Formation « SPLUNK »

Réf : SPLUNK

Splunk est un outil permettant de chercher, analyser et visualiser les données de journalisation. Il permet également la corrélation d'événements afin d'aider les analystes à faire sortir l'information pertinente dans une grande quantité de journaux.

Cette formation vous permettra de configurer, analyser, générer des rapports et créer des alertes personnalisées sur les données en fonction de vos objectifs.

Objectifs

- **Utiliser Splunk pour collecter, analyser et générer des rapports sur les données**
- **Enrichir les données opérationnelles à l'aide de recherches et de flux**
- **Créer des alertes en temps réel, scriptées et d'autres alertes intelligentes afin de détecter les incidents de sécurité**

Durée & horaires

- **3 jours soit 21 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

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

Public visé

- **Analystes**
- **Membres d'un SOC ou d'un CSIRT**
- **Administrateurs sécurité**
- **Responsables sécurité opérationnelle**

Pré-requis

- **Bonnes connaissances en administration système**
- **Pour l'utilisation de Splunk, il n'est pas nécessaire d'être un expert en cybersécurité**

Méthode pédagogique

- **Cours magistral**
- **Démonstrations**
- **Exercices de mise en œuvre**

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

Configurer Splunk

- Obtention d'un compte Splunk.com
- Installer Splunk sous Windows
- Indexer des fichiers et des répertoires via l'interface Web, par ligne de commande, par fichiers de configuration
- Obtenir des données via ports réseau, script ou entrées modulaires
- Mise en oeuvre de l'expéditeur universel (Universal Forwarder)
- Travaux pratiques
    - Mise en œuvre de définition d'extractions de champs, de types d'évènements et de labels

Exploration de données

- Requêtes de SPL
- Opérateurs booléens, commandes
- Recherche à l'aide de plages de temps
- Travaux pratiques
    - Extraire des fichiers de journalisation, les pages Web les plus visitées, le navigateur le plus utilisé, les sites les plus visités...

Tableaux de bord

- Tableaux de bord et intelligence opérationnelle
- Faire ressortir les données
- Types de graphes
- Travaux pratiques
    - Créer, enrichir un tableau de bord avec des graphes liés aux recherches réalisées

Nouvelle application

- Installer une application existante issue de Splunk ou d'un tiers
- Ajouter des tableaux de bord et recherches à une application
- Tableaux de bord interactifs
- Produire de façon régulière (programmée) des tableaux de bord au format PDF
- Travaux pratiques
    - Créer une nouvelle application Splunk
    - Installer une application et visualiser des événements liés aux pare-feux

Modèles de données

- Différents 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

Types d'alertes

- Conditions surveillées
- Actions entreprises suite à alerte avérée
- Devenir proactif avec les alertes
- Travaux pratiques
    - Exécuter un script quand se produit l'erreur de serveur Web 503, écrire les détails associés à l'événement dans un fichier