Formation Understanding Cisco Cybersecurity Operations Fundamentals

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour comprendre les dispositifs d'infrastructure de réseau, les opérations et les vulnérabilités de la suite de protocoles TCP/IP (Transmission Control Protocol/Internet Protocol). Les participants apprendront les concepts de sécurité, les opérations et les attaques courantes des applications réseau, les systèmes d'exploitation Windows et Linux, et les types de données utilisées pour enquêter sur les incidents de sécurité. A l'issue de la formation, ils disposeront des connaissances de base nécessaires pour exercer la fonction d'analyste en cybersécurité de niveau associé dans un centre d'opérations de sécurité centré sur les menaces, afin de renforcer le protocole réseau, de protéger vos appareils et d'accroître l'efficacité opérationnelle. La formation est une combinaison d'études dirigées par un instructeur et d'études à son propre rythme. Le contenu de l'auto-apprentissage sera fourni dans le cadre du didacticiel numérique que les participants recevront au début de la formation et devrait faire partie de votre préparation à l'examen.

Référence	CBROPS
Durée	5 jours (35h)
Tarif	4 090 €HT
Repas	100 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 2 au 6 septembre 2024
du 3 au 7 mars 2025

PARIS

du 2 au 6 septembre 2024
du 3 au 7 mars 2025

VOIR TOUTES LES DATES

Objectifs

| Expliquer le fonctionnement d'un SOC et décrire les différents types de services qui sont effectués du point de vue d'un analyste SOC de niveau 1.
| Expliquer les outils de surveillance de la sécurité du réseau (NSM) dont dispose l'analyste de la sécurité du réseau.
| Expliquer les données dont dispose l'analyste de la sécurité des réseaux.
| Décrire les concepts de base et les utilisations de la cryptographie.
| Décrire les failles de sécurité du protocole TCP/IP et la manière dont elles peuvent être utilisées pour attaquer les réseaux et les hôtes.
| Identifier les technologies courantes de sécurité des points d'extrémité.
| Identifier la chaîne d'exécution et les modèles de diamant pour les enquêtes sur les incidents, ainsi que l'utilisation de kits d'exploitation par les acteurs de la menace.
| Identifier les ressources pour la chasse aux cybermenaces.
| Expliquer la nécessité de la normalisation des données d'événements et de la corrélation des événements.
| Identifier les vecteurs d'attaque courants.

Public

| analyste de cybersécurité de niveau associé qui travaille dans des centres d'opérations de sécurité.

Prérequis

| Familiarité avec les réseaux Ethernet et TCP/IP
| Connaissance pratique des systèmes d'exploitation Windows et Linux
| Connaissance des concepts de base de la sécurité des réseaux

Programme de la formation

Définir le centre d'opérations de sécurité
Comprendre les outils de surveillance de l'infrastructure et de la sécurité du réseau

Explorer les catégories de types de données
Comprendre les concepts de base de la cryptographie
Comprendre les attaques TCP/IP courantes
Comprendre les technologies de sécurité des points finaux
Comprendre l'analyse des incidents dans un SOC centré sur les menaces
Identifier les ressources pour la chasse aux cybermenaces
Comprendre la corrélation et la normalisation des événements
Identifier les vecteurs d'attaque courants
Identifier les activités malveillantes
Identifier les schémas de comportement suspect
Mener des enquêtes sur les incidents de sécurité
Utilisation d'un modèle de carnet de route pour organiser la surveillance de la sécurité
Comprendre les mesures SOC
Comprendre le flux de travail et l'automatisation du SOC
Décrire la réponse aux incidents
Comprendre l'utilisation de VERIS
Comprendre les bases du système d'exploitation Windows
Comprendre les bases du système d'exploitation Linux
Ateliers
| Configurer l'environnement initial du laboratoire de collaboration
| Utiliser les outils NSM pour analyser les catégories de données
| Explorer les technologies cryptographiques
| Explorer les attaques TCP/IP
| Explorer la sécurité des points finaux
| Étudier la méthodologie des pirates
| Chasse au trafic malveillant
| Corréler les journaux d'événements, les PCAP et les alertes d'une attaque
| Enquêter sur les attaques par navigateur
| Analyser les activités DNS suspectes
| Explorer les données de sécurité à des fins d'analyse
| Enquêter sur les activités suspectes à l'aide de Security Onion
| Enquêter sur les menaces persistantes avancées
| Explorer les Playbooks SOC
| Explorer le système d'exploitation Windows
| Explorer le système d'exploitation Linux

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.