

Programme de formation

EBIOS Risk Manager 2018 (EBIOS RM, approfondi)

But de la formation

Comprendre les principes de l'analyse de risques en sécurité de l'information selon EBIOS RM ainsi que les différents concepts qui permettent de l'appliquer :

- Valeurs métier, biens support, critères, impact, vraisemblance, gravité...
- Réaliser les différents exercices portant sur les cinq ateliers, basés sur des cas réels,
- Avoir la capacité de réaliser une analyse de risques sur un cas d'étude lui-même basé sur un cas réel,
- Réaliser l'analyse, proposer et justifier une solution lors d'une soutenance finale.

Pré-requis

- Connaissances générales en systèmes d'information et la sécurité associée.

Type de public

- Personne souhaitant maîtriser la démarche EBIOS
- Personne devant réaliser une appréciation des risques en sécurité, y compris au-delà des risques en sécurité informatique,
- RSSI,
- DPO,
- Chefs de projet SI,
- Consultants en sécurité, ainsi qu'à ceux connaissant d'autres méthodes comme ISO27005, MEHARI.

Moyens pédagogiques

- Support de cours formateur (diaporama),
- Livret d'exercices et correction,
- Description du cas d'étude,
- Outil d'application de la méthode,
- Guides méthodologiques de l'ANSSI (à télécharger sur le site de l'ANSSI).

Sanction de la formation

- QCM pour estimer l'acquisition des connaissances,
- Formulaire d'évaluation de la formation soumis aux élèves,
- Certification G-echo.

G-echo

6 Avenue de la Gare - C24

31380 Garidech

+33.6.03.62.14.40

contact@g-echo.fr



Méthodes pédagogiques

- Cours magistral pour la présentation,
- Vérification des acquis par exercices corrigés,
- Cas pratique par groupes de 5 élèves. Soutenance devant l'ensemble de la promotion.

Cette formation est délivrée par Mr José-Patrick Boé, ancien officier mécanicien de l'armée de l'air diplômé de l'École de l'Air. Après avoir obtenu un diplôme d'ingénieur en informatique de l'ENSEEIH il intègre au début des années 1990 le Service Central de la Sécurité des Systèmes d'Information (SCSSI) devenu plus tard l'Agence Nationale de la Sécurité de l'Information (ANSSI). Il pilote la mise au point des premières versions de la méthode EBIOS et à ce titre en donne les premières formations. Après dix ans il quitte l'administration pour rejoindre le service sécurité d'un groupe du CAC 40 où il est en charge de la protection de l'information. Devenu consultant, 13 ans plus tard, il élargit son expérience de la sécurité de l'information dans les domaines les plus variés.

Cette formation à la méthode EBIOS RM lui donne l'opportunité de partager avec les participants les acquis de son riche parcours.

Durée

21 heures (3 jours).

Déroulement

Cette formation se déroule en trois phases permettant d'appréhender la méthode de manière progressive :

- Phase 1 : Introduction et présentation de EBIOS RM,
- Phase 2 : Explication détaillée illustrée par l'exemple du guide de l'ANSSI (Société de biotechnologie),
- Phase 3 : Phase 3 : Exercices, basés sur des cas réels, à l'issue de chaque atelier,
- Phase 4 : Mise en œuvre dans un cas d'étude.

Après une introduction (présentation des participants et rappel des objectifs) la méthode est présentée en totalité afin de donner une vue d'ensemble des cinq ateliers. L'objectif est de faire comprendre la finalité et d'avoir la vision du déroulement de la méthode. Il s'agit de la phase 1.

L'exposé de la méthode est ensuite repris à son début. Le déroulement de chaque atelier est approfondi et illustré par l'exemple du guide et d'autres exemples réels. Il s'agit de la phase 2.

A l'issue de chaque atelier un exercice pratique est proposé à chaque élève. Il dispose pour cela d'un "livret stagiaire" dont tous les exercices sont systématiquement tirés d'un contexte réel. La diversité de ces cas illustre les différentes possibilités d'application de la méthode (de la PME au site SEVESO en passant par le navire de croisières). Il s'agit de la phase 3.

La dernière journée est consacrée à la conduite de la méthode pour un cas d'étude. Cet exercice rajoute, à l'objectif du maintien de la cohérence tout au long de l'étude, celui d'un travail de groupe et d'une soutenance devant un public. On se rapproche davantage de la réalité du terrain en montrant que l'application d'une méthode ne se résume pas à un exercice intellectuel. Il s'agit de la phase 4.

À l'issue de la formation un livret "corrigé" du livret stagiaire, une proposition pour le cas d'étude et la totalité de la présentation sont remis aux élèves.

1ère journée

Préambule

Objectif : accueillir les élèves et s'accorder sur le déroulement de la formation

- Accueil et présentations réciproques
- Objectifs pédagogiques
- Déroulement

La spécification de la sécurité

Objectif : Faire un bref historique de la méthode EBIOS et positionner l'analyse de risque pour rédiger un cahier des charges.

- Les exigences de sécurité
- L'expression du besoin par la maîtrise d'ouvrage
- La Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS)
- Les objectifs de sécurité

L'analyse de risques

Objectif : Exposer les fondamentaux de l'analyse de risques

- Principe de l'analyse de risques
- La norme ISO 27005
- Principes EBIOS : valeurs métiers / biens supports

Qu'est-ce que la méthode EBIOS Risk Manager ?

Objectif : Exposer dans sa totalité le déroulement de la méthode pour donner une vision d'ensemble.

- Ce que permet EBIOS RM
- L'approche d'EBIOS RM
- Atelier 1 : Cadrage et socle de sécurité
- Atelier 2 : Sources de risque
- Atelier 3 : Scénarios stratégiques
- Atelier 4 : Scénarios opérationnels
- Atelier 5 : Traitement du risque

Atelier 1 : Cadrage et socle de sécurité

Objectif : Expliquer de manière détaillée le déroulement de l'atelier 1 en s'appuyant sur l'exemple du guide et s'assurer de la bonne compréhension par un exercice.

- Objectifs, participants, données de sortie
- Définir le cadre de l'étude
- Définir le périmètre métier et technique
- La cotation de la gravité
- Identifier les événements redoutés
- Déterminer le socle de sécurité
- Faire un bilan de conformité
- Exercice atelier 1

Atelier 2 : Sources de risque

Objectif : Expliquer de manière détaillée le déroulement de l'atelier 2 en s'appuyant sur l'exemple du guide et s'assurer de la bonne compréhension par un exercice.

- Objectifs, participants, données de sortie
- Identifier les sources de risque et les objectifs visés

- Créer les couples sources de risque et objectifs visés (SR/OV)
- Évaluer et sélectionner les couples SR/OV
- Établir la cartographie des sources de risque
- Exercice atelier 2

2ème journée

Atelier 3 : Scénarios stratégiques

Objectif : Expliquer de manière détaillée le déroulement de l'atelier 3 en s'appuyant sur l'exemple du guide et s'assurer de la bonne compréhension par un exercice.

- Objectifs, participants, données de sortie
- Construire la cartographie de menace de l'écosystème
- Sélectionner les parties prenantes critiques
- Élaborer les scénarios stratégiques
- Définir les mesures de sécurité de l'écosystème
- Exercice atelier 3

Atelier 4 : Scénarios opérationnels

Objectif : Expliquer de manière détaillée le déroulement de l'atelier 4 en s'appuyant sur l'exemple du guide et s'assurer de la bonne compréhension par un exercice.

- Objectifs, participants, données de sortie
- Élaborer les scénarios opérationnels
- Les méthodes d'évaluation de la vraisemblance
- Exercice atelier 4

Atelier 5 : Traitement du risque

Objectif : Expliquer de manière détaillée le déroulement de l'atelier 5 en s'appuyant sur l'exemple du guide et s'assurer de la bonne compréhension par un exercice.

- Objectifs, participants, données de sortie
- Réaliser une synthèse des scénarios de risque
- Décider de la stratégie de traitement du risque
- Définir et structurer les mesures de sécurité
- Planifier la mise en œuvre des mesures de sécurité
- Évaluer et documenter les risques résiduels
- Mettre en place le cadre de suivi des risques
- Exercice atelier 5

3ème journée

L'étude de cas

Objectif : Les élèves ont la capacité de réaliser par groupes une étude de cas, basée sur un cas réel, permettant de mettre en œuvre tous les ateliers de la méthode.

- Présentation du contexte du cas d'étude
- Travail par groupes supervisés par le formateur
- Soutenance de chacun des groupes

Bilan

Objectif : Faire, avec les élèves, un bilan partagé sur la formation

- Échanges sur les points forts et axes d'amélioration
- Rédaction des fiches d'appréciation