Certification Analyste Soc Niveau 1

Ref. ***CAS1-10***
Durée : 5.0 jour(s) / 35.0 heures

L'évolution du tout numérique et du tout connecté engengre une augmentation notable des cybermenaces. Toutes les entreprises se doivent d'être vigilantes et doivent pouvoir identifier et réagir au mieux face à ces cybermenaces. C'est toute une force de réaction rapide qui veille et agit pour protéger le plus eficacement nos systèmes et nos données. Les SOC sont une composante majeur de cette force de réaction.

Cette formation certifiantes vise à founir les savoirs fondamentaux nécessaires pour bien aborder ces métiers.
Elle permet de valider des savoirs décrits dans les fiches métiers de l'ANSSI : du SOC Opérateur analyste SOC Responsable du CSIRT Analyste réponse aux incidents de sécurité, Gestionnaire de crise de cybersécurité Analyste de la menace cybersécurité..

Pré-requis :

Connaissances en sécurité des systèmes et réseau
Connaissances sur les réseaux et systèmes informatique

Personnes concernées :

Techniciens et administrateurs système et réseau
Intégrateur de la sécurité
Analyste SOC niveau 1
Responsable SSI
Ingénieurs SSI
Chefs de projets techniques

ECSF Metiers associés :
Cyber Incident responder,digital forensics investigator, Chief Information Security Officer, Cybersecurity Architect, Cybersecurity implementor, Cyber threat intelligence specialist

Objectifs :

- Reproduire les bonnes pratiques d'analyse
- Décrire le processus de gestion des incidents de sécurité de l'information
- Décrire le processus de fonctionnement d'un SIEM et d'un SOC
- Gérer des solutions de de prévention et de détection d'intrusions.
- Identifier des attaques et en extraire les IoC.
- Corréler des IoC

Programme :

JOUR 1

La gestion des incidents de sécurité de l'information
Les normes : ISO 27035
Les acteurs : CSIRT, PSIRT, CERT..
Les IOC
Mittre att@k et incidents de sécurité
Réaliser un programme de gestion des incidents de sécurité de l'information

SOC
Qu'est-ce qu'un SOC ?
Objectifs d'un SOC
Les services et fonctions d'un SOC
Architectures
Les compétences et métiers
Structures et fonctionnement d'un SOC
Mise en place d'un SOC
SOC interne vs SOC externalisé
Mise à jour et communication

Quizz sur le processus de gestion des incidents de sécurité de l'information

JOUR 2

Logs

Principes d'analyses de logs
Les types de logs à collecter
Serveur de log
Les logs windows
Les logs linux
Les logs pour les serveurs WEB
Sauvegarde

Tps : analyse de logs

Equipements de détection d'intrusion
Les NIDS / NDR
La place du NIDS dans l'architecture
Mettre en écoute le NIDS
Se préparer et agir lors d'une détection
Collecte d'information et analyse

JOUR 3

Présentation des règles NIDS / EDR
TP Mise en place de règles et détection d'attaque

Les HIDS / EDR
Centralisation des informations
Réaliser une timeline
Méthodologie d'analyse

TP : analyse d'une intrusion à partir d'une collecte d'informations , mise en place des bonnes pratiques d'analyse

JOUR 4

SIEM
Qu'est-ce qu'un SIEM
Les objectifs d'un SIEM
Les architectures de SIEM
Les outils SIEM

TD : Mise en place d'un SIEM & collecte des événements

Les règles SIEM
TP Mise en place de règles SIEM
Introduction à l'investigation avec SIEM

TD: Investigation avec SIEM

JOUR 5

Examen blanc : préparation examen final. Etude du processus de gestion des incidents de sécurité de l'information. Mise en place bonnes pratiques d'anaylse. Compréhension SOC et SIEM. Gestion d'Ioc.

Examen final : Qcm sur le processus de gestion des incidents de sécurité de l'information, sur les SIEM, SOC, sur les bonnes pratiques d'investigation, sur les outils
Collecte d'IOC selon environnement spécifique
Mise en situation globale de gestion d'un incident de sécurité de l'information

Démarche pédagogique :

Formation orientée sur la pratique
70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

Evaluation et validation :

EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES

Partie théorique et pratique
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.
Il peut se dérouler à distance.

Bureau Veritas Certification assure l'examen final de ce programme de formation.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'Europpean union agency for cybersecurity via l'European Cybersecurity Skills Framework