Formation **Splunk**

Plateforme de stockage, traitement et analyse des données machine (ou machine data), Splunk permet une prise de décisions éclairée grâce à une visibilité en temps réel sur l'ensemble du SI. Notre formation permettra aux participants de prendre Splunk en main et d'en exploiter les principales fonctionnalités pour analyser les données de leur entreprise. Ils apprendront à effectuer des recherches et à générer des rapports en utilisant les diverses commandes Splunk. Composée d'ateliers pratiques basés sur des cas concrets, cette formation Splunk permet d'acquérir l'ensemble des connaissances et compétences nécessaires pour mettre en place une stratégie robuste pour la sécurité de l'information et la gestion des événements avec Splunk.

Durée

4 jours

Objectifs pédagogiques

- 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

Public

Analystes en détection, analyste en conception, analystes forensique, auditeurs, opérationnels en sécurité, responsables sécurité, administrateurs systèmes et réseaux...

Prérequis

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.)

Programme de formation

Introduction à la formation 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

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.