



Rsam Supplemental Guide

SOAR - Threat and Vulnerability Management Vulnerability Import Maps

Document Version: 2017.06.19

June 2017

Contents

About This Document-----	3
About Import Maps -----	3
Predefined Vulnerability Import Maps-----	4
General Tab -----	8
Configuration Items for Dynamic Object Selection Type -----	9
Map Tab -----	12
Filter Tab -----	13
Action Tab -----	15
Import Mode -----	15
Workflow buttons-----	15
Unique ID Tab -----	17
Definition Tab -----	18
Translate Tab -----	19
Management Tab -----	20
Save Import Mapping-----	20
Save Profile-----	20
Predefined High-Volume Vulnerability Import Maps-----	22
Using a Source Identifier -----	23

About This Document

Rsam Integration Guides provide you with the information you need to understand how to use the pre-defined configurations to import data for a particular module. These guides should be referred to gain a better understanding of how the integration is configured and can be leveraged “out-of-the-box”.

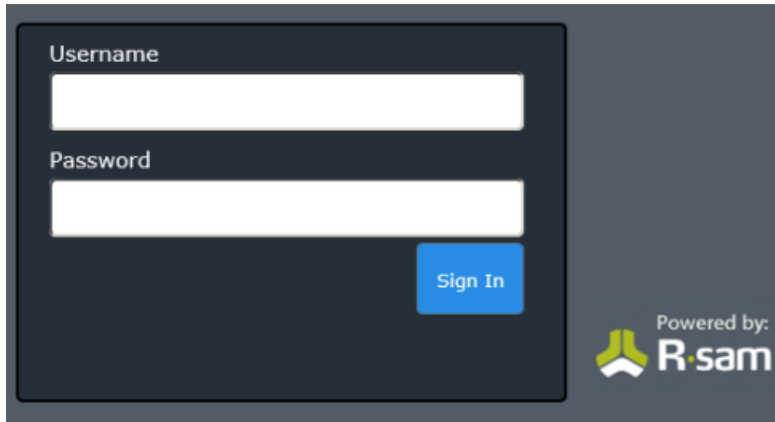
About Import Maps

Rsam’s Security Operations Analytics Reporting Threat and Vulnerability Management (SOAR-TVM) solution contains predefined maps that can be used to import assets and/or vulnerabilities from different sources. Predefined maps are available for all Out-of-the-box (OOTB) Connectors; however, you can also create your own maps in Rsam. This document will guide you through the predefined mapping configurations.

Predefined Vulnerability Import Maps

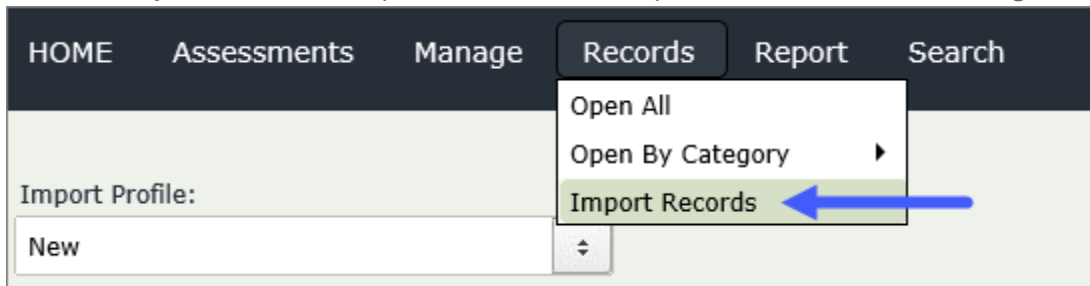
Rsam provides predefined import maps, which you may need to typically customize once to cater to your specific environment requirements. To review and/or update predefined maps, perform the following steps:

1. Log in to Rsam, using an Administrative account or an account that has been granted the privileges to perform imports.

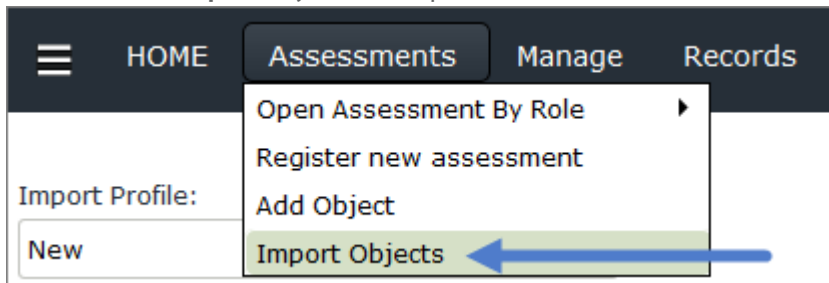


2. Navigate to the required screen:

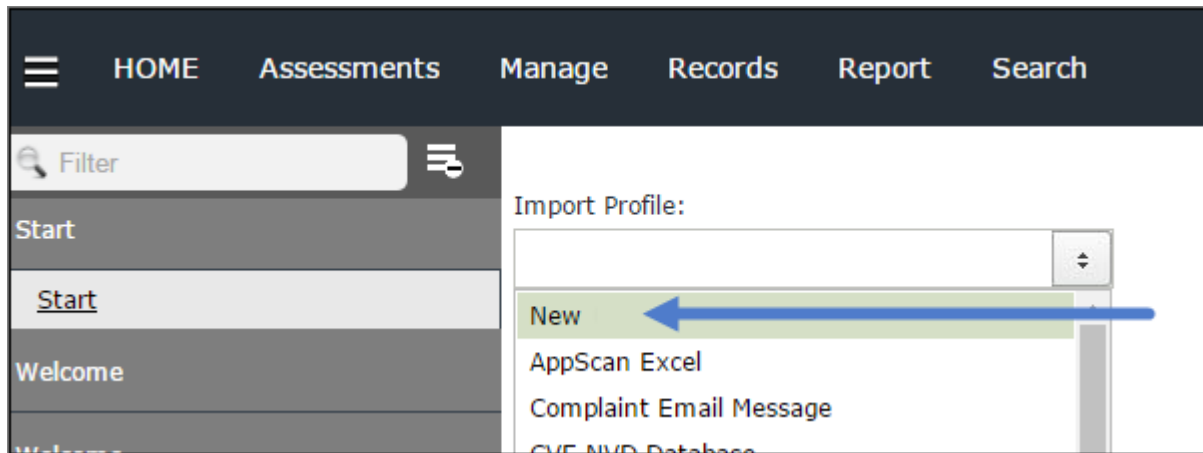
- **Records > Import Records** - To import vulnerabilities, compliance results and the Knowledgebase.



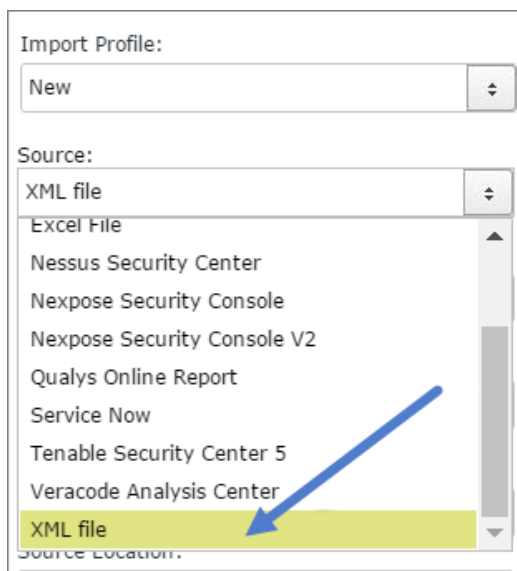
- **Assessments > Import Objects** - To import Asset data.



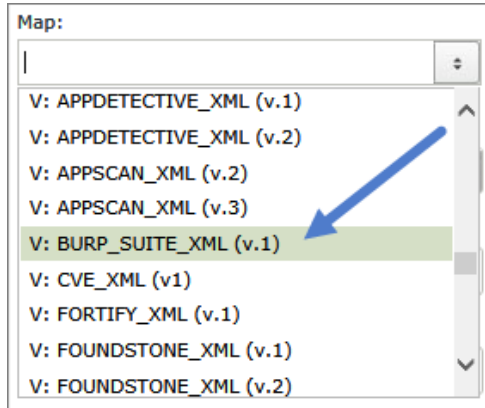
3. Select **New** in the **Import Profile** field. Initially a profile will not be configured; however, a profile can be saved to allow for scheduled imports to occur.



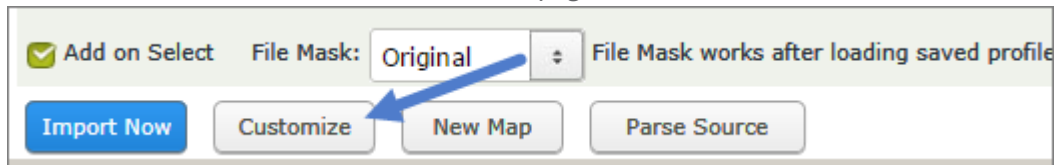
4. Select the desired source applicable for your import type in the Source field.



5. Select the corresponding map from the drop-down available in the **Map** field.



6. Load the data to be imported depending on which import source you are using
 - API – Make the required selections as per the appropriate Integration Guides.
 - Downloaded file (i.e., XML, Excel, Delimited) - Click **Browse**, navigate to the location where the required file is available, and select the file.
7. Click **Customize**, available at the bottom of the page.



The page refreshes to show all the options to customize your import. You can select the required tab and customize the import.

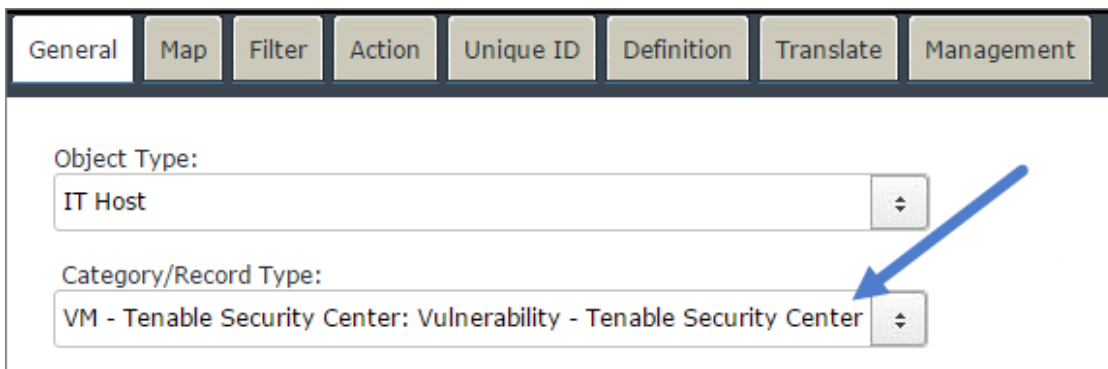
Source Schema ▼ ExternalData ▼ Row Issue_ID Date_Reported Issue_Short_Description Issue_Category	RSAM Record Types ▼ VM: Vulnerability - Burp Suite Workflow Notes Date Opened Open / Closed Days to Closure Required Required Closure Date Days Open Date Closed
General Map Filter Action Unique ID Definition Translate Management	
Object Type: IT Host	Object:
Category/Record Type: 	
Object selection type: Static Object	

General Tab

The General tab helps you to select the object type you want to associate the imported vulnerability records with. Most customers import their vulnerabilities into the IT Host object type, although vulnerabilities can be imported into a single library object. All imported vulnerabilities will be associated with this specific object type which you select in the General tab.

To select the Object Type and Record Type mapping, perform the following steps:

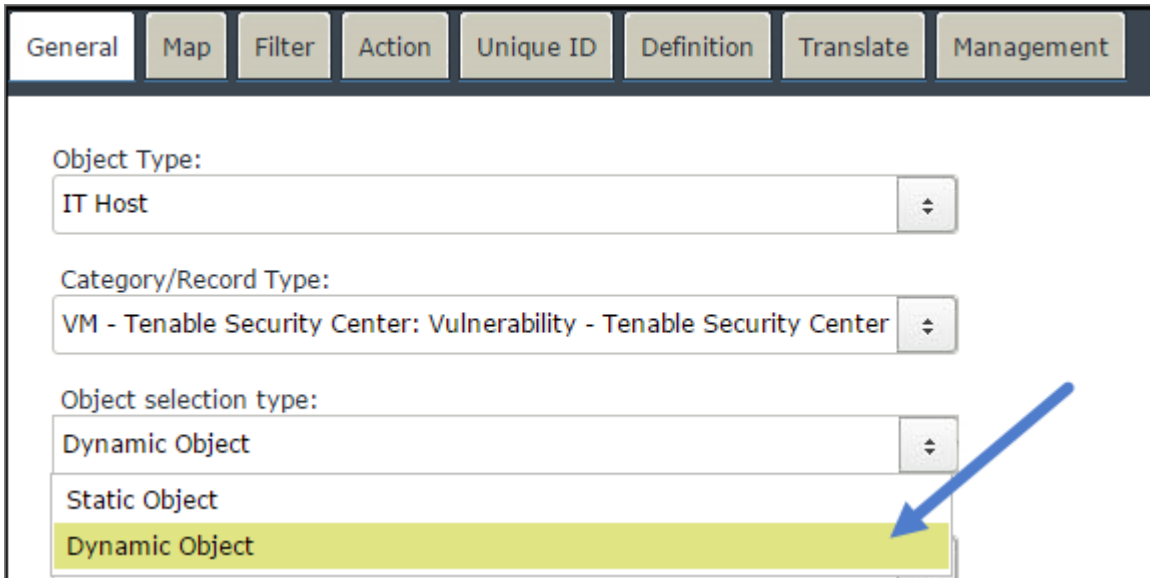
1. Click the **General** tab. The tab is selected by default when the page appears.
2. Select **IT Host** from the **Object Type** drop-down list.
3. Select the Category and Record Type designated for the import of the vulnerability data. This category type should correspond to the data source. Only the Category/Record types associated with the selected object type are listed.



The screenshot shows a software interface with a top navigation bar containing tabs: General, Map, Filter, Action, Unique ID, Definition, Translate, and Management. The 'General' tab is active. Below the tabs, there are two dropdown menus. The first is labeled 'Object Type:' and has 'IT Host' selected. The second is labeled 'Category/Record Type:' and has 'VM - Tenable Security Center: Vulnerability - Tenable Security Center' selected. A blue arrow points to the second dropdown menu.

4. Select the required value from the Object selection type drop-down list. The options available are as follows:
 - **Static Object** - Select this option if you wish to specify the object, such as a vulnerability library, where you wish to record all vulnerabilities for all hosts.
 - **Dynamic Object** - Select this option to dynamically create or match existing objects for which to associate the reported vulnerabilities. To perform the match, this selection requires an identifier to be reported in the importable data source. For example, the object's name or attribute is listed in the data source.

The pre-defined maps in the SOAR-TVM baseline use **Dynamic Object** as the default setting.



General | Map | Filter | Action | Unique ID | Definition | Translate | Management

Object Type:
IT Host

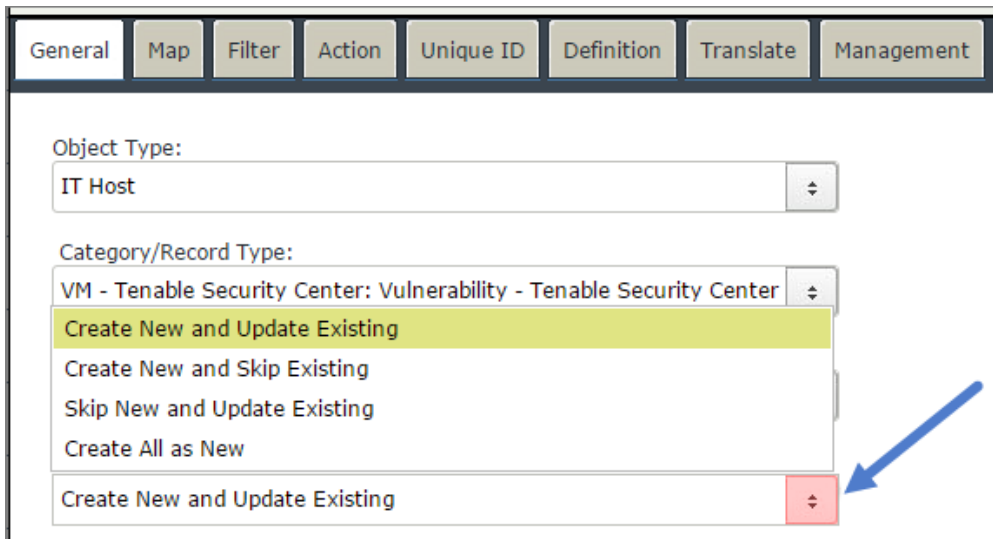
Category/Record Type:
VM - Tenable Security Center: Vulnerability - Tenable Security Center

Object selection type:
Dynamic Object
Static Object
Dynamic Object

Note: If you select **Static Object**, you can skip the steps mentioned in the [Map Tab](#) section.

Configuration Items for Dynamic Object Selection Type

1. Choose the Object Creation Mode (Applicable for Dynamic Object Selection Type ONLY).



General | Map | Filter | Action | Unique ID | Definition | Translate | Management

Object Type:
IT Host

Category/Record Type:
VM - Tenable Security Center: Vulnerability - Tenable Security Center
Create New and Update Existing
Create New and Skip Existing
Skip New and Update Existing
Create All as New
Create New and Update Existing

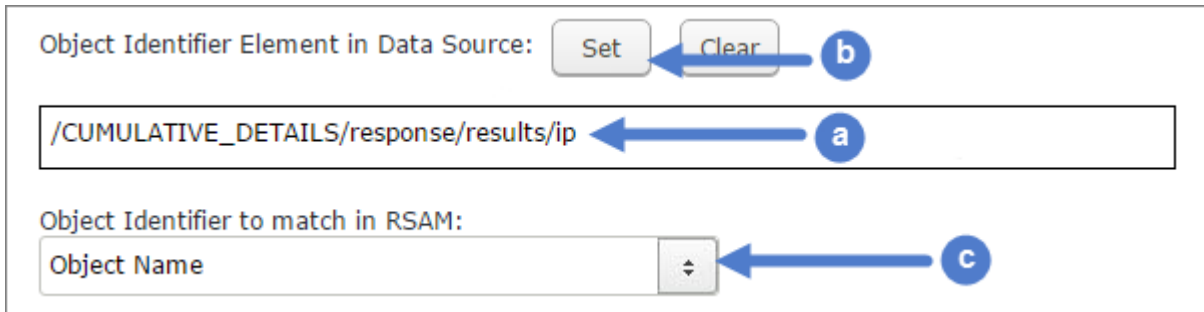
The options are:

- **Create New and Update Existing** - Creates an IT Host object if new hosts are reported in the scan results and links vulnerabilities to that IT Host object. Vulnerabilities related to existing hosts are created or updated.

- **Create New and Skip Existing** - Vulnerabilities will only be imported for new hosts scanned that do not currently exist in Rsam.
- **Skip New and Update Existing** - Only imports vulnerabilities into IT Host objects that already exist in Rsam. If a new IT host is scanned and included in the scan results, the vulnerabilities will not be imported into Rsam.
- **Create All As New** - Creates a new IT Host object for every host reported in the scan results and links vulnerabilities to that IT Host object. Ignores any existing hosts.

The pre-defined maps in the SOAR-TVM baseline use **Create New and Update Existing** as the default option.

- Set the value that should be used to properly identify each unique object in the **Object Identifier Element in Data Source** section:
 - Select the source (XML) element path that contains the value which will identify the object that the imported vulnerabilities will be linked to.
 - Click **Set** to save the selection.
 - Select the Object Identifier in the **Object Identifier to match in Rsam** field. This can be the object name or an attribute within the IT Host object.



Object Identifier Element in Data Source: **b**

a

Object Identifier to match in RSAM:

c

- Choose the **Entity selection type** where the objects are to be created.



Entity selection type:

Entity:

The options available are as follows:

- **Static Entity** – Rsam will create or match IT Host objects (as defined above) under the sub-entity selected in the ‘Entity’ drop-down. Note that if an object exists under a different sub-entity, it will be ignored.



- **Dynamic Entity** - Rsam will create or match IT Host objects (as defined above) under the sub entity matching a value returned in the scan results. The sub-entity name must be available in the scan result output to properly match the IT Hosts across those entities dynamically.

If the entity is not available in the scan results, you will need to create multiple maps using the Static Entity selection and point to the corresponding entity. This also requires the scan results to be filtered to return only the vulnerabilities associated with hosts for the selected entity.

A Source Identifier may also need to be included in each map, as well, to avoid the possibility of inadvertently closing a vulnerability under an incorrect host. See the [Using a Source Identifier](#) section for more details.

An example for using this configuration would be when a customer’s organizational structure and management teams are segregated by region (i.e., Canada, US). Separate sub-entities for each region would restrict responsible teams to manage IT Host objects and related vulnerabilities in their assigned sub-entity without the need for assigning permissions at the object level.

- Select **Dynamic Entity** in the Entity selection type.
- Provide the source (XML) element path to match the identifier against and click **Set**.



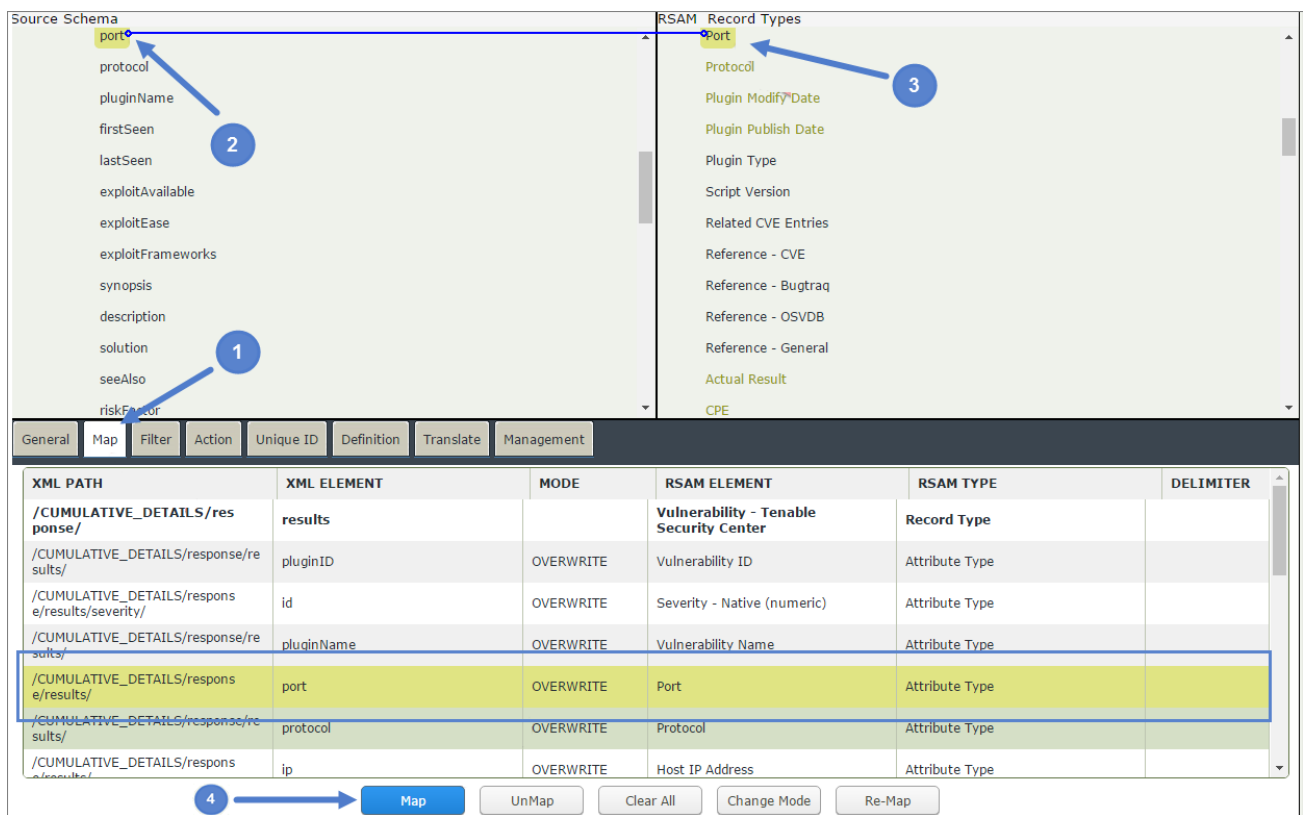
The pre-defined maps in the SOAR-TVM baseline use the default setting of **Static Entity** and **Threat and Vulnerability Management** entity.

Map Tab

The Map tab defines which data elements from the import file will map to the selected attributes in Rsam.

To use the map tab, perform the following steps:

1. Click the **Map** tab.
2. Select the Source Data Point on the left.
3. Select the Rsam Record Attribute Destination on the right.
4. Click the **'Map'** button at the bottom. This saves the mapping, and adds it in the list.



The screenshot shows the 'Map' tab interface. On the left, the 'Source Schema' pane lists various XML elements, with 'port' selected (indicated by a blue circle '2'). On the right, the 'RSAM Record Types' pane lists various attributes, with 'Port' selected (indicated by a blue circle '3'). Below these panes is a table with columns: XML PATH, XML ELEMENT, MODE, RSAM ELEMENT, RSAM TYPE, and DELIMITER. The table contains several rows, with the row for 'port' highlighted in yellow (indicated by a blue circle '4'). At the bottom, there are buttons for 'Map', 'UnMap', 'Clear All', 'Change Mode', and 'Re-Map'.

XML PATH	XML ELEMENT	MODE	RSAM ELEMENT	RSAM TYPE	DELIMITER
/CUMULATIVE_DETAILS/response/	results		Vulnerability - Tenable Security Center	Record Type	
/CUMULATIVE_DETAILS/response/results/	pluginID	OVERWRITE	Vulnerability ID	Attribute Type	
/CUMULATIVE_DETAILS/response/results/severity/	id	OVERWRITE	Severity - Native (numeric)	Attribute Type	
/CUMULATIVE_DETAILS/response/results/	pluginName	OVERWRITE	Vulnerability Name	Attribute Type	
/CUMULATIVE_DETAILS/response/results/	port	OVERWRITE	Port	Attribute Type	
/CUMULATIVE_DETAILS/response/results/	protocol	OVERWRITE	Protocol	Attribute Type	
/CUMULATIVE_DETAILS/response/	ip	OVERWRITE	Host IP Address	Attribute Type	

Note: Additional configurations are typically not necessary beyond this point, however more configuration details are provided below.

Filter Tab

The Filter tab allows you to create specific data filters when importing data. Only data that matches **ALL** filters will be imported.

Note: It is always most efficient to filter the data source before it gets to Rsam for import. However, use Rsam’s filtering capabilities when the data source does not allow the same filtering capability as the Rsam import options.

Rsam accepts XML compatible filter expressions. The following are common expressions:

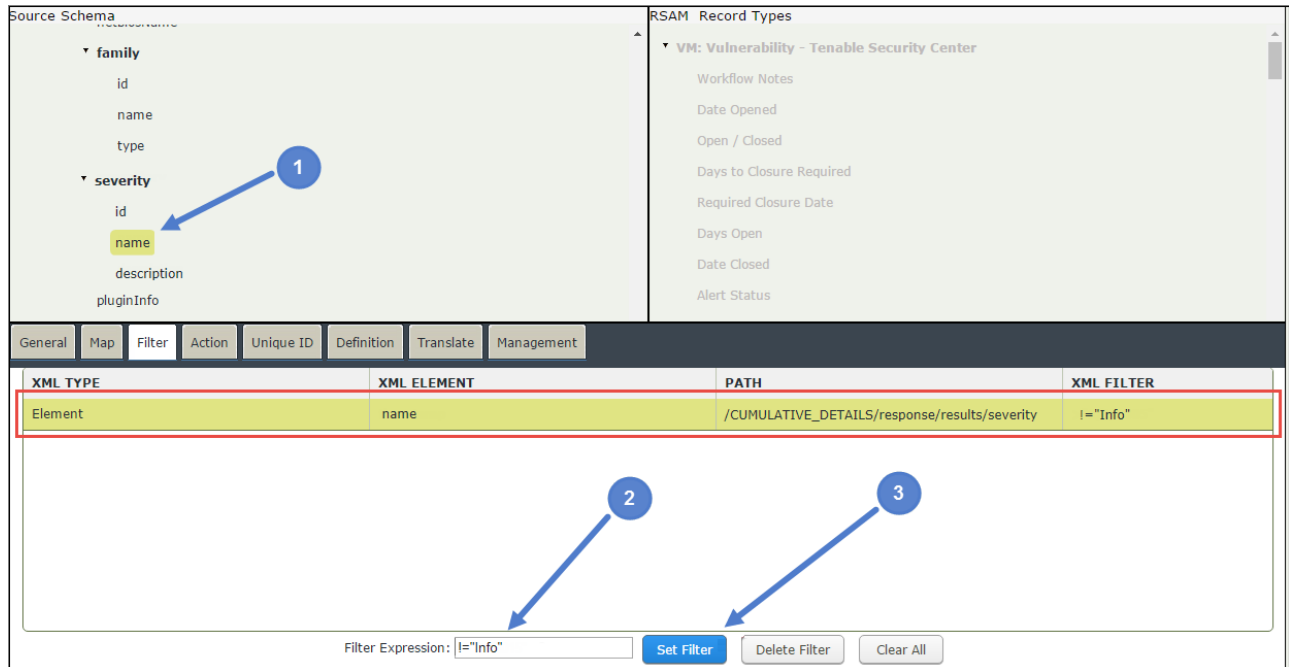
- = Data Value
- > Data Value
- < Data Value
- <> Data Value
- IN (LIST OF VALUES)

General Map Filter Action Unique ID Definition Translate Management			
XML TYPE	XML ELEMENT	PATH	XML FILTER
Attribute	severity	/TENABLE_SECURITY_CENTER5 /NessusClientData_v2/Report/ReportHost /ReportItem	>1

To set a new filter, perform the following steps:

1. Select the Source Schema on the left that needs to be filtered.
2. Enter a filter expression using the examples mentioned above.

3. Click **Set Filter**.



Source Schema

- family
 - id
 - name
 - type
- severity
 - id
 - name
 - description
 - pluginInfo

RSAM Record Types

- VM: Vulnerability - Tenable Security Center
 - Workflow Notes
 - Date Opened
 - Open / Closed
 - Days to Closure Required
 - Required Closure Date
 - Days Open
 - Date Closed
 - Alert Status

General | Map | Filter | Action | Unique ID | Definition | Translate | Management

XML TYPE	XML ELEMENT	PATH	XML FILTER
Element	name	/CUMULATIVE_DETAILS/response/results/severity	!=\"Info\"

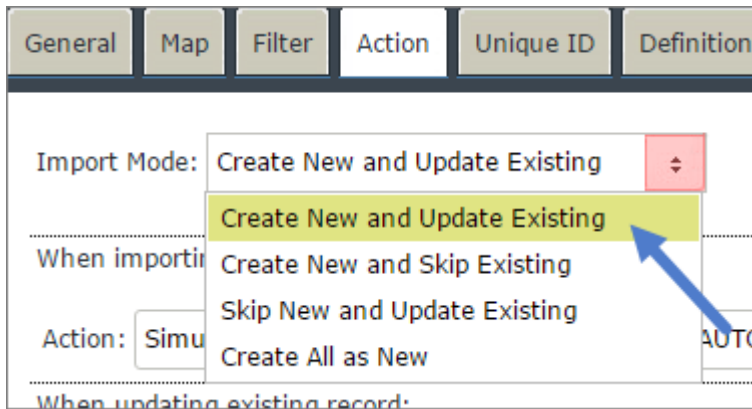
Filter Expression: !=\"Info\"

Set Filter | Delete Filter | Clear All

Action Tab

The Action tab displays the import modes, as well as, the workflow buttons that are pre-configured with the preconfigured map.

Import Mode



The options available are as follows:

- **Create New and Update Existing** - Creates new vulnerabilities and updates existing vulnerabilities.
- **Create New and Skip Existing** - Creates only new vulnerabilities, existing vulnerabilities are ignored.
- **Skip New and Update Existing** - Only updates existing vulnerabilities, new vulnerabilities are ignored.
- **Create All as New** - Create all vulnerabilities as new records.

The pre-defined maps in the SOAR-TVM baseline use **Create New and Update Existing** as the default setting.

Workflow buttons

Customers can review these buttons and the handlers associated with them and adjust as desired. Some of the default actions triggered during the imports are as follows:

- Severity rating is translated to a Universal Severity rating attribute
- Required closure dates based on the severity are calculated (i.e., High requires closure in 90 days)
- Sets date last imported
- Various metric attributes are set to be used for future trending
- Close vulnerability if vulnerability is absent from 2 consecutive scan imports

The Filter tab allows you to create specific data filters when importing data. Only data that matches **ALL** filters will be imported.

Note: By default, importing existing vulnerabilities or vulnerabilities no longer found will not alter the **workflow states** of those vulnerabilities already housed in Rsam. For example, if a vulnerability was declared a false positive during import #1, it will not revert to Open during import #2. This can be configured differently if desired.

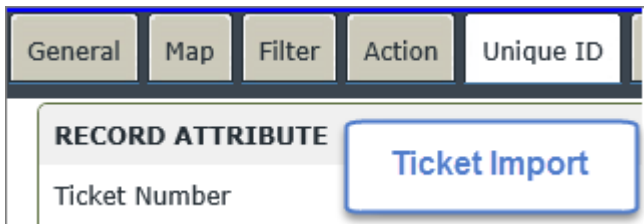
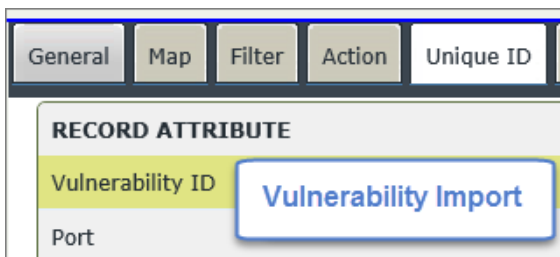
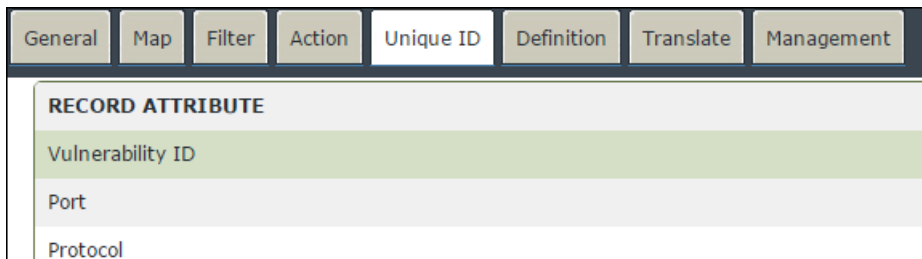
Default workflow buttons for vulnerability imports are as follows:

- New vulnerability is imported - **AUTO: Vulnerability Import (New)**
- Existing vulnerability is imported - **AUTO: Vulnerability Import (Existing)**
- Existing vulnerability is not reported in the result set - **AUTO: Vulnerability Import (No Longer Existing)**

General	Map	Filter	Action	Unique ID	Definition	Translate	Management
Import Mode: <input type="text" value="Create New and Update Existing"/> <input type="checkbox"/> Bind all saved search attributes after import (will take longer to execute imports)							
When importing a new record:							
Action:		<input type="text" value="Simulate Workflow Button"/>		Workflow:		<input type="text" value="AUTO: Vulnerability Import"/>	
When updating existing record:							
Action:		<input type="text" value="Simulate Workflow Button"/>		Workflow:		<input type="text" value="AUTO: Vulnerability Import"/>	
When unmatched record found:							
Action:		<input type="text" value="Simulate Workflow Button"/>		Workflow:		<input type="text" value="AUTO: Vulnerability Import"/>	
Stored procedure to run at the end of the import:							
<input type="text"/>							

Unique ID Tab

The Unique ID tab defines what constitutes a new vulnerability. The object as defined earlier in the **Object Identifier to match in RSAM** section on the General tab is inherently taken into account as part of the unique ID.



The pre-defined maps in the SOAR-TVM baseline use **Vulnerability ID** and **Port** as the default settings.

Definition Tab

The Definitions tab is used to import data which is stored in two disconnected sections of the data source file (i.e., appendix or glossary). A unique ID must exist between the two sections and must be mapped on the Map tab and Definition tab. This attribute must be mapped in Definition ID mode on the Definition tab for Rsam to establish the relationship.

While this is not common, there are predefined maps, such as Nexpose, that will include definition mappings.

Source Schema version

- scans
- ▾ nodes
 - node
 - ▾ VulnerabilityDefinitions
 - ▾ vulnerability
 - id
 - title

General
Map
Filter
Action
Unique ID
Definition
Translate
Management

XML PATH	XML ELEMENT	MODE	RSAM ELEMENT
/NexposeReport/VulnerabilityDefinitions/	vulnerability		Vulnerability - NeXpose
/NexposeReport/VulnerabilityDefinitions/vulnerability/	id	DEFINITION ID	Vulnerability ID
/NexposeReport/VulnerabilityDefinitions/vulnerability/	title	OVERWRITE	Vulnerability Name
/NexposeReport/VulnerabilityDefinitions/vulnerability/	cvssScore	OVERWRITE	CVSBase Score

Translate Tab

The Translate tab is used to replace text/characters in a mapped text attribute and/or map values returned in the XML results to the mapped attribute values in Rsam. The attribute types which may require translation include checkbox, listbox, multi-select and radio buttons.

Some predefined maps include translation entries based to correctly match values mapped from the data source results.

Example

General	Map	Filter	Action	Unique ID	Definition	Translate	Management
XML TYPE	XML ELEMENT	PATH	ORIGINAL_VALUE	NEW VALUE	FULL REPLACE	CASE SENSITIVE	
Element	exploitAvailable	/CUMULATIVE_DETAILS /response/results/	true	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Element	exploitAvailable	/CUMULATIVE_DETAILS/res ponse/results/	false	No	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

The **exploitAvailable** value is mapped to the Exploitable attribute (defined on the Map tab). The values returned for the exploitAvailable XML element are **true** and **false**. Since the Exploitable attribute values in Rsam are **Yes** and **No**, the translations entered above will map the correct value respectively.

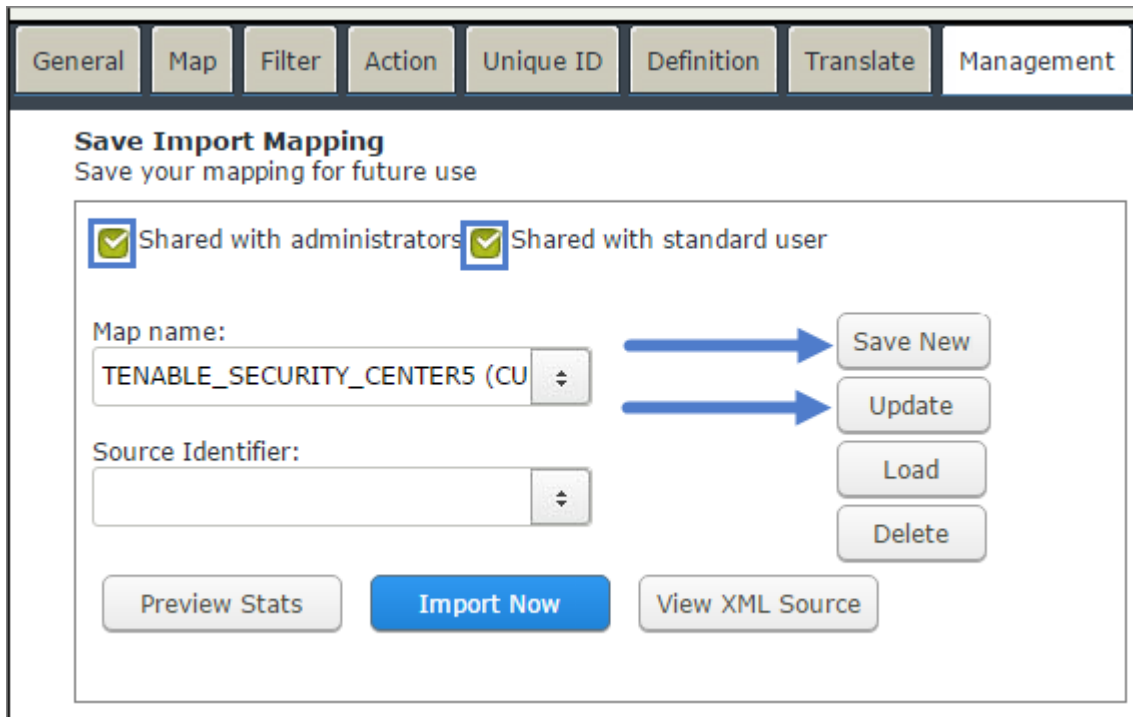
Management Tab

The Management tab allows you to update or save a new map and/or profile. The map includes all the settings on each tab described above. The profile includes the map selected and any information provided on the initial import screen.

Save Import Mapping

To save the import mapping configuration, perform the following steps:

1. Click the **Management** tab to save the map, profile, and preview the import results. If you are updating a map or saving a new map, and the map is to be associated with a profile, you must save the map first and then save the profile.
2. Be sure to select the checkbox corresponding to **Shared with administrators** if saving a new profile to allow all Rsam administrators to view the profile.
3. Select the checkbox corresponding to **Shared with standard user** if any non-admins will be performing these imports.
4. Click **Update** to update the currently selected mapping or click **Save New** to be prompted for a new mapping name.



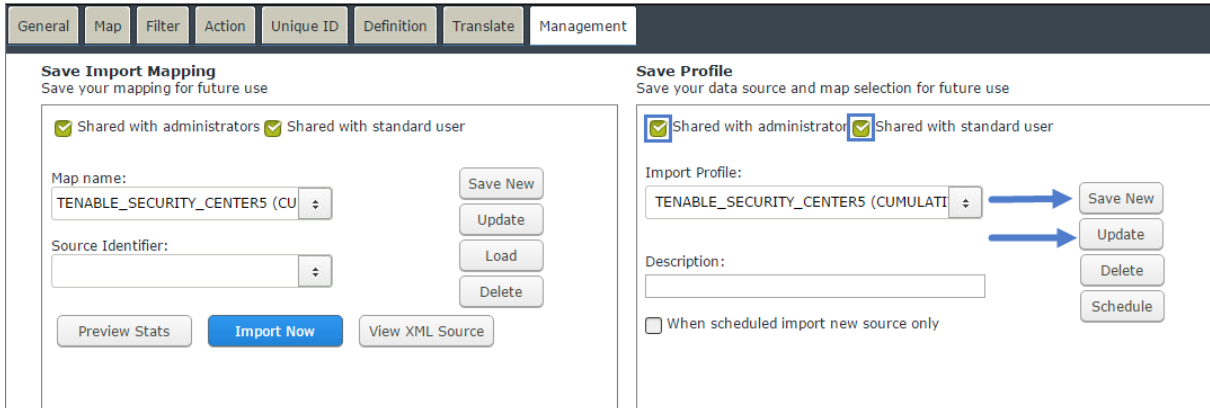
Save Profile

After saving the map, you can save a profile (on the right-hand side of the Management tab) to be used for scheduled imports. A profile saves all information entered into the initial import screen (i.e., credentials, mode, and map).

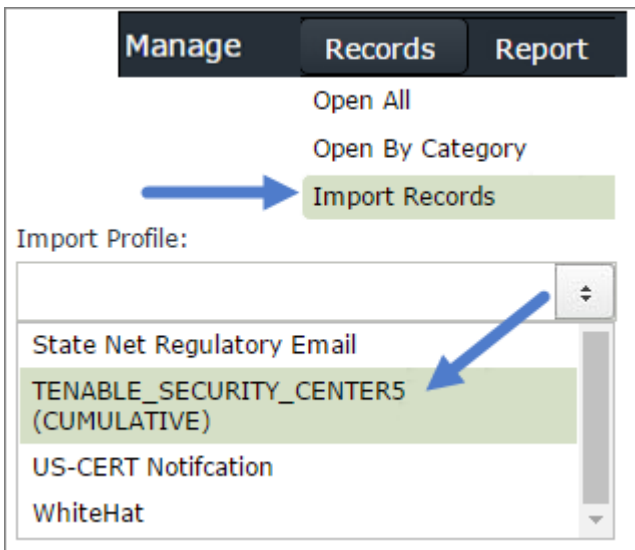
Be sure to select the checkbox corresponding to **Shared with administrators** if saving a new profile to allow all Rsam administrators to view the profile. Select the checkbox corresponding to **Shared with standard user** if any non-admins will be performing these imports.

To save the profile, perform the following step:

1. Click **Update** to update the selected profile or click **Save New** to be prompted for a new profile name.



Next time you go to **Import Records**, the saved profile will be available in the **Import Profile** drop-down and the associated map, credentials, and selections will be shown.



Profiles can then be scheduled to import vulnerabilities on a regular basis using the Rsam Scheduler.

Note: Profiles for imports using a downloaded file must have a UNC path defined.

Predefined High-Volume Vulnerability Import Maps

When performing high-volume vulnerability imports, the map configuration differs slightly. Refer the “High-Volume Vulnerability Imports” tutorial for more information.

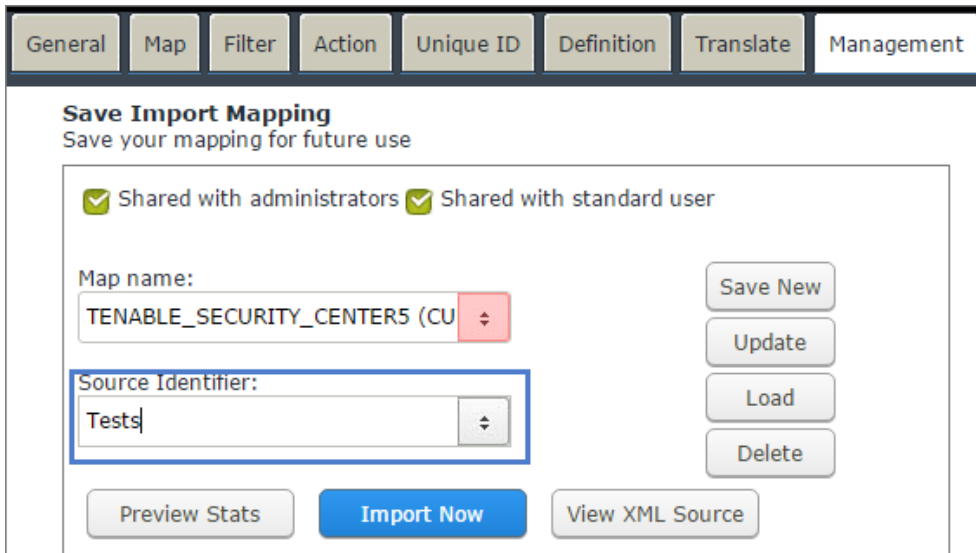
Using a Source Identifier

When scan results are imported into Rsam, criteria defined in the map determine whether an imported record should be treated as new or existing, as well as, identifying vulnerabilities currently in Rsam that are not present in the import file (unmatched). The criteria are comprised of the following fields:

- Record Category/Type
- Object Identifier
- Entity
- All Unique IDs
- Source Identifier

For each host reported in initial and subsequent imports, all vulnerabilities will be reviewed for that host and actioned accordingly based on the workflow buttons specified on the **Action** tab. Recurring imports of scan results for specific target(s) should use the same scan policy/report filters when generating both the initial and subsequent import files. If scan policies/report filters are not the same Rsam may consider those vulnerabilities unmatched and inadvertently mark them as **Closed**.

A source identifier is a text field that is defined by the customer and should be descriptive to identify the import file being used. This text is entered in the **Source Identifier** field on the **Management** tab within the map and then the map is saved with a unique title.



The screenshot shows the 'Management' tab of the 'Save Import Mapping' interface. At the top, there are tabs for 'General', 'Map', 'Filter', 'Action', 'Unique ID', 'Definition', 'Translate', and 'Management'. Below the tabs, the title is 'Save Import Mapping' with the subtitle 'Save your mapping for future use'. There are two checked checkboxes: 'Shared with administrators' and 'Shared with standard user'. The 'Map name' field contains 'TENABLE_SECURITY_CENTERS5 (CU)'. The 'Source Identifier' field contains 'Tests'. On the right side, there are four buttons: 'Save New', 'Update', 'Load', and 'Delete'. At the bottom, there are three buttons: 'Preview Stats', 'Import Now', and 'View XML Source'.

The source identifier written to each vulnerability record during the import can be displayed in searches or used for reporting.



Record	Workflow State	Vulnerability ID	Vulnerability Name	Severity - Native (numeric)	Universal Severity / Risk	Record Import Source ID
<input type="checkbox"/>	Open	18405	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	3	Medium	
<input type="checkbox"/>	Open	26920	MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)	3	Medium	
<input type="checkbox"/>	Open	57690	Terminal Services Encryption Level is Medium or Low	3	Medium	

For example, vulnerabilities found on “Host A” are imported from a file containing scan results of Critical and High severities using map ‘123’. If the next import of vulnerabilities uses map ‘1231 and the import file only includes High severity vulnerabilities, thereby excluding a subset of open vulnerabilities previously imported into Rsam, all vulnerabilities with a severity of Critical for “Host A” will be closed.

To accommodate importing scan results from defined scan targets using different scan policies or report filters, a separate map, including a defined source identifier must be used to denote the import source and prevent subsequent imports from inadvertently closing out vulnerabilities.

Example 1 – Scan Results Using Different Scan Policies

For example, the “Microsoft Patch Import” map has a source identifier of “Microsoft Patches”. It is used to import files which contain scan results from a policy specifically checking for Microsoft patches. The initial import of this scan will write “Microsoft Patches” to the “Record Import Source ID” attribute in every vulnerability record created during this import. When this map is used during subsequent imports, Rsam will ONLY review vulnerability records previously imported that contain “Microsoft Patches” in the source identifier attribute.

If you plan on importing scan results for the same assets for non-Microsoft patch vulnerabilities (same targets, different report filter) you will need to define a separate map with a different source identifier.

Example 2 – Scan Results for Ad-Hoc Scans

Monthly, a scan is run against all assets for all possible vulnerabilities and imported into Rsam. A zero-day exploit is announced and an ad-hoc scan for one vulnerability is run against all assets. To ensure the import of the ad-hoc scan results does not impact any of the existing vulnerabilities in Rsam, a separate map must be used, which includes a distinctive, unique source identifier. The new map can be created by loading the initial import map used, adding the source identifier and clicking **Save New**.

Example 3 – Scan Result File Structure

A customer wants to import all vulnerabilities reported by a scan, however, the data structure of the scan results is listed in two different sections of the import file (e.g., Qualys Confirmed vs. Potential vulnerabilities, Nexpose Test and Service vulnerabilities). In this scenario, two separate maps are required with distinctive, unique source identifiers for those imports:

Nexpose Example	Qualys Example
1. Tests	1. Confirmed
2. Services	2. Potential