



# LogRhythm Official Training

Certified LogRhythm Product Specialist

21<sup>th</sup> July 2010

V1.2

## Contact Information:

**Janne Nyman**

Solutions Consultant, EMEA

LogRhythm, Inc.

email : [janne.nyman@LogRhythm.com](mailto:janne.nyman@LogRhythm.com)

[www.logrhythm.com](http://www.logrhythm.com)

### Introduction

The purpose of this document is to define the course content and recommended participant for the Certified LogRhythm Product Specialist course.

The Certified LogRhythm Product Specialist course is aimed at LogRhythm Partners and End Users that want to have a deeper understanding of LogRhythm rules creation and log parsing. The Certified LogRhythm Product Specialist course introduces the student to the advanced processing rules available within the LogRhythm product, including the creation of new Message Processing Engine rules.

Students will also learn how to configure advanced agent installations.

### Prerequisites and Length

This course is a two day course. Students must be a LogRhythm Customer or work for a LogRhythm Professional Services Partner to attend this course. Students must have also sat on the Certified LogRhythm Installation Engineers Course or the Certified LogRhythm System Administrator Course.

It is recommended students attending the class have experience with LogRhythm and a basic knowledge of Regular Expressions (regex).

### Scope

This guide is for use by LogRhythm Customers and LogRhythm Professional Services Partners.

### Course Content

#### Welcome Orientation and Overview

Participants will be provided with a brief introduction to the facility, area, accommodations, each other, eating arrangements, and plan for the days ahead.

#### LogRhythm Overview & Architecture

This training module will provide the student with an overview of LogRhythm Log and Event Management. This session will provide students with the basic knowledge to understand:

[www.logrhythm.com](http://www.logrhythm.com)

- ≡≡≡ LogRhythm terminology
- ≡≡≡ LogRhythm log data hierarchy
- ≡≡≡ LogRhythm logical objects
- ≡≡≡ LogRhythm Knowledge Base
- ≡≡≡ LogRhythm Solution Architecture

The LogRhythm Overview & Architecture training module provides the pre-requisite foundation knowledge for all other training.

### Section One: Advanced Agent Installation

This training module goes on to provide the student with a working knowledge of:

- ≡≡≡ Deployment Management
  - Managing LogRhythm Logical objects
    - Entities, Networks, and Hosts
    - Log Managers
    - Agents
    - Log Sources
    - Message Processing Engine Policies
    - Alarm Rules
    - People and Users
  - Common Deployment tasks
    - Adding Entities, Networks, and Hosts
    - Deploying a Log Manager
    - Deploying an Agent
  
- ≡≡≡ Configuring LogRhythm Agents for Log Collection
  - Collecting Windows Event Logs
  - Collecting Flat File Logs
  - Collecting Syslog
  - Collecting Netflow
  - Collecting Checkpoint Firewall Logs
  - Collecting Database data with the Universal Database Log Adapter (UDLA)

### Section Two: LogRhythm Message Processing Engine (MPE) Rule Development

The Class is designed for systems administrators and engineers who are supporting custom applications or need to do advanced customization and tuning of their LogRhythm deployment. LogRhythm is a highly flexible and open system that provides the means for you to develop custom rules to meet your organizational data collection and processing demands.

Students will learn all aspects of rule development. They will leave the course with the knowledge & tools required to integrate custom logging devices into LogRhythm and customize LogRhythm's support for commercial logging devices.

This hands-on section will cover items including:

- ☐☐☐ Introduction to Regular Expressions
- ☐☐☐ Rule Function
- ☐☐☐ Rule Definition
- ☐☐☐ Parsing & Attributes
- ☐☐☐ Rule Builder Tool
- ☐☐☐ Tags (Usage, Parsing, Mapping)
- ☐☐☐ Base Rules versus Sub Rules
- ☐☐☐ Naming and Classification

### Section Three: Advanced Alarm Rule Development

Alarm Rules enable automatic detection and notification of specific activity. LogRhythm includes an extremely powerful and flexible system for creating a wide variety of Alarm Rules.

This section provides extensive hands training in the development of sophisticated Alarm Rules for detecting activity in support of compliance, security, and operations objectives.

- ☐☐☐ Overview of the Alarm Rule Processing Engine
- ☐☐☐ Alarm Thresholds, Grouping, and Suppression
- ☐☐☐ Log Source Criteria
- ☐☐☐ Event Criteria
- ☐☐☐ Day & Time Criteria
- ☐☐☐ Advanced Notification Options
- ☐☐☐ Alarm Rule Sharing & Security