



# **Cisco Threat Grid App for IBM QRadar With DSM**

**Operations Guide**

**September 5, 2019**

**Version 1.0.1**

# Contents

---

<b>CONTENTS</b> .....	<b>2</b>
<b>ABOUT THIS OPERATIONS GUIDE</b> .....	<b>3</b>
REVISION HISTORY .....	3
<b>1 INTRODUCTION</b> .....	<b>4</b>
1.1 DOCUMENT PURPOSE .....	4
1.2 APPLICATION SUMMARY .....	4
<b>2 OPERATIONS</b> .....	<b>5</b>
2.1 PRE-REQUISITE .....	5
2.2 INSTALLATION .....	5
2.3 CONFIGURATION OF THE APPLICATION.....	5
2.4 CONFIGURATION OF THE LOG SOURCE .....	7
<b>3 LEGAL NOTICE</b> .....	<b>8</b>

# About This Operations Guide

---

Author                      Aujas Networks Pvt. Ltd.

Change Authority        Aujas Networks Pvt. Ltd.

## Revision History

Revision	Date	Name or User ID	Comments
1.0	06/04/2019	Aujas Networks Pvt. Ltd.	Initial Operations Guide
1.0.1	09/05/2019	Cisco Systems	

# 1 Introduction

---

## 1.1 Document Purpose

The purpose of this document is to outline the operations of the Cisco Threat Grid App for QRadar with DSM and may be used to assist users with installation and execution.

## 1.2 Application Summary

IBM QRadar consolidates log source event data from thousands of device endpoints and applications distributed throughout a network. Cisco Threat Grid provides a sandboxing environment for suspected malicious files, as well as aggregates threat intelligence based on the submitted files.

The Cisco Threat Grid dashlet allows QRadar users to quickly have insight into the files being submitted by their organization and those that are possibly malicious (Threat Score of 90+). Also, the Cisco Threat Grid App allows for use of QRadar's native right-click on IP address, to gain threat intelligence insight from data brought into the QRadar environment from other sources.

## 2 Operations

---

### 2.1 Pre-requisite

The Cisco Threat Grid App for QRadar requires IBM QRadar version 7.2.8 or higher

### 2.2 Installation

The Cisco Threat Grid App for QRadar is available from the IBM Security App Exchange at:

<https://exchange.xforce.ibmcloud.com/hub>

### 2.3 Configuration of The Application

- To make use of the Cisco Threat Grid App the user must enter their Threat Grid required values in the Cisco Threat Grid settings page found within QRadar at **Admin > Plug-ins > Cisco Threat Grid**.



Cisco Threat Grid

- Following Values can be filled for the configuration:

QRadar Settings

- QRadar Server IP

API Settings

- Threat Grid API Key

Found at <https://panacea.threatgrid.com/mask/users/> [your user name]

- Threat Grid API Host:

- panacea.threatgrid.com
- panacea.threatgrid.eu
- FQDN of a Threat Grid Appliance clean interface

- Limit for the Dashboard View: Number of samples to be displayed in the dashlet

# Threat Grid

## Qradar Settings

QRadar Server IP

## API Settings

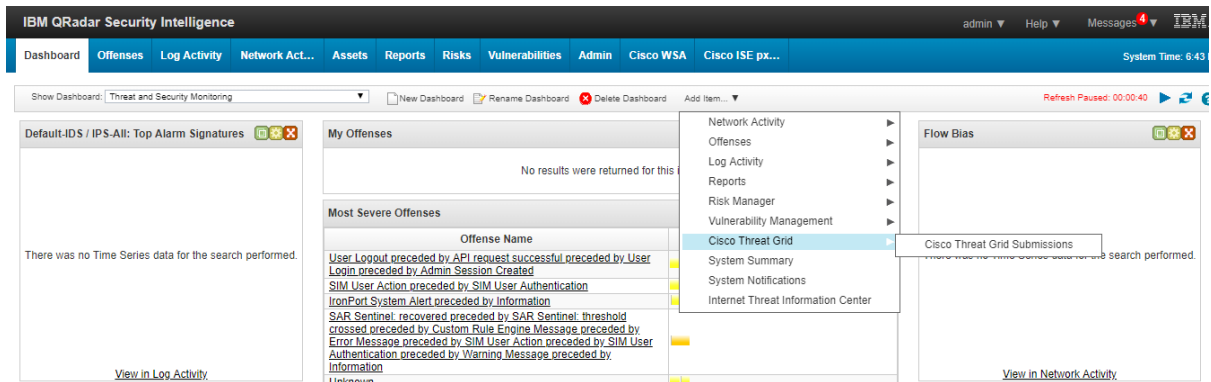
Threat Grid API Key

Threat Grid API Host

Limit for the Dashboard View

**Submit**

- Return to the QRadar **Dashboard** and select **Threat and Security Monitoring** in the **Show Dashboard** drop down menu.
- Click on **Add Item...** and select **Cisco Threat Grid > Cisco Threat Grid Submissions**.



- Sample **Dashboard** is shown below:

Threat Grid Organization Samples		
SHA-256	Threat Score	User
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa	100	joaugustine
271527ee96fac95616055015af31f6d691a5e6df95d388820143ed55aa4139cd	19	joaugustine

- **Right-Click** functionality is also supported in **Log Activity**, for IP addresses:

The screenshot shows the IBM QRadar Security Intelligence interface. At the top, there are navigation tabs: Dashboard, Offenses, Log Activity, Network Act..., Assets, Reports, Risks, Vulnerabilities, Admin, Cisco WSA, and Cisco ISE px... The system time is 7:00 PM. Below the navigation is a search bar with options like 'Quick Searches', 'Add Filter', 'Save Criteria', 'Save Results', 'Cancel', 'False Positive', 'Rules', and 'Actions'. A table of events is displayed with columns: Event Name, Log Source, Event Count, Time, Low Level Category, Source IP, Source Port, Destination IP, and Destination Port. A context menu is open over the 'Source IP' column, showing options like 'Filter on Source IP is 192.168.1.51', 'Quick Filter...', 'False Positive', 'View path from 192.168.1.51 to 192.168.0.231', 'View in DSM Editor', 'More Options...', 'Navigate', 'Information', 'Run Vulnerability Scan', 'Run Forensics Recovery', 'Run Forensics Search', 'Plugin options...', 'Cisco pxGrid - ANC Quarantine', 'Cisco pxGrid - ANC Shutdown', 'Cisco pxGrid - ANC Port Bounce', and 'Search in Cisco Threat Grid'. The status bar at the bottom indicates 'Displaying 1 to 14 of 14 items (Elapsed time: 0:00:00.965)'.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port
Admin Session Destroyed	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:32 PM	SIM User Authentication	192.168.1.51	0	192.168.0.231	0
API request successful	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:32 PM	SIM User Action	192	0	192.168.1.51	0
Admin Session Created	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:32 PM	SIM User Authentication	192	0	192.168.1.51	0
Admin Session Destroyed	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Authentication	192	0	192.168.1.51	0
API request successful	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Action	192	0	192.168.1.51	0
Admin Session Created	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Authentication	192	0	192.168.1.51	0
Information Message	System Notification-2 :: qrad...	1	Feb 19, 2019, 7:00:31 PM	Information	192	0	192.168.0.231	0
Admin Session Destroyed	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Authentication	192	0	192.168.0.231	0
API request successful	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Action	192	0	192.168.0.231	0
Admin Session Created	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Authentication	192	0	192.168.0.231	0
Admin Session Destroyed	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Authentication	192	0	192.168.0.231	0
API request successful	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Action	192	0	192.168.0.231	0
Admin Session Created	SIM Audit-2 :: qradar728_2	1	Feb 19, 2019, 7:00:31 PM	SIM User Authentication	192	0	192.168.0.231	0
Information Message	System Notification-2 :: qrad...	1	Feb 19, 2019, 7:00:30 PM	Information	192	0	127.0.0.1	0

- The Cisco Threat Grid App for IBM QRadar fetches the threat score results of dynamic malware analysis at regular intervals from Cisco Threat Grid using Cisco Threat Grid APIs.
  - These incidents will be stored persistently in IBM QRadar as events and show up in the IBM QRadar Console. This will allow end users to view and use Cisco Threat Grid incident data in IBM QRadar.

## • 2.4 Configuration of The Log Source

1. From the Admin tab on the QRadar navigation bar, scroll down to Log Sources.
2. Click on Add to create a new log source.
3. Enter the required parameters for creating log source:
  - Log Source Type: **Cisco Threat Grid**
  - Log Source Identifier: **hostname of the Threat Grid API Host FQDN**
    - i. For panacea.threatgrid.[com|eu] this is be “panacea”
  - Coalescing Events: **Unchecked**
  - Log Source Extension: **CiscoThreatGridCustom\_ext**

The screenshot shows the 'Add a log source' configuration window. The fields are as follows:

- Log Source Name: [Empty text box]
- Log Source Description: [Empty text box]
- Log Source Type: Cisco Threat Grid (dropdown menu)
- Protocol Configuration: Syslog (dropdown menu)
- Log Source Identifier: panacea (text box)
- Enabled:
- Credibility: 5 (dropdown menu)
- Target Event Collector: eventcollector0 :: 728 (dropdown menu)
- Coalescing Events:
- Incoming Payload Encoding: UTF-8 (dropdown menu)
- Store Event Payload:
- Log Source Language: [Empty dropdown menu]
- Log Source Extension: CiscoThreatGridCustom\_ext (dropdown menu)
- Extension Use Condition: Parsing Enhancement (dropdown menu)

Please select any groups you would like this log source to be a member of:

[Empty text box for group selection]

Save Cancel

4. Click on **Save** and **Deploy Changes**.



## 3 Legal Notice

---

This document transmission (and/or the documents accompanying it) is for the sole use of the intended recipient(s) and may contain information protected by the attorney-client privilege, the attorney-work-product doctrine or other applicable privileges or confidentiality laws or regulations. If you are not an intended recipient, you may not review, use, copy, disclose or distribute this message or any of the information contained in this message to anyone. If you are not the intended recipient, contact the sender by reply e-mail and destroy all copies of this message and attachments.