LogRhythm v7
310 – CORE Fundamentals

LogRhythm University Syllabus

October 2018

310 – CORE Fundamentals Training

The 310 – Complete, CORE Fundamentals Training is a five-day **In-person** Instructor Led, **Virtual** Instructor Led, or **On-site** Instructor Led training course that targets the basic day-to-day analytical and administrative activities performed within the LogRhythm Platform.

Who Should Attend

310 – CORE Fundamentals Training is designed for security analysts, systems and network administrators, engineers, and other LogRhythm users who are responsible for the day-to-day use, 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 *310 – CORE Fundamentals* 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.

LogRhythm CORE Fundamentals Training

310 – CORE Fundamentals Training explores the day-to-day activities in the LogRhythm Platform for Administrators and Analysts. Participants will be introduced to the LogRhythm Client Console's administrative functions and instructed on how to utilize it for administrative purposes. Participants will be introduced to the AI Engine Rule Wizard and receive instruction on the use of the pre-built system rules and creating custom AI Engine Rules to help with threat detection. Participants will be introduced to the features and functionality used by analysts in the LogRhythm Web Console to perform Threat Lifecycle Management.

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

This training consists of the following modules:

Day One:	Administration Fundamentals
Day Two:	Global Administration
Day Three:	AI Engine
Day Four:	Analyst Fundamentals
Day Five:	Security Analytics

310 – CORE Fundamentals 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 and explores the global administrative activities. This course provides participants with the foundation needed to understand the role of an 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 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

Day Four: Analyst Fundamentals

Reducing the time to detect and respond to threats largely determines an organization's ability to avoid damaging cyber incidents. The Analyst Training course introduces the steps taken during Threat Lifecycle Management (TLM) to reduce the mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) to threats. This training consists of the following modules:

- The Role of an Analyst
- Navigating the Web Console
- The Analyst's Tasks
- Customizing the Web Console
- Challenge: Taking Action as an Analyst

Day Five: Security Analytics

Security analysts develop practical hands-on application of the features and functionality of the LogRhythm tools needed to perform Threat Lifecycle Management. This training consists of the following modules:

- Security 101
- Security Types
- Threat Lifecycle Management in the SIEM
- Practice Exercise: Ransomware Attack
- Challenge: Botnet Detection
- Challenge: Reducing Downtime
- Challenge: Comply with Acceptable Use Policies