

# ThreatConnect® SmartResponse™ Plugin LogRhythm®

User Guide

Software Version 1.0

August 4, 2020

30051-02 EN Rev. A

ThreatConnect, Inc. 3865 Wilson Blvd., Suite 550, Arlington, VA 22203 P: 1.800.965.2708 | F: .703.229.4489 www.ThreatConnect.com ©2020 ThreatConnect, Inc.

ThreatConnect<sup>®</sup> is a registered trademark of ThreatConnect, Inc. LogRhythm<sup>®</sup> is a registered trademark of LogRhythm, Inc. SmartResponse<sup>™</sup> is a trademark of LogRhythm, Inc.



www.ThreatConnect.com info@threatconnect.com

TOLL FREE: 1.800.965.2708 LOCAL: +1.703.229.4240 FAX: +1.703.229.4489

THREATCONNECT, INC. 3865 WILSON BLVD., SUITE 550 ARLINGTON, VA 22203



# Table of Contents

OVERVIEW	4
DEPENDENCIES	4
ThreatConnect Dependencies LogRhythm Dependencies	4 4
NSTALLATION	5
Plugin Actions: LogRhythm-to-ThreatConnect Indicator Upload and Enrichment	5
File Configuration	5
Creating a SmartResponse Plugin	5
Importing the SmartResponse Plugin	7
Testing Plugin Actions	8
Using Plugin Actions	.11

. . . .

# **OVERVIEW**

The ThreatConnect integration package for LogRhythm allows LogRhythm users to interact with threat intelligence in ThreatConnect directly from the LogRhythm Console by using a set of LogRhythm plugin actions. The integration package can perform functions such as retrieving Indicator details and reporting observations and false positives to ThreatConnect.

# DEPENDENCIES

# ThreatConnect Dependencies

• Active ThreatConnect Application Programming Interface (API) user and key

NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration on the Account Settings screen within their Private Instance of ThreatConnect.

• ThreatConnect installation zip file (contains ThreatConnect LogRhythm plugin actions): ThreatConnect-LogRhythm-Package\_vX.X

# LogRhythm Dependencies

- LogRhythm Console (web and PC based)
- PowerShell v4+ installed on Platform Manager

# Plugin Actions: LogRhythm-to-ThreatConnect Indicator Upload and Enrichment

LogRhythm plugin actions perform a number of functions, including creating Indicators in ThreatConnect, getting more information about an Indicator, and reporting an observation. These actions are bundled within a LogRhythm SmartResponse. Before these plugins can be created, the ThreatConnect file must be configured.

# File Configuration

Follow these steps to configure the ThreatConnect file:

- 1. Unzip the provided ThreatConnect file, ThreatConnect-LogRhythm-Package\_vX.X.zip, into any folder.
- 2. One of the files within the zip file is named **tc.conf.default**. Rename the file to **tc.conf**.
- **3.** This file controls various aspects of the integration commands. Edit the file, and update the required value and any of the optional values. Detailed information about the settings is in the file itself.

# Creating a SmartResponse Plugin

Follow these steps to create the SmartResponse plugin:

- 1. Run the LogRhythm PC Console application.
- 2. Open the Deployment Manager.
- Click on the Tools menu, and then choose Administration > SmartResponse Plugin Manager (Figure 1).

Rhythm	Console			+	al	192.168.4.59	-	-∂ ×		-
	2. Personal Dashboard	l 🔍 Investigati	е 🧕 Т	fail 🔹 Report Center 🔳	List Manager 🞽 Deploy	ment Monitor 👩 Deploy	ment Manager			
dit Vie	W LooRhythm Tools	Window Help								
on the	in my cograny and room	Trindon Help								
		Monitor	·							
Deploy	ment Manager	Search								
in the second	Final And Final	Report Ctrl+R		L.H. S. Carbon Marihan		D. F. S. Alazar Bulan D				
nuties	Hattorm Manager D	Knowledge	Netwo	ork monitors System monitors	Log Sources Log Processin	Policies Administers Per	pie			_
irm rules		A stanis interation								
)rag a co	lumn header here t	Administration	· 24	Deployment Monitor	Ctrl+D					
Action	Alarm Burerman	Distribution	• 🐻	Deployment Manager	Ctrl+Y	Threshold	Data Segregation Mode	Description	Log Entity	Log Hor
				Windows Host Wizard						
N	Invalid logon Test Alarm	Ena	bled	Automatic Log Source Config	uration	Single Event	None	Used for testing Report Observation on an invalid logon		
	Test Alarm for triggering P	laybook Dis	able	the registered coming		Single Event	None	Test alarm for triggering PB		
Ē	QsEMP : Excessive Suspi	icious Activity Dis	able	Global Log Processing Rule M	anager	100 Events in 60 Min(s), 0_	None	Alarms on excessive occurrences of concerning security events		
П	QsEMP : Successive Atta	cks Dis	able	Data Masking Rule Manager		5 Events in 15 Min(s), 0 Se.	None	Alarms on successive occurrences of concerning security events		
Π	QsEMP : Compromise	Dis	able	Court Director Management		Single Event	None	Alarms on the occurrence of any compromise	Π	
Π	QsEMP : Excessive Login	Failures Dis	able	Smartkesponse Plugin Manag	er	100 Events in 60 Min(s), 0	None	Alarms on excessive login failures	П	
П	QsEMP : Successive Logi	n Failures Dis	able	System Monitor Päckage Man	ager	3 Events in 15 Min(s), 0 Se.	None	Alarms on successive login failures	Π	
Π	QsEMP : Network Device	Excessive. Dis	able	System Monitor Configuration	Policy Manager	100 Events in 60 Min(s), 0	None	Alarms on excessive critical, error, and warning conditions on a N_	Π	
	QsEMP : Network Device	Critical Con. Dis	able	Data Lors Defender Policy Ma		Single Event	None	Alarms on a critical condition on a Network Device		
	QsEMP : "NIX Host Exces	sive Warnin Dis	able	States Selender Folicy ind		100 Events in 60 Min(s), 0	None	Alarms on excessive critical, error, and warning conditions on a *N.		
	QsEMP : "NIX Host Succe	ssive Errors Dis	able	File Integrity Monitor Policy N	lanager	5 Events in 15 Min(s). 0 Se.	None	Alarms on successive critical and error conditions on a *NIX host		
	QsEMP : "NIX Host Critica	al Condition Dis	able	Registry Integrity Monitor Pol	icy Manager	Single Event	None	Alarms on a critical condition on a *NIX host		
	QsEMP : Windows Host E	excessive W_ Dis	able	Log Source Virtualization Tem	plate Manager	100 Events in 60 Min(s), 0	None	Alarms on excessive critical, error, and warning conditions on a wi		
	QsEMP : Windows Host S	uccessive_ Dis	able	Automatic Log Source Accent	ance Rule Manager	5 Events in 15 Min(s), 0 Se.	None	Alarms on successive critical and error conditions on a windows h		
	QsEMP : Windows Host C	Critical Condi. Dis	able	Automotic cog boorce Accept	unce none monoger	Single Event	None	Alarms on a critical condition on a windows host		
	QsEMP : LogRhythm App	liance Hard_ Dis	able	Object Permissions Manager		Single Event	None	Alarm for warning/error events from the LogRhythm Appliance har		
	QsEMP : Network Device	Successive Dis	able 🔒	Security Manager		5 Events in 15 Min(s), 0 Se.	None	Alarms on successive critical and error conditions on a Network D.,		
	QsEMP : Privileged User	Created Dis	able	User Profile Manager		Single Event	None	Alarms on the occurrence of a user account being added to a privil.		
	QsEMP : Afterhours Privil	eged User L. Dis	able	QUENT TOUR	10 10111(0), 0 000(0)	Single Event	None	Alarms on the occurrence of an afterhours administrator login		
	QsEMP : Excessive Audit	Failures Dis	abled	QsEMP: Audit	60 Min(s), 0 Sec(s)	50 Events in 60 Min(s), 0 S.	None	Alarms on excessive audit failures		
	QsEMP : Successive Audi	it Failures Dis	abled	QsEMP: Audit	30 Min(s), 0 Sec(s)	3 Events in 15 Min(s), 0 Se.	None	Alarms on successive audit failures		
	LogRhythm CMDB Databa	se Error Ena	abled	LogRhythm Diagnostics	2 Hour(s), 0 Min(s), 0_	Single Event	None	Alarms when the Case Management Database has utilized more t		
	LogRhythm CMDB Stats W	/arning Ena	abled	LogRhythm Diagnostics	2 Hour(s), 0 Min(s), 0_	Single Event	None	Alarms on the occurrence when the LogRhythm Job Manager is u		
	LogRhythm CMDB Databa	se Warning Ena	bled	LogRhythm Diagnostics	2 Hour(s), 0 Min(s), 0_	Single Event	None	Alarms on the occurrence of the Case Management Database rea		
	LogRhythm AD Sync Failu	re Dis	abled	LogRhythm Diagnostics	2 Hour(s), 0 Min(s), 0_	Single Event	None	The LogRhythm Platform Manager has failed when attempting to		
	LogRhythm Scheduled Re	port Failure Dis	abled	LogRhythm Diagnostics	2 Hour(s), 0 Min(s), 0_	Single Event	None	The LogRhythm Job Manager has encountered an error when atte.		

# Figure 1

4. Select the Create Plugin menu option (Figure 2).

SmartRe	sponse Plugi	in Manager						8		×
Action	s 🕶 🛃 Cre	ate Plugin 👩 Propertie	es							
Action	Name	Create Plugin	Status	Version	Last Updated On	Plugin ID	Plugin GUID	AIE Count	Alarm Count	Act
		Create Plugin						_	-	_

### Figure 2

- Select the folder that contains all the unzipped contents of ThreatConnect-LogRhythm-Package\_vX.X.zip, including the tc.conf file that was renamed and edited during the file configuration process.
- 6. Click the Validate button. A "Success" message will appear (Figure 3).



#### Figure 3

- 7. Click the **Create** button, and then choose a folder in which to save the plugin.
- 8. The SmartResponse plugin will be created with a name similar to the following: ARPlugin\_0000000-0000-0000-0000-0000000000000\_20180118.lpi.

NOTE: The date is the last part of the filename, so if another SmartResponse plugin is created on the same day, the original file will be overwritten.

# Importing the SmartResponse Plugin

**1.** From the **Actions** menu, choose the Import option (Figure 4).

Deploy	ment Manager														
intities	Platform Manager Data Pro	essor	a Al Engine Ne	etwork Monitors System Monitor	s Log Sou	irces Log Process	ing Policies Alarm Rules	People							
arm Rule:	3														
		to a sta	at a diama												
Jrag a co	Jumn neader here to group	by th	lat column.		-		1							1	1
Action	Alarm Rule Nan	ne .	Status	Alarm Rule Group	5	Suppress For	Threshold	Data Segre	egation Mode		Description		-	Log Entity	Log Hos
	E Levelid Jesse Test Aleve		SmartResponse PI	ugin Manager									×		
	Test Alarm for triagering E	0	A												
님	OsEMP : Excessive Suspi	0	Actions*	Create Plugin 😗 Properties		1		1	1		The second second	1	-		H
H	QsEMP : Successive Attac	Acti	Sa Activate		Status	Version	Last Updated On	Plugin ID	Plugin GUID		AIE Count	Alarm Count	Act	H	
H	QsEMP : Compromise		3 Retire								-	-	=		
П	QsEMP : Excessive Login	-	wo Import	nect Integration Commands_23	Active	1	1/11/2018 5:15:39.303 PM	1000000024	6373804a-2311	-4739-beed-b59b6179080c	0	2	5	n n	
H	QsEMP : Successive Logi	_	day Export	nect Integration Commands_24	Active	1	1/18/2018 11:20:58.270 AM	100000025	d6ab0b59-932d	-44b3-8383-1bbe/34e6bt8	0	0	5	П	П
П	QsEMP : Network Device		dan export										N		
	QsEMP : Network Device														
	QsEMP : "NIX Host Exces												'N	- 0	
	QsEMP : "NIX Host Succe														
	QsEMP : "NIX Host Critica														
	QsEMP : Windows Host E												vi	-	
	QsEMP : Windows Host S	1											h		
	QsEMP : Windows Host C												-		
	QsEMP : LogRhythm App	Acti	000							Parameter			ar.	- 🗆	
	QsEMP : Network Device	FRI	W1							(A)	-		P.		
	QsEMP : Privileged User (	K) I	AU							E			vil	- 🗆	
	QsEMP : Afterhours Privil														
	QsEMP : Excessive Audit														
	UsEMP : Successive Audi												-		
	LogHnythm CMDB Databa											Close	L L		
	LogRhythm CMDB Stats V	- 145	Techt 1	LeeDin they Discovering		Heurie) 0 Mir (-)	Cineta Event	Masa		Alarma on the occurrence	of the Case M	in a new set D-t-l	U.		
Ц	LogRinythm CMDB Databas	e War	rning Enabled	LogRnythm Diagnostics	4	Hour(s), U Min(s), I	D. Single Event	None		The Lee Phyther Platform M	or the Case Ma	inagement Data	pase rea.		
U	Logranythm AD Sync Failu	e	Disabled	LogKnythm Diagnostics	4	nour(s), U Min(s), I	J. Single Event	None		The Logrinyalm Platform M	nanager has tai	ied when attem	pung to		

## Figure 4

- 2. Select the file created in the "Creating a SmartResponse Plugin" section.
- **3.** If a window appears warning that the GUID is already being used and asking if you would like to import with a new GUID (Figure 5), click the **Yes** button.



# Figure 5

4. The new SmartResponse will be reflected in the window (Figure 6).

0	Action	ns 🔹 🛃 Create Plugin 👩 Properties								
Acti	on	Name	Status	Version	Last Updated On	Plugin ID	Plugin GUID	AIE Count	Alarm Count	Ac
								-	=	-
1		ThreatConnect Integration Commands_31	Active	1	1/24/2018 11:01:31.663 AM	100000032	22139b14-4beb-46a9-b01e-7bfb9e6899f0	0	1	5

# Testing Plugin Actions

The SmartResponse plugin has five possible actions:

- Create Indicator: Creates an Indicator in ThreatConnect.
- Lookup Indicator: Retrieves information about an Indicator (if it exists) in ThreatConnect.
- **Report False Positive**: Increments the False Positive count for the given Indicator in ThreatConnect.
- **Report Observation**: Increments the Observation count for the given Indicator in ThreatConnect.
- **Trigger Playbook**: Triggers a Playbook within ThreatConnect. A data value can be passed to the Playbook.

Each action can be tested within LogRhythm to determine whether the connections between systems are working and to demonstrate the use of each action.

# NOTE: If a plugin action affects data in ThreatConnect, which is the case for all of the actions except Lookup Indicator, then testing the action will cause the data in ThreatConnect to be updated accordingly.

- **1.** Open the SmartResponse Plugin Manager.
- Select the SmartResponse in the top half of the window. The plugin actions to be tested will show in the list at the bottom of the window. In this example, the ThreatConnect:
   Lookup Indicator action is selected (Figure 7). This action is the simplest to test because it involves only data retrieval and thus does not change any of the data within ThreatConnect.

Action	Name	Status	Version	Last Updated On	Plugin ID	Plugin GUID	AIE Count	Alarm Count	A
							=	=	-
	ThreatConnect Integration Commands_31	Active	1	1/24/2018 11:01:31.663 AM	100000032	22139b14-4beb-46a9-b01e-7bfb9e6899f0	0	1	5
¢									:
c Actions						Parameters			3
c Actions						Parameters			3
< Actions C Actions Threat(	Connect: Lookup Indicator					Parameters			3

### Figure 7

**3.** Double click the selected line, and a window showing all of the parameters that the action takes will appear (Figure 8).

lit View	My LogRhythm Tools	Window H	elp	1.	1 -	1.4.1	,								
Deployn	nent Manager			: Smart Respo	nse Action Prope	erties				- 0 3	<				•
ities P	latform Manager Data Proce	essors AI E	ingine Netwo	Action : Threa	tConnect: Lookup	Indicator									
m Rules				Parameters											
ag a col	umn header here to group I	by that colu	mn.	Define the comma	ind line parameters	s that pass constant value	es or data fields to the	executable location.							
Action	Alarm Rule Name		Status	Name	Switch	Туре	/ Value	Time Zone	Time Format	Test Value	▲ scription		_	Log Entity	Log Hos
		SmartRe	sponse Plugir	Script	-Filetc-lookup-i	in Fixed							×		
	Invalid logon Test Alarm			Debug Mode	-tcdebug	Constant Value						-			
	Test Alarm for triggering P	Action	ns• 🛃 Crea	ThreatConnect	-tcserver	Constant Value									
	QsEMP : Excessive Suspi	Action	Name	ThreatConnect	-tcapiuser	Constant Value					E Count	Alarm Count	Act		
	QsEMP : Successive Attac			ThreatConnect	-tcpw	Constant Value					L COURT	- Count			
	QsEMP : Compromise		ThreatConne	ThreatConnect	-tcowner	Constant Value					-	2	5		
	QsEMP : Excessive Login		ThreatConne	LogRhythm Data	-Irdata	Constant Value					~	0	5		
	QsEMP : Successive Logi			Test Settings											
	QsEMP : Network Device			Execute Smart R	esponse Action Fro	om : From Platfo	omManager	~		Browse			N_		
	QsEMP : Network Device			and the second second						The second s					
	QsEMP : *NIX Host Exces												'N		
	QsEMP : *NIX Host Succe			Script		C3									
	QsEMP : *NIX Host Critica			anumbal eva El	to leak up indicat	teres 1 todahus teres	er tozoiurer toou	toouner ledata t	ctimen tenne tonner	T	-				
	QsEMP : Windows Host E			powersneil.exe -rii	етсноокиряпаса	tor.ps 1 4cdebug 4cserve	er toppuser topw	Acowner Aroata A	cumeoutsecs toproxy -	lest			NI.		
	QsEMP : Windows Host S	<		Results									> h.		
	QsEMP : Windows Host C														
	QSEMP : LogRhythm App	Actions		1									/ ^ Br_		
	GSEMP : Network Device										_				
Ц	USEMP : Privileged User (	▶ ThreatC	onnect: Lookup							Close			VII.		
Ц	GEMP : Atternours Privile .	ThreatC	onnect: Report	Observation						11					
	USEMP : Excessive Audit	ThreatC	onnect: Report	False Positive						11			~		
Ц	Usemin : Successive Audi														L
Ц	LogRinythm CMDB Databa											Close			
H	LogRhythm CMDB Stats V	Manalan	Fashind 1	- Distance		2 Hourie) 0 Min(e) 0	Cineta Event	Mana	AI	arms on the occurrence	of the Case N	anagement Data	hase cer		2
H	LogPhythm CMDB Database	e warning	Disabled L	ogranythm Diagnos	ics	2 Hour(s), 0 Min(s), 0	Single Event	None	AI Th	ha LogPhythm Platform	Manager has f	anagement Data	notion to		-
	Logranythm AD Sync Failure		Disabled L	Logranythm Diagnos	105	2 Hour(s), U Min(s), U 2 Hour(s), 0 Min(s), 0	- Single Event	None	11	he Logrinyulm Platform	manager has t	alleo when attem	pung to_		L

- 4. Set values for each parameter in this window. Most of the parameters are self-explanatory and mirror those in the **tc.conf** file setup. Values entered in this window will override the corresponding values in **tc.conf**. Note the following information about two of the parameters:
  - -tcdebug controls whether debug information is shown or not. The values follow the PowerShell values for log outputs. The most commonly used value is Continue (shows all debug log lines, but does not interrupt the program from running). The default value is SilentlyContinue... (no log lines are output, and the program is not interrupted).
  - -Irdata is the LogRhythm data used by the action. In most cases, it will be an Indicator value (e.g., IP Address, Host). It is a required value.
- 5. Once value(s) have been entered and another field has been clicked in, the Script section of the window will reflect the changes (Figure 9). Typically, all the values mirrored in tc.conf were already set when the plugin was created, and so the only value that must be set here is -lrdata.

Name	Switch	Туре	1	Value	Time Zone	Time Format	Test Value	^
Script	-Filetc-lookup-in	Fixed						
LogRhythm Data	-Irdata	Constant Value	•	123.123.123.123				
ThreatConnect	-tcserver	Constant Value						
ThreatConnect	-tcapiuser	Constant Value	3					
ThreatConnect	-tcpw	Constant Value						
ThreatConnect	-tcowner	Constant Value						
Timeout	-tctimeoutsecs	Constant Value						Y
Execute Smart F	Response Action From	: From	n Platfon	mManager	~		Brow	58
powershell.exe -Fi	ile tc-lookup-indicator	ps1 -Irdata 123	123.123	.123 toserver toap	biuser topw toow	ner tctimeoutsecs tcpr	oxy - Tes	t

6. Once all parameter values have been entered, click the **Test** button towards the bottom right of the window. Click the **Yes** button on the next two dialog boxes (Figure 10 and Figure 11), and then the script will run.



# Figure 11

7. The Results should show the following: Executed: Success (Figure 12).



Script				•	
powershell.exe -File tc-lookup-indicator.ps1 4rdata 123.123.123.123.123 tcserver	-tcapiuser	tcpw tcowner	+ctimeoutsecs	toproxy -	Test
lesults					

8. Click the View Details button to view any output, including debug statements.

# Using Plugin Actions

The most common way to use the plugin actions is to have an Alarm Rule auto-execute them within LogRhythm. The following example demonstrates how to trigger a Playbook to execute within ThreatConnect when an Indicator from incoming LogRhythm data matches an Indicator existing in a LogRhythm List:

1. This example assumes that LogRhythm has an existing List, shown in Figure 13, that contains two Indicators (IP Addresses in this example). For details on how to set up external sources that would fill such Lists, please refer to the LogRhythm documentation.

		•
List Properties	- 0	×
Basic Configuration List Items Additional Settings		•
Testing List for Rules Add Item		
Add Item	Add List	
Filter	Expiration Date	
192.168.4.1	N/A N/A	
<		>
Remove Selected	Reset Expiration	
Import items Export items	OK Cancel Apply	

- 2. Open the Deployment Manager, and click the Alarm Rules tab.
- 3. Click the + button to create a new rule. A window for the rule will open (Figure 14).

Alarm Rule	* · · · ·	
Sala and Sa		
Frimary Criteria Filters reate fitters that identify Events to consider for alarming. All primary or	teria filters must be met in order for an Event to be considered. At least one Primary Otteria filter must be specified.	
Fields Filtered On		Record Type
inimum Event Priority		
ecify the minimum priority an event must have to be considered for a	laming.	
ent priority must be greater than: U		
mary Criteria Include Filters Exclude Filters Day and Time C	riteria Log Source Criteria   Aggregation   Settings   Notify   Actions   Information	

4. On the first tab shown at the bottom of the window, **Primary Criteria**, add a filter that compares the value in the **IP Address (Origin)** column (this column is for the incoming LogRhythm data) with any value in the List (Figure 15). Note that the term **Is** in the **Filter Mode** column indicates that a comparison/IN operation should be performed.

P Address (Origin)									
									 Custom
	Log Message F	ilter					×	<	
	<b>t t</b>	Add New Field Filter:			~	Edit Values	Delete		
	Operator	Field	Filter Mode	Filtered Values					
	•	IP Address (Origin)	ls	Testing List for Rules					
						ОК	Cancel		
inimum Event Priority						ОК	Cancel	1	
inimum Event Priority cdy the minimum priority an event must erit priority must be greater than:	have to be considered for alar	89.			C	ОК	Cancel	1	
inimum Event Priority ectly the minimum priority an event must erit priority must be greater than:	have to be considered for alarr	nng. Iria Log Source Criteria   Aggregation   Se	ttings Notify	Actions Information	C	ОК	Cancel	1	



5. Click on the Actions tab at the bottom of the screen. This tab is where the SmartResponse plugin is chosen and the values are set. In this example, the action is **Report Observation**, and the **LogRhythm Data** parameter is set to **IP Address (Origin)** (Figure 16).

NOTE: Make sure to click the Save Action button on this screen before moving on.

	1									
Execution Sequence	Action Name				Approval(s) Re	equired Exec	cution Target			-
un Actions ®At th	e Same Time 🔿 In the order lis	ted						1	Delete New J	Action
t Action ThreatCo	innect Integration Commands_31:	ThreatConnect: Rep	ort Observation							
arameters Define th	e command line parameters that n	ass constant values	or data fields to th	e executable						
lame	Switch	Tune	Value		-	Time Zone		Time Forma	,	
cript	-File to-report-observation ps	1 Fixed	Turbo			11110 2010		This Conta		_
ogRhythm Data	-Irdata	Alarm Field	< P Address	(Origin)>						
hreatConnect Server UR	L -tcserver	Constant Value								
hreatConnect User ID	-tcapiuser	Constant Value								
hreatConnect User PW	-topw	Constant Value								
pprovals					Execu	te SmartResponse	Action from:			
he action must be approve vel prior to being executed	d by at least one person in each	Add	Add Group	Delete	From F	latformManager				
				-						
evel Name			V	Туре						
wershell.exe -File to-report	observation.ps1 -Irdata <ip addr<="" td=""><td>ess (Origin)&gt; {cserve</td><td>r tcapiuser top</td><td>ow łcowne</td><td>r tctimeoutsec</td><td>в - Соргаху - Соргахуч</td><td>userid toproxypw todeb</td><td>ug SilentlyContinue</td><td>Save A</td><td>ction</td></ip>	ess (Origin)> {cserve	r tcapiuser top	ow łcowne	r tctimeoutsec	в - Соргаху - Соргахуч	userid toproxypw todeb	ug SilentlyContinue	Save A	ction

#### Figure 16

6. The rest of the tabs can be configured as needed for notifications, rule active time frames, etc. Please refer to LogRhythm documentation for full details.

Another way to use plugin actions is to run a SmartResponse Action within the web console to show more data about an Indicator:

1. Open the web console (dashboard) and log in. A screen similar to the one in Figure 17 will appear.



- 2. Click the Logs option in the bottom right-hand corner.
- 3. The resulting screen will show the events that have been captured. The columns can be filtered, marked as favorites, or displayed in themed groups (e.g., Application, Hosts, Location). The example in Figure 18 shows IP Address (Origin), IP Address (Impacted), and Host (Impacted) as favorite columns. It also displays the results of a filter that shows only log lines for which IP Address (Origin) is not blank.

:#LogRhy1	thm	Dashboard	s	Alarms Cases S	earches	Reports								Search	14	49 <del>-</del>	
D									•	Live Data 🛛 🛈	•	a e	📇 🔛 Securit	y Analyst Dashb	°D		Т
s			Ala	arms by Day Past 30 Days	Last 30 Days					Top Directi	OR Last 11		T				
385				1 10 1 1 pr: 24 pr: 31		100.07 km14	lan 21			External Internal Local			Unknown				
	83 Ever			DELY DELY	,		Juiter										
IP Address (Origin)	÷	IP Address (Impacted)	<b>#</b> ≑	Host (Impacted)	± ↓	Log Date	+	Log Count		Priority	44	Log Sou	се Туре		14 (C)	Classi	fical
(NonBlanks)	0	Type Here		Type Here		Select Timeframe		Type Here		Type Here		Type Her	2			Type H	lere
217.171.86.137	*		\$	galageband-ad *	\$	01/17/2018 2:15:52.013 pm	۰	1	\$	25	\$	Syslog - C	ther		\$	Failed f	Susp
82.146.166.56				patrophend with		01/17/2018 1:09:16.023 pm		1		25		Syslog - C	ther			Failed S	Susp
92.62.219.172				pringhanitat *		01/17/2018 12:53:54.020 pm		1		25		Syslog - C	ther			Failed S	Susp
192.168.4.1				pringhead of *		01/17/2018 11:29:22.017 am		1		31		Syslog - C	ther			Failed S	Susp
192.168.4.59				WIN-ONCAG8HNNNM *		01/12/2018 4:21:12:263 pm		1		25		MS Winde	ws Event Logging - A	Application		Authen	atica
192.168.4.59				WIN-ONCAG8HNNNM *		01/12/2018 2:58:14.407 pm		1		25		MS Winde	ws Event Logging - /	Application		Auther	ntica
192.168.4.59				WIN-ONCAG8HNNNM *		01/12/2018 11:13:17.300 am		1		25		MS Winde	ws Event Logging - /	Application		Authen	itica
192.168.4.59				WIN-ONCAG8HNNNM *		01/12/2018 11:11:01.507 am		1		25		MS Winde	ws Event Logging - A	Application		Authen	atica
192.168.4.59			۰	WIN-ONCAG8HNNNM *		01/12/2018 10:48:13.793 am		1		25		MS Winde	ws Event Logging - A	Application		Authen	atica
192.168.4.59				WIN-ONCAG8HNNNM *		01/12/2018 9:41:38.110 am		1		25		MS Winde	ws Event Logging - A	Application		Authen	atica
192.168.4.59				WIN-ONCAG8HNNNM *		01/11/2018 2:52:48.800 pm		1		25		MS Winds	ws Event Logging - /	Application		Authen	ntica
192.168.4.59				WIN-ONCAG8HNNNM *		12/19/2017 3:26:39.807 pm		1		25		MS Winde	ws Event Logging - /	Application		Authen	ntica
192.168.4.59				WIN-ONCAG8HNNNM *		12/19/2017 2:14:37.463 pm		1		25		MS Winde	ws Event Logging - A	Application		Authen	htica
192.168.4.59				WIN-ONCAG8HNNNM *		12/19/2017 2:12:20.447 pm		1		25		MS Winde	ws Event Logging - A	Application		Authen	atica
192.168.4.59				WIN-ONCAG8HNNNM *		12/19/2017 2:06:20.727 pm		1		25		MS Winds	ws Event Logging - A	Application		Authen	atica
192.168.4.59				WIN-ONCAG8HNNNM *		12/19/2017 1:56:36.277 pm		1		25		MS Winde	ws Event Logging - /	Application		Authen	atica
103 169 4 50				WINI CALCACOUNDING &		12/10/2017 1:06:54 412.000		1		26		MAC Islands	ur funnt Longing	antication		-	_

- 4. To find ThreatConnect information about a particular IP Address, select a cell on the row that contains the IP Address in question, and then click on one of the gear icons.
- **5.** A panel will open on the right-hand side of the screen (Figure 19). Under the **Actions** tab, click the down arrow for the **SmartResponse** section. Then choose a plugin action that will show all the parameters to be passed. Make sure the **LogRhythm Data** field is filled in with the IP Address in question. LogRhythm will list all available options when that field is selected.

								6	1				
:#LogRhy1	thm	Dashboards											<u> </u>
					Live Data 🕕 🕓	<u>ب</u> م	🗋 🔡 Securit;	Analyst Dashb		т	۵		
Alarm	ns by D	Day Past 30 Days Last 3				То	p Direction Last 11		т			l: IP Address (Origin)	
						Exter	nal	-					
						Local	al A				Actions		
									1		Value	Field	
10									1.000		value	Field	
												IP Address (Ori	igin)
											Pivot		
	Der 24	Dec 31	lan 14		Alarms				Unknown		Threat Intelligence		
-		-											
owing 44 of 144	183 Ever	nts C	Favoribes	Applicat	ion KBytes/Packets Cl	assification	Host Identity	Location Lo	g Network	2 <b>*</b>			
Address Origin)	- Ŧ	IP Address I (Impacted)	Host (Impacted)	1	Log Date	4	Log Count	∓ ≜ Priorit	v Å		C		
onBlanks)	0	Type Here	Type Here	*	Select Timefra	me	Type Here	Type H	ere	SNC	Smarckesponse		
7.171.86.137	0	6	advantant *	ø	01/17/2018 2:15:52.013 p	m <b>4</b>	F 1	<b>6</b> 25	0	Ĕ			
146.166.56			getrephendrat *	-	01/17/2018 1:09:16.023 p	m	1	25		8 A	meatconnect owne		
62.219.172			pringhand at *		01/17/2018 12:53:54.020	pm	1	25		ILS I	Please Select		
2.168.4.1			advantant -		01/17/2018 11:29:22:017	am	1	31		ETA	LonRhythm Data:		
2.168.4.59			WIN-ONCAG8HNNNM *		01/12/2018 4:21:12 263 p	m	1	25			317 171 06 137		
2.168.4.59			WIN-ONCAG8HNNNM *		01/12/2018 2:58:14.407 p	m	1	25			217.171.00.137		U
2.168.4.59			WIN-ONCAG8HNNNM *		01/12/2018 11:13:17.300	am	1	25					
2 168 4 59			WIN-ONCAG8HNNNM *		01/12/2018 11:11:01 507	am	1	25			Plaxa Salart		
2 168 4 59			WIN-ONCAG8HNNNM *		01/12/2018 10:48:13 793	am	1	25			Theose Selece		
2 168 4 59			WIN-ONCAG8HNNNM *		01/12/2018 9:41:38 110 a	m	1	25					
2 169 4 59			WINLONCACEUNNNM *		01/11/2018 2:52:48 800 0	m	1	25			Please Select		
2 169 4 59			WIN-ONCACEUNNNM *		12/10/2017 2:26:30 807 0	m	1	25					
2 169 4 50					12/10/2017 2:14:27 462 p		1	25					
2.100.4.59			WINCONCAGERINNIN *		12/19/2017 2.14.37.463 p			25			Diax a Colack		
2.108.4.59			WIN-ONCAG8HNNNM *										
2 3 M / 50					12/19/2017 2.12.20.447 p	m	1	25					
2.100.4.55			WIN-ONCAG8HNNNM *		12/19/2017 2:12:20.447 p	m	1	25					

6. Scroll down to the bottom of the panel on the right-hand side of the screen, and click on the **Run** option (Figure 20).

:#Logi	Rhythm	Dashboards											Search 🕴	· 🛓 -
D					🔵 Live Data	00	pa 🔓	Executiv	ve Dashboard	e c	T	۵		
CASES	Log Proces	sing Rate		Log, Event,	and Alarm Trend Last 3	) Days						Field: I	P Address (Impacted)	
				10k					Logs Processed By Dr			Actions		
				1.0k ———								Value	Field	- 1
		4		100	$\sim \sim \sim$	$\sim$	~~		Events					
	0	Log Rate (MPS)												
				1 Jan 07	Jan 14	Jan 21	Jan 28	Feb 04				Please Select		
												Debug Mode:		
	Top Classif	cation Last 128d 22h		Top Comm	on Event Last 128d 22h		Top Log	Source Type Las				SilentlyContinue		8
Cr Pr	ritical olicy		×.	General Error Lo	9		MS Windows	Eve				The statement of the st		
Ar St	ccess Failu tartup a			Configuration M.			MS Windows	Eve						
Fa	ailed			Authentication F	a_ 📃		MS Windows	Eve						
A	uth			AIE: Auth Failure			LooDhather							
Showing 51	of 14674 Eve									Network	*	Execute from: Plat	form Manager 👻	
IP Address	s 🖡	IP Address	Ŧ		<b>#</b>		Ξ.		<b>#</b>	<b>#</b>				
(Origin)	÷	(Impacted)	Host (Imp	acted)	Log Date	+ Timoframa	↓ Lo	g Count	Priority	0 L	NS			
(NOTIBIANK	5 <b>7 U</b>	Type nere	Type Here	last 4	Seler	od:16.017.cm	iy	penere	Type Here	*	EI I			
123.123.12	3 123		*	and a	01/22/2018 113	6:16:017 pm	**		25	*	& AG			
123.123.12	3.123		gringher	- 100 P	01/22/2018 1:3	3:33.017 pm	1		25	5	VILS			

### Figure 20

7. The results will open in a new browser tab (Figure 21).

silial cresponse Oucp	
SmartResponse Action:	ThreatConnect: Lookup Indicator
Run Time: 1072 ms	
Status: Completed suc	ccessfully
Output Results:	
Response: {     "address": {         "id": 12897616,         "owner": {         "id": 1,         "name": "System",         "type": "Organizat         },         "dateAdded": "201         "lattModified": "201         "rating": 4.00,         "confidence": 65,         "threatAssessRatin         "threatAssessConfil         "threatAssessConfil         "webLink":         "https://app.threatcomRaddress=123.123.         "ip": "123.123.123.123.     } }	ion" 6-10-20T15:07:32Z", 18-01-24T16:32:20Z", g": 2.73, idence": 46.37, onnect.com/auth/indicators/details/address.xht 123.123\u0026owner=System", 123"

Figure 21