EBIOS Risk Manager

Ref: PR-CYB-CD-EBIOSRM

Maîtrisez 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 : **2 280,00 € 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.

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.

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.

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.

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.

Scénarios opérationnels

- Élaboration des scénarios opérationnels.
- Évaluation des vraisemblances.
- Pour aller plus loin : Threat modeling, ATT&CK, CAPEC).

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.

Révisions et examen de certification

Modalités

Modalités d'évaluation

Passage d'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.

En bref

21000
stagiaires / an

Des infrastructures pédagogiques uniques

+ de 500
diplômés / an

+ de 400
intervenants

Les prochaines sessions

Du 10/07/24 au 12/07/24	**Paris**	**2 280,00 € HT**
Du 02/10/24 au 04/10/24	**Paris**	**2 280,00 € HT**
Du 11/12/24 au 13/12/24	**Paris**	**2 280,00 € HT**

Nos formations complémentaires

Cybersécurité~Management de la sécurité de l'information
Devenir Lead Cybersecurity Manager ISO/CEI 27032
5 Jours
Présentiel
Mettre en œuvre et manager un programme de cybersécurité basé sur la norme ISO/CEI 27032.

Cybersécurité~Management de la sécurité de l'information
Fondamentaux de la directive NIS 2
1 Jour
Présentiel
Découvrir les concepts fondamentaux de la directive NIS 2

Cybersécurité~Forensic et sécurité opérationnelle
Lead Forensic Examiner
5 Jours
Présentiel
Maîtrisez les concepts et outils d’analyses forensiques dans un contexte judiciaire, ainsi que dans un contexte d’entreprise

Besoin d'informations sur une formation en cybersécurité ?

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

Contactez-nous !

(+33)1 75 43 51 01