LogRhythm – Custom MPE Rules Using Regular Expression Training

LogRhythm University Syllabus

October 2018

Two Day LogRhythm Custom MPE Rules Using Regular Expression Training

LogRhythm *Custom MPE Rules Using Regular Expression* Training is offered as a two-day Instructor Led Virtual Training Course that targets the creation of new MPE Rules in the LogRhythm SIEM for custom devices.

LogRhythm Custom MPE Rules Using Regular Expression Training Syllabus

A Review of Log Processing
Introduction to Regular Expression
Regular Expression in LogRhythm
Creating Custom Rules
Enabling Custom Rules
Best Practices

Who Should Attend

The *Custom MPE Rules Using Regular Expression* Training course is designed for LogRhythm Administrators, Partner Consultants, Sales Engineers, Solution Engineers, and Technical Staff who are responsible for adding new custom Log Sources into the LogRhythm platform.

Prerequisites

There are **NO** prerequisites required to enroll in this course.
The following courses are **recommended** prior to arrival at the *Custom MPE Rules Using Regular Expression* Training:

- *Analyst Training Courses*
  Or
- *Administration Training Courses*
  Or
- *Analyst and Administration Combined Training Courses*

Day One: LogRhythm Custom MPE Rules Using Regular Expression

Consists of the following modules:

- A Review of Log Processing
  - Course Overview
  - LogRhythm Platform
  - Log Source Definitions
  - Data Processor Functions
  - What is RegEx?
- Introduction to RegEx
  - Understanding RegEx
  - Literal Characters
  - Positional Characters
  - Using Literals with Positionals
  - Matching Characters
  - Repetition Characters
  - Character Sets
  - Matching Reserved Characters
  - Capture Groups
  - Optional Matches
  - Greedy vs. Non-Greedy Quantifiers
  - Common Regular Expressions Used in LogRhythm

- RegEx in LogRhythm
  - Build Custom MPE Rules Using RegEx
  - Base-Rule Regular Expressions
  - Parsing Fields and Tags
  - Sub-Rules
  - Catch-All Rules
  - Steps to Create New Base-Rules
  - Processing Settings in the MPE Rule Builder
  - Writing RegExes for use in LogRhythm

Day Two: LogRhythm Custom MPE Rules Using Regular Expression

Consists of the following modules

- Creating Custom Rules
  - Additional Information about the MPE Rule Builder Tool
  - Log Source Type Manager
  - Date Format Manager
  - General RegEx Tips
  - Steps for MPE Rule Creation
  - Hands-on Practice Writing Regular Expressions for new Base-Rules
- Enabling Custom Rules
  - MPE Policy Settings
  - Enabling Custom MPE Rules
  - MPE Rule Processing Logic
  - Rule Library Browser
  - Steps after MPE Rule Creation
  - Hands-on Practice creating Sub-Rules for new Base-Rules
  - Hands-on Practice Enabling Custom MPE Rules
- Best Practices
  - Best Practices when Working with Rules
  - Reviewing Processing Performance
  - The Efficiency of a Regular Expression
  - RegEx Recommended Practices
  - The Whole Process for Custom MPE Rules
- Hands-on Practice Deploying a new Custom Log Source
  - Creating a new Custom Log Source Type
  - Creating a new MPE Base-Rule
  - Creating new Sub-Rules
  - Enabling the new Rules
  - Collecting Log from the new Custom Log Source
  - Verifying the new Custom MPE Rules are Parsing Data Correctly