

SmartResponse Plugin Guide: CyberArk Response Manager

November 16, 2018 – Revision A

Introduction

This guide describes the CyberArk Response Manager SmartResponse Plugin, the plugin's available actions, and how to configure the plugin. This plugin performs a variety of actions in the CyberArk Response Manager platform, including viewing account history details, forcing credential changes, and raising or lowering account security privileges.

Prerequisites

- This SmartResponse Plugin is compatible with LogRhythm Enterprise 7.2.7 and later.
- To use this plugin, you must be running PowerShell v3.0 or later. To determine your PowerShell version, open PowerShell and enter **\$PSVersionTable.PSVersion** at the prompt. If necessary, download a new version from the Microsoft Download Center.
- 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**.
- CyberArk Response Manager (CARM) must be installed and configured. For more information, see the CyberArk Integrations section of the CyberArk Support Vault.

NOTE: The plugin must be executed through a LogRhythm System Monitor Agent installed on the same host as the CARM.

- CyberArk Application Identity Manager must be installed and configured for a privileged account on any endpoint from which you want to execute the plugin.
- Python 2 must be installed in the path of any endpoint from which you want to execute the plugin.
- The plugin requires access to the internet.

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 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 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.

SmartResponse Plugin Actions

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

- Account History
- Disable User
- Enable User
- Force Credential Change
- Lower Account Security Policy
- Raise Account Security Policy

Account History

Description

This plugin displays CyberArk credential access details for a target account during a specific time period.

Use Case

An analyst investigating a user's account history runs this action and receives contextual information such as user, action performed, reason given, and time of action.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details
Address	String	The HostImpactedName value from the Alarm's MetaData field.
User	String	The UserOrigin value from the Alarm's MetaData field.
Time Range	Integer	The time range (in hours) for which you want to retrieve account information. The default value is the previous 4 hours.

Disable User

Description

Using the CyberArk user name as a parameter, this action disables a CyberArk user.

Use Case

When a CyberArk user account is suspected of being compromised, an analyst disables the user account until a final determination can be made.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details
User	String	The UserOrigin value from the Alarm's MetaData field.

Enable User

Description

Using the CyberArk user name as a parameter, this action enables a CyberArk user.

Use Case

An analyst re-enables a user account that was cleared of suspicion or incorrectly disabled during the course of an investigation.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details
User	String	The UserOrigin value from the Alarm's MetaData field.

Force Credential Change

Description

This action marks an account for immediate password change.

Use Case

An analyst detects a security event that requires an immediate password change of a CyberArk account that cannot wait for the next password rotation, and executes this plugin to force the change.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details
Address	String	The HostImpactedName value from the Alarm's MetaData field.
User	String	The UserOrigin value from the Alarm's MetaData field.

Lower Account Security Policy

Description

This action drops an account down to the next lowest security policy listed in the policySecuritySets parameter.

Use Case

An analyst investigating a suspicious privileged account uses this plugin to lower the account's security policy, preventing more privileged user access.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details
Address	String	The HostImpactedName value from the Alarm's MetaData field.
User	String	The UserOrigin value from the Alarm's MetaData field.

Raise Account Security Policy

Description

This action raises an account up to the next highest security policy listed in the policySecuritySets parameter.

Use Case

An analyst raises account show/copy/connect requirements for security purposes, then temporarily moves an individual account to the more restrictive security platform so it can perform specific tasks.

Parameters

This action expects the following parameters to be configured in the Actions tab of an Alarm.

Name	Type	Details
Address	String	The HostImpactedName value from the Alarm's MetaData field.
User	String	The UserOrigin value from the Alarm's MetaData field.

© LogRhythm, Inc. All rights reserved

This document contains proprietary and confidential information of LogRhythm, Inc., which is protected by copyright and possible non-disclosure agreements. The Software described in this Guide is furnished under the End User License Agreement or the applicable Terms and Conditions ("Agreement") which governs the use of the Software. This Software may be used or copied only in accordance with the Agreement. No part of this Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than what is permitted in the Agreement.

Disclaimer

The information contained in this document is subject to change without notice. LogRhythm, Inc. makes no warranty of any kind with respect to this information. LogRhythm, Inc. specifically disclaims the implied warranty of merchantability and fitness for a particular purpose. LogRhythm, Inc. shall not be liable for any direct, indirect, incidental, consequential, or other damages alleged in connection with the furnishing or use of this information.

Trademark

LogRhythm is a registered trademark of LogRhythm, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or service marks of their respective holders.