

Formation Forensics Windows

Présentation

Cette formation en infoforensique couvre les bases de l'investigation numérique, l'analyse de scénarios d'investigation, les investigations sur Internet, et l'infoforensique 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 débiter dans l'infoforensique
- Administrateurs systèmes Windows
- Experts judiciaires en informatique

Programme de la formation

1/ Introduction à l'infoforensique

- 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
- 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

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

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

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

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation (*évaluations en ligne dans l'extranet apprenant*)

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

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