LOGPOINT

Logpoint Training Portfolio

User, Administrator & Director & SOAR Training

www.logpoint.com

GROW YOUR SKILLSET AND IMPROVE THE WORKFLOW

Our Logpoint User and Administrator Training has long been popular with both new and existing users who want to grow their skillset and acquire improved routines for working with or administrating the solution on a daily basis.

Training Setup

Throughout a two-day training session – or five days if completing both user, administrator and Director training – a Logpoint Certified Expert will display the features of the solution, look into real-world use cases, highlight performance considerations and teach how all the various blocks can be combined.

The main 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. Also, emphasis throughout the training will be on ensuring that the course is conducted to accommodate the levels and requests of individual participants.

Training Focuses

PLANNING

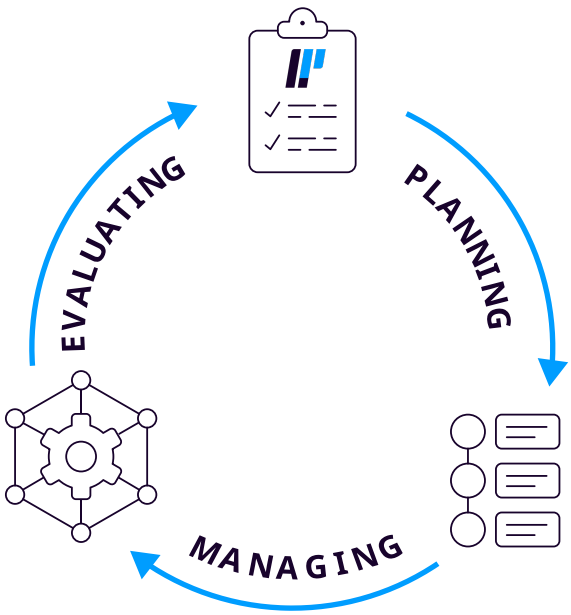
Enables you to plan the implementation and allocate required resources for the deployment process. You will learn to design reports, alerts and dashboards to best suit your Business design requirements.

MANAGING

Allows you to allocate the essential resources to manage your implementation process, and administer the solution once deployed, ensuring it remains updated and relevant on a continuous basis.

EVALUATING

Empowers you to evaluate your installation and analyze if it is providing the value needed to meet your organizational KPIs, or if adjustments are needed based on reevaluated business requirements.



AREAS COVERED

The training sessions may be adjusted to cater to the requests of larger groups of participants such as several participants from the same organization. Overall, we will cover general activities, such as introductions and an overview of SIEM and Logpoint. Each training section is followed by hands-on exercises in a training environment.

"Participating in Logpoint's training has given me new insights on the functionality of the solution. I am now more aware of best practices and small tweaks, which can make a huge difference and can assist me in implementation and operational efforts. Furthermore, the knowledge shared and obtained by engaging with other training participants has not only provided me with use-case examples but also a network of other Logpoint users, which I can consult if I need a second opinion."

– Johan Aagaard, Senior Security Advisor

Logpoint User Training (2 days)

- Logpoint User Introduction
- Logpoint Help Center
- Lab Environment
- Dashboards
- Simple Search
  - Word/Phrase
- Search
  - Key-Value
  - Labels
  - Aggregation
  - Macros
  - Joins
  - Lists
  - Enrichment
- Search Views
- Search Templates
- Reporting
- Alerting
- Logpoint UEBA

Logpoint Administrator Training (2 days)

- Logpoint Administrator Introduction
- Lab Environment
- Logpoint Server Setup
  - License
  - Update
  - Server Settings
  - Profile Settings
- Logpoint Help Center
- Logpoint Configuration
  - Applications
  - Repos
  - Routing Policies
  - Normalization Policies
  - Enrichment Sources
  - Enrichment Policies
  - Processing Policies
  - Log Collection Policies
  - Device Groups
  - Devices
- Device Integration
  - Integrate Windows (LPA)
  - Integrate Linux (rsyslog)
- User Administration
  - Permission Groups
  - User Groups
  - User
  - Incident User Groups
  - Data Privacy Groups
- Logpoint UEBA
  - Requirements
  - Baselining and Scoring
  - Input and Output
  - Licensing
- Backup and Restore
- Snapshots
- Troubleshooting

Logpoint Director Training (1 day)

- Logpoint Introduction
- Director Platform
- Preparing Director and Search Master
- Connecting Logpoint to Director
- Subscription and Impersonation using LPSM
- Deploying and Managing the Logpoint Director Setup using LPSM
- Authentication Mechanisms in Director Console
- Monitoring and Administrating the Fabric-enabled Logpoints using Director Console

WHO SHOULD PARTICIPATE?

IT and Information Security Professionals, such as Consultants, Auditors, Managers, Engineers and Administrators.

All participants stand to gain valuable insight on how to implement, configure, and fine-tune SIEM technology. This enables the participants to automate processes, create compliance reports and documentation and reduce false positives by monitoring, identifying, documenting, and responding to security threats in a more effective way.

Prerequisites

- Work station, desktop or laptop computer
- Remote desktop with NLA (Network Level Authentication)
- The ability to read PDF, PowerPoint, Word and Excel documents
- Chrome, Firefox or Safari browser

Training Details

The Logpoint Training take place on several occasions throughout the year at different European locations. It is comprised of a virtual lab and supporting materials where the training is delivered in a friendly and somewhat technical workshop style. The training sessions accommodate maximum 10 participants. The training will be facilitated by a Logpoint expert and is usually conducted in English, French or German to suit a multilingual audience.

Want to Know More?

We have a proven track record of training customers and partners to ensure they reap the benefits of their Logpoint implementation. Do you want to know more about which of our training tracks that are right for you? Please contact us for more information.

Bespoke Training

We also offer customized training for organizations which focus solely on your organizational needs and deployment. Based on experience, we can recommend a tailored agenda to suit your exact needs.

Top 6 Take Aways

1. Introduction to Logpoint tailored to suit the needs of the individual participants
2. Best-practices when working with the solution
3. Use-case examples from other organizations
4. Networking with other Logpoint users and exchange input
5. Input on how to manage your own or your customer's installation
6. Official Logpoint Training Certificate for each module

For more information, visit **logpoint.com**

Email: **customersuccess@logpoint.com**

LOGPOINT SOAR TRAINING

Course Description

Throughout the training session (full day), a Logpoint Certified SOAR Expert will display the full features of the SOAR solution, look into real-world use cases, highlight best practices and teach how all the various blocks can be combined.

The main focus will include the facilitation of knowledge exchange between participants, as our experience confirms that it is an excellent technique for acquiring familiarity with the solution. The emphasis throughout the training will be on ensuring that the course is conducted to accommodate the levels and requests of individual participants.

All participants stand to gain valuable insight on how to set up the SOAR solution, how to integrate and configure their products in the system and how to begin automating security-focused processes by creating and designing a playbook according to industry best practices and standards that will make responding to security threats practically instantaneous and much more effective.

Prerequisites

- Certified LogPoint User knowledge is extremely helpful but not mandatory.
- A workstation, desktop, or laptop computer.
- Remote desktop with NLA (Network Level Authentication).
- The ability to read PDF, PowerPoint, Word, and Excel documents.
- Chrome, Firefox, or Safari browser.

Course Syllabus

- SOAR - What, Why, Where & When
- The Automation Flow - Alerts, Incidents, Playbooks, Cases
- Playbook Life Cycle - Maturity Model
- Best Practices - Tips & Tricks
- SOAR Setup & Configuration - Vendors, Products & Actions
- Playbook Trigger Types
- Running API Calls
- Playbook Testing & Development
- Using Playbooks for Auditing & Documenting
- Integrating Python Scripts
- Using Conditions and Prompts
- Case Management - Controlling Case Status
- Using JSON Filters
- Performing SIEM Queries from SOAR
- Using For Each Loops and Sub-Playbooks
- Creating Automation Triggers
- Monitoring Playbook Runtimes
- SOAR Maintenance - Export & Import

How do I register?

For inquiries regarding registration and pricing, please reach out to your local Logpoint Representative or email to customersuccess@logpoint.com

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**