Analyse inforensique Windows

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

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.350,00 € HT
Forfait intra : 5.990,00 € HT

Réf.: SE114

Idéal en Distanciel

Après un incident de sécurité, il est indispensable d'analyser les systèmes et de détecter les traces laissées par l'attaque. Cette nécessité de recherche répond à 2 objectifs : d'une part car disposer de ces traces est nécessaire dans le cadre d'une démarche judiciaire et d'autre part parce qu'il est important de comprendre ce qui s'est réellement passé pour éviter que cela ne se renouvelle. Au regard de leur présence extrêmement fréquente pour ne pas dire quasi systématique dans les systèmes d'information, les systèmes Windows doivent faire l'objet de toutes les attentions. Savoir réaliser une analyse inforensique Windows est donc bien souvent une compétence indispensable pour toutes ceux qui exercent un métier lié à la réponse à incident.

A qui s'adresse cette formation ?

Pour qui

- 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
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - 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

2 - Introduction à l'analyse inforensique

- Définition et terminologie
- Les objectifs du inforensique numérique
- Le processus d'investigation des incidents
- La chaîne de traçabilité

3 - 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

4 - 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

5 - Analyse inforensique mémoire

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

6 - 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

Les objectifs de la formation

- 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

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'analyses 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 entité.
- L'apport de consultants experts en audits techniques des SI.
- 100% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence SE114

Dernières places disponibles Session garantie

A distance

du 9 févr. au 11 févr.	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.
du 11 mai au 13 mai	du 14 sept. au 16 sept.	

Toulouse

du 9 févr. au 11 févr.	du 15 juil. au 17 juil.	du 14 sept. au 16 sept.

Aix-en-Provence

du 9 févr. au 11 févr.	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Rennes

du 9 févr. au 11 févr.	du 11 mai au 13 mai	du 14 sept. au 16 sept.

Paris

du 9 févr. au 11 févr.	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.
du 11 mai au 13 mai	du 14 sept. au 16 sept.	

Lille

du 9 févr. au 11 févr.	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Nantes

du 9 févr. au 11 févr.	du 11 mai au 13 mai	du 14 sept. au 16 sept.

Marseille

du 9 févr. au 11 févr.	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Strasbourg

du 11 mai au 13 mai	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Sophia Antipolis

du 11 mai au 13 mai	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Rouen

du 11 mai au 13 mai	du 15 juil. au 17 juil.	du 30 nov. au 2 déc.

Lyon

du 11 mai au 13 mai	du 14 sept. au 16 sept.	du 30 nov. au 2 déc.

Bordeaux

du 11 mai au 13 mai	du 14 sept. au 16 sept.	du 30 nov. au 2 déc.