SOAR-Threat & Vulnerability Management Module

Baseline Configuration Guide

Document Version: 01.00.02 | December 2018

Contents

About Rsam Baseline Configuration Guides

Rsam Baseline Configuration Guides provide you the information needed to understand the pre-defined configurations for each module. These guides should be referenced to gain a better understanding of how the module is configured and can be used out-of-the-box.

Baseline Configuration Overview

This document describes the baseline configuration and structure for the Rsam Security Operations, Analytics and Reporting (SOAR) – Threat & Vulnerability Management (TVM) module (identified as TM for Threat Management and VM for Vulnerability Management from here onwards). The baseline configurations for the SOAR – Threat & Vulnerability Management module allow your users to manage threats from data feed sources and vulnerabilities and findings from scanners applications. The pre-configured activities help streamline your program by leveraging a central repository, allowing for data normalization, workflow and timely reporting in a more automated fashion.

The following is a list of elements that have been configured in the SOAR - Threat and Vulnerability Management module:

- Structure
- Home Page Tabs
- SOAR Workflow
- Importing Data
- Scheduling Imports

The information on the elements mentioned above will provide a baseline understanding before you leverage the *SOAR – Threat and Vulnerability Management Step-by-Step Tutorial* or begin to tailor the module to meet your unique requirements.

SOAR-TVM Structure

Each asset in the SOAR-TVM module is stored as *Object* and each vulnerability or finding discovered on that asset is stored as *Record* within that object. Records may come from a variety of sources; each source is classified as a separate record category and record type (such as Qualys, Nessus, WhiteHat, and so on).

The SOAR – Threat & Vulnerability Management baseline module also includes configurations to store the summary information of findings that are discovered on desktops. This is accomplished by creating an object for each group of workstations (as opposed to each individual workstation), and then creating a single record for each unique type of discovered finding, and then simply how many assets had that finding. This allows you to streamline the data and process when managing high volumes of desktop vulnerabilities.

Notes:

1. Asset information can be captured as attributes (for example, Operating System, Zone, Data Sensitivity, Hosted Applications) in the object. Vulnerability or Issue records can leverage their own attributes as well as those stored in an asset object. This is very helpful when making automated workflow decisions, generating reports, performing searches, and leveraging navigators.

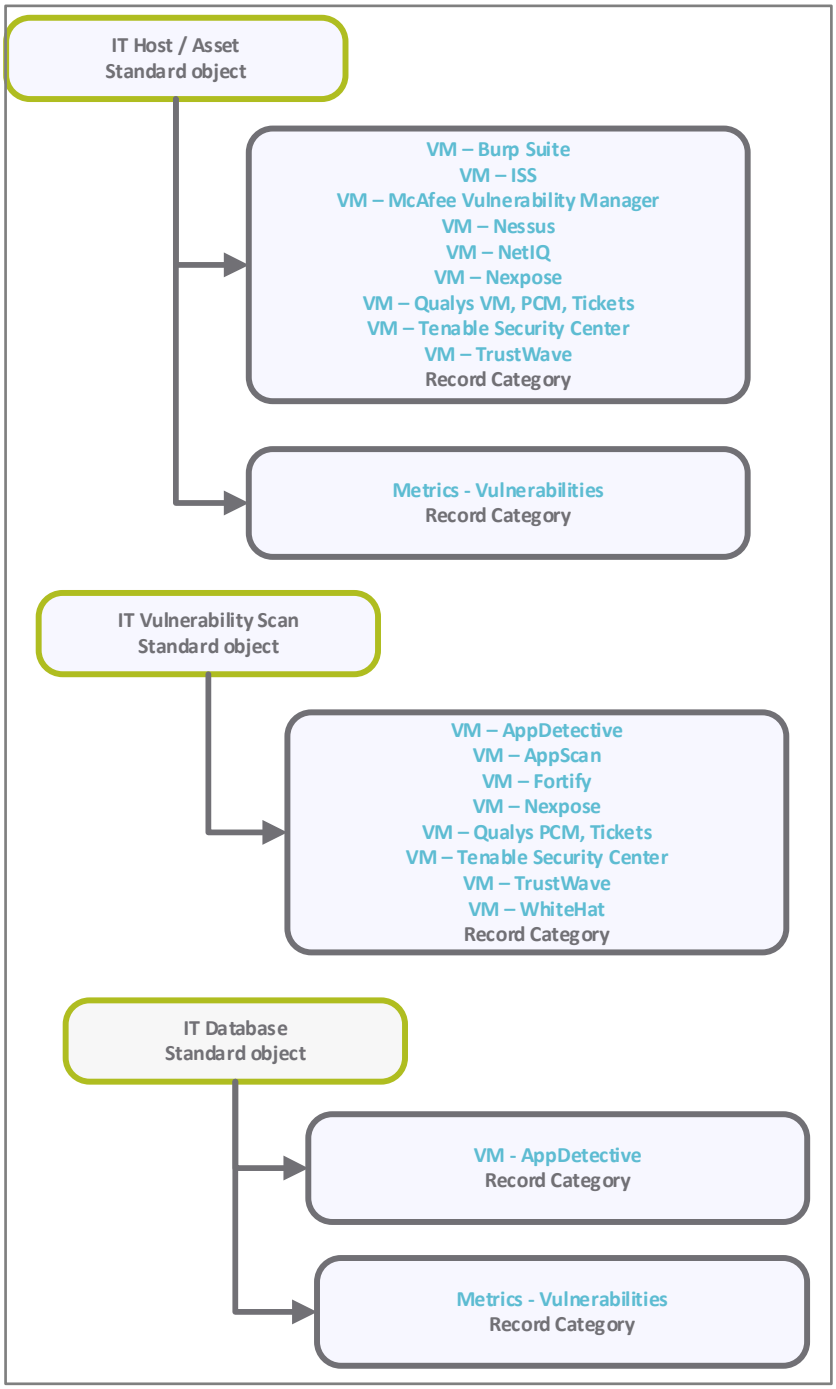
2. Permission assignments can occur at the asset level based on the asset criteria such as operating system, and IP subnet, and more. This provides the assignee access to all records within that asset, and allows them to further assign those records individually. Assigning at an object level is also optimal for performance (as opposed to assigning each record individually).

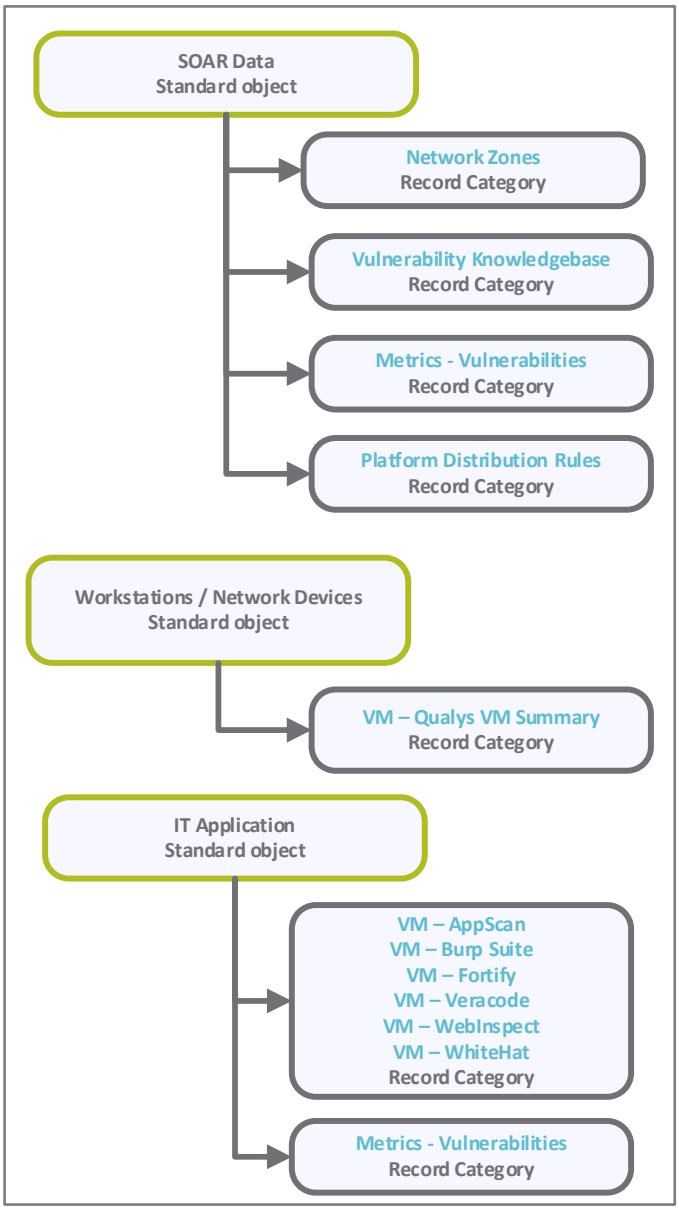
3. Lookup tables can be used to populate attributes automatically within an asset object (IP Subnet, Zone, Operating System, Responsible Team, and so on).

4. Rogue devices can be detected by comparing what has been scanned in the vulnerability scans against the object list (the imported asset inventory).

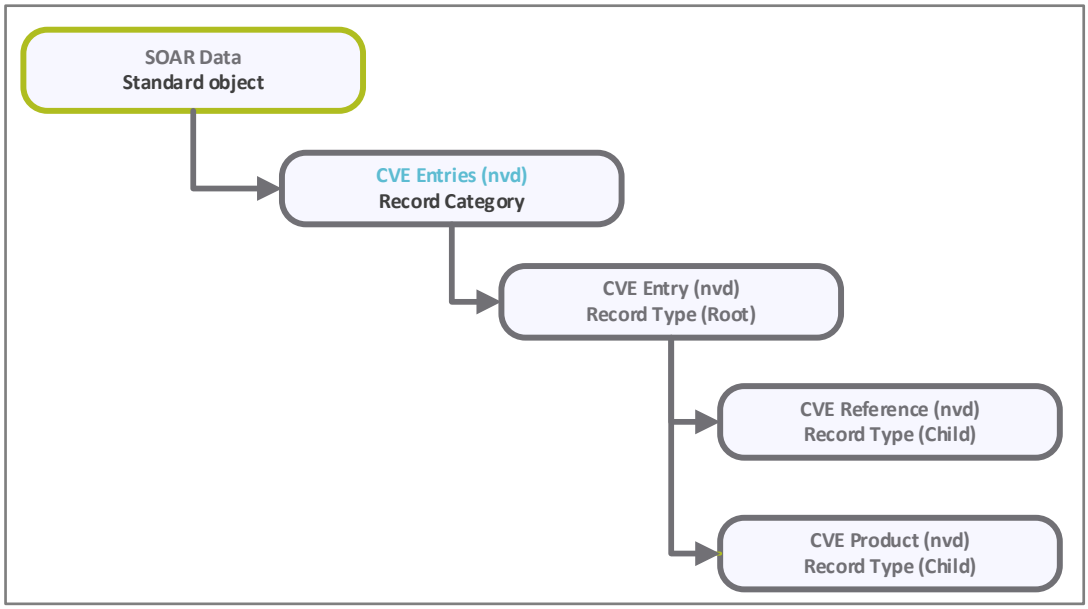
In comparison, the SOAR-TM module has all records stored in a single object. All data feeds integrated for Threat Management can reside within a single library for ease of reporting and management across the organization. This library can also house any number of dictionary, administrative, or knowledgebase information used within the SOAR-TVM use cases.

The following diagrams represents the SOAR-VM structure.




SOAR Data
Standard object
Network Zones
Record Category
Vulnerability Knowledgebase
Record Category
Metrics - Vulnerabilities
Record Category
Platform Distribution Rules
Record Category
Workstations / Network Devices
Standard object
VM – Qualys VM Summary
Record Category
IT Application
Standard object
VM – AppScan
VM – Burp Suite
VM – Fortify
VM – Veracode
VM – WebInspect
VM – WhiteHat
Record Category
Metrics - Vulnerabilities
Record Category

The following diagram represents the SOAR-TM structure.



Object Types

The following table lists the object types pre-configured in this module.

Object Type	Usage
IT Host/Asset	A standard object that uses one object per host / asset. These objects can be created automatically through an asset inventory import, during vulnerability imports, or manually.
Workstations/Network Devices	A standard object that uses one object per group of workstations or network devices (commonly grouped by type, location, or scan). This object comprises a summary of workstation or network device vulnerabilities that are populated using an import file.
IT Application	A standard object that uses one object per application. It stores all application-related information, such as service scans, source code scans, and more.
IT Database	A standard object that uses one object per database. It stores all database-related information, such as database scans.
IT Vulnerability Scan	For more information, see the Variations in the Data Structure section.
SOAR Data	Uses the standard TVM Data object for managing various vulnerability-related data, such as network zones, metrics, and vulnerability knowledge base.

Record Types

The following table lists the record types pre-configured in this module.

Record Type	Usage
Vulnerability – vendor source	One record per vulnerability per host. These records are automatically created during imports. They are generated based on a unique ID that commonly consists of vulnerability ID + Port + Asset IP or DNS name. Rsam saves each vulnerability source such as Qualys, Nessus, Nexpose, Fortify, and WebInspect as a different record type.
VM – Qualys VM Summary	One record per vulnerability ID per workstation group. Each record includes the count of devices containing vulnerability(s) plus a list of IP addresses and DNS names of the effected devices. These record types are automatically created during imports. They are generated based on a unique ID that commonly consists of vulnerability ID + Port.
Vulnerabilities – Metrics	Vulnerability metric records are generated on a periodic basis and can be stored under the TVM Data object or under an IT Application, IT Database or IT Host object.
Network Zones	Lookup table with records specifying the relationship between a network zone (i.e., DMZ, Internal, Extranet) and IP subnet range. Records are manually created and can be automatically linked to an asset during an asset import by comparing the IP of the asset to the subnets recorded in the library. All related attributes are copied into the IT Host/Asset object.
Vulnerability Knowledgebase	Vulnerability knowledge base records contain details about vulnerabilities that can supplement imported vulnerability data. Typically, these records are created automatically during imports, but can also be created manually. Also, these records can be linked automatically to vulnerabilities during a vulnerability import.
CVE Entry (nvd)	This record type is specifically used for Common Vulnerability Enumeration (CVE) coming in from the National Vulnerability Database (NVD). This record can be used to tie several vulnerability records from different sources together. This record type has two components as child records: CVE References and CVE Product. CVE References are sources where the CVE was first documented. CVE Products are known products and their versions that are affected by this CVE.

Variations in the Data Structure

Rsam includes an alternative library-based model that can store all the vulnerabilities in one library object and uses attributes in the records to identify the assets the vulnerabilities reside on. This simplifies the process; however, there won't be any advantage of storing the asset information in the object.

Home Page Tabs

The Baseline Configuration of the SOAR - Threat & Vulnerability Management module contains several Home Page tabs. These tabs can be configured for various roles and then can be assigned to your users to complete their tasks. The following table lists the Home Page tabs available in the SOAR - Threat & Vulnerability Management module.

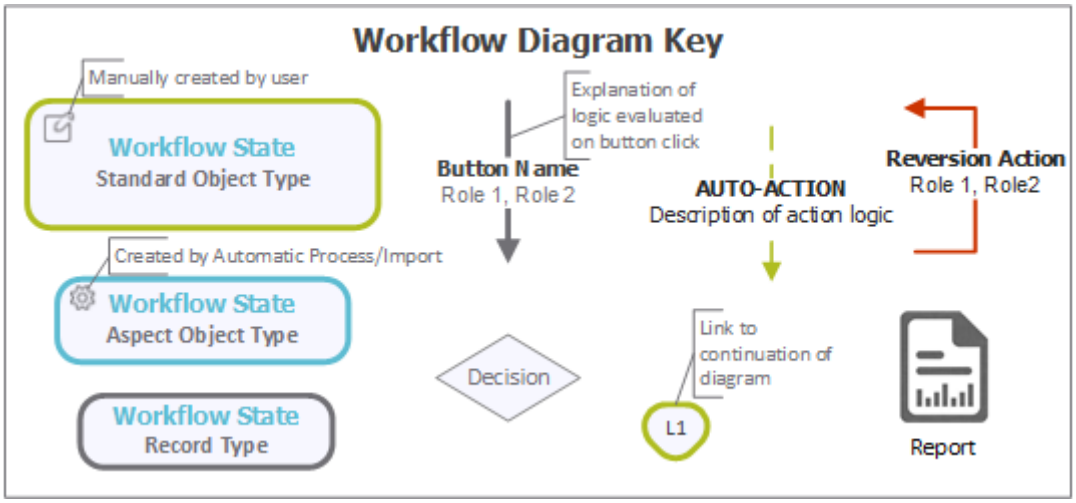
Home Page Tab	Description
VM: Vulnerability Management (grouping data)	Allows quick access to the sub-tabs available in the SOAR - VM module.
VM: Vulnerability Management Home	Provides quick access to various record categories, and quick search across the vulnerability data.
VM: Vulnerability Navigator	Provides multiple links to navigate to the vulnerability data. This is commonly used as a queue to address items in a specific workflow state or with a specific severity.
VM: Vulnerability Management Dashboard	Displays dashboards for hosts and vulnerabilities.
VM: Vulnerability Trends Dashboard	Displays the trend charts for vulnerabilities based on categories.
VM: Vulnerabilities Top 10 Dashboard	Provides access to various dashboards that show top 10 IT Hosts and top 10 vulnerabilities.
VM: Asset Navigator	Allows you to locate an asset (object) and to see all the SOAR - VM data related to that object (including the host & vulnerability information).
VM: Asset Dashboard	Provides access to various dashboards that show the following: • Hosts by operating system and zone • Open vulnerabilities by operating system • Trend of hosts by zone, workflow state, and hosts scanned by month

Home Page Tab	Description
VM: Vulnerability Management Libraries	Provides access to vulnerabilities available in the following categories: • Network zones • Knowledgebase • Knowledgebase with category grouping • Knowledgebase from last 30 days
TM: Threat Management (grouping tab)	Allows quick access to the sub-tabs available in the SOAR - TM module.
TM: Threat Management Home	Provides access to current and historic industry threat data and provides visualization of workflow states and trend of threats from threat feeds.
TM: Threat Navigator	Provides multiple views to better access and manage threat data by platform, workflow state, month, or severity.

SOAR-TVM Workflows

This section covers various details on Vulnerability Management and Threat Management baseline workflows in the SOAR - TVM module.

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

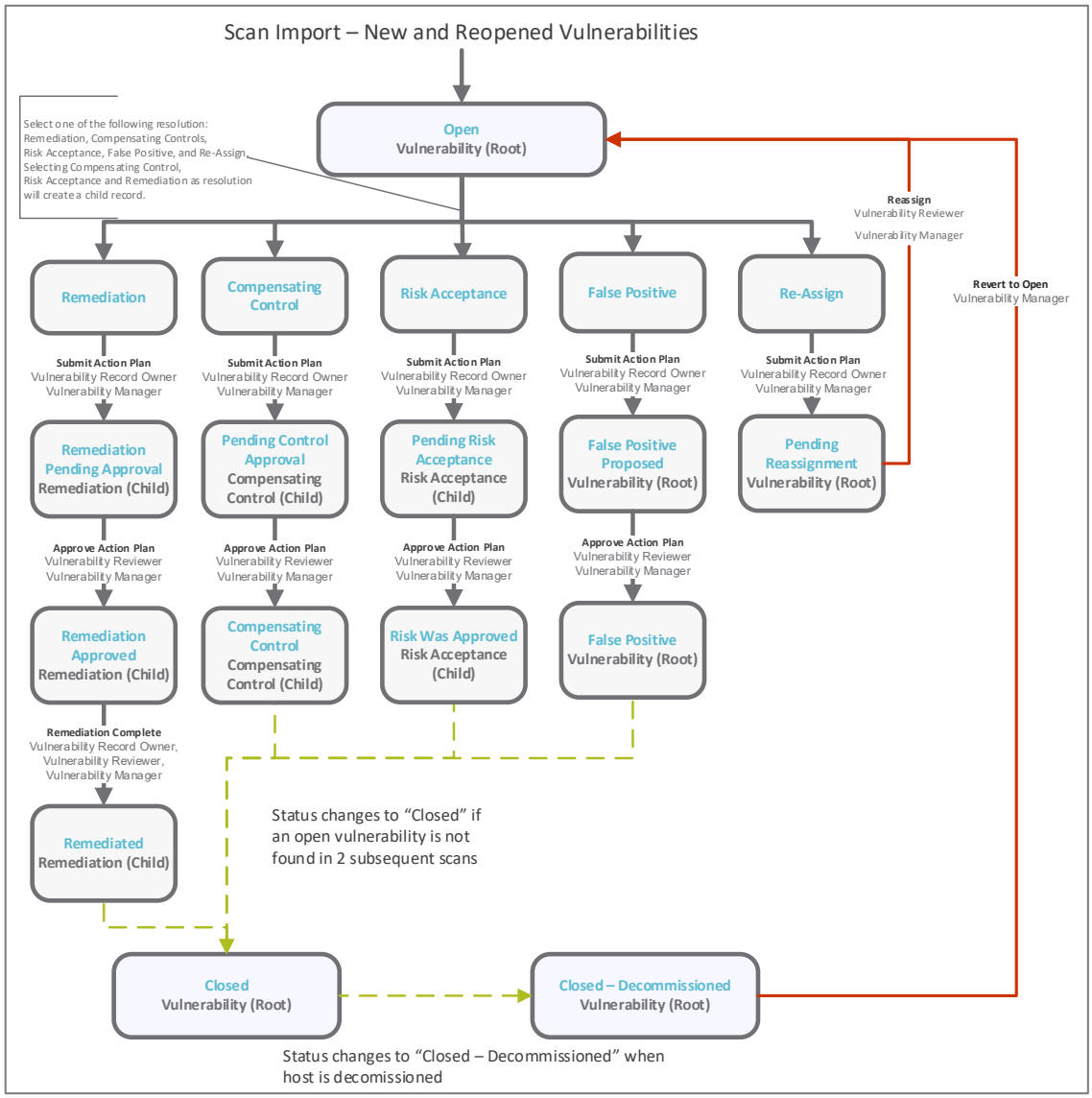


Vulnerability Management Workflow

This section covers the workflow diagram, states, roles, and buttons of the baseline Vulnerability Management workflow in the SOAR - TVM module.

Workflow Diagram

The following diagram represents the baseline Vulnerability Management workflow configured in the SOAR – TVM module.



Workflow States

The following table lists the workflow states associated with the baseline Vulnerability Management workflow.

Workflow State	Description
Open	A vulnerability enters this state when it is discovered. When in the open state, a vulnerability owner selects one of the action plans: False-Positive, Compensating Controls, Risk Acceptance, Remediation, and Reassign.
False Positive Proposed	A vulnerability enters this state when a *Vulnerability Owner* selects the False-Positive action plan and submits the action plan for approval.
Pending Control Approval	A vulnerability enters this state when a *Vulnerability Owner* selects the Compensating Controls action plan and submits the action plan for approval.
Pending Risk Acceptance	A vulnerability enters this state when a *Vulnerability Owner* selects the Risk Acceptance request action plan and submits the action plan for approval.
Remediation Pending Approval	A vulnerability enters this state when a *Vulnerability Owner* selects the Remediation action plan in the **Open** state and submits the action plan for approval
Pending Reassignment	A vulnerability enters this state when a *Vulnerability Record Manager* selects the Reassign action plan in the **Open** state and submits the action plan for the vulnerability to be assigned to an appropriate owner.
False Positive	A vulnerability enters this state when a vulnerability reviewer approves the proposed False-Positive action plan.
Compensating Control	A vulnerability enters this state when a *Vulnerability Reviewer* approves the Compensating Controls action plan.
Risk Was Accepted	A vulnerability enters this state when a *Vulnerability Reviewer* approves the pending Risk Acceptance Request action plan.
Remediation Approved	A vulnerability enters this state when a *Vulnerability Reviewer* approves the pending Remediation action plan.
Remediated	A vulnerability enters this state when a *Vulnerability Owner* marks the approved Remediation action plan as **Remediation Complete**.
Closed – Decommissioned	A vulnerability enters this state when an asset and/or a vulnerability has been marked as **Decommissioned**.

Workflow Roles

The following table lists the workflow roles to perform tasks associated with the workflow states in the baseline Vulnerability Management workflow.

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

User ID	Role	Description
r_vulnerability_owner	Vulnerability Record Owner	This role is assigned to a *Vulnerability Owner* to review the vulnerability and select an action plan. Some of the tasks that can be performed using this role include: • View assigned vulnerabilities • Submit Action Plan • Mark a vulnerability as remediated • Submit a status update • Mark a vulnerability as decommissioned
r_vulnerability_reviewer	Vulnerability Reviewer	This role is assigned to a *Vulnerability Reviewer* to approve an action plan. Some of the tasks performed using this role include: • View assets • View vulnerabilities • Approve / reject action plans for vulnerabilities that have been submitted by a *Vulnerability Owner* • Submit a status update • Mark a vulnerability as decommissioned
r_vulnerability_manager	Vulnerability Manager	This role is assigned to a *Vulnerability Manager* to assign vulnerabilities to the relevant owners (if not assigned automatically). By default, all the vulnerabilities and assets that are manually created or imported are assigned to a user with this role. Some of the tasks that can be performed using this role include: • View assets • Update asset details • View vulnerabilities • Assign vulnerabilities • Mark a vulnerability as decommissioned • Approve / Reject Action Plans for vulnerabilities that have been submitted by a vulnerability owner • Mark a vulnerability as remediated • Submit a status update

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Vulnerability Management workflow.

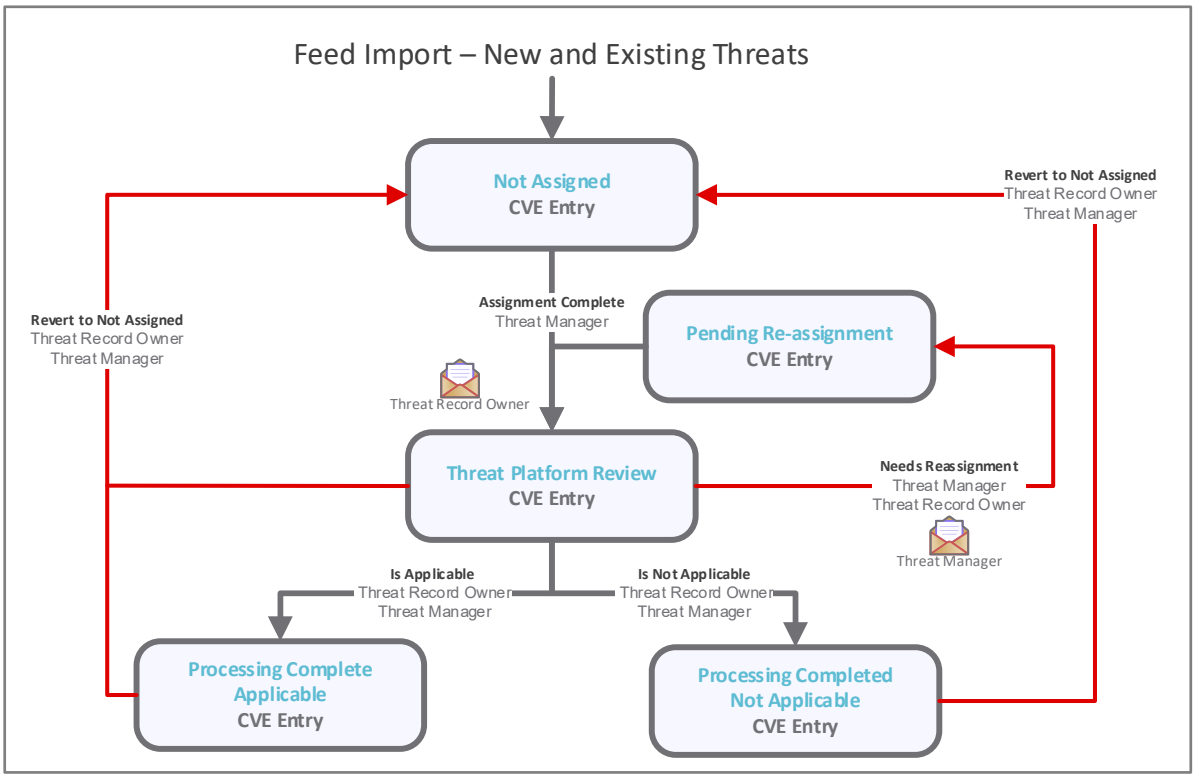
Button	Available to	Notification	Description
VM: Submit Action Plan	Vulnerability Owner Vulnerability Manager	Yes	Available in the **Open** state to select and submit the action plans.
VM: Approve Action Plan	Vulnerability Reviewer Vulnerability Manager	Yes	Available in the False Positive Proposed, Pending Control Approval, Pending Risk Acceptance, and Remediation Pending Approval states to approve the action plans
VM: Reject Action Plan	Vulnerability Reviewer Vulnerability Manager	Yes	Available in the False Positive Proposed, Pending Control Approval, Pending Risk Acceptance, and Remediation Pending Approval states to reject the action plans
VM: Reassign	Vulnerability Reviewer Vulnerability Manager	Yes	Available in the **Pending Reassignment** state to reassign a vulnerability to an appropriate owner.
VM: Remediation Complete	Vulnerability Owner Vulnerability Reviewer Vulnerability Manager	Yes	Available in the **Remediation Approved** state to mark a vulnerability as **Remediation Complete**.
VM: Submit Status Update	Vulnerability Owner Vulnerability Reviewer Vulnerability Manager	Yes	Available in the False Positive, Compensating Control, Risk Was Accepted, Remediation Approved, and Remediated states to provide a status update.
U: Show History	Vulnerability Owner Vulnerability Reviewer Vulnerability Manager	No	Available in all the states to view a log of vulnerability changes.
VM: Revert to Open	Vulnerability Manager	Yes	Available in all the states except the Open, Reassignment, and False Positive Proposed states.

Threat Management Workflow

This section covers the workflow diagram, states, roles, and buttons of the baseline Threat Management workflow in the SOAR - TVM module.

Workflow Diagram

The following diagram represents the baseline Threat Management workflow configured in the SOAR – TVM module.



Workflow States

The following is a list of states associated with the baseline Threat Management workflow.

Workflow State	Description
Not Assigned	A threat enters this state when it is imported. A *Threat Manager* has the ability to assign review for applicability to a threat record owner or decide whether or not the threat is applicable manually.
Platform Review	A threat enters in this state after a *Threat Manager* presses the assignment complete button for the record. The *Threat Record Owner* can decide whether or not the threat is Applicable or is NOT Applicable to the organization.

Workflow State	Description
Pending Re-Assignment	A threat enters this state when a *Threat Record Owner* clicks the **Needs Re-Assignment** button for this record. This will email the threat manager of the re-assignment.
Processing Completed	A threat enters this state when a *Threat Record Owner* or a *Threat Manager* clicks either the Is Applicable or Is NOT Applicable to the organization.

Workflow Roles

The following is a list of workflow roles to perform tasks associated with the states in the baseline Threat Management workflow.

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

User ID	Role	Description
r_threat_owner	Threat Record Owner	This role is assigned to a *Threat Owner* to review the threat and whether or not this threat is applicable to the organization. Some of the tasks that can be performed using this role include: • View assigned threats • Submit for Re-Assignment or Applicability • View Applicability, Reference, Products, and CVSS Details • Document Recommendations for addressing threats
r_threat_reviewer	Threat Reviewer	This role is assigned to a *Threat Reviewer* to review all threats.
r_threat_manager	Threat Manager	This role is assigned to a *Threat Manager* to assign threats to the relevant owners (if not assigned automatically). Some of the tasks that can be performed using this role include: • View all threats • Submit for Assignment, Re-Assignment, or Applicability • View Applicability, Reference, Products, and CVSS Details • Document Recommendations for addressing threats

In addition to the above roles, the Rsam installation package includes an administrative role, U: Object Administrator, as well as a sample user for that role, r_admin. This user has access to all record types, object types, workflow states, and workflow buttons across all Rsam baseline modules. Rsam Administrators should take necessary precautions to restrict standard users from accessing Rsam with this administrative role.

Workflow Buttons

The following is a list of buttons that are available in the various states of the baseline Threat Management workflow.

Button	Available to	Notification	Description
TM: Assignment Complete	Threat Manager	Yes	Available in the **Not Assigned** state to assign platform owner and submit assignment.
TM: Needs Reassignment	Threat Record Owner Threat Manager	Yes	Available in the **Platform Review** state to allow threats to be re-assigned.
TM: Is Applicable	Threat Record Owner Threat Manager	No	Available in the **Platform Review** state to allow threats to be applicable to the organization.
TM: Is NOT Applicable	Threat Record Owner Threat Manager	No	Available in the **Platform Review** state to allow threats to be not applicable to the organization.
TM: Revert to Not Assigned	Threat Manager	No	Available in the **Platform Review** and **Processing Complete** state.

Data Import

Default import maps have been created for the baseline record categories to help you import vulnerabilities and threats with little to no configuration required in your Rsam instance. Import maps allow you to link the data elements provided by your scanners to Rsam attributes. The maps are then associated with an import profile that stores the map, data source, and any required user credentials.

Import maps also determine the association of vulnerability data with Rsam objects. You can use application or host/asset objects to organize related vulnerabilities. Or, as mentioned in the Variations in the Data Structure section, one library object can be used to house all vulnerability data. You can use the Rsam default mappings or create new mappings to meet your specific goals.

Asset Import

Asset inventories can be scheduled for import from a scanning tool or other asset management data sources. Rsam utilizes import profiles and maps to specify the data sources and define how the asset data should be mapped to attributes. These are configured only one-time and can be reused in the future.

Importing asset inventories prior to importing scan data allows Rsam to identify potential decommissioned assets or rogue devices based on the asset import. This works as explained in the following steps:

1. Assets will be in the **Active** workflow state on importing from a data source.
2. Assets that are no longer available after subsequent imports will be transitioned to the **Decommissioned** workflow state. In addition, all the associated vulnerabilities will be marked as **Closed – Decommissioned**.
3. If the asset reappears in a subsequent asset import or through a vulnerability scan, it will be marked as **Active**.
4. If an asset is found during a vulnerability scan, but does not already exist in Rsam, it is marked as **Newly Identified Asset**.

Note: More reliable results can be obtained if assets are imported prior to importing vulnerabilities.

To provide more robust reporting, asset information can be manually entered or imported from scanning tools. Some of the examples are as follows:

1. Import Network Zones/IP Subnets for categorization of an asset based on IP address.
2. Assign responsible parties based on operating system.
3. Document applications hosted on asset.
4. Select criticality factors such as data classification to use in adjusting the risk rating of associated vulnerabilities.

Vulnerabilities and Findings Import

Rsam can schedule and automatically import scan results on a recurring basis. Rsam utilizes import profiles and import maps to select the data sources and define how the scan results should be mapped to attributes. These are configured only one-time and allow imports to recur automatically in future.

Data can be imported using any of the following methods:

1. Files such as XML, Delimited Text, and Excel can be placed in a shared directory on the web server to schedule imports.

2. API connection to scanner console such as Qualys, Nexpose, Tenable, and Veracode APIs.

3. URL-based API calls to scanner console such as Splunk and WhiteHat.

4. Query from an OLEDB data source such as SQL, Oracle, and Access databases.

Each data source contains a pre-configured map that identifies a baseline set of data elements to be imported. While each data source may provide different data elements in the output, the maps include common data elements across these data sources to take advantage of the search and reporting capabilities of Rsam.

The maps define a unique identifier that Rsam will use to designate a new vulnerability from an existing vulnerability. Common unique IDs consist of *Vulnerability ID + Port + IP Address*. For summary imports related to workstations or network devices, the unique ID consists of *Vulnerability ID + Port*.

During an import, handlers are executed to perform the following actions:

- Assign *Vulnerability Owner* based on vulnerability data elements (for example, technology)
- Translate reported scanner severity rating to Universal Severity rating
- Set Exploitable flag
- Set Required Due Dates
- Send email to Vulnerability Managers
- Calculate internal risk ratings
- Track the number of times a remediated vulnerability reappears in a scanner

Import Profiles Optimization

Rsam can manage large volumes of records and it is quite common in the SOAR – VM module. There are several best practices to consider when it comes to optimizing your data import.

While import maps allow you to filter the output returned by data sources, it is recommended to filter the output within your data source first. For example, if you only wish to import vulnerabilities with a severity rating of 3 or above, the scanner output that you want to import should contain only the data meeting your criteria. If no filter is available at the scanner level, set the filters on the **Filter** tab available within an import map.

Another best practice is to use the Rsam Scheduler when running imports containing a large amount of data. Because importing the data using the Rsam Scheduler utilizes the server resources and takes less time to complete the import job. You can also manually import using the web interface. However, you may encounter insufficient memory or timeout errors due to limitations on system requirements.

Refer the *Rsam Performance Guide*, which covers best practices in managing handlers, identifiers, and other configuration elements that affect SOAR – VM module performance.

Imports Schedule

Once you have determined the data that you want to import, you must choose a frequency at which the imports should occur. Imports can be scheduled using the Rsam Scheduler and the saved import profile to seamlessly automate the imports. Imports can also be run manually at any time.

With recurring imports, you can easily update existing vulnerabilities housed in Rsam. This functionality can update existing attributes with most recent scan data (that is an updated fix / resolution for a vulnerability), or can close findings that are not found in subsequent scans. Also, implies that a host may be unavailable in subsequent scans; therefore, configurations in the SOAR – VM module uses a threshold to flag vulnerabilities. For instance, if your organization scans once a month, Rsam will set the workflow state of vulnerabilities not found since two months of the last scan to **Closed – Remediated**. This is especially useful for scanners that do not report vulnerabilities as remediated if a host is decommissioned.

If a vulnerability is marked as **Closed – Remediated** or **Closed – Decommissioned** and is found again in a subsequent scan, Rsam changes the workflow state to **Open** and increments the Reopen Counter on the **Metadata** tab of a vulnerability record.

Auto Assigning Vulnerabilities

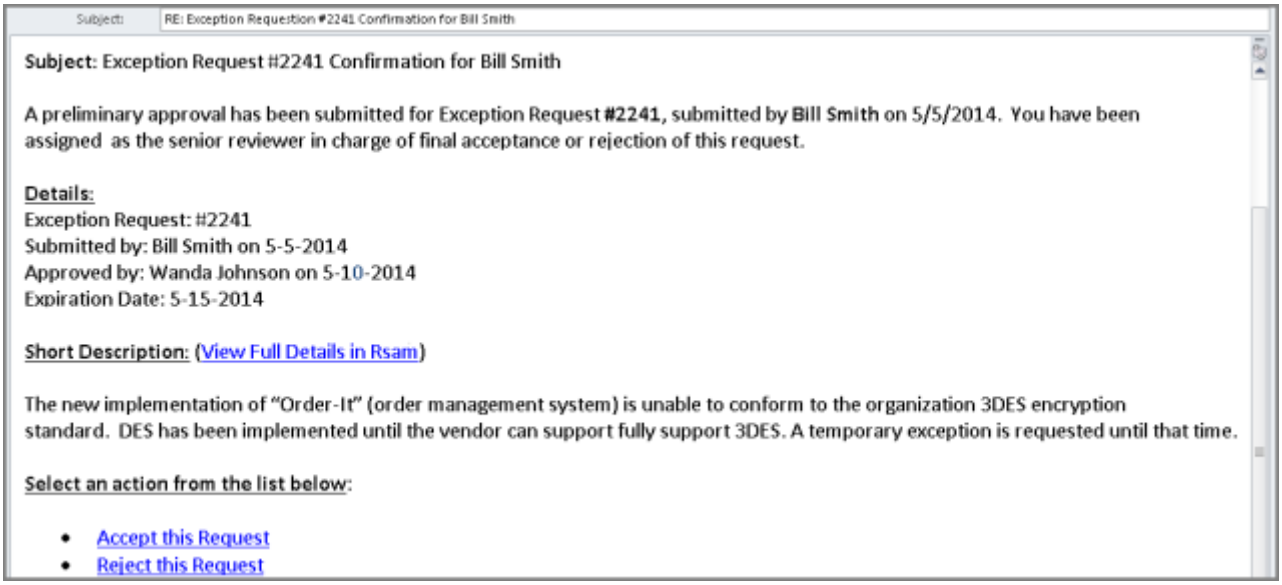
In addition to assigning the asset owners to vulnerabilities manually, Rsam provides the ability to automatically assign owners to individual vulnerabilities based on a specific keyword imported from the data source. This method is commonly used for technologies by the team responsible for addressing risks on those technologies. For example, Java, Adobe, Apache, and SQL are some of the most common technologies that are assigned using this method.

Note: Managing your Rsam instance with many individually assigned vulnerabilities can affect the overall performance of your Rsam instance. Rsam recommends assigning the owners at the object level or at a higher level. Otherwise, consider to upgrade your system requirements. For more information, please refer the *Rsam Performance Guide*.

Appendix 1: 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 follow image illustrates an example notification template that has custom text, data from the record, embedded links to the application, and Offline Decision Making actions.

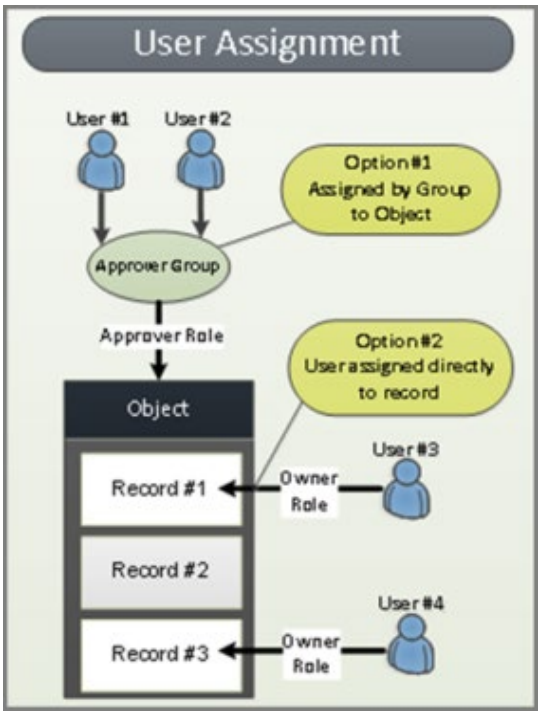


Appendix 2: User Assignment Options

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- Threat & Vulnerability Management Module Tutorial

For a detailed walk-through of the SOAR-Threat & Vulnerability Management Module user experience, refer the *SOAR- Threat & Vulnerability Management Module Step-by-Step Tutorial*. You should have received the *SOAR- Threat & Vulnerability Management Module Step-by-Step Tutorial* along with the SOAR-Vulnerability Management Module instance. If not, contact your Rsam Customer Representative to obtain an electronic copy of the *SOAR- Threat & Vulnerability Management Module Step-by-Step Tutorial*.

Online Help

This document provides an overview of the SOAR- Threat & Vulnerability Management Module configuration. 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.