Le métier d'analyste SOC (Security Operation Center)

Durée : 8 jours

Résumé

Ce parcours de formation permettra de disposer des connaissances utiles à la compréhension du fonctionnement d'un SOC ainsi que des compétences nécessaires à l'accomplissement des tâches d'analyse dans un SOC via l'usage opérationnel d'un outil de SIEM. Enfin il permettra de disposer des moyens de réussir la principale certification, d'Analyste SOC, du marché.

Objectifs

- Connaitre et comprendre l'organisation d'un SOC
- Connaitre l'outillage utilisé par les analystes SOC, et en particulier via l'apprentissage de QRadar SIEM
- Comprendre les problématiques par les cas d'usages
- Comprendre les extensions et évolutions des métiers et des fonctions du SOC
- Etre prêt pour réussir la certification *Analyste QRadar SIEM*

Public visé

Administrateur Systèmes et réseaux

Prérequis

- Connaissances de Windows et Linux et de bonnes notions de réseau
- Connaitre le guide d'hygiène informatique de l'ANSSI
- Avoir suivi le *Parcours introductif à la Cybersécurité* du FAFIEC
- Suivre le MOOC de l'ANSSI (SecNumacademie.gouv.fr)

Contenu :

MODULE 1 (2 jours) :
SOC ET SIEM les essentiels

Introduction au SOC

- Définition et rôle du SOC dans le SI
- L'organisation du SOC et ses processus
- Panorama des menaces et évolutions
- La conformité
- Loi de programmation militaire et OIV
- Les journaux d'évènements
- Les flux réseau
- Les indicateurs de compromission
- Les sources d'information

La sécurité actuelle du SI

- La sécurité périmétrique du S.I
- Sécurité des end points
- Sécurité industrielle
- Segmentation du réseau
- Cloud
- Shadow IT

Rôle et fonctionnement d'un SIEM

- Log management
- La corrélation
- L'importance de la gestion des actifs
- Concepts d'infraction de sécurité
- Les cas d'usage
- La gestion des vulnérabilités
- Implémentation de la PSSI
- Surveillance de la conformité

Travaux intermédiaires : Accéder au site https://www.securitylearningacademy.com/
Suivre les modules introductifs « QRadar »

Lecture : Présentation du SOC d'AlertLogic
https://www.alertlogic.com/assets/files/InfoWorld-SOC-Article.pdf

MODULE 2 (3 jours) :
LES OUTILS DE L'ANALYSTE SOC

L'écosystème du SIEM :

- Les catégories de produits
- Les principaux outils du marché

Le principal outil du marché : IBM QRadar SIEM

- QRadar SIEM, son origine
- Architecture et fonctionnement
- L'interface
- La gestion des logs
- La gestion des flux réseau
- La notion d'identité
- Les tableaux de bord et les rapports

Cinématique d'une infraction de sécurité

- Le concept d'offense
- Comment naviguer ?
- Que faut-il collecter ?
- Comprendre le moteur de règles
- Gestion des faux positifs

Travaux intermédiaires : Recueillir et documenter des cas d'attaque afin d'en étudier les causes et les effets, ainsi que d'imaginer les actions de remédiation.
Travaux utilisés dans la première partie du module 3

MODULE 3 (3 jours)
MISES EN SITUATION, et PERSPECTIVES

Mises en situation

- Le cas « Target », 110 Millions d'enregistrements dérobés : analyse d'une attaque de points de vente en plein Black Friday.
- Discussion ouverte et travail collectif : propositions d'amélioration pour donner suite à l'analyse du cas Target.
- Présentation par les étudiants d'un cas de hack et analyse collective.

Le SIEM, extensions et perspectives ?

- La réponse à incident
- L'analyse de binaires / L'étude forensique
- Les procédures itératives d'amélioration continue

- Le Threat Hunting
- Le rôle de L'ANSSI, du SANS Institute, les CERTs/CSIRTs
- L'écosystème des CERTs et des CSIRTs privés, commerciaux et publics
- Les métiers de la cybersécurité, les certifications reconnues

Préparation et passage de la certification Analyste QRadar

- Rappel des notions et références utiles
- Examen blanc
- Passage de la certification

Informations complémentaires

Support de cours remis aux participants
Cursus introductif QRadar : https://www.securitylearningacademy.com/enrol/index.php?id=685
Accès à une plateforme d'entrainement (QRadar)