

Préparation à la certification EBIOS Risk Manager



Formation incluse dans



70 vidéos



300 slides



20h

NEW !

Introduction

Avec l'explosion des menaces numériques et l'essor des réglementations en matière de cybersécurité, les organisations doivent aujourd'hui démontrer qu'elles sont capables d'identifier, d'évaluer et de traiter efficacement les risques qui pèsent sur leurs systèmes d'information.

Dans ce contexte, la méthode EBIOS Risk Manager, élaborée par l'ANSSI, s'impose comme une approche incontournable pour construire une analyse de risque à la fois stratégique et opérationnelle, alignée sur les enjeux métiers, les menaces actuelles et les obligations réglementaires.

Bien plus qu'un simple exercice de conformité, EBIOS RM permet de piloter la sécurité de manière dynamique, en tenant compte de l'évolution des attaques, des vulnérabilités et des contextes d'usage.

Cette formation vise un double objectif :

- vous permettre de maîtriser la méthode EBIOS RM et ses cinq ateliers de manière concrète et opérationnelle,
- vous préparer efficacement à l'obtention de la certification EBIOS Risk Manager, une certification aujourd'hui très recherchée en France, notamment dans les secteurs sensibles ou réglementés.

Formateur

Boris Motylewski est ingénieur de formation et expert judiciaire en cybercriminalité à la cour d'appel de Montpellier. Il a fondé et dirigé la société ExperLAN, SSII spécialisée dans la sécurité des SI (rachetée par Thalès) puis la société Axiliance, éditeur du pare-feu Web RealSentry (rachetée par Beeware). Il a cofondé la société Securiview, spécialisée dans la détection et remédiation des incidents de sécurité (rachetée par Linkbynet en janvier 2018). Il dirige aujourd'hui la société VeriSafe spécialisée dans la Cybersécurité. Conférencier depuis 1995, Boris Motylewski a formé à ce jour plus de 10 000 professionnels de l'IT (RSSI, DSI, experts cybersécurité, chefs de projet, ingénieurs, auditeurs, consultants, enquêteurs de police judiciaire, DPO, etc...).



A qui s'adresse cette formation ?

Cette formation s'adresse à toute personne souhaitant acquérir une maîtrise approfondie de la gestion des risques numériques selon la méthode EBIOS RM, en lien avec les bonnes pratiques actuelles de cybersécurité.

Elle est particulièrement adaptée aux professionnels ayant déjà une culture informatique et souhaitant évoluer vers des fonctions liées à la cybersécurité, à la conformité, à la gestion des risques ou à la gouvernance.

Elle concerne absolument tous les acteurs impliqués dans la transformation numérique : directions métiers, RSSI, DSI, chefs de projet, juristes IT, consultants, prestataires, mais aussi futurs auditeurs ou analystes sécurité.

Enfin, cette formation est idéale pour celles et ceux qui souhaitent valoriser leur profil avec une certification EBIOS Risk Manager, désormais très prisée dans les appels d'offres publics, les grands comptes et les secteurs sensibles (santé, énergie, défense, finance...).

Prérequis

Aucune connaissance particulière n'est nécessaire pour suivre cette formation.

Objectifs pédagogiques

À l'issue de cette formation, les participants seront capables de :

- Acquérir les compétences nécessaires à la mise en œuvre de la méthode EBIOS RM pour conduire une analyse de risque complète
- Se préparer efficacement à la certification EBIOS Risk Manager, de plus en plus demandée dans les secteurs publics et privés, en particulier pour les fonctions de RSSI, de consultant sécurité ou de chef de projet cyber

Méthodes pédagogiques

Présentation magistrale avec analyse technique et déclinaison opérationnelle de tous les points identifiés dans le programme, exercices d'application et illustrations concrètes avec exemples réels.

Cette formation exclusivement disponible en e-learning est structurée en 7 modules avec pour chaque module :

- Introduction / objectifs
- Contenu pédagogique (le contenu et la durée de chaque module sont détaillés dans le programme de la formation)
- QCM de 10 questions pour valider le module
- Podcast du résumé du module
- Conclusion / synthèse

Accompagnement pédagogique

Le formateur est accessible par email pendant toute la durée de la formation. Le formateur s'engage à répondre aux questions des participants sous 48 heures du lundi au vendredi hors vacances scolaires et jours fériés. Toute question posée est ensuite publiée dans le forum thématique de la formation avec la réponse du formateur. Tous les participants peuvent ensuite contribuer au fil de discussion afin d'enrichir ou de compléter la réponse.

Durée

Cette formation est réalisée en sessions de formation ouverte à distance (FOAD) également appelé e-learning ou distanciel. La durée totale de la formation est de 20 heures (70 sessions vidéos).

Démonstrations

Des extraits vidéos de cette formation sont disponibles à l'adresse : <https://www.verisafe.fr/demo>



Évaluation des acquis & certification

Chaque participant peut s'auto-évaluer en fin de formation via un examen blanc avec une étude de cas et un QCM (60 questions) portant sur l'ensemble du programme de la formation. Un certificat VERISAFE attestant les compétences acquises est délivré à toute personne ayant obtenu un taux de bonnes réponses supérieur ou égal à 70%.



Suivi de la formation & attestation

Une attestation de suivi est délivrée à chaque participant ayant effectué le QCM d'évaluation des acquis (60 questions). Pour accéder au QCM d'évaluation, les participants doivent avoir suivi tous les modules de la formation.

Accès à la plate-forme e-learning & assistance technique

Après validation de son inscription, chaque participant reçoit par e-mail ses identifiants d'accès à la plate-forme e-learning ainsi qu'un guide d'utilisation en format électronique (PDF). Un support technique par e-mail puis par visio-conférence est accessible aux participants pour tout problème concernant la plate-forme e-learning et son fonctionnement.

Modalités et délais d'accès

Merci de consulter les informations disponibles sur notre site : <https://www.verisafe.fr/modalites-inscription-delai-acces>

Accessibilité aux personnes en situation de handicap

Merci de consulter les informations disponibles sur notre site : <https://www.verisafe.fr/accessibilite-psh>

Note concernant l'examen de certification EBIOS RM

L'examen de certification EBIOS RM s'effectue directement en ligne.

Il consiste à répondre à 60 questions et à réaliser une étude de cas.

La certification EBIOS RM est délivrée par un organisme accrédité par le Club EBIOS.



Préparation à la certification EBIOS RM

➤ La méthode d'analyse de risque numéro 1 en France proposée par l'ANSSI

Introduction à EBIOS RM

Présentation de la formation EBIOS RM

- Sommaire & déroulement de la formation
- Obtenir la certification EBIOS RM

La notion de risque en sécurité de l'information

- Qu'est-ce qu'une analyse de risque ?
- La sécurité par une approche « risque »
- La sécurité par une approche « conformité »
- Les principales méthodes d'analyse de risque
- EBIOS RM vs ISO 27005

Présentation de la méthode EBIOS Risk Manager

- Historique d'EBIOS Risk Manager
- Documents de référence de l'ANSSI et du Club EBIOS
- Vocabulaire EBIOS RM
- Qu'est-ce que EBIOS RM ?
- Tour d'horizon des 5 ateliers de la méthode

Podcast Introduction à EBIOS RM

QCM Introduction à EBIOS RM

Atelier 1 : Cadrage et socle de sécurité

Présentation de l'atelier

- Objectifs, participants et livrables
- Déroulement l'atelier

Définir le cadre de l'étude

- Définir le cadre et clarifier les responsabilités
Cycle stratégique et cycle opérationnel

Délimiter le périmètre métier et technique

- Périmètre métier et technique
- Mission / Valeur Métier (VM) / Bien support (BS)
- Exercice d'application

Identifier les événements redoutés (ER)

- Comprendre les événements redoutés
- Évaluer la gravité
- Construire une échelle adaptée
- Exercice d'application

Déterminer le socle de sécurité

- Socle de sécurité : définition et rôle
- Construire un socle de sécurité solide
- Identifier les écarts et évaluer la conformité
- Étude de cas et exercice d'application
- Synthèse de l'atelier

A1-06 - Podcast Atelier 1

A1-07 - QCM Atelier 1

Atelier 2 : Sources de risque

Présentation de l'atelier

- Objectifs, participants et livrables
- Déroulement de l'atelier

Identifier les Sources de Risque (SR) et les Objectifs Visés (OV)

- Comprendre la mécanique des couples SR/OV
- Typologie des attaquants : profils et objectifs visés

Sélectionner les couples SR-OV pertinents

- Évaluer la pertinence des couples SR/OV
- Exemple d'application
- Confronter les résultats avec ceux de l'atelier 1
- Exemples et exercices pratiques

Podcast Atelier 2

QCM Atelier 2

Atelier 3 : Scénarios stratégiques

Présentation de l'atelier

- Objectifs, participants et livrables
- Déroulement de l'atelier
- Vocabulaire de l'atelier

Élaboration des scénarios stratégiques

- Cartographie de la menace sur l'écosystème
- Evaluation de la menace associée aux parties prenantes
- Exemple et exercice d'application
- Construction des scénarios stratégiques
- Définir des mesures de sécurité sur l'écosystème
- Synthèse de l'atelier

Podcast Atelier 3

QCM Atelier 3

Atelier 4 : Scénarios opérationnels

Présentation de l'atelier

- Objectifs, participants et livrables
- Déroulement de l'atelier

Les scénarios opérationnels

- Élaboration des scénarios opérationnels
- Description des modes opératoires
- Evaluer la vraisemblance d'un scénario
- Kill chain, MITRE ATT&CK, CAPEC et NTCTF

Podcast Atelier 4

QCM Atelier 4

A5 - Atelier 5 - Traitement du risque

Présentation de l'atelier

- Objectifs, participants et livrables
- Déroulement de l'atelier
- Vocabulaire de l'atelier

Traitement des risques identifiés

- Réaliser une synthèse des scénarios
- Décider de la stratégie de traitement du risque
- Définir les mesures de sécurité
- Appliquer le plan de traitement du risque
- Evaluer et documenter les risques résiduels
- Mettre en place un cadre de suivi des risques
- Synthèse de l'atelier

Podcast Atelier 5

QCM Atelier 5

Examen blanc EBIOS RM

QCM (60 questions)

Etude de cas SAMBOT (Service d'IA en mode SaaS)