The LogPoint Artisanal Master Class

Advanced Training – Advanced Skills
Training Details

The LogPoint Artisanal Master Class takes place throughout several European locations from Mid-August until Mid-September.

The training sessions accommodate maximum 12 participants, and it will consist of five hours of hands-on work per day. The training will be facilitated by LogPoint expert, Prabhat Pokharel along with a local Technical Engineer.
Responding to Popular Demand

As a result of popular demand following last year’s successful advanced LogPoint Artisanal Master Class sessions, we are now following up with an additional two-day training, which goes beyond the scope of the official LogPoint user- and administrator training and is tailored to suit the needs of more advanced LogPoint users.

Educational Focus
Throughout the two-day training session, our KB Lead Architect will display the newest features of the solution and look into real-world use cases, performance considerations and show how all the various blocks can also be combined. Focus will include facilitation of knowledge exchange between participants, as our experience confirms that to be an excellent technique for acquiring familiarity with the solution. Further, emphasis throughout the two days will be on ensuring the training sessions accommodate the levels and requests of individual participants.

Who Should Participate
To gain most value from enrolling, participants are typically super users of the LogPoint solution or capable of handling large and complex LogPoint installations.
Areas Covered

The training sessions may be adjusted to catering to requests of larger groups of participants such as several participants from the same organization.

Interested?
For more information, please contact us at training@logpoint.com

Day 1
Introduction
• Fundamentals on normalization
• Introduction to the query language
• Saved searches
• Tables etc.

Using Queries for Finding Patterns
• 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
• Idea generation
• Working on use-cases
• War-stories from the field
• Q/A Session

Day 2
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

Input for Product Management
• New features?
• Requests?

Instructor Profile
IT professional with focus on data driven security solutions and data science. With more than seven years of experience in the field of information technology, Prabhat has expert knowledge and hands-on experience in SIEM design, development and deployment.
We Treasure Your Expertise
As you are an expert in the LogPoint solution, we know you hold knowledge others crave 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 to contribute with advice, knowledge and answers to our growing community of LogPoint users.

You access the LogPoint Community site here.

Thank you.