10 January 2020

Threat Detection with AI Engine (AIE)

Course Syllabus

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

www.logrhythm.com

DATE CREATED	TRAINING COURSE SYLLABUS NAME
2/1/2019	Threat Detection with AI Engine (AIE)
VERSION NO.	**CREATED BY**
7.4	LogRhythm Training
PROCEDURE NO.	**PROCESS OWNER**
0	Project Manager
DATE OF LAST UPDATE	**LAST UPDATED BY**
1/8/2020	Project Manager

Threat Detection with AI Engine Training

The Threat Detection with AI Engine training course is offered as a Virtual Instructor Led training course. This course builds upon the AI Engine Fundamentals knowledge foundation to help move your organization to a more mature level of threat detection.

INTRODUCTION

WHO SHOULD ATTEND	The Security and Threat Detection with AI Engine course is designed for administrators who are responsible for the configuration of the LogRhythm Platform.
PREREQUISITES	Users are required to complete the following training courses prior to arrival at the Threat Detection with AI Engine course: ➢ 306 – Administrator Track with LogRhythm Platform Administrator (LRPA) certification ➢ 305 – Analyst Track with LogRhythm Security Analyst (LRSA) certification
COURSE NAME & SUMMARY	**Security and Threat Detection with AI Engine** Reducing the time to detect and respond to threats largely determines an organization's ability to avoid damaging cyber incidents. The Threat Detection with AI Engine course is designed to help your organization utilize additional capabilities of LogRhythm to increase your level of Security Intelligence maturity. This advanced AI Engine course will provide you with the information necessary to utilize more complex AIE Rules and to configure advanced deployment options for AI Engine components. Upon completion of this course you will have the knowledge to install and configure Threat Detection Modules in your environment.

Security and Threat Detection with AIE

AI Engine Fundamentals Review:

- Why is AI Engine so Valuable?
- Rule Block Types
- Review of Statistical Rule Blocks
- Review of Trend Rule Blocks
- Relationships
- Exporting and Importing Rules
- SmartResponses

Advanced AI Engine Configuration:

- Additional Log Sources
- Using Expressions in AIE Rules
- Types of Expressions
- Use Cases for Expressions

An Introduction to Threat Detection Modules:

- What are Threat Detection Modules
- Review of the Knowledge Base (KB) Manager
- KB File Updates

Troubleshooting and Tuning:

- Understanding the Basic Architecture
- Monitoring the Health of AI Engine
- Troubleshooting
- AI Engine Rule Tuning
- AIE Risk Based Priority

Rule Building Challenge Exercises:

- Using Custom Plugins
- Blocking Outbound Host Communication
- Detect Abnormal DNS Usage
- Monitor Traffic on an IDS
- Configure a Whitelist Rule Block
- Extracting Information for an Investigation