Développez vos talents
Certifiez vos compétences

Offre éditeurs

Splunk - Gestion des opérations de cybersécurité

5 jours (35h00) | ★★★★½ 4,6/5 | SPLUNK-CYBER | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Offre éditeurs

À l'issue de ce stage vous serez capable de :

- Utiliser Splunk pour collecter, analyser et générer des rapports sur les données
- Enrichir les données opérationnelles à l'aide de recherches et de flux
- Créer des alertes en temps réel
- Réaliser du scripting sur Splunk
- Intégrer des graphiques avancés
- Utiliser l'API de Splunk
- Mettre en place les bons réflexes d'exploitation de Splunk
- Améliorer l'exploitation de données avec Splunk
- Reconnaître les obligations légales en matière de conservation des données
- Définir la démarche d'une analyse de log
- Interpréter la corrélation et l'analyse avec Splunk
- Déployer Splunk de manière avancée
- Administrer Splunk.

Niveau requis

Avoir des connaissances de base en systèmes et réseaux ainsi qu'en Big Data.

Public concerné

Consultants sécurité, analystes SOC (Security Operation Center), administrateurs et architectes systèmes et réseaux.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Introduction et mise en place de l'environnement des Labs

- Rappel sur les principes du Big Data
- Mise en place d'une méthodologie / stratégie d'exploitation de données
- Principe de vectorisation des données
- Les KPI comme unité de mesure
- Bonnes pratiques de déploiement
- Déploiement avancé
  - Sécurité
  - Clustering
  - Capacity planning
  - Modèle en château
- Le Machine Learning et Splunk
- Déploiement de Splunk sous Windows
- Indexer des fichiers et des répertoires :
  - Via l'interface Web
  - Via le CLI
  - Par des fichiers de configuration...
- Remonter les logs et données via des :
  - Ports réseau
  - Scripts
  - Entrées modulaires
- Mise en oeuvre de l'expéditeur universel (Universal Forwarder)

Prise en main de Splunk

- Exécuter des recherches de base
- Créer des rapports
- Créer des tableaux croisés dynamiques
- Les tableaux de bord et l'intelligence opérationnelle
- Les types de graphes

Exploration de données

- Requêtes de SPL, opérateurs booléens et commandes
- Recherches à l'aide de plages de temps
- Corrélation d'évènements

Application Splunk

- Installer une application existante issue de Splunk ou d'un tiers
- Ajouter des tableaux de bord et recherches à une application
- Tableaux de bord interactifs
- Automatisation du reporting
- Développement d'applications Splunk

Modèles de données

- Les expressions régulières
- Optimiser la performance de recherche
- Données et notion de Pivot
- Introduction à l'administration des données
- Les catégories d'entrées
- Configuration du Forwarder
- Gestion des Forwarders
- Surveiller les entrées

- Entrées réseaux et scriptées
- Entrées "agentless"
- Métriques
- Manipulation des données brutes
- Prise en charge des objets de connaissances

Types d'alertes

- Conditions surveillées
- Etudes de cas
- Plan de réponses aux alertes
- Méthodologie de priorisation et traitement des alertes
- Splunk pour les SOC (Security Operation Center)

Exploitation avancée de Splunk

- Capacity Management
- Troubleshooting et Splunk
- Performance
- REST API Endpoint
- Monitoring
- Déploiement avancé
  - Redondance
  - Authentification
  - Load Balancers
  - Multi-heads
  - Single Sign-On (SSO)...

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)