Formation Analyse inforensic et réponse à incidents de sécurité

Réaliser une analyse post-mortem d'incident de sécurité informatique

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

La probabilité qu'une entreprise soit victime d'une attaque augmente à mesure que les technologies évoluent. Face à ce risque croissant, les systèmes d'information peuvent subir des attaques sans que les responsables de leur sécurité ne les détectent dans l'instant et y apporte une parade. Dans le cas ou des dommages seraient constatés (vols de données par exemple), il existe une technique d'investigation post-incident : l'analyse forensic. Par l'analyse des dommages subits et des traces laissées par les attaquants, elle vise à établir la chronologie évènementielle pour reconstituer l'attaque et collecter des éléments exploitables en justice. Elle permet également d'identifier les actions d'ordre technique à mener pour neutraliser la menace.

Référence	SEC103
Durée	4 jours (28h)
Tarif	2 850 €HT

Objectifs

| Connaître les aspects juridiques de l'analyse forensic
| Savoir mener une analyse forensic
| Savoir reconstituer un incident de sécurité informatique en vue de l'expliquer
| Identifier les sources d'un incident pour mieux se défendre
| Savoir collecter des informations utiles pour établir un dossier avec des preuves

Public

| Consultant en sécurité informatique
| Administrateurs systèmes / réseaux

Prérequis

| Avoir suivi la formation Hacking et Sécurité - Niveau avancé ou disposer des compétences équivalentes

Programme de la formation

Aspects juridiques
| Bases légales de la sécurité de l'information
| Classification des crimes informatiques
| Rôle de l'enquêteur / de l'inforensique
| Acteurs technico-juridiques : CERT, agences nationales, gendarmerie...

Détecter l'incident
| Repérer les anomalies
| Revue des outils de détection d'incident
| Mise en oeuvre d'un IDS / IPS

Réagir suite à un incident
| Conserver les preuves
| Collecter les informations
| Revue des outils de collecte de l'information

Atelier - Analyse d'un système informatique piraté
| Mise en oeuvre d'un laboratoire dédié à la formation
| Analyse des anomalies

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 30 juin au 3 juillet 2025
du 15 au 18 septembre 2025

PARIS
du 30 juin au 3 juillet 2025
du 15 au 18 septembre 2025

AIX-EN-PROVENCE
du 15 au 18 septembre 2025
du 24 au 27 novembre 2025

BORDEAUX
du 30 juin au 3 juillet 2025
du 24 au 27 novembre 2025

GRENOBLE
du 30 juin au 3 juillet 2025
du 24 au 27 novembre 2025

LILLE
du 30 juin au 3 juillet 2025
du 15 au 18 septembre 2025

LYON
du 30 juin au 3 juillet 2025
du 24 au 27 novembre 2025

NANTES
du 30 juin au 3 juillet 2025
du 24 au 27 novembre 2025

VOIR TOUTES LES DATES

| Établir l'incident de sécurité
| Diagnostic technique et neutralisation de la menace
| Recherche de l'origine de l'attaque
| Contre-mesures

Méthode pédagogique

Le passage en revue des principales techniques d'analyse post-mortem. L'utilisation d'outils d'analyse poussés d'un système compromis. Une formation très pratique : l'essentiel de la formation portera sur des outils concrets que chacun peut employer dans son entreprise. L'apport de consultants experts en audits techniques des SI.

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.