Formation : Risk Manager - Méthode EBIOS

EBIOS RM, préparation à la certification

Cours pratique - 2j - 14h00 - Réf. EBU

Prix : 1630 € H.T.

4,2 / 5

BEST | ActionCo | Clé en main

Formation éligible au financement Mobilités

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 pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- 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 concerné

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.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Certification

Ce cours associé au cours EBX (EBIOS RM, examen de certification), la journée de passage d'examen, permet de préparer et passer la certification PECB certified EBIOS risk manager.

PARTICIPANTS

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.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Le support et l'animation sont en français.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 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.

2 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.

3 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.

4 Scénarios stratégiques

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

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 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.

6 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.

Parcours certifiants associés

Pour aller plus loin et renforcer votre employabilité, découvrez les parcours certifiants qui contiennent cette formation :

- Parcours certifiant Manager la cybersécurité des systèmes, applications et bases de données - Réf. ZCN

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.
Découvrez-les sur notre page Comment financer sa formation ou contactez votre conseiller formation.

Financement par les OPCO

- Adhérents Mobilités, découvrez les avantages négociés par votre OPCO en cliquant ici

Horaires

Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.
Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts.
Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

Dates et lieux

CLASSE À DISTANCE
2026 : 18 mai, 8 juin, 8 juin, 7 sep., 7 sep., 12 oct., 2 nov., 7 déc., 7 déc.

PARIS LA DÉFENSE
2026 : 18 mai, 8 juin, 7 sep., 12 oct., 2 nov., 7 déc.

LYON
2026 : 18 mai, 7 sep., 7 déc.

AIX-EN-PROVENCE
2026 : 18 mai, 7 sep.

BORDEAUX
2026 : 18 mai, 7 sep.

LILLE
2026 : 18 mai, 7 sep.

NANTES
2026 : 18 mai, 7 sep., 7 déc.

STRASBOURG
2026 : 18 mai, 7 sep.

TOULOUSE
2026 : 18 mai, 7 sep.