Software Requirements Specification

For GCI Security Smart Response Project

Version 3.0 approved

Prepared by Xavier Cho

General Communications, Inc. (GCI)

3/25/2018

Table of Contents

Revision History

Name	Date	Reason for Changes	Version
Xavier Cho	1/26/2018	Changing the template to fit GCI Security's Project	2.0
Xavier Cho	2/25/2018	Changing the wording after review with client	3.0

1. Introduction

1.1 Purpose

This document describes the requirements specification (SRS) for a software plugin named "smart response", the plugin enables coded scripts on a vulnerability logger called "LogRhythm". This plugin implements outbreak prevention for computers that are in the internal network of GCI. If an outbreak occurs on a computer, actionable scripts will be able to streamline tasks on a bigger scale. This will help manage and automate certain tasks for analysts who work in GCI's security department.

1.2 Document Conventions

PowerShell & XML

Style	Description	Example
Italic	File names, folder names, and extensions	*C:\Development\powershell.exe*.
Monospace	Commands, flags, and environment variables	CMake's -G option.
Bold Monospace	Commands that should be run by the user	Run **cmake -G Ninja ...**
Preformatted	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	# ls –al /files total 14470

1.3 Intended Audience and Reading Suggestions

This document is intended for academic students and staff at the University of Alaska Anchorage. Further down explains the constraints, dependencies, hardware interface(s), software interface(s), required features and nonfunctional requirements. The suggested reading is in chronological order based on the table of contents.

1.4 Project Scope

The scope of the project is to provide three type of scripts for the plugin, two regarding outbreak scenarios and one to help with adding to an IP list of network host and port discovery sweeps.

1.5 References

LogRhythm. "LogRhythm and Carbon Black for Integrated Threat Discovery and Remediation", 2018.
https://logrhythm.com/pdfs/partner-solution-briefs/lr-carbon-black-solution-brief.pdf. Accessed 1/18/2018.

LogRhythm. "LogRhythm and Carbon Black for Integrated Threat Discovery and Remediation", 2018.
https://logrhythm.com/ . Accessed 1/18/2018.

Carbon Black. "Welcome to the predictive security cloud" Carbon Black, 2018.

https://www.carbonblack.com/. Accessed 1/18/2018.

https://security.stackexchange.com/questions/13556/public-dmz-network-architecture

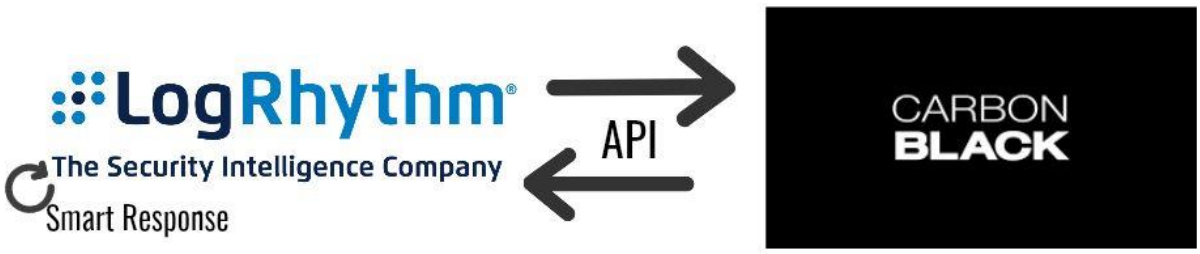
2. Overall Description

2.1 Project Perspective

The issue we are addressing with this project is preventing outbreaks on a company level can be time consuming for GCI's security department. These scripts will be able to free up some time for other tasks or training purposes as the department grows.

1. Lockdown Script: this adds endpoint lockdown functionality to LogRhythm or just PowerShell. This script is most effective for interrupt attacks or outbreaks by taking off the computer offline. The user is logged out by force, but the network interface is disabled if the user logs back in. the host can then be retrieved physically;

2. Isolation Script: this adds an automated performance to interact with Carbon Black using PowerShell. Indicating that if a computer is infected, it can only talk to Carbon Black and is isolated from talking to anything else. LogRhythm connects through Carbon Black by using the Invoke-RestMethod and passing the commands with their parameters through JSON. This is required for the user to have an API key from Carbon Black in order to run the commands. The data being passed will be tokenized rather than sending crucial data over the wire.



3. Host and Port Sweep Script:

   This adds functionality to discover and add to a list of open ports and hosts which allows as a draft list to audit possible security risks for later.

2.2 Product Functions

- IP/ DNS lookup
- Add IP's to list
- Isolate host through carbon black
- Lockdown for physical pickup

2.3 User Classes and Characteristics

The intended audience for smart response are:
- New Security analysts and technicians who can script in PowerShell & write XML. (Power Users)
- Student and Staff at University of Alaska Anchorage

2.4 Operating Environment

Operating environment:
-XML 1.0 (fifth edition)
-PowerShell (Version 5)
-LogRhythm (6.1)
-Windows 7
-Carbon Black (current)

2.5 Design and Implementation Constraints

A constraint in developing the scripts is creating a test environment due to a limited supply of test computers. The next constraint is permissions as a result to the role of an analyst I in GCI's security department.

2.6 User Documentation

- Code documentation will be code documentation such like Sandcastle.
- A general documentation on how to use the smart response.

2.7 Assumptions and Dependencies

A dependency are the permissions to access the software and building the test environment due to the hierarchical approvals and time it takes. Another dependency is software maintenance, my capstone must wait until the software is done with the updates.

3. External Interface Requirements

3.1 User Interfaces

This section describes the logical characteristics between the intended software product and the user interface design. The GUI standards will be followed along with the presence of shortcuts, error messages, tabs, search bar and dashboards. LogRhythm does have a web interface that is compatible with any of the main browsers but works best in chrome.
(Refer to figure 3. & 4.)

3.2 Hardware Interfaces

Since the application is web based, all hardware is required to connect to the internet to interface with LogRhythm and the plugin. GCI's internal network does connect to Juniper, Cisco, Linux and various types of hardware.

3.3 Software Interfaces

- The "smart response" plugin communicates with Carbon Black to call the isolation functions.
- The plugin will also communicate with logs in LogRhythm to recognize what action to take. (Refer to figure 1. & 2.)

3.4 Communications Interfaces

- The LogRhythm uses UDP/TCP with redundancy such as logs are funneled such as syslog's.
- The web client as well as how the plugin responds is through TCP

4. System Features

The major services and functional requirements for the product can be illustrated by system features. This section is organized by use cases for major system features. In the following, necessary description is provided for each use cases in the system. Each use case description provides information of the associated priority of feature, stimulus/response sequences and functional requirements (assumptions). Being a major important section of the SRS, this section is expected to go through iterative improvement to make the most logical sense for the intended scripts.

4.1 Endpoint Lockdown

4.1.1 Description and Priority

- This script is designed to be launched through LogRhythm or a stand allow script. The script locks down the compromised host until physically retrieved for forensics.
- Priority: low

4.1.2 Stimulus/Response Sequences

i. Once an alarm is triggered
ii. Credentials are entered to run scripts
iii. Script runs
iv. If script is rejected, local delegation for physical pickup takes into effect.
v. If script is successful, computer is locked and local delegation for physical pickup takes into effect.

4.1.3 Functional Requirements

i. Disable Network adapter in target
ii. Change/lock the user can't enable the network interface.

4.2 Adding to IP's for open host and port sweep

4.2.1 Description and Priority

- Add list to check IP's on the network to see if it is open as a passive reconnaissance.
- Priority: low

4.2.2 Stimulus/Response Sequences

i. Get-netipaddress
ii. Win_32pingstatus
iii. Create "new-object" instance
iv. Ping, send()
v. Begin.getHostentry()
vi. End.getHostEntry()
vii. TCPClient = new-object syste.net, sockets.topclient
viii. If connected, set to true and add to list

4.2.3 Functional Requirements

i. Add IP to a pointed list
ii. Invoke ping sweep
iii. Verify connectivity with target host

4.3 LogRhythm and Carbon Black Isolation

4.3.1 Description and Priority

- Automates isolation process and interacts with Carbon Black using PowerShell. LogRhythm connects through Carbon Black by using the Invoke-RestMethod and passing the commands with their parameters through JSON.
- Priority: high

4.3.2 Stimulus/Response Sequences

i. LogRhythm Alerts of compromised computer

ii. Analyst approves of action
iii. Script runs
iv. Can execute memory dump function
v. Can execute isolation function from network activity
vi. Can execute to kill process
vii. Can execute to fetch file for later analysts and following up with a deletion.

4.3.3 Functional Requirements

i. Invoke-RestMethod with Carbon Black
ii. memory dump function
iii. isolation function from network activity
iv. kill process function
v. fetch file and delete function

5. Other Nonfunctional Requirements

5.1 Performance Requirements

Response time upon connection between the target host(s) should be in less than 2 seconds for Lockdown and Isolation. The confidence for the ping sweep should fall within the range of 80-90% of accuracy as this is the first draft for this script.

5.2 Safety Requirements

The Information transmission should be securely transmitted without any changes in information.

5.3 Software Quality Attributes

• Availability
If the internet service gets disrupted while sending information to the target host, the system will give an error message.

• Security
The main security concern is for users credentials hence proper handling of the data should be used to avoid hacking.

• Usability
As the system is easy to handle and navigates in the most expected way with no delays. In that case the system program reacts accordingly and transverses quickly between its states.

Appendix A: Glossary

- ***API:*** *application programming interface is a set of subroutine**s**, protocols, and tools for building application software*
- ***GCI:*** *General Communications Inc. a telecommunications corporation operating in Alaska. Through its own facilities and agreements with other providers, GCI provides cable television service, Internet access, Wireline (networking) and cellular telephone service.*
- ***Endpoint Security System:*** *Refers to a methodology of protecting the corporate network when accessed via remote devices such as laptops or other wireless and mobile devices.*
- ***Script:*** *is a list of commands that can be executed without user interaction. A script language is a simple programming language with which you can write scripts.*
- ***UI:*** *The junction between a user and a computer program. An interface is a set of commands or menus through which a user communicates with a program.*
- ***JSON:*** *(JavaScript Object Notation) is a lightweight data-interchange format.*
- ***ISP:*** *Internet Service Provider*
- ***XML:*** *Extensible Markup Language (XML) is used to describe data.*
- ***PowerShell:*** *An automated task framework from Microsoft, with a command line shell and a scripting language integrated into the .NET framework, which can be embedded within other applications.*
- ***SSH:*** *Secure Shell (**SSH**) is a cryptographic network protocol for operating network services securely over an unsecured network.*
- ***SNMP:*** *Simple Network Management Protocol (**SNMP**) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior*
- ***TCP:*** *A set of rules that governs the delivery of data over the Internet or other network that uses the Internet Protocol and sets up a connection between the sending and receiving computers.*
- ***UDP:*** *In computer networking, the User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. This is mainly used for video such as skype and how it transfers the video feed.*
- ***RDP:*** *Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.*
- ***Carbon Black:*** *A company based in Waltham, Massachusetts. Carbon Black develops endpoint security software that detects malicious behavior and prevents malicious files from attacking an organization.*
- ***LogRhythm:*** *LogRhythm, Inc. is an American security intelligence company that unifies Security Information and Event Management, log management, network and endpoint monitoring and forensics, and security analytics.*

Appendix B: Analysis Models

Figure 1.

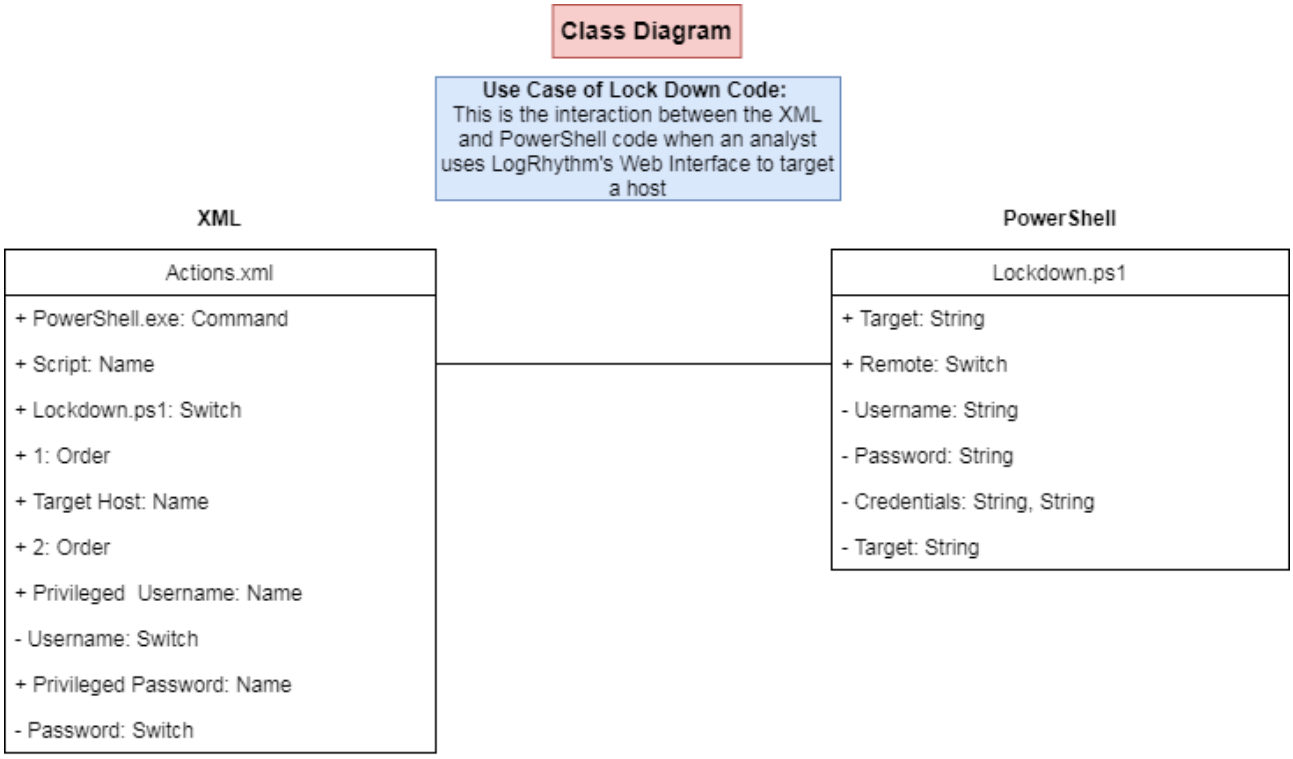


Figure 2.

Use case steps of locking an infected user out of the network through LogRhythm.

Design Schematic and Main Function

KEY:

DENFINITION(S):
-"smart response": the actionable script.

STEPS:
1. All Logs inbound go through LogRhythm for processing.

2. LogRhythm detects the infected user and sends an alert to the security analyst.

3. The security analyst selects the "smart response" from LogRhythm's web UI to respond to the task of stopping the infected user.

4. LogRhythm sends the "smart response" to the infected user.

5. LogRhythm clears the alert once the task is complete.

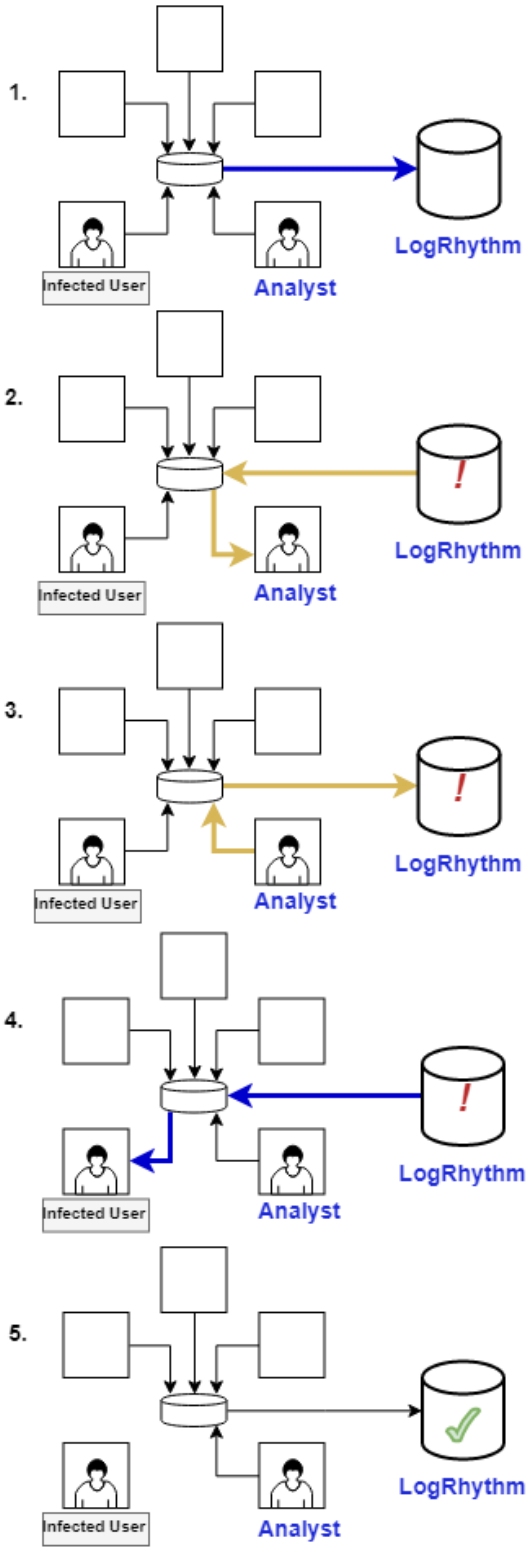


Figure 3.

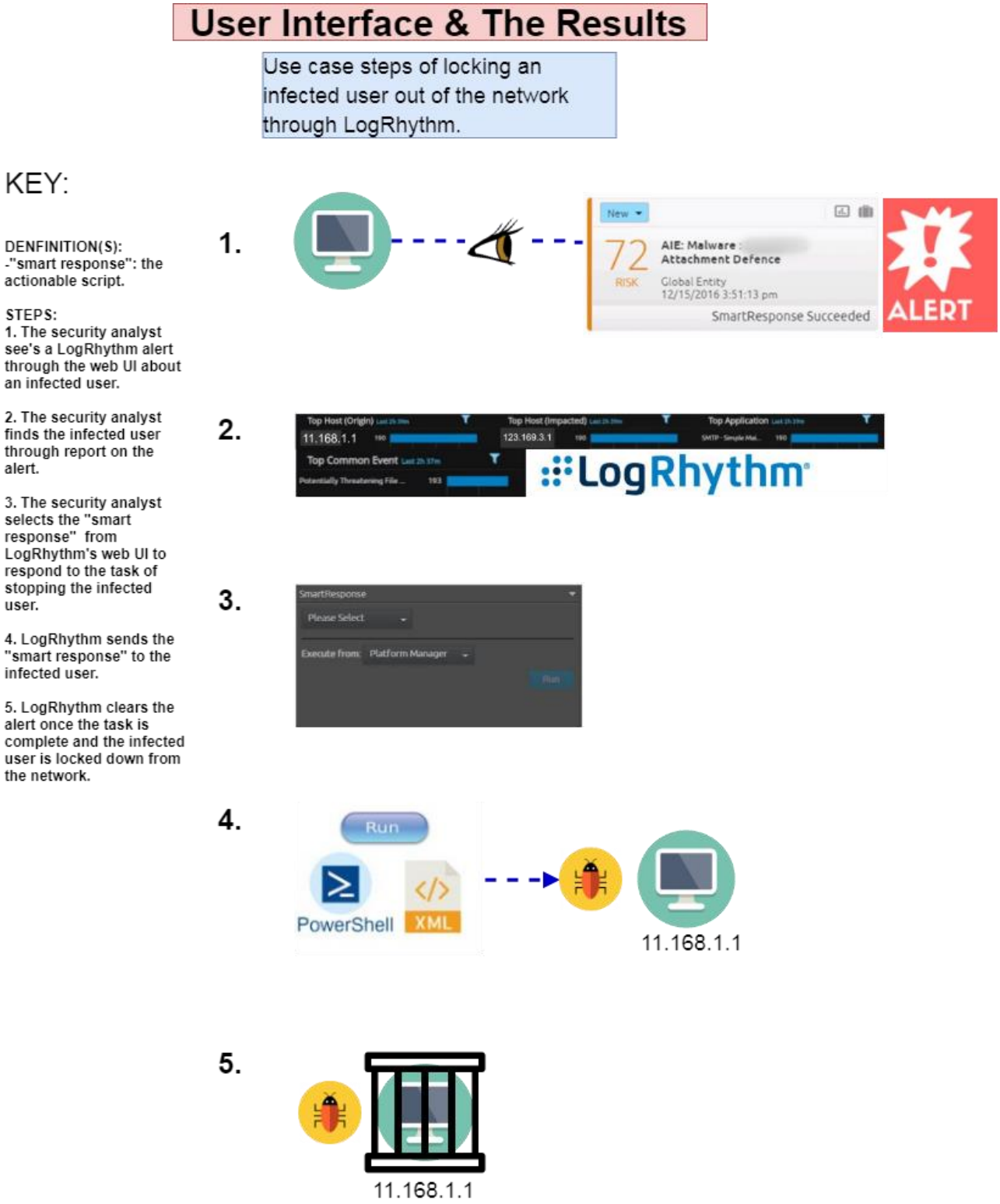
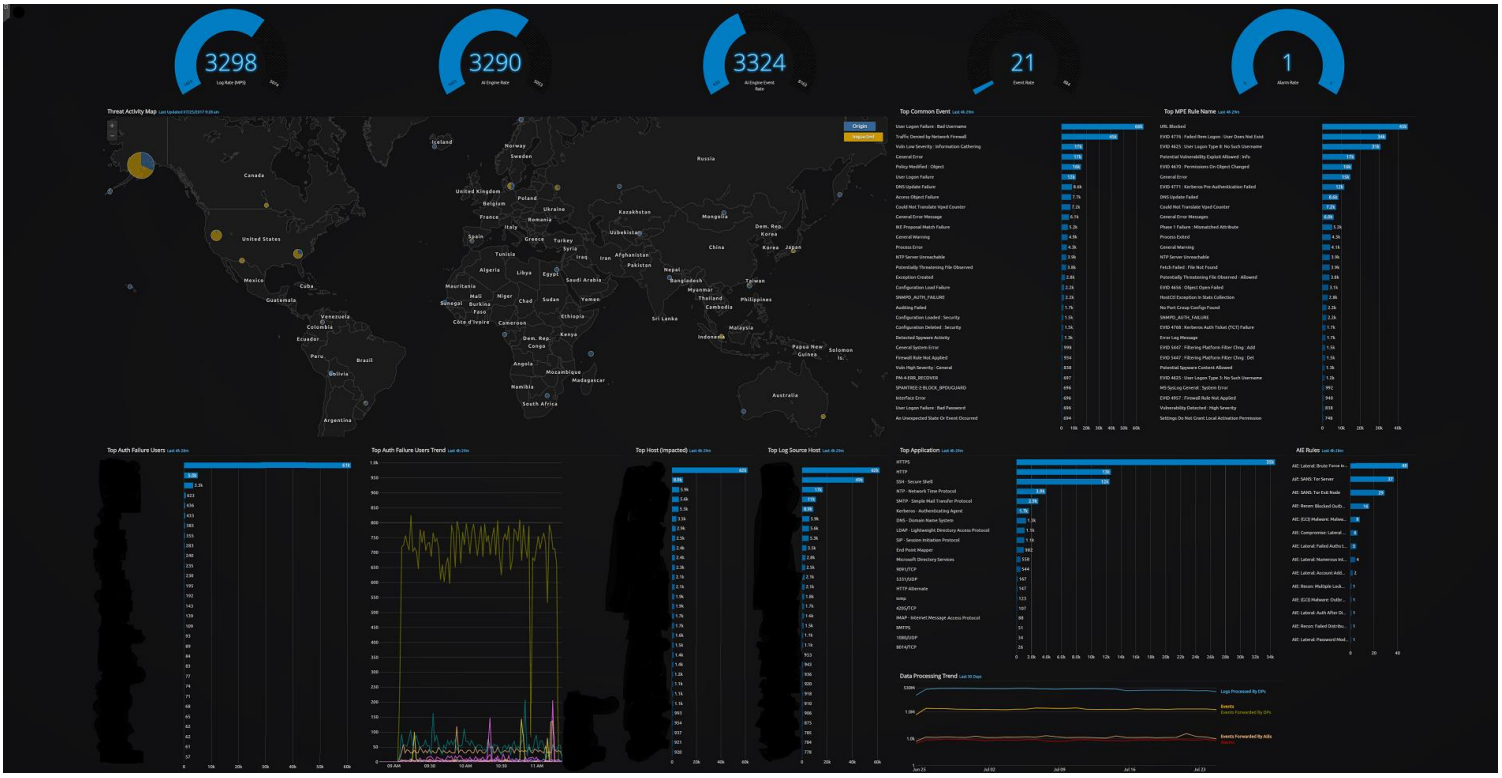

User Interface & The Results
Use case steps of locking an infected user out of the network through LogRhythm.
KEY:
DENFINITION(S):
-"smart response": the actionable script.
STEPS:
1. The security analyst see's a LogRhythm alert through the web UI about an infected user.
2. The security analyst finds the infected user through report on the alert.
3. The security analyst selects the "smart response" from LogRhythm's web UI to respond to the task of stopping the infected user.
4. LogRhythm sends the "smart response" to the infected user.
5. LogRhythm clears the alert once the task is complete and the infected user is locked down from the network.
1.
New
72
RISK
AIE: Malware :
Attachment Defence
Global Entity
12/15/2016 3:51:13 pm
SmartResponse Succeeded
ALERT
2.
Top Host (Origin)
11.168.1.1
Top Host (Impacted)
123.169.3.1
Top Application
Top Common Event
LogRhythm
3.
SmartResponse
Please Select
Execute from:
Platform Manager
Run
4.
Run
PowerShell
XML
11.168.1.1
5.
11.168.1.1

Figure 4.


3298
3290
3324
21
1
Threat Activity Map
Top Common Event
Top MPE Rule Name
Top Auth Failure Users
Top Auth Failure Users Trend
Top Host (Impacted)
Top Log Source Host
Top Application
AIE Rules
Data Processing Trend