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 - 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 - 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

- 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 à 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.

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

- 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.

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