



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation LogPoint Certified User

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

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

Référence	LOG-USER
Durée	2 jours (14h)
Tarif	1 650 €HT

Objectifs

- | Identifier la différence entre les logs bruts et les logs normalisés
- | Faire des recherches dans les logs bruts et/ou normalisés
- | Utiliser les macros, search views et template pour simplifier la recherche
- | Utiliser le module d'enrichissement de LogPoint
- | Configurer des alertes et du reporting dans la solution

Public

- | Administrateurs / Ingénieurs sécurité
- | Responsable de la sécurité des systèmes d'information RSSI

Prérequis

- | Avoir des connaissances dans le monde de la sécurité
- | Administrer des postes de travail (Windows et Linux)
- | Administrer des équipements réseaux (switch, routeur, VLANs)
- | Savoir utiliser les Outils Office et les fichiers PDF

Programme de la formation

Dashboard

Recherches simples

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

Modèle de recherche

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

Agrégation et groupes

Liste et tables

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

Les « Search Views »

Les « Search templates »

Le reporting

Configuration des alertes

Mise en place de l'UEBA

Vue avancée

Introduction à SOAR

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.

Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.