LogRhythm v7.3
Security Analytics Training

LogRhythm University Syllabus

February 2018
LogRhythm Security Analytics Training

The Security Analytics course is offered as an In-person Instructor Led or Virtual Instructor Led training course that reinforces the application of Threat Lifecycle Management using LogRhythm.

Who Should Attend
The Security Analytics training course is designed for security analysts, systems administrators, engineers, and other LogRhythm users who are responsible for the day-to-day use of the LogRhythm platform to detect and respond to Events and Alarms.

Prerequisites
Users are required to complete the following courses prior to arrival at the Security Analytics Training class:

- Introduction to LogRhythm: What is a SIEM? computer-based training (CBT) module
- Introduction to LogRhythm: Administrators and Analysts computer-based (CBT) module
- Analyst Fundamentals Training

Security Analytics Training
Reducing the time to detect and respond to threats largely determines an organization’s ability to avoid damaging cyber incidents. The Security Analytics Training course reinforces the steps taken during Threat Lifecycle Management (TLM) to reduce the mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) to threats. Security analysts develop practical hands-on application of the features and functionality of the LogRhythm tools needed to perform Threat Lifecycle Management.
Consists of the following modules:

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

NOTE: Administrative activities are not covered during this course.

Participants who attend the following courses: Analyst Fundamentals, Security Analytics, and AI Engine Fundamentals will automatically be enrolled into the LogRhythm Security Analyst (LRSA) exam. The exam is not mandatory but may be a prerequisite for taking advanced courses. An LRPA certificate will be granted to those participants that pass the exam with a score of 70% or more.
LogRhythm Security Analytics Training

Security 101
This chapter offers analysts with an introduction to Security. Analysts are provided with a foundation needed to understand Threat Actors, their tools, their motivation, and goals:

- Bad Actors and their Goals
- Bad Actor Tools of the Trade
- Anatomy of an Attack
- Ransomware in Action
- Security in the Headlines
- Timeframe Matters
- Security Tools and Classifications
- Security System and Tools

Security Types
The objective of this chapter is to take a look at the different types of security, what can be used to help with each, and what each of their current threat landscapes are.

- Compliance
- LogRhythm Threat Modules
- User Security
- Network Security
- Endpoint Security
- Application Security
- Advanced Persistent Threats

Threat Lifecycle Management in the SIEM
Provides you hands-on application of the phases of Threat Lifecycle Management:

- The Discovery Process in Action
  - Tools for Discovery
- Qualifying Logs of Interest
- Investigation
  - Mechanics of an Investigation
  - Unstructured Searches
  - Pivoting to quickly Identify Related Data
  - Record your findings in a Case
- Neutralize the Threat

Ransomware Attack
Using the topics and techniques presented in the previous chapters, you will perform the steps in the Threat Lifecycle Management to detect and respond to a new incident:

- Discover
- Qualify
- Investigate
- Neutralize
- Recover

Botnet Detection
You will perform the steps in the Threat Lifecycle Management to track a new Security incident:

- Discover
- Qualify
- Investigate
- Neutralize
- Recover
Reducing Downtime
You will perform the steps in the Threat Lifecycle Management to track a new Operations incident:
- Discover
- Qualify
- Investigate
- Neutralize
- Recover

Comply with Acceptable Use Policies
You will perform the steps in the Threat Lifecycle Management to track a new Compliance incident:
- Discover
- Qualify
- Investigate
- Neutralize
- Recover