

Formation Splunk Analyse des données opérationnelles

Présentation

Ce programme de formation sur Splunk couvre l'installation et la configuration de Splunk, l'indexation de fichiers, et l'exploration de données via des requêtes SPL. Il inclut également la création de tableaux de bord, le développement d'applications, l'utilisation de modèles de données, et la gestion des alertes. Chaque module est accompagné de travaux pratiques pour une application concrète des concepts appris.

Durée : 21,00 heures (3 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

À l'issue de la formation, le participant sera en mesure 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, scriptées et d'autres alertes intelligentes
- Intégrer des graphiques JavaScript avancés
- Utiliser l'API de Splunk

Prérequis

Connaissances de base en logs et sécurité

Public

Administrateurs, ingénieurs système

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

Travaux pratiques : Configurer Splunk. Mise en œuvre de définition d'extractions de champs, de types d'événements 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.

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.

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.

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.