RSA Archer® Suite

6.9

Integration Guide

1.2

Veracode Platform

Contact Information
RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks
RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement
This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses
This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies
This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution
Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

September 2020

Table of Contents

Release Notes

Release 1.2

New and Changed Features

- This version of the integration leverages a script to generate and download the RSA Archer report from the Veracode platform.

Known Issues

If you are not using another source to populate application data other than Veracode, you may see **Error** in the Compliance Rating field. If you are planning to use this field, review the out of the box calculation, and ensure that all supporting fields are being populated appropriately.

Chapter 1: Overview of the Integration

About Veracode and RSA Archer

The integration of Veracode with RSA Archer Suite allows customers to automatically import comprehensive vulnerability scan assessment information into the Software Security Review application within RSA Archer. This allows owners to report on vulnerabilities affecting their business-critical assets in one view. Users can assign ownership to the individual issues, track remediation efforts or accept the associated business risk.

Key Features and Benefits

By using the two products together you can:

Centralize Risk Management – Organizations can leverage their RSA Archer investment by automatically enabling Veracode's application risk intelligence into the RSA Archer Platform to support the centralized management of business processes.

Measure Compliance – By leveraging Veracode's compliance reporting for application security, RSA Archer customers will have a single view into their overall compliance with standards such as PCI.

Shorten Remediation and Mitigation Time – RSA Archer users can shorten remediation cycles through automation of remediation workflow including assigning remediation tasks to mitigate software risks discovered by Veracode.

Automate Acceptance Processes – The RSA Archer Platform allows organizations to set up acceptance thresholds for internal and third-party applications assessed by Veracode to automate the acceptance process.

Requirements

Components	Requirement
RSA Archer Solution	IT & Security Risk Management
RSA Archer Use Case	IT Security Vulnerabilities Program
RSA Archer Applications	Applications
Uses Custom Application	Yes, Software Security Review
Requires On-Demand License	Yes, 1

Applications

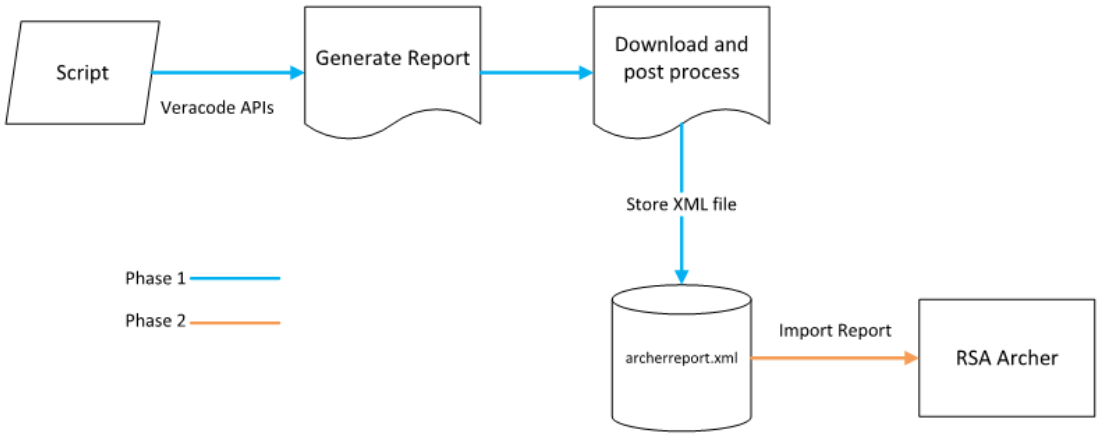
Application	Description
Software Security Review	The Software Security Review application is used to manage the risk brought on by vulnerabilities of Applications being used by the company. This scan result information from Veracode can be used to track and mitigate those risks within RSA Archer.
Applications	The Applications application stores all business applications used by the organization to perform business operations. Examples of applications include payment intake systems and customer account information systems. This repository allows you to view how an application is being used, the people who are using it and the devices supporting it.

Compatible Use Cases and Applications

Related Applications

Application	Use Case	Primary Purpose(s) of the Relationship
Findings	Issues Management	• Mitigate findings through remediation tasks or exception requests. The system calculates residual risk and compliance status based on the resolution of findings.
Remediation Plans	Issues Management	• Review all findings, alerts, and scan results related to a particular issue through one central location. • Provide users with an actionable, repeatable plan to respond to issues found during an audit or assessment.

Integration Diagram



Additional Resources

The following additional resources are available for this application:

- Veracode Archer API documentation

Chapter 2: Configuring Veracode

This section provides instructions for configuring Veracode with the RSA Archer Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Veracode components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Configuring Veracode Platform

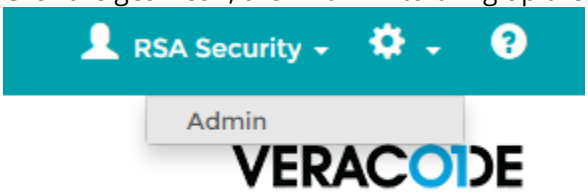
Veracode provides RSA Archer feeds that include information about the applications in an account. For assessments of internally developed or maintained applications, a feed includes scores, a listing of all discovered flaws, and status information about the flaws (new, open, fixed, or reopened). Summary data is included for third-party assessments, including scores and top-risk categories.

Customers who purchased a subscription that includes access to the Archer API can generate and retrieve Archer reports.

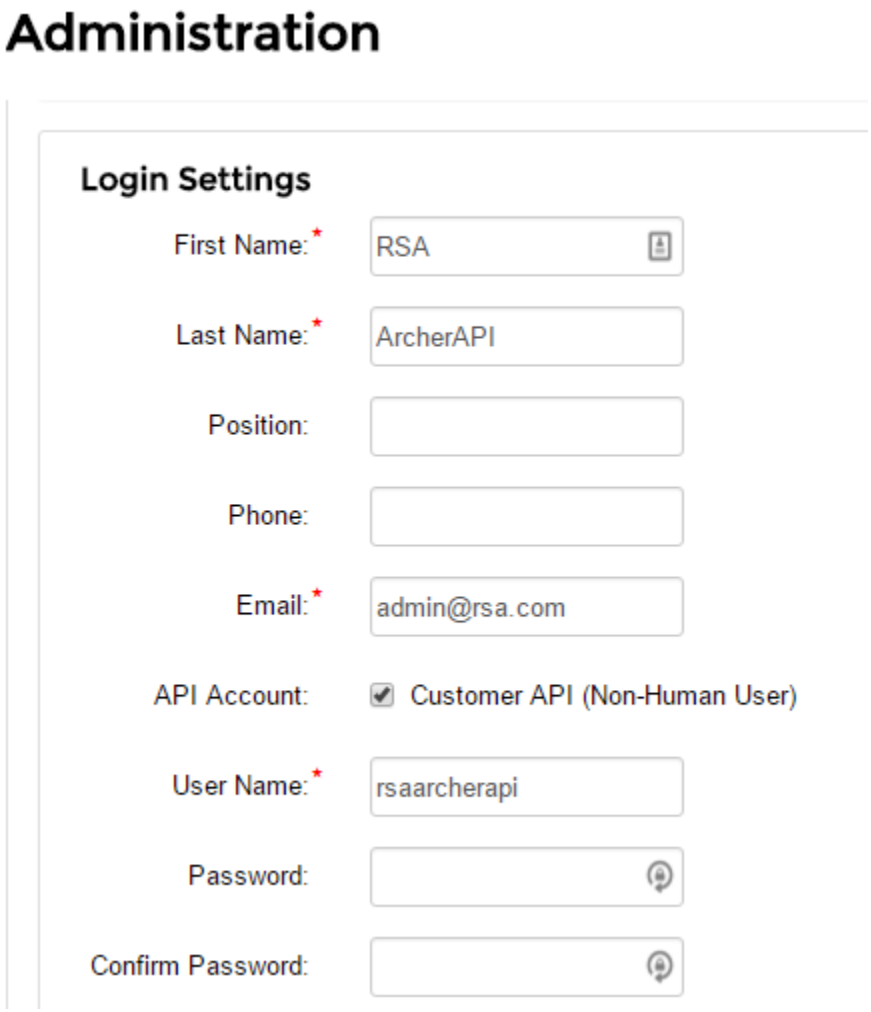
Task 1: Accessing the Archer API

To access the Archer API, you must have a non-human customer API account that has the Archer API role. To create the API customer account, perform the following step:

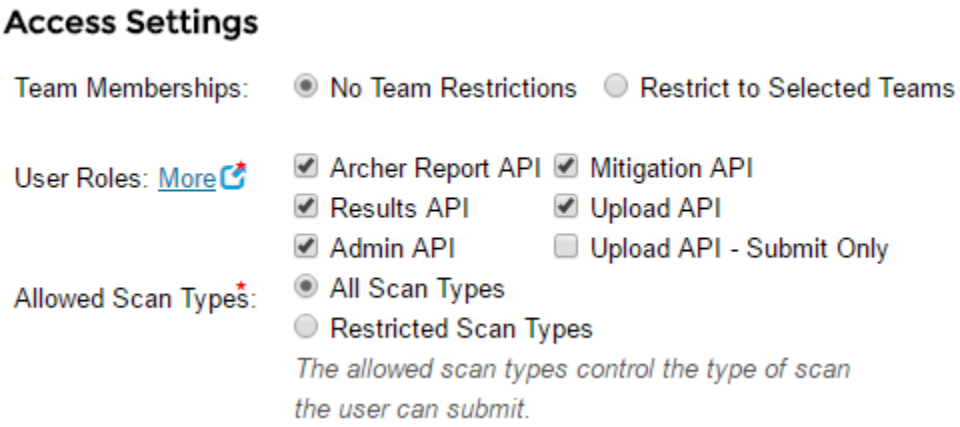
1. Click the gear icon, then **Admin** to bring up the administrative interface.



2. To create a new account for API access, click Add. Click the API Account radio box to denote that this is a non-human user:



3. Ensure that the Archer Report API button is selected as well, and click Save:



4. Now that the API User account has been created, invoke the appropriate Archer API call to generate the Archer report for download via the Data Feed Manager.

Task 2: Generating a Veracode Data File for RSA Archer

To bring Veracode data into RSA Archer, configure a client-side script that generates and downloads the data file using the Veracode Archer APIs.

1. The script can be downloaded from Veracode's Github account: https://github.com/veracode/veracode-archer
2. The sample script provided uses Python 3.x and the Veracode Authentication Tool. Instructions for configuring the tool are in the readme of the script.
3. After downloading the script and installing the required dependencies, you must also configure Veracode API credentials on the server where the script will run.
4. Schedule the script to run periodically, using a system utility such as cron.
5. The Default output of the consumable XML file is: archerreport.xml (same directory as the script).
6. You may need to change/specify the interval to get the data you are looking for. Instructions are in the readme of the script.
7. Any warnings/errors will be logged in a file called vcarcher.log.
8. The XML file will be overwritten as the script runs periodically.

Configuring RSA Archer

To integrate the RSA Archer framework and the Veracode service, the following is required:

- RSA Archer IT Security & Risk Management solution > IT Security Vulnerabilities Program Use Case
- Veracode Software Security Review application (requires on-demand license)

To configure the RSA Archer Platform, download the following component from the RSA Archer Exchange:

Integration Modules	
File Name	**Description**
Veracode_Software_Security_Review_1.2.zip	Software Security Review Application Package

The provided DFX file is configured to use both the Applications application and the application provided in the Software Security Review package (Software Security Review.zip). Once imported, the Software Security Review application is added to the Veracode solution workspace tab (this can also be altered to fit your needs). Once the application is installed, numerous customizations are needed to complete the integration including creating a new sub-form and adding new fields to the Applications application.

Task 1: Installing the Software Security Review Application Package

After downloading the integration files, import the application package to create the **Software Security Review** application. Do the following:

1. Login into RSA Archer. Go to **Administration -> Application Builder -> Install Packages**.

2. Click **Import** and browse to the Software Security Review package file (**Veracode_Software_Security_Review_1.2.zip**).
3. Make sure all mappings in Package Mapper are correct before installing the package.
4. Click **Install** to install the package.
5. This process should complete without any errors. The package will install the **Software Security Review** application into the **Veracode** solution workspace (this workspace is optional).

Task 2: Creating the Modules Sub-Form

To prepare for your integration with the **IT Security & Risk Management** solution you will need to add a sub-form, to the **Applications** application. This sub-form will allow you to import the modules associated with the application.

Important: This sub-form needs to be added to the Applications application.

To do this, perform the following steps:

1. Go to the RSA Archer platform, and click the **Administration** workspace tab.
2. Click **Application Builder** in the Navigation Menu. A menu of Application Builder pages displays.
3. Click the **Manage Sub-Forms** link. The Manage Sub-Forms page opens.
4. Click **New** to add a new sub-form.
5. Choose **Create a new Sub-Form from scratch**, and then click **OK**.
6. In the Name field, enter **Modules**.
7. Enter a description, if desired and then click the **Layout** tab.
8. Create the fields listed in the table below and add them to the layout. Use the following names for the fields:

Field Type	Name
Values List	Analysis Type
Text	Architecture
Text	Compiler
Values List	Operating System
Text	Target URL
Text	Module

9. Save the Sub-Form and exit.

Task 3: Adding Fields to the Applications Application

To prepare for your integration with the Enterprise Management solution, add a number of fields to the **Applications** application. To do this, perform the following steps:

1. Log into the RSA Archer framework and click the **Administration** workspace tab.

2. Click **Application Builder** in the Navigation Menu.
3. Search for the **Applications** application and click **Applications**.
4. Go to the **Layout** tab and create the fields listed in the table below. Use the following names for the fields (if the field already exists there is no need to recreate it):

Field Type	Name
Values List	Assurance Level
Values List	Veracode Rating
Date	Generation Date
Text	Grace Period Expired
Date	Planned Deployment Date
Values List	Policy Compliance Status
Text	Policy Name
Text	Tags
Text	Teams
Sub–Form	Modules

5. Add the fields to the layout in the location desired. You may wish to create a section or tab to house the Veracode-specific fields, but this is an optional step.
6. There is also a **Cross-Reference** field to the **Software Security Review** application that is automatically created upon installation of the application package. Adding this field, called **Software Security Review,** to the layout will give a listing of the flaws that pertain to a particular application.

Once the fields have been created, and the application has been saved, import the data feed configuration files, so that the feeds can populate the fields in the appropriate application(s).

Task 4: Importing the Veracode Download – FTP Data Feed Configuration File

After the Python script is configured, configure the **Veracode Download – FTP** Data Feed to push the XML file into RSA Archer and create the records. To perform the import, do the following:

1. The **Veracode Download – FTP** Data Feed will be uploaded into the system during the **Veracode_Software_Security_Review_1.2.zip** package installation.
2. Browse to **Manage Data Feeds** and click on the **Veracode Download – FTP** Data Feed.
3. Verify settings on the **General Information** tab. Be sure to change the status to **Active** before using the feed.
4. Click Transport, FTP should be the transport type selected.
5. In the Transport Configuration section on the transport tab, the path should be specified.
6. Click the **Data Map** tab to review field mapping and make any necessary changes. A list of recommended field mappings can be found in Appendix B.

Task 5: Activate and Schedule the Veracode Download Data Feed

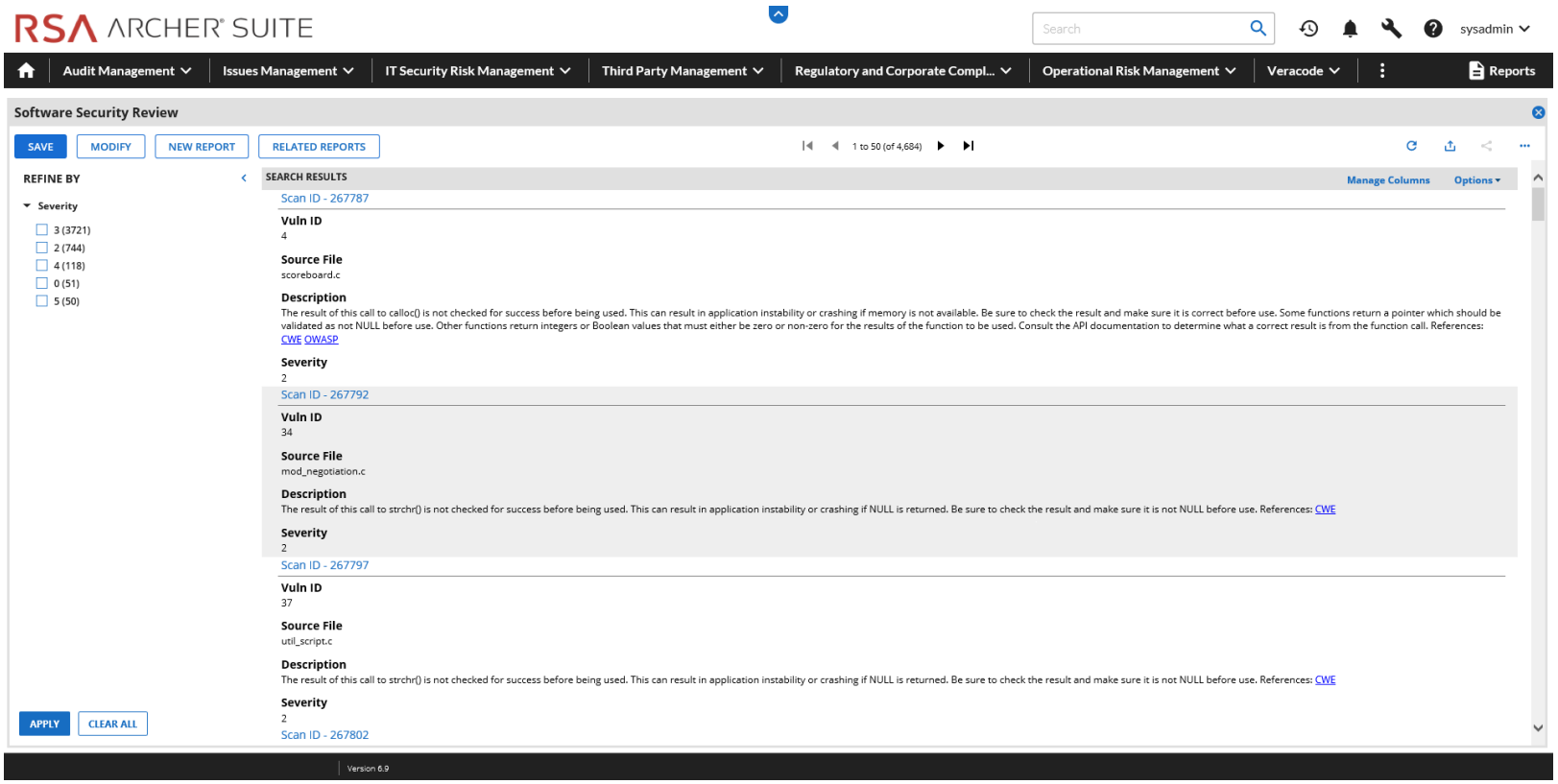
Specify a schedule for the feed to run.

1. Browse to **Manage Data Feeds** and click **Veracode Download** Data Feed.

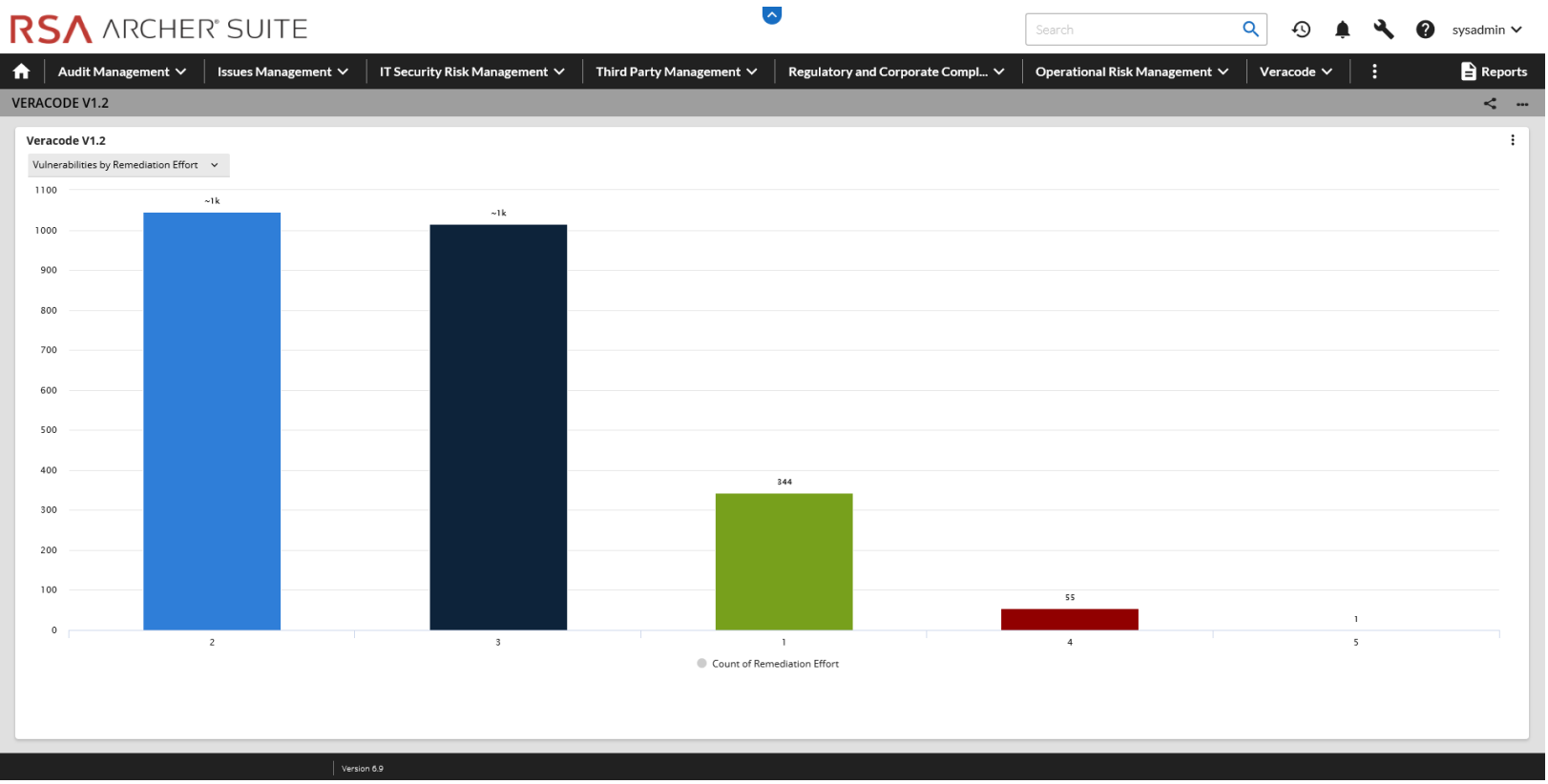
2. Click the **Schedule** tab, and configure the frequency and start time of the Data Feed:
3. Click **Run Data Feed Now** to override the set data feed execution schedule and immediately execute your data feed.
4. Click **Save** to apply your configuration to the data feed. Click the **Run Detail** link for additional information on the status of the feed or to troubleshoot any feed errors.

Chapter 3: Using the Veracode Integration

The integration of Veracode with RSA Archer enables customers to better manage their organization's risk by proactively identifying, tracking, and managing the repair of critical application vulnerabilities. In addition, customers can integrate with other RSA Archer solutions such as **Policy Management** and **IT Security Risk Management** to gain a broader understanding of the risks to the organization.



Utilize RSA Archer's workflow by managing findings and tracking remediations for the exposed vulnerabilities. The Veracode Integration package also comes with reports to help organize scan results in RSA Archer including: "Veracode Scan Results by Severity" and "Top 10 Most Vulnerable Applications".



Appendix A: Certification Environment

Date Tested: September 9, 2020

Product Name	Version Information	Operating System
RSA Archer	6.9	Windows
Veracode	Release 2020.8	n/a

Appendix B: Field Mappings

This table contains the field mappings for the **Veracode Download** data feed (Key fields in bold). RSA Archer target fields that are grayed out are either deprecated or are unused in the integration.

Source Fields	Target Archer Fields
any_scan_due_date	
app_name	**Application Name**
app_origin	
assurance_level	Assurance Level
business_owner	Application Owner
business_unit	**Business Units\Business Unit**
custom0	
custom1	
custom2	
custom3	
custom4	
dynamic_score	
flaws	Software Security Review (SSR)
flaws\app_name	**SSR\Application Name***
flaws\capecid	SSR\Capecid
flaws\categoryid	SSR\Category ID
flaws\categoryname	SSR\Category
flaws\cia_impact	SSR\CIA Impact
flaws\count	SSR\Count
flaws\cwe_description	SSR\CWE Description
flaws\cweid	SSR\CWE ID

flaws\date_first_occurance	SSR\Date First Occurance
flaws\exploit_desc	SSR\Exploit Description
flaws\exploitdifficulty	SSR\Exploit Difficulty
flaws\exploitLevel	SSR\Exploit Level
flaws\flaw_description	SSR\Description
flaws\flaw_issue_id	**SSR\Vun ID***
flaws\functionprototype	SSR\Function Prototype
flaws\functionrelativelocation	SSR\Function Relative Location
flaws\is_latest_build	SSR\Is Latest Build
flaws\line	SSR\Line
flaws\mitigation_status	SSR\Mitigation Status
flaws\mitigation_status_desc	SSR\Mitigation Status Description
flaws\mitigations\action	**SSR\Mitigations\Action**
flaws\mitigations\date	SSR\Mitigations\Date
flaws\mitigations\description	SSR\Mitigations\Description
flaws\mitigations\user	SSR\Mitigations\User
flaws\module	**SSR\Module***
flaws\note	SSR\Note
flaws\pcirelated	SSR\PCI Related
flaws\platform	SSR\Platform
flaws\published_date	SSR\Published Date
flaws\remediation_desc	SSR\Remediation Description
flaws\remediation_status	SSR\Remediation Status
flaws\remediationeffort	SSR\Remediation Effort

flaws\scope	SSR\Scope
flaws\severity	SSR\Severity
flaws\severity_desc	SSR\Severity Description
flaws\sourcefile	SSR\Source File
flaws\sourcefilepath	SSR\Source File Path
flaws\type	SSR\Type
flaws\url	SSR\URL
flaws\version	**SSR\Application Version***
generation_date	Generation Date
grace_period_expired	Grace Period Expired
last_update_date	
lifecycle_stage	
manual_score	
mitigated_rating	
modules	Modules Sub Form
modules\analysis_type	Modules\Analysis Type
modules\architecture	Modules\Architecture
modules\compiler	Modules\Compiler
modules\module	**Modules\Module**
modules\os	Modules\Operating System
planned_deployment_date	Planned Deployment Date
platform	Platform
policy_compliance_status	Policy Compliance Status
policy_name	Policy Name

policy_rules_passed	
poilcy_version	
rating	Veracode Rating
scan_overdue	
static_score	
submitted_date	
tags	Tags
teams	Teams
version	Version

* Note that **Vuln ID**, **Application Version**, **Module**, and **Application Name** are all part of a compound key for the Software Security Review application, therefore their **Order** should all be set to **1** in the **Key Field Definitions** Tab.*