SOAR-TVM Module

Nessus Integration Guide

Document Version: 2017.11.20 | November 2017

Contents

Overview

Rsam's Security Operations Analytics Reporting – Threat and Vulnerability Management solution (SOAR-TVM) provides an integrated approach to manage a broad spectrum of risks across the enterprise. The integration of Nessus with Rsam SOAR-TVM provides customers with deeper insight into their overall organizational risk based on the vulnerabilities on their assets. With the information centralized in one location, it is very simple and easy to report on overall risk mitigation efforts.

Getting Nessus Vulnerabilities into Rsam

This section describes the steps to import Nessus vulnerabilities using a Nessus XML or .NESSUS file and information about predefined import maps.

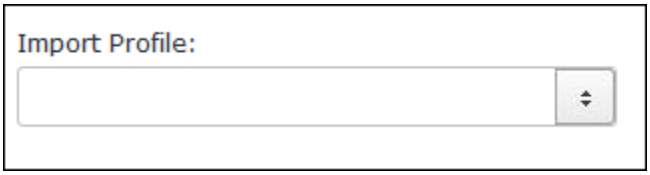
Import Nessus Vulnerabilities

To import Nessus vulnerabilities, perform the following steps:

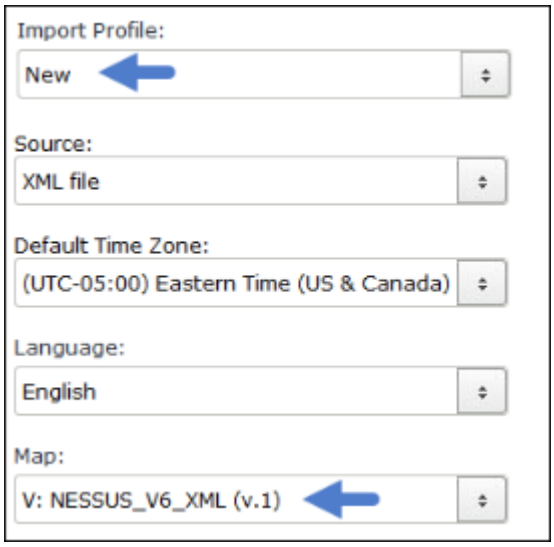
1. Download Nessus vulnerabilities.
2. Confirm the downloaded file is in the proper format. The header should look as follows:

```
<?xml version="1.0"?>
- <NessusClientData_v2>
+<Policy>
```

3. Log in to Rsam as administrator and navigate to **Records** > **Import Records**.
4. Select **New** from the Import Profile drop-down list. A profile can be saved and scheduled to import vulnerabilities at regular intervals.



5. Select **XML** file from the Source drop-down list. This is because the downloaded NESSUS file is in XML or NESSUS format.
6. Select **V: NESSUS_V6_XML (v.1)** from the Map drop-down list.



7. Click **Customize** if you want to make any changes to existing map.

8. Click **Import Now**. The vulnerabilities are imported.

Manage Nessus Import Maps

Refer to **Appendix: Predefined Import Maps** for the list of predefined maps available for importing Nessus vulnerabilities.

For information on how to review and update the predefined maps, refer to the document titled *Supplemental Integration Guide – Managing TVM Import Mappings*.

Appendix: Predefined Import Maps

This section describes import maps used for Nessus integration.

V: NESSUS_V6_XML (v.1)

This maps uses the Vulnerability ID + Port Unique ID.

Rsam Attribute	Path
Actual Result	/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_output
CPE	/NessusClientData_v2/Report/ReportHost/ReportItem/cpe
CVSS Base Score	/NessusClientData_v2/Report/ReportHost/ReportItem/cvss_base_score
CVSS Temporal Score	/NessusClientData_v2/Report/ReportHost/ReportItem/cvss_temporal_score
CVSS Vector Summary	/NessusClientData_v2/Report/ReportHost/ReportItem/cvss_vector
Description	/NessusClientData_v2/Report/ReportHost/ReportItem/description
Exploit Ease	/NessusClientData_v2/Report/ReportHost/ReportItem/exploitability_ease
Exploitable	/NessusClientData_v2/Report/ReportHost/ReportItem/exploit_available
File Name	/NessusClientData_v2/Report/ReportHost/ReportItem/fname
Fix/Resolution	/NessusClientData_v2/Report/ReportHost/ReportItem/solution
Metasploit Framework Exploit	/NessusClientData_v2/Report/ReportHost/ReportItem/exploit_framework_metasploit
Metasploit Name	/NessusClientData_v2/Report/ReportHost/ReportItem/metasploit_name
Plugin Type	/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_type

Rsam Attribute	Path
Port	/NessusClientData_v2/Report/ReportHost/ReportItem/port
Protocol	/NessusClientData_v2/Report/ReportHost/ReportItem/protocol
Reference - Bugtraq	/NessusClientData_v2/Report/ReportHost/ReportItem/bid
Reference - CWE	/NessusClientData_v2/Report/ReportHost/ ReportItem/cwe
Reference - General	/NessusClientData_v2/Report/ReportHost/ReportItem/see_also
Reference - OSVDB	/NessusClientData_v2/Report/ReportHost/ReportItem/osvdb
Related CVE Entries	/NessusClientData_v2/Report/ReportHost/ReportItem/cve
Risk	/NessusClientData_v2/Report/ReportHost/ReportItem/synopsis
Script Version	/NessusClientData_v2/Report/ReportHost/ReportItem/script_version
Service	/NessusClientData_v2/Report/ReportHost/ReportItem/svc_name
Severity - Native (numeric)	/NessusClientData_v2/Report/ReportHost/ReportItem/severity
Vulnerability Check Modify Date	/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_modification_date
Vulnerability Check Publish Date	/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_publication_date
Vulnerability ID	/NessusClientData_v2/Report/ReportHost/ReportItem/pluginID
Vulnerability Name	/NessusClientData_v2/Report/ReportHost/ReportItem/pluginName
Vulnerability Type/Family	/NessusClientData_v2/Report/ReportHost/ReportItem/pluginFamily

Appendix: 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.