Formation Ebios Risk Manager

Ref. ***EBIOS-RM-06***
Durée : 3.0 jour(s) / 21.0 heures

Les menaces sur nos systèmes d'information sont réelles et omniprésentes. Il est essentiel voire vital de comprendre des risques qui pèsent sur notre environnement digital et de pouvoir alors adopter une position en adéquation avec les besoins et la vision de l'entreprise.
EBIOS RM permet d'aborder l'analyse des risques de façon méthodique et en adéquation avec les normes internationnales en vigueurs.

Cette certification permet de valider la maitrise des savoirs indispensables pour mener à bien une analyse des risques. Elle valide un ensemble de savoirs requis pour les fiches métiers de l'ANSSI suivantes : Auditeur de sécurité organisationelle, consultant en cybersécurité, RSSI, Formateur en cybersécurité, Chef sécurité de projet.

Pré-requis :

Connaissance du fonctionnement managérial d'une organisation et connaissance de base en analyse de risque

Personnes concernées :

DSI
RSSI
Risk manager
Chef de projet sécurité
Consultant Sécurité

ECSF METIERS ASSOCIE :
Cyber information Security officer, Cyber security risk manager, Cyber security auditor

Objectifs :

Décrire les concepts de bases liés à la gestion des risques.
Appliquer la méthodologie EBIOS RM
Evaluer le contexte d'une organisation souhaitant mettre en œuvre une analyse des risques.
Organiser des ateliers liés d'analyse de risque.
Sélectionner es typologies de menaces et des vulnérabilités associées.
Evaluer les principaux concepts de gouvernance et ses principaux enjeux et implication en matière de sécurité de l'information.
Elaborer une analyse des risques avec EBIOS RM et son suivi associé.

Programme :

JOUR 1

Les fondamentaux du management du risque
Actifs, Menaces et Vulnérabilités
La gravité du risque
La vraisemblance du risque
Niveau de risque
Scénario de risque
ISO 31000
ISO 27005
Présentation d'EBIOS RM
Atelier 1 : Cadrage et Socle de sécurité
Usages d'EBIOS RM
Valeur métier
Processus Informations
Biens supports
Propriétaire d'actifs
Evénement redouté
Echelle de gravité
Socle de sécurité
Etude de cas
Atelier 2 : Sources de risque
Panorama des attaques récentes
Sources de risques
Objectifs visés
Pertinence d'une source de risque
Etude de cas

JOUR 2

Atelier 3 : Scénarios Stratégiques
Parties prenantes
Niveau de menace
Dépendance
Pénétration
Maturité cyber
Confiance
Cartographie de l'écosystème
Scénarios stratégiques
Etude de cas
Atelier 4 : Scénarios Opérationnels
Scénario Opérationnel
Mode Opératoire :Connaitre, Rentrer, Trouver, Exploiter
Action Elémentaire
Etude du site Mitre Attack
Vraisemblance
Méthode Express
Méthode Standard
Méthode Avancée
Etude de cas

JOUR 3

Atelier 5 : Traitement du risque
Stratégie de traitement du risque
Evaluation des risques
PACS
Synthèse des risques résiduels
Cadre du suivi des risques
Etude de cas

Démarche pédagogique :

Formation orientée sur la pratique

70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

Evaluation et validation :

EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES
Partie théorique et pratique
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties :

- 20 questions de QCM sur la compréhension de la méthodologie EBIOS RM
- Une mise en situation du candidat sur la mise en œuvre d'une analyse de risque avec la méthodologie EBIOS-RM à partir d'une étude de cas fourni au début de l'examen.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'European union agency for cybersecurity via l'European Cybersecurity Skills Framework