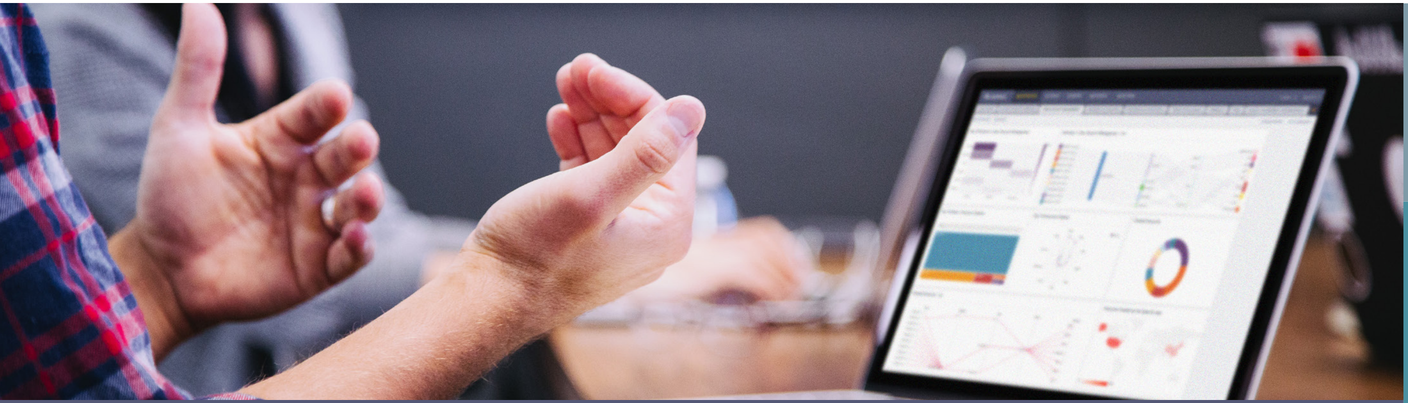

LogPoint Advanced Training

In response to popular demand following last year's successful sessions, we have decided to make the Advanced Admin and Advanced User Trainings a part of our Training portfolio. These offerings grant a learning experience that goes beyond the scope of an official user and is tailored to suit the needs of the most seasoned LogPoint users.

Training Details

The LogPoint Advanced Admin and Advanced User Trainings are on-demand training courses dedicated to super–users that take place in several European locations throughout the year.

The training sessions accommodate a maximum of 12 participants and consist of seven hours of hands-on work per day. The training is facilitated by a regional LogPoint expert and can be held in the local language or English.

Educational Focus

Throughout the four-day training session, your instructor will walk you through the latest features and state-of-the-art use cases of the LogPoint solution. There will be a strong focus on performance considerations and how the various blocks can be combined to gain the most out of your LogPoint solution.

The course consists of two modules, on Day 1 and Day 2, the focus will be on addressing complex admin responsibilities related to Roles, Scaling and Sizing, Configuration, Advanced Workflows and much more. While designing the Advanced Training modules, our goal was to ensure that peer-to-peer knowledge sharing plays an equally integral part as the traditional classroom experience. This key networking element is an excellent opportunity to seek advice and share experience about complex day-to-day projects with your peers. Going forward, the areas covered on Day 3 and Day 4 will focus on enhancing the participants' skill set in crucial areas such as advanced queries, pattern finding, search templates, creation and management of alert rules, and advanced use cases related to Threat Hunting, UEBA or the MITRE ATT&CK® framework.

Who Should Participate?

To gain the most value from the course, we advise participants to only enroll if they have at least six months of experience with the LogPoint solution and experience handling large and complex LogPoint installations.

Areas Covered

Advanced Administrator Training

Day 1

Architecture

- Roles
- Deployment scenarios
- Platforms
- Authentication

Distribution

Scaling and Sizing

Day 2

Advanced workflows

Custom Normalizations

- Signatures
- Writing signatures

Enrichment Integration

- Configuration
- Enrichment Sources
- Enrichment Policies

Bespoke Log Source Integration

Advanced User Training

Day 3

Introduction

- Fundamentals on Normalization
- Introduction to the Query Language
- Saved Searches
- Tables

Pattern Finding

- Introduction to Patterns
    - Writing Advanced Patterns
- Solving Use-Cases
    - Combining Commands
    - Using Tools and Queries
    - Using Threat Intelligence Feeds
    - Demos and Hands-on
- Class Session
    - Group Work on Solving Complex Use Cases
    - Use-Case Creation
    - Fieldwork Stories
    - Q/A Session

Day 4

Alert Rules

- Creation of Rules
- Notifications
- Writing Jinja Templates

Search Templates

- Introduction to Search Templates
- Capabilities
- Use Cases

Advanced Queries part 2

- Follow-Up from Day 1

Class Session

- Idea Generation
- Use-Cases
- Q/A Session

Instructor Profile

Each Advanced Training session is hosted by a senior instructor who has years of documented experience in the field of information technology and security supported by hands-on experience in SIEM design, development, and deployment.

Interested?
training@logpoint.com

We reserve the right to adjust the course content for larger groups of participants or participants from the same organization.

We Treasure Your Expertise

As you are an expert in the LogPoint solution, we know you possess valuable knowledge that will allow many others to succeed.

In the LogPoint Community we often receive requests and questions, which you are more than qualified to assist in answering, and we hope you will use your expertise and contribute your advice, knowledge and insights to our growing community of LogPoint users.

ACCESS THE LOGPOINT COMMUNITY SITE HERE

Thank you

For more information, visit logpoint.com
Email: training@logpoint.com

LOGPOINT