COLLECTE ET ANALYSE DES LOGS AVEC SPLUNK

CODE STAGE : S0007

OBJECTIFS

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 dcode2utf('8217',0)implémenter Splunk pour analyser et surveiller les systèmes
Comprendre comment écrire des requêtes avancées de recherche dans les données

DURÉE

2 jours

PUBLIC

Administrateurs systèmes et réseaux

PRÉ-REQUIS

Connaissances de base des réseaux et des systèmes

PROGRAMME

INSTALLER SPLUNK ; RÉCUPÉRER/INJECTER LES DONNÉES
Concepts Big Data
Installer Splunk sous Windows
Indexer des fichiers et des répertoires via lcode2utf('8217',0)interface Web
Mise en oeuvre de lcode2utf('8217',0)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

EXPLORATION DE DONNÉES

Requêtes avec Search Processing Language, ou SPL, un langage développé par Splunk
Opérateurs booléens, commandes
Recherche à lcode2utf('8217',0)aide de plages de temps

Travaux pratiques : mise en oeuvre de définition d'extractions de champs, de types dcode2utf('8217',0)évènements et de labels ; traitement de fichiers csv ; extraire des statistiques de fichiers de journalisation Firewall

TABLEAUX DE BORD (BASE)
Les tableaux de bord et lcode2utf('8217',0)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

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 lcode2utf('8217',0)analyse des événements Windows dans une optique de scénarii dcode2utf('8217',0)attaques

INSTALLATION Dcode2utf('8217',0)APPLICATION
Installer une application existante issue de Splunk ou dcode2utf('8217',0)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

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

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

ALERTES
Conditions surveillées
Déclenchement dcode2utf('8217',0)actions suite à alerte avérée
Devenir proactif avec les alertes

Travaux pratiques : exécuter un script lorsqucode2utf('8217',0)un attaquant parvient à se connecter sur un serveur par Brute Force SSH