



Formation Risk Manager - Méthode EBIOS

EBIOS RM, préparation à la certification

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

La méthode EBIOS permet d'apprécier et de traiter les risques relatifs à la sécurité des SI en se fondant sur une expérience éprouvée en matière de conseil SI et d'assistance MOA. A l'issue de la formation, l'apprenant sera capable de manager les risques relatifs à la sécurité de l'information en se fondant sur les principes et usages de la méthode EBIOS.

Objectifs

- | Comprendre les concepts et les principes d'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

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

Prérequis

| 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 de la formation

La méthode EBIOS risk manager

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

Cadrage et socle de sécurité

- | Identification du périmètre métier et technique.
- | Identification des événements redoutés et évaluation de leurs niveaux de gravité.
- | Déterminer le socle de sécurité.
- | Travaux pratiques : Identifier les événements redoutés.

Sources de risques

- | Identifier les sources de risques (SR) et leurs objectifs visés (OV).
- | Évaluer la pertinence des couples.
- | Évaluer les couples SR/OV et sélectionner ceux jugés prioritaires pour l'analyse.
- | Évaluer la gravité des scénarios stratégiques.
- | Travaux pratiques : Identifier les sources de risques (SR) et leurs objectifs visés (OV). Évaluer les couples SR/OV.

Scénarios stratégiques

- | Évaluer le niveau de menace associé aux parties prenantes.

Référence	EBU
Durée	2 jours (14h)
Tarif	1 570 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 2 au 3 décembre 2024*

PARIS

du 25 au 26 novembre 2024*

AIX-EN-PROVENCE

du 2 au 3 décembre 2024

BORDEAUX

du 2 au 3 décembre 2024

LILLE

du 2 au 3 décembre 2024

LYON

du 2 au 3 décembre 2024

NANTES

du 2 au 3 décembre 2024

SOPHIA-ANTIPOLIS

du 2 au 3 décembre 2024

STRASBOURG

du 2 au 3 décembre 2024

[VOIR TOUTES LES DATES](#)

(*) session confirmée

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

Scénarios opérationnels

- | Élaboration des scénarios opérationnels.
- | Évaluation des vraisemblances.
- | Threat modeling, ATT&CK.
- | Common Attack Pattern Enumeration and Classification (CAPEC).
- | Travaux pratiques : Élaboration des scénarios opérationnels. Évaluation des vraisemblances.

Traitement du risque

- | Réalisation d'une synthèse des scénarios de risque.
- | Définition de la stratégie de traitement.
- | Définir les mesures de sécurité dans un PACS.
- | Évaluation et documentation des risques résiduels.
- | Mise en place du cadre de suivi des risques.
- | Travaux pratiques : Définir les mesures de sécurité dans un Plan d'Amélioration Continue de la Sécurité (PACS). Mise en place du cadre de suivi des risques.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

- | Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
- | Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
- | Privilégier une connexion filaire plutôt que le Wifi.
- | Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
- | Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
- | Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
- | Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
- | Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
- | Horaires identiques au présentiel.

Accessibilité



Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.