Collecte et Analyse des Logs avec Splunk

Lien : https://innov-systems.com/formation/collecte-et-analyse-des-logs-avec-splunk

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC156

CATÉGORIE
LOG : exploitation des données

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- S'approprier les principes de fonctionnement et l'architecture de Splunk
- Apprendre à installer Splunk
- Savoir collecter, analyser et générer des rapports sur plusieurs types de données
- Comprendre et mettre en pratique la recherche avec le langage SPL (Search Processing Language)
- Savoir appliquer les différentes techniques de visualisation de données en utilisant les graphes et tableaux de bord
- Construire des modèles de données et conduire des recherches basées sur le Pivot
- Exploiter la puissance de la plateforme pour mettre en œuvre des recherches avancées et enrichir des ensembles de données
- Créer des alertes en temps réel et être en mesure de réagir efficacement à différents événements

POUR QUI ?

- Administrateurs systèmes et réseaux

Innov Systems

Programme détaillé

1 / Introduction

- Retour sur quelques concepts Big Data

2 / Présentation de Splunk

- Vue d'ensemble de Splunk
- L'utilité de Splunk. Cas d'usage
- Vue d’ensemble des produits de la galaxie Splunk : Splunk Enterprise, Splunk Cloud, Splunk Light, Hunk…
- Atouts et limites de la plateforme
- Les principaux composants : CLI, interface Web, daemon et data store
- L’architecture fonctionnelle de Splunk : Search Heads, Indexers et Forwarders
- Produits concurrents : ELK, Graylog, Sumo Logic…

3 / Installation de Splunk

- Installer Splunk sous Windows
- Créer un compte
- Indexer fichiers et dossiers
- Installer et commencer à utiliser l’Universal Forwarder
- Gestion des Indexes
- Durée de rétention des données

4 / Démarrer avec Splunk : recherches simples

- Les différents types d’entrées
- Effectuer des recherches basiques
- Utiliser la saisie automatique
- Restreindre une recherche avec des plages temporelles

Innov Systems

- Utiliser la Timeline
- Une première introduction au langage SPL
- Travailler avec les évènements
- Comprendre et utiliser les champs
- S’approprier les différentes vues pour la recherche
- Sauvegarder des résultats de recherche

5 / Exploration de données

- Principes de fonctionnement et langage SPL (Search Processing Language)
- Comprendre la syntaxe SPL et l’anatomie d’une recherche
- Opérateurs booléens, commandes
- Spécifier les index dans une recherche
- Utiliser les commandes tables, rename, fields, dedup, sort...
- Commandes de transformation
- Créer et concaténer des sous-requêtes
- Manipuler et filtrer les résultats
- Recherche à l’aide de plages de temps

6 / Reporting : création de rapports

- Vue d’ensemble des possibilités de visualisation de données avec Splunk
- Sauvegarder une recherche en tant que rapport
- Modifier et partager des rapports
- Intégrer et mettre en forme des graphiques et tableaux
- Créer et enrichir des tableaux de bord

7 / Créer et enrichir des tableaux de bord

- Les tableaux de bord et l’intelligence opérationnelle, faire ressortir les données
- Les types de graphes
- Commandes avancées de SPLLookup

Innov Systems

- Produire de façon régulière (programmée) des tableaux de bord au format PDF

8 / Création d’une application Splunk

- Créer une application Splunk à partir de l’interface Web
- Ajouter des tableaux de bord à l’application
- Gérer les permissions
- Ajouter des liens dans les graphiques et créer des tableaux de bord interactifs

9 / Modèles de données et utilisation de l’outil Pivot

- Introduction aux modèles de données et à la commande Pivot
- Définir les attributs d’un modèle de données
- Créer un modèle de données
- Mettre à profit des expressions régulières
- Optimiser la performance de recherche
- Pivoter des données

10 / Enrichissement de données

- Corrélation d’évènements et transactions
- Comparaison de transactions vs. stats
- Mettre à profit plusieurs sources de données
- Identifier les relations entre champs
- Prédire des valeurs futures
- Découvrir des valeurs anormales

11 / Créer des alertes

- Conditions surveillées
- Déclenchement d’actions suite à alerte avérée
- Devenir proactif avec les alertes

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

02 au 05 Fév. 2027	Présentiel - Casablanca
30 Mars au 02 Avr. 2027	Présentiel - Casablanca
25 au 28 Mai 2027	Présentiel - Casablanca
20 au 23 Juil. 2027	Présentiel - Casablanca
21 au 24 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés