

ARIMES - DOCUMENTATION UTILISATEUR

Interlocuteur ADACIS sur ce dossier : Christophe MAILLET

Titre	ARIMES – Fiche technique – Documentation utilisateur
Version	V 1.5
Classification	C0-Public
Reference	[ARI-UTI]

Versions du document

Version	Date	Auteur	Description
0.1	11/06/2020	Mathieu Brulin	Création du document
1.0	21/07/2020	Christophe Maillet	Version initiale
1.1	07/10/2020	Matthieu Renard	Mise à jour suite à l'ajout de nouvelles fonctionnalités
1.2	18/12/2020	Matthieu Renard	Ajout de quelques précisions (cartographie de menace numérique, mesures de sécurité de l'écosystème).
1.3	22/12/2020	Matthieu Renard	Ajout de précisions sur le mode revue de risques de l'activité 5.2
1.5	23/04/2021	Matthieu Renard	Révision de la documentation suite aux évolutions de l'application. Version de l'application Arimes V1.0
1.5	21/07/2021	Margaux Maillet	Ajout de la procédure de démarrage

Diffusion du document

Date	Destinataire	Pour information	Pour application	Pour validation
21/07/2021	C Maillet			X
21/07/2021	Utilisateurs		X	

TABLE DES MATIERES

1.	Introduction	4
2.	Procédure de Demarrage	5
2.1.	Installation de l'application Arimes	5
2.1.2.	Démarrer l'installation	6
2.2.	Utiliser le fichier de test.....	7
3.	Présentation générale	8
3.1.	Généralités	8
3.2.	Fenêtre de l'application	8
3.2.1.	Minimiser, maximiser, fermer ou redimensionner la fenêtre	8
3.2.2.	Action sur les onglets de l'application	8
3.2.3.	Action sur les tableaux de l'application	9
3.3.	Boutons de l'application	10
3.3.1.	Portées et info-bulles des boutons de l'application.....	10
3.3.2.	Description des boutons.....	10
4.1.	Vision globale de l'onglet accueil	12
4.2.	Sélection de la langue de l'application	12
5.	Atelier 1 – Cadrage et socle de sécurité	13
5.1.	Activité 1.1 – Définir le cadre de l'étude	14
5.2.	Activité 1.2 – Définir le périmètre métier et technique	15
5.3.	Activité 1.3 – Identifier les événements redoutés et évaluer leur niveau de gravité	16
5.4.	Activité 1.4 – Déterminer le socle de sécurité.....	17
6.	Atelier 2 Sources de Risques / Objectifs Visés	18
6.1.	Vue configuration.....	18
6.2.	Activité 2.1 Identifier les sources de risques et objectifs visés.....	18
6.3.	Activité 2.2 Evaluer les couples Source de Risque/Objectif Visé.....	19
6.4.	Activité 2.3 Sélectionner les couples SR/OV	19
7.	Atelier 3 Scénarios stratégiques	20
7.1.	Vue configuration.....	20
7.2.	Activité 3.1 Construire la cartographie.....	21
7.3.	Activité 3.2 Scénarios stratégiques	22
7.4.	Activité 3.3 Définir les mesures de sécurité.....	23
8.	Atelier 4 Scénarios opérationnels	24
8.1.	Vue configuration.....	24
8.2.	Activité 4.1 Elaborer les scénarios opérationnels	25
8.3.	Activité 4.2 Evaluer la vraisemblance des scénarios opérationnels	26
9.	Atelier 5 Traitement du risque	27
9.1.	Vue configuration.....	27
9.2.	Activité 5.1 Réaliser une synthèse des scénarios de risque	28
9.3.	Activité 5.2 Stratégie de traitement du risque	29
10.	Fenêtres contextuelles.....	31
10.1.	Fenêtre d'ajout ou de modification d'un élément	31
10.2.	Fenêtre de filtre	32
10.3.	Fenêtre d'export	34

10.3.1.	Export pour rendu (rapport).....	34
10.3.2.	Export pour import	35
10.4.	Fenêtre d'import.....	36
10.5.	Fenêtre de versions.....	37
11.	Import de données utilisateur	38
11.1.	Import d'exigences	38
11.2.	Import de la métrique de cotation de l'atelier 2	39
11.3.	Import de critères de cotation des parties prenantes (atelier 3)	40
11.4.	Import des catégories de parties prenantes (activité 3.1).....	41
11.5.	Import de la métrique de cotation de l'atelier 4	42
11.6.	Généralités sur les imports CSV utilisateur.....	43

1. INTRODUCTION

Ce document a pour objectif de présenter l'application ARIMES – logiciel d'appréciation et de traitement des risques numériques selon la méthode EBIOS *Risk Manager*.

Pour toutes questions sur la méthodologie, deux liens utiles

<https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/>

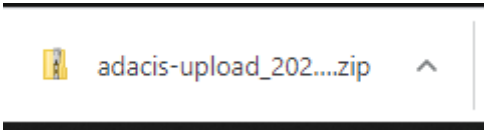
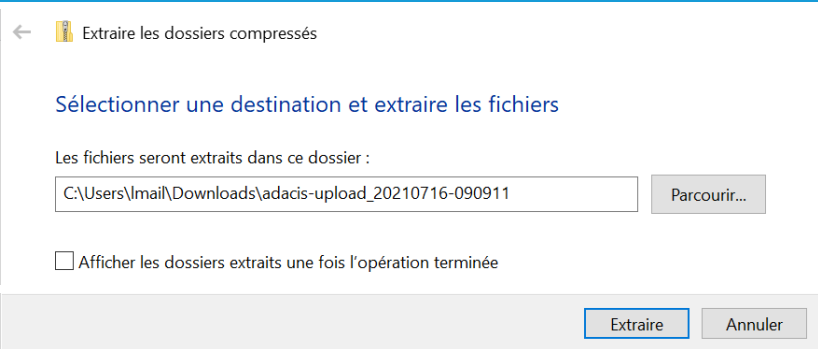
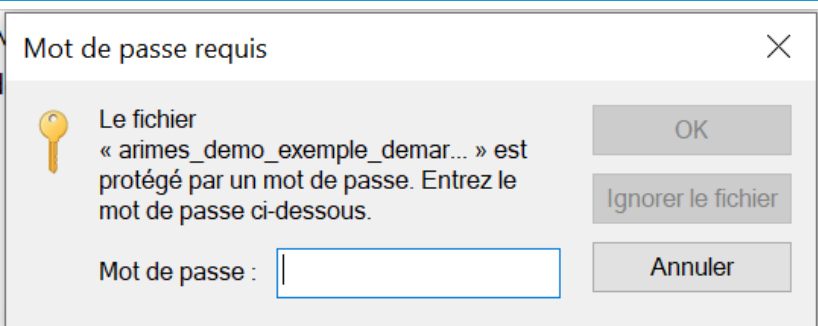
<https://club-ebios.org/site/faq/>

La documentation concerne la version V1.0 de l'application.

2. PROCEDURE DE DEMARRAGE

2.1. Installation de l'application Arimes

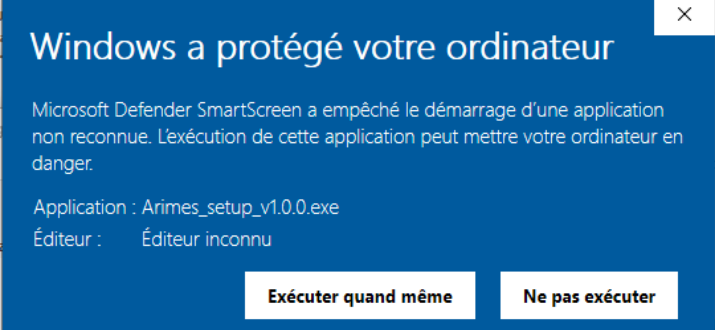
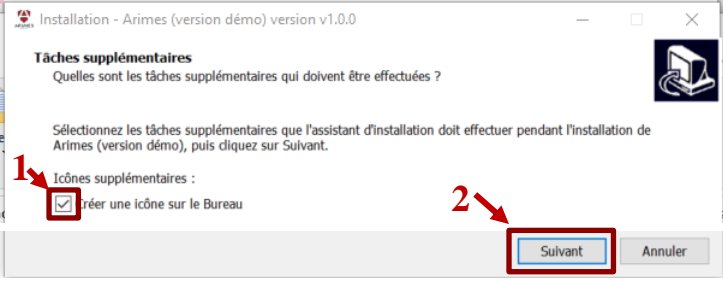
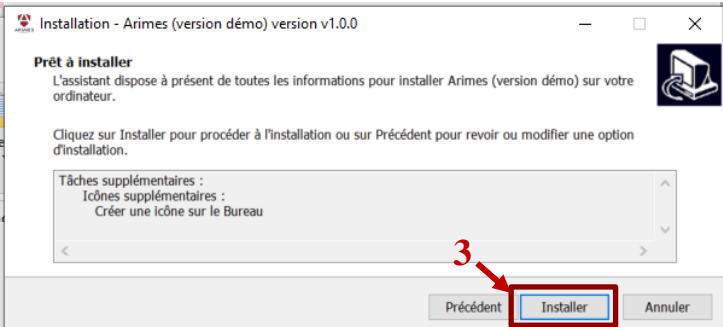
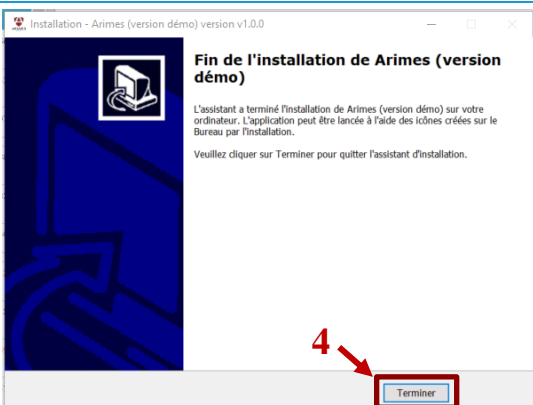
2.1.1. Téléchargement du dossier

Téléchargement de l'appli	
Actions à réaliser	Description
https://secureupload.adacis.net/download/XSntwrXXXXXXXXXX/XXXXXXXXXXXXXXXXXXXX/adacis-upload_20210716-090911.zip	Cliquer sur le lien donné
	Un dossier de ce type est téléchargé
	Dézipper le dossier
 <p>Mdp : ZJkJOXXX</p>	Entrer le mot de passe donné

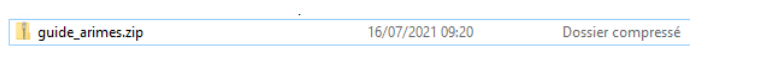

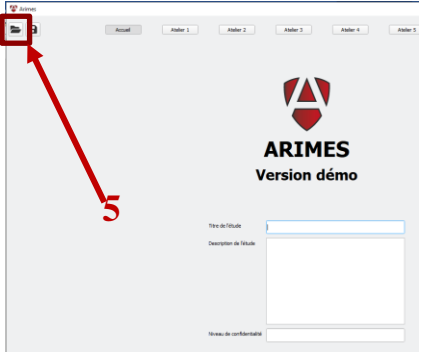
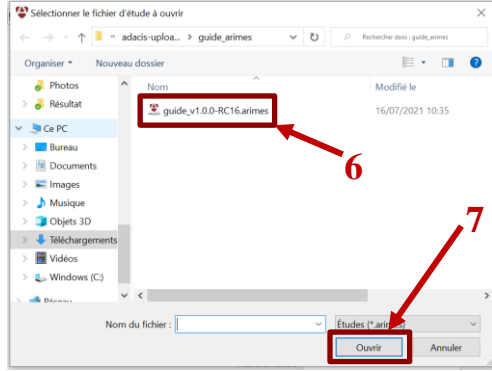
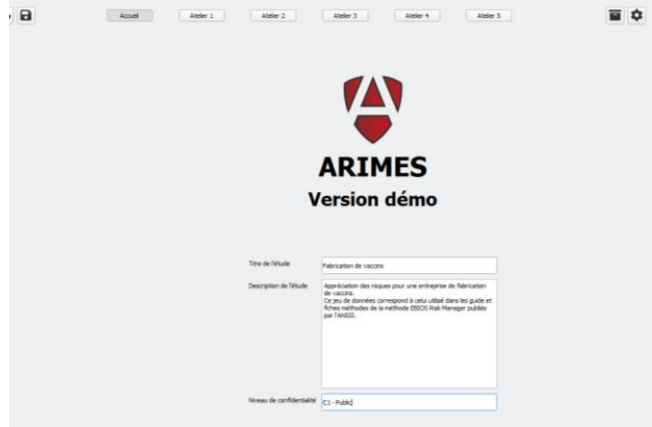
Le fichier qui est téléchargé comporte :

- Arimes_demo_exemple_demarrage.zip : Ce dossier comporte l'exécutable d'Arimes.
- ARIMES-Documentation_Utilisateur_v1.4.pdf : Ce fichier explique comment utiliser le logiciel Arimes ainsi que ses différentes fonctionnalités.
- Guide_arimes.zip : Ce dossier comporte l'exemple d'analyse de risque donné par l'ANSSI pour comprendre les différentes imbrication du logiciel Arimes.

2.1.2. Démarrer l'installation

Généralités – Tableaux de l'application			
Actions disponibles		Description	
Nom	Modifié le	Type	Dézipper le dossier « arimes_demo_exemple_demaarrage.zip »
arimes_demo_exemple_demarrage.zip	16/07/2021 09:20	Dossier compressé	
Nom	Modifié le	Type	Double cliquer sur le fichier : « Arimes_setup_v1.0.0.exe »
Arimes_setup_v1.0.0.exe	16/07/2021 10:07	Application	
			Si une pop-up de protection Windows apparaît, alors cliquer sur « Exécuter quand même »
			La pop-up d'installation s'ouvre. 1/ Cocher la case pour la création d'un icône 2/ Cliquer sur « Suivant »
			3/ Cliquer sur « Installer » Le téléchargement va s'effectuer
			4/ Cliquer sur « Terminer »

2.2. Utiliser le fichier de test

Généralités – Boutons de l'application		Description						
		Dézipper le dossier « guide_arimes.zip ».						
<table border="1"> <thead> <tr> <th>Nom</th> <th>Modifié le</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>guide_v1.0.0-RC16.arimes</td> <td>16/07/2021 10:28</td> <td>Fichier ARIMES</td> </tr> </tbody> </table>		Nom	Modifié le	Type	guide_v1.0.0-RC16.arimes	16/07/2021 10:28	Fichier ARIMES	Ce fichier est extrait.
Nom	Modifié le	Type						
guide_v1.0.0-RC16.arimes	16/07/2021 10:28	Fichier ARIMES						
		Ouvrir Arimes, en double cliquant sur l'icône du Bureau.						
		5/ Cliquer sur le petit icône « Ouvrir une étude »						
		6/ Sélectionne le fichier Arimes « guide_v1.0.0-R16.arimes » 7/ Cliquer sur « Ouvrir »						
		L'étude est téléchargée dans le logiciel Arimes.						

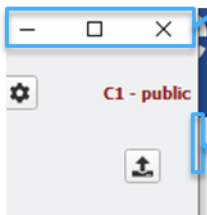




3. PRESENTATION GENERALE

3.1. Généralités

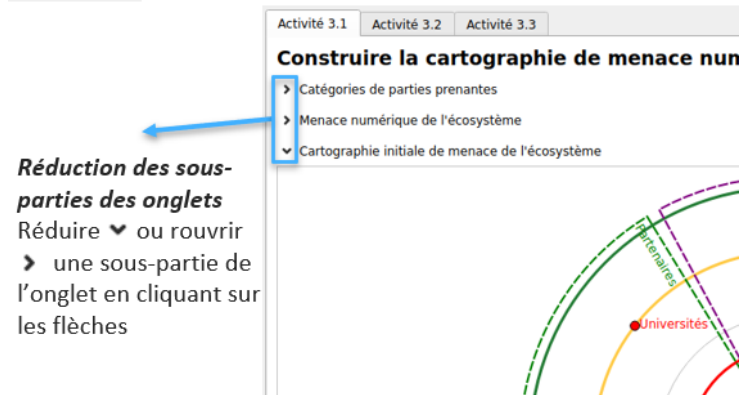
ARIMES utilise la bibliothèque Qt, qui utilise le thème du système pour l’affichage graphique. Certains éléments graphiques, notamment les bordures des fenêtres, peuvent donc différer de ceux présentés dans ce document. Ces éléments sont ceux utilisés par le système, il convient donc de se référer à la documentation du système ou de Qt dans le cas où ce document n’apporterait pas de réponses aux questionnements potentiels.

3.2. Fenêtre de l’application


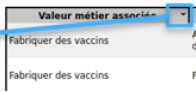
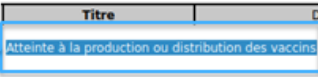
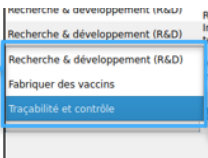
3.2.1. Minimiser, maximiser, fermer ou redimensionner la fenêtre

Généralités – Fenêtre de l’application	
Actions disponibles sur la fenêtre	Description
<p>Actions sur la fenêtre Minimiser, maximiser ou fermer l’application.</p>  <p>Redimensionner la fenêtre Les bordures de la fenêtre permettent de la redimensionner</p>	<p>Minimiser, maximiser, fermer ou redimensionner L’application lance une fenêtre avec laquelle il est possible d’interagir :</p> <ul style="list-style-type: none"> - Minimiser , maximiser  ou fermer l’application  - Redimensionner l’application  en positionnant le curseur de la souris sur les bordures de la fenêtre

3.2.2. Action sur les onglets de l’application

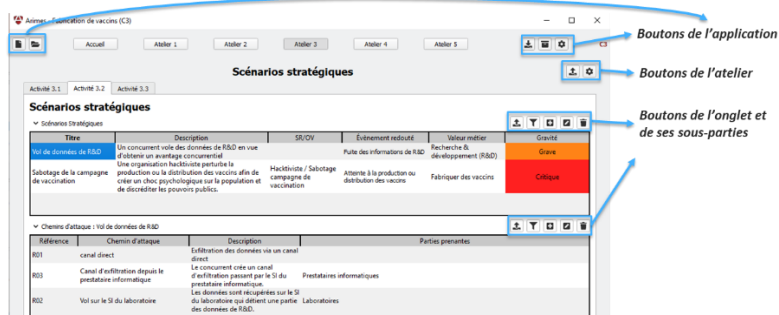

Généralités – Onglets de l’application	
Actions disponibles sur les onglets	Description
<p>Réduction des sous-parties des onglets Réduire ▼ ou rouvrir ▶ une sous-partie de l’onglet en cliquant sur les flèches</p> 	<p>Réduire les sous-parties des onglets Il est possible de réduire une sous-partie dans les onglets en cliquant sur les flèches de réduction ou de réouverture.</p>

3.2.3. Action sur les tableaux de l'application

Généralités – Tableaux de l'application	
Actions disponibles sur les tableaux	Description
<p>Modifier la largeur des colonnes</p> <p>Modifier la largeur des colonnes en glissant le séparateur de colonnes vers la droite ou la gauche</p> 	<p>Redimensionner les colonnes du tableau</p> <p>Il est possible de modifier la largeur des colonnes en faisant glisser le séparateur de colonnes vers la droite ou la gauche.</p>
<p>Tri alphabétique des valeurs des colonnes</p> 	<p>Tri alphabétique</p> <p>Il est possible d'effectuer un tri alphabétique en cliquant sur l'intitulé de la colonne (tri ascendant ou descendant).</p> <p>À partir de la version 1.0.0-RC3, le tri sur des colonnes de valeurs d'échelles se fait dans l'ordre de l'échelle, et non pas alphabétiquement.</p>
<p>Edition des valeurs</p> <p>Double cliquer sur une case pour modifier sa valeur</p> 	<p>Edition des valeurs (texte)</p> <p>Il est possible d'éditer les valeurs des cases du tableau en double-cliquant sur la case à modifier. Certaines valeurs ne sont pas modifiables dans certains tableaux. Il s'agit en général de champs en lecture seule, qui sont modifiables depuis une autre activité.</p>
<p>Liste à choix multiple</p> <p>Double cliquer sur une case pour accéder à la liste</p> 	<p>Edition des valeurs (liste déroulante)</p> <p>Certaines cases disposent d'une édition sous forme de liste déroulante. Double-cliquer sur la case du tableau pour éditer sa valeur à travers la liste à choix multiple associée. Lorsque l'association est multiple, des cases à cocher sont présentes sur chaque élément de la liste, et permettent d'associer plusieurs éléments.</p>























3.3. Boutons de l'application

3.3.1. Portées et info-bulles des boutons de l'application

Généralités – Boutons de l'application	
Boutons de l'application	Description
	<p>Portées des boutons de l'application</p> <p>Les boutons de l'application sont positionnés en fonction de leur portée :</p> <ul style="list-style-type: none"> - Boutons de l'application - Boutons de l'atelier sélectionné - Bouton de l'onglet sélectionné et de ses sous-parties
	<p>Affichage des info-bulles</p> <p>Laisser le curseur de la souris sur un bouton pour afficher une info-bulle.</p>

3.3.2. Description des boutons

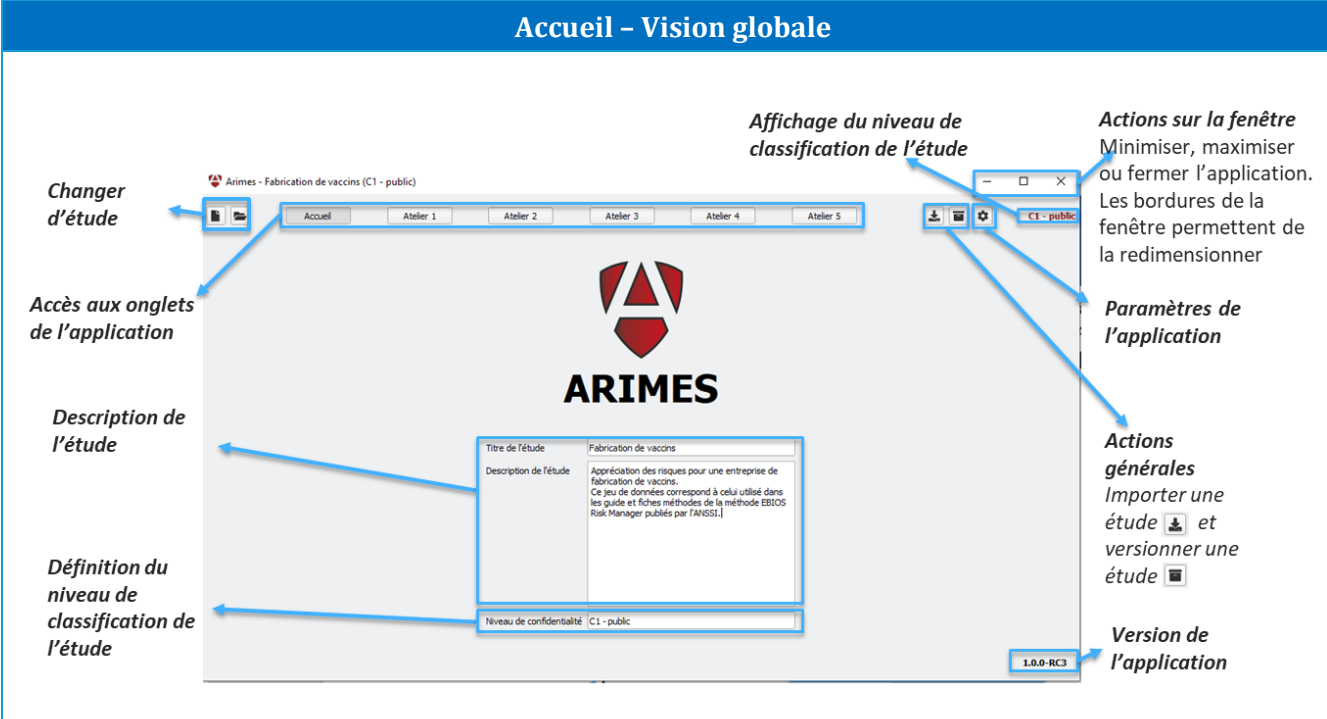
Généralités – Boutons de l'application	
Boutons de l'application	Description

	Créer une nouvelle étude vide
	Ouvrir une étude existante
	Importer des données depuis un export ARIMES
	Importer des données depuis un fichier CSV utilisateur (<i>depuis v1.0.0-RC3</i>)
	Exporter des données (format JSON ou CSV, pour import ultérieur)
	Exporter des données (format PDF, ODT, CSV, ou HTML) pour présentation de l'étude (rapport)
	Versionner l'étude
	Accès à la vue « configuration »
	Retour sur la vue « édition » (présent uniquement sur les vues « configuration »)
	Filtrer les données
	Effacer le filtre (lorsqu'un filtre est activé)
	Ajouter un élément
	Modifier un élément
	Supprimer un élément
	Basculer en vue « horizontale » (Activité 4.1)
	Basculer en vue « verticale » (Activité 4.1)
	Monter une ligne dans un tableau (pour ordonner les éléments d'une échelle)
	Descendre une ligne dans un tableau (pour ordonner les éléments d'une échelle)
	Ajouter une ligne d'un tableau vers un autre tableau (configuration activité 3.1)
	Retirer une ligne d'un tableau vers un autre tableau (configuration activité 3.1)
	Recalculer tout ce qui a été calculé automatiquement (activité 4.2)
	Tout recalculer, y compris ce qui a été modifié manuellement (activité 4.2)

4. PAGE D'ACCUEIL DE L'APPLICATION

4.1. Vision globale de l'onglet accueil

Accueil – Vision globale



Changer d'étude

Accès aux onglets de l'application

Description de l'étude

Définition du niveau de classification de l'étude

Affichage du niveau de classification de l'étude

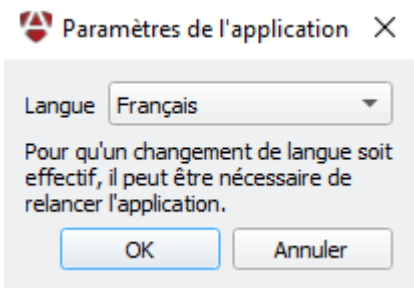

Actions sur la fenêtre
Minimiser, maximiser ou fermer l'application. Les bordures de la fenêtre permettent de la redimensionner

Paramètres de l'application


Actions générales
Importer une étude et versionner une étude

Version de l'application

4.2. Sélection de la langue de l'application

Accueil – Sélection de la langue de l'application	
Sélection de la langue de l'application	Description
	<p>Pour modifier la langue de l'application, cliquer sur le bouton  de paramètre de l'application.</p> <p>Une fenêtre s'ouvre : sélectionner la langue souhaitée et redémarrer l'application.</p>

5. ATELIER 1 – CADRAGE ET SOCLE DE SECURITE

L'atelier 1 est accessible depuis le bouton  et a pour objectif :

- La définition du cadre de l'étude
- La définition du périmètre métier et technique
- L'identification des évènements redoutés
- La définition du socle de sécurité

Cet atelier est découpé en 4 activités :

- Activité 1.1 – Définir le cadre de l'étude
- Activité 1.2 – Définir le périmètre métier et technique
- Activité 1.3 – Identifier les évènements redoutés et évaluer leur niveau de gravité
- Activité 1.4 – Déterminer le cadre de sécurité

Accès aux activités de l'atelier 1

Les activités sont accessibles en cliquant sur les onglets appropriés sur la page Atelier 1.



5.1. Activité 1.1 – Définir le cadre de l'étude

La définition du cadre de l'étude est accessible depuis la **page Atelier 1** et à travers l'**onglet Activité 1.1**, comme illustré sur la Figure suivante :

Activité 1.1 – Définir le cadre de l'étude

Identification des objectifs de l'étude
Ajouter , modifier ou supprimer les éléments du cadre de l'étude

Définition du cadre temporel de l'étude
Préciser les dates de début et de fin pour les cycles : opérationnel et stratégique

Cadrage et socle de sécurité

Activité 1.1 Activité 1.2 Activité 1.3 Activité 1.4

Définir le cadre de l'étude

Objectifs de l'étude

OBJETIF DE L'ETUDE	1	2	3	4	5
Identifier le socle de sécurité adapté à l'objet de l'étude	X				
Etre en conformité avec les référentiels de sécurité numérique	X				X
Evaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			X		
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		X	X		
Réaliser une étude préliminaire des risques pour identifier les					

Participants

Nom	Prénom	Fonction	Responsabilité
Dupont	Michelle	Direction	Valider les résultats de l'étude
Moullins	Charles	Consultant cyber	Conseil
Béranger	Jean	DSI	Responsable MCO et MCS du SI
Lefermier	Ivan	Relations commerciales	Conseil sur les parties prenantes externes
Brunel	Mireille	RSSI	RSSI

Matrice RACI

Participants	Ateliers				
	1	2	3	4	5
Dupont	AI	I	AI		AI
Moullins		C	C	C	C
Béranger	C			C	CI
Lefermier			CI		
Brunel	RI	RAI	RI	RAI	RI

Identification des participants à l'étude
Ajouter , modifier ou supprimer les participants à l'étude

Matrice RACI des participants
Préciser la matrice RACI des participants

Définition des éléments de planning de l'étude
Ajouter , modifier ou supprimer les participants à l'étude

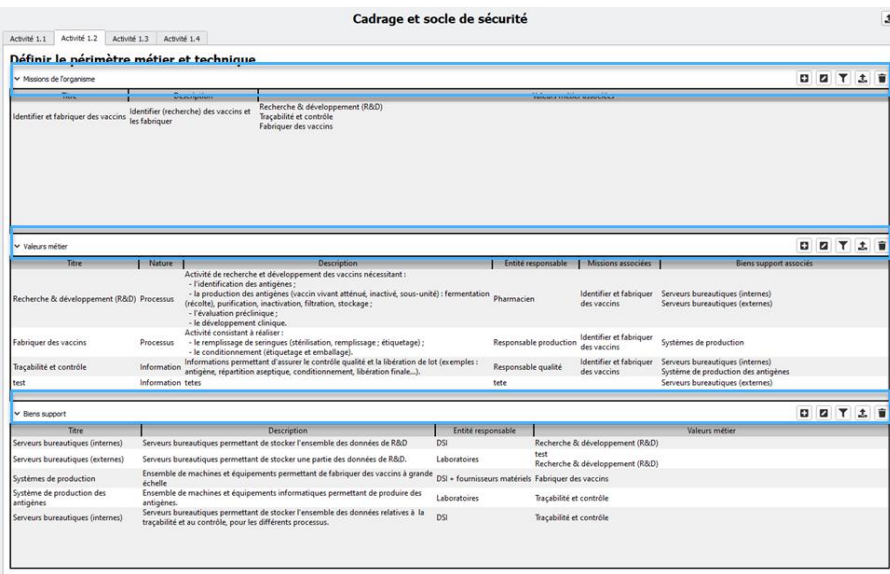
Figure 1 - Illustration de l'onglet : Activité 1.1 - Définir le cadre de l'étude

5.2. **Activité 1.2 – Définir le périmètre métier et technique**

Cette activité a pour objectif de recenser :

- Les missions relatives à l'objet de l'étude
- Les valeurs métiers associées aux différentes missions
- Les bien supports associés aux valeurs métiers

Activité 1.2 – Définir le périmètre métier et technique



Identification des missions de l'objet étudié
Ajouter , modifier ou supprimer des missions

Identification des valeurs métier de l'étude
Ajouter , modifier ou supprimer des valeurs métier

Identification des biens support
Ajouter , modifier ou supprimer des valeurs métier

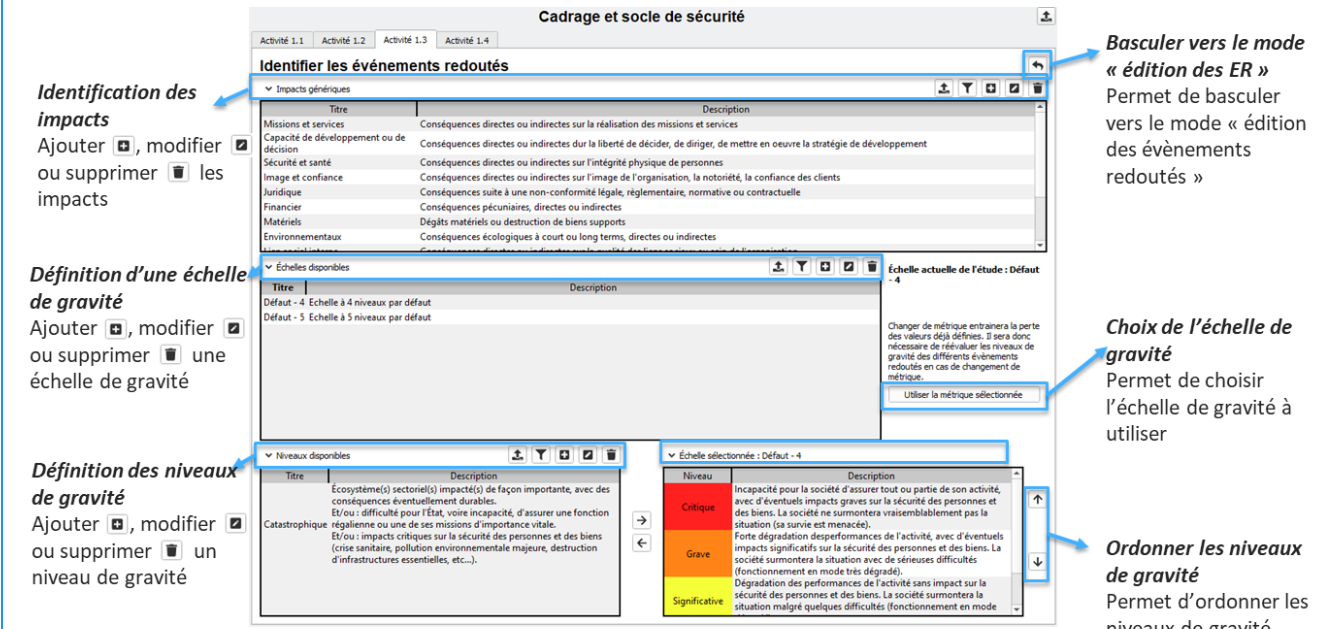
Figure 2 - Illustration de l'onglet : Activité 1.2 - Définir le périmètre métier et technique

5.3. **Activité 1.3 – Identifier les événements redoutés et évaluer leur niveau de gravité**

L'onglet Activité 1.3 comporte 2 vues :

- Vue configuration : permet la définition des impacts et de l'échelle de gravité
- Vue édition : permet la définition des événements redoutés identifiés

Activité 1.3 – Définir le périmètre métier et technique (vue configuration)



Identification des impacts
Ajouter , modifier ou supprimer les impacts

Définition d'une échelle de gravité
Ajouter , modifier ou supprimer une échelle de gravité

Définition des niveaux de gravité
Ajouter , modifier ou supprimer un niveau de gravité

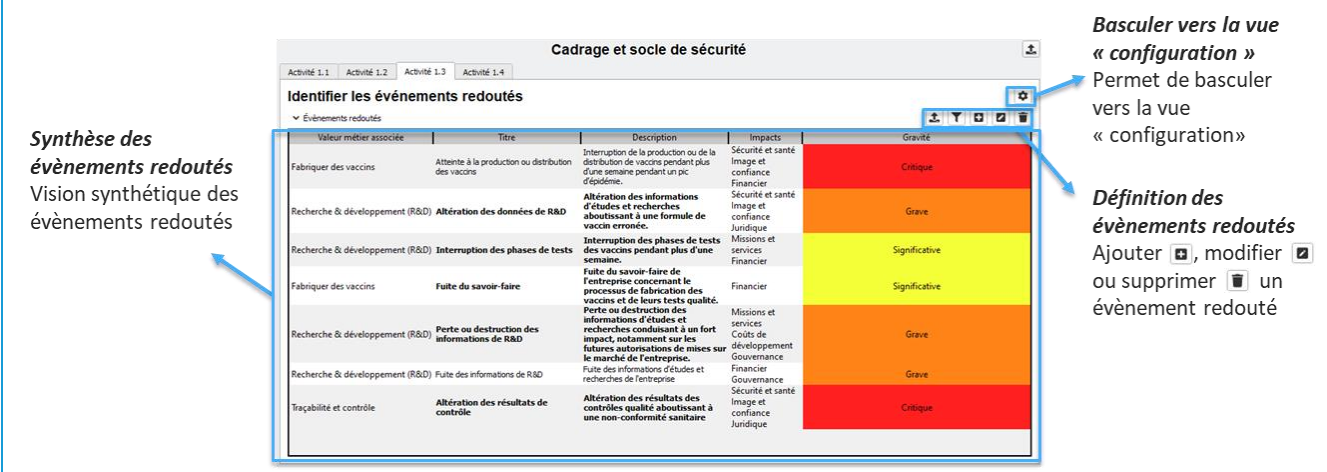
Basculer vers le mode « édition des ER »
Permet de basculer vers le mode « édition des événements redoutés »

Choix de l'échelle de gravité
Permet de choisir l'échelle de gravité à utiliser

Ordonner les niveaux de gravité
Permet d'ordonner les niveaux de gravité

Figure 3 - Illustration de la vue Configuration de l'activité 1.3 - Identifier les événements redoutés

Activité 1.3 – Définir le périmètre métier et technique (vue édition)



Synthèse des événements redoutés
Vision synthétique des événements redoutés

Basculer vers la vue « configuration »
Permet de basculer vers la vue « configuration »

Définition des événements redoutés
Ajouter , modifier ou supprimer un événement redouté

Valeur métier associée	Titre	Description	Impacts	Gravité
Fabriquer des vaccins	Atteinte à la production ou distribution des vaccins	Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie.	Sécurité et santé Image et confiance Financier	Critique
Recherche & développement (R&D)	Altération des données de R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée.	Sécurité et santé Image et confiance Juridique	Grave
Recherche & développement (R&D)	Interruption des phases de tests	Interruption des phases de tests des vaccins pendant plus d'une semaine.	Missions et services Financier	Significative
Fabriquer des vaccins	Fuite du savoir-faire	Fuite du savoir-faire de l'entreprise concernant le processus de fabrication des vaccins et de leurs tests qualité.	Financier	Significative
Recherche & développement (R&D)	Perte ou destruction des informations de R&D	Perte ou destruction des informations d'études et recherches conduisant à un fort impact, notamment sur les futures autorisations de mises sur le marché de l'entreprise.	Missions et services Crédit de développement Gouvernance	Grave
Recherche & développement (R&D)	Fuite des informations de R&D	Fuite des informations d'études et recherches de l'entreprise.	Financier Gouvernance	Grave
Trasabilité et contrôle	Altération des résultats de contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire.	Sécurité et santé Image et confiance Juridique	Critique

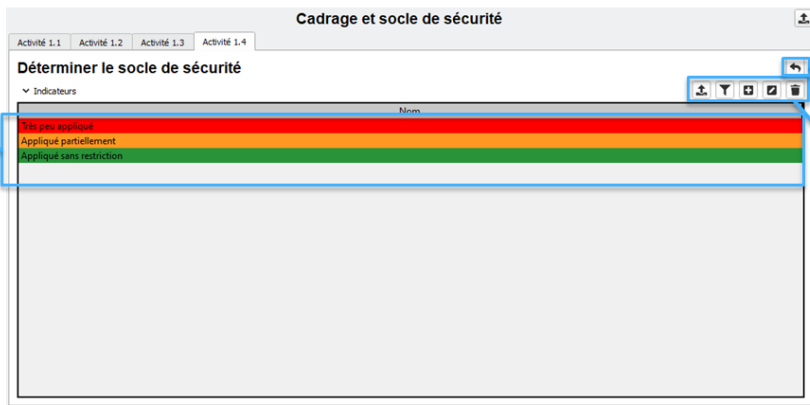
Figure 4 - Illustration de la vue Edition de l'activité 1.3 - Identifier les événements redoutés

5.4. **Activité 1.4 – Déterminer le socle de sécurité**

L'onglet Activité 1.4 comporte 2 modes :

- Vue configuration : permet la définition des états d'application
- Vue édition : permet la définition des référentiels et des exigences applicables

Activité 1.4 – Définir le périmètre métier et technique (vue configuration)



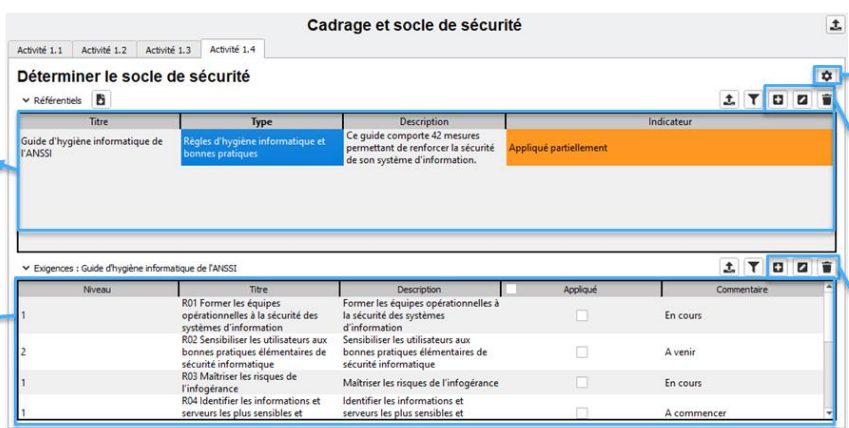
Synthèse des indicateurs
Vision synthétique des indicateurs définis pour l'activité 1.4

Basculer vers la vue « édition »
Permet de basculer vers la vue « édition » du socle de sécurité

Définition des indicateurs
Ajouter , modifier ou supprimer un indicateur

Figure 5 - Illustration de la vue Configuration de l'activité 1.4 – Cadrage et socle de sécurité

Activité 1.4 – Définir le périmètre métier et technique (vue édition)



Synthèse des indicateurs
Vision synthétique des référentiels

Basculer vers la vue « configuration »
Permet de basculer vers la vue « configuration » du socle de sécurité

Définition des référentiels
Ajouter , modifier ou supprimer un référentiel

Synthèse des exigences
Vision synthétique des exigences

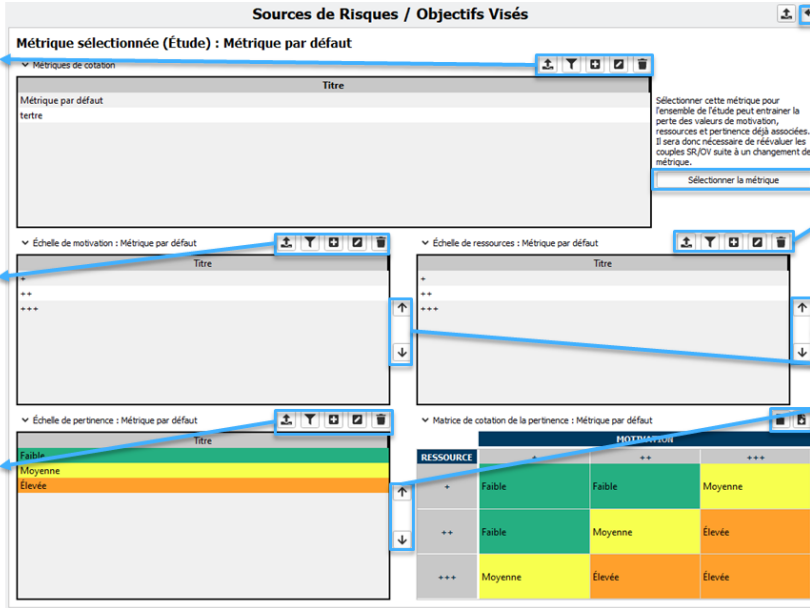
Définition des exigences
Ajouter , modifier ou supprimer une exigence

Figure 6 - Illustration de la vue Édition de l'activité 1.4 – Cadrage et socle de sécurité

6. ATELIER 2 SOURCES DE RISQUES / OBJECTIFS VISÉS

6.1. Vue configuration

Atelier 2 – Sources de risques et objectifs visés (vue configuration)



Définition des métriques de cotation
Ajouter , modifier ou supprimer une métrique de cotation

Définition de l'échelle de motivation
Ajouter , modifier ou supprimer un niveau dans l'échelle

Définition de l'échelle de pertinence
Ajouter , modifier ou supprimer une échelle de pertinence

Basculer vers la vue « édition »

Sélection de la métrique de cotation

Définition de l'échelle des ressources
Ajouter , modifier ou supprimer un niveau dans l'échelle

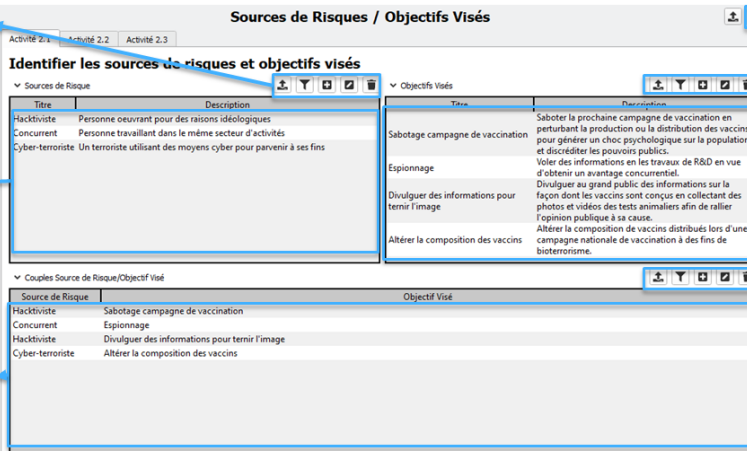
Classification des niveaux des échelles

Exporter/importer la métrique de cotation de la pertinence

Figure 7 - Illustration de la vue Configuration de l'atelier 2

6.2. Activité 2.1 Identifier les sources de risques et objectifs visés

Activité 2.1 – Sources de risques et objectifs visés (vue édition)



Définition des sources de risque
Ajouter , modifier ou supprimer une source de risque

Édition des sources de risques
Double-cliquer sur les cases du tableau pour éditer les sources de risques

Association des couples SR / OV
Double-cliquer sur les cases du tableau pour associer les couples SR / OV

Basculer vers la vue « configuration »

Définition des objectifs visés
Ajouter , modifier ou supprimer un objectif visé

Édition des objectifs visés
Double-cliquer sur les cases du tableau pour éditer les objectifs visés

Définition des couples SR/OV
Ajouter , modifier ou supprimer un couple SR/OV

Figure 8 - Illustration de l'activité 2.1 – SR/OV

6.3. *Activité 2.2 Evaluer les couples Source de Risque/Objectif Visé*

Activité 2.2 – Évaluer les couples SR/OV

Synthèse des couples SR / OV
Vision synthétique des couples SR/OV définis à l'Atelier 2.1

Sources de Risques / Objectifs Visés

Activité 2.1
Activité 2.2
Activité 2.3

Évaluer les couples Source de Risque/Objectif Visé

▼ Couples Source de Risque/Objectif Visé

Source de Risque	Objectif Visé	Motivation	Ressource	Moyenne	Pertinence
Hacktiviste	Sabotage campagne de vaccination	++	++	Moyenne	
Concurrent	Espionnage	+++	+++	Élevée	
Hacktiviste	Divulguer des informations pour ternir l'image	++	+	Faible	
Cyber-terroriste	Altérer la composition des vaccins	-	++	Faible	

Evaluation des couples SR/OV
Double-cliquer sur les cases du tableau pour évaluer les couples SR/OV en termes de Motivation et Ressource

Figure 9 - Illustration de l'activité 2.2 – Évaluer les couples SR/OV

6.4. *Activité 2.3 Sélectionner les couples SR/OV*

Activité 2.3 – Sélectionner les couples SR/OV

Synthèse des couples SR/OV
Vision synthétique des couples SR/OV définis lors des Ateliers 2.1 et 2.2

Sources de Risques / Objectifs Visés

Activité 2.1
Activité 2.2
Activité 2.3

Sélectionner les couples Sources de Risque / Objectifs Visés prioritaires

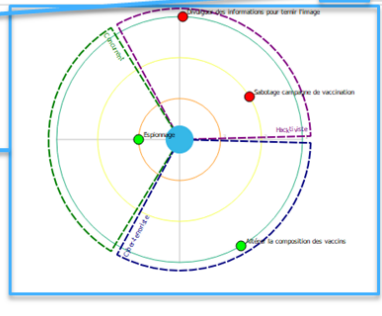
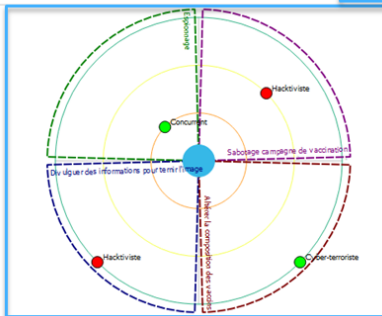
▼ Couples Source de Risque/Objectif Visé

Source de Risque	Objectif Visé	Motivation	Ressource	Pertinence	Relevance
Hacktiviste	Sabotage campagne de vaccination	++	++	Moyenne	<input type="checkbox"/>
Concurrent	Espionnage	+++	+++	Élevée	<input checked="" type="checkbox"/>
Hacktiviste	Divulguer des informations pour ternir l'image	++	+	Faible	<input checked="" type="checkbox"/>
Cyber-terroriste	Altérer la composition des vaccins	-	++	Faible	<input type="checkbox"/>

Sélection des couples SR/OV jugés pertinents

Zoomer /dézoomer

▼ Radar (vision par source de risque)
▼ Radar (vision par objectif visé)

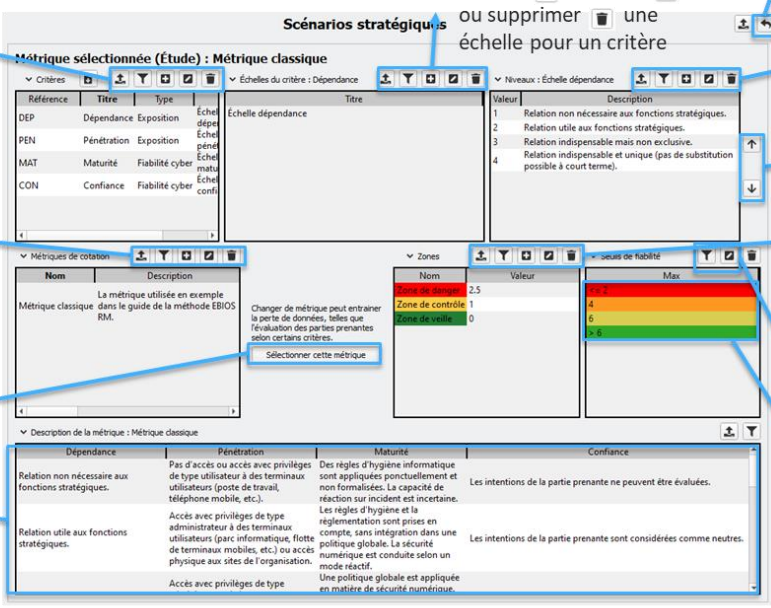
Radar (vision par source de risque)




Figure 10 - Illustration de l'activité 2.3 – Sélectionner les couples SR/OV




7. ATELIER 3 SCENARIOS STRATEGIQUES

7.1. Vue configuration

Atelier 3 – Vue configuration






Définition des critères
Ajouter , modifier  ou supprimer  un critère




Définition des métriques de cotation
Ajouter , modifier  ou supprimer  une métrique de cotation

Sélection de la métrique de cotation




Synthèse de la métrique de cotation
Vision synthétique de la métrique de cotation

Définition des échelles
Ajouter , modifier  ou supprimer  une échelle pour un critère

Basculer vers la vue « édition »

Définition des niveaux
Ajouter , modifier  ou supprimer  un niveau d'échelle

Classification des niveaux des échelles

Définition des zones
Ajouter , modifier  ou supprimer  une zone

Éditer les seuils de fiabilité
Double cliquer sur les cases du tableau pour éditer les seuils de fiabilité

Référence	Titre	Type	Échelle	Titre
DEP	Dépendance	Exposition	Échelle dépendance	Échelle dépendance
PEN	Pénétration	Exposition	Échelle pénétration	
MAT	Maturité	Fiabilité cyber	Échelle maturité	
CON	Confiance	Fiabilité cyber	Échelle confiance	

Nom	Description
Métrique classique	La métrique utilisée en exemple dans le guide de la méthode EBIOS RM.

Nom	Valeur
Zone de danger	2.5
Zone de contrôle	1
Zone de veille	0

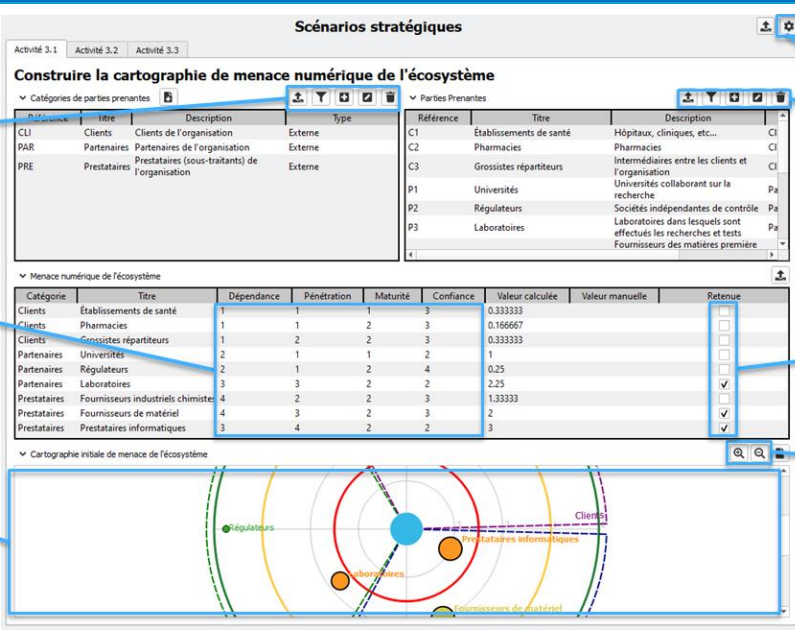
Min	Max
4	6
6	8

Dépendance	Pénétration	Maturité	Confiance
Relation non nécessaire aux fonctions stratégiques.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
Relation utile aux fonctions stratégiques.	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
	Accès avec privilèges de type	Une politique globale est appliquée en matière de sécurité numérique.	

Figure 11 - Illustration de la vue Configuration de l'Atelier 3

7.2. **Activité 3.1 Construire la cartographie**

Activité 3.1 – Construire la cartographie de menace numérique de l'écosystème



Scénarios stratégiques

Activité 3.1 | Activité 3.2 | Activité 3.3

Construire la cartographie de menace numérique de l'écosystème

▼ Catégories de parties prenantes

Id	Titre	Description	Type
CLI	Clients	Clients de l'organisation	Externe
PAR	Partenaires	Partenaires de l'organisation	Externe
PRE	Prestataires	Prestataires (sous-traitants) de l'organisation	Externe

▼ Parties Prenantes

Référence	Titre	Description	Type
C1	Établissements de santé	Hôpitaux, cliniques, etc...	CI
C2	Pharmacies	Pharmacies	CI
C3	Grossistes répartiteurs	Intermédiaires entre les clients et l'organisation	CI
P1	Universités	Universités collaborant sur la recherche	Pa
P2	Régulateurs	Sociétés indépendantes de contrôle	Pa
P3	Laboratoires	Laboratoires dans lesquels sont effectués les recherches et tests	Pa
	Fournisseurs	Fournisseurs des matières premières	Pa

▼ Menace numérique de l'écosystème

Catégorie	Titre	Dépendance	Pénétration	Maturité	Confiance	Valeur calculée	Valeur manuelle	Retenue
Clients	Établissements de santé	1	1	1	3	0.333333		<input type="checkbox"/>
Clients	Pharmacies	1	2	2	3	0.166667		<input type="checkbox"/>
Clients	Grossistes répartiteurs	1	2	2	3	0.333333		<input type="checkbox"/>
Partenaires	Universités	2	1	1	2	1		<input type="checkbox"/>
Partenaires	Régulateurs	2	1	2	4	0.25		<input type="checkbox"/>
Partenaires	Laboratoires	3	3	2	2	2.25		<input checked="" type="checkbox"/>
Prestataires	Fournisseurs industriels chimiste	4	2	2	3	1.333333		<input checked="" type="checkbox"/>
Prestataires	Fournisseurs de matériel	4	3	2	3	2		<input checked="" type="checkbox"/>
Prestataires	Prestataires informatiques	3	4	2	2	3		<input checked="" type="checkbox"/>

▼ Cartographie initiale de menace de l'écosystème

Annotations :

- Définition des catégories de parties prenantes** : Ajouter , modifier ou supprimer un critère
- Évaluation des parties prenantes selon les critères sélectionnés**
- Définition des parties prenantes** : Ajouter , modifier ou supprimer un critère
- Sélection des parties prenantes jugées pertinentes**
- Basculer vers la vue « configuration »**
- Zoomer/Dézoomer**
- Cartographie de menace de l'écosystème**

Figure 12 - Illustration de l'activité 3.1 – Construire la cartographie de menace numérique de l'écosystème

Dans cette activité, le niveau de menace des parties prenantes est évalué afin de sélectionner les parties prenantes dites *critiques*. Les parties prenantes critiques sont celles qui seront utilisées pour construire les scénarios stratégiques de l'activité suivante (3.2). Sur la cartographie de menace, les parties prenantes critiques apparaissent avec une auréole grisée (une « ombre »), et une étiquette écrite en gras italique.

Il est également possible de cliquer sur le cercle d'une partie prenante dans la cartographie pour rendre une partie prenante critique ou lui retirer cet attribut.

7.3. *Activité 3.2 Scénarios stratégiques*

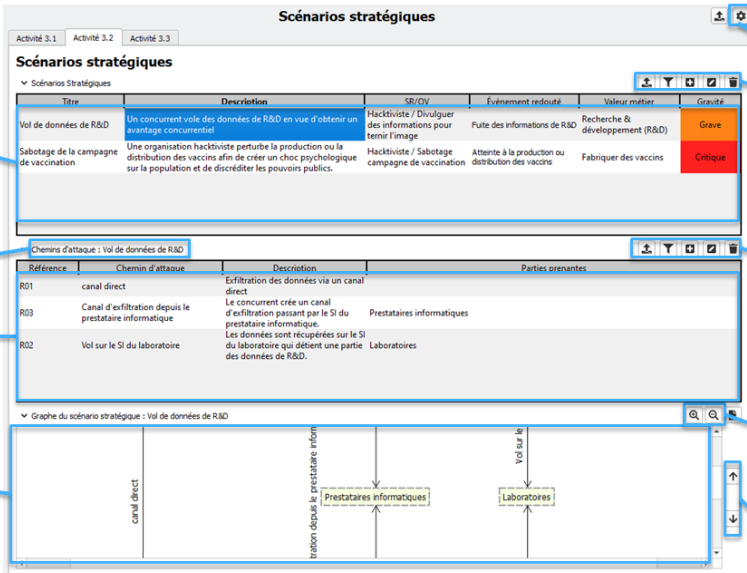
Activité 3.2 – Scénarios stratégiques

Édition des scénarios stratégiques
Double-cliquer sur les cases du tableau pour éditer les scénarios stratégiques

Scénario stratégique considéré

Édition des chemins d'attaque
Double-cliquer sur les cases du tableau pour éditer les chemins d'attaque

Graphe du scénario stratégique sélectionné



Basculer vers la vue « configuration »

Définition des scénarios stratégiques
Ajouter , modifier ou supprimer un scénario stratégique

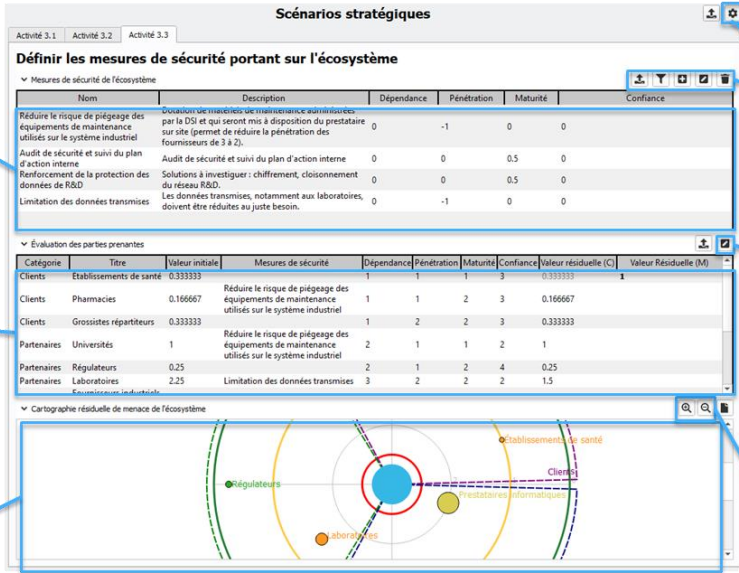
Définition des chemins d'attaque
Ajouter , modifier ou supprimer un chemin d'attaque

Ordonner les parties prenantes sur le chemin

Figure 13 - Illustration de l'activité 3.2 – Scénarios stratégiques

7.4. Activité 3.3 Définir les mesures de sécurité

Activité 3.3 – Définir les mesures de sécurité portant sur l'écosystème



Édition des mesures de sécurité de l'écosystème
Double-cliquer sur les cases du tableau pour éditer les scénarios stratégiques

Édition des mesures de sécurité et synthèse de l'évaluation des parties prenantes
Vue synthétique de l'évaluation des parties prenantes. Double cliquer sur la case Mesures de sécurité pour associer une mesure de sécurité à une partie prenante.

Cartographie de menace résiduelle de l'écosystème

Basculer vers la vue « configuration »

Définition des mesures de sécurité de l'écosystème
Ajouter , modifier ou supprimer un scénario stratégique

Édition des mesures de sécurité des parties prenantes
Modifier les mesures de sécurité des parties prenantes

Exporter la cartographie résiduelle de menace de l'écosystème

Figure 14 - Illustration de l'activité 3.3 – Définir les mesures de sécurité portant sur l'écosystème

Les mesures de sécurité portant sur l'écosystème s'évaluent en termes de différences : une mesure qui réduit le critère de pénétration peut par exemple la réduire de 1, en mettant une valeur de -1 dans la colonne pénétration de la mesure. Associer la mesure à une partie prenante réduira alors la valeur de pénétration de la partie prenante de 1.

Remarque : les valeurs des critères des parties prenantes ne peuvent pas être inférieures à la valeur minimale de l'échelle associée, ni être supérieures à la valeur maximale de l'échelle associée. Si la valeur calculée venait à sortir de l'intervalle, la valeur minimale (ou maximale) de l'échelle sera alors attribuée.

8. ATELIER 4 SCENARIOS OPERATIONNELS

8.1. Vue configuration

Atelier 4 – Vue configuration

Définition d'une séquence d'attaque
Ajouter , modifier ou supprimer une séquence d'attaque

Sélection de la séquence d'attaque

Définition des niveaux de probabilité
Ajouter , modifier ou supprimer un niveau de probabilité

Définition des niveaux de l'échelle de vraisemblance
Ajouter , modifier ou supprimer un niveau de l'échelle de vraisemblance

Scénarios opérationnels

Séquence sélectionnée (Étude) : CyberKillChain

Titre

CyberKillChain

Phases : CyberKillChain

Connaître
Rentrer
Trouver
Exploiter

Titre

Reconnaissance... externe de la cible

Description

Lors de la phase de reconnaissance, la source de risque va rechercher dans l'ensemble de ses bases disponibles les informations nécessaires à la planification de son attaque. Les données collectées pourront être de nature technique ou concerner l'organisation de la cible et de son écosystème. Les moyens employés peuvent être très variés :

- réseaux sociaux (social engineering)
- Internet (poubelles numériques, sites) ;
- forums et salons professionnels ;

Changer de séquence peut entraîner la perte de données, notamment au niveau de l'ordre des actions dans les modes opératoires.

Selectionner cette killchain

Probabilité de succès

Nom

Quasi-certaine
Très élevée
Significative
Faible

Difficulté technique

Nom

Faible
Modérée
Élevée
Très élevée

Échelle de vraisemblance

Nom	Description
Quasi-certain	La source de risque va très certainement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est très élevée.
Très vraisemblable	La source de risque va probablement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est élevée.
Vraisemblable	La source de risque est susceptible d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
Peu vraisemblable	La source de risque a relativement peu de chances d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est faible.

Matrice de cotation de la vraisemblance

Probabilité de succès	Difficulté technique			
	Faible	Moderée	Élevée	Très élevée
Quasi-certaine	Quasi-certain	Quasi-certain	Très vraisemblable	Très vraisemblable
Très élevée	Quasi-certain	Très vraisemblable	Vraisemblable	Vraisemblable
Significative	Très vraisemblable	Vraisemblable	Vraisemblable	Peu vraisemblable
Faible	Très vraisemblable	Vraisemblable	Peu vraisemblable	Peu vraisemblable

Basculer vers la vue « édition »

Définition des catégories d'actions
Ajouter , modifier ou supprimer une catégorie d'actions

Définition des phases de la séquence d'attaque
Ajouter , modifier ou supprimer une phase de la séquence d'attaque

Définition des niveaux de difficulté technique
Ajouter , modifier ou supprimer un niveau de difficulté technique

Définition de la matrice de cotation
Double cliquer sur les cases du tableau pour éditer la matrice de cotation

Figure 15 - Illustration de la vue Configuration de l'Atelier 4 – Scénarios opérationnels

8.2. **Activité 4.1 Elaborer les scénarios opérationnels**

Activité 4.1 – Élaborer les scénarios opérationnels

Edition des scénarios opérationnels
Double-cliquer sur les cases du tableau pour éditer les scénarios opérationnels

Edition des actions élémentaires du scénario opérationnel considéré
Double cliquer sur les cases du tableau pour éditer les actions élémentaires.

Visualisation du graphe du scénario opérationnel sélectionné

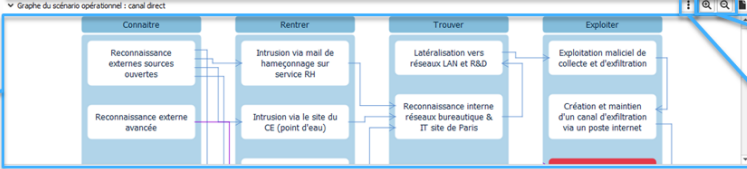
Basculer vers la vue « configuration »

Références	Scénario opérationnel	Description opérationnelle	Scénario Origine	Chemin d'attaque
R01	Canal direct	Exfiltration des données via un canal direct.	Vol de données de R&D	canal direct
R03	Canal d'exfiltration depuis le prestataire informatique	Le concurrent crée un canal d'exfiltration passant par le SI du prestataire informatique. Les données sont récupérées sur le SI du laboratoire qui détiennent une partie des données de R&D.	Vol de données de R&D	Canal d'exfiltration depuis le prestataire informatique
R02	Vol sur le SI du laboratoire	Un attaquant compromet l'outil de maintenance utilisé par le fournisseur de matériel afin de porter atteinte à la production des vaccins.	Vol de données de R&D	Vol sur le SI du laboratoire
R04	Compromission de l'outil de maintenance	Sabotage de la campagne de vaccination	Compromission de l'outil de maintenance	Compromission de l'outil de maintenance

Acteurs du scénario opérationnel : canal direct

Nom	Catégorie	Phase	Bien support	Successeurs	Couleur des flèches
Reconnaissance externes sources ouvertes	Reconnaissance externe de la cible	Connaitre	Serveurs bureautiques (internes)	Intrusion via un canal d'accès préexistant Intrusion via mail de hameçonnage sur service RH Intrusion via le site du CE (point d'eau) Corruption d'un personnel de l'équipe de R&D	

Graphe du scénario opérationnel : canal direct



Définition des actions du scénario opérationnel
Ajouter , modifier ou supprimer une action élémentaire du chemin d'attaque

Zoomer/Dézoomer

Basculer vers la vue « verticale » du graphe

Figure 16 - Illustration de l'activité 4.1 – Élaborer les scénarios opérationnels


8.3. *Activité 4.2 Évaluer la vraisemblance des scénarios opérationnels*

Activité 4.2 – Évaluer la vraisemblance des scénarios opérationnels

Recalculer tout ,
ou **tout ce qui n'est pas changé manuellement** ,
selon la méthode et l'algorithme sélectionnés

Synthèse des actions élémentaires et de leur probabilité
Vue synthétique des actions élémentaires et de leur probabilité

Synthèse des modes opératoires
Vue synthétique de modes opératoires pour le scénario opérationnel considéré



The screenshot shows the 'Scénarios opérationnels' interface. At the top, there are tabs for 'Activité 4.1' and 'Activité 4.2'. The main title is 'Évaluer la vraisemblance des scénarios opérationnels'. Below this, there are dropdown menus for 'Méthode d'évaluation' (set to 'Méthode Standard') and 'Algorithme de calcul' (set to 'Algorithme standard (vraisemblance = probabilité minimale)').

Références	Scénario opérationnel	Description opérationnelle	Scénario d'origine	Vraisemblance
R01	Canal direct	Exfiltration des données via un canal direct	Vol de données de R&D	Très vraisemblable
R03	Canal d'exfiltration depuis le prestataire informatique	Le concurrent crée un canal d'exfiltration passant par le SI du prestataire informatique	Vol de données de R&D	Quasi-certain
R02	Vol sur le SI du laboratoire	Les données sont récupérées sur le SI du laboratoire qui détient une partie des données de R&D.	Vol de données de R&D	Vraisemblable
R04	Compromission de l'outil de maintenance	Un attaquant compromet l'outil de maintenance utilisé par le fournisseur de matériel afin de porter atteinte à la production des	Sabotage de la campagne de vaccination	Vraisemblable

Below the table, there are sections for 'Actions du scénario opérationnel : Canal direct' and 'Modes opératoires du scénario opérationnel : Canal direct', each with a table of actions and their probabilities.

Basculer vers la vue « configuration »

Choix de la méthode d'évaluation

Choix de l'algorithme de calcul

Synthèse des scénarios opérationnels
Vue synthétique des scénarios opérationnels (Activité 4.1)

Figure 17 - Illustration de l'activité 4.2 – Évaluer la vraisemblance des scénarios opérationnels

Remarque : la probabilité des actions dénote la probabilité de succès de l'action, et non pas la probabilité d'occurrence.

9. ATELIER 5 TRAITEMENT DU RISQUE

9.1. Vue configuration

Atelier 5 – Vue configuration

Définition des niveaux de risque
Ajouter , modifier ou supprimer un niveau de risque

Définition des catégories de mesures de sécurité
Ajouter , modifier ou supprimer une catégorie de mesure de sécurité

Définition des statuts des mesures de sécurité
Ajouter , modifier ou supprimer un statut de mesure de sécurité

⌵ ⌴ ⌵ ⌴ ⌵ ⌴ ⌵ ⌴ ⌵ ⌴ ⌵ ⌴

Niveaux de risque

Niveau de risque	Acceptabilité	Intitulé des actions
Faible	Acceptable en l'état	Aucune action n'est à entreprendre. Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme.
Moyen	Tolérable sous contrôle	Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé.
Élevé	Inacceptable	

Cotation des niveaux de risque

Gravité	Vraisemblance			
	Très vraisemblable	Moyen	Peu vraisemblable	Très peu vraisemblable
Critique	Élevé	Élevé	Moyen	Moyen
Grave	Élevé	Élevé	Moyen	Faible
Significative	Élevé	Moyen	Faible	Faible
Mineur	Moyen	Moyen	Faible	Faible

Catégories de mesures de sécurité

Titre
Gouvernance et anticipation
Protection
Défense
Résilience

Statuts des mesures de sécurité

Titre
à lancer
En cours
terminé

Complexités de mesures de sécurité

Titre
+
++
+++

Basculer vers la vue « édition »

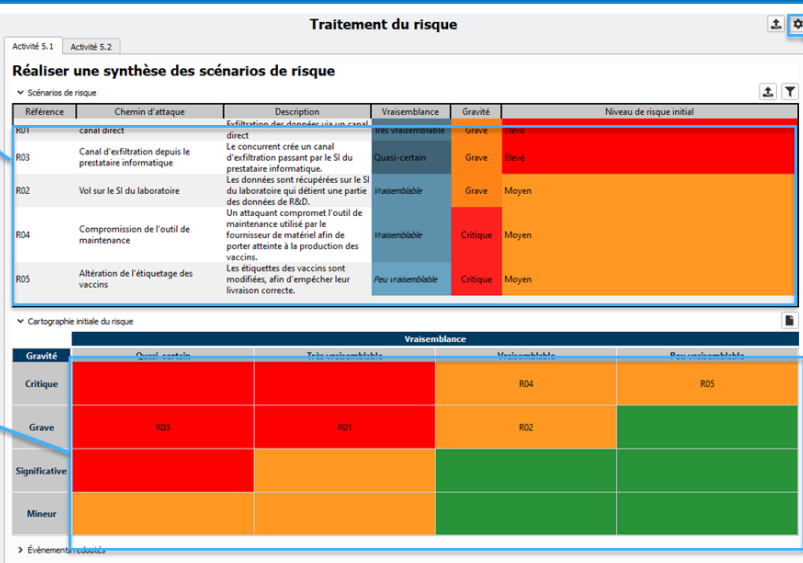
Édition de la matrice de cotation
Double cliquer sur les cases du tableau pour éditer la matrice de cotation

Définition des niveaux de complexité des mesures de sécurité
Ajouter , modifier ou supprimer un niveau de complexité

Figure 18 - Illustration de la vue Configuration de l'Atelier 5 – Traitement du risque

9.2. **Activité 5.1 Réaliser une synthèse des scénarios de risque**

Activité 5.1 – Réaliser une synthèse des scénarios de risque



Synthèse des scénarios de risque
Vue synthétique des scénarios de risque et de leur cotation initiale

Cartographie des niveaux de risque
Vue synthétique de la cartographie des niveaux de risque

Basculer vers la vue « configuration »

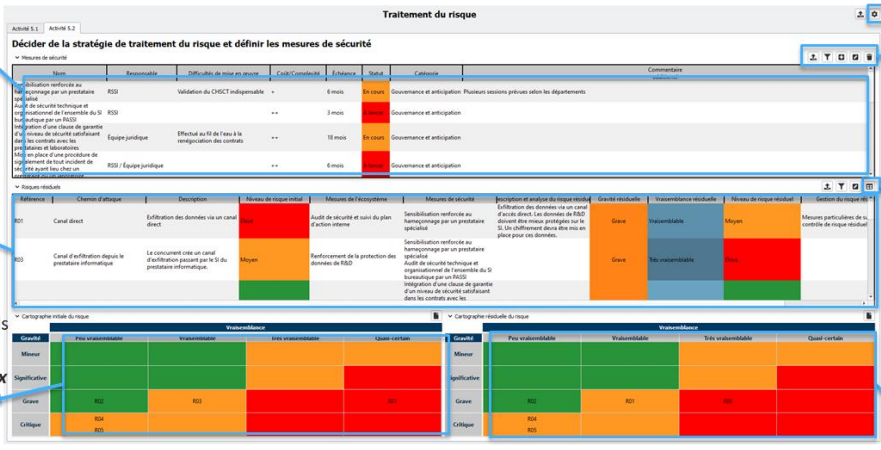
Référence	Chemin d'attaque	Description	Vraisemblance	Gravité	Niveau de risque initial
R01	canal direct	Exfiltration des données via un canal direct	Très vraisemblable	Grave	Critique
R03	Canal d'exfiltration depuis le prestataire informatique	Le concurrent crée un canal d'exfiltration passant par le SI du prestataire informatique.	Quasi-certain	Grave	Élevé
R02	Vol sur le SI du laboratoire	Les données sont récupérées sur le SI du laboratoire qui détient une partie des données de R&D.	Vraisemblable	Grave	Moyen
R04	Compromission de l'outil de maintenance	Un attaquant compromet l'outil de maintenance utilisé par le fournisseur de matériel afin de porter atteinte à la production des vaccins.	Vraisemblable	Critique	Moyen
R05	Altération de l'étiquetage des vaccins	Les étiquettes des vaccins sont modifiées, afin d'empêcher leur livraison correcte.	Peu vraisemblable	Critique	Moyen

Gravité	Vraisemblance			
	Quasi-certain	Très vraisemblable	Moyennement vraisemblable	Peu vraisemblable
Critique			R04	R05
Grave	R01	R01	R02	
Significative				
Mineur				

Figure 19 - Illustration de l'activité 5.1 – Réaliser une synthèse des scénarios de risque

9.3. Activité 5.2 Stratégie de traitement du risque

Activité 5.2 – Décider de la stratégie de traitement du risque et définir les mesures de sécurité





Édition du tableau des mesures de sécurité
Double cliquer sur les cases du tableau pour éditer les mesures de sécurité

Édition du tableau de risques résiduels
Double cliquer sur les cases du tableau pour éditer les risques résiduels

Cartographie des niveaux de risque (initial)
Vue synthétique de la cartographie des niveaux de risque (Activité 5.1)

Basculer vers la vue « édition »

Définition des mesures de sécurité
Ajouter , modifier ou supprimer  une mesure de sécurité

Basculer dans le mode « revue de risque »
Vue de chaque risque séparément.

Cartographie des niveaux de risque (résiduel)
Vue synthétique de la cartographie des niveaux de risque résiduels.

Figure 20 - Illustration de l'activité 5.2 – Décider de la stratégie de traitement du risques

Dans cette activité, il est également possible de visualiser les risques résiduels un par un, dans un mode « revue de risque », en cliquant sur le bouton permettant de basculer en mode « revue de risque ». Les risques sont alors présentés un risque à la fois, dans le format suivant :

Activité 5.2 – Mode revue de risques

Mode « revue de risque » des risques résiduels

▼ Risques résiduels

R01 - Canal direct

▼ Description et analyse du risque résiduel

Exfiltration des données via un canal d'accès direct. Les données de R&D doivent être mieux protégées sur le SI. Un chiffrement devra être mis en place pour ces données.

▼ Évènement redouté

Titre	Description	Valeur métier associée	Impacts	Gravité
Fuite des informations de R&D	Fuite des informations d'études et recherches de l'entreprise	Recherche & développement (R&D)	Financier Gouvernance	Grave

▼ Mesures de traitement du risque existantes et complémentaires

Mesures de l'écosystème	Mesures de sécurité
Audit de sécurité et suivi du plan d'action interne	Sensibilisation renforcée au hameçonnage par un prestataire spécialisé

▼ Évaluation du risque résiduel

Gravité initiale : Grave Vraisemblance initiale : Quasi-certain Niveau de risque initial : Élevé

Gravité résiduelle : Grave Vraisemblance résiduelle : Vraisemblable Niveau de risque résiduel : Moyen

▼ Gestion du risque résiduel

Mesures particulières de suivi et de contrôle de risque résiduel.

Basculer en mode liste
Vue synthétique de la cartographie des niveaux de risque résiduels.

Figure 21 - Illustration de l'activité 5.2 – Mode revue de risques

Les éléments modifiables le sont à la fois dans le mode « liste » classique et dans le mode « revue de risque ».

Remarque :



L'export est disponible pour les deux modes : sous forme de table avec le mode classique et sous forme de plusieurs tableaux présentés comme dans le mode de revue de risques.

Remarque :

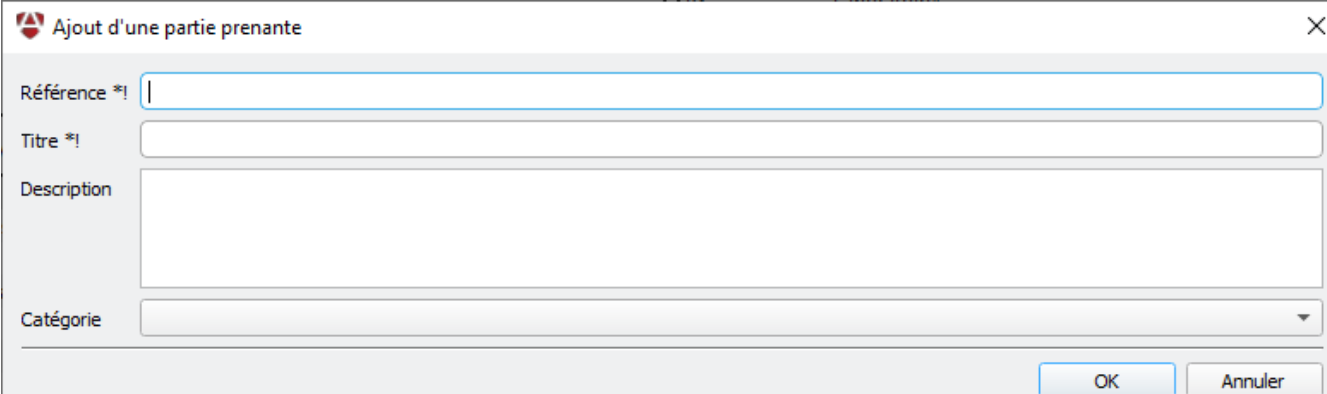
Il est possible d'évaluer les niveaux de risque résiduels en effectuant un glisser-déposer de son étiquette dans la cartographie des niveaux de risque résiduels

10. FENETRES CONTEXTUELLES

10.1. Fenêtre d'ajout ou de modification d'un élément

En différents endroits de l'application, il est possible d'ajouter un élément ou d'en modifier en cliquant sur un bouton  ou , respectivement. Cela ouvre une fenêtre présentant un formulaire permettant de renseigner les différents champs de l'élément. En cas de modification, les champs seront remplis avec les valeurs actuelles de l'élément à modifier.

Il existe différents types de champs, comme le montre l'image suivante affichant le formulaire d'ajout d'une partie prenante (activité 3.1) :



Les champs « Référence » et « Titre » sont des champs de texte court, le champ « Description » est un champ de texte long, et le champ « Catégorie » est une liste déroulante. Il existe d'autres types de champs, tels que des champs de date et des champs numériques.

Une fois les éléments renseignés, la validation se fait en cliquant sur le bouton « OK » ; il est possible d'annuler l'ajout ou la modification en cliquant plutôt sur le bouton « Annuler ». Les intitulés de ces boutons peuvent changer selon le système utilisé.

Les champs dont l'étiquette est marquée d'une astérisque « * » sont des champs obligatoires, qui ne peuvent pas être vides.

Les champs dont l'étiquette est marquée d'un point d'exclamation « ! » sont des champs dont la valeur doit être unique.


Dans l'exemple précédent, les champs « Référence » et « Titre » sont à la fois obligatoires et uniques.

Lorsqu'un champ ne respecte pas les critères demandés (unicité, non vide), la validation du formulaire ne se fait pas, et le(s) champ(s) en question apparai(ssen)t avec un style différent (un liseré rouge par exemple) permettant de les repérer.

Remarque :

Les champs numériques sont renseignés à l'aide d'éléments graphiques permettant de renseigner des nombres entiers. Il est toutefois, à certains endroits, possible de modifier les valeurs par la suite, en double-cliquant dans la case du tableau, afin de renseigner des nombres à virgule.

10.2. Fenêtre de filtre

La plupart des tableaux présentés dans l'application disposent d'un bouton  permettant d'ajouter un filtre sur les éléments à afficher. Cliquer sur ce bouton ouvre une fenêtre présentant un formulaire permettant d'activer le filtrage pour chaque colonne, en renseignant le filtre souhaité. Lorsque plusieurs colonnes sont sélectionnées, seules les lignes dont toutes les colonnes satisfont chacun des filtres demandés sont affichées.

Considérons la fenêtre suivante, montrant le formulaire de filtre des événements redoutés (activité 1.3) :



Filtrer les événements redoutés

Titre

Description

Valeur métier associée

- Recherche & développement (R&D)
- Fabriquer des vaccins
- Traçabilité et contrôle

Gravité

- Critique
- Grave
- Significative
- Mineur

Impacts

- Missions et services
- Capacité de développement ou de décision
- Sécurité et santé
- Image et confiance
- Juridique
- Financier
- Matériels
- Environnementaux
- Lien social interne
- Patrimoine culturel
- Coûts de développement
- Gouvernance

OK Annuler

Dans cet exemple, les colonnes « Gravité » et « Impacts » ont été choisies pour disposer de filtres. Les valeurs des autres colonnes n'influeront pas sur l'affichage ou non des lignes. Seules les lignes disposant d'une gravité « Critique » ou « Grave » ET disposant d'au moins un impact parmi ceux sélectionnés (« Missions et services », « Sécurité et santé », « Juridique », « Matériels », « Environnementaux », « Gouvernance ») seront affichés.

Ainsi, filtrer sur plusieurs colonnes réduit le nombre de lignes affichées, mais ajouter des valeurs dans les filtres des différentes colonnes (par exemple, « Gravité » ou « Impacts ») augmente le nombre de lignes, puisqu'il s'agit de valeurs acceptées.




Lorsqu'un filtre est actif sur un tableau, le bouton  est remplacé par le bouton , qui permet alors de désactiver le filtre. Les valeurs renseignées dans les différents champs subsistent, mais aucune colonne ne filtre. En ouvrant à nouveau la fenêtre de filtre, il devient possible de réactiver les filtres pour chaque colonne avec les mêmes valeurs que précédemment, en cochant la case correspondante.

Remarque :

Les filtres sur les champs de texte (longs ou courts) sont des expressions régulières, il est donc nécessaire d'échapper certains caractères.

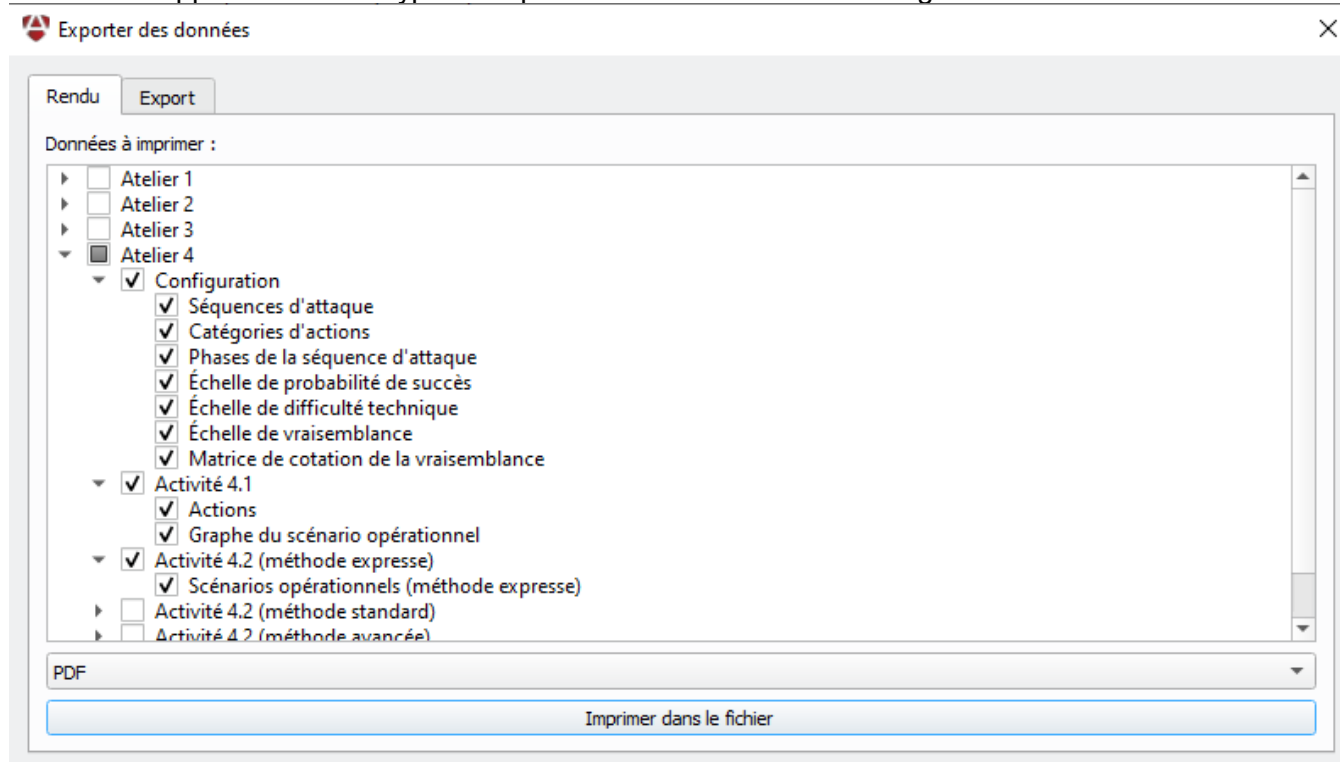
10.3. Fenêtre d'export

La fenêtre d'export permet d'exporter les données de l'étude. L'application dispose de deux types d'export, chacun représenté par un onglet différent dans la fenêtre d'export. La fenêtre est accessible en

cliquant sur un bouton  ou . Les éléments disposant du bouton  ne sont exportables que sous forme de rapport. Les deux types d'export sont l'export pour import et l'export pour rendu (rapport). L'export pour import produit un fichier qui contient les données nécessaires pour pouvoir être importé ultérieurement dans l'application. Ce fichier n'est pas destiné à être modifié ou lu. Ce type d'export peut se faire au format CSV ou au format JSON. Favoriser le format JSON en cas de doute. Le second type d'export est l'export de rendu, qui produit un visuel similaire à celui de l'application.

10.3.1. Export pour rendu (rapport)

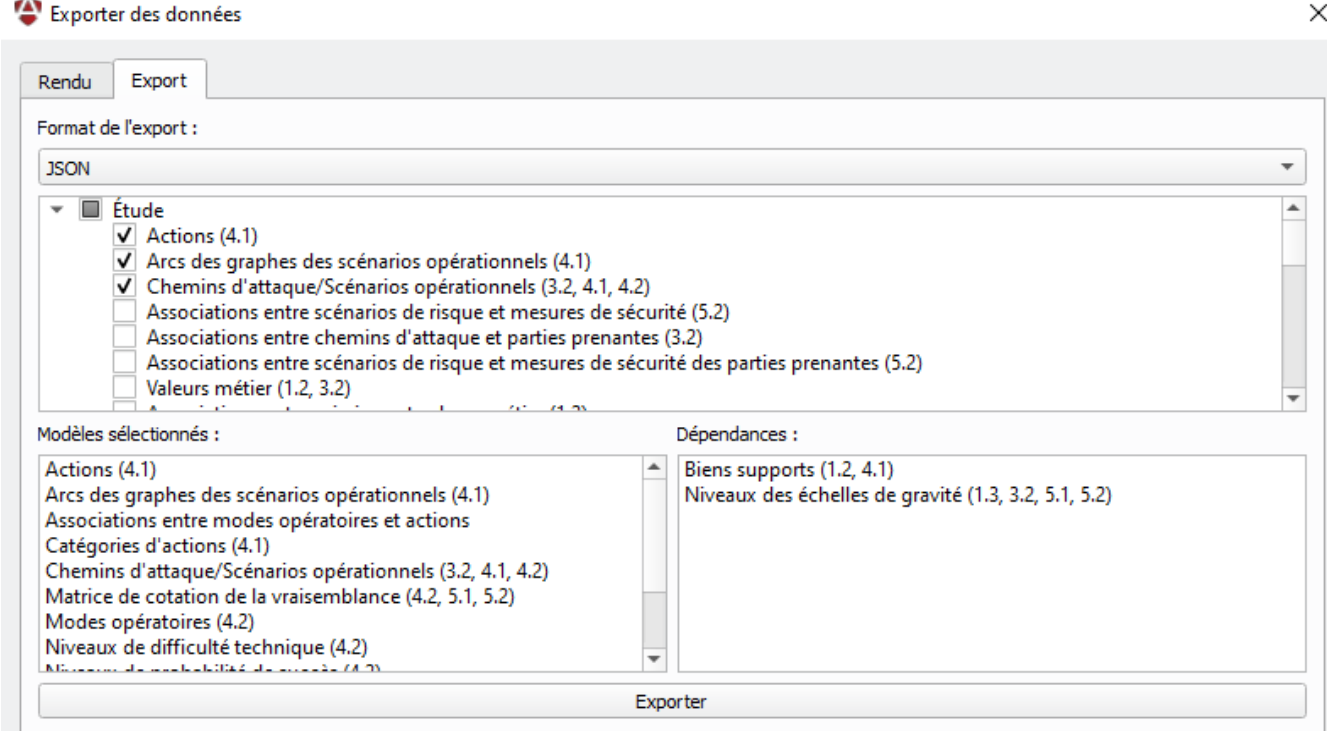
Le premier type d'export est l'export pour rendu, qui permet de générer des « rapports » de l'étude. Ces rapports contiennent uniquement les données de l'application, présentées dans un format proche de celui de l'application. Ce type d'export est accessible via l'onglet « Rendu » de la fenêtre :



Ici, ce ne sont pas les données mais les éléments graphiques (tableaux, cartographies) de l'application qui sont à sélectionner. Chacun des éléments sélectionnés sera présenté dans le document, avec un titre, puis l'élément (tableau, image pour les radars, etc...), à la suite, dans l'ordre de l'application. Le format d'export est à choisir parmi PDF, ODT (texte enrichi, permet de modifier les éléments par la suite), CSV (contient uniquement les données, pas de graphiques), ou HTML.

10.3.2. Export pour import

L'onglet pour ce type d'export est le deuxième, nommé « Export » :



Ce type d'export propose les données à exporter, qui peuvent être sélectionnées ou non en cochant les cases correspondantes. En fonction des données sélectionnées, certaines autres données nécessaires pour garantir l'intégrité seront également sélectionnées comme dépendances. Ainsi, l'export des scénarios stratégiques nécessitera par exemple l'export des évènements redoutés car ceux-ci sont liés aux scénarios stratégiques.

Une fois les données (« modèles ») à exporter sélectionnées, cliquer sur le bouton « Exporter » ouvrira une autre fenêtre afin de sélectionner le fichier dans lequel enregistrer les données. Ces données pourront ensuite être importées dans d'autres analyses via la fonction d'import.


En fonction du bouton utilisé, les données sélectionnées à l'ouverture de la fenêtre changent pour correspondre à celles qui sont associées au bouton (données de l'atelier, ou d'une table en particulier par exemple).

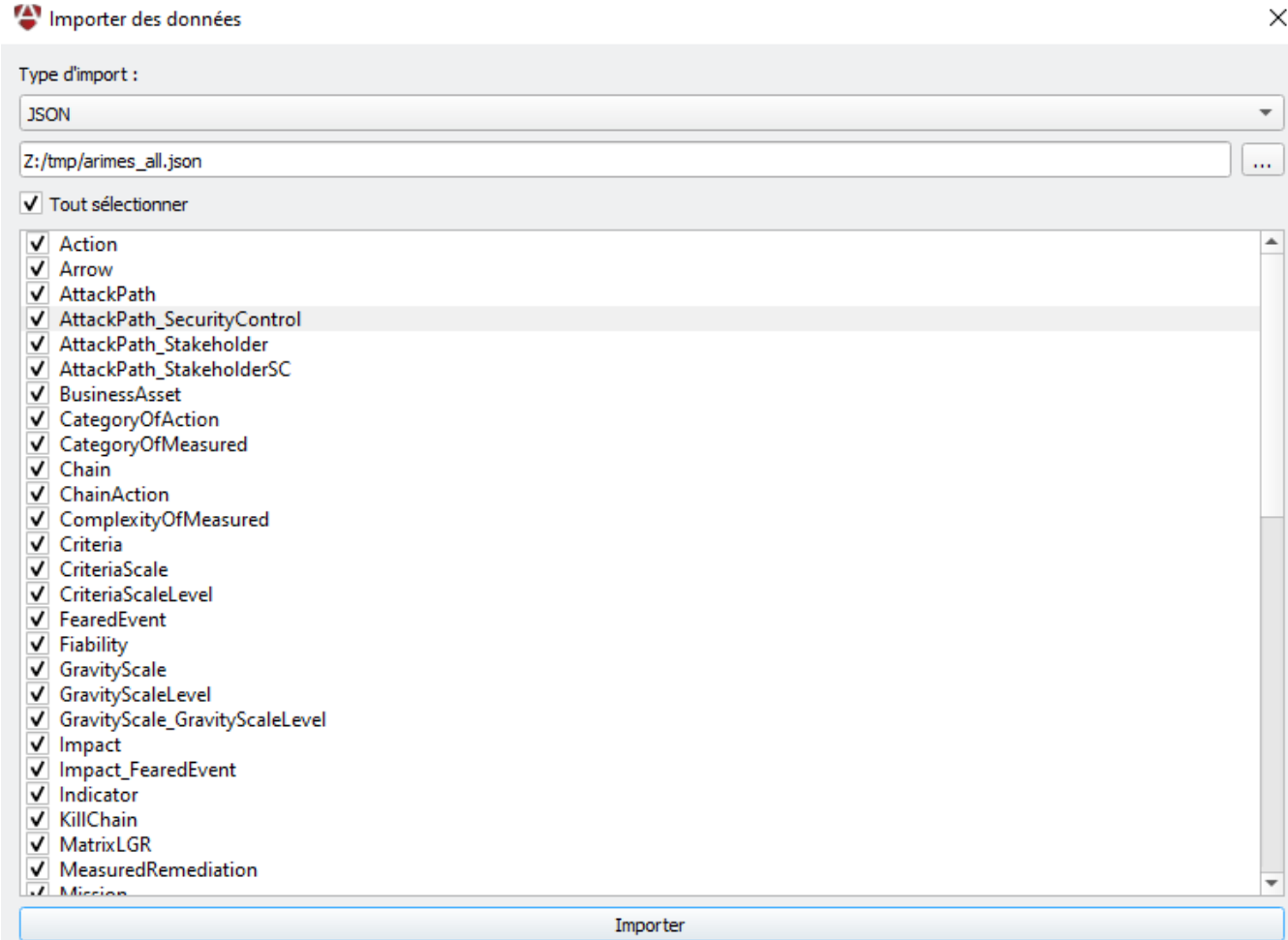
Remarque :

Les fichiers générés par cette fonctionnalité d'export identifient les éléments par un identifiant numérique. Il est donc déconseillé de modifier ces fichiers avant de les importer, car une mauvaise manipulation pourrait porter atteinte à l'intégrité du fichier.

Les identifiants numériques affichés dans l'export ne seront pas nécessairement (c'est même peu probable) ceux des éléments une fois importés. Tenter de modifier les fichiers d'export ou les fichiers .arimes en supposant le contraire pourrait mener à des résultats inattendus.

10.4. Fenêtre d'import

La fenêtre d'import est accessible en cliquant sur le bouton . Celle-ci présente un formulaire permettant de spécifier le type de données (JSON ou CSV), le nom du fichier à importer, ainsi que la liste des éléments du fichier qu'il faut importer.



Importer des données

Type d'import :
JSON

Z:/tmp/arimes_all.json

Tout sélectionner


- Action
- Arrow
- AttackPath
- AttackPath_SecurityControl
- AttackPath_Stakeholder
- AttackPath_StakeholderSC
- BusinessAsset
- CategoryOfAction
- CategoryOfMeasured
- Chain
- ChainAction
- ComplexityOfMeasured
- Criteria
- CriteriaScale
- CriteriaScaleLevel
- FearedEvent
- Fiability
- GravityScale
- GravityScaleLevel
- GravityScale_GravityScaleLevel
- Impact
- Impact_FearedEvent
- Indicator
- KillChain
- MatrixLGR
- MeasuredRemediation
- Mission

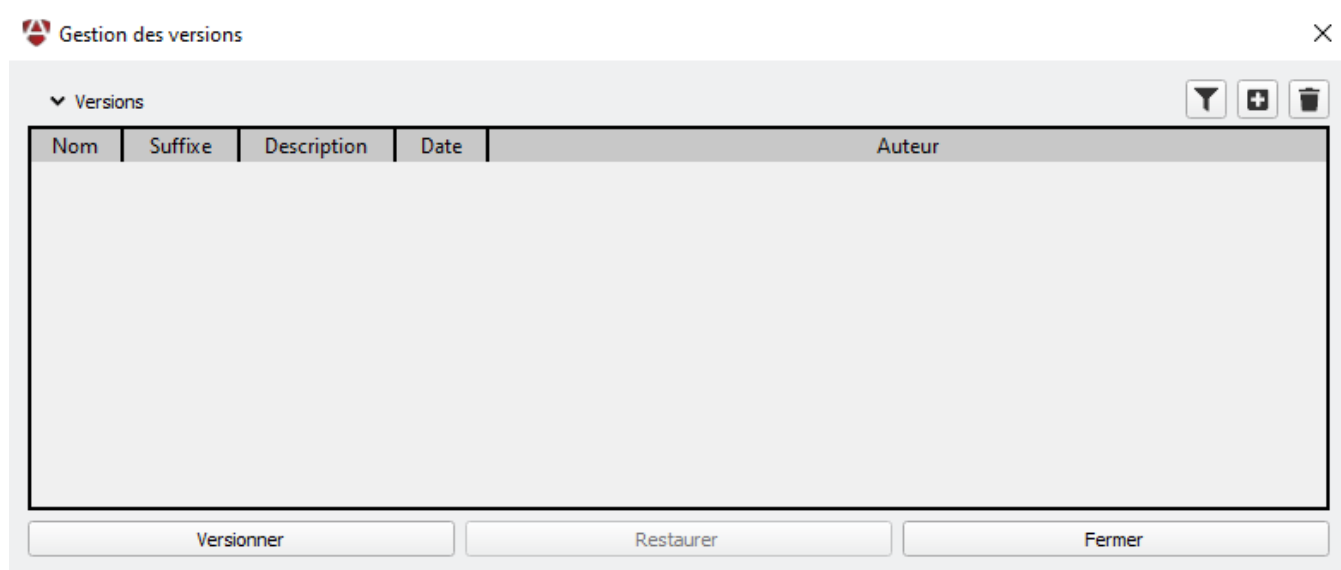
Importer

Il est possible de n'importer qu'une partie des éléments du fichier en cochant ou décochant les éléments.

Lors de l'import de données, il se peut qu'un conflit soit détecté, c'est-à-dire un élément à importer qui est similaire à un élément existant. Dans ce cas, l'application demandera s'il faut copier l'élément ou le fusionner. Dans le cas d'une fusion, l'élément à importer sera considéré comme étant l'élément existant ; si des éléments sont associés à cet élément dans le fichier à importer, alors ils seront associés à l'élément existant à la place. Il est possible de choisir au cas par cas s'il convient de fusionner ou de copier, mais il est également possible de faire un choix pour tous les autres conflits, avec le bouton « Fusionner tout » par exemple.

10.5. Fenêtre de versions

La fenêtre de version est accessible avec le bouton . Celle-ci permet de créer une version de l'étude, et de voir les versions existantes dans un tableau :




Il est également possible de visualiser l'étude telle qu'elle était dans une autre version, en sélectionnant la version et en cliquant sur le bouton « Versionner ». L'application affiche alors l'étude telle qu'elle était lorsque la version a été créée. L'application est toutefois en mode lecture seule, l'étude n'est plus modifiable. Afin de modifier l'étude, il est nécessaire de revenir à son état actuel en cliquant sur bouton « Restaurer » de la fenêtre.

Remarque :

Le champ « suffixe » est un champ qui nécessite seulement d'être unique. Lorsqu'une version est créée, toutes les tables de la base de données sont dupliquées, avec le suffixe ajouté au nom de chaque table. Il s'agit donc d'une capture instantanée de l'état de la base de données. Afin de ne pas rencontrer d'erreurs, éviter les caractères spéciaux dans le suffixe.

11. IMPORT DE DONNEES UTILISATEUR

Certains éléments de l'application peuvent être importés à partir de fichiers CSV fournis par l'utilisateur. Ces fichiers CSV n'ont rien à voir avec les fichiers CSV fournis par l'export de l'application. Le format de ces fichiers dépend des données à importer, et est décrit ci-après. Un tel import est accessible avec le

bouton  , qui est disponible pour importer des exigences (activité 1.4), la métrique de cotation de l'atelier 2 (configuration de l'atelier 2), les critères de l'atelier 3 (configuration de l'atelier 3), les catégories de parties prenantes (activité 3.1), et la métrique de cotation de l'atelier 4 (configuration de l'atelier 4).


11.1. Import d'exigences

L'import d'exigences est accessible via le bouton  situé sur la table des référentiels dans l'activité 1.4 :

Cadrage et socle de sécurité

Activité 1.1 Activité 1.2 Activité 1.3 Activité 1.4

Déterminer le socle de sécurité

▼ Référentiels 

Titre	Type	Description	Indicateur
Guide d'hygiène informatique de l'ANSSI	Règles d'hygiène informatique et bonnes pratiques	Ce guide comporte 42 mesures permettant de renforcer la sécurité de son système d'information.	Appliqué partiellement

▼ Exigences : Guide d'hygiène informatique de l'ANSSI


Niveau	Titre	Description	Appliqué	Commentaire
1	R01 Former les équipes opérationnelles à la sécurité des systèmes d'information	Former les équipes opérationnelles à la sécurité des systèmes d'information	<input type="checkbox"/>	En cours
2	R02 Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique	<input type="checkbox"/>	A venir
1	R03 Maîtriser les risques de l'infogérance	Maîtriser les risques de l'infogérance	<input type="checkbox"/>	En cours
1	R04 Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau	<input type="checkbox"/>	A commencer
1	R05 Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour	<input checked="" type="checkbox"/>	Terminé
2	R06 Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs	<input checked="" type="checkbox"/>	Terminé
2	R07 Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés	<input type="checkbox"/>	A venir

Il est nécessaire d'avoir au préalable créé et sélectionné le référentiel dans lequel doit se faire l'import. Le format du fichier CSV est le suivant :

- Une exigence par ligne
- Sur chaque ligne, dans l'ordre : le niveau, le titre, la description, l'état (appliqué ou non), et le statut.

- Les champs titre, description et statut sont des champs libres, le niveau est un entier arbitraire, et l'état doit être 0 si l'exigence n'est pas appliquée, ou 1 si elle l'est.

11.2. Import de la métrique de cotation de l'atelier 2

L'import de la métrique de cotation de l'atelier 2 se fait via le bouton  situé sur la matrice de cotation, dans la vue configuration de l'atelier 2 :

Sources de Risques / Objectifs Visés

Métrique sélectionnée (Étude) : Métrique par défaut

▼ Métriques de cotation

Titre

Métrique par défaut
tertre

Sélectionner cette métrique pour l'ensemble de l'étude peut entraîner la perte des valeurs de motivation, ressources et pertinence déjà associées. Il sera donc nécessaire de réévaluer les couples SR/OV suite à un changement de métrique.

Sélectionner la métrique

▼ Échelle de motivation : Métrique par défaut

Titre

+
++
+++

▼ Échelle de ressources : Métrique par défaut

Titre

+
++
+++

▼ Échelle de pertinence : Métrique par défaut

Titre

Faible
Moyenne
Élevée


▼ Matrice de cotation de la pertinence : Métrique par défaut

RESSOURCE	MOTIVATION		
	+	++	+++
+	Faible	Faible	Moyenne
++	Faible	Moyenne	Élevée
+++	Moyenne	Élevée	Élevée

Le format du fichier CSV est le suivant :




- Sur la première ligne, la liste des ressources, dans l'ordre
- Sur la seconde ligne, la liste des valeurs de motivation, dans l'ordre
- Sur la troisième ligne, la liste des valeurs de pertinence, dans l'ordre, avec pour chaque valeur le nom, suivi de la couleur (au format #89ABCD, où 89ABCD est le code hexadécimal de la couleur)
- Sur les lignes suivantes, les valeurs de pertinence telles qu'elles doivent apparaître dans le tableau (dans l'exemple ci-dessus, il y aurait donc trois lignes : « Faible, Faible, Moyenne », « Faible, Moyenne, Élevée » et « Moyenne, Élevée, Élevée »).

11.3. Import de critères de cotation des parties prenantes (atelier 3)




L'import de critères d'évaluation des parties prenantes se fait via le bouton  situé sur le tableau de critères dans la vue configuration de l'atelier 3 :

Scénarios stratégiques

Métrique sélectionnée (Étude) : Métrique classique

▼ Critères  ▼ Échelles du critère : Dépendance  ▼ Niveaux : Échelle dépendance 


Référence	Titre	Type	Échelle	Titre	Valeur	Description
DEP	Dépendance	Exposition	Échelle dépendance	Échelle dépendance	1	Relation non nécessaire aux fonctions stratégiques.
PEN	Pénétration	Exposition	Échelle de pénétration		2	Relation utile aux fonctions stratégiques.
MAT	Maturité	Fiabilité cyber	Échelle de maturité cyber		3	Relation indispensable mais non exclusive.
CON	Confiance	Fiabilité cyber	Échelle de confiance		4	Relation indispensable et unique (pas de substitution possible à court terme).

▼ Métriques de cotation  ▼ Zones  ▼ Seuls de fiabilité 

Nom	Description
Métrique classique	La métrique utilisée en exemple dans le guide de la méthode EBIOS RM.

Changer de métrique peut entraîner la perte de données, telles que l'évaluation des parties prenantes selon certains critères.

Nom	Valeur	Max
Zone de danger	2.5	<= 2
Zone de contrôle	1	4
Zone de veille	0	6
		> 6


▼ Description de la métrique : Métrique classique 

Dépendance	Pénétration	Maturité	Confiance
Relation non nécessaire aux fonctions stratégiques.	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
Relation utile aux fonctions stratégiques.	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
Relation indispensable mais non	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode	Les intentions de la partie prenante sont connues et probablement positives.

Le fichier CSV doit avoir le format suivant :



- Sur chaque ligne, un critère avec une échelle et les niveaux de l'échelle
- Pour chaque critère, sur la même ligne, dans l'ordre : la référence du critère, le titre du critère, le type du critère, le nom de l'échelle, puis pour chaque niveau de l'échelle, deux colonnes : une valeur et une description.
- Le type du critère peut être 1, ou n'importe quelle valeur commençant par « e » ou « E » pour « Exposition », sinon le type sera considéré comme étant « Fiabilité »
- Il est nécessaire de créer la métrique utilisant ces critères ensuite, avec la formule adéquate, de façon habituelle.

11.4. Import des catégories de parties prenantes (activité 3.1)

L'import des catégories de parties prenantes se fait en utilisant le bouton  situé sur le tableau de catégories de parties prenantes, dans l'activité 3.1 :

Activité 3.1 Activité 3.2 Activité 3.3

Construire la cartographie de menace numérique de l'écosystème

▼ Catégories de parties prenantes  ▼ Parties Prenantes 

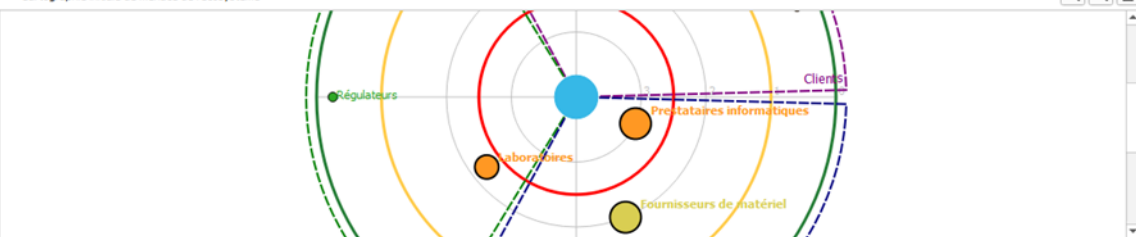
Référence	Titre	Description	Type
CLI	Clients	Clients de l'organisation	Externe
PAR	Partenaires	Partenaires de l'organisation	Externe
PRE	Prestataires	Prestataires (sous-traitants) de l'organisation	Externe

Référence	Titre	Description	Catégorie
C1	Établissements de santé	Hôpitaux, cliniques, etc...	Clients
C2	Pharmacies	Pharmacies	Clients
C3	Grossistes répartiteurs	Intermédiaires entre les clients et l'organisation	Clients
P1	Universités	Universités collaborant sur la recherche	Partenaires
P2	Régulateurs	Sociétés indépendantes de contrôle	Partenaires
P3	Laboratoires	Laboratoires dans lesquels sont effectués les recherches et tests	Partenaires
F1	Fournisseurs industriels chimistes	Fournisseurs des matières premières pour la recherche et la production	Prestataires

▼ Menace numérique de l'écosystème

Catégorie	Titre	Dépendance	Pénétration	Maturité	Confiance	Valeur calculée	Valeur manuelle	Retenue
Clients	Établissements de santé	1	1	1	3	0.333333		<input type="checkbox"/>
Clients	Pharmacies	1	1	2	3	0.166667		<input type="checkbox"/>
Clients	Grossistes répartiteurs	1	2	2	3	0.333333		<input type="checkbox"/>
Partenaires	Universités	2	1	1	2	1		<input type="checkbox"/>
Partenaires	Régulateurs	2	1	2	4	0.25		<input type="checkbox"/>
Partenaires	Laboratoires	3	3	2	2	2.25		<input checked="" type="checkbox"/>
Prestataires	Fournisseurs industriels chimistes	4	2	2	3	1.333333		<input type="checkbox"/>
Prestataires	Fournisseurs de matériel	4	3	2	3	2		<input checked="" type="checkbox"/>
Prestataires	Prestataires informatiques	3	4	2	2	3		<input checked="" type="checkbox"/>

▼ Cartographie initiale de menace de l'écosystème



La cartographie initiale de menace de l'écosystème est un diagramme circulaire centré sur un point bleu. Elle est divisée en zones concentriques et radiales. Les zones radiales sont étiquetées : 'Régulateurs' (à gauche), 'Laboratoires' (en bas à gauche), 'Fournisseurs de matériel' (en bas à droite), et 'Clients' (à droite). Des arcs concentriques sont également présents, avec des étiquettes 'Prestataires informatiques' et 'Clients' à l'extérieur.

Le format du fichier CSV doit être le suivant :

- Sur chaque ligne une catégorie
- Pour chaque catégorie, dans l'ordre : la référence, le titre, la description, le type
- Le type peut être 1 ou n'importe quelle valeur commençant par « i » ou « l » pour « interne », sinon le type sera considéré comme externe.

11.5. Import de la métrique de cotation de l'atelier 4



L'import de la métrique de cotation dans la configuration de l'atelier 4 se fait en utilisant le bouton situé sur la matrice de cotation dans la vue configuration de l'atelier 4 :

Scénarios opérationnels

Séquence sélectionnée (Étude) : CyberKillChain

▼ Séquences d'attaque

Titre
CyberKillChain

▼ Phases : CyberKillChain

Nom
Connaître
Rentrer
Trouver
Exploiter

▼ Catégorie d'actions

Titre	Description
Reconnaissance... externe de la cible	Lors de la phase de reconnaissance, la source de risque va rechercher dans l'ensemble de ses bases disponibles les informations nécessaires à la planification de son attaque. Les données collectées peuvent être de nature technique ou concerner l'organisation de la cible et de son écosystème. Les moyens employés peuvent être très variés : - réseaux sociaux (social engineering) ; - Internet (poubelles numériques, sites) ; - forums de discussion sur Internet ; - forums et salons professionnels ; - faux client, faux journaliste, etc. ; - prise de contact directe (anciens salariés, etc.) ; - officines ou agences spécialisées (sources

▼ Probabilité de succès

Nom
Quasi-certaine
Très élevée
Significative
Faible

▼ Difficulté technique

Nom
Faible
Modérée
Élevée
Très élevée

▼ Échelle de vraisemblance

Nom	Description
Quasi-certain	La source de risque va très certainement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est très élevée.
Très vraisemblable	La source de risque va probablement atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est élevée.
Vraisemblable	La source de risque est susceptible d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
Peu vraisemblable	La source de risque a relativement peu de chances d'atteindre son objectif en empruntant l'un des modes opératoires envisagés. La vraisemblance du scénario de risque est faible.

▼ Matrice de cotation de la vraisemblance

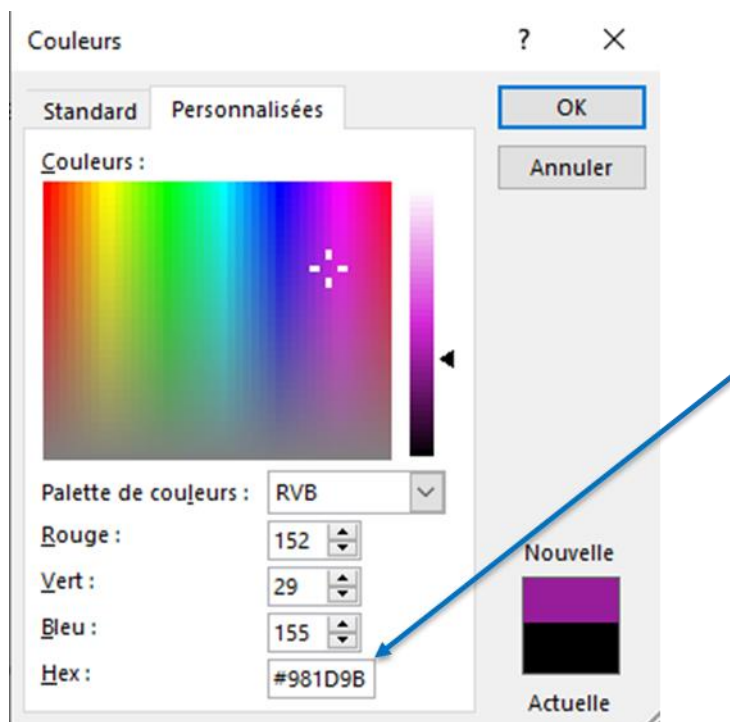
Probabilité de succès	Difficulté technique			
	Faible	Modérée	Élevée	Très élevée
Quasi-certaine	Quasi-certain	Quasi-certain	Très vraisemblable	Très vraisemblable
Très élevée	Quasi-certain	Très vraisemblable	Vraisemblable	Vraisemblable
Significative	Très vraisemblable	Vraisemblable	Vraisemblable	Peu vraisemblable
Faible	Très vraisemblable	Vraisemblable	Peu vraisemblable	Peu vraisemblable

Le format du fichier CSV doit être le suivant (similaire à l'import de la métrique de l'atelier 2) :

- Sur la première ligne, les valeurs de probabilité de succès, dans l'ordre, deux colonnes par élément : la première contient l'étiquette et la seconde la couleur (au format #89ABCD, où 89ABCD est la représentation hexadécimale RGB de la couleur)
- Sur la seconde ligne, les valeurs de difficulté technique, dans l'ordre, au même format (étiquette puis couleur)
- Sur la troisième ligne, les valeurs de vraisemblance, avec trois colonnes par valeur : le nom, la couleur (au même format que sur les autres lignes) puis la description
- Sur les autres lignes, la matrice de cotation telle qu'elle doit apparaître dans l'application, avec les étiquettes de la vraisemblance. Par exemple, pour l'exemple ci-dessus, elle serait constituée de quatre lignes : « Quasi-certain, Quasi-certain, Très vraisemblable, Très vraisemblable », « Quasi-certain, Très vraisemblable, Vraisemblable, Vraisemblable », « Très vraisemblable, Vraisemblable, Vraisemblable, Peu vraisemblable », « Très vraisemblable, Vraisemblable, Peu vraisemblable, Peu vraisemblable ».

11.6. Généralités sur les imports CSV utilisateur

- Les fichiers doivent être au format CSV « classique », c'est-à-dire que le séparateur de colonnes doit être la virgule « , ». Pour insérer une virgule dans une entrée, il faut mettre l'ensemble des données de la colonne entre guillemets « " ». Pour insérer un guillemet « " », il faut mettre la colonne entre guillemets « " » et doubler les guillemets à insérer. Par exemple, le champ « Présentation du projet "Arimes", application de mise en œuvre d'analyse de risques selon la méthode EBIOS Risk Manager » doit être renseigné comme cela : « "Présentation du projet ""Arimes"", application de mise en œuvre d'analyses de risques selon la méthode EBIOS Risk Manager" ».
- Le renseignement de couleurs se fait en utilisant le code hexadécimal de la couleur, précédé d'un croisillon « # ». Le code hexadécimal est simplement une représentation des composantes rouge, vert, et bleu (RGB), dans cet ordre, en hexadécimal. Certains logiciels permettent d'obtenir cette valeur :



On peut remarquer que la valeur est constituée des composantes Rouge : 152, qui donne 98 en hexadécimal, Vert : 29, qui donne 1D en hexadécimal et Bleu : 155 qui donne 9B en hexadécimal, d'où le code hexadécimal « #981D9B ».