Formation cybersécurité : Devenir EBIOS Risk Manager

Ref: PR-CYB-CD-EBIOSRM



Maîtriser les principes et les concepts fondamentaux de l’appréciation des risques et de la gestion optimale des risques liés à la sécurité de l’information selon la méthode EBIOS

DURÉE : **3 Jours** (21H)
Prix : **2 325,00 € HT**

PRÉSENTIEL
FORMATION QUALIFIANTE

Objectifs et compétences visés

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS RM.
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d’information appartenant à un organisme via la réalisation concrète d’une appréciation des risques via EBIOS RM.
- Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS.

À qui s'adresse la formation ?

Profils

- Responsables de la sécurité des systèmes d’information.
- Membres d’une équipe de sécurité des systèmes d’information.
- Tout individu responsable de la sécurité des systèmes d’information, de la conformité et du risque dans une organisation.
- Tout individu mettant en œuvre une analyse de risques ou impliqué dans un programme de gestion des risques.
- Consultants / professionnels en systèmes d’information.
- Délégués à la protection des données.

Prérequis

Aucun prérequis n'est nécessaire à cette formation.
Le suivi du MOOC de l'ANSSI et du Club EBIOS (https://lms.club-ebios.org/formations/ebiosrm) n'est pas un prérequis mais est fortement recommandé.

Contenu de la formation

Introduction à la méthode EBIOS

- Les fondamentaux de la gestion des risques
- Présentation d'EBIOS - Zoom sur la cybersécurité (menaces prioritaires)
- Principales définitions EBIOS RM

Atelier 1 - Cadrage et socle de sécurité

- 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
- Déterminer le socle de sécurité

Atelier 2 - Sources de risques

- Identifier les sources de risques et leurs objectifs visés
- Évaluer la pertinence des couples
- Évaluer les couples et sélectionner ceux jugés prioritaires pour l'analyse
- Relier les évènements redoutés aux couples

Atelier 3 - Scénarios stratégiques

- Évaluer le niveau de menace associé aux parties prenantes
- Construction d'une cartographie de menace numériques de l'écosystème et les parties prenantes critiques
- Élaboration des scénarios stratégiques
- Définition des mesures de sécurité sur l'écosystème

Atelier 4 - Scénarios opérationnels

- Élaboration des scénarios opérationnels
- Evaluation des vraisemblances
- Pour aller plus loin : Threath modeling, AAT&CK, CAPEC

Atelier 5 - Traitement du risque

- Réalisation d'une synthèse des scénarios de risque
- Définition de la stratégie de traitement
- Définir les mesures de sécurité dans un plan d'amélioration continue de la sécurité
- Évaluation et documentation des risques résiduels
- Mise en place du cadre de suivi des risques

Matinée de révisions

- Sujets libres
- Préparation à l’examen

Examen de certification PECB

Modalités de la formation

Modalités d'évaluation

Cette formation se conclut par un examen de certification PECB.

Nos plus

- Formation animée par un consultant CNPP certifié ISO/CEI 27005 Risk Manager et EBIOS Risk Manager.
- Disponible également en visioconférence

CNPP en quelques chiffres

21000
stagiaires / an


Des infrastructures pédagogiques uniques

+ de 500
diplômés / an

+ de 400
intervenants

98%
de stagiaires satisfaits en 2025

Besoin d'informations sur une formation en cybersécurité ?

Nous sommes à votre écoute pour échanger sur votre prochaine formation en cybersécurité.

Contactez-nous !

+33 (0)8 06 00 03 80