Analyse inforensic et réponse à incidents de sécurité

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

Présentiel ou en classe à distance

4 jours (28 h)

Prix inter : 2.950,00 € HT
Forfait intra : 8.990,00 € HT

Réf.: SE103

Idéal en Distanciel

La probabilité qu'une organisation 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.

A qui s'adresse cette formation ?

Pour qui

- Consultant en sécurité informatique
- Administrateurs systèmes / réseaux

Prérequis

- Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" (SE101) ou disposer des compétences équivalentes
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - 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...

2 - Détecter l'incident

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

3 - Réagir suite à un incident

- Conserver les preuves
- Collecter les informations
- Revue des outils de collecte de l'information

4 - Atelier – Analyse d'un système informatique piraté

- Mise en oeuvre d'un laboratoire dédié à la formation
- Analyse des anomalies
- Établir l'incident de sécurité
- Diagnostic technique et neutralisation de la menace
- Recherche de l'origine de l'attaque
- Contre-mesures

Les objectifs de la formation

- 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
- Comprendre les sources d'un incident pour mieux se défendre
- Savoir collecter des informations utiles pour établir un dossier avec des preuves

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- 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 établissement.
- L'apport de consultants experts en audits techniques des SI.
- 86% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence SE103

Dernières places disponibles Session garantie

Rouen

du 16 févr. au 19 févr.	du 27 avr. au 30 avr.	du 19 oct. au 22 oct.

Toulouse

du 16 févr. au 19 févr.	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Paris

du 16 févr. au 19 févr.	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.
du 27 avr. au 30 avr.	du 19 oct. au 22 oct.	

Sophia Antipolis

du 16 févr. au 19 févr.	du 27 avr. au 30 avr.	du 19 oct. au 22 oct.

Bordeaux

du 16 févr. au 19 févr.	du 20 juil. au 23 juil.	du 19 oct. au 22 oct.

A distance

du 16 févr. au 19 févr.	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.
du 27 avr. au 30 avr.	du 19 oct. au 22 oct.	

Strasbourg

du 16 févr. au 19 févr.	du 27 avr. au 30 avr.	du 19 oct. au 22 oct.

Lyon

du 16 févr. au 19 févr.	du 20 juil. au 23 juil.	du 19 oct. au 22 oct.

Rennes

du 27 avr. au 30 avr.	du 19 oct. au 22 oct.	du 30 nov. au 3 déc.

Nantes

du 27 avr. au 30 avr.	du 19 oct. au 22 oct.	du 30 nov. au 3 déc.

Marseille

du 27 avr. au 30 avr.	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Lille

du 27 avr. au 30 avr.	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Aix-en-Provence

du 27 avr. au 30 avr.	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.