

Logpoint Certified User Logpoint

PRESENTATION DE LA FORMATION LOGPOINT User

Cette formation de 2 jours apprend aux stagiaires à mettre en œuvre les solutions LogPoint sur la version 7.X . Ce cours se base sur de nombreux labs de prise en main et inclut de la documentation technique en support.

DURÉE DE LA FORMATION

2 jours, soit 14 heures

PUBLIC CONCERNE

Cette formation s'adresse essentiellement aux professionnels de la sécurité.

PRE-REQUIS

Il est recommandé d'avoir les connaissances suivantes pour suivre ce cours :

- L'administration de poste de travail (Windows et Linux).
- L'administration des équipements réseau (switch, routeur, VLANs)
- Savoir utiliser les Outils Office et les fichiers PDF.

OBJECTIFS DE LA FORMATION

A l'issue de cette formation vous serez en mesure de :

- Différencier les logs bruts et les logs normalisés
- Rechercher dans les logs bruts et/ou normalisés
- Simplifier les recherches en utilisant les macros, search views et template
- Exploiter le module d'enrichissement de LogPoint
- Configurer des alertes et du reporting dans la solution

MIEL

5 Parc Burospace
91570 BIEVRES
SIRET : 33131183700032

Centre Agréé :
N°11 91 03 54 591

Pour consulter le
planning des formations
: www.miel.fr/formation

Formations sur Paris,
Bievres (91) et en
régions

Pour les Personnes en
Situation de Handicap
(PSH), contactez le
Service Formation.

Coordonnées Service
Formation et
Réclamations
01 60 19 16 27
formation@miel.fr

APPELEZ LE 01 60 19 16 27

CONTENU DE COURS

Module 1 : Introduction sur Logpoint

Module 2 : Dashboard

Module 3 : Recherches simples

- Recherche en utilisant des mots
- Recherche en utilisant des phrases

Module 4 : Modèle de recherche

- Utilisation des clefs et des valeurs
- Utilisation des labels
- Réaliser des agrégations
- Créer des macros
- Recherche Basic et Standard

Module 5 : Agrégation et groupes

Module 6 : Liste et tables

- Utilisation d'une liste
- Configuration de l'enrichissement

Module 7 : Les « Search Views »

Module 8 : Les « Search templates »

Module 9 : Le reporting

Module 10 : Configuration des alertes

Module 10 : Mise en place de l'UEBA

Module 12 : Vue avancée

Module 13 : Introduction à SOAR

CERTIFICATION PREPAREE

Cette formation prépare à la certification LogPoint User.

PASSAGE DE LA CERTIFICATION

Le prix de la formation comprend la certification, qui est obtenue en suivant la formation.

C'est la seule certification pour cette formation.

PRÉREQUIS CERTIFICATION

Aucune certification technique préalable n'est nécessaire pour passer cette certification. Il faut suivre cette formation pour être certifié à l'issue.

APPELEZ LE 01 60 19 16 27

DESCRIPTIF DE COURS

FREQUENCE DE LA FORMATION

La formation LogPoint User est planifiée uniquement sur demande (dès lors que nous avons enregistré au minimum 3 participants).

Miel se réserve le droit d'annuler une session jusqu'à 5 jours avant sa date de début en cas d'insuffisance d'inscriptions (3 personnes minimum).

MODALITÉS D'ÉVALUATION DES ACQUIS

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques (des labs de formation fournis par l'éditeur)
- Et, en fin de formation, par un questionnaire d'autoévaluation

MODALITÉS D'ACCES

Cette formation est disponible en présentiel ou en classe à distance, avec un programme et une qualité pédagogique identiques.

SUPPORT DE FORMATION

Le support de cours est fourni en fichier PDF et les labs sont en anglais.

TARIF DE LA FORMATION

Prix public : 1 650 € HT / personne (inter-entreprises)

APPELEZ LE 01 60 19 16 27