

Vous allez apprendre à

Cette formation vous permettra de passer en revue les techniques nécessaires pour auditer une application mobile iOS, ainsi que les vulnérabilités les plus courantes sur ce type d'applications.

Que vous soyez auditeur technique ou bien développeur, la connaissance des mauvaises pratiques de sécurité ainsi que les techniques d'exploitation est nécessaire. Venez approfondir vos connaissances sur les vulnérabilités liées à cette plateforme à travers cette formation !

Public visé

- Administrateurs systèmes et réseaux

Les objectifs de la formation

- 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
- Savoir configurer les alertes et les rapports

Les prérequis de la formation

- Connaissances de base des réseaux et des systèmes

Programme de la formation

Module 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

Module 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'événements et de labels ; traitement de fichiers csv ; extraire des statistiques de fichiers de journalisation Firewall

Module 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

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

Module 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

Module 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

Module 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

Module 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



2 Jours
14 Heures



Sur demande



+33 1 89 62 34 30



formation@acgcybersecurity.fr



Campus Cyber, Tour
Eria, 5 Rue Bellini 92800
Puteaux, FRANCE

Toutes nos formations sont
accessibles aux personnes en
situation de handicap.

ACG CyberAcademy 2025