DOCAPOSTE Institute

Formation Forensics réseaux

Présentation

Cette formation couvre la cybercriminalité moderne, la gestion des preuves numériques, l'analyse forensic des réseaux, l'audit et la sécurité, ainsi que la rédaction de rapports d'investigation forensic. Elle combine théorie et pratique pour une compréhension approfondie et appliquée.

Durée : 35,00 heures (5 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

- Réaliser des analyses forensics sur un réseau.
- Mettre en œuvre des méthodes d'investigation sur les réseaux filaires et sans fil.
- Appliquer une méthodologie de rédaction de rapports d'audit forensic après des tests d'intrusion.
- Identifier les traces laissées lors d'une intrusion sur un réseau informatique.

Prérequis

- Maîtrise des bases en sécurité informatique et en administration réseaux/systèmes.

Public

Cette formation s'adresse aux ingénieurs, administrateurs systèmes et réseaux, ainsi qu'aux responsables de la sécurité informatique.

Programme de la formation

1/ Cybercriminalité moderne

- Typologie des crimes informatiques.
- Gestion des incidents de sécurité et rôle du CERT.
- Mise en place d'un laboratoire d'investigation réseau.
- Analyse et compréhension des attaques réseau.
- Détection et protection contre les intrusions, cadre législatif français.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

- Travaux pratiques : Analyse de trafics liés à des attaques DDoS, infections malveillantes, et communications BotNet vers des serveurs C2.

2/ Preuve numérique

- Définition et typologie des preuves numériques.
- Évaluation et sécurisation des éléments électroniques d'une scène de crime.
- Collecte et préservation de l'intégrité des preuves.
- Travaux pratiques : Duplication bit à bit des données, vérification d'intégrité, capture de trafic réseau, et analyse des données numériques.

3/ Analyse forensic des réseaux

- Architecture des réseaux et vulnérabilités.
- Techniques d'investigation sur les réseaux filaires et sans fil.
- Analyse de captures de trames réseau.
- Identification de différents types d'attaques : ARP Storm, DHCP Starvation, ARP Spoofing, scans réseau, exfiltration de données...
- Travaux pratiques : Simulations d'attaques sur des réseaux filaires et sans fil, et investigation forensic des connexions détectées sur une scène de crime.

4/ Audit et sécurité

- Systèmes de détection et de prévention des intrusions (IDS/IPS).
- Étapes essentielles des tests d'intrusion.
- Supervision de la sécurité réseau.
- Travaux pratiques : Analyse des réseaux et détection d'intrusions avec des outils IDS/IPS tels que Snort.

5/ Rapports d'investigation forensic

- Importance des rapports d'investigation.
- Méthodologie de rédaction et modèles de rapports d'audit forensic.
- Travaux pratiques : Rédaction d'un rapport d'audit forensic complet à partir des investigations réalisées.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

DOCAPOSTE Institute

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 :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE - 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

- 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 - 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