Cisco Threat Grid App for IBM QRadar With DSM

Operations Guide

September 5, 2019

Version 1.0.1

Contents

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

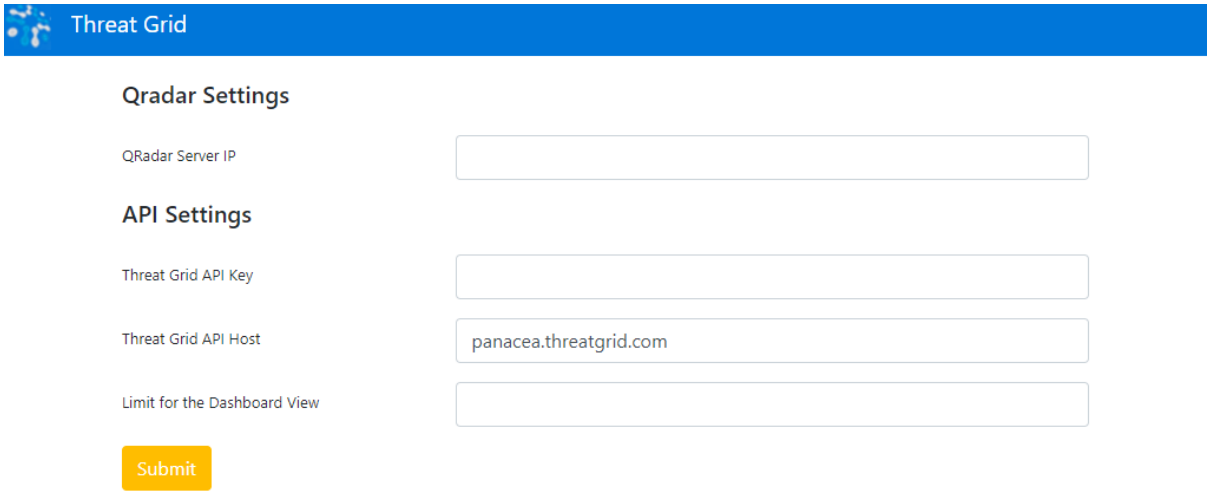
- To make use of the Cisco Threat Grid App the user must enter their Threat Grid required values in the Cisco Threat Grid settings page found within QRadar at **Admin** > **Plug-ins** > **Cisco Threat Grid.**

- Following Values can be filled for the configuration:

  QRadar Settings
  - QRadar Server IP

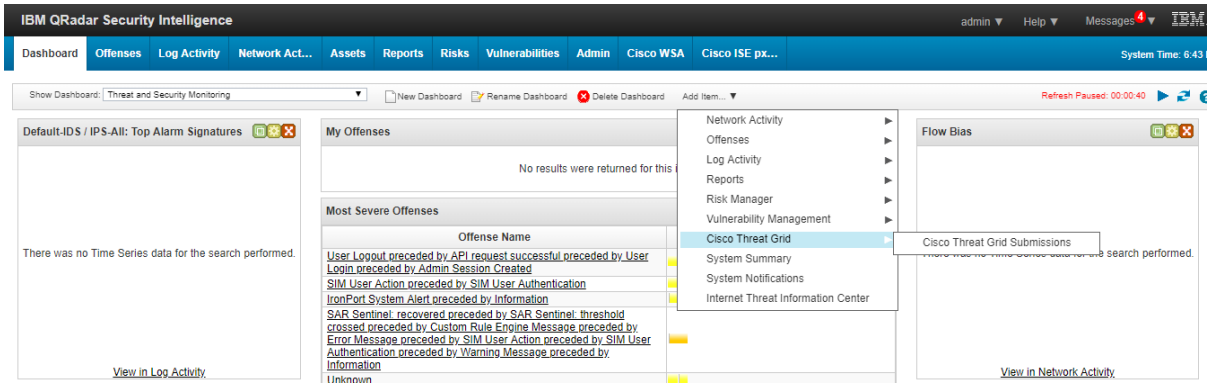
  API Settings
  - Threat Grid API Key

    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

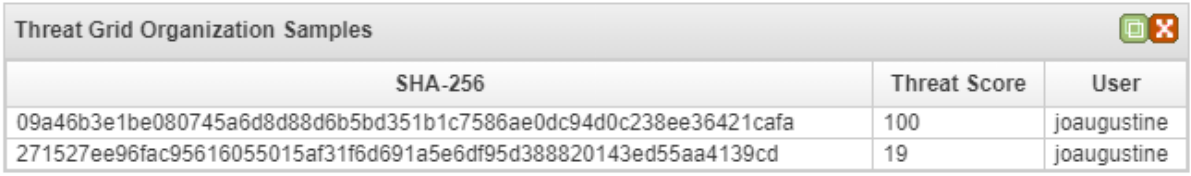


- Return to the QRadar **Dashboard** and select **Threat and Security Monitoring** in the **Show Dashboard** drop down menu.

- Click on **Add Item…** and select **Cisco Threat Grid** > **Cisco Threat Grid Submissions.**



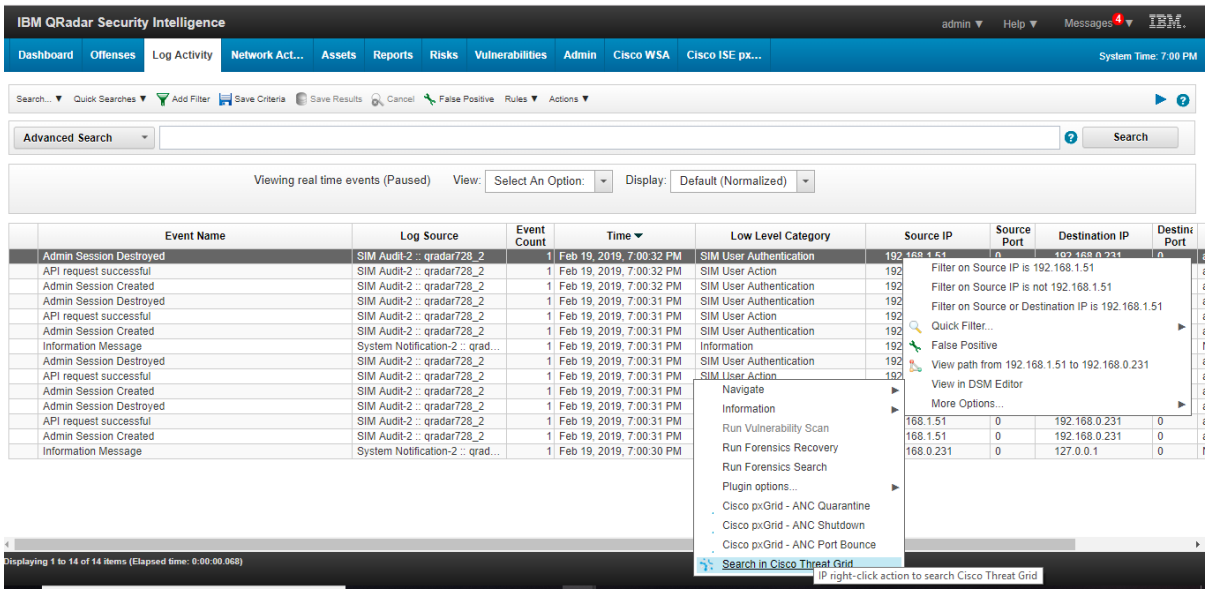
- Sample **Dashboard** is shown below:



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 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.

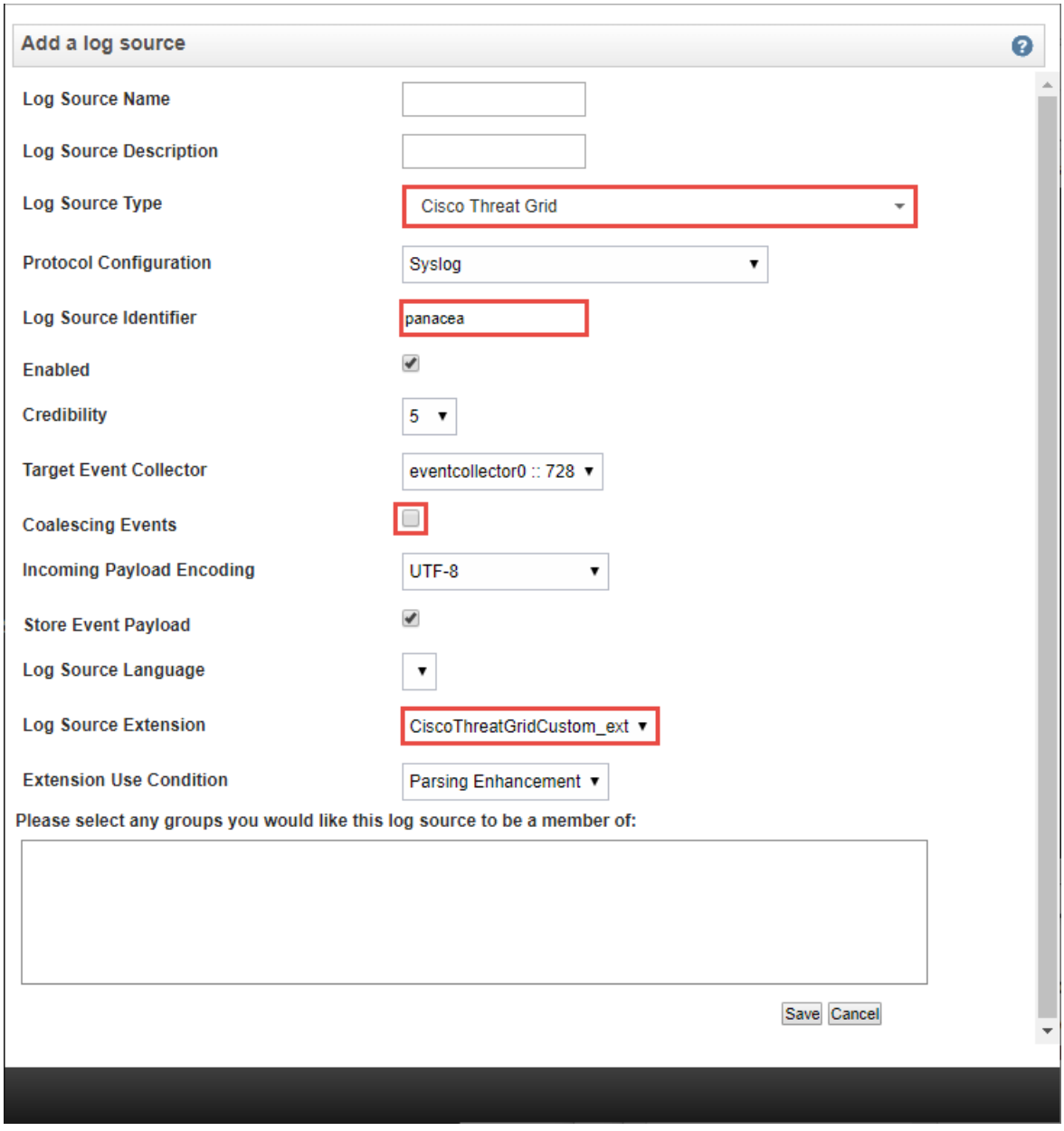
  These incidents will be stored persistently in IBM QRadar as events and show up in the IBM QRadar Console. This will allow end users to view and use Cisco Threat Grid incident data in IBM QRadar.

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**



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.