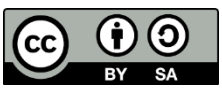
Démarche « Flash » guide d'utilisation

[Titre]

Date	:	6 octobre 2021
Statut	:	Version finale
Classification	:	Publique
Nombre de pages	:	18
Réalisation		Document réalisé par le club EBIOS
Responsable des travaux	:	FRAUSTO Paul - MICHELIN
Contributeurs		BOE José-Patrick CORBEL Pierre - Niji OLIVE Jean – CGI PAUL Stéphane – Thales
Validation	:	Groupe de travail
Approbation	:	Conseil d'administration
Licence	:	

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
14/01/2020	Création initiale	FRAUSTO Paul	Document de travail
12/04/2021	Restructuration du document	OLIVE Jean	Document de travail
20/04/2021	Proposition	BOÉ José-Patrick	Document de travail
03/05/2020	Contenu ajouté	FRAUSTO Paul	Document de travail
09/06/2021	Validation des commentaires et amendements, création de la RC	FRAUSTO Paul	Release candidate
17/06/2021	Validation des commentaires et amendements à la version (RC) soumise aux contributeurs du groupe de travail, création de la RC 2	FRAUSTO Paul	Release candidate
05/07/2021	Validation des commentaires et amendements à la version (RC 2) soumise aux praticiens, création de la RC 3	FRAUSTO Paul	Release candidate
6/10/2021	Approbation du Conseil d'Administration du Club EBIOS Création de la version publique	FRAUSTO Paul	Publique

Introduction

La méthode EBIOS Risk Manager est pensée pour s'adapter à l'objectif de l'étude. C'est ce principe pragmatique qui est retenu pour proposer une approche dite « Flash » afin de réaliser une étude préliminaire des risques en un temps réduit (9-10 heures).

Le principal bénéfice recherché de l'approche « Flash » est d'obtenir l'adhésion du métier à la démarche et l'appropriation de ses risques dans un temps limité, avec au final des résultats concrets.

La réalisation d'un schéma du système et de son écosystème est le point clé de la démarche « flash ». Ce schéma de principe permet de visualiser les valeurs métiers, les biens support, les parties prenantes, les sources de risques et les chemins d'attaque.

Pour dérouler l'approche « Flash », un nombre de prérequis doit être respecté. Le principal est la connaissance du domaine qui permet de disposer des informations précises nécessaires à l'étude (valeur métier, source de risques, parties prenantes, scénarios stratégiques).

L'approche « Flash » n'a pas pour but de conduire une étude de risque complète et détaillée, ou d'être une approche clé en main (checklist). Tous les risques ne seront pas forcément identifiés, mais cette démarche permet d'identifier rapidement les plus pertinents et de planifier un traitement adapté.

Ce document a un double objectif : le premier est de présenter l'approche « Flash », le second est de présenter un modèle du livrable dit « rapport de l'analyse de risques », en indiquant pour chaque étape, les bonnes pratiques à mettre en œuvre pour tenir dans le temps imparti.

Ce document ne se substitue pas au guide Méthode EBIOS de l'ANSSI qui reste la référence pour l'application de la méthode et qui en fixe le vocabulaire.
L'approche « flash » qui est ici décrite constitue une contribution proposée par un groupe de praticiens de la méthode EBIOS. Tout organisme souhaitant l'appliquer possède toute latitude pour l'adapter à son propre contexte.

Convention d'écriture :

Les textes :
surlignés en gris sont à personnaliser ou à compléter,
en italiques et écrits en vert sont des notes à l'attention du rédacteur,
écrits en bleu sont des exemples à remplacer.

Sommaire

1 PRESENTATION DE L'APPROCHE « FLASH »

1.1 OBJECTIF

L'objectif de l'approche « Flash » est de réaliser l'analyse de risques en mobilisant les acteurs pendant une seule séance de travail d'une durée limitée (2-3 heures).

Cette séance permet de conduire la réflexion selon les axes suivants :

- Besoins de sécurité,
- Les dangers dus à l'absence des bonnes pratiques (socle de sécurité),
- Les menaces liées à l'écosystème,
- Les risques spécifiques pesant sur l'objet de l'étude,
- L'identification des axes d'amélioration de la sécurité.

Livrable attendu : Rapport de l'analyse de risques avec des scénarios stratégiques (dont un scénario opérationnel au moins pour illustrer la menace et estimer la vraisemblance), niveau de risque et proposition de mesures de mitigation.

1.2 PRINCIPES DE L'APPROCHE

Pour parvenir à une telle optimisation de l'analyse de risques, les principes sont les suivants :

- Faire piloter l'étude et animer les ateliers par un sachant, maîtrisant l'écosystème de l'objet d'étude (comprendre rapidement les éléments échangés en atelier) et le déroulement de la méthode (animer les ateliers avec une gestion du temps adaptée).
- Exploiter une base de connaissances capitalisée sur des projets proches (une partie des valeurs métiers a déjà été évaluée, des parties prenantes ont déjà été étudiées dans d'autres projets, des scénarios stratégiques sont applicables à la cible) pour préparer la collecte de données et pré-remplir l'analyse.
- Utiliser une technique d'animation permettant de collecter de manière collaborative les éléments de l'analyse à partir d'un schéma de principe et de fiches synthétisant tous les éléments de traitement des risques.
- Rester à un niveau d'analyse adaptée en limitant le nombre de scénarios envisagés, sans se noyer dans les détails ou se focaliser sur une technique d'attaque.

1.3 BENEFICES ATTENDUS

Le bénéfice attendu de l'approche « Flash » par rapport à une approche « classique » est d'arriver à des résultats concrets, le tout en un temps limité. En s'assurant de :

- Obtenir l'adhésion du métier sur la démarche Flash et l'appropriation des risques,
- Identifier les risques les plus importants,
- Prioriser des mesures de traitement des risques.

1.4 PREREQUIS

Afin que l'approche « Flash » se déroule dans le temps défini, il est nécessaire que les prérequis suivants soient respectés:

1.4.1 Prérequis d'organisation

- Le pilote de l'étude EBIOS Risk Manager (qui sera également l'animateur principal des entretiens) n'est pas forcement membre du projet mais il fait partie de l'équipe sécurité SI pour laquelle l'étude est menée et il est partie prenante des résultats. Il a la connaissance du contexte de l'étude (système d'information, PSSI, parties prenantes, principaux fournisseurs, sources de risques liés au contexte…) et accès aux documents qui le décrivent.
- L'ensemble des parties prenantes internes (métier, architectes fonctionnels, architectes techniques, SSI, …) s'est engagé à participer à l'atelier.
- Un modèle de description des risques existe.

1.4.2 Prérequis sur la gouvernance SSI (capitalisation)

- Les parties prenantes récurrentes dans ce type d'environnement ont été caractérisées et leurs appréciations en matière de maturité et de confiance ont été évaluées.
- Les couples « sources des risques / objectifs visés », déjà rencontrés dans des études précédentes et jugés pertinents dans le contexte du projet, ont été caractérisés.
- Il existe un catalogue des scénarios stratégiques liés au contexte de l'étude.

1.4.3 Prérequis sur les travaux déjà réalisés sur la cible

- La PSSI est déployée avec les principes de base et d'hygiène et/ou l'écart par rapport aux bonnes pratiques pour l'objet de l'étude a déjà été identifié, par exemple via le contrôle interne en place.
- La classification des valeurs métiers est réalisée, selon l'impact sur les critères DICT.

1.5 Limites de l'approche

- Comme la méthode EBIOS Risk Manager le préconise, la liste des risques résultant de l'étude se limite aux plus pertinents, ce n'est pas une étude complète et fine qui est conduite.
- La démarche s'appuie fortement sur une capitalisation issue des résultats d'analyses de risques précédentes (voir prérequis en §1.4).

1.6 Organisation

L'approche « Flash » se déroule en 3 interactions clés avec les représentants du projet :

1. PREPARATION (1-2h) : Présenter l'approche méthodologique au commanditaire (Métier, DSI, RSSI, …), présentation de l'objet de l'étude, fixer le périmètre de l'étude et l'organisation (participants, planning, …) de l'atelier "Analyse de risques Flash".
2. COLLECTE DES DONNEES SPECIFIQUES, ANALYSE ET FORMALISATION (7h) :
    a. Une seule séance de travail est organisé, cette séance dit "Analyse de risques Flash" regroupe les objectifs des 5 ateliers proposés par la méthode EBIOS Risk Manager pour identifier les axes prioritaires d'amélioration de la sécurité.
    b. Rédaction du rapport de l'analyse de risques hors séance.
3. RESTITUTION (1h) : Restitution de l'analyse de risques. Présentation des principaux scénarios stratégiques, niveaux de risques définis et principales mesures de traitement.

1.7 Outillage

- Tableau blanc pour décrire schématiquement le système et son environnement.
- Moyen pour présenter :
    - La démarche,
    - Les différentes échelles, critères d'évaluation des sources de risques et des parties prenantes,
    - Restitution de l'analyse de risques.
- Modèle pré-rempli pour :
    - Présentation de l'approche-cadrage,
    - Formaliser l'analyse de risques,
    - Restitution de l'analyse de risques.

2 ETAPE PREPARATION

2.1 PREPARATION DU CADRAGE

2.1.1 Objectif

Durée : 1h

- Préparation de la réunion de cadrage, prise de connaissance générale de l'objet à étudier.
- Phase optionnelle avec des représentants du commanditaire.

2.1.2 Données d'entrée

- Informations technico-fonctionnelles de l'objet à étudier et son environnement : L'objectif est de pouvoir délimiter précisément le périmètre et de construire une modélisation des biens supports (Schéma de principe).
- Modèle pré-rempli de présentation de l'approche-cadrage.

2.1.3 Organisation et tâches

Personnalisation du modèle de présentation de l'approche-cadrage qui servira de support pour la réunion.

Réalisation du schéma de principe de l'objet de l'étude : description macro (schématisée) décrivant les principales briques technologiques, les principaux flux entre le(s) système(s) d'information / applications et les principales parties prenantes.

2.1.4 Comment procéder ?

A partir des données d'entrée, schématiser l'objet de l'étude.

Proposer le périmètre de l'étude selon les itérations avec les autres systèmes d'information / applications et la connaissance de l'environnement à étudier.

Travail hors séance pour collecter les éléments de la capitalisation.

2.1.5 Facteurs de réussite

Garder une vue d'ensemble avec le schéma de principe de l'objet de l'étude, l'objectif est d'en présenter une vue macro et claire, celle-ci facilitera la définition/validation du périmètre de l'étude dans la réunion de cadrage.

Identifier clairement les flux ou autres interactions avec les systèmes externes, exclus du périmètre.

Le modèle doit inclure la présentation de la démarche « Flash » en 3-4 diapositives, ne pas décrire la méthode EBIOS Risk Manager complète, mais seulement les principes. Inclure dans ce modèle une représentation graphique de l'organisation et de la durée de l'approche « Flash », incluant l'objectif et les livrables attendus dans chaque étape.

2.1.6 Résultat

Support de la réunion de cadrage, avec la vue macro de l'objet de l'étude (schéma de principe) et une proposition de périmètre à étudier.

2.2 REUNION DE CADRAGE

2.2.1 Objectif

Durée : 1h
Présentation de la démarche d'analyse de risques, validation du périmètre de l'analyse de risques et du planning.

L'objet est d'inviter les commanditaires pour leur présenter le contexte et collecter les éléments pour permettre aux animateurs de préparer la séance de travail.

2.2.2 Données d'entrée

Support de la réunion de cadrage personnalisé à l'issue de l'étape précédente.

2.2.3 Organisation et tâches

- Présentation des principes de la méthode EBIOS Risk Manager et de l'approche "Flash".
- Présentation de la solution (vue macro, utilisation du schéma général de l'objet de l'étude).
- Présentation et validation du périmètre proposé pour l'analyse de risques.
- Indiquer clairement ce qui est hors périmètre de l'étude et demander que cela fasse l'objet d'une étude sécurité par ailleurs.
- Identification des participants à l'atelier analyse de risques « flash » :
    - Représentant(s) métier(s) :
        - Quelqu'un qui sait comment la solution fonctionne ou va fonctionner (use cases).
        - Quelqu'un qui doit valider l'impact et la gravité si un évènement redouté se produit.
    - Représentant(s) technique(s) :
        - Quelqu'un qui connait la solution technique, y compris les échanges avec d'autres applications / services.
        - Quelqu'un qui connait l'infrastructure / services utilisés par la solution.
    - Représentant de la sécurité des systèmes d'information.

Définir le planning prévisionnel (à confirmer avec les participants ciblés).

A l'issue de la réunion, collecter tous les éléments pertinents des précédentes études d'analyse de risques pour enrichir les éléments invariants.

2.2.4 Comment procéder ?

- Utilisation du support pour la réunion de cadrage.
- Animation d'une réunion.

2.2.5 Facteurs de réussite

- Insister sur l'importance que les « sachants » soient présents à l'atelier « Analyse de risque Flash ».
- Insister sur l'approche pragmatique peu consommatrice en temps.
- Sensibiliser le commanditaire sur :
    - Le besoin de se poser la question sur les impacts et risques à chaque changement / évolution de l'objet de l'étude.
    - Le besoin de valider et suivre le plan de traitement des risques.
    - L'importance d'impliquer le(s) métier(s) pour valider l'impact et la gravité.
    - L'importance d'un analyste sécurité pour apporter son expertise dans l'identification des scénarios stratégiques.

2.2.6 Résultat

- Périmètre de l'analyse de risques validé.
- Planning prévisionnel avec la liste des participants.
- Sensibilisation du commanditaire.

3 ETAPE COLLECTE DES DONNEES SPECIFIQUES, ANALYSE ET FORMALISATION

3.1 ATELIER COLLECTE DES DONNEES ET ANALYSE

3.1.1 Objectif

Durée : 2 – 3h
L'atelier vise à étudier les points suivants :

- Qui ou quoi pourrait porter atteinte aux missions métier, dans quels buts ? Et comment s'en protéger ?
- Comprendre l'écosystème de l'objet de l'étude, identifier les acteurs et les valeurs métiers, ainsi que les biens supports.
- Identifier les événements redoutés associés aux valeurs métiers et confirmer / ré-évaluer la gravité de leurs impacts.
- Comprendre les écarts avec la politique de sécurité applicable.
- Valider / compléter / adapter les sources de risques et leurs objectifs visés, en lien avec le contexte particulier de l'étude.
- Valider / compléter / adapter la liste des parties prenantes et leur niveau de menace.
- Identifier les scénarios stratégiques, avec les chemins d'attaque les plus pertinents (définir au moins un scénario opérationnel par scénario stratégique).
- Evaluer le niveau de risque.
- Identifier des mesures de protection.

3.1.2 Données d'entrée

- Schéma de principe de l'objet de l'étude préparé pour la réunion de cadrage.
- Périmètre de l'analyse de risques.
- Principales valeurs métiers, leurs évènements redoutés et niveau d'impact / gravité (issue d'études précédentes).
- Mesures de sécurité existantes et permettant de contribuer à la protection contre les évènements redoutés.
- Principaux écarts avec les règles d'hygiène de sécurité des systèmes d'information.
- Sources de risques / Objectifs visés caractérisés.
- Parties prenantes récurrentes caractérisées.
- Echelles (d'impact / gravité, d'évaluation des sources de risques et parties prenantes, de vraisemblance, du niveau de risques).

3.1.3 Organisation et tâches

Le déroulé de l'atelier :

- Première partie (durée conseillée : 1h) :
    - Focus sur la vue métier : compléter le schéma général de l'objet de l'étude, avec le positionnement de :
        - Valeurs métiers.
        - Principales parties prenantes.
        - Identification des sources de risques / objectifs visées.
    - Identification des scénarios stratégiques (vus par le métier) avec ses principaux chemins d'attaque et validation / réévaluation de leur gravité.

  - Identification des mesures pour limiter la menace que représentent les parties prenantes.
- Deuxième partie (durée conseillée : 1h30) :
  - Focus aspects technico-fonctionnels de l'objet de l'étude :
    - Identification des biens supports (principales briques technologiques, systèmes d'information / applications).
    - Principaux flux entre le(s) système(s) d'information / applications.
    - Écarts avec les règles d'hygiène SSI et la PSSI.
  - Identifier des scénarios opérationnels restants, en tenant compte de toutes les mesures déjà proposées. Au moins un scénario opérationnel par scénario stratégique est décrit, le niveau du risque pour ces scénarios peut ainsi être évalué.
- Troisième partie (durée conseillée : 0h30) :
  - Focus sur les mesures de réduction des menaces liées
    - aux parties prenantes.
    - aux actions élémentaires évoquées dans les scénarios opérationnels.
  - Eventuellement aborder la limite acceptable des mesures évoquées.

Les participants à l'atelier :

- Représentants métiers.
- Représentants techniques (Architectes fonctionnel / technique / sécurité).
- Spécialistes en analyse de la menace numérique -> analyste sécurité.
- Selon l'étude : tests d'intrusion.

3.1.4 Comment procéder ?

Utiliser le tableau blanc (ou toute autre moyen collaboratif) pour représenter et compléter le schéma général de l'objet de l'étude et son écosystème. Cette vue est indispensable pour visualiser les différents éléments de l'étude et comprendre leur positionnement et les échanges. Ce schéma devra contenir une majorité des éléments discutés (valeurs métiers et leurs besoins, biens supports, les flux, les parties prenantes, les chemins d'attaque, les axes de sécurisation).

- Commencer par échanger avec le(s) métier(s) sur les principaux cas d'usage métier ou principaux processus métier (« comment marche votre solution ? »), faire ressortir les principales valeurs métiers et identifier / compléter leur position dans le schéma.
  - Si de nouvelles valeurs métiers apparaissent, présenter l'échelle au(x) métier(s) pour évaluer la gravité des évènements redoutés associés.
- Positionner les parties prenantes pour identifier clairement qui a accès à quelle(s) valeur(s) métier(s).
- Définir les scénarios stratégiques et les noter au tableau, avec leur gravité :
  - La description d'un scénario stratégique doit contenir : la source de risque, le chemin d'attaque, la ou les valeurs métiers, le ou les évènements redoutés et l'objectif visé.

    Exemple : Un groupe de cybercriminels est mobilisé pour exfiltrer des données hébergées dans un SaaS exposé sur Internet et demander une rançon.
- Marquer les principaux flux sur le schéma général afin de présenter les différents accès à l'objet d'étude.
- Marquer les principales briques technologiques (biens supports) et leurs écarts avec les règles d'hygiène SSI et la PSSI.
- Positionner les sources de risques directement dans le bien support vulnérable, cette action servira de support pour définir les scénarios opérationnels.
- Définir la vraisemblance des scénarios opérationnels, et indiquer le niveau de risque de chaque scénario opérationnel.

Au fil de l'atelier noter / capturer les mesures de sécurité et pour chaque scénario opérationnel confirmer / compléter ces mesures.

Principaux sujets à aborder :

- Cas d'usage métiers (type des données inclus).
- Lieu de stockage des données et sauvegardes.
- Les moyens d'accès des partenaires / fournisseurs au système.
- Architecture applicative / Architecture réseaux.
- Gestion des utilisateurs finaux et des droits d'accès.
- Gestion des utilisateurs privilégiés et des droits d'accès.
- Exploitation et maintenance du système (MCO/MCS).
- Système d'accès physique.

3.1.5 Facteurs de réussite

- Un praticien est essentiel pour animer l'atelier et doit avoir préparé l'atelier avec sa vision issue des éléments qu'il a collecté dans la capitalisation.
- S'assurer d'avoir les bonnes personnes dans l'atelier (représentant métier, « sachant » fonctionnel, « sachant » technique et sécurité, spécialiste de la menace SI).
- Utiliser un vocabulaire spécifique au projet (évènements redoutés, sources de risques, parties prenantes, mesures de sécurité) et éviter les termes des spécialistes de la pratique d'EBIOS (notamment si l'animateur sent que le vocabulaire EBIOS perturbe la réflexion).
- Limiter l'étude aux évènements redoutés les plus sévères, ne pas se perdre dans les détails.
- Réévaluer les sources de risques et parties prenantes si nécessaire et surtout identifier les nouvelles pour les évaluer.
- Pour optimiser le temps, il est conseillé de limiter l'étude à 5 scénarios stratégiques aussi représentatifs que possible des types d'attaque.
- Il est conseillé de limiter l'analyse à une illustration d'un scénario opérationnel qui permettra d'évaluer le niveau du risque.
- Le tableau blanc est l'outil de prise de notes, annoter l'information qui permettra de formaliser les scénarios stratégiques.

3.1.6 Résultat

Livrables (non formalisés) :

- Schématisation de l'objet de l'étude et de son écosystème, incluant :
  - Principales valeurs métiers et gravités associées ;
  - Parties prenantes « re-caractérisées » ;
  - Sources de risques et objectifs visés « re-caractérisés » ;
- Scénarios stratégiques avec leurs scénarios opérationnels les plus pertinents (représentés sur le schéma de principe) avec leurs niveaux de risques et les principales mesures de réduction des risques (notes dans le tableau blanc).

3.2 ANALYSE ET FORMALISATION

3.2.1 Objectif

Durée : ½ journée
Formaliser le rapport d'analyse des risques, notamment sous la forme de fiches de risques.

3.2.2 Données d'entrée

- Résultats de l'atelier COLLECTE DES DONNEES ET ANALYSE.
- Modèle pré-rempli pour formaliser l'étude de sécurité.
- Modèle pré-rempli pour la restitution de l'étude de sécurité.

3.2.3 Organisation et tâches

- Rédaction du rapport de l'analyse.
- Préparation du support de restitution.

3.2.4 Comment procéder ?

Utilisez le modèle pré-rempli pour formaliser l'étude sécurité. Le tableau scénario stratégique permet de résumer les informations capturées dans l'atelier COLLECTE DES DONNEES ET ANALYSE.

Utiliser un modèle pré-rempli pour la restitution de l'étude sécurité pour présenter le schéma général de l'objet, le périmètre et les scénarios stratégiques avec leur scénario opérationnel et les principales mesures de mitigation proposées.

3.2.5 Facteurs de réussite

- Utiliser le catalogue des risques pertinents pour le domaine concerné afin d'aller plus vite dans la phase de formalisation des scénarios stratégiques.
- Identifier des quick wins / quick start parmi les mesures de sécurité proposées.
- Indiquer seulement les principales mesures de sécurité dans la restitution de l'étude et s'assurer de la faisabilité des mesures proposées.
- Consacrer du temps à l'explication du scénario stratégique (vu macro du chemin d'attaque) et justifier la vraisemblance par rapport aux écarts / vulnérabilités identifiés.
- Formaliser dans un vocabulaire compréhensible pour le management les risques résiduels issus de l'étude.
- Proposer les prochaines étapes, notamment la définition d'un plan d'action pour le traitement des risques identifiés.

3.2.6 Résultats

- Rapport de l'analyse de risques.
- Support de restitution.

4 ETAPE RESTITUTION

4.1 REUNION DE RESTITUTION ET DE FIXATION DES OBJECTIFS DE SECURITE

4.1.1 Objectif

Durée : 1h
Réunion de restitution de l'analyse de risques « Flash ».

4.1.2 Données d'entrée

- Rapport de l'analyse de risques.
- Support de restitution.

4.1.3 Organisation et tâches

- Présenter les principaux enjeux de sécurité et les facteurs d'exposition du projet.
- Présenter les principaux scénarios stratégiques et leur niveau de risque.
- Présenter les principales mesures de sécurité proposées avec leur « pour & contre ». Décider des mesures à déployer.
- Expliquer clairement les risques résiduels résultant des choix faits.
- Proposition / validation des prochaines étapes.

Les participants à la réunion :

- Direction.
- Commanditaire.
- Représentants métiers.
- Représentants techniques (Architectes fonctionnel / technique / sécurité).
- Spécialistes en analyse de la menace numérique -> analyste sécurité.

4.1.4 Comment procéder ?

Utilisation du support de restitution réalisé dans la phase précédente.

4.1.5 Facteurs de réussite

- Présenter les scénarios stratégiques dans l'ordre décroissant du niveau de risque.
- Présenter sur une seule planche, le risque, ces principales mesures de sécurité, et le ou les risques résiduels résultant.
- Faire évaluer par l'équipe projet l'applicabilité des mesures de sécurité dans des délais et des coûts raisonnables, et que leurs impacts sont acceptables pour le métier. Dans le cas où l'équipe projet ne peut réaliser ce contrôle, indiquer les mesures qui ont un fort coût ou impact.
- Acter que la prochaine étape est l'appropriation du plan de traitement des risques par l'équipe projet, en distinguant le cas échéant les mesures indispensables avant la mise en production.
- Définir la date de validation du plan de traitement des risques et confirmer qui est le responsable de ce plan d'action.

4.1.6 Résultats

- Définition des objectifs de sécurité (au sens choix des options de traitement des risques).

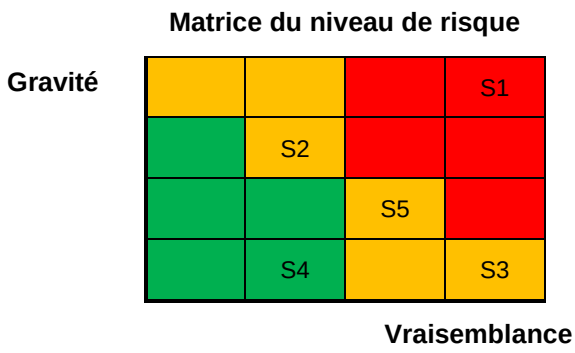
- Risques résiduels.
- Planning des prochaines étapes validé (notamment l'action de réalisation et validation du plan de traitement des risques par l'équipe projet / le commanditaire).

5 MODÈLE : RAPPORT ÉTUDE SÉCURITÉ

5.1 SYNTHÈSE

Ce chapitre montre les principaux scenarios stratégiques identifiés dans cet étude…. La matrice suivante présente le niveau de risque de ces scenarios.

Matrice du niveau de risque

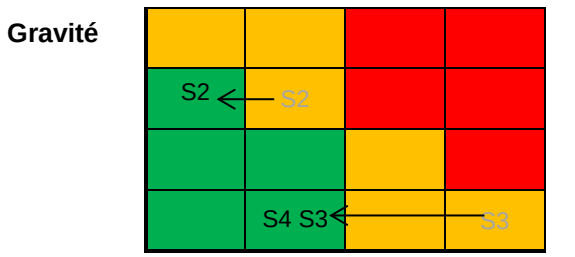


Scénarios de risque :

S1. Description du scénario de risque 1
S2. Description du scénario de risque 2
S3. …

Les risques résiduels sont calculés en considérant que toutes les mesures de sécurité proposées sont appliquées. Dans la mesure du possible, les scénarios sont reformalisés pour insister sur le scénario persistant qui nécessitera une décision managériale.

Matrice du niveau de risque résiduel



Risqué éliminé : S1

Conclusions

Exemple : le principal risque résiduel est au niveau moyen parce que le fournisseur de la solution X a des accès à privilèges pour le support de niveau 3. Des mesures de surveillance doivent être mises en place pour monitorer les actions du support.

5.2 Valeur métier ou enjeux de sécurité

Tableau avec les principales valeurs métiers et leur gravité

5.3 Evaluation des parties prenantes

Tableau avec les principales parties prenantes (PP) et l'évaluation de leur menace
Attention à ne pas générer un débat trop long sur l'appréciation du danger que représentent les PP

5.4 Schéma du système

Schéma de principe de l'objet de l'étude

5.5 Description des risques et axes d'amélioration

Scénario de risque 1

Description du scénario de risque qui doit indiquer la valeur métier, la source de risque, l'objectif visé, le chemin d'attaque et/ou la partie prenante.

Exemple : Un groupe de cybercriminels est mobilisé pour exfiltrer et chiffrer des données hébergées dans un SaaS exposé sur Internet et demander une rançon.

Description du scénario opérationnel

Le scénario opérationnel doit décrire les principales étapes du ou des chemins d'attaque

Exemple :

1. Les cybercriminels découvrent (via des outils automatiques de scan) une vulnérabilité sur la solution SaaS du fournisseur X.
2. Les cybercriminels exploitent la vulnérabilité.
3. Les cybercriminels accèdent à la base de données et exfiltrent l'information.
4. Les cybercriminels chiffrent les données et demandent une rançon.
5. La production est indisponible, le service n'est plus fourni pour Y temps.

Observations (*indiquer les faiblesses qui rendent pertinent le scénario opérationnel)*

Authentification

Exemple : politique de mot de passe faible, y compris pour les administrateurs de la solution SaaS.

Gestion de l'exploitation

Exemple : pas de politique de patch management définie, serveur front-office sans patch de sécurité depuis X temps.

Sécurité des échanges

Exemple : utilisation de protocoles obsolètes (SSL v1).

Règles de développement sécurisés

Exemple : pas de pratiques *security by design* (librairies obsolètes dans le code de la solution SaaS).

Gravité	*Indiquer la gravité de la valeur métier*	**Vraisemblance**	*Indiquer la vraisemblance du scénario*	**Niveau de risque**	*Indiquer le niveau de risque*

Action pour traiter le risque (réduction)

1 : Déployer la solution SaaS on-premise, étant donné que l'accès depuis Internet n'est pas nécessaire.

2 : Inclure une annexe sécurité dans le contrat en demandant une garantie de développement sécurisé et des mesures SSI au fournisseur.

…

Gravité	*Indiquer la gravité résiduelle lié à la valeur métier*	**Vraisemblance**	*Indiquer la vraisemblance résiduelle*	**Niveau de risque résiduel**	*Indiquer le niveau de risque résiduel*

Le scénario tel quel disparait avec les mesures de traitement du risque déployées. D'autres scénarios (attaque Inside, supply chain attack) restent d'actualité sans les mesures propres de traitement.

6 MODELE : Schématisation de la cible