CLUBEBIOS

EBIOS RISK MANAGER

Comment exploiter les non-conformités du socle de sécurité dans une analyse EBIOS RM ?

Date	:	20/03/2026
Statut	:	Validé
Classification	:	Public
Nombre de pages	:	9
Responsable des travaux	:	Ian GRISPAN
Validation	:	Collège des praticiens
Approbation	:	Conseil d'administration
Licence	:	

Ce document a été réalisé par le Club EBIOS

Club EBIOS, 11 rue de Lourmel, 75015 PARIS

Responsable(s) des travaux :

- Ian GRISPAN

Contributeur(s) :

- Thomas FITOUSSI
- Damien AUVRAY
- Nicolas VAN CAUTER
- Mohammed HEBBAR

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
1.0	Version initiale	Collège des praticiens	Validé

Sommaire

1. Objet de la fiche

Cette fiche propose une démarche structurée pour transformer les non-conformités du socle de sécurité en informations utiles à l'analyse de risque dans EBIOS RM.

La non-conformité n'est pas un simple « écart à combler », mais un fait générateur susceptible d'influer sur les chemins d'attaque (atelier 3), sur les modes opératoires (atelier 4), et/ou d'alimenter le plan de traitement (atelier 5).

2. Définitions

RISQUE (Guide EBIOS RM v1.5) **:** Possibilité qu'un événement redouté survienne et que ses effets impactent les missions de l'objet de l'étude. Dans le contexte cyber où s'inscrit EBIOS Risk Manager, un risque est décrit sous la forme d'un scénario de risque.

Scénario de risque (INTENTIONNEL) (Guide EBIOS RM v1.5) : Scénario complet, allant de la source de risque à l'objectif visé par elle, décrivant un chemin d'attaque et le scénario opérationnel associé. NOTE : dans le cadre de ce guide, on considère uniquement les scénarios de risque numérique de nature intentionnelle. ***Pour les risques non intentionnel, voir fiche méthode du collège des praticiens : Comment traiter les risques non intentionnel.***

Socle de sécurité (Guide EBIOS RM v1.5) : C'est l'expression de mesures :

- permettant de traiter les risques non délibérés ou non ciblés (souvent s'appuyant sur des référentiels standards) ;
- qui ne nécessitent pas d'être justifiées par une approche par scénario (ateliers 3 et 4). En particulier, des mesures provenant de référentiels ou de législation dont l'application est obligatoire et sans interprétation.

Les mesures du socle de sécurité font partie intégrante du plan de traitement du risque, au même titre que les autres mesures issues des ateliers 3, 4 et 5.

Non conformité : écart avéré à une exigence du socle. Elle peut concerner des composants techniques, des processus, des données, ou des parties prenantes externes (prestataires, SaaS/IaaS/PaaS, partenaires, filiales) par des engagements contractuels. L'analyse de ces écarts peut provenir de résultats d'audit ou d'analyse d'écarts précédents.

Exploitabilité : capacité, pour une source de risque, de convertir l'écart en opportunité dans un chemin d'attaque (atelier 3) puis en mode opératoire concret (atelier 4).

Action Élémentaire : Action unitaire exécutée par une source de risque sur un bien support dans le cadre d'un scénario opérationnel.

Mesure de sécurité (Guide EBIOS RM v1.5) : Moyen de traiter un risque prenant la forme de solutions ou d'exigences pouvant être inscrites dans un contrat.

Vulnérabilité : Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

3. Intégration dans EBIOS RM

Atelier 1 — Cadrage & socle. Il convient de qualifier les écarts au socle de sécurité selon qu'ils relèvent de l'hygiène essentielle ou d'exigences normatives, réglementaires ou contractuelles applicables. Il peut être intéressant pour les écarts portant directement sur des biens supports, de les transcrire sous forme de vulnérabilités applicables à ces bien supports et de les capitaliser dans un catalogue des vulnérabilités[1] du système étudié.

Atelier 3 — Scénarios stratégiques. Les non conformités pertinentes et exploitables dans le scénario stratégique sont analysées afin de déterminer si elles peuvent être utilisées comme vecteur d'attaque, notamment via l'écosystème de parties prenantes.

Atelier 4 — Scénarios opérationnels. Les non conformités (transposées en vulnérabilités applicables aux biens supports, cf. catalogue des vulnérabilités) retenues issues du socle de sécurité peuvent alimenter les modes opératoires de l'atelier 4 sous forme d'actions élémentaires.

Atelier 5 — Traitement. Les mesures issues des différents ateliers sont intégrées au plan de traitement des risques :

- **mesures de l'atelier 1 qui traitent d'un écart du socle associées à un scénario de risque.**
- **mesures ad hoc de l'atelier 2 liées au contexte d'emploi et de menace,**
- **mesures de l'atelier 3 sur les parties prenantes**;
- **mesures de l'atelier 4 sur les actions élémentaires** ;

4. Démarche opératoire en 4 étapes

1) Identifier les non-conformités du socle de sécurité lors de l'atelier 1. Faire une liste des écarts non conformes au socle de sécurité.

2) pendant l'atelier 3. Analyser les écarts de cette liste lors de l'atelier 3 pour déterminer si l'un d'entre eux peut être exploité dans le cadre de chemins d'attaque. L'objectif est d'identifier et qualifier tout nouveau chemin plausible et son effet du fait de cette non conformité / vulnérabilité.

Pour ce faire il est important de lier les justifications des niveaux de dangerosité ou des chemins d'attaque retenus pour ces non-conformités.

3) Pendant l'atelier 4. Analyser les écarts de cette liste lors de l'atelier 4 pour déterminer si l'un d'entre eux permet d'identifier des modes opératoires supplémentaires concrets : enchaînements d'actions permettant à la source de

[1] Point d'attention : le catalogue des vulnérabilités du système est de fait le document le plus sensible du système et doit être protégé en conséquence. (Voir Conclusion)

risque d'atteindre son objectif visé. Une étape préalable qui peut faciliter cela est de transcrire les non-conformités applicables à des biens supports en tant que vulnérabilités contextualisées à ces biens supports, dans un "catalogue des vulnérabilités" du système.

4) Pendant l'atelier 5 : Consolider le traitement des non-conformités. Lier chaque mesure du Plan de Traitement des Risques à un scénario de risque. Le Plan de Traitement des Risques peut contenir des mesures qui couvrent un ou plusieurs risques. Lors de la consolidation des non conformité dans le PTR, il peut être utile de pouvoir identifier l'origine des mesures de sécurité : non-conformités du socle de sécurité, vulnérabilités issues de résultats d'audit, mesures "additionnelles" sur des actions élémentaires (cf. atelier 4).

5. Risques de dérive

Le risque de dérive observé dans la prise en compte des résultats de l'étude du socle de sécurité est la création d'un effet tunnel de conformité.

Tunnel de conformité. La tentation de transformer mécaniquement et directement les écarts de conformité en risques peut occulter la réflexion liée à une approche par scénarios.

- **On s'écarte de la définition du risque selon EBIOS RM.** En EBIOS RM, un risque est formé par un scénario complet : il relie une source de risque à un objectif visé, en explicitant un chemin d'attaque (atelier 3) et un scénario opérationnel (atelier 4). Une non-conformité décrite isolément (ex. « pas d'authentification forte) n'est pas un risque : elle ne dit rien de qui pourrait nous attaquer, quel serait son objectif, comment il réalise son objectif et en quoi cela impacterait nos valeurs métiers, tous ces éléments sont traités au travers des ateliers 2 et 3.
- **Limitation de la faisabilité (atelier 4).** Sans scénario opérationnel, il est impossible de vérifier l'exploitabilité amont (l'attaquant peut-il se mettre en position d'exploiter l'écart ?) et aval (peut-il, après exploitation, atteindre son objectif — exfiltrer, altérer, interrompre ?). L'atelier 4 sert précisément à éprouver ces hypothèses afin de déterminer si ces scénarios sont 'réalisables'.

Afin d'éviter cet effet de **tunnel de conformité**, il est important de **ne pas inscrire tel quel les non-conformités du socle comme « risques »** dans la synthèse des risques de l'atelier 5 car cela contourne le principe d'approche par scénario.

6. Points d'attention

Focus sur les écarts au socle de sécurité :

NOTE : *En substance il est a priori toujours possible d'associer / illustrer une non-conformité au socle par/dans un scénario de risque. Mais il n'est à prendre en considération que si ce scénario est pertinent dans l'étude et le contexte du système étudié.*

Il faut avoir en tête qu'intrinsèquement toutes les exigences qu'il contient proviennent d'un scénario de risque qui a déjà été formalisé quelque part, par le passé … et souvent de multiples fois !

D'où l'intérêt du socle de sécurité en se disant que si l'on retrouve systématiquement un ensemble de scénarios dont le moyen de les couvrir se fait toujours avec les mêmes mesures de sécurité (typiquement le cas des scénarios basiques), il sera toujours moins coûteux d'annoncer directement la mise en oeuvre systématique de ces mesures (i.e. le "socle de sécurité") et de vérifier ensuite qu'il est suffisamment (et correctement) mis en oeuvre, plutôt que de réinventer la roue systématiquement (cf. le changement de paradigme entre EBIOS RM et les versions précédentes d'EBIOS).

Si l'on veut le détail de ces scénarios basiques, les travaux du BSI allemand et plus précisément leur IT-Grundschutz-Kompendium, proposent un croisement plutôt exhaustif (et régulièrement mis à jour) entre chaque mesure de sécurité et chaque menace élémentaire…

IT-Grundschutz-Kompendium est consultable sur le site du BSI Allemand, ici : https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

7. Conclusion

Par défaut, toutes mesures jugées pertinentes issues des différents ateliers associées à un scénario de risque doivent être inscrites dans le Plan de Traitement des Risques. Si aucun scénario de risque n'est retenu concernant une mesure de sécurité issue d'un écart au socle de sécurité (inexploitabilité démontrée, contrôles compensatoires robustes), celle-ci ne devrait pas être inscrite dans le PTR.

NOTE : *Le plan de traitement des risques est le document qui regroupe les mesures permettant de traiter les risques, son objectif est de pouvoir prioriser ces mesures par rapport au niveau des risques les plus importants qu'elles couvrent.*

En effet, mettre les mesures non liées à un risque dans le PTR permet d'avoir toutes les mesures dans un seul et même document, cependant cela vous expose aux limites suivantes :

- Les mesures n'étant pas liées à un risque, il sera difficile d'atteindre l'objectif et l'utilité du PTR, à savoir, prioriser l'application des mesures en fonction du niveau de risque qu'elles couvrent.
- Il sera également plus difficile de justifier l'application de ces mesures auprès d'une autorité hormis l'application du concept de défense en profondeur.