

LOGPOINT POUR LES ADMINISTRATEURS

Faites face aux défis de sécurité grâce à la solution LogPoint

Code : LP-A

La formation Admin LogPoint vous enseignera les compétences nécessaires pour mettre en place la solution LogPoint et configurer la collecte des journaux de manière optimale.

Il s'agit d'une solution européenne unique sur le marché, certifiée CSPN qui vous permettra de faire face à vos défis de sécurité.

Apprenez à configurer les paramètres de sécurité, analyser les journaux pour identifier les menaces potentielles, mettre en place des stratégies de sauvegarde et de récupération des données.

En résumé, la formation vous donnera des compétences nécessaires pour gérer de manière optimale la solution LogPoint dans divers scénarios et garantir la sécurité et la fiabilité du système.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% d'exercices pratiques), ainsi que par la grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction sur LogPoint

- Présentation de l'environnement de LAB
- Configuration du serveur LogPoint :
 - Gestion des licences
 - Mises à jour
 - Paramètres des serveurs
 - Paramètre du profil
- Configuration de LogPoint :
 - Applications
 - Repositories
 - Politiques de routage
 - Politique de normalisation
 - Sources d'enrichissement
 - Processing Policies
 - Politiques de collecte des logs

JOUR 2

- Configuration d'un Device
- L'agent LogPoint :
 - Installation d'un agent LogPoint Windows (LPA)
 - Utilisation de la fonctionnalité Windows File Integrity
- Administration des utilisateurs :
 - Groupes de permissions
 - Groupes d'utilisateurs
 - Groupes d'utilisateurs en cas d'incident
 - Groupe sur la confidentialité des données
- Solution UEBA :
 - Exigences
 - Évaluation et notation
 - Entrées et sorties
 - Licences
- Sauvegarde et restauration
- Snapshots
- Support et dépannage sur LogPoint



**PROCHAINES
DATES**

Sur demande

**OBJECTIFS**

À la fin de la formation, vous serez capable de :

- Analyser les composants et la structure de la solution
- Définir les règles de normalisation
- Définir les règles d'enrichissement
- Définir les règles des stratégies de stockage des journaux (Logs)
- Paramétrer la collecte des journaux (Logs)

**INFORMATIONS GÉNÉRALES****Code** : LP-A**Durée** : 2 jours**Prix** : 1 600 € HT**Horaires** : 9h30 - 17h30**Lieu** : Levallois (92)**PUBLIC VISÉ**

- Administrateur système et/ou réseau
- Tous salariés IT souhaitant exploiter la plateforme LogPoint

**PRÉ-REQUIS**

- Avoir des connaissances en sécurité informatique
- Savoir administrer un poste de travail (Windows et Linux)
- Connaître les équipements réseaux
- Savoir utiliser les outils Office et les fichiers PDF

**RESSOURCES**

- Support de cours
- 50% d'exercices pratiques
- 1 PC par personne