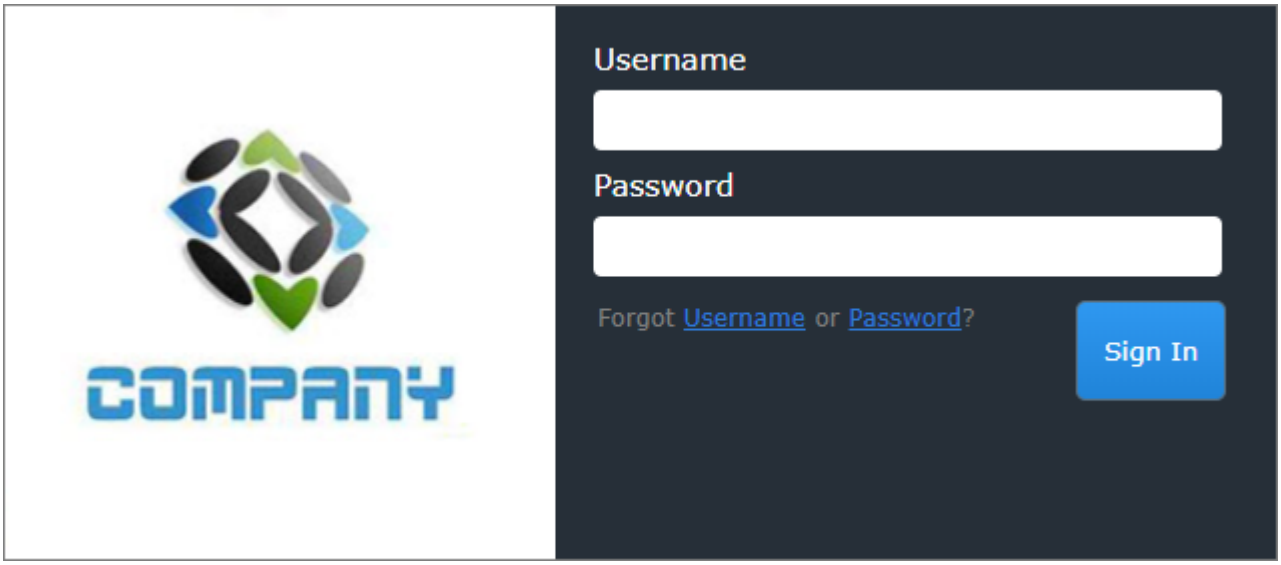
Rsam Sandbox Environment

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, 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 SOAR-Threat & Vulnerability Management

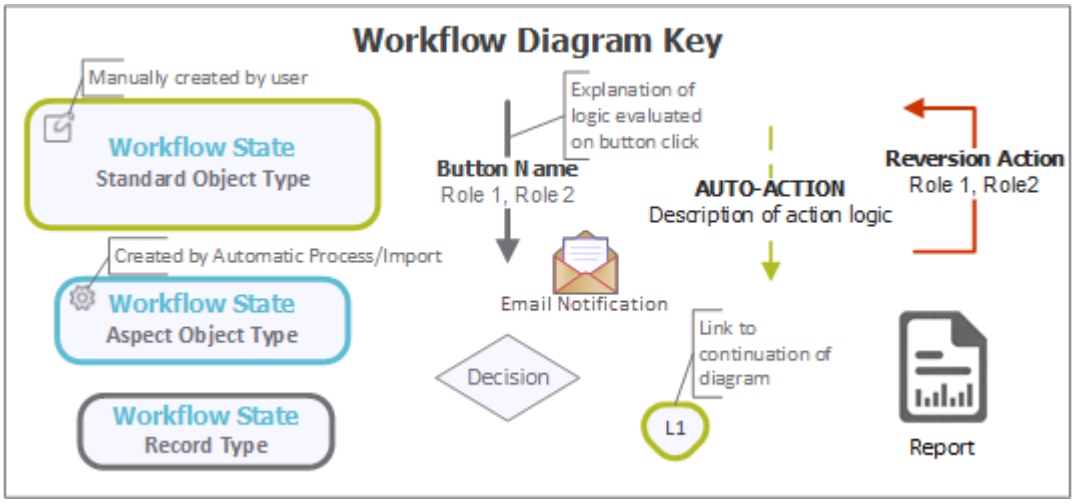
Overview

The Rsam Security Operations, Analytics and Reporting (SOAR) – Threat & Vulnerability Management module is designed for users tasked with a responsibility to resolve vulnerabilities attached to assets in their organizations. This tutorial provides a step-by-step procedure to walk you through one path of a SOAR - Threat & Vulnerability Management workflow within the module.

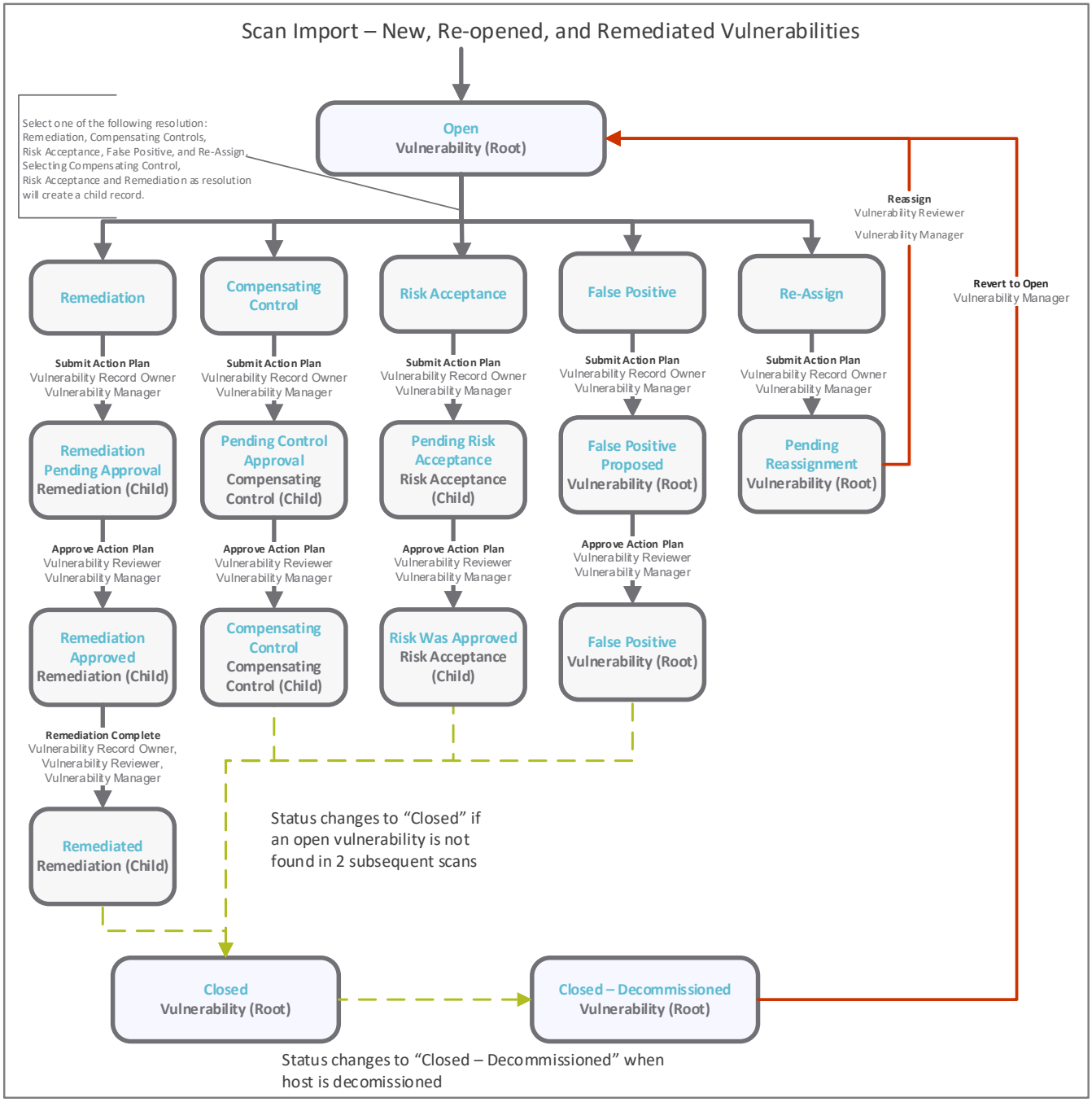
To help you get started, some assets and vulnerabilities have been pre-loaded from some of the most common scanner tools. Import profiles and maps have also been provided along with the ability to make your own. To get more insights into the SOAR -Vulnerability Management module, please obtain the *SOAR- Threat & Vulnerability Management Baseline Configuration Guide* from your Rsam Representative.

SOAR - Vulnerability Management Workflow

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



The following diagram depicts the out-of-the-box SOAR - Vulnerability Management workflow.



User Accounts

User Accounts are required to authorize individuals to access a specific Rsam module. The Rsam sandbox for SOAR - Vulnerability Management comes with pre-populated sample accounts.

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

Account ID	User Name	Business Responsibilities
r_vulnerability_manager	Vulnerability Manager	User with the ability to assign responsibilities to the users, approve remediation activities, and perform all tasks of the *Vulnerability Owner* and *Vulnerability Reviewer*.
r_vulnerability_owner	Vulnerability Owner	User responsible for reviewing all assigned vulnerabilities and submitting and managing any action plans such as False-Positive and Remediation.
r_vulnerability_reviewer	Vulnerability Reviewer	User responsible for reviewing and either approving or rejecting the data entered by the *Vulnerability Owner*.

The default password for all accounts in the SOAR - Threat & Vulnerability Management 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 explained in the tutorial.

Step	User	Description
Step 1: Verifying Vulnerability Records	Vulnerability Manager	This step comes pre-configured with the SOAR - Vulnerability Management module.
Step 2: Selecting the False-Positive Action Plan	Vulnerability Owner	In this step, the *Vulnerability Owner* user selects the False Positive action plan to resolve a vulnerability.
Step 3: Approving False-Positive Action Plan	Vulnerability Reviewer	In this step, the *Vulnerability Reviewer* user reviews and approves the False Positive Proposed action plan that was submitted by the *Vulnerability Owner* user.

Step-by-Step Procedure

This section contains the workflow steps we follow for this SOAR - Threat & Vulnerability Management tutorial. Following this path, you are flagging a vulnerability using the False-Positive action plan. This path was chosen as is a common path to follow, though you are welcome to explore other paths as well.

Before you move on to practice each step, consider the following:

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 *Vulnerability Manager* user account in one session if desired.

b. Workflow state transitions send 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 later in this tutorial.

Step 1: Verifying Vulnerability Records

The SOAR - Threat & Vulnerability Management module comes preloaded with vulnerability records from several scanner output files. In this step, a *Vulnerability Manager* verifies whether vulnerabilities records exist in your Rsam instance containing the SOAR - Vulnerability Management module.

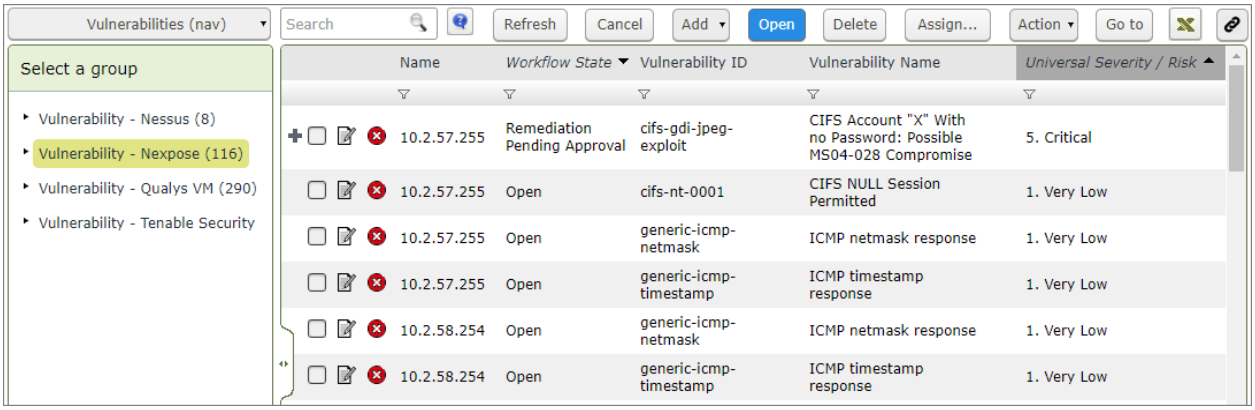
1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the SOAR - Vulnerability Management module.

2. Sign in as the *Vulnerability Manager* user. Enter **Username** as ***r_vulnerability_manager*** and **Password** as ***password***.

3. From within the navigation panel at the left-hand side, navigate to **Vulnerability Management** > **Vulnerability Navigator**.

The **Vulnerability Navigator** appears.

4. In the Vulnerability Navigator, verify that the vulnerability groups containing vulnerability records created from the scanner output files are available.



Note: By default, in the SOAR – VM module, the owner of the vulnerabilities identified on assets is pre-set to the **r_vulnerability_owner** user.

Step 2: Selecting the False-Positive Action Plan

In this step, the *Vulnerability Owner* selects and submits the *False-Positive* action plan to the *Vulnerability Reviewer* for approval. As part of this tutorial, the user will resolve a vulnerability present on the asset object with IP address 10.2.57.255.

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the SOAR - Vulnerability Management module.

2. Sign in as the *Vulnerability Owner* user. Enter **Username** as ***r_vulnerability_owner*** and **Password** as ***password***.

3. From within the navigation panel at the left-hand side, navigate to **Vulnerability Management** > **Vulnerability Navigator**.

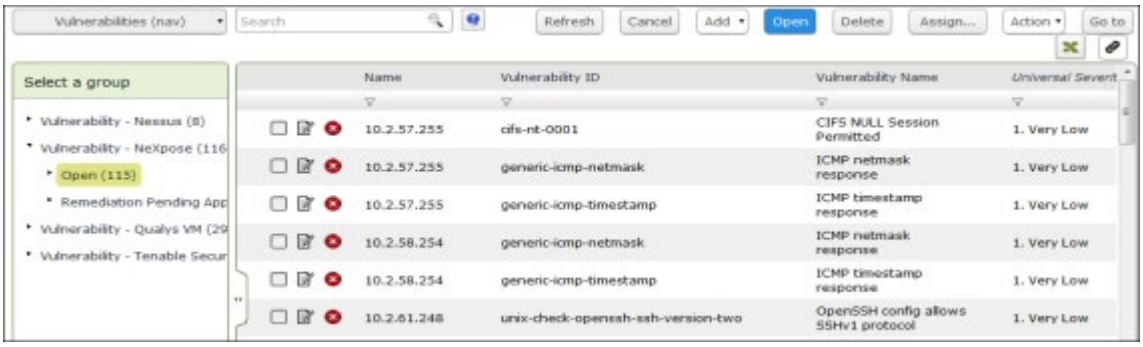
   The Vulnerability Navigator appears.

4. From within the Vulnerability Navigator with **Vulnerabilities (nav)** selected, click a vulnerability group in which the vulnerabilities for the asset are present. To work with Nexpose vulnerabilities, expand **Vulnerability - NeXpose**, and click **Open**.

   The vulnerabilities in the **Open** state appear.

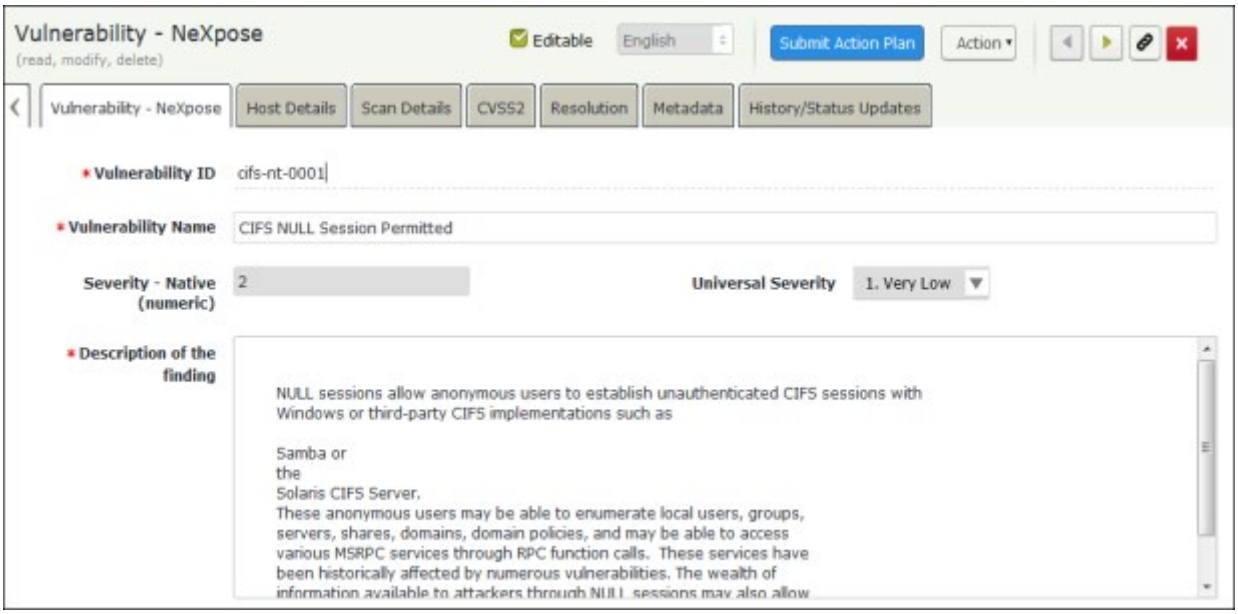
5. Use one of the following methods to open a vulnerability:

   - Double-click a vulnerability of interest.
   - Select a vulnerability of interest, and then click **Open**. Select more than one vulnerability to perform bulk changes.
   - Click the icon in the vulnerability record row.



The **Vulnerability - NeXpose** record opens with the **Vulnerability - NeXpose** tab selected.

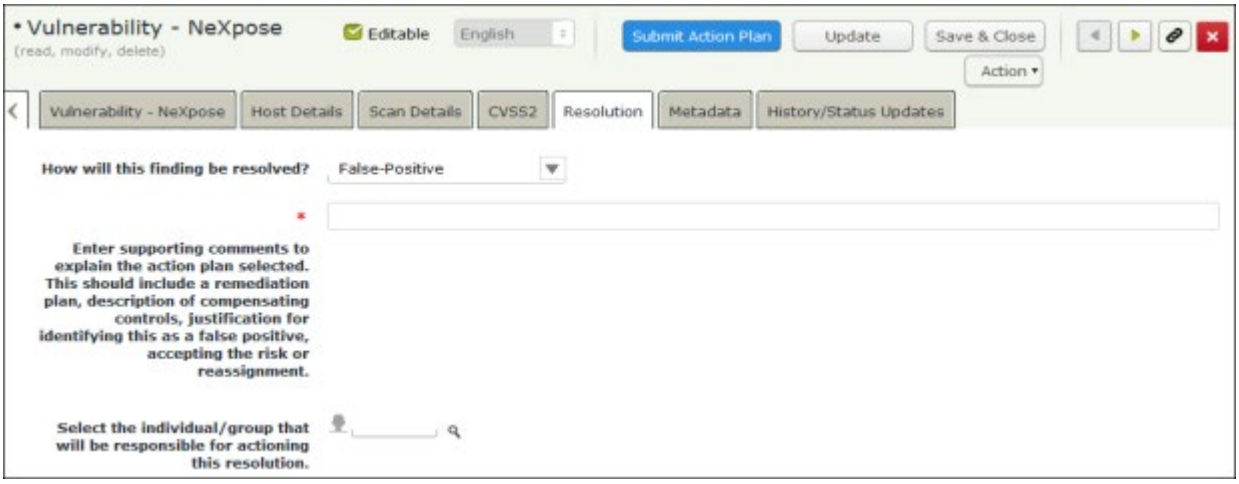
6. Review the scanner imported details on the **Vulnerability - NeXpose** tab.



7. Click the **Resolution** tab.

8. In the **How will this finding be resolved field**, select **False-Positive**. The other action plans in this list box are Remediation, Compensating Controls, Risk Acceptance Request, and Re-assign.

Note: You may want to select the Re-assign action plan if you are not the appropriate Vulnerability Owner.



9. Complete all the required details on the **Resolution** tab.

10. Click **Submit Action Plan**.

    The vulnerability record workflow enters the **False Positive Proposed** state.

Notes:
1. If the selected action plan is Remediation, the vulnerability record workflow enters the **Remediation Pending Approval** state.

2. If the selected action plan is Compensating Controls, the vulnerability record workflow enters the **Pending Control Approval** state.

3. If the selected action plan is Risk Acceptance Request, the vulnerability record workflow enters the **Pending Risk Acceptance** state.

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 SOAR - Threat & Vulnerability Management module.

Step 3: Approving the False-Positive Action Plan

In this step, you will log in to Rsam as the *Vulnerability Reviewer* user to approve the False-Positive action plan that was submitted by the *Vulnerability Owner* user.

1. Open an Rsam supported browser and enter the URL of your Rsam instance containing the SOAR - Threat & Vulnerability Management module.

2. Sign in as the Vulnerability Reviewer user. Enter **Username** as ***r_vulnerability_reviewer*** and **Password** as ***password***.

3. From within the navigation panel at the left-hand side, navigate to **Vulnerability Management** > **Vulnerability Navigator**.

   Note: You may also navigate to **Vulnerability Management** > **Dashboard** to see the graphical representation of vulnerabilities assigned to you.

4. From within the vulnerability navigator with **Vulnerabilities (nav)** selected, expand **Vulnerability - NeXpose**, and then click **False Positive Proposed**.

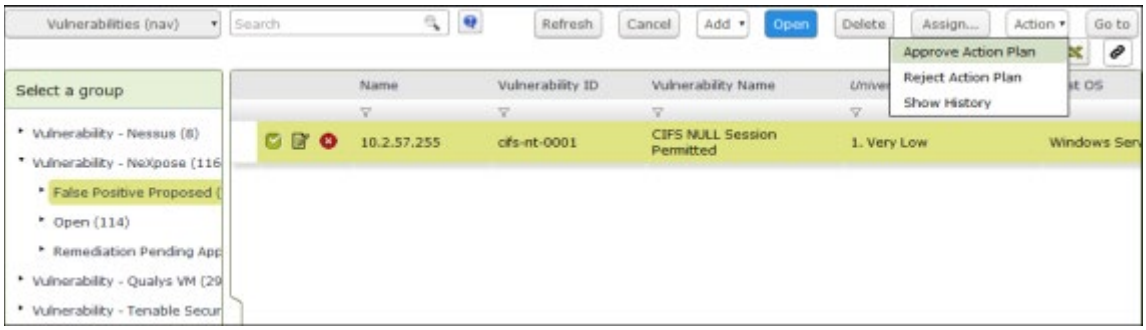
   The vulnerability records in the **False Positive Proposed** state appear.

5. Locate the vulnerability that was submitted in Step 2: Selecting the False-Positive Action Plan.

6. Select the check box in the vulnerability row.

7. Use one of the following methods to approve an action plan:

   - Click the **Action** button at the top-right corner and select **Approve Action Plan** from the options that appear.



- Open the vulnerability record and click the **Approve Action Plan** button at the top.

  The vulnerability record workflow enters the **False Positive** state.

  Notes:
  1. If the approval is for the *Remediation* action plan, the vulnerability record workflow enters the **Remediation Approved** state.

  2. If the approval is for the *Compensating Controls* action plan, the vulnerability record workflow enters the **Compensating Control** state.

  3. If the approval is for the *Risk Acceptance Request* action plan, the vulnerability record workflow enters the **Risk Was Accepted** state.

  4. If the action plan is *Rejected*, the vulnerability record is moved back to the **Open** state and the *Vulnerability Owner* is notified.

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 SOAR - Threat & Vulnerability Management module.

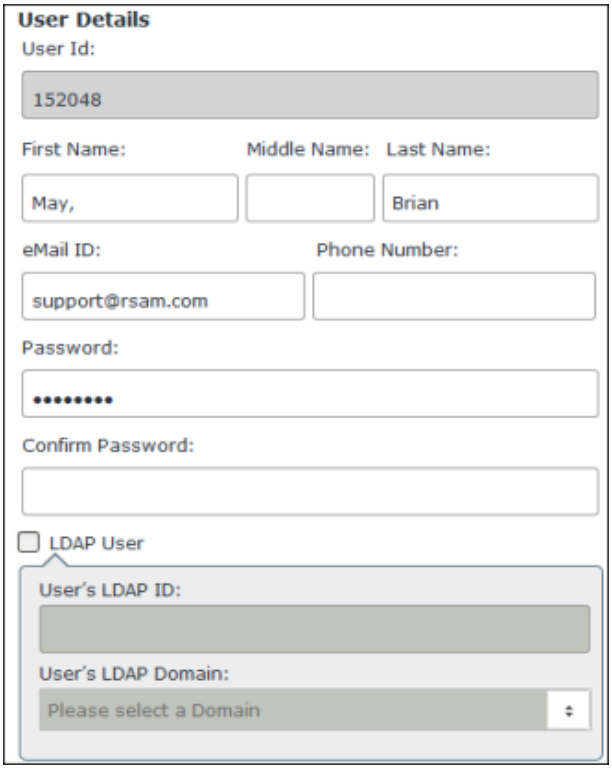
Appendix 1: Email Notifications and Offline Decision Making

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 SOAR - Threat & Vulnerability Management 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.



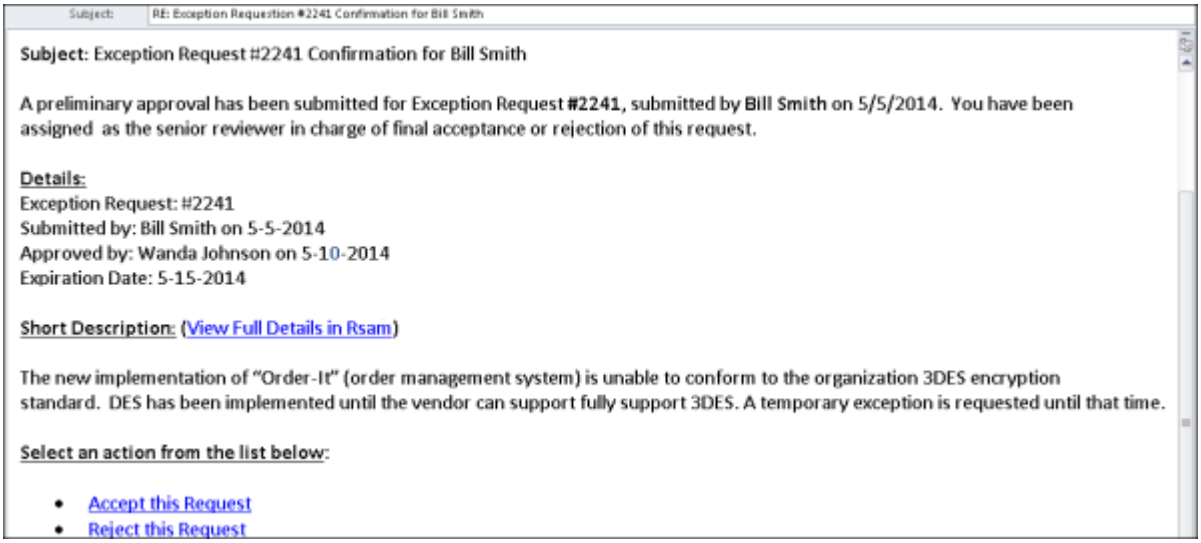
6. Click **OK**.

   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.



Subject: RE: Exception Requestion #2241 Confirmation for Bill Smith

Subject: Exception Request #2241 Confirmation for Bill Smith

A preliminary approval has been submitted for Exception Request **#2241**, submitted by **Bill Smith** on 5/5/2014. You have been assigned as the senior reviewer in charge of final acceptance or rejection of this request.

Details:
Exception Request: #2241
Submitted by: Bill Smith on 5-5-2014
Approved by: Wanda Johnson on 5-10-2014
Expiration Date: 5-15-2014

Short Description: (View Full Details in Rsam)

The new implementation of "Order-It" (order management system) is unable to conform to the organization 3DES encryption standard. DES has been implemented until the vendor can support fully support 3DES. A temporary exception is requested until that time.

Select an action from the list below:

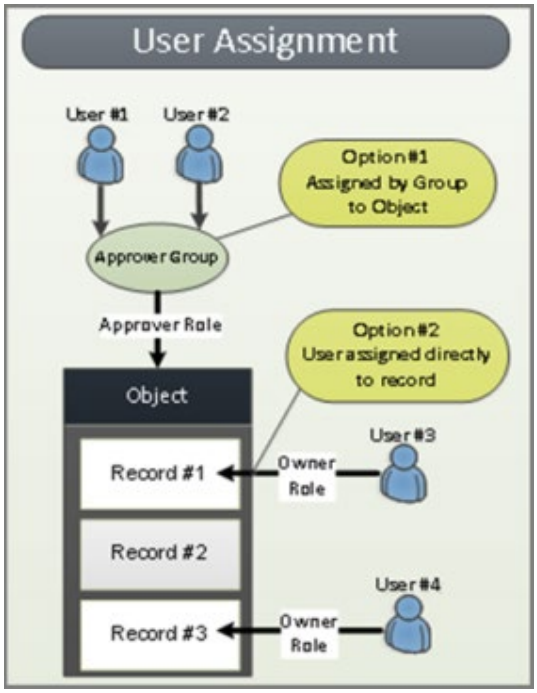
- Accept this Request
- Reject this Request

Appendix 2: User Assignment Options

Rsam allows organizations to customize configurations and workflows to their specific business practices. There are many methods by which users can be assigned roles (such as, who is responsible for reviewing and approving exceptions). The following are the most common assignment methods:

- Individual users are assigned to a group. The group is then assigned to the object under which the records are saved. When assigned to the object, the group is also given a specific role. This accomplishes the following:
    - All users in that group inherit the role assigned to the group in the context of the object and all the records under that object.
    - All users in that group have the functionality allocated to that role in the context of the object and all of the records under that object.
- Individual users are assigned a specific role directly in a record. This provides the same result as above – granting the user the functionality with the allocated role. However, it is only in the context of that specific record. No other permissions are granted to the parent object or any other record under that object.

The method for implementing the assignment can also be customizable. The assignment can be manually made through an attribute, assigned when the records are created or imported, or automatically made at different points in the workflow.



Appendix 3: Rsam Documentation

SOAR-TVM Module Baseline Configuration Guide

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

Online Help

This tutorial provides the step-by-step instructions for the Rsam SOAR- Threat & Vulnerability Management 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.