DOCAPOSTE Institute

Formation Analyse Forensic et réponse à incidents de sécurité

Présentation

Cette formation avancée vise à vous doter des compétences essentielles pour mener des analyses Forensic approfondies à la suite d'incidents de sécurité informatique. Grâce à des simulations pratiques, vous apprendrez à collecter, analyser et préserver les preuves numériques tout en renforçant la sécurité de votre système d'information.

Durée : 28,00 heures (4 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

À l'issue de la formation, les participants seront en mesure de :

- Réagir efficacement face à une intrusion informatique.
- Collecter et préserver l'intégrité des preuves électroniques.
- Analyser les intrusions après coup.
- Mettre en place des actions correctives pour améliorer la sécurité globale.

Prérequis

Une bonne connaissance des systèmes, réseaux et principes fondamentaux de la sécurité informatique est recommandée.

Public

Cette formation s'adresse aux ingénieurs, administrateurs systèmes et réseaux, ainsi qu'aux responsables de la sécurité souhaitant approfondir leurs connaissances en analyse forensic.

Programme de la formation

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

1/ Analyse forensic des systèmes

- Introduction à l'informatique judiciaire et aux crimes numériques.
- Rôle de l'enquêteur informatique.

2/Cybercriminalité moderne

- Types de cybercrimes.
- Cadre de gestion des incidents de sécurité.
- Analyse des attaques réseau et détection d'intrusions.
- Travaux pratiques : Analyse de logs réseau, mise en place de SNORT.

3/ Collecte d'informations

- Identification des événements de sécurité.
- Journaux système, SIEM (Security Information and Event Management).
- Travaux pratiques : Analyse des historiques utilisateur et des logs Web (ex. : injection SQL).

4/ Analyse de logs

- Tri et visualisation des traces avec Splunk.
- Travaux pratiques : Installation, configuration et analyse des logs avec Splunk.

5/ Gestion des preuves numériques

- Principes de la collecte et préservation des preuves.
- Travaux pratiques : Duplication de données, vérification d'intégrité, récupération de fichiers supprimés.

6/ Analyse forensic sous Windows

- Acquisition et analyse des données volatiles et non volatiles.
- Analyse des fichiers système, registre Windows, mémoire vive et historique de navigation.
- Travaux pratiques : Injection d'un utilisateur, récupération de mot de passe, analyse des données du registre et du cache.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Equilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulé de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France