Formation

N° de déclaration : 11 91 05892 91

Gestion des Logs avec Splunk niveau 1

Référence : FSESP1

- **Durée : 3 jours**
- Type : Intra sur mesure, Classe Virtuelle
- Dates : nous consulter
- Certification : Non

Localisations :

- In Situ, ou
- Evry

Supports :

- Support de cours électronique
- Attestation de formation
- Feuille d'évaluation
- Feuille d'émargement

Prix :

Nous consulter

Renseignements : 09 72 58 01 05

Analyser les Logs de sécurité avec le Logiciel Splunk

Objectifs

Ce cours permettra aux participants d'acquérir une vision d'ensemble des problématiques de la gestion de la sécurité et plus particulièrement de la gestion des Logs de sécurité avec l'outil SPLUNK. Le cours initiera les participants aux fonctions de Reporting et au développement d'« APPs »

Participants

Ingénieurs systèmes et réseaux, Ingénieurs sécurité, Ingénieurs d'exploitation

Pré-requis

Les élèves doivent avoir une connaissance de base de la sécurité Informatique

Points Clefs

- Architecture
- Introduction à la gestion des Logs de sécurité
- Les bonnes et pratiques
- La législation française sur la durée de conservation des logs
- Architecture et Frameworks
- Collecte et indexation des données
- Exploitation des données
- Authentification des transactions
- Création et représentation de rapports
- Création d'APPs

Etape Suivante

N/A

Formateur

Consultant Formateur expert en sécurité informatique

Programme

Jour 1

- Les bonnes et pratiques
- Architecture et Frameworks
- Collecte et indexation des données
- Exploitation des données
- Authentification des transactions
- Intégration aux annuaires LDAP et aux serveurs AD
- Introduction au « Searching et Reporting »

Jour 2

- Utilisation des requêtes et génération de rapports
- Les fonctions et commandes de requêtes
- La création de rapports
- La représentation des rapports
- Le traitement des données
- Cas pratique sur la création de rapports

Jour 3

- Introduction au développement d'APPs
- Création d'APPs
- Configurations
- Création de modèles
- Cas pratique sur la création d'une APP