ThreatQuotient

ThreatQuotient for Rapid7 InsightVM Operation

Version 1.0.0

April 29, 2019

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document "as is", without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Last Updated: Monday, 29 April 2019

Contents

WARNING AND DISCLAIMER....................2

CONTENTS....................4

LIST OF FIGURES AND TABLES....................5

INTRODUCTION....................6

1.1 APPLICATION FUNCTION....................6
1.2 PREFACE....................6
1.3 AUDIENCE....................6
1.4 SCOPE....................6

THREATQUOTIENT FOR RAPID7 INSIGHTVM OPERATION INSTALLATION....................7

1.5 SETTING UP THE INTEGRATION....................7
1.6 CONFIGURING THE OPERATION....................8
1.7 USING THE OPERATION....................10
1.7.1 Get Affected Assets....................10
1.7.2 Query....................11

TRADEMARKS AND DISCLAIMERS....................12

List of Figures and Tables

FIGURE 1: OPERATIONS MANAGEMENT – INSTALL 7
FIGURE 2: INSTALL OPERATION 7
FIGURE 3: ADD OPERATION 8
FIGURE 4: ADD OPERATION 8
FIGURE 5: OPERATIONS MANAGEMENT – CONFIGURATION 9
FIGURE 6: OPERATION CONFIGURATION 9
FIGURE 7: OPERATION GET AFFECTED RESULTS 10
FIGURE 8: OPERATION QUERY GENERAL RESULTS EXAMPLE 11
FIGURE 9: OPERATION QUERY VERDICT RESULTS EXAMPLE 11
FIGURE 10: OPERATION QUERY SOLUTIONS RESULTS EXAMPLE 11

TABLE 1: THREATQUOTIENT SOFTWARE & APP VERSION INFORMATION 6

Introduction

1.1 Application Function

The ThreatQuotient for Rapid7 InsightVM Operation allows a ThreatQ user to execute two CVE actions on their Rapid7 InsightVM instance. First, it allows users to query for CVE details in their Rapid7 InsightVM instance. This action will return information on the vulnerability, such as the scores and solutions. Second, it allows users to query Rapid7 InsightVM to see if any configured sites or assets are vulnerable to a specific CVE. This action will show information on the asset as well as solutions to the vulnerability.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for Rapid7 InsightVM Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers
2. ThreatQuotient Professional Services Project Team and Engineers

1.4 Scope

This document covers the implementation of the application only.

Table 1: ThreatQuotient Software & App Version Information

<table>
<tr><th>Software/App Name</th><th>File Name</th><th>Version</th></tr>
<tr><td>ThreatQ</td><td colspan="2">Version 3.6.x or greater</td></tr>
<tr><td>ThreatQuotient for Rapid7 InsightVM Operation</td><td colspan="2">Version 1.0.0</td></tr>
</table>

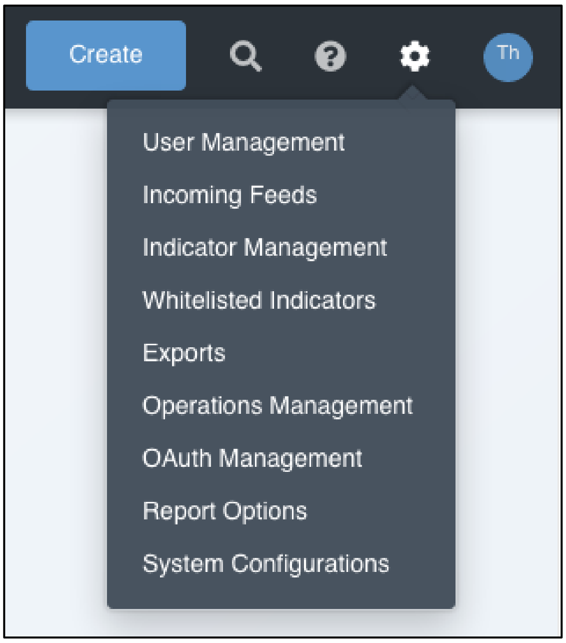
ThreatQuotient for Rapid7 InsightVM Operation Installation

1.5 Setting up the Integration

Ensure the file `tq_op_rapid7_insight_vm-1.0.0-py3-none-any.whl` is available on the device being used to administer the ThreatQ instance in which the ThreatQuotient for Rapid7 InsightVM Operation is being installed or upgraded.

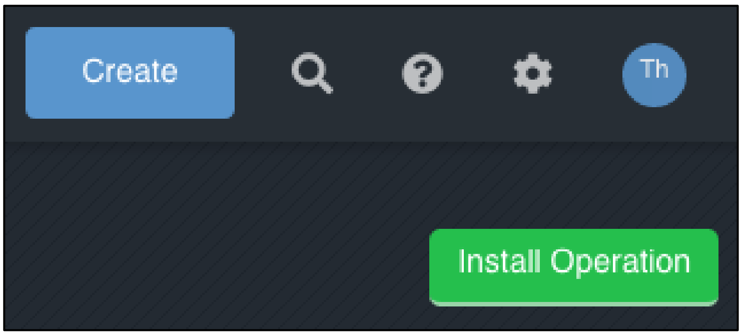
1. Navigate to the Settings icon > Operations Management.

Figure 1: Operations Management – Install



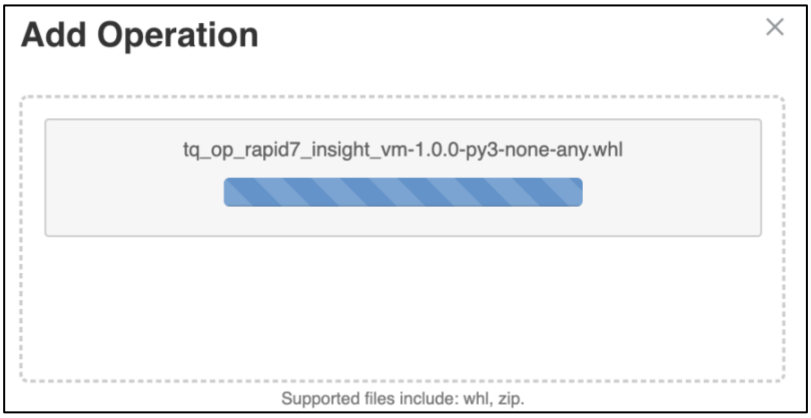
2. Click **Install Operation** in the upper right corner.

Figure 2: Install Operation



3. Drag the `tq_op_rapid7_insight_vm-1.0.0-py3-none-any.whl` to the Add Operation Popup or **Click to Browse** to the required file.

Figure 3: Add Operation



Add Operation

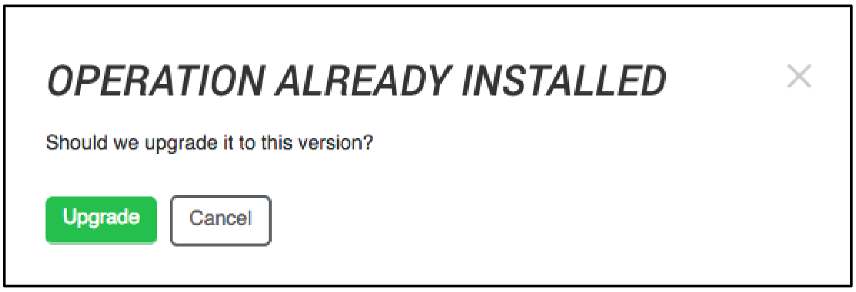
tq_op_rapid7_insight_vm-1.0.0-py3-none-any.whl

Supported files include: whl, zip.

4. Click on **Install** or **Upgrade**.

You may be presented with OPERATION ALREADY INSTALLED as shown below.

Figure 4: Add Operation



OPERATION ALREADY INSTALLED

Should we upgrade it to this version?

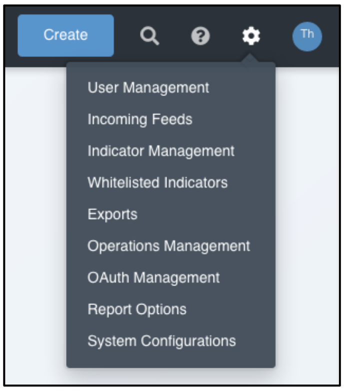
5. Installation or upgrade is now complete.

1.6 Configuring the Operation

The following section covers the configuration of the ThreatQuotient for Rapid7 InsightVM Operation.

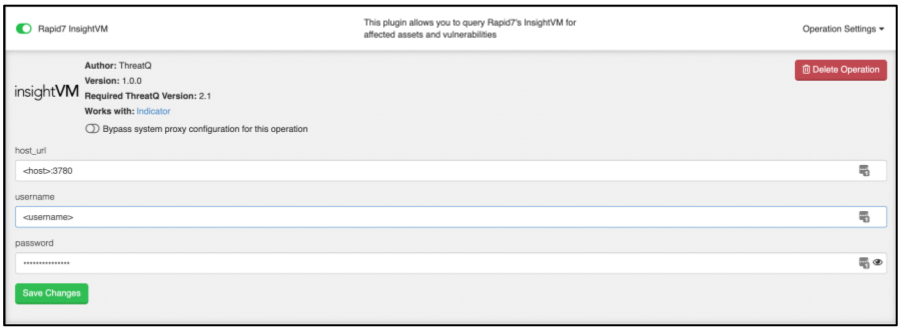
1. Navigate to the **Settings icon** > **Operations Management**.

Figure 5: Operations Management – Configuration



2. Expand the **Operations Settings** configuration.

Figure 6: Operation Configuration



This plugin allows you to query Rapid7's InsightVM for affected assets and vulnerabilities

Author: ThreatQ
Version: 1.0.0
Required ThreatQ Version: 2.1
Works with: Indicator

○ Bypass system proxy configuration for this operation

host_url
<host>:3780

username
<username>

password
•••••••••••••••

3. **host_url**: Your Rapid7 InsightVM URL
4. **username**: Your Rapid7 InsightVM username to use with the API
5. **password:** Your Rapid7 InsightVM password associated with the above username
6. Click **Save Changes**. The operation is now ready to be used.

1.7 Using the Operation

The following section covers the use of the ThreatQuotient for Rapid7 InsightVM Operation.

This operation comes with two actions you can execute on Rapid7 InsightVM.

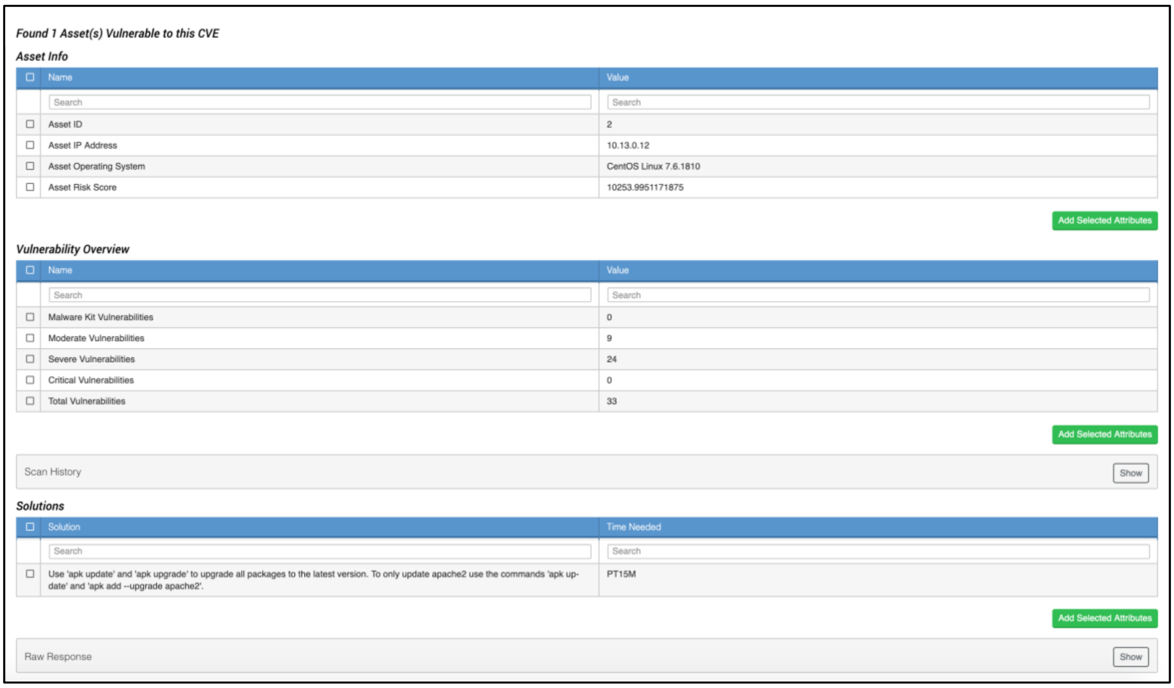
- Get Affected Assets
- Query

1.7.1 Get Affected Assets

This action allows you to query Rapid7 InsightVM and see if you have any assets/sites affected by the specific CVE.

Running this action will give you results similar to the following example.

Figure 7: Operation Get Affected Results



Found 1 Asset(s) Vulnerable to this CVE

Asset Info

□	Name	Value
	Search	Search
□	Asset ID	2
□	Asset IP Address	10.13.0.12
□	Asset Operating System	CentOS Linux 7.6.1810
□	Asset Risk Score	10253.9951171875

Vulnerability Overview

□	Name	Value
	Search	Search
□	Malware Kit Vulnerabilities	0
□	Moderate Vulnerabilities	9
□	Severe Vulnerabilities	24
□	Critical Vulnerabilities	0
□	Total Vulnerabilities	33

Solutions

□	Solution	Time Needed
	Search	Search
□	Use 'apk update' and 'apk upgrade' to upgrade all packages to the latest version. To only update apache2 use the commands 'apk update' and 'apk add --upgrade apache2'.	PT15M

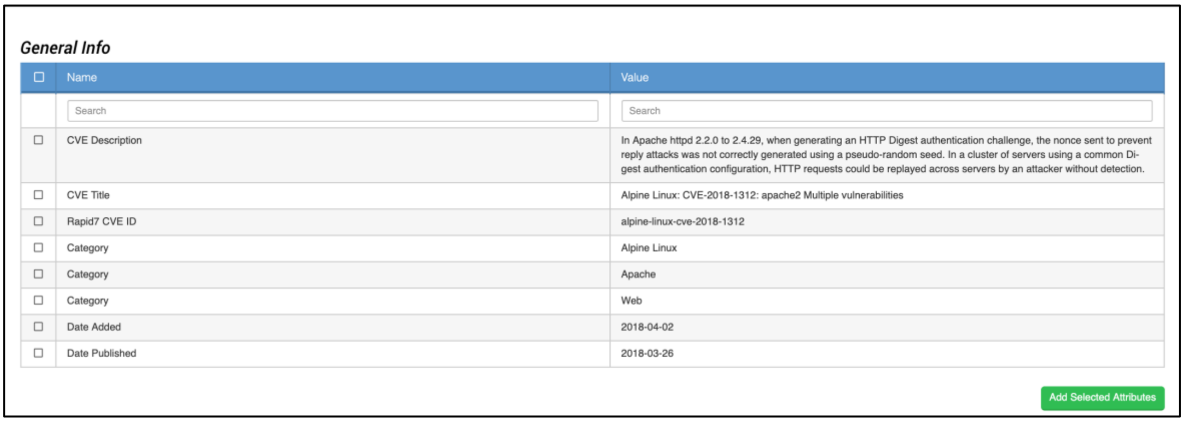
If there are no assets affected by the vulnerability, you will receive a message saying there are no affected assets.

1.7.2 Query

This action allows you to query your Rapid7 InsightVM to see what information and scores it has for the vulnerability.

Running the action will show you results similar to the following:

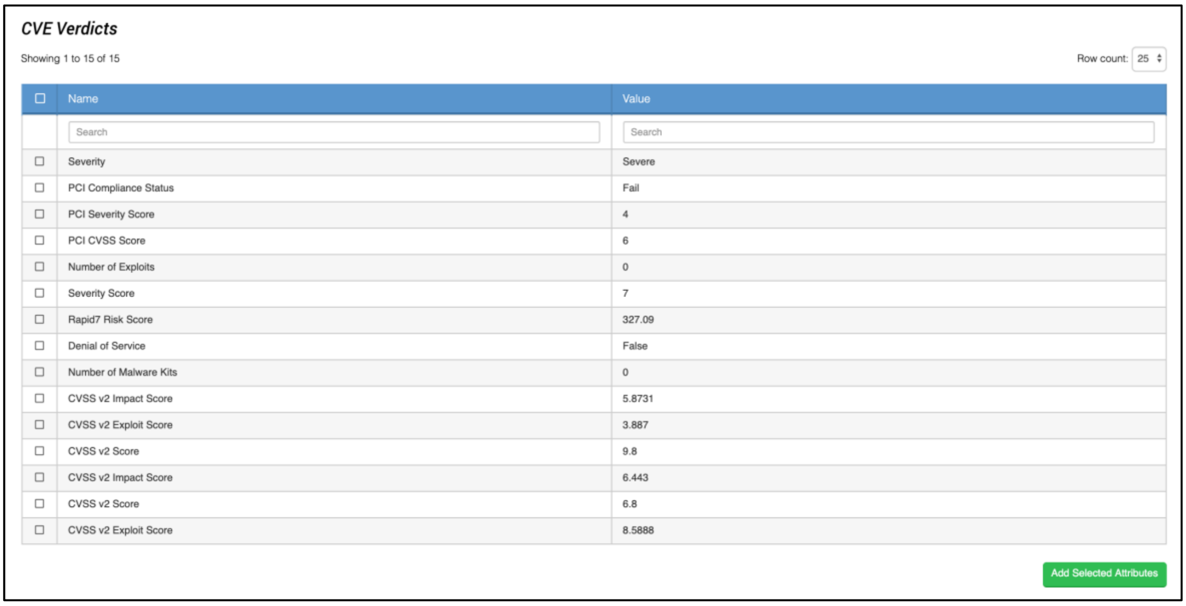
Figure 8: Operation Query General Results Example



General Info

□	Name	Value
	Search	Search
□	CVE Description	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
□	CVE Title	Alpine Linux: CVE-2018-1312: apache2 Multiple vulnerabilities
□	Rapid7 CVE ID	alpine-linux-cve-2018-1312
□	Category	Alpine Linux
□	Category	Apache
□	Category	Web
□	Date Added	2018-04-02
□	Date Published	2018-03-26

Figure 9: Operation Query Verdict Results Example



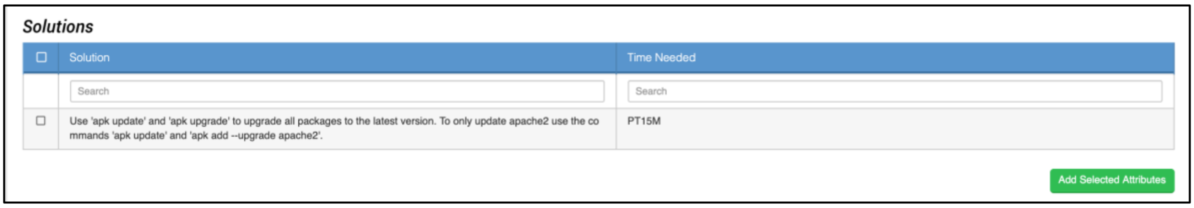
CVE Verdicts

Showing 1 to 15 of 15

Row count: 25

□	Name	Value
	Search	Search
□	Severity	Severe
□	PCI Compliance Status	Fail
□	PCI Severity Score	4
□	PCI CVSS Score	6
□	Number of Exploits	0
□	Severity Score	7
□	Rapid7 Risk Score	327.09
□	Denial of Service	False
□	Number of Malware Kits	0
□	CVSS v2 Impact Score	5.8731
□	CVSS v2 Exploit Score	3.887
□	CVSS v2 Score	9.8
□	CVSS v2 Impact Score	6.443
□	CVSS v2 Score	6.8
□	CVSS v2 Exploit Score	8.5888

Figure 10: Operation Query Solutions Results Example



Solutions

□	Solution	Time Needed
	Search	Search
□	Use 'apk update' and 'apk upgrade' to upgrade all packages to the latest version. To only update apache2 use the commands 'apk update' and 'apk add --upgrade apache2'.	PT15M

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.