LogRhythm v7
306 – Administration Product Training

LogRhythm University Syllabus

October 2018

306 – Administration Product Training

The *306 – Administration Product Training* is a three-day **In-person** Instructor Led, **Virtual** Instructor Led, or **On-site** Instructor Led training course that targets the basic day-to-day administrative activities performed within the LogRhythm Platform.

Who Should Attend

306 – Administration Product Training is designed for systems administrators, engineers, and other LogRhythm users who are responsible for the basic maintenance and configuration of the LogRhythm Platform.

Prerequisites

Participants are required to complete the following computer-based training (CBT) modules prior to arrival at the *306 – Administration Product Training*:

- *Introduction to LogRhythm: What is a SIEM?*
- *Introduction to LogRhythm: Administrators and Analysts*

Participants must pass a ten-question quiz at the end of each course, with a score of 70% or more, to receive credit for completion.

306 – Administration Product Training

306 – Administration Product Training explores the day-to-day activities in the LogRhythm Platform for administrators. Participants can expect to leave with an understanding of administrative functions within the LogRhythm Client Console and will be equipped with the tools to effectively manage the log data collected.

The course includes hands-on exercises to provide experience with the administrative functions of the LogRhythm Platform.

This training consists of the following modules:

- Day One: Administration Fundamentals
- Day Two: Global Administration
- Day Three: AI Engine

306 – Administration Product Training

Day One: Administration Fundamentals

Administration Fundamentals Training explores the day-to-day administrative activities of the LogRhythm Platform. Administrators will be introduced to the LogRhythm Console's administrative functions. Participants can expect to leave with an understanding of managing the LogRhythm Platform and will be equipped with the tools to effectively manage the collection of log data. This training consists of the following modules:

- Introduction to LogRhythm
- Platform Overview
- Object Management with Entities and Lists
- System Monitors
- Log Sources
- Users, Profiles, and Permissions

Day Two: Global Administration

Global Administration Training expands on the LogRhythm Platform beyond the Administration Fundamentals Training course. This course provides participants with the foundation needed to understand the role of an Global Administrator and basic knowledge of:

- Reports
- The Knowledge Base, Platform Manager, and Other Settings
- Health Monitoring and Maintenance
- Tuning and Configuration
- Challenge: Restoring Historic Data
- Challenge: Tuning of Log Processing

Day Three: AI Engine Fundamentals

AI Engine Fundamentals Training explores the administrative activities for the AI Engine. Participants can expect to leave with an understanding of how AI Engine functions, an understanding the configuration of AI Engine Rules, and common threats and attack scenarios for which the rules are configured to monitor. The course is comprised of the following topics:

- Introduction to AI Engine
- AI Engine Rules
- Threshold and Unique Values Rule Blocks
- Behavioral Rule Blocks
    - Whitelist
    - Statistical
    - Trend

Certification

LogRhythm Platform Administrator (LRPA)

By attending and completing the training, participants will be prepared to take an exam to obtain the LogRhythm Platform Administrator (LRPA) certificate.

The **LRPA** exam is a written exam comprised of multiple-choice questions testing a candidate's knowledge on managing and maintaining the LogRhythm Platform. Candidates will have 90-minutes to complete the exam. Candidates must pass the written exam with a score of 70% or more to receive a LogRhythm Platform Administrator (LRPA) certificate. If a passing score is not obtained, candidates must wait 30 days before taking the exam again.