




# Analyse de risques

## WIZARDS & DICE

 Créateur : Axel MOURILLON – Chef de projet

 Date de Création : 14/04/2025

 Dernier modificateur : <Prénom NOM> – <Rôle>

 Date de modification : JJ/MM/2025

 Version : 1.0



# Table des matières

<b>Table des figures.....</b>	<b>2</b>
<b>I. Introduction.....</b>	<b>3</b>
<b>II. Atelier 1 – Cadrage et socle de sécurité.....</b>	<b>4</b>
A) Cadrage de l'analyse de risques.....	4
1/ Objectifs de l'étude.....	4
2/ Rôles et responsabilités.....	4
3/ Cadre temporel.....	5
4/ Périmètre de l'infrastructure analysée.....	5
B) Périmètre métier et technique.....	5
1/ Missions de Wizards & Dice.....	5
2/ Valeurs métier.....	5
3/ Biens supports.....	6
C) Événements redoutés et gravité de ceux-ci.....	6
D) Socle de sécurité.....	10
1/ L'intérêt de l'utilisation d'un socle de sécurité pour EBIOS RM.....	10
2/ Référentiels applicables et état d'application.....	10
<b>III. Atelier 2 – Sources de risques.....</b>	<b>11</b>
A) Contexte et matrices de références.....	11
B) Couples de sources de risques et objectifs visés prioritaires.....	12
<b>IV. Atelier 3 – Scénarios stratégiques.....</b>	<b>13</b>
A) Cartographie du niveau de dangerosité.....	13
1/ Parties prenantes.....	13
2/ Cartographie de la menace.....	14
B) Scénarios stratégiques.....	15
1/ Premier scénario.....	16
2/ Deuxième scénario.....	18
3/ Troisième scénario.....	19
4/ Quatrième scénario.....	19
<b>V. Atelier 4 – Scénarios opérationnels.....</b>	<b>21</b>
A) Éléments de compréhension des schémas.....	21
B) Scénario opérationnel 1.....	22
1/ Déroulé.....	22
2/ Vraisemblance.....	22
C) Scénario opérationnel 2.....	23
1/ Déroulé.....	23
2/ Vraisemblance.....	23
<b>VI. Atelier 5 – Traitement du risque.....</b>	<b>26</b>
A) Cadre de l'atelier et criticité.....	26
B) Traitement du risque.....	27
1/ Premier scénario opérationnel.....	27
2/ Deuxième scénario opérationnel.....	28
C) Autres aspects de l'atelier.....	29
<b>VII. Conclusion.....</b>	<b>30</b>





# Table des figures

Figure 1 : Scénario stratégique 1 – concurrent visant à bloquer le site.....	16
Figure 2 : Scénario stratégique 2 – concurrent visant à donner une mauvaise image.....	18
Figure 3 : Scénario stratégique 3 – vengeur (client) visant à arnaquer/frauder le SAV.....	19
Figure 4 : Scénario stratégique 4 – hacker visant à générer de l'argent (par un service de hacking ou une rançon).....	19
Figure 5: Tableau des indices de vraisemblances.....	21
Figure 6 : Scénario opérationnel d'un concurrent cherchant à bloquer le site web.....	24
Figure 7 : Scénario opérationnel d'un hacker cherchant à voler et/ou détruire nos données.....	25





# I. Introduction

Au cours de ce document, nous allons appliquer la méthode "EBIOS Risk Manager" (ou "EBIOS RM"), soit "Gestion des Risques via l'Expression des Besoins et l'Identification des Objectifs de Sécurité". Cette méthode, publiée par l'Agence Nationale de la Sécurité et des Systèmes d'Information (ANSSI), est reconnue pour son adaptabilité par rapport aux objectifs du projet analysé. S'appliquant à tout type de structures, quels qu'en soient la taille, le secteur d'activité et les systèmes d'information, cette analyse de risques constitue une étape majeure dans la vie de Wizards & Dice. Bien qu'elle soit requise pour répondre aux attentes du jury, cette analyse EBIOS va mettre en lumière les risques majeurs qui pourraient perturber notre projet, ce qui va nous permettre de concentrer nos efforts en priorité sur les aspects les plus critiques.

La gestion des risques EBIOS se décompose en cinq ateliers, commençant d'une vision large pour aller de plus en plus dans le détail. Le premier atelier posera le cadre de ce qui sera analysé. Le second abordera les sources de risques ainsi que ce qu'elles visent. Le troisième et le quatrième traiteront respectivement des scénarios stratégiques et opérationnels afin de cartographier plus en détail les risques les plus critiques. Le cinquième et dernier atelier va lui fournir des propositions de traitements et de suivis des risques mis en lumière et détaillés par les quatre ateliers précédents.

Il est à noter que chaque atelier sollicite normalement l'intervention de plusieurs acteurs pouvant changer entre chaque atelier. Par exemple, l'atelier 1 sollicite des populations décisionnaires au sein de l'entreprise afin d'avoir une vision globale, tels que les membres de la direction des métiers de l'entreprise ainsi que le Directeur des Systèmes d'Information (DSI). À l'inverse, l'atelier 4 fait appel à des populations plus techniques, à même de répondre directement aux risques rencontrés, le Responsable de la Sécurité des Systèmes d'Information, le DSI, et éventuellement un spécialiste en cybersécurité. Cela étant dit, de par la taille de notre équipe projet, mais également à cause de l'implication de chacun de ses membres au sein des différents aspects du projet, nous avons effectué les cinq ateliers tous ensemble. Chacun était libre d'intervenir au mieux de ses capacités et de ses connaissances du sujet abordé, et cela au cours de chaque atelier. Ainsi, nous pensons avoir été en mesure de couvrir tous les aspects de cette analyse de risque, macro comme micro.

Aussi, la méthode EBIOS prévoit normalement deux cycles : un cycle stratégique pour revoir l'ensemble de l'étude et particulièrement les scénarios stratégiques ; et un cycle opérationnel, qui revient sur les scénarios opérationnels en fonction des incidents survenus, des nouvelles vulnérabilités apparues et de l'évolution des méthodes de travail et des systèmes d'information. Malheureusement, à cause des contraintes temporelles et organisationnelles du projet, nous n'aurons le temps que pour une version allégée du cycle stratégique, afin de revoir la pertinence de notre analyse de risques par rapport à l'infrastructure Wizards & Dice.





## II. Atelier 1 – Cadrage et socle de sécurité

### Introduction de la section :

Cette section traite de l'atelier 1 de la méthode d'analyse de risques EBIOS.

- Cadrage de l'analyse de risques : rappelle les objectifs de l'étude de risques et le cadre général dans lequel celle-ci s'inscrit.
- Périmètre métier et technique : définit le périmètre de l'étude.
- Événements redoutés et gravité de ceux-ci : établit les principaux événements redoutés et la gravité de ceux-ci.
- Socle de sécurité : traite de l'intérêt de l'utilisation de référentiels et de ceux utilisés comme base de la sécurité de notre projet.

### A) Cadrage de l'analyse de risques

#### 1/ Objectifs de l'étude

Bien qu'évoqué dans l'introduction, clarifions les objectifs de cette analyse de risques dans le contexte de Wizards & Dice. Cette analyse constitue le cinquième jalon sur les neufs que compte le système d'évaluation du projet. De par le contexte de ce projet tutoré, le professeur référent pour ce jalon, M. Florian DUCHEMIN, a adapté les attentes du modèle EBIOS. La liste qui nous a été fournie n'est évidemment pas exhaustive, mais elle justifie que nous limitons de surcroît le nombre d'éléments abordés dans ce document. Ainsi, les éléments constituant la plupart des livrables attendus sont les suivants :

- Le choix d'un référentiel, d'une norme ou d'un standard comme socle de sécurité.
- L'identification de 5 valeurs métiers maximum et leur(s) bien(s) support associé(s).
- L'identification de 2 événements redoutés minimum par valeur métier.
- L'identification de 4 paires de sources de risques/objectifs visés maximum.
- L'identification des parties prenantes liées.
- 4 scénarios stratégiques.
- 2 scénarios opérationnels avec mesure de remédiation.

En plus de l'aspect académique de ce rendu de jalon, cette analyse exposera les éléments les plus critiques, c'est-à-dire ce qui peut le plus facilement et/ou le plus gravement mettre le projet en péril. Connaître ces aspects nous permet de renforcer les points de sécurité en rapport direct avec ceux-ci, mais aussi de nous préparer à répondre aux incidents éventuels qui pourraient survenir.

#### 2/ Rôles et responsabilités

Comme abordé en introduction, la méthode d'analyse EBIOS requiert l'intervention de plusieurs profils différents au cours des différents ateliers. De par le nombre de membres de notre équipe et l'implication de chacun dans plusieurs aspects du projet, chacun a participé à tous les ateliers.





Nous nous sommes mis d'accord sur la plupart des éléments importants ensemble dans les grandes lignes, puis nous nous sommes répartis équitablement le travail et le fonctionnement de l'emploi du temps de chacun pour fournir une analyse claire et synthétique.

### 3/ Cadre temporel

Cette analyse a été réalisée sur 3 semaines, où chacun avait des tâches liées à cette analyse, en plus des tâches sur l'infrastructure du projet, à l'IUT et au travail en entreprise.

### 4/ Périmètre de l'infrastructure analysée

Afin de garder un cadre clair, nous nous focaliserons sur les parties les plus pertinentes de l'infrastructure de notre projet. Cela inclut :

- Le site web : ce sont toutes les pages web, des pages de boutiques à celles du forum, ainsi que toutes autres fonctions du site.
- L'infrastructure réseaux : ce sont les conteneurs, les machines virtuelles, les hôtes physiques, le NAS et l'accès à Internet.
- L'emplacement des hôtes physiques : ce sont les lieux de stockage du matériel informatique, mais également ceux des produits vendus.
- Les accès aux applications et aux comptes hébergés par des tiers : les principales utilisées dans notre projet sont Git, Bitwarden, les réseaux sociaux de Wizards & Dice et nos comptes mails.

## B) Périmètre métier et technique

### 1/ Missions de Wizards & Dice

Pour rappel, Wizards & Dice est un site de e-commerce et communautaire autour du jeu de rôle (JDR) qui a la particularité d'être auto-hébergé par nos soins. Le but est d'avoir un site fonctionnel, mais surtout sécurisé, pour que nos clients puissent passer commande et échanger sur le JDR en toute sécurité et avec confiance.

Ce type de service possède naturellement des risques qui lui sont propres, notamment vis-à-vis des sites concurrents ou de fraudes sur les commandes. Nous développerons les plus graves d'entre eux au cours de cette analyse.

### 2/ Valeurs métier

Tout d'abord, voici un rappel de la définition d'une **valeur métier** dans le cadre de la méthode EBIOS : c'est une composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé. Le tableau ci-après synthétise les valeurs métiers de notre projet.







Valeur métier (VM)	Dénomination de la valeur métier	Nature de la valeur métier	Description	Entité ou personne responsable
Valeur métier 1	Vente de produits	Service	Acheter des objets et de passer des commandes.	Personnel de l'équipe de Wizards & Dice
Valeur métier 2	Plateforme de discussion	Service	Discuter avec d'autres utilisateurs et voir les anciens messages.	
Valeur métier 3	Comptes clients	Information	Posséder un compte nominatif ressemblant diverses informations.	
Valeur métier 4	Relation client	Service	Mettre en avant le site et assurer un niveau de service après-vente correct.	
Valeur métier 5	Stock de produits	Bien matériel	Avoir des objets (physiques et numériques) à proposer.	

### 3/ Biens supports

Voici un rappel de la définition d'un **bien support** dans le cadre de la méthode EBIOS : c'est une composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être numérique, physique ou organisationnel. Le tableau ci-dessous traite des biens supports de notre projet.

Bien support (BS)	Dénomination du bien support	Valeur(s) métier(s) associée(s)	Description	Entité ou personne responsable
Bien support 1	Site web	VM 1 à 4	Interface principale pour les clients et vitrine de nos produits.	Personnel de l'équipe de Wizards & Dice
Bien support 2	Serveurs physiques	VM 1 à 4	Élément hébergeant nos machines virtuelles, essentiel à l'infrastructure.	
Bien support 3	Gestion des stocks	VM 1 à 3 et VM 5	Composant indispensable pour satisfaire les commandes.	
Bien support 4	Dépôt des stocks	VM 5	Lieu physique de stockage des produits (à traiter le temps).	
Bien support 5	Réseaux sociaux / mail	VM 4	Vitrine publicitaire et lieu d'échange entre nous et les clients.	

## C) Événements redoutés et gravité de ceux-ci

Dans le cadre de notre étude de risque, plusieurs événements redoutés (ER) ont été identifiés selon les valeurs métiers impactées. Le tableau ci-dessous synthétise les principaux événements redoutés que nous avons relevés, ainsi que la valeur métier qu'ils impactent, la catégorie d'impact, la gravité de l'événement sur une échelle de 1 (peu grave) à 4 (très grave), et enfin un commentaire pour apporter quelques précisions.





Événement redouté	Valeur métier	Catégories d'impact	Gravité	Commentaires/ justification
<b>ER 1 : Pertes des données de commandes</b>	Vente des produits (VM1)	- Perte financière - Retards de livraison - Insatisfaction client	3	Retards dans le traitement des commandes, clients insatisfaits, perte de revenus
<b>ER 2 : Blocage des ventes</b>	Vente des produits (VM1)	- Perte de CA - Interruption de l'activité commerciale	4	Le système de vente est au cœur du business, blocage impactant directement la survie financière
<b>ER 3 : Pertes de données clients</b>	Comptes clients (VM2)	- Violation du RGPD - Perte de confiance - Poursuites juridiques	3	Risque juridique et d'image important lié à la confidentialité
<b>ER 4 : Usurpation d'identité</b>	Comptes clients (VM2)	- Atteinte à l'image, - Responsabilité juridique Pertes pour les clients	3	Risque juridique élevé, et perte de confiance majeure de la part des clients. Et risque d'impact sur la sécurité des clients
<b>ER 5 : Blocage de la plateforme</b>	Plateforme de discussion (VM3)	- Rupture de communication communautaire - Frustration utilisateur - Baisse d'activité sur le forum	2	Forum non vital pour l'activité principale. Impact modéré sur l'engagement communautaire
<b>ER 6 : Publication de contenu interdit / inapproprié</b>	Plateforme de discussion (VM3)	- Atteinte à l'image - Modération difficile - Éventuelles plaintes juridiques	3	Du contenu choquant ou illégal peut nuire à la réputation, surtout s'il reste visible longtemps
<b>ER 7 : Diffamation / image négative de grande envergure</b>	Relation clients (VM4)	- Perte de réputation - Désengagement des clients	3	L'image est un actif clé, surtout dans les secteurs sensibles
<b>ER 8 : Fraude au SAV</b>	Relation clients (VM4)	- Pertes financières	1	Fraude limitée et contrôlable via un SAV manuel, sans effet notable sur l'activité.
<b>ER 9 : Vol / dégradation</b>	Stockage (physique et numérique) (VM5)	- Perte matérielle - Perte de données - Perte d'argent	3	La perte / vol physique ou logique peut retarder la production, mais surtout impacter la sécurité des personnes et des biens
<b>ER 10 : Indisponibilité de la gestion des stocks</b>	Stockage (physique et numérique) (VM5)	- Retards - Mauvaise allocation des ressources - Rupture de stock	2	Impact surtout logistique, mais gérable avec des solutions manuelles







L'un des scénarios les plus critiques concerne la vente des produits (VM1), avec en particulier le blocage du site de vente (ER2). Étant donné que le site représente le cœur de l'activité commerciale, toute indisponibilité – que ce soit par attaque, panne ou sabotage – entraîne une interruption immédiate des ventes et une perte directe de chiffre d'affaires, justifiant un niveau de gravité élevé (4). De même, la perte des données de commandes (ER1) peut perturber les livraisons, créer de l'insatisfaction client et entraîner des pertes financières, bien que dans une moindre mesure (gravité 3).

Les comptes clients (VM2) constituent également un axe sensible, notamment en cas de perte de données personnelles (ER1) ou d'usurpation d'identité (ER2). Ces scénarios soulèvent des enjeux juridiques liés au RGPD, mais aussi des risques en termes de réputation et de confiance des utilisateurs. Les conséquences incluent potentiellement des poursuites, une perte de crédibilité et des répercussions sur l'image de la société (gravité 3 pour les deux ER).

Concernant la plateforme de discussion (VM3), son blocage (ER1) impacte la dynamique communautaire sans pour autant menacer l'activité principale (gravité 2). En revanche, la publication de contenu choquant ou inapproprié (ER2) peut sérieusement détériorer l'image de l'entreprise, surtout si ces contenus restent visibles, ce qui justifie un niveau de gravité plus élevé (3).

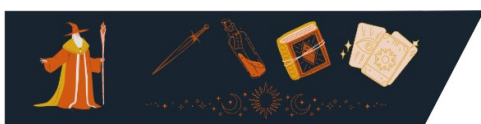
Du côté de la relation client (VM4), la diffamation ou la diffusion d'image négative (ER1) est particulièrement problématique dans les secteurs sensibles où la notoriété et la réputation sont cruciales (gravité 3). En revanche, la fraude au SAV (ER2), comme de fausses réclamations ou modifications de commande abusives, reste limitée grâce aux procédures manuelles en place, et son impact est donc évalué comme faible (gravité 1).

Enfin, en ce qui concerne la gestion du stockage (VM5), la dégradation ou le vol (ER1) de ressources physiques ou numériques peut entraîner une perte de données, des retards de production et des coûts matériels (gravité 3). Une indisponibilité de la gestion des stocks (ER2) peut perturber la logistique, mais des solutions manuelles permettent généralement d'en atténuer les effets (gravité 2).

Voici un rappel de la définition de la **gravité** dans le cadre de la méthode EBIOS : c'est une estimation du niveau et de l'intensité des effets d'un risque. La gravité fournit une mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects.

Voici un rappel de la définition de la **vraisemblance** dans le cadre de la méthode EBIOS : c'est une estimation de la faisabilité ou de la probabilité qu'un risque se réalise, selon l'échelle adoptée (très faible, peu vraisemblable, quasi certain, etc.).

À partir de ces définitions, nous avons pu établir la matrice de pertinence ci-après. Celle-ci nous permettra d'établir quel événement redouté est le plus pertinent dans notre infrastructure en fonction de sa gravité et de la vraisemblance de son apparition.





		Vraisemblance			
Gravité		Invraisemblable	Vraisemblable	Très vraisemblable	Quasiment certain
	Critique	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
	Grave	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent	Très pertinent
	Peu grave	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
	Sans gravité	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent

Le tableau ci-dessous met en relation gravité et probabilité d'occurrence des événements redoutés pour déduire la pertinence de chaque événement redouté. Les valeurs métiers impactées apparaissent également pour plus de clarté.

Évènements redoutés	Gravité	Vraisemblance	Pertinence
<b>VM 1 : Vente de produits</b>			
<b>ER 1</b> : Pertes des données de commandes	Grave	Très vraisemblable	Plutôt pertinent
<b>ER 2</b> : Blocage des ventes	Critique	Quasiment certain	Très pertinent
<b>ER 4</b> : Usurpation d'identité	Critique	Très vraisemblable	Très pertinent
Modification frauduleuse (ex : changement prix)	Grave	Vraisemblable	Plutôt pertinent
<b>VM 2 : Plateforme de discussion</b>			
<b>ER 3</b> : Perte d'une donnée client	Grave	Vraisemblable	Plutôt pertinent
<b>ER 4</b> : Usurpation d'identité	Critique	Quasiment certain	Très pertinent
<b>VM 3 : Comptes clients</b>			
<b>ER 5</b> : Blocage de la plateforme	Grave	Très vraisemblable	Plutôt pertinent
<b>ER 6</b> : Publication de contenu interdit	Peu grave	Quasiment certain	Plutôt pertinent
<b>VM 4 : Relation client</b>			
<b>ER 7</b> : Diffamation ou atteinte à l'image	Grave	Très vraisemblable	Plutôt pertinent
<b>ER 8</b> : Fraude (SAV notamment)	Peu grave	Quasiment certain	Plutôt pertinent
Perte des comptes (réseaux sociaux)	Peu grave	Vraisemblable	Moyennement pertinent
<b>VM 5 : Stock de produits</b>			
<b>ER 9</b> : Dégradation ou vol des produits en stock	Critique	Très vraisemblable	Très pertinent
<b>ER 10</b> : Indisponibilité des moyens de gestion des stocks	Grave	Vraisemblable	Plutôt pertinent





## D) Socle de sécurité

### 1/ L'intérêt de l'utilisation d'un socle de sécurité pour EBIOS RM

Afin de se baser sur des références communes et admises comme les bonnes pratiques à appliquer, la méthode EBIOS prend appui sur des référentiels officiels ou internes. Les principaux sont les recommandations de l'ANSSI, l'établissement d'une Politique de Sécurité du Système d'Information (PSSI), les différents référentiels ISO, voire même les exigences de certains clients ou fournisseurs.

L'intérêt de ce type de socle est de poser une base de sécurité à appliquer, censée couvrir les aspects généraux de la sécurité du projet. En tant que données qu'elles sont déjà mises en place ou prévues, ce socle permet de centrer et de cadrer l'analyse correctement au départ, de mettre en valeur les efforts fournis, d'évaluer des risques résiduels ou encore de servir de base pour des mesures additionnelles.

### 2/ Référentiels applicables et état d'application

À la vue de la nature de notre projet, notre équipe d'utiliser les référentiels suivants :

- Le (RGPD), pour le périmètre en général, mais en particulier les aspects liés aux données personnelles de nos clients.  
Elle oblige à mettre en œuvre des mesures de sécurité adaptées pour éviter l'accès non autorisé aux données personnelles.
- Le Payment Card Industry Data Security Standard (PCI-DSS, ou "Norme de Sécurité de l'Industrie des Cartes de Paiement" en français), pour les parties impliquant des données de paiement.  
Applicable aux services de paiement, renforce également la sécurité des composants web, même si elle est optionnelle ici.
- Le référentiel applicatif de l'ANSSI, pour traiter les quelques points qui auraient pu être laissés de côté précédemment, en particulier pour les questions applicatives.  
Le guide de l'ANSSI pour la sécurisation d'un site web, qui impose :
  - le durcissement du serveur,
  - la gestion des mises à jour logicielles,
  - l'application de correctifs de sécurité,
  - des contrôles d'accès et de surveillance renforcés.

Il est important de noter que, de par le statut de projet tutoré de notre infrastructure, l'établissement d'un état d'application précis de ces normes n'est pas un des éléments perçus comme prioritaire par notre équipe. De nombreuses autres tâches doivent être effectuées d'ici la fin du projet et, bien que nous ayons un ordre d'idée de ce qui est en place et de ce qui est ne l'est pas au sein de notre infrastructure, le savoir avec plus de précision serait contre-productif pour le reste du projet. Pour ces raisons, nous ne détaillerons pas l'état d'application des référentiels utilisés au sein de notre SI.





## III. Atelier 2 – Sources de risques

### Introduction de la section :

Cette section traite de l'atelier 2 de la méthode d'analyse de risques EBIOS.

- Contexte et matrices de références : aborde le contexte de choix des sources de risques analysés et établit les références d'analyses.
- Couples de sources de risques et objectifs visés prioritaires : synthétise les couples de sources de risques et d'objectifs que nous analyserons plus en profondeur.

### A) Contexte et matrices de références

Au cours de ce second atelier, nous allons traiter des sources. L'énoncé demande clairement le traitement de 4 couples de sources de risques et de leur objectif visé **maximum**. Dans la réalité du projet, il y en a évidemment plus. Nous avons donc majoritairement choisi des sources de risques pertinentes dans le contexte de Wizards & Dice, mais également une source de risque moins pertinente mais suffisamment différente des autres pour nous paraître intéressante à analyser.

Par ailleurs, afin de déterminer les sources de risques les plus pertinentes pour en poursuivre l'analyse, il est d'abord important de bien comprendre les références que nous utiliserons pour qualifier ces sources de risques.

Le tableau ci-dessous cartographie les différents niveaux de motivations, de ressources et de pertinence que nous utiliserons au cours de l'atelier 2 :

Référentiel des niveaux	Motivation	Ressources	Pertinence
1	Faible	Limitées	Peu pertinent
2	Moyenne	Moyennes	Moyennement pertinent
3	Forte	Importantes	Plutôt pertinent
4	Extrême	Significatives	Très pertinent

Bien que le tableau précédent établisse les niveaux de pertinence utilisés, la façon de les utiliser est déterminée par la matrice ci-dessous :

		Ressources			
Motivation		Limitées	Moyennes	Importantes	Significatives
	Extrême	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
	Forte	Moyennement pertinent	Moyennement pertinent	Plutôt pertinent	Très pertinent
	Moyenne	Peu pertinent	Moyennement pertinent	Moyennement pertinent	Plutôt pertinent
	Faible	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent





## B) Couples de sources de risques et objectifs visés prioritaires

Le tableau ci-dessous synthétise les sources de risques que nous avons retenues, ainsi que leurs objectifs visés, le type de motivation qui les pousserait à agir, leurs niveaux de motivation et de ressources et enfin la pertinence du danger qu'elles représentent.

Sources de risque	Objectifs visés	Type de motivation	Motivation	Ressources	Pertinence
Concurrent	Bloquer le site	Stratégique	Extrême	Importantes	Très pertinent
Concurrent	Mauvaise image	Stratégique	Extrême	Importantes	Très pertinent
Vengeur (client)	Arnaque, fraude	Financière, Idéologique	Forte	Limitées	Plutôt pertinent
Hacker isolé	Argent	Financière	Moyenne	Limitées	Peu pertinent

Il est à noter que nous avons choisi le hacker isolé car nous pensons qu'il amène une certaine diversité dans les risques analysés, malgré une pertinence plutôt faible.







## IV. Atelier 3 – Scénarios stratégiques

### Introduction de la section :

Cette section traite de l'atelier 3 de la méthode d'analyse de risques EBIOS.

- Cartographie du niveau de dangerosité : répertorie les parties prenantes et le niveau de menace de celles-ci.
- Scénarios stratégiques : détaille et analyse les scénarios stratégiques retenus.

### A) Cartographie du niveau de dangerosité

#### 1/ Parties prenantes

Nous avons identifié plusieurs parties prenantes susceptibles d'interagir avec notre système d'information, que ce soit en tant qu'acteurs internes, partenaires de confiance ou sources potentielles de menace. Les parties prenantes sont les suivantes :

Partie prenante	Type d'acteur
Cl1 – Client A	Client
Co1 – Concurrent A	Concurrent
Pe1 – Wizards & Dice (S.I)	Personnel
H1 – Hacker A	Hacker
P1 – Fournisseur paiement	Prestataire
P2 – Fournisseur nom de domaine	Prestataire
P3 – Fournisseur d'accès internet	Prestataire
P4 – Prestataire SaaS / Cloud (Bitwarden)	Prestataire
P5 – Prestataire de sécurité (StormShield)	Prestataire

Voici plus de détails vis-à-vis de nos parties prenantes :

- **Cl1 – Client A :**  
Représente l'utilisateur final du service, pouvant être à l'origine de réclamations, de fuites involontaires ou même de scénarios malveillants dans un cadre vengeur.
- **Co1 – Concurrent A :**  
Constitue une source de risque directe, notamment par des attaques visant à nuire à l'image de l'entreprise ou à bloquer l'accès à nos services (DDoS, sabotage indirect).
- **Pe1 – Wizards & Dice (S.I) :**  
L'organisation elle-même, incluant ses collaborateurs internes, qui peuvent être la cible d'ingénierie sociale ou d'exploitation de vulnérabilités.
- **H1 – Hackeur A :**  
Acteur externe malveillant pouvant initier des attaques complexes (phishing, malware, ransomware).
- **P1 – Fournisseur de paiement :**  
Essentiel au bon fonctionnement des transactions, toute interruption ou compromission aurait un impact majeur.





- **P2 – Fournisseur de nom de domaine :**  
Contrôle la résolution DNS du site ; une attaque à ce niveau peut rendre le site inaccessible.
- **P3 – Fournisseur d'accès Internet :**  
Vecteur clé pour assurer la disponibilité des services ; un DDoS ciblé ou une interruption aurait un effet immédiat.
- **P4 – Prestataire SaaS/Cloud (Bitwarden) :**  
Hébergeur ou outil externalisé pouvant contenir des données sensibles ; sa compromission est critique.
- **P5 – Prestataire de sécurité (StormShield) :**  
Joue un rôle fondamental dans la protection des flux et la surveillance réseau ; sa fiabilité est un élément majeur du dispositif de défense.

## 2/ Cartographie de la menace

Cette cartographie des parties prenantes permet de mieux visualiser les zones de dépendance, de prioriser les mesures de sécurité et de modéliser les scénarios d'attaque réalistes en se basant sur des interactions existantes ou possibles avec notre système. On peut y observer les parties prenantes, leur type, ainsi que leur score en fonction de leur exposition, de leur fiabilité et de leur niveau de menace.

Nom des parties prenantes	Type d'acteur	Exposition			Fiabilité cyber			Niveau de menace
		Dépendance	Pénétration	Total	Total	Maturité cyber	Confiance	
Cl1 – Client A	Client	3	1	3	1	1	1	3
Co1 – Concurrent A	Concurrent	1	1	1	2	2	1	0,5
Pe1 – Wizards & Dice (S.I)	Personnel	3	4	12	12	3	4	1
H1 – Hacker A	Hacker	1	1	1	1	1	1	1
P1 – Fournisseur paiement	Prestataire	3	2	6	4	2	2	1,5
P2 – Fournisseur nom de domaine	Prestataire	3	1	3	4	2	2	0,75
P3 – Fournisseur d'accès internet	Prestataire	3	1	3	4	2	2	0,75
P4 – Prestataire SaaS / Cloud (Bitwarden)	Prestataire	2	2	4	4	2	2	1
P5 – Prestataire de sécurité (Stormshield)	Prestataire	3	1	3	4	2	2	0,75

Comme évoqué, chaque acteur est évalué selon deux axes principaux : l'exposition (avec la dépendance et la pénétration) et la fiabilité cyber (avec la maturité en sécurité et le niveau de confiance). Le niveau de menace est ensuite calculé par la formule :

$$\text{Niveau de menace} = \frac{\text{Dépendance} \times \text{Pénétration}}{\text{Maturité cyber} \times \text{Confiance}}$$





Par exemple, le client (Cl1) a une dépendance forte (3) car il est essentiel à l'activité, mais n'a pas d'accès à des ressources sensibles (pénétration = 1), avec une faible maturité et confiance, ce qui donne un niveau de menace élevé (3).

À l'inverse, le personnel interne (Pe1) est très exposé (dépendance et accès aux serveurs critiques), mais sa maturité et confiance élevées réduisent significativement le risque (niveau de menace = 1).

Le hacker (H1) a un très faible niveau de pénétration (1) car il n'a pas encore accédé au système, mais il reste dangereux car il est malveillant (confiance = 1) et n'a aucune politique de sécurité (maturité = 1), ce qui place sa menace à 1 également.

Les prestataires sont notés selon leur rôle dans l'infrastructure :

- Les fournisseurs critiques (paiement, sécurité) ont une dépendance élevée, et leur maturité ou confiance parfois limitée augmente leur niveau de menace.
- Les services cloud (Bitwarden) ou de paiement ont un accès potentiellement plus large, mais leur niveau de sécurité réduit l'exposition globale.

Donc, l'analyse des parties prenantes permet d'identifier les acteurs les plus exposés ou les plus critiques pour la sécurité de l'organisation. Elle repose sur une double évaluation de leur exposition et de leur fiabilité cyber, ce qui permet de calculer un niveau de menace pour chacun.

Cette étape permet de prioriser les efforts de cybersécurité, en identifiant les points de vigilance et les partenaires ou utilisateurs à surveiller plus étroitement dans les scénarios ultérieurs.

## B) Scénarios stratégiques

Un des scénarios prévus par le guide de l'ANSSI pour la sécurisation Web serait sur celui des vulnérabilités (celles de XSS particulièrement). Pour être plus précis, nous parlons du scénario "d'exploitation d'une vulnérabilité technique sur le site web". Il désigne l'exploitation d'une faille technique applicative ou système (comme une injection SQL, XSS, ou un défaut d'authentification) visant à compromettre directement la sécurité du site web. Par exemple, un attaquant pourrait profiter d'un champ de formulaire mal protégé pour injecter un code malveillant.

Nous avons choisi d'exclure ce scénario, car ce type de menace est déjà couvert par les référentiels de sécurité adoptés (cf. II- D) 2/ *Référentiels applicables et état d'application*). Pour rappel, les dispositifs mis en place pour réduire ce risque sont :

- Le suivi des préconisations du guide de l'ANSSI pour la sécurisation d'un site web (durcissement, gestion des mises à jour, correctifs de sécurité, contrôles d'accès).
- Le suivi de l'article 32 du RGPD, pour la mise en œuvre de mesures de sécurité limitant les accès aux données personnelles.
- Le suivi de la norme PCI-DSS, renforçant la sécurité des composants web (optionnelle dans ce cas).

Ces vulnérabilités sont considérées comme traitées par défaut dans le périmètre de sécurité actuel, ce qui rend inutile le traitement des scénarios stratégiques associés. Cet exemple de scénario est donc exclu de l'analyse de risque détaillée.



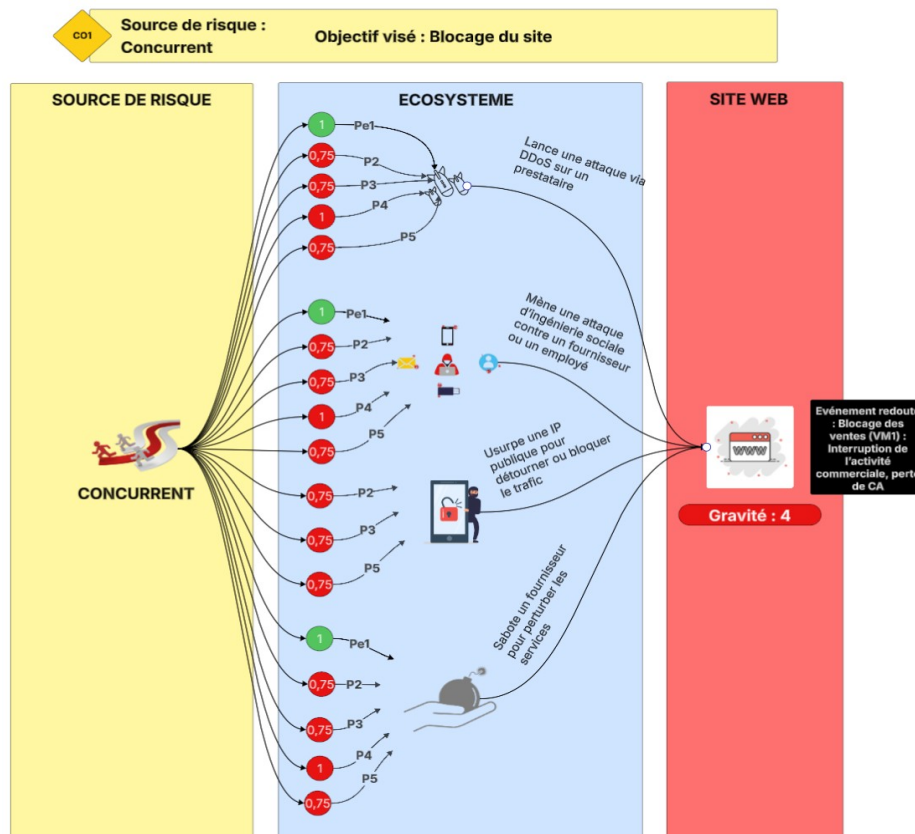


De par le cadrage formulé préalablement à cette analyse de risques, nous préférons focaliser nos efforts sur des scénarios qui ne sont pas déjà traités par les références de notre socle de sécurité. Afin de réserver les 4 analyses de scénarios stratégiques à des cas pertinents, nous avons donc focalisé notre attention sur certains scénarios. Ici, nous parlons de scénarios ne relevant pas de simples failles techniques, mais plutôt de stratégies adverses plus complexes. N'étant pas toujours anticipées par les guides ou référentiels, ces manœuvres d'attaques justifient une analyse approfondie. Parmi elles, il y a :

- Attaques par ingénierie sociale  
Elles visent à obtenir des identifiants ou à manipuler les collaborateurs.
- Détournements via des services tiers  
Cela cible surtout nos prestataires DNS, SaaS, ou d'hébergement.
- Utilisation de moyens détournés  
Nous parlons ici d'usurpation d'adresse IP ou de sabotage indirect.
- Mise en œuvre de malwares ou de ransomwares  
Le fonctionnement de ce type de malware repose souvent sur des failles humaines ou organisationnelles, plutôt que techniques.

C'est la raison pour laquelle les scénarios conservés dans cette étude (blocage du site, fraude au SAV, diffamation, ransomware, etc.) s'appuient sur des chemins d'attaque plus vraisemblables, moins encadrés par des référentiels, et donc plus pertinents pour notre projet.

## 1/ Premier scénario



**Figure 1 : Scénario stratégique 1 – concurrent visant à bloquer le site**





Le schéma précédent décrit le premier scénario stratégique. Il analyse par quel chemin stratégique un concurrent ayant pour but de bloquer les ventes de notre site passerait pour arriver à ses fins. Nous avons isolé 4 chemins d'attaques par lesquels il pourrait atteindre son objectif.

Le premier chemin décrit une attaque DDoS. Il Le concurrent accède à notre SI indirectement via le prestataire (par une interruption de service, une surcharge ou bien une exploitation de faille). Le concurrent lance une attaque par déni de service distribué (DDoS) via un botnet ou un service commandé sur le dark web. Cette attaque cible directement les infrastructures d'un prestataire critique (hébergement, réseau ou sécurité), provoquant une surcharge des serveurs et rendant la plateforme de vente temporairement inaccessible pour les utilisateurs.

Le deuxième chemin décrit une attaque par ingénierie sociale contre un fournisseur ou un employé. Il met en jeu 5 parties prenantes : prestataire d'accès Internet (P3), SaaS/cloud (P4), nom de domaine (P2), Wizards & Dice (Pe1) et prestataire de sécurité (P5). Le concurrent accède à notre SI en obtenant des identifiants ou en détournant des accès. Il piège un intervenant pour obtenir des accès ou perturber l'infrastructure liée au site.

Le troisième chemin décrit l'usurpation d'une de nos IP publique pour détourner ou bloquer le trafic. Il met en jeu 3 parties prenantes : le fournisseur d'accès internet (P3) ; le fournisseur de nom de domaine (P2) et le prestataire de sécurité (P5). Le concurrent accède à notre SI par une redirection ou un blocage de trafic réseau. L'IP publique du site ou de l'infra est usurpée pour perturber les accès ou interférer dans les communications.

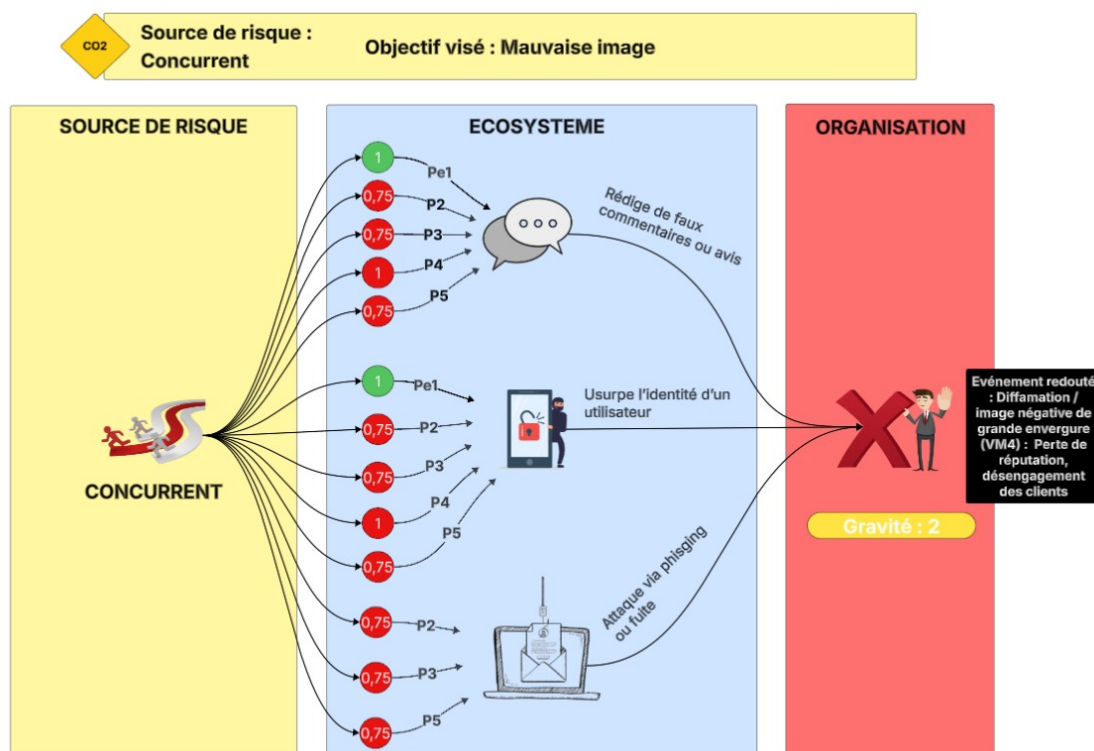
Le dernier chemin décrit le sabotage d'un fournisseur pour perturber nos services. Il met en jeu 5 parties prenantes : prestataire d'accès Internet (P3), SaaS / cloud (P4), nom de domaine (P2), Wizards & Dice (Pe1) et prestataire de sécurité (P5). Le concurrent accède à notre SI en interrompant volontairement des services via un sabotage physique. Il pousse un fournisseur à l'arrêt de son service (panne, sabotage direct), rendant ainsi le site indisponible.







## 2/ Deuxième scénario



**Figure 2 : Scénario stratégique 2 – concurrent visant à donner une mauvaise image**

Le schéma précédent décrit le deuxième scénario stratégique. Il analyse par quel chemin stratégique un concurrent ayant pour but de diffamer notre image de marque et de donner une image négative de notre site passerait pour arriver à ses fins. Nous avons isolé 3 chemins d'attaques par lesquels il pourrait atteindre son objectif.

Le premier chemin décrit la rédaction de faux commentaires ou avis. Il met en jeu 5 parties prenantes : le prestataire d'accès Interne (P3), le Wizards & Dice (Pe1), le client A (Cl1), le prestataire de sécurité (P5) et le SaaS/Cloud (P4). Le concurrent accède à notre SI par des accès à la plateforme de discussion (publique ou via faux compte). Il poste de faux commentaires négatifs sur le forum ou les pages produits, pour nuire à la réputation de l'entreprise.

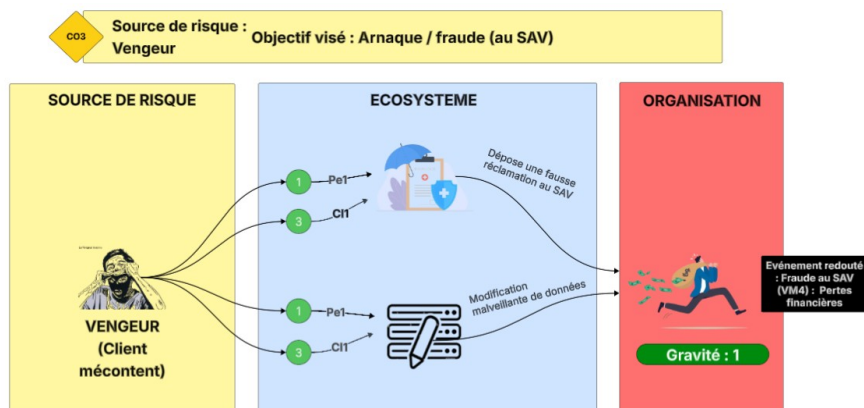
Le deuxième chemin décrit l'usurpation de l'identité d'un utilisateur. Il met en jeu 4 parties prenantes : Wizards & Dice (Pe1), client A (Cl1), prestataire de sécurité (P5) et SaaS/Cloud (P4). Le concurrent accède à notre SI par des accès au compte d'un client ou d'un collaborateur. Il vole ou falsifie des identifiants pour publier en se faisant passer pour un utilisateur connu.

Le troisième chemin décrit une campagne de phishing ou une fuite de données. Il met en jeu 3 parties prenantes : Wizards & Dice (Pe1), prestataire de sécurité (P5) et SaaS / Cloud (P4). Le concurrent accède à notre SI par un accès à un compte administrateur ou modérateur. Il accède à un compte privilégié pour modifier du contenu légitime existant de manière malveillante.





### 3/ Troisième scénario



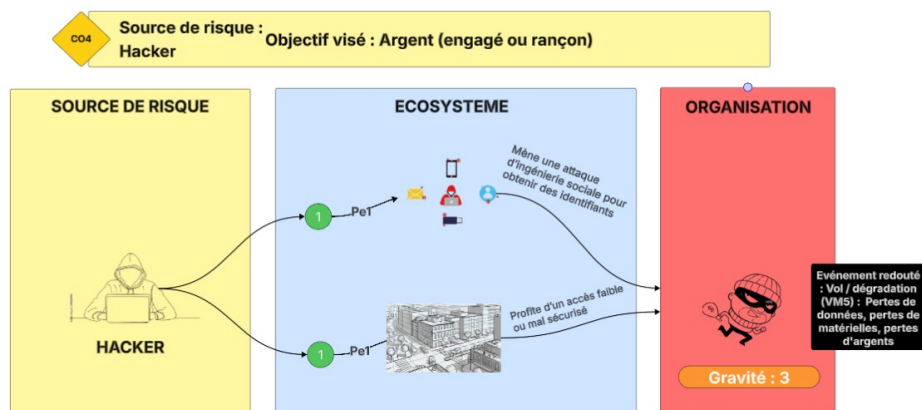
**Figure 3 : Scénario stratégique 3 – vengeur (client) visant à arnaquer/frauder le SAV**

Le schéma précédent décrit le troisième scénario stratégique. Il analyse par quel chemin stratégique un client mécontent qui chercherait à se venger et ayant pour but de frauder le Service Après-Vente (SAV) de notre site passerait pour arriver à ses fins. Nous avons isolé 2 chemins d'attaques par lesquels il pourrait atteindre son objectif.

Le premier chemin décrit une fausse réclamation auprès de notre SAV. Il met en jeu 2 parties prenantes : Wizards & Dice (S.I – Pe1) et client A (Cl1). Le client accède à notre SI par les accès à son compte. Il signale un faux problème sur une commande (ex : article non reçu ou défectueux) pour obtenir un remboursement ou un avoir.

Le deuxième chemin décrit une modification malveillante de données. Il met en jeux 2 parties prenantes : Wizards & Dice (S.I – Pe1) et client A (Cl1). Le client accède à notre SI par les accès à son compte. Il modifie une commande en cours (adresse, contenu...) dans un but frauduleux, pour détourner le colis ou en abuser.

### 4/ Quatrième scénario



**Figure 4 : Scénario stratégique 4 – hacker visant à générer de l'argent (par un service de hacking ou une rançon)**





Le schéma précédent décrit le quatrième et dernier scénario stratégique. Il analyse par quel chemin stratégique un hacker ayant pour but de nous voler de l'argent ou de dégrader l'infrastructure de notre site passerait pour arriver à ses fins. Nous avons isolé 2 chemins d'attaques par lesquels il pourrait atteindre son objectif.

Le premier chemin décrit une attaque par ingénierie sociale pour obtenir des identifiants. Il met en jeu 1 partie prenante : Wizards & Dice (S.I – Pe1). Le hacker accède à notre SI par un poste utilisateur/collaborateur. Il piège un employé (phishing) pour obtenir un accès interne pour ensuite supprimer/voler le contenu de notre base de données.

Le dernier chemin décrit l'exploitation d'un accès faible ou mal sécurisé. Il met en jeu 3 parties prenantes : Wizards & Dice (S.I – Pe1), prestataire d'accès interne (P3) et SaaS/Cloud (P4). Le hacker accède à notre SI par un accès aux fichiers ou à une base de données. Il déploie un malware ou ransomware sur le SI pour chiffrer les données critiques.





## V. Atelier 4 – Scénarios opérationnels

### Introduction de la section :

Cette section traite de l'atelier 4 de la méthode d'analyse de risques EBIOS.

- Éléments de compréhension des schémas : regroupe des éléments permettant la bonne compréhension des schémas opérationnels.
- Scénario opérationnel 1 : aborde le déroulé et explique la vraisemblance du premier scénario opérationnel.
- Scénario opérationnel 2 : aborde le déroulé et explique la vraisemblance du second scénario opérationnel.

### A) Éléments de compréhension des schémas

Avant de voir les schémas opérationnels que nous avons cartographiés, il est nécessaire de comprendre comment nous avons représenté cette cartographie.

Tout d'abord, chaque analyse se lit de gauche à droite, suivant le trajet de la source de risque choisie jusqu'à l'objectif visé, en passant par l'écosystème et soit par les systèmes des prestataires soit par le système de Wizards & Dice. Les étapes de chaque chemin d'attaque sont représentées par des flèches, symbolisant une méthode d'attaque, pointant des actions, symbolisant les points d'étapes de l'attaque.

De plus, chaque méthode et chaque action sont annotées d'un indice au format "VX", où X peut aller de 0 à 4. Cet indice illustre la vraisemblance de l'action : plus il est élevé, plus l'action paraît vraisemblable. Le tableau ci-dessous décrit plus précisément à quels niveaux correspond chaque indice :

NIVEAU DE VRAISEMLANCE	LÉGENDE	ÉGALE EN POURCENTAGE	DESCRIPTION
V4 : Très probable		90%	La source de risque atteindra presque à coup sûr son objectif, dépendant de sa méthode pour y arriver. <b>La probabilité que le scénario se réalise est très élevée.</b>
V3 : Très vraisemblable		75%	Il est très probable que la source de risque atteigne son objectif, dépendant de sa méthode pour y arriver. <b>La probabilité que le scénario se réalise est élevée.</b>
V2 : Vraisemblable		50%	La source de risque a de bonnes chances d'atteindre son objectif, dépendant de sa méthode pour y arriver. <b>La probabilité que le scénario se réalise est significative.</b>
V1 : Peu Vraisemblable		25%	La source de risque a peu de chances d'atteindre son objectif par, dépendant de sa méthode pour y arriver. <b>La probabilité que le scénario se réalise est faible.</b>
V0 : Invraisemblable		10%	Il est très improbable que la source de risque atteigne son objectif, peu importe les moyens utilisés. <b>La probabilité que le scénario se réalise est très faible.</b>

**Figure 5: Tableau des indices de vraisemblances**





## B) Scénario opérationnel 1

### 1/ Déroulé

Le premier schéma opérationnel que nous avons décidé d'analyser est disponible à la page 24. Nous avons décidé de l'isoler afin qu'il puisse être visible avec la meilleure qualité possible.

Ce schéma décrit un concurrent qui pourrait bloquer le site. Nous avons dégagé trois chemins par lesquels il pourrait atteindre cet objectif :

- Par la corruption d'un des employés de nos prestataires.  
À partir de là, le concurrent peut utiliser la personne corrompue pour accéder au réseau, injecter du code malveillant dans les services que nous vend le prestataire, bloquant ainsi le service, entraînant le blocage du site.  
Il pourrait également avoir corrompu un employé de notre fournisseur d'accès Internet (FAI), faire pression sur lui pour couper le réseau de notre infrastructure, entraînant le blocage du site.
- Par l'achat de service malveillant sur le dark web.  
À partir de là, le concurrent aura acheté les services d'un hacker, qui aura de multiples options pour agir. Il pourrait user de botnets d'avis négatifs pour s'attaquer à la confiance que nous porte notre prestataire de paiement. Si ce dernier perd trop confiance en nous, il rompra ses services, entraînant le blocage du site.  
Si le hacker décide de cibler l'adresse IP publique du site Wizards & Dice, il peut pratiquer un IP spoofing, usurpant notre adresse et se servant d'une fausse version de notre site pour blacklister Wizards & Dice. Cela perturberait le bon fonctionnement du site, entraînant son blocage.  
Toujours en ciblant l'adresse IP publique du site, mais aussi en ciblant l'adresse IP publique de notre pare-feu UTM, il pourrait lancer une attaque par DDoS. Cela aussi perturberait le fonctionnement du site, entraînant son blocage.  
Enfin, il pourrait accéder au site et utiliser des méthodes d'escalade de privilèges pour créer une backdoor et/ou un faux compte admin. Il pourrait ainsi accéder ultérieurement aux éléments de notre infrastructure. Il essaiera sûrement de détruire notre site ou de supprimer nos bases de données, entraînant le blocage du site.
- Par des techniques d'ingénierie sociale, telles que le phishing.  
À partir de là, le concurrent aura probablement récupéré les identifiants d'un compte. Si le compte n'a pas suffisamment d'accès, il essaiera d'effectuer une escalade de privilèges. Une fois des droits suffisants en sa possession, il pourrait créer une backdoor et/ou un faux compte admin pour accéder ultérieurement aux éléments de notre infrastructure. Cela dit, il essaiera sûrement de détruire notre site ou de supprimer nos bases de données, entraînant le blocage du site.

### 2/ Vraisemblance

Sur un plan général, ce scénario opérationnel est hautement vraisemblable. En effet, seules quelques actions et méthodes ont un indice V2 ou inférieur. Cela dit, nous pouvons noter que le chemin d'attaque par lequel le concurrent achèterait les services d'un hacker pour cibler l'IP publique du serveur web puis dégraderait la réputation de l'adresse IP publique du serveur web est le moins probable de tous.







## C) Scénario opérationnel 2

### 1/ Déroulé

Le second schéma opérationnel que nous avons décidé d'analyser est disponible à la page 25. Nous avons décidé de l'isoler afin qu'il puisse être visible avec la meilleure qualité possible.

Ce schéma décrit comment un hacker qui pourrait voler ou dégrader nos données. Nous avons dégagé trois chemins par lesquels il pourrait atteindre cet objectif :

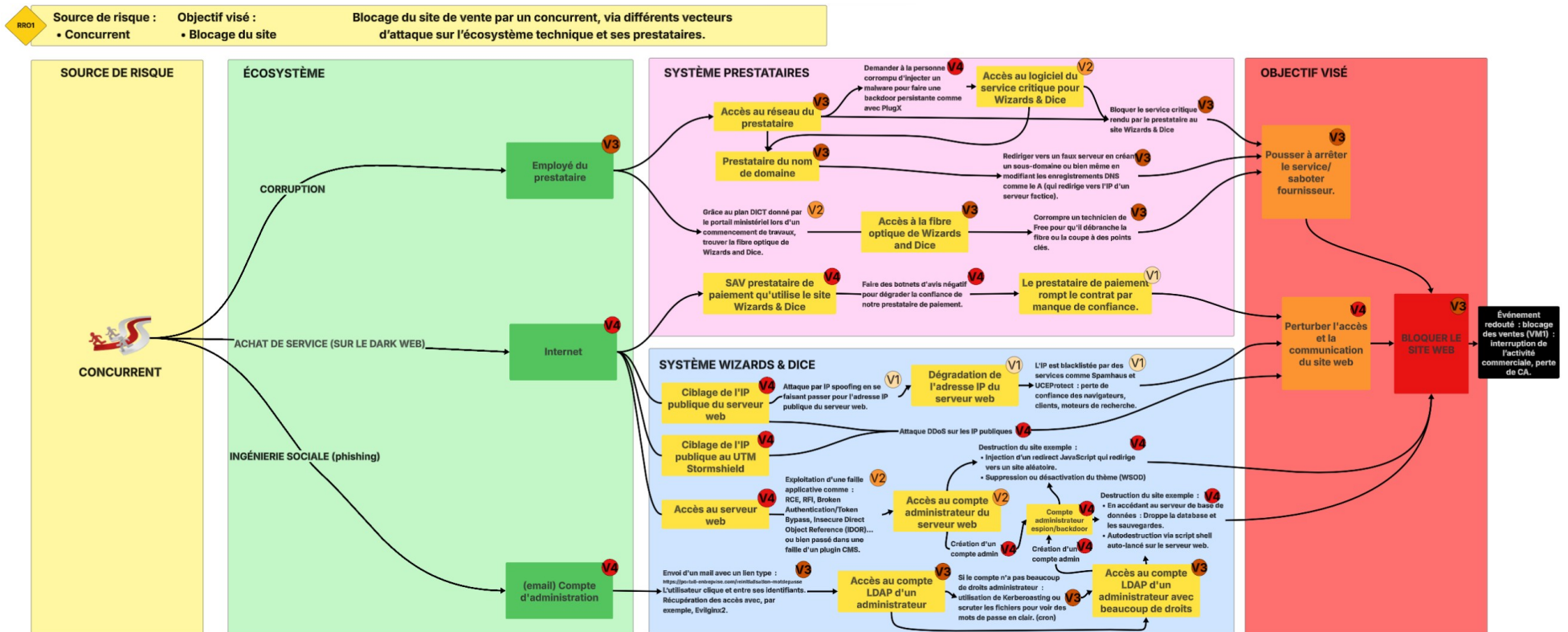
- Par la corruption d'un des employés de nos prestataires.  
À partir de là, le hacker peut utiliser la personne corrompue pour injecter du code malveillant via les services que nous vend le prestataire, se créant ainsi un backdoor. Ensuite, plusieurs options de méthodes résultant au vol de nos données s'offrent à lui, lui permettant d'atteindre son objectif.
- Par le scan et la recherche, accédant au serveur web de Wizards & Dice.  
À partir de là, le hacker pourrait accéder au site, exploiter une faille pour accéder au compte administrateur du site. Ensuite, il peut user de diverses méthodes pour voler et/ou détruire nos données, atteignant son objectif.
- Par le scan et la recherche, accédant à l'interface de notre pare-feu StormShield.  
À partir de là, le hacker pourrait accéder à l'interface d'administration du pare-feu StormShield, effectuer une attaque de brute force ou exploiter une vulnérabilité pour accéder au compte administrateur du site. Ensuite, il peut user de diverses méthodes pour voler et/ou détruire nos données, atteignant son objectif.
- Par des techniques d'ingénierie sociale, telles que le phishing.  
À partir de là, le hacker aura probablement récupéré les identifiants d'un compte. Si le compte n'a pas suffisamment d'accès, il essaiera d'effectuer une escalade de privilèges. Une fois des droits suffisants en sa possession, il pourrait créer une backdoor et/ou un faux compte admin pour accéder ultérieurement aux éléments de notre infrastructure. En plus de cela, le hacker pourrait mettre en place un ransomware pour bloquer les données. Cela dit, il volera nos données ou les détruira, lui permettant d'atteindre son objectif.

### 2/ Vraisemblance

Sur un plan général, ce scénario opérationnel est hautement vraisemblable. En effet, seules quelques actions et méthodes ont un indice V2 ou inférieur. Cela dit, nous pouvons noter que le chemin d'attaque par lequel le hacker accède à l'interface de StormShield et obtient les comptes administrateur de l'UTM est le moins probable de tous.



## Wizards & Dice Analyse de risques



**Figure 6 : Scénario opérationnel d'un concurrent cherchant à bloquer le site web**



# Wizards & Dice Analyse de risques

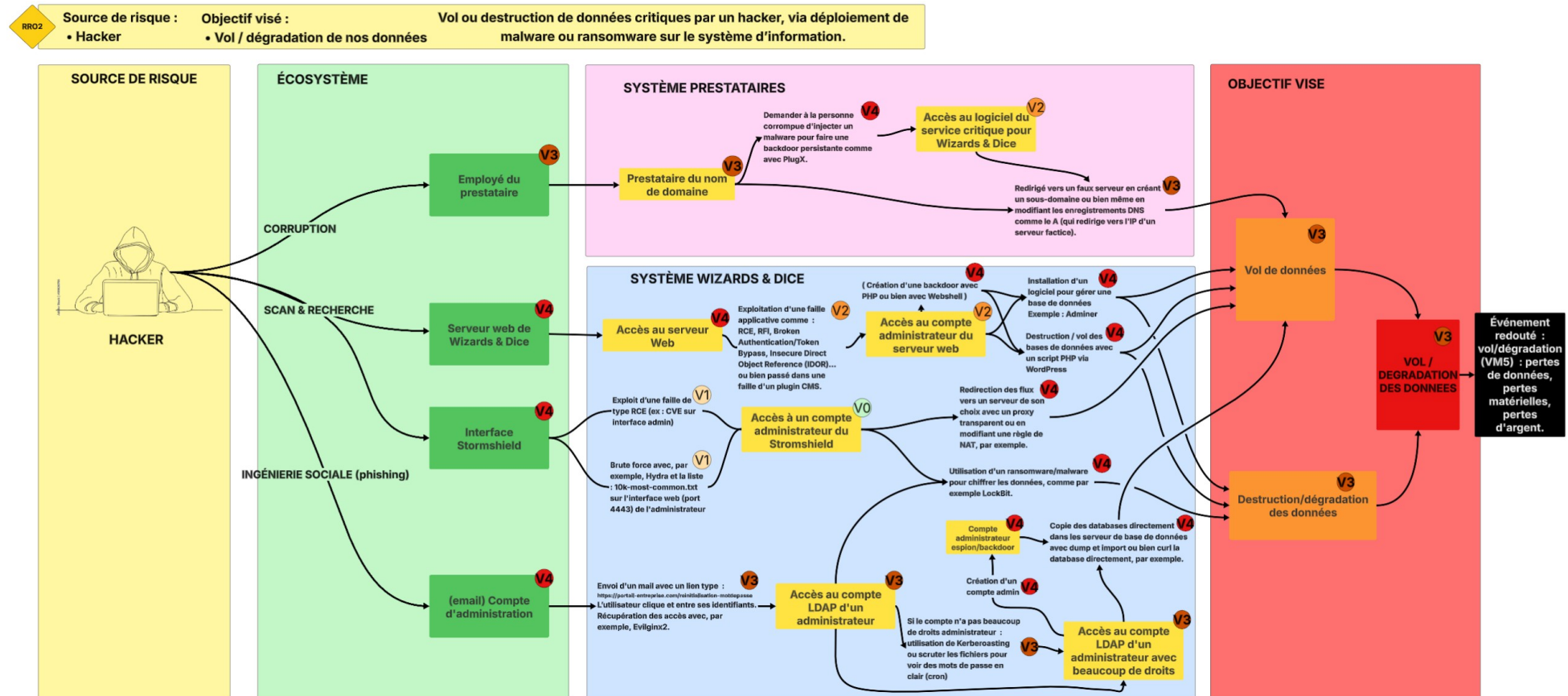


Figure 7 : Scénario opérationnel d'un hacker cherchant à voler et/ou détruire nos données





## VI. Atelier 5 – Traitement du risque

### Introduction de la section :

Cette section traite de l'atelier 5 de la méthode d'analyse de risques EBIOS.

- Cadre de l'atelier et criticité : rappelle le cadre de l'atelier et les niveaux de criticités.
- Traitement du risque : regroupe les mesures pour traiter les risques mis en avant pour le scénario opérationnel.
- Autres aspects de l'atelier : aborde les autres aspects de l'atelier qui ne seront pas trop détaillés.

### A) Cadre de l'atelier et criticité

Dans le cadre de l'analyse EBIOS RM pour le projet Wizards & Dice, des scénarios stratégiques ont été identifiés comme particulièrement critiques. Ces scénarios ont été traduits en scénarios opérationnels (2 scénarios opérationnels) pour évaluer leur vraisemblance et prioriser les actions à mettre en place.

Le scénario lié au blocage du site par un concurrent présente une gravité élevée (4) et une vraisemblance forte (3), ce qui en fait un risque initial majeur (R1) à traiter en priorité. De même, le scénario impliquant un hacker visant un vol ou une dégradation présente une gravité significative (3) pour une vraisemblance modérée (2), correspondant au risque initial R2.

Il est donc nécessaire de comprendre comment nous classifions le niveau de risques, déterminé par le niveau de gravité et de vraisemblance.

		Vraisemblance			
Gravité		1- Limitées	2- Modérée	3- Élevée	4- Signifi- catives
	4- Signifi- cative	Risque tolérable	Risque tolérable	Risque inacceptable	Risque inacceptable
	3- Élevée	Risque tolérable	Risque tolérable	Risque inacceptable	Risque inacceptable
	2- Moyenne	Risque acceptable	Risque tolérable	Risque tolérable	Risque tolérable
	1-Faible	Risque acceptable	Risque acceptable	Risque tolérable	Risque tolérable

Cette matrice de criticité permet de visualiser l'évaluation des scénarios de risque, en croisant deux axes : la gravité de l'impact (vertical) et la vraisemblance de sa survenue (horizontal). On distingue trois zones de priorité d'action :

- Zone rouge – Risque inacceptable : nécessite un traitement immédiat. Par exemple, le scénario R1 (concurrent – blocage du site) a un niveau de risque inacceptable en raison de sa forte gravité (4) et de sa vraisemblance élevée (3).
- Zone orange – Risque tolérable : des mesures correctives sont à prévoir. Les scénarios R2, R3 et R4 s'y trouvent, signalant un risque à surveiller de près mais sous contrôle si les traitements sont bien appliqués.
- Zone verte – Risque acceptable : aucun traitement prioritaire n'est requis, un simple suivi est suffisant.







Des mesures de remédiation ont été envisagées pour chaque situation, permettant de réduire les niveaux de menace : le scénario concurrent passe alors en R3, et le scénario hacker en R4, représentant leur niveau de risque résiduel après application des protections. Ces ajustements permettent de mieux cibler les efforts de sécurité et d'aligner les ressources avec les priorités identifiées.

## B) Traitement du risque

### 1/ Premier scénario opérationnel

Pour rappel, le premier scénario opérationnel est le blocage du site de vente par un concurrent, via différents vecteurs d'attaque sur l'écosystème technique et ses prestataires.

Ce scénario opérationnel décrit un cas où le concurrent cherche à rendre le site de vente inaccessible dans le but d'interrompre l'activité commerciale. Il utilise différentes méthodes : attaque DDoS, sabotage d'un prestataire, usurpation d'adresse IP publique, attaque par ingénierie sociale sur un fournisseur ou un collaborateur. Les vulnérabilités résiduelles susceptibles d'être exploitées dans ce scénario :

- Faible résilience DDoS de certains prestataires (P3, P4)
- Faible sécurisation de comptes utilisateurs ou administrateurs.
- Faible redondance DNS ou cloud SaaS
- Dépendance critique à quelques prestataires

Il est à noter que d'autres causes ou facteurs aggravants peuvent jouer dans ce scénario, tels que le manque de visibilité sur les sous-traitants des prestataires (chaîne d'approvisionnement), un Service-Level Agreement (SLA) non précis ou trop peu contraignant, ou l'absence d'un Security Operations Center (SOC) ou de monitoring en temps réel. L'événement redouté concerné est le blocage des ventes (ER2 – impacte la VM1), qui peut engendrer une interruption de l'activité commerciale et une perte de chiffre d'affaires.

Les mesures de traitement du risque existantes au sein de notre infrastructure sont les règles de pare-feu applicatif (Stormshield) avec anti-DDoS, la surveillance basique du réseau et l'authentification renforcée pour l'accès au SI interne.

Les mesures de traitement du risque complémentaires qui pourraient être déployées dans notre infrastructure sont les suivantes :

- Mise en place d'un CDN avec capacité anti-DDoS.
- Redondance DNS et cloud SaaS.
- Clauses SLA avec obligation de continuité de service.
- Audit de la surface d'exposition publique (IP, DNS).
- Formation des employés contre l'ingénierie sociale.
- Surveillance proactive de l'image du site (monitoring uptime).







Nous évaluons donc le risque résiduel ainsi :

		Gravité	Vraisemblance	Niveau de risque initial
Status	Initiale	Élevée	Élevée	Risque inacceptable
	Résiduelle	Élevée	Limitées	Risque tolérable

Pour gérer ces risques résiduels, nous avons pensé à mettre en place les mesures suivantes :

- Suivi régulier des engagements contractuels des prestataires.
- Tests de montée en charge et exercices de crise.
- Intégration d'outils de supervision SI avec alertes automatiques.
- Mise à jour régulière du plan de continuité d'activité (PCA).

## 2/ Deuxième scénario opérationnel

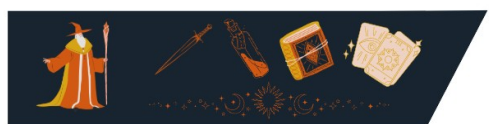
Pour rappel, le deuxième scénario opérationnel est le vol ou la destruction de données critiques par un hacker, via déploiement de malware ou de ransomware sur le système d'information.

Ce scénario opérationnel décrit un cas où le hacker cherche à compromettre la disponibilité ou l'intégrité des données critiques de l'entreprise. Il peut le faire via une compromission d'accès (brute force, attaque via service exposé, vol d'identifiants), puis le déploiement d'un ransomware ou malware pour chiffrer ou exfiltrer des fichiers sensibles. Le point d'entrée peut venir d'un poste utilisateur, d'un service mal sécurisé (P4 – Cloud, P3 – Accès Internet) ou d'un prestataire indirectement visé. Les vulnérabilités résiduelles susceptibles d'être exploitées dans ce scénario :

- Faible cloisonnement du SI interne.
- Services exposés accessibles via IP publique.
- Utilisation d'identifiants faibles ou partagés.
- Accès trop large pour certains comptes d'administration.
- Absence d'antivirus ou de protection sur certains points d'entrée.

Il est à noter que d'autres causes ou facteurs aggravants peuvent jouer dans ce scénario, tels que l'absence de sauvegarde hors ligne ou chiffrée, le manque de journalisation des accès, l'absence de politique de mot de passe renforcée et l'absence de segmentation réseau entre services critiques et le reste du SI. L'événement redouté concerné est le vol ou la dégradation (ER1 – impacte les VM2 et 3), qui peut engendrer une perte ou une indisponibilité des données et un impact financier et/ou juridique.

Les mesures de traitement du risque existantes au sein de notre infrastructure sont la restriction d'accès SSH et l'authentification renforcée, la mise en place d'un antivirus sur les postes utilisateurs et la sauvegarde quotidienne automatique (locale).





Les mesures de traitement du risque complémentaires qui pourraient être déployées dans notre infrastructure sont les suivantes :

- Sauvegarde hors ligne chiffrée et rotation régulière.
- Segmenter le réseau (DMZ, VLAN spécifiques).
- Restreindre les droits administrateurs.
- Scanner de vulnérabilités automatique (avec alertes).
- Journalisation et supervision des accès sensibles.
- Campagne de sensibilisation contre les pièces jointes piégées/phishing.

Nous évaluons donc le risque résiduel ainsi :

		Gravité	Vraisemblance	Niveau de risque initial
Status	Initiale	Élevée	Modérée	Risque tolérable
	Résiduelle	Élevée	Limitées	Risque tolérable

Pour gérer ces risques résiduels, nous avons pensé à mettre en place les mesures suivantes :

- Vérification régulière des logs d'accès/alertes de l'antivirus.
- Simulation d'intrusion ou test de restauration des sauvegardes.
- Revue trimestrielle des comptes à privilèges.
- Mise à jour des procédures en cas de compromission (PRA/PCA).
- Test de restauration mensuel.

## C) Autres aspects de l'atelier

L'atelier 5 est normalement composé d'autres éléments, tels que le plan de traitement du risque ou encore le cadrage du suivi des risques. De plus, les éléments de stratégie de traitement de risques devraient normalement être plus détaillés, tout comme la synthèse des risques résiduels. Bien que les deux derniers points figurent en partie pour chacun des scénarios opérationnels abordés, nous avons choisi de ne pas détailler les points précédents.

En effet, le sujet de cette analyse porte spécifiquement sur les éléments cités en introduction et au cours de l'atelier 1. Les autres points étant hors du cadre défini plutôt, nous avons jugé qu'il n'était pas nécessaire de les traiter. Cela nous a permis de concentrer nos efforts sur d'autres éléments de cette analyse de risques.





## VII. Conclusion

L'analyse de risques réalisée pour le projet Wizards & Dice a permis d'identifier de manière structurée les principales menaces pesant sur notre infrastructure, en suivant rigoureusement la méthode EBIOS Risk Manager. Au fil des ateliers, nous avons cadré le périmètre technique et métier, évalué les sources de risques pertinentes, construit des scénarios stratégiques et opérationnels réalistes, et proposé des mesures de traitement adaptées.

Notre étude a mis en lumière deux risques majeurs : le blocage du site de vente par un concurrent et le vol ou la dégradation de données critiques par un acteur malveillant. Ces risques, classés initialement comme "inacceptables" ou "tolérables", ont fait l'objet de plans de traitement précis, visant à réduire leur vraisemblance et à renforcer la résilience globale du projet. Les mesures proposées — telles que la mise en place de CDN anti-DDoS, la segmentation réseau, ou encore la sensibilisation des collaborateurs aux attaques par ingénierie sociale — permettront de diminuer efficacement l'exposition aux menaces les plus critiques.

Par ailleurs, l'adoption d'un socle de sécurité fondé sur le RGPD, le PCI-DSS et les recommandations de l'ANSSI a fourni un cadre solide pour évaluer et justifier nos choix de sécurité. Ces référentiels, bien que non appliqués de manière exhaustive à ce stade du projet, ont constitué une référence précieuse pour orienter nos décisions.

Cette analyse a aussi montré l'importance d'un suivi régulier de la menace et de l'état du système d'information. Une simple analyse ponctuelle ne saurait suffire : il sera nécessaire, dans le futur, d'intégrer un cycle continu d'amélioration de la sécurité, en tenant compte des évolutions technologiques et des nouvelles menaces.

Enfin, bien que la contrainte de temps nous ait conduits à simplifier certains aspects (notamment le traitement détaillé des risques résiduels), l'ensemble de cette analyse constitue une base solide pour renforcer la sécurité de Wizards & Dice. En nous concentrant sur les risques les plus critiques et en proposant des mesures pragmatiques, nous avons posé les fondations d'une infrastructure fiable, capable de soutenir l'activité et la croissance du projet à long terme.

