User Manual to GCI Security Smart Response

# Table of Contents

Contents

[Table of Contents iii](#_Toc513199656)

[Introduction v](#_Toc513199657)

[Smart Response - Lockdown Script 3](#_Toc513199658)

[Summary 3](#_Toc513199659)

[Tutorial 3](#_Toc513199660)

[Limitations 3](#_Toc513199661)

[Smart Response – Host and Port Sweep Script 5](#_Toc513199662)

[Summary 5](#_Toc513199663)

[Tutorial 5](#_Toc513199664)

[Limitations 5](#_Toc513199665)

[Smart Response – Carbon Black Script 7](#_Toc513199666)

[Video provides a powerful way 7](#_Toc513199667)

[Themes and styles also 7](#_Toc513199668)

[Video provides a powerful way 7](#_Toc513199669)

# Introduction

This user manual will be a basic guide on how to utilize the scripts that are stand alone as well as its limitations, conditions and maintenance.

Before diving into this document, it is advised to know PowerShell as well as xml. These scripts are meant to run on windows-based computers due to GCI’s computer base is mainly windows.

# Smart Response - Lockdown Script

Summary

This is a simple script that enables a quick and dirty lockdown on a target host. This can be used stand alone or with LogRhythm in tandem with the reporting and alarm reports. This can be used for specific cases due to its limitations stated below. prerequisites to using this script, one would need the highest credentials as an admin and target host.

Tutorial

Stand alone:

1. Open your terminal
2. Then do the command with the target IP. Example: \\(IP-Address) \c$
3. Drop the script into that target computer in a directory
4. Run the script by this command example using the IP and the path of the directory

Invoke-Command -ComputerName Server01, Server02 -FilePath c:\Scripts\DiskCollect.ps1

With LogRhythm: after the script has been imported into LogRhythm, enter the data to the target host with your admin credentials. Create an alarm that uses IP data and make sure that this script is held by the queue and needs to be approved to run. The tab on the right in LogRhythm’s web UI select the script on the target host and click run.

Limitations

Limitations to this script are:

1. You need to send your admin credentials.
2. The credentials are converted to text and is not secure using it along without LogRhythm.
3. This script only works on windows OS.

# Smart Response – Host and Port Sweep Script

Summary

This in tandem with LogRhythm can be useful for creating an internal report for basic penetration testing. Scanning for open ports, IP’s and other addresses can help reduce risk in a company.

Tutorial

With LogRhythm: after the script has been imported into LogRhythm, enter in the start IP address and the and IP address for the range in which you would like to scan. The tab on the right in LogRhythm’s web UI select the script on the target host and click run.

Limitations

Limitations to this script are:

1. You could just use Nmap or various tools.
2. This script only works on windows OS.

# Smart Response – Carbon Black Script

Summary

This script mainly works with LogRhythm and functions in Carbon Black with PowerShell. The invoke command and passing arguments and commands happen in a JSON body. Prerequisites to using this script, having an API key for Carbon Black and a target. This helps reduce switching dashboards and executing commands with LogRhythm and Carbon Black.

Tutorial

With LogRhythm: the certain commands available are:

1. Get
2. Delete
3. Isolate
4. Memdump
5. Kill
6. The command below shows the parameters needed after importing your script into LogRhythm. The items needed to run this command are a target host, API key, URL to the carbon black server and a target file, host or process. The tab on the right in LogRhythm’s web UI select the script on the target host and click run.
7. .\Carbon\_Black\_Response.ps1 -hostname '<target host>' -key '<your API key>' -baseURL '<url to your Carbon Black server>' -command 'delete/get/isolate/memdump/kill' -object '<target file on remote system>'

Limitations

Limitations to this script are:

1. This can only be run with LogRhythm.
2. The feed for the information is sent only to LogRhythm from carbon black and not the other way around and will have to use the alerts in LogRhythm.
3. Only events that need these commands you can respond automatically.
4. This script is dangerous if left unchecked and needs to be held by the queue of approvals before running.
5. This script only works on windows OS