Custom MPE Rules Using Regular Expression Course Syllabus
Custom MPE Rules Using Regular Expression

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.

INTRODUCTION

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

None

Some recommendations (but not limited to):

- Introduction to LogRhythm - What is a SIEM
- Introduction to LogRhythm - Administrators and Analysts
- What's New in LogRhythm v 7.4
- Web Console - An Introduction Video

COURSE NAME

Custom MPE Rules Using Regular Expression
### DAY ONE:

**A Review of Log Processing**
- Course Overview
- LogRhythm Platform
- Log Source Definitions
- Data Processor Functions
- What is RegEx?

**Introduction to RexEx**
- 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

### DAY TWO:

**Creating Custom Rules**
- Additional Information about the MPERule Builder Tool
- Log Source Type Manager
- Date Format Manager
- General RegEx Tips
- Steps for MPERule 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 MPERule 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 MPEBase-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