18 August 2020

LogRhythm University

305 – Analyst Fundamentals Training Syllabus

LogRhythm, Inc – 4780 Pearl East Cir Boulder, CO 80301 – (720) 881-5400

www.logrhythm.com

DATE CREATED	TRAINING COURSE SYLLABUS
08/12/2020	305-Analyst Fundamentals Training
VERSION NO.	**CREATED BY**
7.5	LogRhythm Training
INTERNAL/EXTERNAL	**PROCESS OWNER**
External	Project Manager
DATE OF LAST UPDATE	**LAST UPDATED BY**
8/13/2020	LogRhythm Training

305 – Analyst Product Training

The 305 – Analyst Fundamentals Training is a 16-hour 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.

INTRODUCTION

WHO SHOULD ATTEND	305 – Analyst Fundamentals 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	Familiarity with Windows and Windows Command line or PowerShell functions Some recommendations (but not limited to): Introduction to LogRhythm - What is a SIEM Introduction to LogRhythm - Administrators and Analysts What's New in LogRhythm v7.5 Web Console - An Introduction Video
305 – ANALYST PRODUCT TRAINING	305 – Analyst Fundamentals 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.

305 – Analyst Fundamentals Training – Modules and Topics

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. Additionally, 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:

- Web Console Overview
- Logs, Alarms, and Data Analysis
- Case Management and Gathering Evidence
- The Analysts Tasks
- Customizing the Web Console
- Taking Action as an Analyst
- Security 101
- Security Types
- Threat Intelligence
- Threat Lifecycle Management in LogRhythm
- Challenge: Ransomware Attack
- Challenge: Living off the Land Attack
- Challenge: Reducing Downtime
- Challenge: Comply with Acceptable Use Policies

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, True or False, and Select All That Apply questions. The exam tests 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.**