AF-SPLU - COLLECTE ET ANALYSE DE LOG SPLUNK

INFORMATIONS

Référence : AF-SPLU

Prix de la formation : 1400 € HT par personne

Durée : 2 jours

Pauses-café et déjeuners offerts

Cours pratique en présentiel ou en classe à distance

ÉQUILIBRE THÉORIE / PRATIQUE : Alternance de cours théorique, d'exemples et d'exercices pratiques réalisés par les participants sur la base de l'étude de cas à la fin de chaque thème

VÉRIFICATION DES CONNAISSANCES : Des QCM et des exercices pratiques sont réalisés tout au long et à la fin de formation afin de vérifier l'acquisition des connaissances par les participants.

Délai d'accès : 1 mois de délai à compter de la réception de la demande de formation

AVIS GÉNÉRAL

★★★★☆ 4/5

HANDICAP

@forSSIc accorde un soin particulier à l'accueil des personnes en situation de handicap et propose un panel de dispositions en fonction des situations et des lieux de formation. Pour plus d'informations veuillez nous contacter auprès de l'adresse suivante : contact@forssic.fr

DESCRIPTION

Splunk, numéro un sur son marché, propose aux administrateurs systèmes et réseaux un panel d'outils et des fonctionnalités aussi variées que performantes. Cette formation vous permettra de comprendre les concepts Splunk, d'écrire des requêtes de recherche, appliquer les différentes techniques de visualisation, comprendre comment utiliser Splunk pour analyser et surveiller les systèmes, savoir configurer les alertes et les rapports.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- 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

PROGRAMME DE LA FORMATION

1 - INTRODUCTION À SPLUNK :

- Qu'est-ce que Splunk ?
- Qu'est-ce qu'une donnée ?
- Comment fonctionne Splunk ?
- Comment déployer Splunk ?
- A quoi servent les applications Splunk ?
- Quelles solutions pour améliorer Splunk ?

2 - COMPOSANTS SPLUNK :

- Les Forwarders
- L'indexeur
- Les Search Heads
- Les modèles de déploiements

3 - OBTENIR DES DONNÉES :

- Processus temporel de l'index de Splunk
- Types des saisies de données et métadonnées par défaut
- Ajouter une entrée avec Splunk Web
- Définir le type de source, paramétrage et résumé

4 - LES RECHERCHES BASIQUES :

- Assistant de recherche
- Affichage des résultats de la recherche
- Les plages de temps : sélectionner, abréviation, gérer la chronologie
- Contrôle et enregistrement des panneaux de recherche. Affichage de l'historique

5 - UTILISER DES CHAMPS DE RECHERCHE :

- Que sont les champs ? Découverte, spécificité et description, utilisation
- La fenêtre Flelds
- Distinction entre != et NOT
- Les différents modes de recherche

6 - LES MEILLEURS PRATIQUES :

- Bonne pratique de recherche
- Travailler avec des index

7 - LE LANGAGE DE RECHERCHE SPLUNK :

- Syntaxe de la langue de recherche
- Pipeline de recherche, la rendre plus lisible

PUBLIC CONCERNÉ

Administrateurs système et réseaux

PRÉREQUIS

- **Connaissance de base des réseaux et des systèmes**

SOLUTION DE FINANCEMENT

Pour trouver la meilleure solution de financement adaptée à votre situation : contactez votre conseiller formation.
Il vous aidera à choisir parmi les solutions suivantes :

- Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
- Le dispositif FNE-Formation.
- L'OPCO (opérateurs de compétences) de votre entreprise.
- Pôle Emploi sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

HORAIRES

En présentiel, les cours ont lieu de 9h à 12h30 et de 14h à 17h30. Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts. En classe à distance, la formation démarre à partir de 9h. Pour les stages pratiques de 4 ou 5 jours, quelque soit la modalité, les sessions se terminent à 15h30 le dernier jour.

- Création d'un tableau et ses champs
- Utilisation des commandes Fields, Dedup, Sort

8 - LES COMMANDES DE TRANSFORMATION :

- Commande Top (unique et multiple)
- Commande Rare
- Commande Stats : Opérations statistiques
- Mise en forme des tableaux stats

9 - CRÉATIONS DE RAPPORTS ET DE TABLEAUX DE BORD :

- Que sont les rapports ? Les nommer intelligiblement, création à partir d'une recherche
- Exécuter des rapports, les modifier
- Création de tableaux et des visualisations
- Modifier la visualisation
- Ajouter un rapport à un tableau de bord, le modifier, l'exporter, le définir par défaut

10 - LES PIVOTS ET LA PRÉPARATION DE LA DONNÉE :

- Ouvrir un pivot, sélectionner la plage horaire, diviser les lignes, l'ajouter au tableau de bord
- Organiser les résultats, les visualiser

11 - CRÉATION ET UTILISATION DE LOOKUPS :

- Qu'est-ce que lookup ? Exemple de fichier
- Créer lookup, ajout d'un nouveau fichier dans la table de lookup
- Utilisation de lookup automatique
- Commande inputlookup et lookup
- Création d'une définition de lookup
- Options avancées, lookup basés sur le temps

12 - CRÉATION DE RAPPORTS ET ALERTE PROGRAMMÉE :

- Création d'un rapport programmé, planifié, programme
- Gestion des rapports : modifier les autorisations, les intégrer
- Création d'une alerte, définir les autorisations
- Alerte en temps réel ou planifiée
- Définir les conditions des déclencheurs

AVIS CLIENTS

★★★★☆ 4/5

Moyenne calculée sur l'ensemble des formations animées par @ForSSIc pour divers clients sur l'année 2022