Formation Collecte et analyse des Logs avec Splunk

Optimiser l'exploitation des données machines et logs

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

L'exploitation centralisée des données machines issues des logs des serveurs et postes de travail du parc de l'entreprise dépasse désormais de loin l'historique gestion des alertes. Splunk, numéro un sur son marché, propose aux administrateurs systèmes et réseaux un panel d'outils et des fonctionnalités aussi variées que performantes. La recherche d'informations et la production de rapports s'en trouve facilités par les différents modèles à disposition, ainsi les administrateurs peuvent se consacrer aux diverses taches d'exploitation. C'est précisément pour savoir tirer profit de ces différents outils que cette formation a été conçue. A l'issue de ces 2 jours, les participants disposeront des compétences et connaissances leur permettant d'optimiser et d'exploiter les données machines et logs du parc informatique de leur entreprise.

Référence	RES240
Durée	2 jours (14h)
Tarif	1 590 €HT

Objectifs

| Expliquer les concepts Splunk Utilisateur et Splunk Administrateur
| Installer Splunk
| Ecrire des requêtes de recherche simple dans les données
| Appliquer les différentes techniques de visualisation de données en utilisant les graphes et tableaux de bord
| Implémenter Splunk pour analyser et surveiller les systèmes
| Ecrire des requêtes avancées de recherche dans les données
| Configurer les alertes et les rapports

Public

| Administrateurs systèmes et réseaux

Prérequis

| Connaissances de base des réseaux et des systèmes

Programme de la formation

Installer Splunk ; récupérer/injecter les données
| Concepts Big Data
| Installer Splunk sous Windows
| 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
| Travaux pratiques : installer et configurer Splunk ; utiliser Universal Forwarder pour récupérer des logs Apaches/Linux et Active Directory/Windows

Exploration de données
| Requêtes avec Search Processing Language, ou SPL, un langage développé par Splunk
| Opérateurs booléens, commandes
| Recherche à l'aide de plages de temps
| Travaux pratiques : mise en oeuvre de définition d'extractions de champs, de types d'évènements et de labels ; traitement de fichiers csv ; extraire des

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 10 au 11 juillet 2025
du 30 au 31 octobre 2025

PARIS
du 10 au 11 juillet 2025
du 30 au 31 octobre 2025

AIX-EN-PROVENCE
du 30 au 31 octobre 2025

BORDEAUX
du 30 au 31 octobre 2025

GRENOBLE
du 30 au 31 octobre 2025

LILLE
du 30 au 31 octobre 2025

LYON
du 30 au 31 octobre 2025

NANTES
du 10 au 11 juillet 2025

RENNES
du 10 au 11 juillet 2025

ROUEN
du 30 au 31 octobre 2025

SOPHIA-ANTIPOLIS
du 30 au 31 octobre 2025

VOIR TOUTES LES DATES

statistiques de fichiers de journalisation Firewall

Tableaux de bord (Base)
| 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

Tableaux de bord (Avancé)
| Commandes avancées de SPLLookup
| Produire de façon régulière (programmée) des tableaux de bord au format PDF
| Travaux pratiques : créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées ; création de nombreux tableaux de bord basés sur l'analyse des événements Windows dans une optique de scénarii d'attaques

Installation d'application
| Installer une application existante issue de Splunk ou d'un tiers
| Ajouter des tableaux de bord et recherches à une application
| Travaux pratiques : créer une nouvelle application Splunk ; installer une application et visualiser les statistiques de trafics réseaux

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

Alertes
| Conditions surveillées
| Déclenchement d'actions suite à une alerte avérée
| Devenir proactif avec les alertes
| Travaux pratiques : exécuter un script lorsqu'un attaquant parvient à se connecter sur un serveur par Brute Force SSH

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.