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.

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

- Localiser et combler le point d'entrée de l'intrusion.
- 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

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

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.

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