Analyse inforensique réseau

Mettre en oeuvre la détection et effectuer l'analyse à la suite d'un incident de sécurité informatique

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.290,00 € HT
Forfait intra : 6.250,00 € HT

Réf.: SE115

Idéal en Distanciel

Jusqu'à récemment, l'informatique était centrée sur le disque, la collecte d'un ordinateur et de plusieurs disques assurait la collecte de toutes les preuves numériques pertinentes. Aujourd'hui, cependant, l'informatique est devenue centrée sur le réseau et toutes analyse inforensique nécessite une analyse des données réseaux pour récupérer les preuves les plus pertinentes. Que ce soit pour la détection de l'incident ou l'analyse suite à l'incident pour comprendre ce qu'il s'est passé, l'analyse réseau est aujourd'hui un élément indispensable.

A qui s'adresse cette formation ?

Pour qui

- Ingénieur réseaux
- Administrateur réseaux

Prérequis

- Bonnes connaissances en sécurité informatique et en réseaux TCP/IP
- Connaissances de bases sur les commandes Linux
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction inforensique réseau

- Qu'est-ce que la inforensique ?
- Relation de l'analyse inforensique réseau avec les autres domaines de la inforensique numérique
- Collecte de preuves réseau
- Les NIDS/NIPS
- Quelques outils
- Utilisation de Wireshark

2 - Journalisation et surveillance

- Conditions à la mise en oeuvre d'une analyse inforensique du réseau
- Analyse de la chronologie
- Agrégation, corrélation et normalisation des données
- Collecte et stockage des données
- Principes juridiques de base
- Utilisation de Snort/Suricata

3 - Détection

- Distinguer le trafic régulier du trafic suspect/malveillant
- Détecter les intrusions
- Threat intelligence
- Mise en oeuvre d’une baseline et analyse

4 - Analyse / Interprétation des données

- Vue d’ensemble
- Chaîne de contrôle
- Analyses d’attaques

Les objectifs de la formation

- Connaître les conditions de mise en oeuvre d’une analyse inforensique réseau
- Être capable de réaliser une analyse inforensique réseau
- Comprendre comment distinguer le trafic régulier du trafic suspect/malveillant
- Savoir effectuer la collecte des preuves réseaux

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

- Cette formation alternant parties théoriques et ateliers pratiques permet aux participants d'acquérir les connaissances pour être capable de réaliser une analyse inforensique réseau.
- Des ateliers pratiques au plus proche de la réalité du terrain.
- L’apport de consultants experts en analyse inforensique réseau.

Dates et villes 2026 - Référence SE115

Dernières places disponibles Session garantie

Lille

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 5 oct. au 7 oct.

A distance

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.
du 18 mai au 20 mai	du 5 oct. au 7 oct.	

Paris

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.
du 18 mai au 20 mai	du 5 oct. au 7 oct.	

Marseille

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 5 oct. au 7 oct.

Rouen

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.

Sophia Antipolis

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.

Strasbourg

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.

Aix-en-Provence

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 5 oct. au 7 oct.

Toulouse

du 23 févr. au 25 févr.	du 20 juil. au 22 juil.	du 5 oct. au 7 oct.

Bordeaux

du 18 mai au 20 mai	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.

Lyon

du 18 mai au 20 mai	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.

Rennes

du 18 mai au 20 mai	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.

Nantes

du 18 mai au 20 mai	du 20 juil. au 22 juil.	du 21 déc. au 23 déc.