Splunk, analyse des données opérationnelles chercher, analyser et visualiser les données générées par son SI (Serveur, Sonde, Réseau, …)

Cours Pratique de 3 jours - 21h
Réf : PUK - Prix 2025 : 2 440 HT
Le prix pour les dates de sessions 2026 pourra être révisé

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.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant 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

LE PROGRAMME

dernière mise à jour : 01/2024

1) 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 œuvre de l'expéditeur universel (Universal Forwarder).

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

2) 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...

3) 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.

4) 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.

PARTICIPANTS

Administrateurs systèmes et réseaux.

PRÉREQUIS

Connaissances de base des réseaux et des systèmes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

- 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.

5) 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.

6) 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.

7) 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.

LES DATES

CLASSE À DISTANCE
2025 : 06 oct.

2026 : 25 mars, 01 juin, 16 sept.,
02 déc.