MY TRUST PARTNER

Cybersecurite - Conformite - IA

EBIOS Risk Manager : methodologie et mise en oeuvre

Les 5 ateliers, livrables type et exemples concrets

LIVRE BLANC MTP 2026

www.mytrustpartner.fr - contact@mytrustpartner.fr - +33 1 84 16 05 27

Sommaire

1. EBIOS RM : une methode francaise de reference

Origine et raison d'etre

EBIOS (Expression des Besoins et Identification des Objectifs de Securite) est la methode francaise de gestion des risques cyber, developpee et maintenue par l'ANSSI. La version Risk Manager (RM) publiee en 2018 modernise l'approche en l'alignant sur ISO 27005 et en integrant la notion de scenarios d'attaque issus de la threat intelligence.

Quand l'utiliser ?

Pour toute analyse de risques cyber structuree : projet SI sensible, certification ISO 27001 ou HDS, conformite NIS2, homologation RGS, fusion-acquisition. EBIOS RM est aussi pertinent pour une PME structuree que pour un operateur d'importance vitale.

Les livrables types

Analyse des risques documentee, cartographie des scenarios d'attaque, plan de traitement priorise, reste de risque assume. Ces livrables sont attendus par les auditeurs (ISO 27001, controle ANSSI) et par les assureurs cyber.

2. Atelier 1 - Cadrage et socle de securite

Objectif

Definir le perimetre de l'analyse : systemes, processus metiers, parties prenantes, reglementations applicables, enjeux business. Identifier les elements critiques : valeurs metier (ce qui a de la valeur pour l'organisation), biens supports (ce qui materialise les valeurs metier).

Le socle de securite

Inventaire des mesures de securite deja en place (controles existants). Point de depart pour evaluer le delta entre le niveau actuel et le niveau cible. Exemples : ISO 27001, politique de securite, EDR, MFA, sauvegardes.

Livrables de l'atelier

Note de cadrage (1 a 3 pages), cartographie des valeurs metier et biens supports, synthese du socle de securite existant. Duree typique : 1 a 2 jours d'atelier avec DSI, RSSI, metiers.

3. Atelier 2 - Sources de risque et objectifs vises

Identifier les attaquants

Typologie des sources de risque : cybercriminels (motivation financiere), activistes (motivation ideologique), concurrents (espionnage), services etatiques, initie malveillant, initie imprudent. Chacune avec son niveau de motivation, ses capacites, ses ressources.

Les objectifs vises

Ce que cherche l'attaquant : gain financier (rancon, fraude), espionnage (propriete intellectuelle, donnees clients), deni de service (sabotage), atteinte a la reputation. Cartographier les combinaisons sources x objectifs les plus pertinentes.

Livrables

Liste des sources de risque retenues, justification de la selection (vraisemblance, impact potentiel), matrice sources x objectifs. Duree : 0,5 a 1 jour.

4. Atelier 3 - Scenarios strategiques

Les chemins d'attaque

Pour chaque couple source x objectif, decrire les chemins d'attaque possibles a haut niveau : quel bien support est vise en premier, comment l'attaquant progresse vers la valeur metier. Utilisation d'une representation arbre d'attaque.

Gravite et vraisemblance

Gravite : impact business si le scenario se realise (financier, image, juridique, vies humaines). Vraisemblance : probabilite intrinseque d'occurrence, compte tenu du socle de securite. Echelles qualitatives 1 a 4.

Scenarios retenus

Les scenarios dont le couple gravite x vraisemblance depasse un seuil (defini par le comite de pilotage) passent a l'atelier suivant. Typiquement 5 a 15 scenarios pour une entreprise de taille moyenne.

5. Atelier 4 - Scenarios operationnels

Descente au niveau technique

Pour chaque scenario strategique retenu, decrire les etapes techniques concretes : reconnaissance, intrusion initiale, mouvement lateral, escalade de privileges, persistance, exfiltration, chiffrement. Reference a la matrice MITRE ATT&CK.;

Exemple concret : ransomware sur AD

Etape 1 : phishing cible RH avec macro Office. Etape 2 : execution du loader, deploiement de Cobalt Strike. Etape 3 : decouverte AD (BloodHound). Etape 4 : exploitation d'un compte privilegie oublie. Etape 5 : propagation via PsExec. Etape 6 : chiffrement masse des serveurs de fichiers.

Evaluation detaillee

Reevaluation de la vraisemblance au regard des mesures techniques concretes. Certaines etapes peuvent etre bloquees (EDR, MFA), d'autres passent. La vraisemblance globale depend du maillon le plus faible.

6. Atelier 5 - Traitement et reste de risque

Les 4 strategies de traitement

Eviter (supprimer l'activite a risque), reduire (mettre en place des mesures), transferer (assurance cyber, externalisation), accepter (formaliser la decision de ne rien faire). Chaque scenario doit avoir une strategie.

Plan d'action

Liste des mesures de securite a deployer, chiffrage, priorisation (par ratio benefice/cout), calendrier. Distinction court terme (quick wins) vs moyen/long terme (investissements structurants).

Reste de risque

Une fois les mesures deployees, il reste un risque residuel qui doit etre formellement accepte par la direction. Documenter cette acceptation (comite de pilotage, comite de risque, conseil d'administration selon criticite).

Revue periodique

EBIOS RM n'est pas un one-shot. Revue annuelle minimum, ou a chaque changement majeur (nouveau SI, acquisition, evolution de la menace). Reintegrer les retours d'experience incidents.

7. Mise en oeuvre avec MTP

Notre methodologie

My Trust Partner dirige vos analyses EBIOS RM de bout en bout : animation des 5 ateliers, redaction des livrables, presentation en comite de pilotage. Nos consultants sont certifies EBIOS RM par le Club EBIOS. Duree typique : 4 a 8 semaines selon perimetre.

Livrables finaux

Rapport d'analyse des risques (50 a 100 pages), cartographie dynamique des scenarios, plan de traitement chiffre, note de synthese direction (3 pages), support de presentation. Formats compatibles ISO 27001, NIS2, RGS.

Contact

Diagnostic gratuit sur demande. contact@mytrustpartner.fr, 01 84 16 05 27, www.mytrustpartner.fr. Formations EBIOS RM labellisees SecNumEdu-FC disponibles sur formation.mytrustpartner.fr

My Trust Partner

Cybersecurite - Conformite - IA

Labellise SecNumEdu-FC par l'ANSSI sur l'ensemble de notre catalogue formation.

Contact

www.mytrustpartner.fr
contact@mytrustpartner.fr
+33 1 84 16 05 27