Gouvernance, risque et conformité

EBIOS RM Piloter la cybersécurité par la maîtrise du risque numérique

Vous allez apprendre à

Dans un monde où le numérique est devenu le socle de toutes les activités économiques, la maîtrise des risques cyber n'est plus un luxe, mais une nécessité stratégique.

Aujourd'hui, les cyberattaques ne sont plus le fruit de pirates isolés : elles sont organisées, ciblées, furtives et souvent destructrices. Rançongiciels, espionnage industriel, compromission de fournisseurs, détournement de messagerie professionnelle... le quotidien des organisations, même modestes, est exposé à des attaques de plus en plus sophistiquées.

Face à cela, les directions, les responsables sécurité, les chefs de projets et les référents cyber doivent être capables de comprendre les menaces, d'en mesurer l'impact réel, et d'y répondre avec méthode, rigueur et lucidité.

C'est l'objectif de cette formation : vous fournir les compétences et les outils pour identifier, analyser, prioriser et traiter les risques numériques, en vous appuyant sur la méthode EBIOS Risk Manager développée et recommandée par l'ANSSI.

Public visé

- Risk Managers / Responsables SSI
- RSSI / DSI / MOA / Directeurs projets
- Consultants en sécurité des SI
- Auditeurs SI & SMSI/ homologateurs SSI
- Responsables conformité (NIS2, RGPD, ISO 27001)
- Chefs de projets numériques

Les objectifs de la formation

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

- Mettre en œuvre la méthode EBIOS Risk Manager sur un cas réel ou simulé
- Comprendre les concepts fondamentaux : risque, menace, vulnérabilité, gravité
- Identifier les biens supports, objectifs visés et sources de risque
- Élaborer des scénarios stratégiques et opérationnels, orientés sur les menaces
- Choisir et planifier des mesures de traitement des risques
- Consolider une démarche complète de management des risques SSI
- Accompagner une organisation vers une cybersécurité raisonnée, pilotée et documentée

Les prérequis de la formation

- Connaissances générales en sécurité des systèmes d'information
- Familiarité avec les SI, les notions de gouvernance ou d'audit
- Appétence pour les démarches méthodologiques & collaboratives

Programme de la formation

Jour 1 : Fondamentaux & Atelier 1 : Cadrage et socle

- Introduction & Attentes
- Le risque, gravité, niveau de risque (ISO 27005)
- Vue globale de la méthode EBIOS RM (5 ateliers + étude de cas)
- **Atelier 1 :**
  - Identification des biens supports / valeurs métier
  - Définition des événements redoutés
  - Socle de sécurité (référentiels existants, mesures techniques & organisationnelles)
  - Exercice : cas pratique + tableau d'analyse du socle

Jour 2 : Ateliers 2 à 4 : Menaces & scénarios

- **Atelier 2 :**
  - Définition des couples SR/OV
  - Classification, cartographie
  - Exercice : SR/OV sur cas secteur santé
- **Atelier 3 :**
  - Cartographie des parties prenantes
  - Construction des scénarios stratégiques
  - Exercice : attaque via prestataire externe
- **Atelier 4 :**
  - Transformation en scénarios techniques
  - Notions de MITRE ATT&CK, TTP
  - Évaluation de vraisemblance
  - Démonstration : mapping d'une attaque avec MITRE

Jour 3 : Atelier 5 & Étude de cas finale

- **Atelier 5 :**
  - Choix des mesures (ISO 27001, ANSSI, guides sectoriels)
  - Acceptation ou transfert du risque
  - Suivi du plan d'action
  - Exercice : classification + fiche de traitement
- **Étude de cas finale :**
  - Rejeu complet des 5 ateliers sur cas industriel
  - Soutenance par groupes (oral + livrable)
  - Retour critique collectif