

# Collecte et analyse des Logs avec Splunk

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Cybersécurité - sécurité informatique

**Action collective :** Non

**Filière :** Sécurité défensive

**Rubrique :** SOC (Security Operations Center)

**Code de formation :** SO007

## € Tarifs

**Prix public :** 1565 €

### Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les 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.

**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

**CPF -MonCompteFormation**

Contactez nous pour plus d'information : [contact@aston-institut.com](mailto:contact@aston-institut.com)

## PRÉSENTATION

### Objectifs & compétences

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

### Public visé

Administrateurs systèmes et réseaux

### Pré-requis

Connaissances de base des réseaux et des systèmes

## 📍 Lieux & Horaires

**Durée :** 14 heures

**Délai d'accès :** Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

## PROGRAMME

### 1 - 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

### 2 - 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 statistiques de fichiers de journalisation Firewall

### 3 - 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

### 4 - 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

## 📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

recherches réalisées ; création de nombreux tableaux de bord basés sur l'analyse des événements Windows dans une optique de scénarii d'attaques

### 5 - 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

### 6 - 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

### 7 - 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

### 8 - 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

## MODALITÉS

### Modalités

**Modalités** : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

**Pédagogie** : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

**Ressources techniques et pédagogiques** : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

**Pendant la formation** : mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels.

### Méthode

**Fin de formation** : entretien individuel.

**Satisfaction des participants** : questionnaire de satisfaction réalisé en fin de formation.

**Assiduité** : certificat de réalisation.

**Validations des acquis** : grille d'évaluation des acquis établie par le formateur en fin de formation.

### Les plus de la formation

Une formation délivrée par des experts de la cybersécurité  
Une première mise en pratique de Splunk

## CERTIFICATIONS

Cette formation fait l'objet d'une évaluation formative.