LOGPOINT POUR LES UTILISATEURS

Faites face aux défis de sécurité grâce à la solution LogPoint

Code : LP-U

Cette formation User LogPoint vous enseignera les compétences nécessaires pour résoudre des problèmes de cybersécurité complexes et atténuer efficacement les menaces grâce à la solution de SIEM LogPoint.
Il s'agit d'une solution européenne unique sur le marché, certifiée CSPN qui vous permettra de faire face à vos défis de sécurité.
Acquérir la compétence pour transformer des données complexes en informations exploitables est essentiel pour offrir une meilleure visibilité sur la sécurité d'une entreprise.
Maîtriser la détection des menaces en temps réel, identifier les tendances et anticiper les attaques potentielles.
Élaborer des tableaux de bord personnalisés pour visualiser et analyser l'état de la sécurité de votre entreprise.
Cette formation offre une expertise précieuse dans le domaine de la sécurité informatique, fournissant les outils nécessaires pour une défense efficace des systèmes et des données.

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
- Centre d'aide LogPoint
- Tableaux de bord
- Recherches simples :
  - Recherche par mot
  - Recherche par des phrases
- Modèles de recherches
- Utilisation de clé-valeur
- Utilisation de Labels
- Réalisation de l'agrégation
- Macros
- Recherches basiques
- Recherches standards

JOUR 2

- « Search View »
- Templates de recherche
- Reporting
- Configuration des alertes
- LogPoint UEBA

PROCHAINES DATES

Sur demande

OBJECTIFS

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

- Connaître la différence entre les logs bruts et/ou les logs normalisés
- Faire des recherches sur les Logs bruts
- Faire des recherches sur les Logs normalisés
- Maîtriser l'usage des macros
- Maîtriser l'usage des différentes vues de recherche
- Maîtriser l'usage des templates des recherches
- Maîtriser l'usage des tableaux de bord
- Utiliser le module d'enrichissement
- Mettre en place des alertes et des rapports au sein de la solution

INFORMATIONS GÉNÉRALES

Code : LP-U
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