Risk Manager – Méthode EBIOS

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Pilotage de la sécurité organisationnelle

Rubrique : Certifications ISO

Éligible au CPF : Oui
Code CPF : 36399

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Comprendre les concepts et les principes de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) Cartographier les risques Maîtriser les éléments de gestion des risques de base pour la sécurité de l'information en utilisant la méthode EBIOS Analyser et communiquer les résultats d'une étude EBIOS

Public visé

Consultants, responsables sécurité des SI, gestionnaires des risques, toute personne impliquée dans des activités d'appréciation des risques informatiques…

Pré-requis

Connaître le guide sécurité de l'ANSSI, avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes sur la sécurité des systèmes d'information.

PROGRAMME

Programme détaillé

Jour 1 matin

Chapitre 1

Objectifs et structure de cours
- Présentation du groupe
- Points généraux
- Objectifs et structure de la formation
- Approche pédagogique
- Évaluation des apprentissages

Chapitre 2

Introduction à la méthode EBIOS Risk Manager
- Fondamentaux de la gestion des risques
- Présentation d'EBIOS
- Zoom sur la cybersécurité (menaces prioritaires)
- Principales définitions EBIOS RM

Exercice 1 : Comprendre la terminologie
- Concept phare et atelier de la méthode EBIOS RM
- Récapitulatif

Chapitre 3

Atelier 1 «Cadrage et socle de sécurité»
- Présentation de l'atelier
- Définition du cadre de l'étude et du projet
- Identification du périmètre métier et technique
- Identification des évènements redoutés et évaluation de leur niveau de gravité

Code de formation : MG214

€ Tarifs

Prix public : 2380 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Campus : Ensemble des sites

Durée : 14 heures

Délai d'accès :
Jusqu'à 8 jours avant le début de la formation

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 12 / 12 / 2024
: Ensemble des sites
: Distanciel possible
: 14 heures
: 2 jours

• Détermination du socle de sécurité
Exercice 2 : Identifier les évènements redoutés
• Récapitulatif de l'atelier

Jour 1 après-midi

Chapitre 4

Atelier 2 «Sources de risques»
• Présentation de l'atelier
• Identification des sources de risques (SR) et de leurs
• Objectifs Visés (OV)
• Évaluation de la pertinence des couples
• Évaluation des couples SR/OV et sélection de ceux jugés prioritaires pour l'analyse
• Évaluation de la gravité des scénarios stratégiques
Exercice 3 : Évaluer les couples SR/OV • Récapitulatif de l'atelier

Jour 2 matin

Chapitre 5

Atelier 3 «Scénarios stratégiques»
• Présentation de l'atelier
• Évaluation du niveau de menace associé aux parties prenantes
• Construction d'une cartographie de menace numérique de l'écosystème et des parties prenantes critiques
Exercice 4 : Évaluer le niveau de menace associé aux parties prenantes
• Élaboration des scénarios stratégiques
Exercice 5 : Élaborer des scénarios stratégiques
• Définition des mesures de sécurité sur l'écosystème
• Récapitulatif de l'atelier

Jour 2 après-midi

Chapitre 6

Atelier 4 «Scénarios opérationnels»
• Présentation de l'atelier
• Élaboration des scénarios opérationnels
• Évaluation des vraisemblances
• Pour aller plus loin (Threat modeling, ATT&CK, CAPEC)
Exercice 6 : Créer un scénario opérationnel

Chapitre 7

Atelier 5 «Traitement du risque»
• Présentation de l'atelier
• Réalisation d'une synthèse des scénarios de risque
• Définition de la stratégie de traitement
• Définition des mesures de sécurité dans un plan d'amélioration continue de la sécurité (PACS)
• Évaluation et documentation des risques résiduels • Mise en place du cadre de suivi des risques
Exercice 7 : Créer un PACS (Plan d'amélioration continue de la sécurité)
• Conclusion

MODALITÉS

Modalités

Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.