Collecte et analyse des Logs avec Splunk

Optimiser l'exploitation des données machines et logs

Présentiel ou en classe à distance

2 jours (14 h)

Prix inter : 1.650,00 € HT
Forfait intra : 4.550,00 € HT

Réf.: SR240

Idéal en Distanciel

L'exploitation centralisée des données machines issues des logs des serveurs et postes de travail du parc de l'entreprise dépasse désormais de loin l'historique gestion des alertes. Splunk, numéro un sur son marché, propose aux administrateurs systèmes et réseaux un panel d'outils et des fonctionnalités aussi variées que performantes. La recherche d'informations et la production de rapports s'en trouve facilités par les différents modèles à disposition, ainsi les administrateurs peuvent se consacrer aux diverses taches d'exploitation. C'est précisément pour savoir tirer profit de ces différents outils que cette formation a été conçue. A l'issue de ces 2 jours, les participants disposeront des compétences et connaissances leur permettant d'optimiser et d'exploiter les données machines et logs du parc informatique de leur établissement.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs systèmes et réseaux

Prérequis

- Connaissances de base des réseaux et des systèmes
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Installer Splunk ; récupérer/injecter les données

- Concepts Big Data
- Installer Splunk sous Windows
- Indexer des fichiers et des répertoires via l'interface Web
- Mise en oeuvre de l'Universal Forwarder
- Gestion des Indexes
- Durée de rétention des données
- Travaux pratiques : installer et configurer Splunk ; utiliser Universal Forwarder pour récupérer des logs Apaches/Linux et Active Directory/Windows

2 - Exploration de données

- Requêtes avec Search Processing Language, ou SPL, un langage développé par Splunk
- Opérateurs booléens, commandes
- Recherche à l'aide de plages de temps
- Travaux pratiques : mise en oeuvre de définition d'extractions de champs, de types d'évènements et de labels ; traitement de fichiers csv ; extraire des statistiques de fichiers de journalisation Firewall

3 - Tableaux de bord (Base)

- Les tableaux de bord et l'intelligence opérationnelle, faire ressortir les données
- Les types de graphes
- Travaux pratiques : créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées

4 - Tableaux de bord (Avancé)

- Commandes avancées de SPLLookup
- Produire de façon régulière (programmée) des tableaux de bord au format PDF
- Travaux pratiques : créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées ; création de nombreux tableaux de bord basés sur l'analyse des événements Windows dans une optique de scénarii d'attaques

5 - Installation d'application

- Installer une application existante issue de Splunk ou d'un tiers
- Ajouter des tableaux de bord et recherches à une application
- Travaux pratiques : créer une nouvelle application Splunk ; installer une application et visualiser les statistiques de trafics réseaux

6 - Modèles de données

- Les modèles de données
- Mettre à profit des expressions régulières
- Optimiser la performance de recherche
- Pivoter des données
- Travaux pratiques : utiliser la commande pivot, des modèles pour afficher les données

7 - Enrichissement de données

- Regrouper les événements associés, notion de transaction
- Mettre à profit plusieurs sources de données
- Identifier les relations entre champs
- Prédire des valeurs futures
- Découvrir des valeurs anormales
- Travaux pratiques : mise en pratique de recherches approfondies sur des bases de données

8 - Alertes

- Conditions surveillées
- Déclenchement d'actions suite à une alerte avérée
- Devenir proactif avec les alertes
- Travaux pratiques : exécuter un script lorsqu'un attaquant parvient à se connecter sur un serveur par Brute Force SSH

Les objectifs de la formation

- Être capable de comprendre les concepts Splunk Utilisateur et Splunk Administrateur
- Apprendre à installer Splunk
- Pouvoir écrire des requêtes de recherche simple dans les données
- Savoir appliquer les différentes techniques de visualisation de données en utilisant les graphes et tableaux de bord
- Être en mesure d'implémenter Splunk pour analyser et surveiller les systèmes
- Comprendre comment écrire des requêtes avancées de recherche dans les données
- Savoir configurer les alertes et les rapports

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une formation délivrée par des experts de la cybersécurité
- Une première mise en pratique de Splunk
- 82% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence SR240

Dernières places disponibles Session garantie

Rouen

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.

Nantes

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 1 oct. au 2 oct.

A distance

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.
du 23 avr. au 24 avr.	du 1 oct. au 2 oct.	

Paris

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.
du 23 avr. au 24 avr.	du 1 oct. au 2 oct.	

Lyon

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.

Rennes

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 1 oct. au 2 oct.

Bordeaux

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.

Sophia Antipolis

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.

Strasbourg

du 12 févr. au 13 févr.	du 23 juil. au 24 juil.	du 26 nov. au 27 nov.

Lille

du 23 avr. au 24 avr.	du 1 oct. au 2 oct.	du 26 nov. au 27 nov.

Aix-en-Provence

du 23 avr. au 24 avr.	du 1 oct. au 2 oct.	du 26 nov. au 27 nov.

Marseille

du 23 avr. au 24 avr.	du 1 oct. au 2 oct.	du 26 nov. au 27 nov.

Toulouse

du 23 avr. au 24 avr.	du 1 oct. au 2 oct.	du 26 nov. au 27 nov.