Gestion des risques et EBIOS RM

Évaluer les risques SSI selon des démarches reconnues et conformes aux cadres réglementaires

DESCRIPTION

Pilier de toute stratégie de cybersécurité, l'analyse de risques SSI permet d'anticiper les menaces, de prioriser les mesures de protection et de garantir une maîtrise durable des enjeux métier, réglementaires et opérationnels.

Cette formation permet de comprendre, structurer et mettre en œuvre une démarche d'analyse des risques SSI, en s'appuyant sur les principaux référentiels réglementaires et normatifs. Elle vise à développer la capacité à identifier, analyser et évaluer les risques, tout en interprétant les exigences réglementaires applicables à un contexte donné.

À travers une approche progressive, les participants acquièrent les fondamentaux nécessaires, puis sont amenés à mobiliser des méthodes d'analyse de risques SSI adaptées, à formaliser leurs résultats et à appréhender les risques portants sur les dispositifs visés. Une initiation à la méthode EBIOS Risk Manager (EBIOS RM) vient compléter ce parcours, permettant de découvrir une approche structurée et reconnue pour conduire une analyse de risques SSI.

OBJECTIFS PEDAGOGIQUES

- Expliquer les enjeux, les concepts et les points clés d'une démarche d'analyse des risques liés à la sécurité des systèmes d'information
- Appliquer et documenter un processus d'analyse et de gestion des risques du SI, en intégrant les exigences réglementaire applicables (ex. NIS2, RGPD)
- Expliquer la méthode Ebios Risk Manager pour conduire une analyse de risques adaptée à un contexte donné

PUBLIC CIBLE

- Tout collaborateur souhaitant comprendre les enjeux de la gestion des risques liés à la sécurité du système d'information
- Collaborateurs IT, sécurité des systèmes d'information (SSI) et fonctions techniques, impliqués dans la mise en œuvre ou le maintien de la sécurité du SI
- Manager et responsable métier

PRE-REQUIS

Stage pratique
Sécurité

Code :
ANRCO

Durée :
3 jour(s) (21,00 heures)

Exposés : **40 %**
Cas pratiques : **40 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 2 500,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

- Connaissances de base IT recommandées

METHODE PEDAGOGIQUE
Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION
L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

Jour 1

FONDAMENTAUX ET CADRE DE L'ANALYSE DE RISQUES

Introduction aux notions de risque, analyse de risques SSI et cadre réglementaire

Intégration de l’analyse de risque dans une démarche de certification/homologation

Poser le contexte de gestion des risques

- Définir le périmètre, les objectifs et les critères d’évaluation du risque pour un cas d’usage (organisation, SI, actifs critiques)

Identifier les sources d'exigences réglementaires applicables (ex. obligations NIS/NIS2, PSSI-E), et les lier aux objectifs de sécurité.

Réaliser l'inventaire des actifs et des menaces :

- Cartographier les actifs (données, applications, infrastructures, processus) et leurs propriétaires pour les besoins de l'analyse.
- Qualifier menaces, vulnérabilités et scénarios pertinents, en s'appuyant sur des échelles qualitatives/quantitatives.

Identifier et évaluer les risques

Apprécier la vraisemblance et les conséquences de scénarios d'incident et calculer/estimer les niveaux de risque selon les critères établis

Documenter les hypothèses, données et résultats pour assurer traçabilité et auditabilité

Jour 2

TRAITEMENT DES RISQUES, CONFORMITÉ & GOUVERNANCE

Évaluation et priorisation des risques SSI

- Classer les risques (seuils, heatmaps) et prioriser les scénarios pour décision (réduction, transfert, acceptation), en intégrant les contraintes réglementaires et de gouvernance

Plan de traitement des risques et preuves de conformité

- Concevoir un plan de traitement de risques : mesures de sécurité (préventives/détectives/correctives), indicateurs, responsables, délais, preuves attendues (politiques, procédures, enregistrements)
- Aligner les décisions (acceptation/exceptions) avec la gouvernance sécurité et le processus de gestion des dérogations (ex. workflow eGRC/Archer, approbations)

Communication, suivi et amélioration continue

- Structurer la communication vers les parties prenantes (métier, RSSI, audit, conformité) et organiser la revue périodique des risques et du plan de traitement
- Définir les indicateurs d'efficacité (réduction d'exposition, suivi de la remédiation) et les mécanismes de contrôle pour l'amélioration continue
- Organisation du suivi, Rôles & Responsabilités incluant les modalités

Jour 3

INITIATION À LA MÉTHODOLOGIE D'ANALYSE DE RISQUE EBIOS RM

Introduction à la méthode EBIOS Risk Manager (RM)

Présentation générale d'EBIOS Risk Manager : Origine et philosophie de cette méthode

Principes clés : approches orientées menaces, scenarios stratégiques et opérationnels, prise en compte des sources de menace

Cycle global et livrables

Rôles impliqués dans la démarche (métiers, SSI, direction, experts)

Vue d'ensemble des 5 ateliers :

- Atelier 1 - Cadrage et socle de sécurité
- Atelier 2 - Sources de menace
- Atelier 3 - Scénarios stratégiques
- Atelier 4 - Scénarios opérationnels
- Atelier 5 - Traitement du risque

Focus sur les livrables

Étude de cas fil rouge : mise en pratique de la démarche Ebios RM

- Travail en sous-groupes sur un cas simple
- Présentation du contexte
- Application guidée :
  - Identification des biens essentiels
  - Choix d'une source de menace
  - Construction d'un scénario stratégique
  - Esquisse d'un scénario opérationnel
- Restitution et échanges

Facteurs clés de succès et erreurs courantes : animation des ateliers et Implication des parties prenantes, Choix du bon niveau de détail adapté aux enjeux…

Conclusions

- Synthèse des messages clés
- Quand et comment initier une démarche EBIOS RM ?
- Articulation avec :
  - Le SMSI
  - Les audits SSI
  - Les projets IT / Cloud
- Session de questions - réponses

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com