LogRhythm v7
305 – Analyst Product Training

LogRhythm University Syllabus

October 2018

305 – Analyst Product Training

The *305 – Analyst 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 analytical activities performed within the LogRhythm Platform.

Who Should Attend

305 – Analyst Product Training is designed for security analysts, systems administrators, engineers, and other LogRhythm users who are responsible for the day-to-day analysis of the data in the LogRhythm Platform.

Prerequisites

Participants are required to complete the following computer-based training (CBT) modules prior to arrival at the *305 – Analyst 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.

305 – Analyst Product Training

305 – Analyst Product Training explores the day-to-day activities in the LogRhythm Platform for analysts. Participants are introduced to the features and tasks that enable analysts to optimally perform Threat Lifecycle Management (TLM).

The course includes hands-on exercises to provide experience with the analytical functions of the LogRhythm Platform. Participants can expect to leave with an understanding of analytical functions within the LogRhythm platform and will be equipped with the tools to effectively analyze the log data collected.

This training consists of the following modules:

- Day One: Analyst Fundamentals
- Day Two: Security Analytics
- Day Three: AI Engine Fundamentals

305 – Analyst Product Training

Day One: 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 Two: 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

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

Certification

LogRhythm Security Analyst (LRSA)

By attending and completing the training, participants will be prepared to take an exam to obtain the LogRhythm Security Analyst (LRSA) certificate.

The **LRSA** exam is a written exam comprised of multiple-choice questions testing a candidate's knowledge on using the LogRhythm platform for the analysis of data. 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 Security Analyst (LRSA) certificate. If a passing score is not obtained, candidates must wait 30 days before taking the exam again.