IMPLEMENTING CISCO CYBERSECURITY OPERATIONS

Ce cours permet aux apprenants de comprendre le fonctionnement d'un centre d'opérations de sécurité (SOC, Security Operations Center) et les compétences et connaissances d'introduction nécessaires dans cet environnement. Il se concentre sur les compétences de niveau d'introduction nécessaires pour un analyste SOC au niveau d'associé. Plus précisément, comprendre l'analyse de base des menaces, la corrélation d'événements, identifier les activités malveillantes et comment utiliser un manuel pour la réponse aux incidents.

CODE DE LA FORMATION:
CS-SC-SECOPS

ÉDITEUR OU CONSTRUCTEUR:
CISCO

VERSION:
V1.0

DURÉE:
5 JOURS

PRÉREQUIS:

Il est recommandé, mais non obligatoire, que les étudiants possèdent les connaissances et les compétences suivantes:

- Compétences et connaissances équivalentes à celles apprises dans la partie 1 (ICND1) des Périphériques de réseau Cisco interconnectés
- Connaissance pratique du système d'exploitation Windows
- Connaissance pratique des réseaux Cisco IOS et des concepts

OBJECTIFS:

À la fin de ce cours, vous serez capable de:

- Définir un SOC et les différents rôles dans un SOC
- Comprendre les outils et les systèmes d'infrastructure SOC
- Apprendre l'analyse d'incident de base pour un SOC centré sur les menaces
- Explorer les ressources disponibles pour aider à une enquête Expliquer la corrélation et la normalisation des événements de base
- Décrire les vecteurs d'attaque communs
- Apprendre comment identifier une activité malveillante
- Comprendre le concept d'un playbook
- Décrire et expliquer un manuel de réponse aux incidents
- Définir les types de métriques SOC
- Comprendre le système de gestion de flux de travail SOC et l'automatisation

CONTENU:

Module 1: Vue d'ensemble du SOC
Leçon 1: Définition du centre des opérations de sécurité
Leçon 2: Comprendre les outils et les données de NSM
Leçon 3: Comprendre l'analyse des incidents dans un SOC axé sur les menaces
Leçon 4: Identifier les ressources pour la chasse aux menaces cybernétiques
Module 2: Enquêtes sur les incidents de sécurité
Leçon 1: Comprendre la corrélation et la normalisation des événements
Leçon 2: Identifier les vecteurs d'attaque communs

Leçon 3: Identifier les activités malveillantes
Leçon 4: Identifier les schémas de comportements suspects
Leçon 5: Mener des enquêtes sur les incidents de sécurité
Module 3: Opérations SOC
Leçon 1: Décrire le PlayBook SOC
Leçon 2: Comprendre les paramètres SOC
Leçon 3: Comprendre le SOC WMS et l'automatisation
Leçon 4: Description du plan de réponse aux incidents
Leçon 5: Annexe A - Description de l'équipe d'intervention en cas d'incident de sécurité informatique
Leçon 6: Annexe B - Comprendre l'utilisation de VERIS