# COLLECTE ET ANALYSE DE DONNÉES MACHINE AVEC SPLUNK

IRE12 | 2 jours (14h) 1 490,00 €HT

## Objectifs

Comprendre les concepts Splunk • Écrire des requêtes de recherche • Appliquer les différentes techniques de visualisation • Utiliser Splunk pour analyser et surveiller les systèmes • Configurer les alertes et les rapports

## Profil Stagiaire(s)

Administrateurs systèmes et réseaux, ingénieur sécurité

## Pré-requis

Connaissances de base des systèmes et des réseaux

## Profil Animateur(s)

Consultant Splunk


## Contactez-nous

Conseiller formation
09 88 66 10 00
inscriptions@demos.fr

## PROGRAMME

**Concepts et installation**
Concepts Big Data
Présentation de Splunk
Installer Splunk sous Windows

**Récupérer les données**
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

**Exploration de données**
Requêtes avec le langage Search Processing Language (SPL)
Définition d'extractions de champs, de types d'évènements et de labels

**Tableaux de bord**
Faire ressortir les données avec les tableaux de bord
Les types de graphes
Produire de façon programmée des tableaux de bord au format PDF

**Installation d'applications**
Installer une application existante issue de Splunk ou d'un tiers
Ajouter des tableaux de bord à une application

**Modèles de données**
Les différents modèles de données
Mettre à profit des expressions régulières
Optimiser la performance de recherche
Pivoter des données

**Installation d'applications**
Installer une application existante issue de Splunk ou d'un tiers
Ajouter des tableaux de bord et recherches à une application

**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

**Alertes**
Conditions surveillées
Déclenchement d'actions suite à une alerte avérée
Devenir proactif avec les alertes

## Méthodes pédagogiques & Evaluation

**Suivi & Evaluation**
Pour assurer un suivi individuel, Demos a mis en place 2 types d'évaluation :
Une évaluation de compétences en ligne en début et en fin de formation qui peut prendre différentes formes selon le contenu de la formation suivie : Tests d'évaluation des acquis, cas pratiques, mises en situation, soutenance devant un jury pour les formations à finalité certifiante.
Une évaluation de la satisfaction de chaque stagiaire est réalisée en ligne. Cette évaluation est complétée par l'appréciation du formateur à l'issue de chaque session.

**Ressources pédagogiques**
Support de formation, exercices…

**Moyens techniques**
Nos centres de formation DEMOS, accessibles aux personnes à mobilité réduite, sont tous équipés :

- Salles de formation lumineuses, spacieuses, design, ergonomiques, mobiles et équipées d'écrans plasma, de PC portables/fixes si nécessaire à la formation suivie
- Accès au wifi haut débit sur l'ensemble des lieux
- Espace de colearning et webcorners
- Cafés, collations et rafraîchissement sont offerts

Les sessions "A distance" sont réalisées avec l'outil de visioconférence Teams, permettant au formateur d'adapter sa pédagogie.