EXPERT

FORMATION ANALYSTE SOC

MISE EN PLACE D'UN SIEM EN OPEN SOURCE

Maîtrisez votre gestion d'évènements via les solutions de SIEM en open source !

Cette formation permettra de comprendre le fonctionnement des malwares, de les identifier et de les éradiquer proprement, en assurant la pérennité des données présentes sur le SI. Des bonnes pratiques et outils adaptés seront abordés tout au long de la formation et mis en pratique lors des travaux dirigés.

Code : SIEM

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

La technologie SIEM (Security Information and Event Management)
- Présentation du SIEM
- Qu'est-ce qu'un SIEM ?
- Le fonctionnement d'un SIEM
- Les objectifs d'un SIEM et de la corrélation des donnéesRéseaux virtuels et réseaux partagés

JOUR 2

Le Lab
- Le SIEM au sein d'une architecture réseau
- Présentation du Lab de formation
- Préparation du Lab

Mise en place de Windows Server
- Installation de Windows Server R2
- Configuration du serveur
- Activation et configuration du domaine
- Activation et configuration du service Active Directory (AD)

JOUR 3

Présentation de ELK (Elasticsearch, Logstash et Kibana)
- Présentation de la suite ELK
- Découverte de Elasticsearch
- Découverte de Logstash
- Découverte de Kibana

Elasticsearch
- Approche théorique : terminologie
- Application Full REST et utilisation

Travaux pratiques
- Présentation de la solution Cloud
- Installation de Elasticsearch
- Configuration du fichier : yml

Logstash
- Approche théorique : fonctionnement de Logstash

Travaux pratiques
- Installation de Logstash
- Fichier Input

JOUR 4

Kibana
- Utilisation de l'interface Discover
- Visualize et les différentes visualisations
- Comment créer des alertes ?
- Exporter en PDF les données Dashboard
- Comment sécuriser Kibana ?

Travaux pratiques
- Installation et configuration

Détection d'intrusion et remontée d'alertes sur l'Active Directory
- Présentation du scénario et de l'objectif
- Approche théorique sur l'agent WinlogBeat
- Travaux pratiques
- Mise en place de WinlogBeat
- Configurer le Dashboard sur Kibana
- Détecter une intrusion admin dans l'AD
- Détecter une intrusion Pfsens et remonter l'alerte dans le dashboard

PROCHAINES DATES

17 mars 2025
7 juillet 2025
1er septembre 2025
24 novembre 2025

OBJECTIFS

- Traiter des incidents de sécurité et leur management
- Aborder les problématiques liées à la détection d'intrusion, ainsi que leurs limites
- Mettre en place le Prelude SIEM avec implémentation de sondes SNORT et d'agents HIDS dans un réseau existant
- Prendre les bonnes décisions suite à l'analyse des remontées d'informations et à leur corrélation.

INFORMATIONS GÉNÉRALES

Code : SIEM

Durée : 4 jours

Prix : 3 990 € HT

Horaires : 9h30 - 17h30

Lieu : Levallois (92) ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Pentester
- Administrateurs système
- RSSI
- Consultants en sécurité de l'information
- Toute personne ayant des notions d'administration système (si possible ayant pratiqué)

PRÉ-REQUIS

- Avoir des connaissances générales en système, réseau et développement.

RESSOURCES

- Support de cours
- Nombreux travaux pratiques
- 1 PC par personne