Formation Analyse inforensique Windows

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

Référence	SEC114
Durée	2 jours (14h)
Tarif	2 210 €HT

Objectifs

| Savoir réaliser une investigation numérique sur un ordinateur Windows
| Pouvoir utiliser les outils d'investigation
| Être capable de collecter et préserver l'intégrité des preuves

Public

| Administrateur / Ingénieur système et réseau
| Analyste SOC / Inforensique
| Personnes souhaitant se lancer dans l'inforensique

Prérequis

| Bonnes connaissances dans les systèmes Windows, en réseau et en cybersecurité

Pogramme de la formation

Introduction à Windows et à la cybersécurité
| OS Windows : les chiffres
| Les vulnérabilités Windows
| Les menaces les plus communes
| Inforensique numérique Windows
| La base de registre

Introduction à l'analyse inforensique
| Définition et terminologie
| Les objectifs du inforensique numérique
| Le processus d'investigation des incidents
| La chaîne de traçabilité

Analyse inforensique réseau
| Définition et terminologie
| Les types de collectes réseaux
| Les outils d'analyse réseau
| Wireshark dans un cadre d'investigation
| Analyse de flux réseaux malveillant

Analyse inforensique des traces
| Définition et terminologie
| La collecte des traces
| Les outils d'analyse des traces
| Les événements Windows
| Analyse d'événement suite à une activité malveillante

Analyse inforensique mémoire
| Définition et terminologie
| La collecte de la mémoire
| Les outils d'analyse mémoire
| Maitrise de volatility
| Analyse mémoire sur système

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 1er au 2 juillet 2024
du 28 au 29 octobre 2024

PARIS

du 1er au 2 juillet 2024
du 28 au 29 octobre 2024

VOIR TOUTES LES DATES

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

Analyse inforensique du système de fichiers
| Définition et terminologie
| Système de fichiers Windows
| La collecte du stockage de masse
| Les outils
| Analyse d'activité malveillante sur système Windows

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).
| 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.