



# **SOAR-TVM Module**

## **Veracode Integration Guide**

Document Version: 2017.11.20 | November 2017

Rsam © 2017. All rights reserved

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

# Contents

Overview	3
Getting Veracode Data into Rsam	4
Import Vulnerabilities from Veracode Analysis Center	4
Importing Vulnerabilities Using a Downloaded Veracode XML File	6
Manage Import Maps	8
Appendix 1: Pre-Defined Import Maps	9
V: VERACODE_DETAIL_API (v.1)	9
V: VERACODE_DETAIL_XML (v.1)	11
Appendix 2: Translated Values	13
Veracode Exploitability Ratings	13
Veracode Flaw Severities	14
Veracode Effort to Fix	14
Appendix 3: Rsam Documentation	15
Inline Help	15

## Overview

---

Rsam's Security Operations Analytics Reporting-Threat and Vulnerability Management solution (TVM) provides an integrated approach to manage a broad spectrum of risks across the enterprise. Our integration with Veracode Analysis Center allows companies to import application and vulnerability data into one centralized location that can be supplemented with information from other data sources used across the organization. The aggregation of this data gives context to your vulnerability and compliance results, driving prioritization of risk mitigation efforts and providing deeper insight into and a simplified way of reporting on overall organizational risk.

# Getting Veracode Data into Rsam

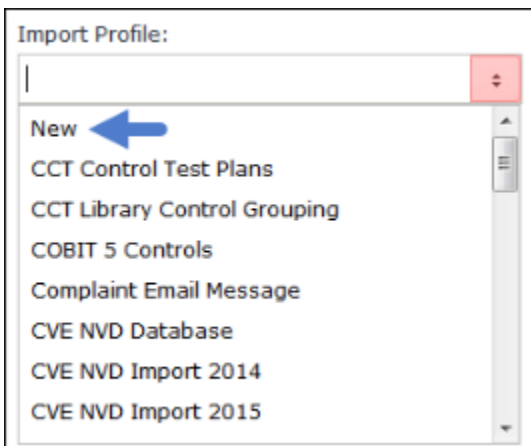
This document will guide you through the steps necessary to configure RSAM SOAR-TVM to successfully import Veracode Vulnerability data. Rsam will import the Veracode vulnerability data, as well as, list all instances where this flaw was found during the Static, Dynamic and Manual analysis.

You can connect directly to Veracode’s Analysis Center through Rsam or can manually import XML files that have been exported from Veracode.

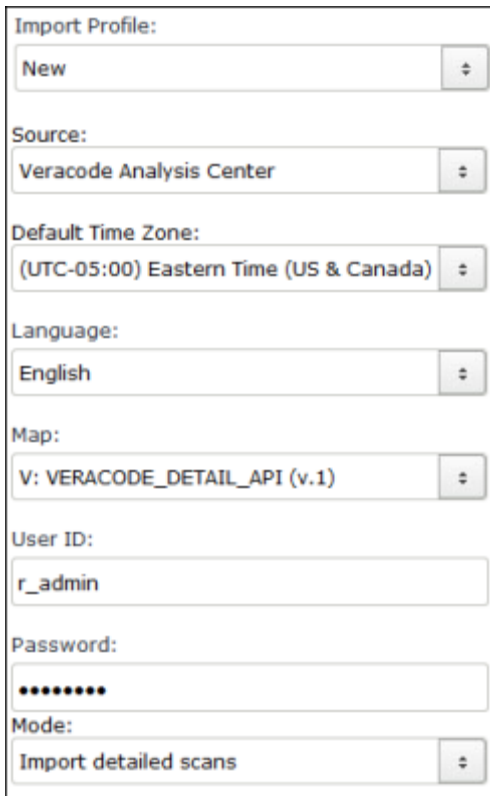
## Import Vulnerabilities from Veracode Analysis Center

Perform the following steps to import Veracode vulnerabilities:

1. Log in to Rsam as an administrator and navigate to **Records > Import Records**.
2. Select **New** from the **Import Profile** drop-down list. Initially a profile will not be configured; however, a profile can be saved to allow for scheduled imports to occur.

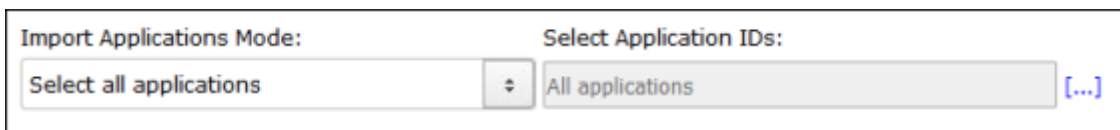


3. Select **Veracode Analysis Center** from the **Source** drop-down list.
4. Select **V: Veracode\_Detail\_API (v.1)** from the **Map** drop-down list.
5. Enter your Veracode credentials in the **User ID** and **Password** fields.
6. Select **Import detailed scans** from the **Mode** drop-down list.



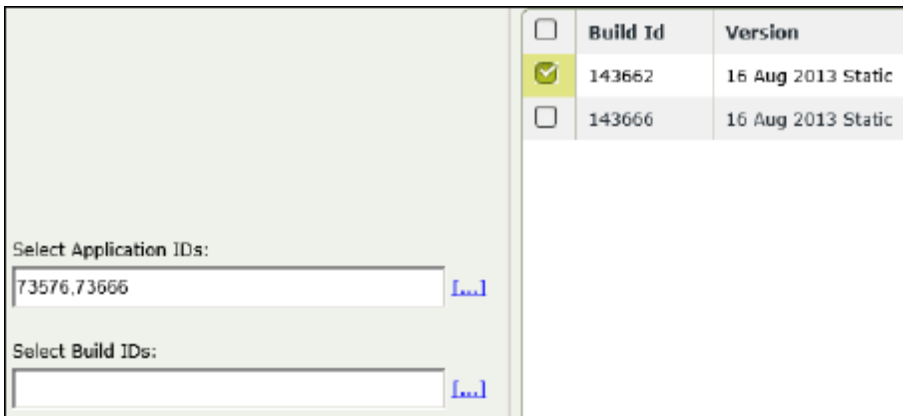
7. Select any of the following applications mode from the **Import Applications Mode** drop-down list.

- **Select all applications** – Imports all applications.
- **Select specific applications** – Click the [\[...\]](#) select icon, or type a comma delimited list of application IDs. Clicking the [\[...\]](#) select icon will display a list of all applications, where you can select the desired applications you want to import.



8. Select the builds you wish to import from the You have two options:

- **Select all latest builds** – Imports the most recent scan results for the selected applications.
- **Select specific builds** – Click the [\[...\]](#) select icon, or type a comma delimited list of build IDs. Clicking the [\[...\]](#) select icon will display a list of builds for the selected applications, where you can select the desired builds you want to import.



- Click the **Customize** button at the bottom. You will need to customize the map only once to update it for your environment. After the customization is complete, no other changes are required.
- Click **Import Now**. The vulnerabilities are imported.

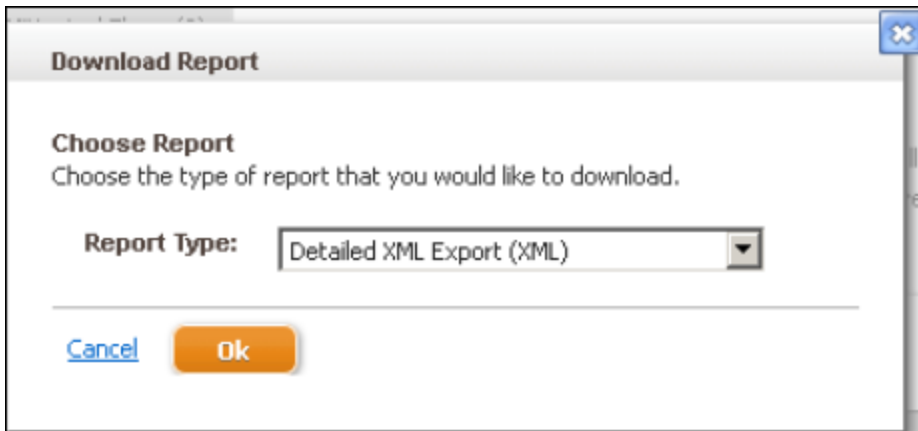
## Importing Vulnerabilities Using a Downloaded Veracode XML File

Perform the following steps to import vulnerabilities using a Veracode XML file:

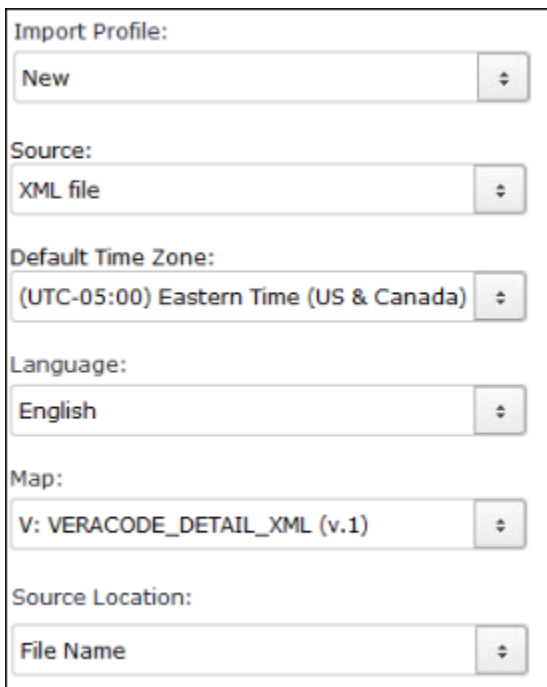
- From within the Veracode Analysis Center console, access the report results you want to download.
- Select **Veracode Report** and click the download arrow button in green.



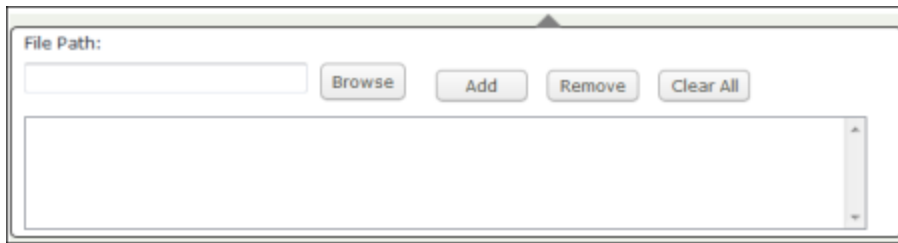
- Select **Detailed XML Export (XML)** from the **Report Type** drop-down list.



4. Log in to Rsam as an administrator and navigate to **Records > Import Records**.
5. Select **New** from the **Import Profile** field. Initially a profile will not be configured; however, a profile can be saved to allow for scheduled imports to occur.
6. Select **XML file** from the **Source** drop-down list.
7. Select **V: Veracode\_Detail\_XML (v.1)** from the **Map** drop-down list.



8. Click **Browse** and select the Veracode XML report file.



9. Click the **Customize** button at the bottom. You will need to customize the map only once to update it for your environment. After the customization is complete, no other changes are required.
10. Click **Import Now**. The vulnerabilities are imported.

## Manage Import Maps

Veracode data is imported into three record types in Rsam. The main vulnerability data is mapped to the parent Veracode Vulnerability record. All instances of flaws discovered are listed in the respective child record for that vulnerability.

Refer to [Pre-Defined Import Maps](#) for the list of predefined maps available for each import mode listed above.

Refer to the document titled *Supplemental Integration Guide – Managing TVM Import Mappings* for more information on reviewing and updating the predefined maps.



# Appendix 1: Pre-Defined Import Maps

## V: VERACODE\_DETAIL\_API (v.1)

**Unique ID:** Vulnerability ID + Flaw ID (for Dynamic Flaws and/or Static Flaws)

Rsam Attribute	Path
<b>Build ID</b>	/DetailedScanReport/detailedreport/build_id
<b>Category ID</b>	/DetailedScanReport/detailedreport/severity/category/categoryid
<b>Description</b>	/DetailedScanReport/detailedreport/severity/category/desc/para/text
<b>Fix/Resolution</b>	/DetailedScanReport/detailedreport/severity/category/recommendations/para/text
<b>Vulnerability ID</b>	/DetailedScanReport/detailedreport/severity/category/cwe/cweid
<b>Vulnerability Name</b>	/DetailedScanReport/detailedreport/severity/category/cwe/cwename

### Dynamic Flaws

Rsam Attribute	Path
<b>Category</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/categoryname
<b>Category ID</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/categoryid
<b>Effort to Fix (Numeric)</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/remediationeffort
<b>Flaw ID</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/issueid
<b>Severity - Native (numeric)</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/severity
<b>Web Attack</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/vuln_p

Rsam Attribute	Path
<b>Parameter</b>	parameter
<b>Web URL</b>	/DetailedScanReport/detailedreport/severity/category/cwe/dynamicflaws/flaw/url

### Static Flaws

Rsam Attribute	Path
<b>Category</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/category name
<b>Category ID</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/categoryid
<b>Code File Name</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/sourcefile
<b>Code File Path</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/sourcefilepath
<b>Effort to Fix (Numeric)</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/remediationeffort
<b>Exploit Level</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel
<b>Flaw ID</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/issueid
<b>Line of Code</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/line
<b>Mitigating Description</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/mitigation_status_desc
<b>Mitigating Status</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/mitigation_status
<b>Module</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/module
<b>Severity - Native (numeric)</b>	/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/severity

## V: VERACODE\_DETAIL\_XML (v.1)

**Unique ID:** Vulnerability ID + Flaw ID (for Dynamic Flaws, Manual Flaws and/or Static Flaws)

Rsam Attribute	Path
<b>Category ID</b>	/detailedreport/severity/category/categoryid
<b>Description</b>	/detailedreport/severity/category/cwe/description/text/text
<b>Fix/Resolution</b>	/detailedreport/severity/category/recommendations/para/text
<b>Vulnerability ID</b>	/detailedreport/severity/category/cwe/cweid
<b>Vulnerability Name</b>	/detailedreport/severity/category/cwe/cwename

### Dynamic Flaws

Rsam Attribute	Path
<b>Category</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/categoryname
<b>Category ID</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/categoryid
<b>Effort to Fix (Numeric)</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/remediationeffort
<b>Flaw ID</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/issueid
<b>Severity - Native (numeric)</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/severity
<b>Web Attack Parameter</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/vuln_parameter
<b>Web URL</b>	/detailedreport/severity/category/cwe/dynamicflaws/flaw/url

### Manual Flaws

Rsam Attribute	Path
<b>Attack Vector ID</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/inputvector
<b>Category</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/categoryname
<b>Category ID</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/categoryid
<b>Effort to Fix (Numeric)</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/remediationeffort

Rsam Attribute	Path
<b>Exploit Level</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/exploitLevel
<b>Fix/Resolution</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/remediation_desc
<b>Flaw ID</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/issueid
<b>Severity - Native</b> (numeric)	/detailedreport/severity/category/cwe/manualflaws/flaw/severity
<b>Web URL</b>	/detailedreport/severity/category/cwe/manualflaws/flaw/location

### Static Flaws

Rsam Attribute	Path
<b>Category</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/categoryname
<b>Category ID</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/categoryid
<b>Code File Name</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/sourcefile
<b>Code File Path</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/sourcefilepath
<b>Effort to Fix</b> (Numeric)	/detailedreport/severity/category/cwe/staticflaws/flaw/remediationeffort
<b>Exploit Level</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel
<b>Flaw ID</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/issueid
<b>Line of Code</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/line
<b>Module</b>	/detailedreport/severity/category/cwe/staticflaws/flaw/module
<b>Severity - Native</b> (Numeric)	/detailedreport/severity/category/cwe/staticflaws/flaw/severity

## Appendix 2: Translated Values

During import, Rsam translates the following Veracode data elements to the matching Rsam values available for the mapped attribute.

### Veracode Exploitability Ratings

Rsam sets the value of the "Exploit Level" based on the translated values shown below.

Path	Original Value	Rsam Value
/DetailedScanReport/detailedreport/severity/category/cwe/manualflaws/flaw/exploitLevel	-2	Very Unlikely
/DetailedScanReport/detailedreport/severity/category/cwe/manualflaws/flaw/exploitLevel	-1	Unlikely
/DetailedScanReport/detailedreport/severity/category/cwe/manualflaws/flaw/exploitLevel	0	Neutral
/DetailedScanReport/detailedreport/severity/category/cwe/manualflaws/flaw/exploitLevel	1	Likely
/DetailedScanReport/detailedreport/severity/category/cwe/manualflaws/flaw/exploitLevel	2	Very Likely
/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel	-2	Very Unlikely
/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel	-1	Unlikely
/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel	0	Neutral
/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel	1	Likely
/DetailedScanReport/detailedreport/severity/category/cwe/staticflaws/flaw/exploitLevel	2	Very Likely

## Veracode Flaw Severities

Veracode flaw severities are defined on a five point scale. Rsam sets the corresponding values of the "Universal Severity" attribute as defined in the table below.

Severity	Rsam Value	Description
<b>5</b>	Very High	The offending line or lines of code is a very serious weakness and is an easy target for an attacker. The code should be modified immediately to avoid potential attacks.
<b>4</b>	High	The offending line or lines of code have significant weakness, and the code should be modified immediately to avoid potential attacks.
<b>3</b>	Medium	A weakness of average severity. These should be fixed in high assurance software. A fix for this weakness should be considered after fixing the very high and high for medium assurance software.
<b>2</b>	Low	This is a low priority weakness that will have a small impact on the security of the software. Fixing should be consideration for high assurance software. Medium and low assurance software can ignore these flaws.
<b>1</b>	Very Low	Minor problems that some high assurance software may want to be aware of. These flaws can be safely ignored in medium and low assurance software.
<b>0</b>	Informational	Issues that have no impact on the security quality of the application but which may be of interest to the reviewer.

## Veracode Effort to Fix

Each flaw instance receives an effort to fix rating based on the classification of the flaw. The effort to fix rating is given on a scale of 1 to 5 and is mapped to the "Effort to Fix (Numeric)" attribute. This value will be displayed in Rsam with the corresponding text shown below.

Effort to Fix	Description
<b>5</b>	Complex design error. Requires significant redesign.
<b>4</b>	Simple design error. Requires redesign and up to 5 days to fix.
<b>3</b>	Complex implementation error. Fix is approx. 51-500 lines of code. Up to 5 days to fix.
<b>2</b>	Implementation error. Fix is approx. 6-50 lines of code. 1 day to fix.
<b>1</b>	Trivial implementation error. Fix is up to 5 lines of code. One hour or less to fix.

# Appendix 3: Rsam Documentation

## Inline Help

To get familiar with the specific Rsam features used in this configuration, refer the Rsam Help, Rsam Administrator Help, or both. The Online help you can access depends on your user permissions.

### Procedure:

1. Sign in to your Rsam instance. For example, sign in as **Example Administrator** user. Enter **Username** as **r\_admin** and **Password** as **password**.
2. Mouse hover over **Help** and select an Online help in the menu that appears. Depending on your user permissions, you will be able to access the Rsam Help, Rsam Administrator Help, or both. The following image shows the Rsam Administrator Help, opened from the **Example Administrator** user account.

