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 évènements 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 évènements 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.

		Vraisemblance			
		Invraisemblable	**Vraisemblable**	**Très vraisemblable**	**Quasiment certain**
Gravité	**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 évènements redoutés pour déduire la pertinence de chaque évènement redouté. Les valeurs métiers impactées apparaissent également pour plus de clarté.

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

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.

II. Formalisation des workflow

Introduction de la section :
Cette section rappelle de façon synthétique les workflow que l'équipe projet suit afin à travailler de manière cohérente et unifié

- Organisation interne : traite du planning, des tâche, des incidents, des ressources financières de l'équipe et des tickets
- Communication entre les membres : aborde les façon de communiquer entre membre
- Bonnes pratiques : rassemble les pratiques à suivre pour se faciliter la vie tout au long du projet

A) Organisation interne

1/ Planning

Consulter le planning organisationnel :

Le planning organisationnel du projet est présent au chemin suivant dans l'arborescence de fichiers du projet :
GestionDeProjet\GestionInterne\Planning Organisationnel

En accord avec ce qui a été décidé par les membres du projet, seul le chef de projet à l'autorisation de modifier ce fichier, afin d'éviter les changements arbitraires et les confusions dans l'avancé des différentes tâches. Les autres membres ne doivent donc **EN AUCUN CAS** modifier le planning eux-même. Pour apporter quelconque modification il faut passer par les tickets Taïga (voir paragraphes suivants)

Quant un membre du projet ne souhaite que consulter le planning organisationnel, il peut donc l'ouvrir mais il ne doit surtout **pas enregistrer les changements** au moment de la fermeture de celui-ci.

2/ Tâches

Avancement d'une tâche au cours du projet :

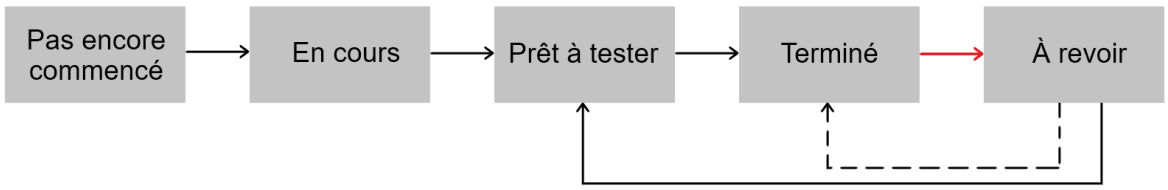

Figure 1 : Étapes d'avancements d'une tâche / sous-tâche au cours du projet

Légende :

- Flèche rouge : changement d'état en cas de problème post complétion de la tâche
- Flèche pointillé : changement mineur (ne nécessitant pas des tests approfondis)

4/ Règle de nommage des documents

Exemple de fichier respectant la règle de nommage : Vente_ListeDeTestsA-Faire_v1-5.pdf
Règle de nommage :

- Utiliser le titre du documents :
  Il doit tenir sur les lignes prévues par le template. Il peut être moins long, mais ne doit pas être plus long

- Utiliser le format suivant :
  - Majuscule en début de chaque mot, minuscules partout ailleurs
  - Pas d'espaces ni de caractères accentués
  - Utiliser "-" pour les séparations de lisibilité ("à traiter" devient "A-Traiter")
  - Utiliser "_" pour les séparations de sens (concepts, idées, etc)

  ⇒ Ainsi, dans l'exemple, le titre du document est : "Vente – Liste de tests à faire" Il devient donc "Vente_ListeDeTestsA-Faire"
- Ajouter la version à la fin, sous ce format : "_vX-Y"
  Voir à la section II. C) 3/Templates de documents, au paragraphe "Versionnage", pour plus de détails sur le versionnage des documents

5/ Bonnes pratiques de rédaction

Plusieurs éléments aident à l'uniformité des documents de l'équipe :

- Lien hypertexte
  Éviter les liens hypertextes "crus", c'est-à-dire sous la forme d'une URL classique du type "https://www.youtube.com/".
  Utiliser les options de l'éditeur de texte pour transformer le texte d'apparence du lien en quelque chose de clair, de concis et d'intelligible (ici avec Youtube)
  www.youtube.com/"

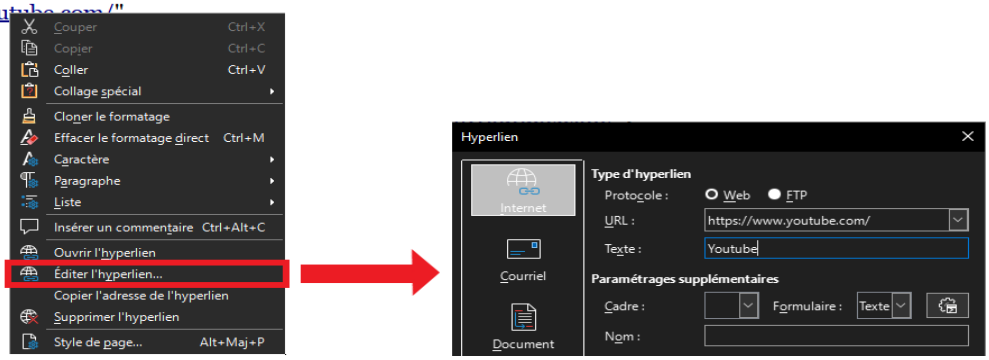

Figure 5 : Édition d'un lien hypertexte

- Privilégier les guillemets universels (⇒ "abc") plutôt que les guillemets traditionnels (⇒ « abc »). Les options d'auto-correction grammaticale sont présente dans tous les éditeurs de textes.
- Quand un fichier, un répertoire ou un chemin de l'arborescence est mentionné dans un document, formater cette mention en italique.

  Quand on mentionne un fichier particulièrement, il n'est pas nécessaire de préciser sa version, au vue de la nature changeante de celle-ci

Exemple :
  - *SyntheseDesMethodesDeTravail.pdf*
  - *wizards-n-dices/GestionDeProjet/SyntheseDesMethodesDeTravail.pdf*
- Pour écrire du code dans un document :
  - Privilégié une partie "Annexes" le plus souvent possible. Dans le cas contraire, utiliser une "zone de texte"
  - Police : Consolas
  - Taille : 8
  - Pas d'accentuation des caractères (gras, italique, souligner, etc.)
  - Respecter les indentations et les lignes le plus souvent possible
- Notes générales
  - Ne pas sur-utiliser les accentuations des caractères : (gras, italique, souligner, …)
    → Si tout est "important", plus rien ne l'est vraiment
  - Rester flexibilité …
    Les templates sont jolis, mais ce sont des références avant tout. Modifier quelques légers détails intelligemment peuvent rehausser le niveau de finition des documents et les rendre plus agréables, cohérents et lisibles
    Par exemple :
    - Réduire la police de 1 à 2 points pour faire rentrer un image dans la page
    - Sautez plus de lignes
    - Reformuler pour faire tenir le texte sur une seule ligne
      etc
  - … tout conservant de la rigueur :
    Étant donné l'ampleur du projet, il est nécessaire de faire preuve de **RIGUEUR**
    - Pas de majuscule à des endroits inappropriés
    - Faire des phrases
    - Évitez les mots et les tournures de phrases familières
      Le mot d'ordre ici, c'est d'**être professionnel** dans nos méthodes de travail

6/ Rigueur technique

Quand un membre de l'équipe travaille sur des éléments techniques, il lui est vivement recommandé de prendre en note ce qui vient d'être fait. Il n'est pas demandé d'être précis à la commande prête, mais plutôt de garder une tracesoit des modifications apportées à la configuration existante soit des éléments déployées pendant une première configuration.

Pour faciliter cette prise de notes, un template au format TXT est disponible dans le répertoire associé de l'arborescence. Avant de créer un document, les membres sont priés de vérifier s'il n'existe pas déjà un document de prise de notes relative au sujet qu'ils veulent traiter. De plus, le format TXT permet un versionnage facile au début du contenu du fichier : il est recommandé de bien garder ce versionnage à jour