Formation Splunk, analyse des données opérationnelles

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Splunk est un outil qui ambitionne de nous aider dans la collecte et le tri de l'information pertinente : un outil que l'on pourrait désigner par "corrélateur d'événements". Cette formation vous permettra de configurer, analyser et générer des rapports sur les données en fonction de vos alertes personnalisées.

Référence	PUK
Durée	3 jours (21h)
Tarif	2 290 €HT
Repas	repas inclus

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, scriptées et d'autres alertes intelligentes
| Intégrer des graphiques JavaScript avancés
| Utiliser l'API de Splunk

Public

| Administrateurs systèmes et réseaux.

Prérequis

| Connaissances de base des réseaux et des systèmes.

Programme de la formation

Configurer Splunk
| L'obtention d'un compte Splunk.com.
| Installer Splunk sous Windows.
| Indexer des fichiers et des répertoires via l'interface Web, CLI, par fichiers de configuration.
| Obtenir des données via ports réseau, script ou entrées modulaires.
| Mise en oeuvre de l'expéditeur universel (Universal Forwarder).
| Travaux pratiques : Configurer Splunk. Mise en oeuvre de définition d'extractions de champs, de types d'évènements et de labels.

Exploration de données
| Requêtes de SPL. Opérateurs booléens, commandes.
| Recherche à l'aide de plages de temps.
| Travaux pratiques : Extraire des fichiers de journalisation, les pages Web les plus visitées, le navigateur le plus utilisé, les sites les plus visités...

Tableaux de bord
| 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.

Nouvelle application
| 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.
| Produire de façon régulière (programmée) des tableaux de bord au format PDF.
| Travaux pratiques : Créer une nouvelle application Splunk. Installer une application et visualiser des événements liés aux switchs Cisco.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 22 au 24 mai 2024
du 23 au 25 septembre 2024
du 16 au 18 décembre 2024

PARIS
du 16 au 18 septembre 2024
du 9 au 11 décembre 2024

LYON
du 22 au 24 mai 2024
du 23 au 25 septembre 2024
du 16 au 18 décembre 2024

VOIR TOUTES LES DATES

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.

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.

Types d'alertes
| Conditions surveillées.
| Actions entreprises suite à alerte avérée.
| Devenir proactif avec les alertes.
| Travaux pratiques : Exécuter un script quand se produit l'erreur de serveur Web 503, écrire les détails associés à l'événement dans un fichier.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.