Contextual SmartResponse Plugin Guide: VirusTotal

November 14, 2017 – Revision A

Introduction

This guide describes the VirusTotal SmartResponse Plugin, the plugin's available actions, and how to configure the plugin. The plugin submits a file or URL to VirusTotal (www.virustotal.com) for analysis. The returned information includes:

- Detection information from multiple scan engines
- The date of first scan/submission
- The positive detection ratio
- VirusTotal's permanent link for the scan report, which can contain additional submission type-specific scan results and other information

Prerequisites

- To use this SmartResponse Plugin, you must be running LogRhythm Web Console version 7.2.3 or later.
- You must be running .Net Framework 4.5.2. You can verify your .Net version by checking in the Windows Control Panel—click **Start**, click **Control Panel**, and then click **Programs and Features**.
- Any host system—other than the Platform Manager—that intends to execute this plugin must add the SmartResponse executable folder to the Windows "Path" environment variable. If the LogRhythm agent is installed in the default location, this path is C:\Program Files\LogRhythm\LogRhythm System Monitor\state\SmartResponse\Plugin\bin.

  To add the SmartResponse folder to the path variable:

  1. Click **Start**, and then click **Control Panel**.
  2. Click **System and Security**, click **System**, and then click **Advanced system settings**.
  3. Click the **Advanced** tab, and then click **Environment Variables**.
  4. In the System Variables section, navigate to the "Path" variable, and then click **Edit**.
  5. Add the path to the existing string, separating the new text with a single semicolon.
     - For example, <*existing environment variables*>; C:\Program Files\LogRhythm\LogRhythm System Monitor\state\SmartResponse\Plugin\bin
- The Plugin requires access to the internet from the executing host.
- You must have a VirusTotal API key. To acquire an API key, you must first sign up for a free account on VirusTotal.com. For more information, see https://www.virustotal.com/en/user/<*username*>/apikey.

Import the Plugin

To import a SmartResponse Plugin:

1. Log in to the Client Console as a Global Administrator.
2. On the main toolbar, click **Deployment Manager**.
3. On the **Tools** menu, click **Administration**, and then click **SmartResponse Plugin Manager**.

   The SmartResponse Plugin Manager window appears.
4. Click the **Actions** menu, and then click **Import**.
5. Locate and select the SmartResponse Plugin (*.lpi) that you want to import, and then click **Open**.
6. If you are prompted to accept the terms of the Sample Code License Agreement, read and accept the terms, and then click **OK**.

   The plugin loads in the SmartResponse Plugin Manager, and the associated actions are now available in the Web Console.

NOTE: For more information about SmartResponse actions or manual execution from the Client Console, see the application Help in the LogRhythm Client Console.

Run the Plugin from the Web Console

1. Log in to the Web Console, and then click **Dashboards**.
2. In the lower-right corner of the screen, click the **Logs** tab.
3. Click a log entry, and then click the gear symbol that appears in any column.

   The Inspector panel appears at the right side of the screen.
4. Scroll to the Smart Response section of the Inspector panel.
5. From the Plugin menu, select **Contextual Virus Total Query**.
6. From the Action menu, select either **VirusTotal : Scan File** or **VirusTotal : Scan URL**.

   For more information on these actions, see SmartResponse Plugin Actions.
7. Enter the following information:
   a. If running the Scan File action: In the Data File Path field, enter the full file path to the target file that will be submitted to VirusTotal. In the VirusTotal API Key field, enter the VirusTotal API Key.
   b. If running the Scan URL action: In the URI/URL field, enter the full target URI/URL that will be submitted to VirusTotal. In the VirusTotal API Key field, enter the VirusTotal API Key.
8. From the Execute from menu, select whether to run this plugin from either the **Platform Manager** or a designated Agent.
9. Click **Run**.

   The SRP results open in a new tab.

SmartResponse Plugin Actions

Each SmartResponse Plugin can have one or more actions. This plugin contains the following actions:

- Upload a file to VirusTotal for analysis.
- Submit a URI/URL to VirusTotal for analysis.

VirusTotal : Scan File

Description

This action uploads a file from a defined path on the target machine to VirusTotal for analysis. Once uploaded and analyzed, VirusTotal returns the results of the file scan, as well as which, if any, scanners returned positive results.

Use Case

A file observed during an investigation is suspected to be malicious. This SmartResponse Plugin sends the file to VirusTotal, whose antivirus scanning engines run against the file.

Parameters

This action expects the following dynamic or user-supplied parameters to be configured in the Actions tab of an Alarm:

Name	Type	Details
File Path/Name	String	The full file path to the target file that will be submitted to VirusTotal for scanning
VirusTotal API Key	Encrypted String	The VirusTotal API Key (see Prerequisites)

VirusTotal : Scan URL

Description

This action submits a URI/URL to VirusTotal for analysis. Once uploaded and analyzed, VirusTotal returns the results of the URL scan, as well as which, if any, scanners returned positive results.

Use Case

A URL observed during an investigation is suspected to be malicious. This SmartResponse Plugin sends the URL to VirusTotal, whose antivirus scanning engines run against the URL.

Parameters

This action expects the following dynamic or user-supplied parameters to be configured in the Actions tab of an Alarm:

Name	Type	Details
URI/URL	String	The full target URI/URL that will be submitted to VirusTotal for scanning
VirusTotal API Key	Encrypted String	The VirusTotal API Key (see Prerequisites)