DOCAPOSTE Institute

Formation Forensics Windows

Présentation

Cette formation en inforensique couvre les bases de l'investigation numérique, l'analyse de scénarios d'investigation, les investigations sur Internet, et l'inforensique Linux. Elle inclut des travaux pratiques pour une application concrète des concepts appris.

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

Objectifs de la formation

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

- Conduire une investigation numérique sur un poste Windows
- Analyser les intrusions rétrospectivement
- Collecter, préserver et garantir l'intégrité des preuves numériques

Prérequis

Maîtriser les bases essentielles en sécurité des systèmes d'information.

Public

Cette formation s'adresse à :

- Toute personne souhaitant débuter dans l'inforensique
- Administrateurs systèmes Windows
- Experts judiciaires en informatique

Programme de la formation

1/ Introduction à l'inforensique

- Délimitation du périmètre d'investigation
- Méthodologie "First Responder" et analyse post-mortem
- Systèmes de fichiers, horodatage et acquisition des données
- Collecte des données persistantes et volatiles

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

- Gestion des supports chiffrés et récupération de données supprimées
- Analyse des registres Windows et des journaux système (événements, antivirus, etc.)

Travaux pratiques :
- Acquisition et analyse de disques durs
- Recherche et restauration de données supprimées

2/ Étude de cas – Scénarios d'investigation
- Analyse de téléchargements et d'accès à des contenus sensibles
- Identification de traces d'exécution de programmes
- Analyse des journaux SMTP et des traces WiFi
- Exploration des données Exif des photos (géolocalisation)
- Détection d'exfiltration d'informations

Travaux pratiques :
- Analyse de fichiers supprimés et données non allouées

3/ Investigations sur Internet
- Analyse des artefacts d'Office 365 et SharePoint
- Traces sur Active Directory Windows
- Bases de l'analyse de la mémoire RAM
- Étude des navigateurs Internet (Chrome, Edge, Firefox)

Travaux pratiques :
- Analyse des historiques de navigation et artefacts liés

4/ Inforensique Linux
- Principes de l'inforensique sur postes de travail et serveurs Linux
- Analyse des journaux serveurs Web
- Construction et interprétation d'une frise chronologique du système de fichiers

5/ Synthèse et outils avancés
- Création d'une frise chronologique enrichie d'artefacts
- Introduction aux outils d'analyse de gros volumes de données

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

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 - 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 - 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