ENQUÊTE POST-PIRATAGE

Apprendre à mener une enquête post piratage/cyberattaque afin d'en tirer les leçons et s'améliorer

PRÉSENTATION DE LA FORMATION

Cette formation approfondie vous permettra d'acquérir les compétences nécessaires pour analyser les traces laissées par les pirates, identifier les vulnérabilités de sécurité et mettre en œuvre des contre-mesures efficaces pour renforcer la sécurité de votre infrastructure informatique. En fin de formation, vous serez en mesure de produire un Plan de Reprise d'Activité pour votre organisation.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les techniques de piratage informatique
- Maîtriser les outils d'investigation numérique
- Appliquer les méthodes d'analyse post-incident
- Développer des stratégies de réponse efficaces

MOYENS & MÉTHODES

- Documents pédagogiques
- Cahier d'exercices pratiques
- Exercices pratiques en ligne
- Nécessite un ordinateur

PUBLIC & PRE-REQUIS

- Public concerné : personne en charge de la réalisation d'une enquête informatique
- Pré-requis : aucun

MODALITÉS D'ÉVALUATION

- Quiz & auto-évaluations
- Test fin de parcours
- Certificat de réalisation

TARIFS & NB DE PARTICIPANTS

- Participants : 2 à 10 maximum
- Tarif par personne : 2200 €

DÉLAIS & DURÉE

- En distanciel
- En présentiel (entreprise)
- Durée : 28 heures (4j)

Calendrier de sessions joint

CONTACT (inscriptions et handicap)

SCHOETTEL Audrey / audrey.schoettel@revisium.fr / 0 805 035 135

ENQUÊTE POST-PIRATAGE

Apprendre à mener une enquête post piratage/cyberattaque afin d'en tirer les leçons et s'améliorer

PROGRAMME DE LA FORMATION

Module 1 : Introduction

✓ Définition et concepts de base
✓ Importance de l'enquête post-piratage
✓ Les étapes de l'enquête
✓ Rôles et responsabilités de l'enquête
✓ Méthodologies et outils couramment utilisés
✓ Légalité et éthique durant l'enquête
✓ Etude de cas : enquête réussie
✓ Exercice pratique : simuler une première réponse à une intrusion

Module 2 : Préparation à l'enquête

✓ Collecte et préservation des preuves
✓ Analyse de la scène de crime numérique
✓ Identification des parties prenantes
✓ Création d'un plan d'enquête
✓ Gestion de la chaîne de custody
✓ Méthodes de collecte de données
✓ Étude de cas : Préparation à l'enquête
✓ Exercice pratique : Élaboration d'un plan d'enquête

Module 3 : Collecte, tri, et analyse des données

✓ Collecte et tri des données
✓ Analyse des journaux d'activité
✓ Analyse de la vulnérabilité exploitée
✓ Identification des vecteurs d'attaque
✓ Analyse de la chronologie des événements
✓ Utilisation d'outils d'analyse forensique
✓ Étude de cas : Analyse des données avec succès
✓ Exercice pratique : Analyse des journaux d'activité

ENQUÊTE POST-PIRATAGE

Apprendre à mener une enquête post piratage/cyberattaque afin d'en tirer les leçons et s'améliorer

PROGRAMME DE LA FORMATION

Module 4 : Attribution et identification des auteurs
- ✓ Techniques de détermination de l'origine de l'attaque
- ✓ Profilage des attaquants
- ✓ Analyse des indicateurs de compromission (IOC)
- ✓ Collaboration avec les forces de l'ordre
- ✓ Utilisation de l'intelligence de menace
- ✓ Réponse légale à l'identification des auteurs
- ✓ Étude de cas : Attribution réussie
- ✓ Exercice pratique : Analyse des IOC

Module 5 : Containment et éradication
- ✓ Stratégies de containment
- ✓ Isolation des systèmes compromis
- ✓ Éradication des malwares
- ✓ Patching des vulnérabilités
- ✓ Restauration des systèmes
- ✓ Réponse aux incidents en temps réel
- ✓ Étude de cas : Containment et éradication efficaces
- ✓ Exercice pratique : Isolation et éradication

Module 6 : Restauration et amélioration de la sécurité
- ✓ Plan de restauration des services
- ✓ Révision de la politique de sécurité
- ✓ Mise en place de correctifs de sécurité
- ✓ Formation et sensibilisation du personnel
- ✓ Surveillance continue
- ✓ Rapport final d'enquête`
- ✓ Étude de cas : Restauration et amélioration de la sécurité
- ✓ Exercice pratique : Plan de restauration des services

ENQUÊTE POST-PIRATAGE

Apprendre à mener une enquête post piratage/cyberattaque afin d'en tirer les leçons et s'améliorer

PROGRAMME DE LA FORMATION

Module 7 : Prévention des futurs incidents

- ✓ Analyse des leçons apprises
- ✓ Mise en place de contrôles de sécurité avancés`
- ✓ Surveillance continue des menaces`
- ✓ Tests de pénétration et audit de sécurité
- ✓ Sensibilisation à la sécurité
- ✓ Gestion des vulnérabilités
- ✓ Étude de cas : Prévention des futurs incidents réussie
- ✓ Exercice pratique : Plan de sensibilisation à la sécurité