DOCAPOSTE Institute

Formation Analyse Forensic

Présentation

Cette formation enseigne comment réagir efficacement à une intrusion, améliorer la sécurité grâce à l'Analyse Forensic, et analyser un système d'exploitation Windows. Elle combine théorie et travaux pratiques pour une compréhension approfondie et appliquée.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

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

- Appliquer les bonnes pratiques en cas d'intrusion sur un système.
- Collecter et garantir l'intégrité des preuves électroniques.
- Mener une analyse approfondie des intrusions après leur survenue.

Prérequis

Une solide maîtrise de la sécurité informatique et des réseaux/systèmes est requise.

Il est recommandé d'avoir suivi la formation sur la collecte et l'analyse des logs, ainsi que sur l'optimisation de la sécurité des systèmes d'information.

Public

Cette formation s'adresse aux ingénieurs et administrateurs systèmes et réseaux.

Programme de la formation

J1 : Réagir efficacement à une intrusion

- Identifier les signes d'une intrusion réussie dans un système d'information.
- Comprendre l'ampleur des actions menées par les attaquants.
- Réagir de manière appropriée en cas d'intrusion.
- Identifier les serveurs compromis et évaluer l'étendue de l'attaque.
- Localiser et combler le point d'entrée de l'intrusion.

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

- Utiliser les outils Unix/Windows pour rechercher et collecter les preuves.
- Procéder au nettoyage des systèmes affectés et à leur remise en production en toute sécurité.

J2 : L'analyse Forensic pour améliorer la sécurité

- Introduction à l'informatique judiciaire : différents types de crimes informatiques et rôle de l'enquêteur.
- Les enjeux de la cybercriminalité moderne.
- Comprendre la preuve numérique et son rôle dans l'analyse Forensic.

J3 : Analyse Forensic d'un système d'exploitation Windows

- Étapes d'acquisition, d'analyse et de réponse en cas d'incident.
- Comprendre les processus de démarrage d'un système Windows et leur impact sur l'analyse forensic.
- Collecter et analyser les données volatiles (RAM) et non volatiles (disques).
- Étudier le fonctionnement des mots de passe et du registre Windows.
- Analyser la mémoire vive, les fichiers systèmes Windows, ainsi que les caches, cookies et historiques de navigation.
- Examiner les événements enregistrés dans les journaux du système.

Travaux pratiques :

- Injection d'un utilisateur malveillant et cassage de mot de passe.
- Collecte et analyse des données volatiles issues de la mémoire vive.
- Référencement des fichiers et calcul du hash pour garantir leur intégrité.
- Exploration des données du navigateur, du registre Windows et des autres artefacts du système.

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.

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

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.
- 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

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 119411179 94 auprès du préfet de région d'Ile-de-France