SmartResponse Plugin Guide:

Office 365 Security & Compliance Controller

December 17, 2018 – Revision B

Author: Jtekt Source: https://github.com/Jtekt/LogRhythm

Introduction

This guide describes the Office 365 Security & Compliance Controller Plugin, the plugin's available actions, and how to configure the plugin. This plugin submits commands via powershell to Microsoft's Security & Compliance Center API.

Prerequisites

- This SmartResponse Plugin is compatible with LogRhythm Enterprise 7.3.4 and later.
- An Office 365 tenant is required.
- Appropriate permissions and credentials are required to use this plugin. These steps are outlined on *Appendix A*.
- The PowerShell execution policy on the host where the SmartResponse plugin will be executed must allow the execution of scripts. Set this policy to either AllSigned or Unrestricted.
- This plugin requires access to the internet.
    - https://ps.compliance.protection.outlook.com

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. On the **Actions** menu, click **Import.**
5. Locate and select the SmartResponse Plugin (.lpi file) that you want to import, and then click **Open**.
6. If you are prompted to accept the terms of a 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 Actions tab of LogRhythm Alarm Rules.

   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 **365 S&C**
6. From the Action menu, select a plugin action.
7. Enter the required information for your selected action.
8. From the Execute from menu, select whether to run this plugin from either the **Platform Manager** or a designated agent.
9. Click **Run**.

SmartResponse Plugin Actions

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

- Search
- Purge*
- Search & Purge*

**Deleted content is removed with the -PurgeType of Soft. Details on this are available from Microsoft here: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesearchaction?view=exchange-ps*

Search

Description

This action initiates a content search against all tenant exchange locations. Content search can be based on any combination of the four fields: Sender, Recipient, Subject, Attachment.

Use Case

In response to an investigation, an analyst can initiate an Office 365 content search for a specific attachment, sender , subject, or recipient. These results are available within the Security and Compliance – Content Search page available at https://protection.office.com.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm. Note that some parameters are required to run the plugin, while others are optional.

Name	Type	Details	Required?
Username	String	Account used to conduct the search. Format: user@domain.com	Yes
ID	String	Unique identifier for the requested search.	Yes
Sender	String	E-mail address of sender	No
Recipient	String	E-mail address of recipient	No
Subject	String	E-mail subject **Subject must be contained within ‘ ‘ characters.**	No
Attachment Name	String	E-mail attachment name	No
Password	String	Account used to conduct the search.	Yes

Purge

Description

This action initiates a content purge against all items identified by a content search. Content purge can is based on the provided ID string. The ID provided must be a previously completed content search.

Use Case

In response to an investigation, an analyst can initiate an Office 365 content purge based on the results of a content search.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm. Note that some parameters are required to run the plugin, while others are optional.

Name	Type	Details	Required?
Username	String	Account used to conduct the search. Format: user@domain.com	Yes
ID	String	Existing content search Name.	Yes
Password	String	Account used to conduct the search.	Yes

Search & Purge

Description

This action initiates a content search followed by a content purge against all items identified by the content search.

Use Case

In response to an investigation, an analyst can initiate an Office 365 content search and purge.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm. Note that some parameters are required to run the plugin, while others are optional.

Name	Type	Details	Required?
Username	String	Account used to conduct the search. Format: user@domain.com	Yes
ID	String	Unique identifier for the requested search.	Yes
Sender	String	E-mail address of sender	No
Recipient	String	E-mail address of recipient	No
Subject	String	E-mail subject **Subject must be contained within ‘ ‘ characters.**	No
Attachment Name	String	E-mail attachment name	No
Password	String	Account used to conduct the search.	Yes

Appendix A – 365 Security and Compliance Permissions

It is advised to create a custom role with only the required permissions associated with this plugin.

1. Log into Office 365 Security and Compliance center
2. Navigate to Permissions
3. Select **Create**
    a. Enter name: SIEM Operations
    b. Description: S&C permissions required to permit authorized security analysts to perform content searches and quarantines.
4. Click on menu option: **Next**
5. Select: **Choose roles**
6. Select: **+ Add**
7. Search for and select the following:
    a. Export
    b. Search and Purge
    c. Compliance Search
8. Click: **Add**
9. Click: **Done**
10. Select: **Next**
11. Select: **Choose members**
    a. Add appropriate users or service account
12. Click: **Next**
13. Select: **Create role group**