Analyste SOC : détection d'intrusion et investigation SIEM

Date et durée

Code formation : CYBER002FR
Durée : 5 jours
Nombre d'heures : 35 heures

Description

Face à la recrudescence et à la complexité des cyberattaques, la mise en place d'un **Security Operations Center (SOC)** est devenue une nécessité pour toute organisation. Cette formation d'analyste SOC vous apporte les compétences fondamentales pour intégrer une équipe de cyberdéfense et jouer un rôle clé dans la protection des systèmes d'information. Vous apprendrez à **détecter, analyser et répondre efficacement aux incidents de sécurité** qui menacent une entreprise.
Ce **programme de formation SOC** vous guidera dans la mise en œuvre de technologies de sécurité essentielles.
Il vous apprendra à déployer des solutions de détection sur **les postes de travail (EDR) et sur le réseau (NIDS**). Puis, il vous permettra de centraliser et d'analyser les événements à l'aide d'un système de gestion des événements (SIEM).
Les cours abordent l'ensemble du processus, de **la collecte des logs à la création de règles de corrélation** pertinentes pour identifier les activités suspectes.
À l'issue de ce cours de 5 jours, vous aurez acquis une véritable posture d'**analyste en cybersécurité**. Vous serez en mesure de mener une investigation numérique de A à Z : analyser en profondeur les traces d'une attaque pour en extraire les indicateurs de compromission (IoC) et utiliser le SIEM pour **qualifier les menaces et orchestrer la réponse aux incidents**.

Objectifs

À l'issue de cette formation d'Analyste SOC, vous atteindrez les objectifs suivants :

- maîtriser le rôle, les fonctions et la structure d'un Security Operations Center (SOC) pour en comprendre le fonctionnement global ;
- déployer et configurer des solutions de détection d'intrusions, comme les NIDS (détection réseau) et les EDR (détection sur les terminaux), pour protéger les infrastructures ;
- implémenter et administrer un système de gestion des informations et des événements de sécurité (SIEM), de la collecte des journaux à la mise en place de règles de détection ;
- analyser les traces d'une attaque informatique pour en extraire les indicateurs de compromission (IoC) et en comprendre le mode opératoire ;
- apprendre à mener une investigation numérique en utilisant les outils du SOC, notamment le SIEM, pour qualifier et répondre aux incidents de sécurité.

Points forts

- **Formateur expert en cybersécurité** : la formation est dispensée par un professionnel certifié avec une expérience de terrain en SOC, garantissant un enseignement ancré dans les réalités du métier.

- **Cours axées sur l'application** : le programme consacre une part importante aux travaux pratiques (TP) sur les technologies clés (EDR, NIDS, SIEM), vous plongeant dans des scénarios d'attaques et des investigations sur des cas concrets.
- **Acquisition d'une posture d'analyste** : au-delà des outils, le cursus est conçu pour vous apprendre à penser comme un analyste (savoir analyser des attaques, extraire des indicateurs de compromission (IoC) et mener une investigation de A à Z).

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Fondamentaux en infrastructure et sécurité IT :** une bonne compréhension des systèmes et réseaux informatiques (principes TCP/IP et systèmes d'exploitation) ainsi qu'une familiarité avec les concepts de base de la cybersécurité.

Public

Cette formation s'adresse aux publics suivants :

- **les techniciens et administrateurs systèmes et réseaux** qui désirent se spécialiser dans la détection et la réponse aux incidents de sécurité ;
- **les intégrateurs de la sécurité** qui souhaitent maîtriser la mise en œuvre et l'opération des outils d'un SOC (SIEM, EDR, NIDS) ;
- **les responsables et ingénieurs SSI** qui veulent comprendre le fonctionnement d'un SOC pour mieux piloter la stratégie de cyberdéfense ;
- **les chefs de projets techniques** en charge du déploiement d'un SOC ou d'outils de sécurité ;
- **toute personne souhaitant évoluer vers le métier d'analyste en cybersécurité.**

Programme

Module 1 : maîtriser les fondements du SOC

- La définition, les objectifs et les fonctions d'un Security Operations Center (SOC).
- Les différentes structures et le fonctionnement d'une équipe SOC.
- Les étapes clés pour la mise en place d'un centre de sécurité opérationnel.

Module 2 : protéger les terminaux avec les solutions HIDS/EDR

- Présentation des systèmes de détection d'intrusion sur les hôtes (HIDS) et des solutions EDR (Endpoint Detection and Response).
- L'application de règles de détection spécifiques aux terminaux.

Travaux pratiques :

- Mettre en place des règles et détecter des attaques sur les terminaux.

Module 3 : surveiller le réseau avec les solutions NIDS/NDR

- Présentation des systèmes de détection d'intrusion réseau (NIDS) et des solutions NDR (Network Detection and Response).

- Le positionnement stratégique et la mise en écoute d'un NIDS au sein de l'architecture.

Travaux pratiques :

- Analyser des captures réseau (PCAP) malveillantes pour identifier des attaques et extraire des indicateurs de compromission (IoC).

Module 4 : piloter la détection et l'investigation avec un SIEM

- La définition, les objectifs et les différentes architectures d'un Security Information and Event Management (SIEM).
- La mise en place de règles de corrélation SIEM pour l'analyse d'événements.
- Les méthodologies fondamentales d'investigation avec un SIEM.

Travaux pratiques :

- Déployer un SIEM et configurer la collecte des événements.
- Créer et appliquer des règles de détection sur le SIEM.
- Mener une investigation complète sur un cas d'incident concret à l'aide du SIEM.