Formation « SPLUNK »

Réf : SPLUNK

Splunk permet à de très nombreuses équipes opérationnelles, SOC, CSIRT de réaliser efficacement leurs investigations numériques, détection d'attaques ou chasse, en facilitant les opérations de recherche & manipulation des journaux quelques soient le volume de données.

Cette formation vous permettra d'apprendre à utiliser Splunk pour les cas d'usage de la sécurité informatique, elle complète bien les formations SECUBLUE et SECUSOC en vous fournissant les clés pour exploiter au mieux cet outil puissant.

Cette formation n'est pas une présentation exhaustive des capacités de Splunk, elle a été construite pour pouvoir être efficace et pertinente dans l'utilisation de Splunk.

Objectifs

- **Découvrir le fonctionnement et les capacités de Splunk**
- **Apprendre le langage SPL pour requêter les données efficacement**
- **Enrichir les données opérationnelles à partir de sources externes**
- **Créer des tableaux de bord dynamiques pour l'aide à la décision et la synthèse d'informations**
- **Créer des requêtes matures pour la détection d'attaque**

Durée & horaires

- **4 jours soit 28 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Analystes en détection (SOC)**
- **Analyste en conception (SOC, CSIRT)**
- **Analystes forensique (CSIRT)**
- **Auditeurs**
- **Opérationnels en sécurité**
- **Responsables sécurité opérationnelle**

Pré-requis

- **Connaissances informatiques générales (qu'est-ce qu'une adresse IP, une authentification, etc.)**
- **Compréhension des enjeux généraux en sécurité informatique (qu'est-ce qu'une attaque par bruteforce, une exfiltration de données, etc.)**

Méthode pédagogique

La formation est délivrée à travers un mélange de cours magistral et démonstrations sur le produit. Les apprenants ont tous accès à un Splunk pendant toute la durée de la formation leur permettant de reproduire les exemples fournis en cours. Des travaux pratiques de mise en œuvre sont fournis aux apprenants sur les concepts clés. Les travaux pratiques possèdent tous un énoncé et une solution détaillée, permettant aux apprenants de valider leurs exercices. Les formateurs supervisent la réalisation des travaux pratiques et accompagnent les apprenants ayant besoin d'aide. Pour les apprenants venant

en salle de formation, le déjeuner est offert et est un moment privilégié de partage entre apprenants et formateurs.

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification Splunk par HS2.**

Programme

Introduction à Splunk
- Produits de la marque Splunk
- Fonctions de Splunk Enterprise
- Architecture
- Flux de données

Ajouter des données
- Processus d'indexation
- Téléversement à travers l'interface graphique
- Organisation de la donnée dans les indexes
- Envoi à travers un Universal Forwarder
- Envoi à travers un collecteur syslog
- Supervision de modifications dans des fichiers
- Envoi par API
- Extraction de champs
- Normalisation des champs

Requêter
- - Accès aux données indexées
- - Filtre temporel
- - Paramètres des tâches de recherche
- - Exploration des résultats
- - Modes de recherche
- - Différences entre les événements et les statistiques
- - Commandes
  - Search
  - Fieldsummary
  - Where
  - fields
  - rename
  - rex
  - eval
    - Fonctions d'évaluation
  - dedup
  - sort
  - head
  - tail
  - fillnull
  - table
- - Calculs statistiques
  - Commande stats
  - Fonctions d'agrégations
  - Agrégats multiples
  - Combinaison des fonctions d'agrégation et des fonctions d'évaluation
- Manipulation des JSON
- Enrichissement de données
  - Types de lookups
  - Manipulation des lookups
  - Recoupement des données
  - Utilisation des lookups pour faire une chasse de marqueurs
    - Jointures
  - Macros de recherche
  - Sous-recherches

Configurer
- Fichiers de configuration
- Précédence des configurations
- Périmètres et gestion des droits
- Objets de connaissance
- Partage d'objets

- Installation d'une application

Tableaux de bord

- Utilisation des tableaux de bord Studio
- Forces et limitations du moteur
- Sélecteurs et filtres
- Commande timechart
- Requêtes chaînées
- Utilisation des tokens
- Interactivité des tableaux de bord

Requêtes avancées

- Commandes bin et transaction
- Requêtes pour l'investigation numérique
- Requêtes pour la détection
- Détection par seuil
- Création d'alertes pour un SOC

Conclusion

- Ressources pertinentes pour l'apprentissage continu