Network Monitor for Analysts
Course Syllabus
The Network Monitor for Analysts Training course is designed for security analysts, systems administrators, managers, engineers, and other LogRhythm users who are responsible for the day-to-day use of the LogRhythm Network Monitor platform to detect and respond to Events and Alarms.

Reduction the time to detect and respond to threats largely determines an organization’s ability to avoid damaging cyber incidents. The Network Monitor for Analysts 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 Network Monitor tool needed to perform Threat Lifecycle Management.

- Consists of the following modules:
  - Network Monitor Overview
  - Navigation in Network Monitor
  - Creating Dashboards
  - The Analyst’s Tasks: Using Threat Lifecycle Management
  - Deep Packet Analytics

NOTE: Administrative activities are not covered during this course.
LogRhythm Network Monitor for Analysts

Network Monitor Overview:

This chapter provides you with the foundation needed to understand the Network Monitor platform and basic knowledge of:
➢ An Overview of Network Monitor
➢ Data Collection
➢ Network Monitor in Action
➢ Web Management Interface

Navigation in Network Monitor:

Provides you with a working knowledge of Network Monitor and the functions contained within to help you perform:
➢ Data Discovery
➢ Packet Capture Data and File Attachments
➢ Alarms
➢ PCAP Replay
➢ Help

Creating Dashboards:

Provides you hands-on application with the following:
➢ Dashboard Creation Workflow
➢ Create a Search from Discover
➢ Make Visualizations with Visualize
➢ Make a Dashboard

The Analyst's Tasks: Using Threat Lifecycle Management:

Using the topics and techniques presented in the previous chapters, you will perform the steps in the Threat Lifecycle Management to track a new incident:
➢ Gathering Forensic Data
➢ Discovery
➢ Qualification of Data and Alarms
➢ Investigation of Data and Alarms
➢ Neutralize
➢ Recovery

Deep Packet Analytics:

This will be an introduction into DPA Rules which includes the foundation of how they work and what we want to achieve with them:
➢ Overview
➢ Rule Examples
➢ Managing Rules