Splunk - Déploiement et Administration

5 jours - 35 heures	Code formation : ADHSYS0707

adhara France

adhara.fr

Objectifs

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. Maîtriser les bons réflexes d'exploitation de Splunk. Améliorer l'exploitation de données avec Splunk. Connaître les obligations légales en matière de conservation des données. Connaître la démarche d'une analyse de log. Appréhender la corrélation et l'analyse avec Splunk. Déployer Splunk de manière avancée. Administrer Splunk.

Participants

Tout consultant sécurité, analyste SOC (Security Operation Center), administrateur et architecte systèmes et réseaux.

Prérequis

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

Pédagogie

La pédagogie est basée sur le principe de la dynamique de groupe avec alternance d'apports théoriques, de phases de réflexion collectives et individuelles, d'exercices, d'études de cas et de mises en situations observées. Formation / Action participative et interactive : les participants sont acteurs de leur formation notamment lors des mises en situation car ils s'appuient sur leurs connaissances, les expériences et mettront en œuvre les nouveaux outils présentés au cours de la session.

Remarques

Certification

Profil de l'intervenant

Consultant-formateur expert. Suivi des compétences techniques et pédagogiques assuré par nos services.

Moyens techniques

Encadrement complet des stagiaires durant la formation. Espace d’accueil, configuration technique des salles et matériel pédagogique dédié pour les formations en centre. Remise d’une documentation pédagogique papier ou numérique à échéance de la formation.

Méthodes d'évaluation des acquis

Un contact téléphonique est systématiquement établi avec le stagiaire ou la personne chargée de son inscription afin de définir le positionnement. Si besoin, un questionnaire est adressé pour valider les prérequis en correspondance et obtenir toute précision nécessaire permettant l’adaptation de l’action. Durant la formation, des exercices individuels et collectifs sont proposés pour évaluer et valider les acquis du stagiaire. La feuille d’émargement signée par demi-journée ainsi que l’évaluation des acquis sont adressées avec la facture.

Programme

Programme de formation

Splunk - Déploiement et Administration

5 jours - 35 heures	Code formation : ADHSYS0707

adhara France

adhara.fr

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, CLI, par fichiers de configuration...)
Remonter les logs et données via ports réseau, scripts ou 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 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

Splunk - Déploiement et Administration

5 jours - 35 heures | Code formation : ADHSYS0707

Types d'alertes

Conditions surveillées
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...)