Formation Analyse Forensic

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

Réaliser une analyse post-mortem (aussi appelée inforensic) d'incidents de sécurité informatique est devenue essentiel pour préserver des preuves. Suite à des simulations d'attaques, vous apprendrez à collecter et préserver les preuves, les analyser et améliorer la sécurité du SI après l'intrusion.

Référence	AFB
Durée	3 jours (21h)
Tarif	2 390 €HT
Repas	repas inclus

Objectifs

| Maîtriser les bons réflexes en cas d'intrusion sur une machine
| Collecter et préserver l'intégrité des preuves électroniques
| Analyser l'intrusion a posteriori

Public

| Ingénieur/administrateur systèmes et réseaux.

Prérequis

| Bonnes connaissances en sécurité informatique et en réseaux/systèmes.
| Avoir suivi le cours "Collecte et analyse des logs, optimiser la sécurité de votre SI".

Programme de la formation

Comment gérer un incident ?
| Les signes d'une intrusion réussie dans un SI.
| Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
| Comment réagir face à une intrusion réussie ?
| Quels serveurs sont concernés ?
| Savoir retrouver le point d'entrée et le combler.
| La boite à outils Unix/Windows pour la recherche des preuves.
| Nettoyage et remise en production des serveurs compromis.

Analyser les incidents pour mieux se protéger : L'analyse Forensic
| Informatique judiciaire : types de crimes informatiques, rôle de l'enquêteur informatique.
| La cybercriminalité moderne.
| La preuve numérique.

Analyse forensic d'un système d'exploitation Windows
| Acquisition, analyse et réponse.
| Compréhension des processus de démarrage.
| Collecter les données volatiles et non volatiles.
| Fonctionnement du système de mot de passe, du registre Windows.
| Analyse des données contenues dans la mémoire vive, des fichiers Windows.
| Analyse du cache, cookie et historique de navigation, historique des événements.
| Travaux pratiques : Injection d'un utilisateur. Casser le mot de passe. Collecter, analyser les données de la mémoire vive. Référencer, faire le hash de tous les fichiers. Explorer les données du navigateur, du registre.

Méthode pédagogique

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

- du 27 au 29 novembre 2024*
- du 17 au 19 février 2025
- du 28 au 30 avril 2025
- du 21 au 23 juillet 2025
- du 22 au 24 octobre 2025

PARIS

- du 20 au 22 novembre 2024*
- du 10 au 12 février 2025
- du 14 au 16 avril 2025
- du 7 au 9 juillet 2025

LYON

- du 17 au 19 février 2025
- du 28 au 30 avril 2025
- du 22 au 24 octobre 2025

VOIR TOUTES LES DATES

(*) session confirmée

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.