Arimes Version 1.2.0

Adacis

25 mars 2025

	Liste	des Figures	iii
1	Intro	duction	1
2	Procé 2.1 2.2	d ure de démarrage Installation de l'application Arimes	3 3 3
3	Prése 3.1 3.2 3.3	ntation générale de l'application Généralités sur l'interface d'Arimes Description des boutons globaux de l'application Description générale de l'interface des tables	5 5 6 7
4	Prése 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8	ntation détaillée de l'applicationPrésentation des éléments globaux de l'applicationPage d'accueilAtelier 1 : Cadrage et socle de sécuritéAtelier 2 : Sources de Risques et Objectifs VisésAtelier 3 : Scénarios stratégiquesVersion simplifiée de l'atelier 3Atelier 4 : Scénarios opérationnelsAtelier 5 : Traitement du risque	9 9 . 17 . 18 . 26 . 29 . 33 . 34 . 39

Figure 2.1: Page d'accueil de l'application.	4
Figure 3.1: Détail de l'interface générale de l'application	6
Figure 3.2: Exemple de table de l'application	7
Figure 3.3: Redimensionnement d'une colonne en étirant l'en-tête.	8
Figure 4.1: Modale de versioning	0
Figure 4.2: Onglet Export de la modale d'export	1
Figure 4.3: Fenêtre modale d'import	2
Figure 4.4: Onglet <i>Rendu</i> de la fenêtre modale d'export	3
Figure 4.5: Exemple d'identifiant d'export	4
Figure 4.6: Exemple de template Word affichant les objectifs de l'étude	4
Figure 4.7: Rapport produit par le template montré dans Figure 4.6	5
Figure 4.8: Fenêtre modale d'export docx	6
Figure 4.9: Fenêtre modale de configuration de l'application	7
Figure 4.10: Page d'accueil de l'application	8
Figure 4.11: Activité 1.1	9
Figure 4.12: Activité 1.2	0
Figure 4.13: Activité 1.3	1
Figure 4.14: Configuration de l'activité 1.3	1
Figure 4.15: Activité 1.4	2
Figure 4.16: Configuration de l'activité 1.4	3
Figure 4.17: Activité 2.1	6
Figure 4.18: Version simplifiée de l'atelier 2	7
Figure 4.19: Configuration de l'atelier 2	7
Figure 4.20: Activité 2.2	8
Figure 4.21: Activité 2.3	9
Figure 4.22: Page de configuration de l'atelier 3	0
Figure 4.23: Activité 3.1	1
Figure 4.24: Activité 3.2	2
Figure 4.25: Activité 3.3	3
Figure 4.26: Version simplifiée de l'activité 3.1	4
Figure 4.27: Page de configuration de l'atelier 4	5
Figure 4.28: Activité 4.2 : méthode expresse	7
Figure 4.29: Activité 4.2 : méthode standard	8
Figure 4.30: Activité 4.2 : méthode avancée	9
Figure 4.31: Page de configuration de l'atelier 5	0
Figure 4.32: Activité 5.1	1
Figure 4.33: Activité 5.2	2
Figure 4.34: Activité 5.3	3

Chapitre 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

- Le guide officiel de la méthode
- La FAQ du club EBIOS

La documentation concerne la version 1.2.0 de l'application.

Procédure de démarrage

2.1 Installation de l'application Arimes

L'application Arimes existe pour Windows ou Linux.

2.1.1 Installation pour Windows

L'installation sur Windows s'effectue à l'aide de l'installeur Windows présent dans l'archive fournie. Il suffit d'exécuter le fichier arimes_setup_<version>.exe (par exemple arimes_setup_1.2.0.exe), et de suivre le programme d'insallation. Par défaut, le programme d'installation installera l'application dans le dossier AppData de l'utilisateur installant l'application. Cela permet d'installer le logiciel même sans disposer de droits élevés sur la machine, mais présente l'inconvénient de devoir installer l'application pour chaque utilisateur.

Il est toutefois possible que des politiques organisationnelles empêchent l'installation. Dans ce cas, contacter les administrateurs de la machine afin de leur demander d'installer l'application.

Il est également possible que Windows détecte l'application comme une application dangereuse et refuse d'exécuter le programme d'installation. Dans ce cas, il faut aller dans les propriétés de l'exécutable (clic droit -> propriétés depuis l'explorateur de fichiers) et cocher la case « Débloquer » en bas de la fenêtre.

Une fois l'application installée, celle-ci devient disponible depuis le menu démarrer. Le plus simple est de chercher Arimes depuis le menu démarrer ; si l'installation s'est bien effectuée, l'application devrait apparaitre.

2.1.2 Pour Linux

Pour Linux, il n'y a pas besoin d'exécuter de programme d'installation, il suffit d'accéder au dossier de l'application dans l'archive fournie, et d'exécuter le script Arimes. Il est possible de créer un lien symbolique vers ce script dans un dossier du PATH de l'utilisateur afin de pouvoir lancer l'application simplement avec la commande Arimes.

Note L'exécutable Arimes est un script qui permet d'éxécuter le véritable binaire du dossier bin en utilisant les bibliothèques du dossier lib. L'application est ainsi fournie avec toutes ses dépendances, et ne requiert l'installation d'aucun autre élément.

2.2 Premier lancement de l'application

Lors du lancement de l'application, celle-ci ouvre la dernière étude ouverte. Si le fichier n'existe plus (ou lors du premier lancement), une fenêtre s'ouvre proposant trois choix : créer une nouvelle étude,

ouvrir une étude existante ou quitter l'application :



Sélectionner l'option ouvrir une autre étude afin d'ouvrir, par exemple, l'étude d'exemple fournie avec le logiciel.

Conseil Il n'est pas recommandé de créer une nouvelle étude, car cela demande de redéfinir toutes les échelles et la configuration. Créer une étude vide, contenant la configuration adaptée à l'organisation, et s'en servir comme base pour les nouvelles études est la méthode conseillée pour commencer une étude.

Une fois l'étude sélectionnée, celle-ci s'ouvre et la page d'accueil du logiciel s'affiche :



Figure 2.1. Page d'accueil de l'application

Présentation générale de l'application

Arimes est une application permettant de conduire des études des risques cyber selon la méthode EBIOS Risk Manager. L'application essaie de se rapprocher visuellement du guide de la méthode, et adopte le même code couleur que celle-ci. Ainsi, l'application présente les cinq ateliers de la méthode dans des éléments séparés, chacun étant divisé en plusieurs activités, qui correspondent à celles présentent dans le guide.

L'application est une application de type *standalone*, qui permet de mener une étude à la fois. Toutes les données des études sont stockées dans des fichiers .arimes, qui contiennent l'intégralité des éléments propres à une étude. Il est donc possible d'échanger, de copier, ou encore d'archiver ces fichiers afin de pouvoir collaborer sur une étude ou de les réutiliser ultèrieurement. Ces fichiers disposent d'un format propre à la version du logiciel utilisée. Lorsqu'une étude créée avec une version précédente est ouverte dans une version plus récente de l'application, celle-ci effectue une migration de l'étude afin de la transformer dans le format de la nouvelle version. Cette opération s'effectue sans perte de données, mais une sauvegarde est tout de même réalisée dans un fichier portant le nom de l'étude .arimes avec le suffixe .old ajouté (ou .old_1, .old_2, etc... en fonction des fichiers déjà existants) avant d'effectuer la migration. L'application demande confirmation avant de procéder à la migration d'une étude.

3.1 Généralités sur l'interface d'Arimes

Note 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.

Arimes Expert - Fabrication de vaccins (C1 - Public)	~
Accueil Actier 3 Actier 3 Actier 5	C1 - Public
3 Cadrage et socle de sécurité	4 🔳
Activite 1.1 Activite 1.2 Activite 1.3 Activite 1.4	
Définir le cadre de l'étude	
Cycles stratégiques et opérationnels 10	0 2 i T 1 0
Type Nom Date de début Date de fin Contraintes Cycle créé durant la migration de l'étude dans la nouvelle version Contraintes Final de l'étude dans la	Hypothèses
Stratégique Test export 05/03/2025 05/03/2025 Pas de contrainte. Pas de	
	,
Objectifs de létude Varticipants Varticipant	
	Societe
Matrice RACI (Responsible, Accountable, Consulted, Informed)	
Ateliers	
	4 5
v Ülementr da olympian	
entremain of particular default parts de fin Description	
	Þ

Figure 3.1. Détail de l'interface générale de l'application

L'application se décompose en six pages principales : une page d'accueil, et une page pour chaque atelier de la méthode. Ces pages sont accessibles via les boutons correspondant dans le bandeau supérieur central de l'application (élément 1 de Figure 3.1).

Les boutons présents dans le bloc 2 sont toujours visibles, quelle que soit la page sélectionnée. Ces boutons sont détaillés dans la section 3.2.

Sur les pages des ateliers, le titre de l'atelier est présent en 3 et des actions spécifiques à l'atelier sont possibles avec l'utilisation des boutons en 4. Les ateliers suivent le code couleur du guide.

3.2 Description des boutons globaux de l'application

Les boutons globaux sont les boutons toujours visibles du bloc 2 de l'image Figure 3.1. Ces boutons sont les suivants :

- Dermet de créer une nouvelle étude vide (déconseillé, voir la note à ce sujet)
- En permet d'ouvrir une étude existante (.arimes). Lors du démarrage d'une nouvelle étude, il est conseillé d'ouvrir une étude contenant les échelles et les éléments de configuration propres à l'entreprise plutôt que de créer une étude vide.
- Deprive de créer une copie de l'étude actuelle. L'application sauvegarde toutes les modifications en temps réel, le bouton de sauvegarde crée seulement une copie du fichier .arimes, mais ne l'ouvre pas (l'application continuera d'écrire dans le fichier original). Afin d'ouvrir la nouvelle étude, utiliser le bouton d'ouverture d'une étude existante.

permet de créer des versions archivées de l'étude. Il n'est pas conseillé d'utiliser cette fonctionnalité car elle augmente significativement la taille du fichier de l'étude sur le disque. Afin de créer des versions de l'étude, le plus simple est simplement de créer des copies de l'étude (.arimes) dans des fichiers séparés.

- exporté de l'application.
- permet d'exporter les données de l'étude, soit pour créer un rendu (rapport), soit pour pouvoir les réimporter ulérieurement.
- permet de générer un rapport au format Docx à partir d'un fichier de template.
- permet d'accéder à la configuration générale de l'application (langue) et d'afficher des informations concernant la version et les changements apportés (changelog).

3.3 Description générale de l'interface des tables

✓ Miss	ions de l'organisme 🚯 2			3[۵	1	r 1	¢ 2
	Intitulé	Description	Valeurs métier associées					
Identifi	er et fabriquer des vaccins	Identifier (recherche) des vaccins et les fabriquer	Fabriquer des vaccins Traçabilité et contrôle test Recherche & développement (R&O)					

Figure 3.2. Exemple de table de l'application

La plupart des éléments de l'application sont présentés dans des tables telles que celle de Figure 3.2. Ces tables montrent les éléments existants et permettent leur modification. Certains éléments de l'application sont différents (par exemple des graphiques). Ces éléments seront détaillés dans les parties spécifiques de ce guide.

Le titre des tables et des autres éléments (élément 1 de Figure 3.2) est un bouton cliquable qui permet de cacher ou montrer la table. Cacher des éléments permet de laisser plus de place aux autres éléments afin de mieux les visualiser.

L'info-bulle d'aide (élément 2 de Figure 3.2) permet d'obtenir des informations concernant ce que la

méthode préconise pour remplir la table. L'aide s'affiche au survol de l'icône 🔍

Les tables permettent d'effectuer les actions suivantes sur les éléments associés, à travers les boutons du bloc 3 :

- 🕒 ce bouton permet d'ouvrir le formulaire de création
- Ce bouton permet d'ouvrir le formulaire d'édition, afin d'éditer la ligne sélectionnée. Ce bouton n'a aucun effet si aucune ligne de la table n'est sélectionné
- Les lignes sélectionnée(s)
- Ce bouton permet d'ouvrir le formulaire de filtre, qui permet de n'afficher que les éléments répondant aux critères indiqués dans la table
- Ce bouton (qui remplace le bouton de filtre lorsqu'un filtre est appliqué sur la table) permet d'annuler les effets de filtre

- 🖆 ce bouton permet d'ouvrir le formulaire d'export, avec les données de la table déjà sélectionnées
- ce bouton permet d'ouvrir le formulaire de configuration de la table, qui permet de sélectionner des colonnes à cacher

Il est également possible d'éditer des champs directement depuis la table en double-cliquant sur la case à éditer. Un éditeur s'ouvre alors, dépendant du type de données. Afin de valider l'édition, il est parfois nécessaire de sélectionner une case différente du tableau pour fermer l'éditeur.

Les colonnes des tableaux peuvent être redimensionnées en étirant les bords des cellules dans l'en-tête (voir Figure 3.3). Il est également possible de changer l'ordre des colonnes des tables en faisant un glisser-déposer de l'en-tête de la colonne à déplacer. Cliquer sur une colonne permet de trier les éléments de la table selon les valeurs de la colonne sélectionnée.



Figure 3.3. Redimensionnement d'une colonne en étirant l'en-tête

Présentation détaillée de l'application

Cette section présente l'ensemble des fonctionnalités offertes par l'application, en détaillant les différentes pages et les éléments qui les composent.

4.1 Présentation des éléments globaux de l'application

4.1.1 Création, ouverture et sauvegarde d'études

Les boutons **b**, **b** et **b** permettent respectivement de créer une nouvelle étude, ouvrir une étude existante (à partir d'un fichier .arimes) et de sauvegarder une copie de l'étude actuelle.

Toutes ces actions utilisent des boites de dialogues propres au système d'exploitation utilisé et à son environnement graphique afin de sélectionner le fichier où enregistrer ou à ouvrir.

Note Toutes les actions effectuées dans l'application sont immédiatement sauvegardées dans l'étude sélectionnée. C'est pourquoi le bouton de sauvegarde ne fait qu'enregistrer une copie de l'étude, mais n'ouvre pas cette copie. Ce bouton est à utiliser pour sauvegarder une version spécifique de l'étude. L'idée est donc d'avoir un fichier de travail, dont des copies seront créées lorsque des versions seront nécessaires.

Cela permet d'éviter de créer un fichier correspondant à une version et de le modifier par la suite en effectuant des modifications via l'application.

Note La sauvegarde d'une copie peut être faite au niveau du système en copiant le fichier d'étude (.arimes). Les deux actions sont strictement identiques.

4.1.2 Versioning de l'étude

L'application propose une fonction de versioning intégrée, qui permet de créer des versions de l'étude qu'il est ensuite possible de consulter en lecture seule. Cette fonctionnalité est accessible avec le

bouton . Elle ouvre une fenêtre modale telle que celle de Figure 4.1

1	1				Gestion des versions			~ ^ X
	 ✓ Versior 	ns 🚯						T 🗢
	Nom	Suffixe	Description	Date		Auteur		
		Versior	nner		Restaurer	Fe	ermer	

Figure 4.1. Modale de versioning

Cette modale permet d'accéder à une table permettant de consulter et créer des versions. Les versions disposent d'un nom et d'un suffixe qui doivent être uniques, ainsi que d'une description et d'un auteur. Le suffixe est utilisé en interne comme nom pour les données relatives à cette version.

Le bouton Versionner permet de visualiser la version sélectionnée, en basculant l'application en lecture seule. Afin de revenir à la version qui était en cours de modifications, utiliser le bouton Restaurer.

Attention! Il n'est pas conseillé d'utiliser cette fonctionnalité. Créer des copies du fichier .arimes est plus performant et évite les erreurs d'utilisation de l'application.

Cette fonctionnalité duplique intégralement l'étude en cours dans le fichier .arimes. Le fichier de l'étude contient donc toutes les données de l'étude pour chacune des versions existantes. Cela comporte l'inconvénient d'augmenter la taille du fichier de l'étude à chaque version créée. En cas d'archivage de l'étude, ce fichier sera donc de plus en plus gros. Bien que la taille de ces fichiers tende à rester faible, mieux vaut privilégier la copie du fichier .arimes.

De plus, la visualisation des versions bascule l'application en mode lecture seule. Ce mode est persistant au redémarrage de l'application, et peut causer une incompréhension de l'utilisateur, qui ne comprend pas nécessairement pourquoi l'étude est en lecture seule.

4.1.3 Import et export de données



Les boutons et et permettent respectivement d'importer des données, d'exporter des données dans différents formats et de réaliser un export avec des paramètres spécifiques pour le format Docx.

L'application distingue deux types d'export :

- 1. Les exports pour import, qui peuvent être réalisés au format JSON on CSV
- 2. Les rendus, dont le but est de fournir un document visualisable afin de générer un rapport par exemple. Plusieurs formats de fichier sont proposés par l'application, le plus intéressant étant le format Docx.

Export et import de données

La modale d'export accessible via le bouton comporte un onglet Export tel que dans Figure 4.2. Cet onglet permet d'exporter les données de l'application dans un fichier au format JSON ou CSV, afin de pouvoir les importer dans une autre étude via le bouton

Exporter des	données v ^ X
Rendu Export	
1 JSON	•
 Cátude Associations entre exigences (1.4) et mesures de sécu Actions (4.1) Base de connaissances d'actions (configuration 4) Arcs des graphes des scénarios opérationnels (4.1) Chemins d'attaque/Scénarios opérationnels (3.2, 4.1, 4.1) 	4.2)
Modèles sélectionnés : D	Vépendances :
Actions (4.1) Arcs des graphes des scénarios opérationnels (4.1) Associations entre chemins d'attaque et parties prenantes Associations entre exigences (1.4) et mesures de sécurité (Associations entre exigences (1.4) et mesures de sécurité d	4
Export	ter 5

Figure 4.2. Onglet Export de la modale d'export

Il est possible de n'exporter que certains éléments de l'étude, en les sélectionnant dans la fenêtre (élément 2 de Figure 4.2). Certains éléments ont des dépendances à d'autres éléments, qui devront nécessairement être importés également. Les éléments sélectionnés apparaissent dans la zone Modèles sélectionnés (élément 3 de Figure 4.2) et les dépendances dans la zone Dépendances de la fenêtre (élément 4 de Figure 4.2).

Une fois le format (élément 1 de Figure 4.2) et les éléments sélectionnés, le bouton Exporter (élément 5 de Figure 4.2) permet de sauvegarder le résultat de l'export dans un fichier (JSON ou CSV selon le format sélectionné).

Ce fichier peut ensuite être utilisé pour importer des élément dans une étude.

Afin d'importer les éléments, le bouton permet d'ouvrir une fenêtre modale telle que dans Figure 4.3.

Importer des données	~ ^ ×
Type d'import :	
JSON	•
2/tmp/arimes/export.json	3
Tout sélectionner	
Actions (4.1) Base de connaissances d'actions (configuration 4) Arcs des graphes des scénarios opérationnels (4.1) Chemins d'attaque/Scénarios opérationnels (3.2, 4.1, 4.2) Associations entre scénarios de risque et mesures de sécurité (5.2) Associations entre chemins d'attaque et parties prenantes (3.2) Associations entre scénarios de risque et mesures de sécurité des parties prenantes (5.2) Valeurs métier (1.2, 3.2) Associations entre valeurs métier et biens supports (1.2) Catégories d'actions (4.1) Catégories de mesures de sécurité (5.2) Modes opératoires (4.2) Associations entre modes opératoires et actions Complexités des mesures de sécurité (5.2) Critères d'évaluation des parties prenantes (3.1, 3.3) Échelles des critères (3.1, 3.3) Cycles stratégiques et opérationnels (5.3) Format de date (5.2) Kiveaux de fiabilité (3.1, 3.3)	
Importer 5	

Figure 4.3. Fenêtre modale d'import

Dans la Figure 4.3, renseigner le format (JSON ou CSV, élément 1) et le fichier à importer (élément 2) qui correspond à un fichier exporté tel que décrit précédemment. Il est possible de parcourir les fichiers grâce au bouton situé à côté du chemin à renseigner (élément 3). Une fois un fichier sélectionné, les éléments présents dans le fichier sont affichés dans la zone prévue à cet effet (élément 4). Il est possible de n'importer que certains éléments parmi tous ceux présents dans le fichier source. Certains éléments non sélectionnés seront tout de même importés s'il s'agit de dépendances indispensables à certains éléments sélectionnés. Par exemple, les chemins d'attaque n'existent que relativement à un scénario stratégique, ainsi ceux-ci seront importés si les chemins d'attaque le sont.

Export des données pour visualisation (rapport)

L'application fournit une fonctionnalité permettant d'exporter les données pour visualisation (rapport). Contrairement à l'export précédent, ici ce sont les tableaux de l'application et les graphes qui sont exportés. Parmi ces rendus, la plupart font un rendu de l'ensemble des éléments sélectionnés à la suite dans le format demandé. L'exception est l'export au format Docx, qui se fait avec l'utilisation de templates. Ces templates sont des fichiers Docx qui servent de canevas, et qui peuvent avoir n'importe quel contenu. L'export dans ces templates va simplement remplacer les occurrences de « variables » par les éléments de l'étude.

Afin d'effectuer un rendu, ouvrir la modale d'export avec le bouton *i*, et sélectionner l'onglet Rendu tel que dans Figure 4.4.



Figure 4.4. Onglet *Rendu* de la fenêtre modale d'export

Une fois les données à exporter (élément 1) et le format (élément 2) sélectionnés, le bouton imprimer dans le fichier permet de sélectionner le fichier dans lequel enregistrer les éléments. Dans le cas d'un export au format Docx, un fichier de template sera également demandé. *Spécificités de l'export Docx*

L'export Docx fonctionne selon un mécanisme de templating qui permet d'obtenir des rapports dans un format complexe avec peu de besoins de modifications une fois les données exportées. Ainsi, il est possible de créer un template comprenant toutes les informations sur l'étude, le projet, le contexte, etc... Puis d'y insérer les éléments de l'étude grâce à la fonctionnalité d'export vue précédemment. Les éléments exportés sont :

- les titres des tables ou graphiques ;
- les tables ;
- les graphiques

Chaque élément de l'application dispose d'un identifiant d'export qui s'affiche au survol du titre de l'élément. Dans les templates, il est possible d'exporter les titres des éléments en utilisant une variable \${<identifiant>Title}. L'élément associé (table ou graphique) peut être inséré dans le template avec la variable \${<identifiant>Object}.

Par exemple, pour exporter les objectifs avec leur nom (identifiant Objective, voir Figure 4.5), il faut utiliser les variables \${ObjectiveTitle} et \${ObjectiveObject} pour insérer le titre et la table, respectivement. Comme c'est le cas pour les objectifs, qui dépendent de leur cycle, il se peut que les variable Object insèrent une liste de tableaux ou une liste de graphiques, en fonction des éléments donc ils dépendent.



Figure 4.5. Exemple d'identifiant d'export

Ainsi, avec un document .docx contenant les éléments suivants :

^ICe texte ne sera pas changé par l'export.

Le template peut contenir des titres

Des sous-titres

Sur plusieurs niveaux

Et de la **mise** <u>en</u> forme, avec de la couleur.

Tout ceci sera inchangé.

L'application va changer le titre qui suit :

\${ObjectiveTitle}

Et insérer les tables des objectifs à la place de ce qui suit :

\${ObjectiveObject}

Il est possible d'écrire n'importe où dans le document, seules les variables connues de l'application (entre \${ et }} seront modifiées. Le reste du document reste intact.

Figure 4.6. Exemple de template Word affichant les objectifs de l'étude

Le résultat après export Docx est le suivant :

Ce texte ne sera pas changé par l'export.

Le template peut contenir des titres

Des sous-titres

Sur plusieurs niveaux

Et de la mise <u>en</u> forme, avec de la couleur.

Tout ceci sera inchangé.

L'application va changer le titre qui suit :

Objectifs de l'étude

Et insérer les tables des objectifs à la place de ce qui suit :

Objectifs pour le cycle Cycle créé durant la migration de l'étude dans la nouvelle version

	ATELIER A CONDUIRE						
OBJECTIF DE L'ETUDE	1	2	3	4	5		
Identifier le socle de sécurité adapté à l'objet de l'étude	х						
Etre en conformité avec les référentiels de sécurité numérique	х				х		
Evaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			х				
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		Х	Х				
Réaliser une étude préliminaire des risques pour identifier les axes prioritaires d'amélioration de la sécurité	х	х	х		х		
Conduire une étude des risques complète et fine, par exemple sur un produit de sécurité ou en vue de l'homologation d'un système	x	x	x	x	x		
Orienter un test de sécurité et notamment un test d'intrusion			х	х			
Orienter les dispositifs de détection et de réaction, par exemple au niveau d'un centre opérationnel de la sécurité (SOC)			х	x			

Il est possible d'écrire n'importe où dans le document, seules les variables connues de l'application (entre \${ et }) seront modifiées. Le reste du document reste intact.

Figure 4.7. Rapport produit par le template montré dans Figure 4.6.

Dans les exports ainsi produits, les tableaux exportés sont exportés sous forme de tables dans le docu-

ment, et peuvent donc être modifiés après l'export directement depuis l'application d'édition de documents Docx (Word, Libreoffice, OnlyOffice, etc...).

Afin d'exporter à l'aide de templates Docx, le bouton permet d'ouvrir une fenêtre modale spécifique qui permet de personnaliser quelques éléments, comme le montre Figure 4.8 :

(<u>1</u>)	Expor	~ ^ ×
Chemin du templa	atel tation/details/misc/template_object	tive.docx 3
 Paramètres 	Z /presentation/details/misc/report_0	
Couleur des ligne	s paires des tableaux 🛛 🗾 5	
Couleur des ligne	s impaires des tableaux 📃 🧕	
Couleur de fond d	les en-têtes 📃 🕇	
Couleur de la poli	ce des en-têtes 8	
	√ ОК	S Annuler

Figure 4.8. Fenêtre modale d'export docx

À partir de cette fenêtre, il est possible de procéder à l'export dans un template renseigné dans le champ 1, dont le rendu sera enregistré dans le fichier donné dans le champ 2. Les boutons 3 et 4 permettent de parcourir le système de fichiers afin de les sélectionner. Les boutons 5, 6, 7 et 8 permettent de personnaliser certaines couleurs dans l'export des tables (couleurs des lignes des tableaux, et des en-têtes).

4.1.4 Configuration

Le bouton

permet d'ouvrir la fenêtre des paramètres de l'application :



Figure 4.9. Fenêtre modale de configuration de l'application

Cette modale permet de changer la langue de l'application (élément 1), de cacher les bulles d'aide dans les différents éléments de l'application (2), de demander confirmation ou non à la fermeture de l'application (3), de visualiser la version (4) et les changements de versions (changelog - 5).

Note Un changement de langue nécessite un redémarrage de l'application pour être pris en considération.

4.2 Page d'accueil

La Figure 4.10 présente les informations relatives à l'application ainsi qu'à l'étude actuellement chargée.



Figure 4.10. Page d'accueil de l'application

Sur Figure 4.10, la version de l'application correspondant à la licence (démo, freemium, expert) est indiquée sous le logo et le nom de l'application (1). Viennent ensuite des détails sur l'étude :

- Sélections des mode expert et mode express (2)
- Titre de l'étude (3)
- Description de l'étude (4)
- Niveau de confidentialité de l'étude (5), qui apparait sur toutes les pages en haut à droite de l'application (6).

Dans le bas de page, sont indiqués les éléments suivants :

- Un watermark contenant les informations sur le propriétaire de la licence accordée pour l'utilisation de l'application (7)
- Le chemin absolu de l'étude actuellement chargée (8)
- La version de l'application exécutée (9)

4.3 Atelier 1 : Cadrage et socle de sécurité

L'atelier 1 comporte quatre activités correspondant chacune à un paragraphe du guide.

4.3.1 Activité 1.1 : Définition du cadre de l'étude

L'activité 1.1 a pour but la définition du cadre de l'étude. Il s'agit de définir les objectifs, les participants et le cadre temporel de l'étude à réaliser.

Dans l'application, Figure 4.11 permet de définir ces éléments pour différents cycles.

			Cadrage et	socle de sécurité						
Activité 1.1 Activité 1.2 Activité 1.3 Activité 1.4										
Définir le cadre de l'étude										
 Cycles stratégiques et opérationnels 1 										₹±¢
Type Nom	 Date de débu 	ut Date de fin	Contraintes			Hypoth	nèses			
Stratégique Première version de l'étude	03/06/2024	29/07/2024								
Stratégique Révision dans le cadre de l'homologation	01/01/2025	03/02/2025								
 Objectifs de l'étude 2 				Participants 🚯 🛛	3					T ± ¢
		ATELIER A CONDUIR	E	Nom Prénom	Fonction	Responsabilité				Société
OBJECTIF DE L'ETUDE 1	2	3	4 5	Dupont Michelle Mauline Charles	Direction	Valider les résultats de l'étude				
Identifier le socle de sécurité				Béranger lean	DSI	Responsable MCO et MCS du SI				
adapté à l'objet de l'étude				Lefermier Ivan	Relations commercial	Conseil sur les parties				
Etre en conformité avec les			v	Brunel Mireille-b	RSSI	prenantes externes				
numérique			^	4	1001	1001				•
Evaluer le niveau de menace de l'écosystème vis-à-vis de l'objet		x		✓ Matrice RACI (Respo	nsible, Accountable, Consi	ulted, Informed) 🚯 4				
de l'étude							Ateliers			
Identifier et analyser les				Particip	ants	1 2	3	4		5 ^
scénarios de haut niveau, intégrant l'écosystème	×	x		Michelle Dupon	t (Direction) AI	I	AI		AI	
Réaliser une étude préliminaire				Charles Moulins (Co	nsultant cyber)	с	с	с		
des risques pour identifier les X	×	x	×	lean Béranc	er (DSD)			c	cı	
de la sécurité				Turn Lafornian (Dalasi			a			
Conduire une étude des risques				Ivan Letermier (Relacio	ons commerciales)		u			
				 Mireille-h Bru 	nel (RSSI) RI	RAI	RI	RAI	RI	v
✓ Éléments de planning										¥±¢
Intitulé Date de début	Date de fin				Description					^
Réunion de cadrage 03/06/2024 0	3/06/2024 - D - Ic	ivite 1.1 : éfinition des objectifs Jentification des particip	oants et de leurs rôles et responsabilités							
Activités 1.2 & 1.3 05/06/2024 0	5/06/2024 Déf	inition du périmètre mé	étier et technique, et des évènements re	doutés.						
Activité 1.4 - GH 10/06/2024 1	0/06/2024 Ana	alyse d'écart au Guide d'	Hygiène informatique de l'ANSSI.							
Atelier 2 24/06/2024 2	4/06/2024 Ide	ntification, évaluation e	t sélection des couples SR/OV.							

Figure 4.11. Activité 1.1

Les cycles représentent les différentes itérations de l'étude. Un cycle peut être un cycle opérationnel s'il revient seulement sur les ateliers 4 et 5 (par exemple pour prendre en considération l'implémentation de nouvelles mesures de sécurité) ou un cycle stratégique s'il fait évoluer des éléments de contexte (périmètre métier et technique, évènements redoutés, scénarios stratégiques, etc...). Le tableau des cycles (1) permet de définir les différents cycles de l'étude, avec leur type (opérationnel ou stratégique), un nom, une date de début, une date de fin, des contraintes potentielles ainsi que des hypothèses.

Les autres éléments de l'activité sont dépendants du cycle sélectionné dans la table des cycles (1). Ainsi, lorsqu'aucun cycle n'est sélectionné, les autres éléments sont désactivés. Sélectionner un cycle permet d'afficher et modifier les objectifs (2), les participants (3), la matrice RACI (4) et les éléments de planning (5) de ce cycle.

Une fois un cycle sélectionné, il est donc possible de définir les objectifs propres à ce cycle dans le tableau dédié (2). Ce tableau permet également d'indiquer les ateliers sur lesquels porter une attention particulière pour chaque objectif. Afin d'indiquer qu'un objectif est lié à un atelier, il suffit de double-cliquer sur la case du tableau correspondant. Cela permet également de retirer un lien déjà créé.

L'activité 1.1 permet également d'identifier les participants avec leurs fonctions et rôle (3), et leurs responsabilités vis-à-vis de l'étude à l'aide d'une matrice RACI (4). La matrice RACI permet d'indiquer pour chaque participant ses rôles parmi Réalisateur (Responsible - R), approbateur (Accountable - A), consulté (Consulted - C) et informé (Informed - I).

Enfin, l'activité 1.1 permet d'indiquer les différents éléments de planning afin de détailler le cadre temporel de l'étude (5). Il est par exemple possible d'y indiquer les dates des différents ateliers de travail effectués.

4.3.2 Activité 1.2 : Périmètre métier et technique

Figure 4.12 permet de définir le cadre métier et technique de l'étude.

Arthurs Arthurs 1.7				Cadrage et socle	de sécurité								1
Définir le périmètre	métier et technique												
 Missions de l'organisme)1										T	1	۵
Intitulé		Description				Valeurs métier a	ssociées						
Identifier et fabriquer des vacc	ns Identifier (recher fabriquer	che) des vaccins et les	Traçabilité et contrôle Fabriquer des vaccins Recherche & développement	(R&D)									
✓ Valeurs métier									٥	2	T	±	\$
V Valeurs métier 2 Intitulé Nature Activité de recherche et développement des vaccins nécessitant : - i-fidentification des ancions nécessitant :		associés				^							
Recherche & développement (F	&D)	Processus	Activité de recherche et déw - l'identification des antigèn - la production des antigèn fermentation (récolte), purif - l'évaluation préclinique; - le développement clinique	eloppement des vaccins nécessi nes ; es (vaccin vivant atténué, inactiv ication, inactivation, filtration, si a.	itant : vé, sous-unité) : tockage ;	Pharmacien	Identifier et fabriquer des vaccins	Serveurs bureautiques (internes) Serveurs bureautiques (externes) Réseau Interne					
Fabriquer des vaccins		Processus	Activité consistant à réaliser - le remplissage de seringu - le conditionnement (étiqu	: es (stérilisation, remplissage ; é letage et emballage).	itiquetage) ;	Responsable production	Identifier et fabriquer des vaccins	Systèmes de production					
4								Serveurs bureautiques (internes) Système de production des antigènes Réseau Interne					v
✓ Biens support ① 3									۵		T	1	۵
Nom		Description		Propriétaire	Vale	urs métier		Mesures de sécurité					^
Serveurs bureautiques (externes)	Serveurs bureautiques perme	ttant de stocker une partie de	es données de R&D.	Laboratoires	Recherche & développ	ement (R&D)							1
Systèmes de production	Ensemble de machines et équ échelle	ipements permettant de fabr	iquer des vaccins à grande	DSI + fournisseurs matériels	Fabriquer des vaccins								
Système de production des antigènes	Ensemble de machines et équ	ipements informatiques perr	nettant de produire des	Laboratoires	Traçabilité et contrôle								
Serveurs bureautiques	Serveurs bureautiques perme	ttant de stocker l'ensemble d	es données relatives à la	DSI	Traçabilité et contrôle								
Réseau Interne	Etablissement de devis Création de projets Gérer du contenu du site inter	net		DSI	Traçabilité et contrôle Recherche & développ	ement (R&D)							
Sous réseau Ethernet	Answell Answell Answell Answell Barber Striker Associate Valuers makiner associate Barber Striker Associate Makiner Striker Associate Barber Striker Associate Processon Processon Astotie Greenberger Striker Associate Barber Striker Associate Striker Astociate Barber Striker Associate Striker Striker Astociate Barber Striker Astociate Processon Processon Processon Barber Striker Astociate Striker Astociate Barber Striker Astociate Striker Striker Barber Striker Astociate Striker Astociate Barber Striker Astociate												

Figure 4.12. Activité 1.2

En accord avec la méthode EBIOS Risk Manager, l'activité permet de définir le périmètre métier à travers des mifssions (1) et des valeurs métier (2), et le périmètre technique de l'étude à travers des biens support (3).

Il est également possible d'associer des missions et des valeurs métier, et d'associer des valeurs métier aux biens support.

4.3.3 Activité 1.3 : Évènements redoutés

Figure 4.13 permet de définir et d'évaluer la gravité des évènements redoutés (2). Afin d'apprécier la gravité des évènements redoutés, des impacts peuvent être associés aux évènements redoutés, et une colonne de justification permet d'indiquer les raisons du choix du niveau de gravité.

		Cadrage et socle de sécurité				
Activité 1.1 Activité 1.2 A	ctivité 1.3 Activité 1.4					1
Évènements redoutés	2					T 1
Valeur métier	Intitulé	Description	Impacts	Gravité 🔶	Justification	
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		
Traçabilité 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		
Recherche & développement (R&D)	Altération des données de R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée.	Image et confiance Sécurité et santé Juridique	Majeur		
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 Coûts de développement Gouvernance	Majeur		
Recherche & développement (R&D)	Fuite des informations de R&D	Fuite des informations d'études et recherches de l'entreprise	Financier Gouvernance	Majeur		
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 Disponibilité niveau 4 Disponibilité niveau 3	Important		
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	Important		
	k					

Figure 4.13. Activité 1.3

Afin de définir les impacts et l'échelle de gravité, une Figure 4.14 est accessible via le bouton 💌 (1).

		c	Cadrage et	socle	de sécurit	é								2
Activité 1.1 Activité 1.2 Activ	tivité 1.3 Activité 1.4										٥	0	T 2	1 <u>5</u> 1 5
Intitulé					Descrip	tion								^
Missions et services	Conséquences directes ou indirectes sur la réalisation des n	nissions et services												
Capacité de développement ou de décision	Conséquences directes ou indirectes dur la liberté de décide	er, de diriger, de mettre en oeuvre la	stratégie de dé	veloppen	ent	h								
Sécurité et santé	Conséquences directes ou indirectes sur l'intégrité physique	e de personnes												
Image et confiance	Conséquences directes ou indirectes sur l'image de l'organi	sation, la notoriété, la confiance des	clients											
Juridique	Conséquences suite à une non-conformité légale, règlemen	taire, normative ou contractuelle												
Financier	Conséquences pécuniaires, directes ou indirectes													
Matériels	Dégâts matériels ou destruction de biens supports													
Environnementaux	Conséquences écologiques à court ou long terms, directes	ou indirectes												
Lien social interne	Conséquences directes ou indirectes sur la qualité des liens	sociaux au sein de l'organisation												
Patrimoine culturel	Conséquences directes ou indirectes sur les connaissances	non-explicites accumulées par l'orga	anisation, sur le	savoir-fai	e, sur les capa	cités d'innovation, sur le	es références culturel	lles communes						
Coûts de développement	Conséquences directes ou indirectes sur les coûts de dévelo	ppement												
Gouvernance	Conséquences directes ou indirectes qui limitent la capacité	de gouvernance de l'organisation												
	= Critique													Ψ
✓ Échelles disponibles ① 3									T 1 0	Échelle de grav	rité utilisée	dans l'ét	ude : Dé	faut -
	Nom						Description			4				
Défaut - 4		Echelle à 4 niveaux par défaut												
Défaut - 5		Echelle à 5 niveaux par défaut												
										Changer l'échel valeurs déjà dé réévaluer les ni évènements res d'échelle. Utiliser l'é	le de gravit finies. Il ser veaux de gr doutés en c chelle de g	e entraine a donc néo avité des o as de chan ravité séleo	ra la pert cessaire d différents gement ctionnée	e des Je ;
4									•					
✓ Niveaux disponibles ❶ 5			₹±¢		✓ Échelle séle	ctionnée : Défaut - 4 🌘	06						4	3
Nom	Description		_		Niveau			Descr	iption				_	1
Écosystème(s)	sectoriel(s) impacté(s) de façon importante, avec des conséqu	iences éventuellement durables.			Critique	Conséquences généra	ralisées sur l'ensemble	e du système d'inform	ation audité.					1
Catastrophique	é pour l'Etat, voire incapacité, d'assurer une fonction régalien	ne ou une de ses missions d'import	ance vitale.		Majeur	Conséquences restrei	intes sur une partie o	du système d'informat	ion audité.					_
destruction d'in	critiques sur la securite des personnes et des biens (crise sai afrastructuras essentielles etc.)	litaire, poliution environnementale i	majeure,	-	Important	conséquences isolées	s sur des points préci	is du système d'inform	ation audité.					
destruction of	indot detailes essentienes, etemp			+	Mineur	Pas de conséquence o	directe sur la sécurité	é du système d'inform	ation audité.					
														*

Figure 4.14. Configuration de l'activité 1.3

Depuis cette page, il est possible de revenir à la Figure 4.13 via le bouton de retour (1). La configuration permet de définir les impacts à considérer dans l'étude (2), ainsi que les échelles de gravité disponibles (3). Le bouton Utiliser l'échelle de gravité sélectionnée (4) permet de choisir l'échelle sélectionnée dans la table des échelles (3) comme échelle de gravité pour l'étude. Il est possible de définir des niveaux pour les différentes échelle depuis la table des niveaux (5), et de les ordonner et leur attribuer une couleur spécifique à chaque échelle via la table affichant l'échelle sélectionnée (6). L'échelle affichée dans la table (6) est celle sélectionnée dans la table des échelles (3). Afin d'utiliser un niveau dans l'échelle, le sélectionner dans la table (5) puis utiliser la flèche allant vers la

droite 🚬. Pour retirer un niveau de l'échelle actuellement sélectionnée, le sélectionner dans la table

de l'échelle (6) puis utiliser la flèche allant vers la gauche

4.3.4 Activité 1.4 : Socle de sécurité

Note Cette activité présente des fonctionnalités propres à certaines licences. Il se peut donc que certaines fonctionnalités soient absentes de l'application selon la licence utilisée.

Figure 4.15 permet de déterminer le socle de sécurité, en définissant les référentiels de sécurité à appliquer à l'objet de l'étude (3) et les exigences qu'ils contiennent (5).

	Cadrage et socle de sécurité											
Activité	1.1 Activité 1.2 Activité 1.3 Activité 1.4											
Déte	rminer le socle de sécurité							_	_		å 🌣 🛛	
3 × Réf	érentiels 🚯 🗅 👍	7			December		To discharge de soute main			T	τ¢	
Guide	d'hygiène informatique de l'ANSSI	Règles de base & hygiène Ce	e guide comporte 4	2 mesures permettant	de renforcer la sécurité de son système d'in	formation.	Appliqué partiellement					
Guide							Très peu appliqué					
			•									
			-									
5 v Evir	annear - Guida d'hugiàna informatique de l'ANSSI 🛛 🗖 🚍 💪										1.0	
Nivez		Description	oplig	ué Commentaire	Catégorie	État d'application	Justification				-	
1	R01 Former les équipes opérationnelles à la sécurité des	Former les équipes opérationnell	les à la		I - Sensibiliser et former	Non appliqué	,					
1	R02 Sensibiliser les utilisateurs aux bonnes pratiques	Sensibiliser les utilisateurs aux be pratiques élémentaires de sécuri	onnes té		I - Sensibiliser et former	Derogation						
	elementaries de securite informatique_[standard]	informatique Sensibiliser les utilisateurs aux bo	onnes			acceptee						
2	R02 Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique_[Renforcé]	pratiques élémentaires de sécuri informatique	té		I - Sensibiliser et former	Assez appliqué						
1	R03 Maîtriser les risques de l'infogérance_[Standard]	Maîtriser les risques de l'infogéra	ince 🗌		I - Sensibiliser et former	Assez appliqué						
1	R04 Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau_[Standard]	plus sensibles et maintenir un scl	héma du		II - Connaître le système d'information	Non appliqué					v	
v Car	tographie du niveau d'application des exigences par catégorie	du référentiel : Guide d'hyaiène inf	ormatique de l'ANS	51 7						Q	Q D	
					Sensibiliser et former						1	
			X - Pour aller p	lus loin	4 II - Conn	aître le système d'inform	ation					
					3.06							
				/ /								
					2 2019							
		VIII - Maintenir le système d'inform	ation à jour		1	III - Authentifier et	contrôler les accès					
				2.5	3,13						¥	

Figure 4.15. Activité 1.4

Dans cette activité, les exigences affichées dans le tableau des exigences (5) sont celles du référentiel sélectionné dans le tableau des référentiels (3). La licence expert de l'application dispose d'un bouton

permettant de basculer entre le mode expert et le mode classique de l'activité (1). Le mode expert de l'activité donne accès à des colonnes supplémentaires dans la table des exigences (5) ainsi qu'à un graphe représentant les niveaux d'application des exigences selon les différentes catégories (7).

Afin d'évaluer les niveaux de conformité des référentiels, et les niveaux d'application des exigences

pour le mode expert, une Figure 4.16 est accessible via le bouton (2).

Cadrage et s	socle de sécurité		1
Déterminer le socie de sécurité V indicateurs de conformé aux réferenties de sécurité			1 <u>≗</u> ●2 ▼ ± ≎
	Nom		
Très peu appliqué			
Appliqué partiellement			
Applique sans restriction			
k			
v États des exigences n 4	 Configuration du radar 5 		
Nam	1	~	
Derogation	Ignorer les valeurs négatives	v	
acceptée	Échelle min	0	<u> </u>
Non applique 0	Échelle max	5	0
A lancer 0	-		
Très peu 1 annious	Т		
Peu appliqué 2			
Assez appliqué 4			
Appliqué 5	4		
	-		
	J		

Figure 4.16. Configuration de l'activité 1.4

La page de configuration permet de définir l'échelle permettant d'évaluer le niveau de conformité des référentiels (3). En mode expert, elle permet également de définir l'échelle permettant l'évaluation de l'état d'application des exigences de sécurité (4). La valeur associée aux états d'application est le score à leur associer dans le graphe (7 de Figure 4.15). En mode expert, la page de configuration permet aussi de configurer le graphe, en permettant d'ignorer les valeurs négatives et de définir le score souhaité pour les valeurs minimale et maximale du graphe (5). Ignorer les valeurs négatives permet par exemple de ne pas prendre en considération un état d'application Non appliqué, en lui attribuant une valeur négative dans la configuration de l'échelle (4). Depuis la page de configuration,

il est possible de basculer entre le mode expert et le mode classique avec le bouton 📠 (1) et de

revenir à la page de l'activité via le bouton 🛄 (2).

Import d'exigences de sécurité

L'application permet d'importer les exigences de sécurité dans un référentiel de deux façons différentes :

- 1. Via le bouton (4), à partir d'un fichier CSV contenant une exigence par ligne, avec les colonnes dans l'ordre suivant : Niveau, Intitulé, Description, Appliqué, Commentaire, Catégorie, Statut, Justification, Couleur (du statut). Les statuts qui n'existent pas sont créés automatiquement, avec la couleur indiquée sur la première ligne où le statut apparait. Cette fonctionnalité est dépréciée, lui privilégier la fonctionnalité suivante :
- 2. Via le bouton (6), à partir de fichiers JSON, YAML, XML ou CSV. Pour le format des fichiers, voir Exemples d'imports d'exigences.

Dans les deux cas, les exigences seront importées dans le référentiel sélectionné dans la table des référentiels (3).

Exemples d'imports d'exigences

Les exemples suivants permettent d'importer des exigences dans le référentiel sélectionné dans la

table des réféfrentiels (3) avec le bouton (6) :

En JSON :

```
{
    "requirements": [
        {
            "title": "Requirement 1",
            "description": "Description 1",
            "category": "Catégorie 1",
            "justification": "Justification 1",
            "level": 1,
            "statusLevelName": "Appliqué"
        },
        {
            "title": "Requirement 2",
            "description": "Description 2",
            "category": "Catégorie 2",
            "justification": "Justification 2",
            "level": 2,
            "statusLevelName": "Non appliqué"
        },
        {
            "title": "Requirement 3",
            "description": "Description 3",
            "category": "Catégorie 1",
            "justification": "Justification 3",
            "level": 1,
            "statusLevelName": "Peu appliqué"
        }
    ]
```

Une alternative possible pour le format JSON est la suivante :

```
[
    {
        "title": "Requirement 1",
        "description": "Description 1",
        "category": "Catégorie 1",
        "justification": "Justification 1",
        "level": 1,
        "statusLevelName": "Appliqué"
    },
    {
        "title": "Requirement 2",
        "description": "Description 2",
        "category": "Catégorie 2",
        "justification": "Justification 2",
        "level": 2,
        "statusLevelName": "Non appliqué"
    },
        "title": "Requirement 3",
        "description": "Description 3",
        "category": "Catégorie 1",
        "justification": "Justification 3",
        "level": 1,
        "statusLevelName": "Peu appliqué"
    }
```

Les autres formats sont équivalents, seule la syntaxe change. En YAML :

```
requirements:
  - title: YAML 1
   description: YAML Desc 1
   category: YAML catégorie 1
   justification: YAML justification 1
   level: 1
   statusLevelName: Appliqué
   title: YAML 2
   description: YAML Desc 2
   category: YAML catégorie 2
    justification: YAML justification 2
   level: 2
   statusLevelName: Non appliqué
  - title: YAML 3
   description: YAML Desc 3
   category: YAML catégorie 1
    justification: YAML justification 3
    level: 1
    statusLevelName: Peu appliqué
```

Tout comme en JSON, l'alternative suivante est possible pour le format YAML :

```
- title: YAML 1
 description: YAML Desc 1
 category: YAML catégorie 1
  justification: YAML justification 1
 level: 1
 statusLevelName: Appliqué
- title: YAML 2
 description: YAML Desc 2
 category: YAML catégorie 2
 justification: YAML justification 2
 level: 2
 statusLevelName: Non appliqué
- title: YAML 3
 description: YAML Desc 3
 category: YAML catégorie 1
 justification: YAML justification 3
 level: 1
 statusLevelName: Peu appliqué
```

En CSV, le format suivant peut être utilisé (4 lignes importées) :

```
title, description, category, justification, level, statusLevelName
Requirement CSV 1, Description 1, Catégorie 1, Justification 1, 1, Appliqué
Requirement CSV 2, Description 2, Catégorie 2, Justification 2, 2, Non appliqué
Requirement CSV 3, Description 3, Catégorie 1, Justification 3, 1, Peu appliqué
"Requirement CSV avec un saut de ligne dans la description", "Description avec un
saut de ligne", Catégorie 2, "Justification avec un autre
saut de ligne", 1, Appliqué
```

Enfin, le format XML suivant permet également d'importer des exigences :



4.4 Atelier 2 : Sources de Risques et Objectifs Visés

L'atelier 2 permet de définir, évaluer et sélectionner les couples Sources de Risque (SR) et Objectifs Visés (OV). Figure 4.17 permet de définir les couples SR/OV, l'activité 2.2 permet de les évaluer, et l'activité 2.3 de sélectionner les couples à considérer dans la suite de l'étude.

Dans Figure 4.17, les boutons (1), (2) et (3) sont communs à toutes les activités de l'atelier, et permettent respectivement de basculer dans la version simplifiée de l'atelier, d'exporter les éléments de l'atelier et d'accéder à la page de configuration de l'atelier.

		Sources de Risques / (Objectifs Visés	18 8 2 3
Identifier	les sources de risques et objectifs visés			
✓ Sources de r	isques 🚯 👍	0 2 👅 T ± 🌣	Objectifs visés 0 5	0 🖬 👅 🕇 单
Nom	Description		Intitulé	Description
Officine spécialisée	Profil de « obermercenaire « doté de capacités informatiques généralement élevées distinguer des szerprédidés avec qui la intrançe truteriles herrit de défi et la quête d lucratit. De tels groupes peuvent s'organier en officines spécialisées proposant de v ce type de hacker chevronné et stouwent à lorging de la conception et de la créator (éventuilement monitysés) qui sont ensuite utilisables « dés en main » par d'auters motivations particulies auters que la qué nimancie	sur le plan technique. Il est de ce fait à e reconnaissance mais avec un objectif éritables services de piratage. i d'outils et kits d'attaques accessibles en ligne groupes d'attaquants. Il n'a pas de t motisé nas une quiéte de reconnaissance.	Lucratif	Operation visant un gain financier, de façon directe o unidrecte. Geferalement liée au crime organisti, on per le tetre : escroquere un Internet, Bahardiment d'argent, escrisonio ou détournement d'argent, manipulation de marchés financiers, fabrillation de documents administratifs, Supprison d'arbent, etc
Amateur Vengeur	robin o musere e au paddar 5 ocu da banna comunataria en moniparsi, u sociale, d'anussement, de delf. Attaques basiques mais capacité à utiliser les kits dat Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aig salarié licencié pour faute grave, prestataire mécontent suite au non-renouvellemen Ce profil d'attaquant se caractérise par sa détermination et sa connaissance interne et	under pår une quete de recommissionee aques accessibles en ligne üe ou un sentiment d'injustice (exemples : t d'un marché, etc.). des systèmes et processus organisationnels.	Défi, amusement	Defarition ten accriter y num objects in min fan in fan in monome. Opération vient à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de simple amusement. Même si fobjectif est essentiellement ludique et sans volonté particulière de nuire, ce type d'opération peut avoir de lourdes conséquences pour la víctime.
	Cela peut le rendre redoutable et lui conferer un pouvoir de nuisance important. Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportuniste e (exemples : concurrent déloval, client malhonnête, escroc, fraudeur).	t parfois guidées par l'appât du gain	Sabotage de la campagne de vaccination	Saboter la prochaine campagne nationale de vaccination en perturbant la production ou la distribution des vaccins, pour générer un choc psychologique sur la population et discréditer les pouvoirs publics.
Malveillant pathologique	Ici, soit l'attaquant dispose d'un socle de connaissances en informatique qui l'amène soit il exploite par lui-même des kits d'attaques disponibles en ligne, soit il décide de	à tenter de compromettre le SI de sa cible, sous-traiter l'attaque informatique en faisant	Vol d'informations	Voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel.
Concurrent	appel à une officine spécialisée. Dans certains cas, l'attaquant peut porter son attent prestataire peu scrupuleux) et tenter de la corrompre. Profil d'une organisation dont les activités sont proches de celles de l'objet étudié. Le	ion sur une source interne (salarié mécontent, concurrent peut utiliser des moyens cyber	Nuire à l'image de la société Demander une rançon	Divulguer au grand public des informations sur la façon dont les vaccins sont conçus en collectant des photos et vidéos des tests animaliers afin de rallier fopinion publique à sa cause. Menace d'altération de la composition de vaccins distribués lors d'une campagne nationale de
× Couples sou	ann de pouvoir acquerir un avantage (exemple : espionnage industriei).		-	vaccination sous couvert de bioterronsme a des inis dextorsion d'une rançon.
	Source de Risque			Objectif Visé
Activiste idéolo	gique	Sabotage de la campagne de vaccination		ovjecu ne
Concurrent		Vol d'informations		
Activiste idéolo	gique	Nuire à l'image de la société		
Crime organisé		Demander une rançon		

Figure 4.17. Activité 2.1

La Figure 4.18 permet de définir des couples SR/OV qui seront tous considérés comme retenus, sans avoir besoin d'évaluer leur pertinence. La configuration de l'atelier devient alors superflue, puisqu'elle permet de définir la métrique à utiliser pour évaluer la pertinence des couples SR/OV, et

seule Figure 4.17 est disponible (3). Le bouton [1] (1) permet de revenir à la version complète de

l'atelier.

Solution		Sources de Risques / Objectifs Visés 1🔛 🜉										
Section de la conception de la conceptio	Activité 2.1 3	1										
Vorgers of under stripper de la conference de la concrete de	Identifier	les sources de risques et objectifs visés										
Non Description Description Provide on permittenest sold de conditionent diverse sur le pain technique. Il est de fait à distinguer des sorgie sold des conditionent diverse sur le pain technique. Il est de fait à distinguer des sorgie sold des conditionent diverse proposat de virturalité. Description Officie e une resource source source de biographic diverse source de la conception et de la concoc	✓ Sources de r	risques 🚯	0 2 📋 🝸 ± 🕈	 Objectifs visés 		10						
Profit de s optemerenaire - doit de capacités informatiques ginéralement lévées sur le plan technique. Il et de ce fait à le contrement de capacités informatiques ginéralement lévées sur le plan technique. Il et de ce fait à le contrement de capacités informatiques ginéralement lévées sur le plan technique. Il et de ce fait à le contrement de capacités proposant de le capacité de contrement de la capacité de contrement de la capacité de contrement de la ce fait de contrement de la capacité de la capacité de contrement de contrement de la capacité de la cap	Nom	Description		Intitulé	Description							
Anatadu sociale, dramusement, de dél. Attuques basiques mais capacité à utiliser les ist drataques accessibles en ligne vengeur capacité autiliser les ist drataques accessibles en ligne saniserient. Meme si bipectif attaquant sont de les dres de renconnaisance sociale, de dél ou de simple anusement. Meme si bipectif est essentiellement duique et sans volonte particulière de nuine, ce type dipertaine particulière et autorités part a defen de renconnaisance internet est aprèris guides par nage intert. Meme si bipectif est essentiellement duique et sans volonte particulière de nuine, ce type dipertaine particulière et autorités part a defen de nuisance important. Les aprèris guides par nage internation et au comprense sonneren délyal, deir mainornete, ce type dipertaine particulière et aprèris guides par nage internation et au comprense internet estante est	Officine spécialisée	Profil de « opermercenaire » doté de capacités informatiques généralement distinguer des scripci-kiddie avec qui li partage toutefois l'esprit de défiet et a lucratif. De tet groupes pevent storganiere en officines pelcaliades proposa Ce type de hacker chevronné est souvent à l'origine de la conception et de la (ventuellement monaryls) qui sont ensuite utilisables « déle manin » par de motivations particulières autres que le gain financie.	élevées sur le plan technique. Il est de ce fait à juête de reconnaissance mais avec un objectif nt de véritables envices de piratage. création doutils et kits d'attaques accessibles en ligne autres groupes d'attaquants. Il n'a pas de ques, et motivé par une quéte de reconnaissance	Lucratif	Opération visant un gain financier, de façon directe ou indirecto. Genéralement liée au cirro organisé, on peut cetter : escroqueria su internet, biadroiment d'argent, encision ou dédournement d'argent, manipulation de marché financiers, faisification de documents administratific, busynation d'identific, étc Il est à note que certaines opérations à luc la busynamest recourt à un mode opératoine matratification activité mais foisécer finan lesse financies.	e iur						
Cel à port le moitre redoctable et lu conter rui pouvoir de nuisance important. Le moitvoirie de e pouver augrine autonable de vaccination en perturbant à production ou is Sabotage de la campagne de vaccination pouver per sourcerne délya. Lem nahion de se son frandeur. Sabotage de la campagne de vaccination pouver per sourcerne de logie autorité est de sourcerne de la contexter transpontent le si de sa contexter pouver per sourcerne de la pouver augrine autorité est de la campagne de vaccination pouver sourcerne de la pouver augrine autorité est de la campagne de vaccination pouver per sourcerne de la pouver augrine de la contexter transpontent le si de sa contexter Pouver per source de risque / objectifs vides concurrent * Couples source de risque / objectifs vides Source de risque / objectifs vides Source de risque / objectifs vides Concurrent * Couples sources de risque / objectifs vides Source de risque / objectifs vides Source de risque / objectifs vides Concurrent * Couples sources de risque / objectifs vides Source de risque / obje	Amateur Vengeur	sociale, d'amusement, de défi. Attaques basiques mais capacité à utiliser les k Les motivations de ce profil d'attaquant sont guidées par un esprit de vengea salarié licencié pour faute grave, restataire mécontent suite au non-renouve Ce profil d'attaquant se caractérise par sa détermination et sa connaissance in	its d'attaques accessibles en ligne nce aigüe ou un sentiment d'injustice (exemples : llement d'un marché, etc.). iterne des systèmes et processus organisationnels.	Défi, amusement	Opération visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou de sir amusement. Même si l'objectif est essentiellement ludique et sans volonté particulière de nuire, ce type d'opération peut avoir de lourdes conséquences pour la victime.	nple						
Makelian ki, soit hättagaand dispose dun soite de connaissances en informatigue qui annie à tenter de componentre le Si de s aduit Ved er des informations en explorant. Its travaux de R&D en vue d'obtenri un avantage concurrentian Ved reissance publicance de sind stratagaand dispose fun soite de connaissances en informatigue qui annie à tenter de componentre le Si de s aduit Ved er des informations en explorant. Its travaux de R&D en vue d'obtenri un avantage concurrentian Ved d'informations Profit d'une organisation dont le sactivités sont proches de celles de l'objet étudité. Le concurrent peut utiliser des moyens cyber Ved d'informations Ved d'informations Profit d'une organisation dont le sactivités sont proches de celles de l'objet étudité. Le concurrent peut utiliser des moyens cyber Ved er des informations en explorant. Its travaux de R&D en vue d'obtenri un avantage concurrent V couples sources de risques / objectifs visés Image de la société Devolute en vue d'obtenri une zonçen Source de Risque Sabotage de la campage e vaccination Objectif Visé Activite bédologique Ved d'informations Profit d'une organisé Concurrent Ved d'informations Polectif Visé		Cela peut le rendre redoutable et lui conferer un pouvoir de nuisance importa Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportu (exemples : concurrent déloval, client malhonnête, escroc, fraudeur).	int. iniste et parfois guidées par l'appât du gain	Sabotage de la campagne de vaccination	Saboter la prochaine campagne nationale de vaccination en perturbant la production ou la distribution des vaccins, pour générer un choc psychologique sur la population et discrédit pouvoirs publics.	er les						
appel a une dificies spécialisée. Dans certains cas, fattaquant peut porter son attention sur une source interne (salarie microanter) Profit d'une organisation den l'es autritiés sont conque. Le concurrent peut utiliser des moyers opter Profit d'une agrinaution den l'es autritiés sont proches de celles de l'abjet étudié. Le concurrent peut utiliser des moyers opter v Couples sources de risques / objectifs visie Concurrent Les conces de risques / objectifs visie Concurrent Les conces de la société Concurrent Les conces de la société Crime organisé Crime organisé	Malveillant pathologique	Ici, soit l'attaquant dispose d'un socle de connaissances en informatique qui l'a soit il exploite par lui-même des kits d'attaques disponibles en ligne, soit il déc	amène à tenter de compromettre le SI de sa cible, cide de sous-traiter l'attaque informatique en faisant	Vol d'informations	Voler des informations en espionnant les travaux de R&D en vue d'obtenir un avantage concurrentiel.							
afin de pouver acquierr un avantage (exemple : exponnage industriel).	Concurrent	appel à une officine spécialisée. Dans certains cas, l'attaquant peut porter son prestataire peu scrupuleux) et tenter de la corrompre. Profil d'une organisation dont les activités sont proches de celles de l'objet étu	attention sur une source interne (salarié mécontent, adié. Le concurrent peut utiliser des moyens cyber	Nuire à l'image de la société Demander une rancon	Divulguer au grand public des informations sur la façon dont les vaccins sont conçus en collectant des photos et vidéos des testes animaliers afin de ralileir rópinion publique à sa caus Menace d'altération de la composition de vaccins distribués lors d'une campagne nationale de							
	M Couples cou	atin de pouvoir acquerir un avantage (exemple : espionnage industriei).			vaccination sous couvert de bioterrorisme a des fins d'extorsion d'une rançon.							
Activite lóbologique Sabotage de la campagne de vaccination Concurrent Vol d'informations Céritorie lóbologique Nure à Insage de la société Crime organisé Demander une rançon	Coupies sou	Source de Risque			Dhiantif Visé							
Concurrent Vol d'informations Karbiète lédécôque Nuré à Innage de la société Crime organisé Demander une rançon	Activiste idéolo	ogique	Sabotage de la campagne de vaccination		sujecti rise							
Activiste idéologique Nuire à l'image de la société Crime organisé Demander une rançon	Concurrent		Vol d'informations									
Crime organisé Demander une rançon	Activiste idéolo	gique	Nuire à l'image de la société									
	Crime organisé	à	Demander une rançon									

Figure 4.18. Version simplifiée de l'atelier 2

4.4.1 Activité 2.1 : Définition des couples SR/OV

Figure 4.17 permet de définir les sources de risques (4), leurs objectifs visés (5) et les couples qu'ils forment (6).

4.4.2 Configuration de l'atelier 2



Figure 4.19. Configuration de l'atelier 2

Afin de pouvoir évaluer la pertinence des couples SR/OV définis dans Section 4.4.1, il est nécessaire de disposer d'une métrique d'évaluation de la pertinence. Afin de définir des métriques, accéder à la

Figure 4.19 avec le bouton (élément 3 de Figure 4.17). Sur cette page, les métriques disponibles sont affichées dans la table des métriques (4). Les autres tables (6, 7, 8, 9) affichent les éléments de la métrique sélectionnée dans la table des métriques. Les métriques de cotation de la pertinence des couples SR/OV sont constituées d'une échelle de motivation (6), d'une échélle de ressources (7), d'une échelle de pertinence (8) et d'une matrice de cotation (9) permettant de calculer automatiquement un niveau de pertinence à partir d'un niveau de motivation et d'un niveau de ressources. Le bouton Sélectionner la métrique permet d'utiliser la métrique sélectionnée dans la table des métriques (4) comme métrique pour l'étude.

Avertissement Changer la métrique de cotation de l'étude supprimera tous les niveaux de motivation, ressource et pertinence attribués aux couples SR/OV.

Pour revenir aux activités, utiliser le bouton (3).

4.4.3 Activité 2.2 : Évaluation des couples SR/OV

Figure 4.20 permet d'évaluer les couples SR/OV définis dans l'activité 2.1 selon la métrique sélectionnée dans la configuration de l'atelier (1).



Figure 4.20. Activité 2.2

4.4.4 Activité 2.3 : Sélection des couples SR/OV

Figure 4.21 permet de sélectionner les couples SR/OV à retenir pour la suite de l'étude.



Figure 4.21. Activité 2.3

La table des couples SR/OV (1) permet de sélectionner les couples à retenir. Les cartographies des couples SR/OV par source de risque (2) et par objectif visé (3) permettent de visualiser les différents couples SR/OV et leurs niveaux de pertinence. Il est possible de sélectionner les couples SR/OV directement depuis les cartographies en cliquant sur le rond associé au couple SR/OV souhaité. Les ronds rouges représentent les couples retenus (dangereux), et les verts les couples non retenues (moins dangereux).

permet d'exporter le graphe dans un document.

4.5 Atelier 3 : Scénarios stratégiques

L'atelier 3 est composé de 3 pages d'activités et d'une page de configuration. L'activité 3.1 permet d'étudier les parties prenantes et d'établir la cartographie de dangerosité de l'écosystème. L'activité 3.2 s'intéresse aux scénarios stratégiques et aux chemins d'attaque qui les composent. Dans l'activité 3.3, les mesures de sécurité de l'écosystème sont définies et la cartographie de dangerosité de l'écosystème est réévaluée en prenant en considération ces mesures de sécurité.

4.5.1 Configuration de l'atelier 3

Le bouton (élément 3 de Figure 4.23) permet d'accéder à la configuration de l'atelier depuis n'importe laquelle de ses activités.

La Figure 4.22 permet de définir les éléments nécessaires à l'évaluation des parties prenantes et à leur représentation dans la cartographie de dangerosité.



Figure 4.22. Page de configuration de l'atelier 3

Dans cette page, les trois tables sur la première ligne (2, 3 et 4) permettent de définir les *critères* à utiliser pour l'évaluation des parties prenantes. Ces critères sont définis dans la table des critères (2), et disposent de plusieurs échelles qui peuvent être définies grâce à la table des échelles des critères (3). Seules les échelles du critère sélectionné dans la table des critères (2) s'affichent dans la table des échelles de critères (3). Les niveaux des échelles sont définis dans la table des niveaux des échelles de critère (4). Seuls les niveaux de l'échelle sélectionnée dans la table des échelles de critères (3) sont affichés dans la table des niveaux des échelles de critères (4).

La table des métriques (5) permet de définir plusieurs métriques d'évaluation de la dangerosité des parties prenantes. Ces métriques permettent de calculer un *niveau de dangerosité* pour les parties prenantes, à partir de l'évaluation faite selon les différents critères. Pour cela, une *formule* est renseignée dans la métrique (champ Formule). Cette formule peut contenir des opérations arithmétiques de base (+, -, *, / pour l'addition, la soustraction, la multiplication et la division respectivement), qui sont priorisées de façon usuelle (c'est-à-dire que les opérations de multiplication et de division sont prioritaires sur l'addition et la soustraction). Afin de changer l'ordre d'évaluation, des parenthèses (et) peuvent être utilisées. Dans la formule, il est possible de substituer des variables par les valeurs des critères de la partie prenante. Ces variables sont de la formule [REF], où REF est la référence du critère (champ Référence) telle que définie dans la table des critères (2). Afin de pouvoir être utilisé dans une métrique, un critère doit être associé à la métrique (champ Critères).

Par exemple, pour les critères du guide de dépendance (référence DEP), pénétration (référence PEN), maturité cyber (référence MAT) et confiance (référence CON), la formule définie dans le guide peut être définie par ([DEP] * [PEN]) / ([MAT] * [CON]).

Conseil Les espaces sont ignorées dans la formule, elles peuvent permettre de rendre la formule plus lisible.

Le bouton Sélectionner cette métrique (6) permet d'utiliser la métrique sélectionnée dans la table des métriques (5) dans l'étude.

Avertissement Changer de métrique peut faire perdre les niveaux de cotation attribués aux parties prenantes dans l'étude.

Les tables de zones (7) et de seuils de fiabilité (8) permettent de configurer la cartographie de dangerosité de l'écosystème. Les zones (7) correspondent aux cercles de couleur dans la cartographie,

délimitant des zones. Par exemple, la cartographie peut disposer d'une zone de danger correspondant aux niveaux de dangerosité supérieurs à 2.5. Les seuls de fiabilité (8) permettent d'attribuer des couleurs différentes aux parties prenantes dans la cartographie de dangerosité de l'écosystème en fonction de leur fiabilité cyber. La fiabilité cyber correspond au produit des critères de la métrique sélectionnée de type Fiabilité cyber.

Enfin, la table de description de la métrique (9) permet de visualiser l'ensemble des échelles des critères associés à la métrique sélectionnée dans la table des métriques (5).

Une fois la configuration de l'atelier effectuée, il est possible de revenir aux activités grâce au bouton



4.5.2 Activité 3.1 : Construction de la cartographie de menace de l'écosystème et identification des parties prenantes critiques

Figure 4.23 a pour objectifs la construction de la cartographie de dangerosité de l'écosystème et la sélection des parties prenantes.

Scénarios stratégiques												2 2	
Activité 3.1	Activité 3.2 Activité 3.3												23
Construi	re la cartographie de	dangerosité	de l'écosys	stème et i	dentifie	er les parties prei	nantes criti	ques					
✓ Catégorie:	s de parties prenantes 🚯 🖪	4					T 1 ¢		nantes 🕕 5			T	1
Référence	Nom	Descript	tion			Туре		Référence	Nom	Description			^
PAR	Partenaires	Partenaires de l'or	ganisation			Externe		C1	Établissements de santé	Hôpitaux, cliniques, etc			
PRE	Prestataires	Prestataires (sous-	traitants) de			Externe		C2	Pharmacies	Pharmacies			_
CLI	Clients	Tous types de clien	nts			Externe		C3	Grossistes répartiteurs	Intermediaires entre les clients et l'organisation			
FOU	Fournisseurs	Fournisseurs de l'a	organisation			Externe		P1	Universités	Universités collaborant sur la			
SER	Services connexes techniques	Services et suppor	rts proposés			Interne				recherche Sociétés indépendantes de			
		par une DSI Entité commerciale	e utilisatrices					P2	Régulateurs	contrôle			
SER-M	Services connexes metier	des données métie	ers			Interne			Laboratology	Laboratoires dans lesquels sont			
FIL	Filiales	nationales ou inter	rnations			Interne		r5	Laboratoires	tests			
								4					
✓ Dangerosi	té de l'écosystème 🛛 🏮												1 0
Catégorie	Nom	Dépendance	Pénétration	Maturité	Confianc	e Dangerosité calculée	Dangerosité forcé	Retenue		Justification	n initiale		
Clients	Établissements de santé	1	1	1	3	0.33							
Clients	Pharmacies	1	1	2	3	0.17							
Clients	Grossistes répartiteurs	1	2	2	3	0.33							
Partenaires	Péquiateurs	2	1	2	2	0.25							
Partenaires	Laboratoires	3	3	2	2	2.25		✓					
Prestataires	Fournisseurs industriels chimistes	4	2	2	3	1.33							
Prestataires	Fournisseurs de matériel	4	3	2	3	2		✓					
Prestataires	Prestataires informatiques	3	4	2	2	3		✓					
✓ Cartograp	hie initiale de dangerosité de l'éd	cosystème 7										Q	Q
	According to the second s												

Figure 4.23. Activité 3.1

Dans l'atelier 3, les boutons (1), (2), (3) sont présents sur l'ensemble des pages d'activités, et permettent respectivement de basculer dans le mode simplifié de l'atelier, d'exporter les éléments de l'atelier, et de basculer sur la Figure 4.22.

Dans Figure 4.23, la cartographie de dangerosité est construite d'abord en définissant des catégories de parties prenantes (4), qui permettront de grouper les parties prenantes définies dans la table des parties prenantes (5). Une fois les parties prenantes définies, leur niveau de dangerosité est évalué selon la métrique d'évaluation des parties prenantes sélectionnée depuis la Section 4.5.1. À cette fin, la table de dangerosité de l'écosystème (6) présente une colonne pour chaque critère associé à la métrique, qui permet d'attribuer une valeur selon l'échelle du critère en double-cliquant sur la case du tableau. Une fois l'ensemble des critères évalués pour une partie prenante, l'application calcule automatiquement le niveau de dangerosité de la partie prenante à l'aide de la formule définie dans la métrique. Il est toutefois possible de forcer une valeur de dangerosité avec la colonne Dangerosité forcée. Une fois le niveau de dangerosité connu de l'application (le niveau forcé prévaut sur le niveau calculé si les deux existent), la partie prenante apparait sur la cartographie initiale de dangerosité de l'écosystème (7).

4.5.3 Activité 3.2 : Élaboration des scénarios stratégiques

Figure 4.24 a pour objectif l'élaboration des scénarios stratégiques et des chemins d'attaque qui les composent.

Autor 2.1	Scénarios stratégiques 🔯 🚨 🗖											
Élaborer d	es scénario	s stratégi	ques									
 Scénarios str 	ratégiques 🚯	1	4							T 1 0		
Int	itulé		Description	SR/OV	Évènement redouté	Valeur métier	Gravité					
Vol de données		Un concurrent concurrentiel	t vole des données de R&D en vue d'obtenir un avantage	Concurrent / Voler de	5 Fuite des informations de R&D	Recherche & développement (R&D)	Majeur					
Sabotage de la vaccination	campagne de	Une organisat des vaccins afi discréditer les	ion hacktiviste perturbe la production ou la distribution in de créer un choc psychologique sur la population et de pouvoirs publics.	Activiste idéologique / Sat la campagne nationale vaccination	de Atteinte à la production ou distribution des vaccins	Fabriquer des vaccins	Critique					
✓ Chemins d'al	ttaque : Vol de do	onnées de R&D	02					0 0 1		T ± ¢		
Référence *	Chemin d	'attaque	Description				Parties prenantes					
R01	canal direct		Exfiltration des données via un canal direct									
R02	Vol sur le SI du la	aboratoire	Les données sont récupérées sur le SI du laboratoire qui données de R&D.	détient une partie des P3	- Laboratoires							
R03	Canal d'exfiltratio prestataire inforr	on depuis le matique	Le concurrent crée un canal d'exfiltration passant par le s informatique.	il du prestataire F3 -	- Prestataires informatiques							
4										,		
💙 Graphe du s	cénario stratégiqi	ue : Vol de don	nées de R&D 3					4	1	Q		
					canal direct							
			Concurrent	Vol su	Ir le SI du laboratoire	> Voler des	informations					

Figure 4.24. Activité 3.2

La table des scénarios stratégiques (1) permet de définir des scénarios stratégiques à partir d'un couple SR/OV retenu dans Section 4.4.4 et d'un évènement redouté issu de Section 4.3.3. Lors de la sélection d'un évènement redouté dans le formulaire de création ou d'édition du scénario stratégique, le niveau de gravité est automatiquement positionné sur le niveau de l'évènement redouté. Il est toutefois possible de changer le niveau de gravité du scénario stratégique.

Avertissement Le niveau de gravité du scénario stratégique pouvant différer du niveau de gravité de son évènement redouté, changer la gravité d'un évènement redouté ne change *pas* la gravité des scénarios stratégiques qui lui sont associés. Il est nécessaire de changer la gravité de chacun des scénarios le cas échéant.

La table des chemins d'attaque (2) permet de visualiser et d'éditer les chemins d'attaque du scénario stratégique sélectionné dans la table des scénarios stratégiques (1). Ces chemins d'attaque sont dessinés dans le graphe du scénario stratégique (3). Il est possible de changer l'orientation du graphe avec le bouton •••• (4). Seules les parties prenantes critiques retenues dans Section 4.5.2 peuvent être associées aux chemins d'attaque. Le graphe (3) permet de changer l'ordre des parties prenantes dans le cas où plusieurs parties prenantes seraient associées à un chemin d'attaque. Afin de changer l'ordre des parties prenantes, glisser-déposer la partie prenante à sa position souhaitée.

4.5.4 Activité 3.3 : Définition des mesures de sécurité de l'écosystème

Figure 4.25 a pour objectifs la définition des mesures de sécurité de l'écosystème et la réévaluation de la cartographie de dangerosité de l'écosystème.

					Scér	narios stra	atégiques						4	1
Activité 3.1	Activité 3.2 Activité 3.3													
Définir le	es mesures de sécuri	ité sur l'écosy	stême											-
 Mesures of 	le sécurité de l'écosystème	• 1											T	T Ö
Dádaine la sia	Intitulé	ante de maintenance	utilia in aus la Datation de maté		Descrip	tion			Dépendance	Pénétration	Maturité	Confiance		
système indu	ique de piegeage des equipem Istriel		prestataire sur sit	rieis de maintenan e (permet de rédui	ce administrees p re la pénétration	des fournisseu	i seront mis a d irs de 3 à 2).	isposition du	0	-1	0	0		
Audit de sécu	urité et suivi du plan d'action in	terne	Audit de sécurité	et suivi du plan d'a	tion interne				0	0	0.5	0		
Renforcemen	nt de la protection des données	s de R&D	Solutions à invest	iguer : chiffrement,	cloisonnement o	du réseau R&D.			0	0	0.5	0		
Limitation de	is données transmises		Les données trans	smises, notammen	t aux laboratoire	s, doivent être	réduites au just	e besoin.	0	-1	0	0		
✓ Évaluation	n des parties prenantes 10 2	2												2 0
Catégorie	Nom	Valeur initiale	Mesures de sécurité	Dépendance	Pénétration	Maturité	Confiance	Valeur résiduelle (C) Valeur Résid	duelle (M)		Justification résiduelle	_	^
Clients	Établissements de santé	0.33		1	1	1	3	0.33	1					
Clients	Pharmacies	0.17	Réduire le risque de piégeage des équipements de maintenance utilisés sur le système industriel	1	1	2	3	0.17						
Clients	Grossistes répartiteurs	0.33		1	2	2	3	0.33						
Partenaires	Universités	1	Réduire le risque de piégeage des équipements de maintenance utilisés sur le système industriel	2	1	1	2	1						
Partenaires	Régulateurs	0.25		2	1	2	4	0.25						
		2	Limitation des données							4				¥
 Cartograp 	hie initiale de menace de l'écos	système 🍮				લ લ	Cartog	raphie résiduelle de r	menace de l'écosy	stême 4			થ	۹ 🔳
			seure à matériel	Aartenake	istes répartiteurs					Fournisseurs (• inversite gertenens • ordeness répartiteurs		•

Figure 4.25. Activité 3.3

Dans Figure 4.25, la table des mesures de sécurité de l'écosystème (1) permet de définir les mesures de sécurité de l'écosystème, et leurs valeurs selon les critères de la métrique sélectionée pour l'évaluation des parties prenantes. Les valeurs des mesures de sécurité seront ajoutées aux valeurs initiales des parties prenantes telles que définies à Section 4.5.2 pour chaque critère, ce qui permettra une réévaluation du niveau de dangerosité avec la formule définie dans la métrique. La table d'évaluation des parties prenantes (2) permet d'associer les mesures de sécurité aux parties prenantes taffiche les niveaux résiduels pour chacun des critères, ainsi que le niveau de dangerosité résiduel.

Par exemple, avec 4 critères, si une partie prenante a des niveaux $1 \ 2 \ 2 \ 3$, lui associer une mesure de sécurité avec les valeurs $0 \ 1 \ 0 \ 0$ mènera a des valeurs résiduelles de $1 \ 3 \ 2 \ 3$. La dangerosité résiduelle est ensuite calculée avec les valeurs résultantes ($1 \ 3 \ 2 \ 3$).

Note Les valeurs pour chaque critère ne peuvent pas sortir des valeurs de l'échelle du critère. Ainsi, ajouter une mesure de sécurité 0 -1 0 0 à une partie prenante avec des niveaux 2 1 3 2 mènera aux niveaux résiduels 2 1 3 2, identiques aux niveaux originaux (en supposant que le second critère n'ait pas de valeur inférieure à 1).

Les graphes de l'activité (3 et 4) représentent les cartographies initiale (3) et résiduelle (4) de la dangerosité de l'écosystème. La cartographie initiale (3) présente les mêmes données que celle présentée dans Section 4.5.2 ; elle est répétée ici afin de pouvoir visualiser l'évolution des parties prenantes suite à l'implémentation des mesures de sécurité par la comparaison des deux graphes.

Note La cartographie dessinée ici peut différer de celle de l'activité 3.1 par l'utilisation d'échelles différentes. Les données sont bien les mêmes, seule l'échelle utilisée peut changer. L'activité 3.3 utilise la même échelle pour les deux cartographies, afin de simplifier la comparaison des deux, alors que l'activité 3.1 ne prend en considération que les valeurs initiales pour le calcul de son échelle.

4.6 Version simplifiée de l'atelier 3

Le bouton [1] (1 de Figure 4.23) permet de basculer l'atelier 3 en mode simplifié. Ce mode présente seulement deux activités au lieu de 3 (3.1 et 3.2), en s'affranchissant de l'évaluation de la dangerosité

des parties prenantes. Toutes les parties prenantes définies dans la version simplifiée sont considérées comme étant des parties prenantes critiques, qui pourront être utilisées pour construire des chemins d'attaque.

Cette version simplifiée peut être utilisée afin de construire rapidement des scénarios stratégiques et chemins d'attaque sans s'attarder sur l'évaluation de la dangerosité des parties prenantes. Elle est surtout adaptée pour effectuer une étude dont le cadre temporel serait restreint, mais n'est pas recommandée pour mener à bien une étude complète conforme à la méthode, dans le cadre d'une homologation par exemple.

Depuis la version simplifiée, il est possible de revenir à la version classique de l'atelier avec le bouton

(élément 1 de Figure 4.26).

4.6.1 Activité 3.1 (version simplifiée)

L'activité 3.1, dans sa version simplifiée, présente les mêmes éléments que dans sa version standard, sans les éléments de calcul de la dangerosité des parties prenantes.

Autor 2.4			Scénarios stratégiques	2		10 2
Construir Catégories	e la cartographie de de parties prenantes	dangerosité de l'écosy 2	stème et identifier les parties prenantes critiques		T	1 0
Référence	Nom	Description	Tune	_		
PAR	Partenaires	Partenaires de l'organisation	Externe			
PRE	Prestataires	Prestataires (sous-traitants) de l'organisation	Externe			
CLI	Clients	Tous types de clients	Externe			
FOU	Fournisseurs	Fournisseurs de l'organisation	Externe			
SER	Services connexes techniques	Services et supports proposés par une DSI	Interne			
SER-M	Services connexes métier	Entité commerciale utilisatrices des données métiers	Interne			
FIL	Filiales	nationales ou internations	Interne			
✓ Parties Prei	nantes 🚯 3				T	1
Référence	Nom	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 première pour la recherche et la production de vaccins	Prestataires			
F2	Fournisseurs de matériel	Fournisseurs de matériel pour la recherche et la production de vaccins	Prestataires			
F3	Prestataires informatiques	Sociétés de prestation gérant les éléments du SI	Prestataires			

Figure 4.26. Version simplifiée de l'activité 3.1

Dans Figure 4.26, il est possible de définir les catégories de parties prenantes de la même façon que dans la version standard depuis la table de catégorie des parties prenantes (2). La table des parties prenantes (3) permet de définir les parties prenantes. Contrairement à la version standard de l'activité, il n'y a pas d'évaluation de la dangerosité des parties prenantes. En conséquences, toutes les parties prenantes sont considérées comme retenues.

4.6.2 Activité 3.2 (version simplifiée)

La version simplifiée de l'activité 3.2 est identique à sa version standard.

4.7 Atelier 4 : Scénarios opérationnels

L'atelier 4 est composé de deux pages d'activités et d'une page de configuration. L'activité 4.1 permet de construire les scénarios opérationnels, en définissant les actions élémentaires et les modes opératoires qui les composent. L'activité 4.2 permet d'évaluer la vraisemblance des scénarios opérationnels définis dans l'activité 4.1, selon la méthode souhaitée (expresse, standard ou avancée). Les différentes

méthodes de calcul de la vraisemblance sont présentées dans la fiche méthode 8 du complément à la méthode édité par l'ANSSI.

4.7.1 Configuration de l'atelier 4

Le bouton (élément 3 de l'image de l'activité 4.1) permet d'accéder à la configuration de l'atelier depuis n'importe laquelle de ses activités.

La Figure 4.27 permet de définir les éléments nécessaires à la construction des modes opératoires, et à l'évaluation de la vraisemblance des scénarios opérationnels.



Figure 4.27. Page de configuration de l'atelier 4

Tout d'abord, la Figure 4.27 permet de définir les séquences d'attaque (*kill chains*) disponibles dans l'application (2). Les phases de la séquence d'attaque séléectionnée dans la table des séquences d'attaque (2) peuvent être éditées dans la table des phases (3). Il es possible de choisir la séquence d'attaque à utiliser pour l'étude avec le bouton Sélectionner cette killchain (5). Ces séquences d'attaque permettent de structurer les modes opératoires en différentes phases dans l'activité 4.1.

Il est également possible de définir des catégories d'actions depuis la table des catégories d'actions (4). Ces catégories peuvent associer aux actions pour aider à les classer, lors de la construction des modes opératoires dans l'activité 4.1. La base de connaissance d'actions (6) permet de saisir des actions prédéfinies, qui peuvent être utilisées pour remplir automatiquement les champs des actions lors de la construction des modes opératoires dans l'activité 4.1.

Les éléments suivants (7, 8, 9, 10) permettent de définir la métrique de cotation de la vraisemblance à utiliser dans l'activité 4.2, grâce à une échelle de probabilité de succès (7), une échelle de difficulté technique (8) et une échelle de vraisemblance (9), qui peut être calculée à partir des deux échelles précédentes grâce à la matrice de cotation de la vraisemblance (10).

Le bouton (1) permet de revenir aux activité de l'atelier 4.

4.7.2 Activité 4.1 : Construction des scénarios opérationnels

L'activité 4.1 permet de définir les scénarios opérationnels, en construisant des graphes d'attaque composés d'actions élémentaires liées entre elles pour former des modes opératoires techniques.

Activité 4.1	Activité 4.2			Scénarios opéra	tionnels		1 * ± 2
Élaborer le	es scénarios opératio	nnels					T ± 0
Référence *	Scénario opérationnel	Description opérationnelle	Scénario Stratégique				Chemin d'attaque
R01 R02	Canal direct Vol sur le SI du laboratoire	canal direct Les données sont récupérées sur le SI du laboratoire qui détient une partie des données de R&D.	Vol de données de R&D Vol de données de R&D	canal direct Vol sur le 51 du laboratoire			
RO3	Canal d'exfiltration depuis le prestataire informatique	Le concurrent crée un canal d'exfiltration passant par le SI du prestataire informatique. Un attaquant compromet l'outil	Vol de données de R&D	Canal d'exfiltration depuis le prestat	aire informatique		
R04	Compromission de l'outil de	de maintenance utilisé par le fournisseur de matériel afin de	Sabotage de la campagne de	Compromission de l'outil de mainte	nance		v >
✓ Actions du s	cénario opérationnel : canal dire	a 05					6 🖻 🖬 🖬 🍸 ± 🌣
a. 1.2.2	Intitulé	Catégorie		Phase	Bien support Serveurs pureautiques	Successeurs	
Création et ma	intien d'un canal d'exfiltration via	Pilotage et exploitation de	e l'attaque	Exploiter	(internes) Serveurs bureautiques (internes)	Voler des informations	Exploitation maliciel de collecte et d'exfiltration
Corruption d'u	n personnel de l'équipe de R&D	Recrutement d'une source, c personnel	orruption de	Rentrer	Serveurs bureautiques (internes)	Voler des informations	Reconnaissance externes sources ouvertes
Reconnaissand	e externe avancée	Reconnaissance externe o	de la cible	Connaitre	Serveurs bureautiques	Corruption d'un prestataire d'entretien des locaux	
Corruption d'u locaux	n prestataire d'entretien des	Recrutement d'une source, c personnel	orruption de	Rentrer	Serveurs bureautiques (internes)	Clé USB piégée connectée sur un poste de R&D	Reconnaissance externe avancée
Clé USB piégée	e connectée sur un poste de R&D	Intrusion ou piège ph	ysique	Rentrer	Serveurs bureautiques (internes)	Voler des informations	Corruption d'un prestataire d'entretien des loca
✓ Graphe du s	scénario opérationnel : canal dire	ct 7					
			Connaitre Reconnaissance externe avancée Reconnaissance externes sources ouvertes	Rentree OU Intrusion via un canal d'accès préexistant Intrusion via mail de hameçonnage sur senvice RH	Trouver Latéralisation vers réseaux LAN et R&D Reconnaissance interne réseaux bureautique & IT site de Paris	Exploiter Exploitation maliciel de collecte et d'exfiltration d'un canal d'exfiltration via un poste internet	-

Dans cette activité, la table des scénarios opérationnels présente les chemins d'attaque définis dans Section 4.5.3. Pour chacun de ces chemins d'attaque, il est possible de définir un scénario opérationnel. Pour construire un scénario opérationnel, sélectionner le scénario souhaité dans la table des scénarios opérationnels (4). La liste des actions du scénario s'affiche alors dans la table des actions (5), et son graphe d'attaque est dessiné dans la zone du graphe (7). Afin de modifier le mode opératoire, il est possible d'éditer les actions depuis la table des actions (5), ou bien de faire les modifier directement depuis le graphe (7). Depuis le graphe, un double-clic dans une des phases permet de créer une nouvelle action dans cette phase ; un double-clic sur une action permet d'éditer l'action ; il est possible de créer une transition entre deux actions en sélectionnant l'action source puis l'action destination ; un double-clic sur une transition permet d'éditer la transition.

Les modifications apportées via le graphe sont identiques à celles apportées via la table des actions. La table des actions permet cependant de dupliquer une action dans d'autres scénarios, grâce au

bouton (6). Afin de dupliquer une action, sélectionner l'action à dupliquer dans la table des actions (5) puis cliquer sur le bouton (6). Un formulaire s'ouvre alors pour demander vers quels scénarios dupliquer l'action. Sélectionner les scénarios, puis valider le formulaire afin de dupliquer l'action dans les scénarios sélectionnés.

Note Lors de la duplication d'une action, les éléments saisis dans l'activité 4.2 (niveaux de probabilité de succès et de difficulté technique, et justification) sont également copiés.

Le graphe permet de créer des groupes d'action en déplaçant une action sur une autre action. Ces groupes d'action peuvent être des groupes ET ou des groupes OU. Pour changer le type d'un groupe d'action, double-cliquer sur l'en-tête du groupe (qui comporte le label ET ou OU). Les groupes d'actions ET permettent d'indiquer que les actions doivent toutest être réalisées pour que le mode opératoire puisse être rempli, alors que les groupes d'actions OU permettent d'indiquer que l'une des actions du groupe doit être effectuée. Dans le calcul des modes opératoires, les actions d'un groupe ET sont simplement mises les unes à la suite des autres, alors que pour un groupe OU, un mode opératoire sera créé pour chaque action contenue dans le groupe.

4.7.3 Activité 4.2 : Évaluation de la vraisemblance des scénarios opérationnels

L'activité 4.2 permet d'évaluer la vraisemblance des scénarios opérationnels selon les trois méthodes proposées par la méthode : la méthode expresse, la méthode standard et la méthode avancée.

Méthode expresse

Pour utiliser la Figure 4.28, sélectionner Méthode expresse comme méthode d'évaluation (élément 1 de Figure 4.28, disponible sur les trois méthodes de l'activité).

Activité 4 1	Activité 4.2			Scénarios opé	rationnels			0 a 0
Évaluer la	vraisemblance des s	cénarios opérationne	els					Méthode d'évaluation : Méthode Expresse 🔻
Méthode exp	2 resse C C 3							
✓ Scénarios e	opérationnels 🚯 4							T 1 0
Référence	Chemin d'attaque	Scénario opérationnel	Description opérationnelle	Scénario Stratégique	Probabilité	Difficulté	Vraisemblance	Justification initiale
R04	Compromission de l'outil de maintenance	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.	Sabotage de la campagne de vaccination	Quasi-certaine	Élevée	Très vraisemblable / modérée	
R05	Altération de l'étiquetage des vaccins	Altération de l'étiquetage des vaccins	Les étiquettes des vaccins sont modifiées, afin d'empêcher leur livraison correcte.	Sabotage de la campagne de vaccination	Quasi-certaine	Faible	Quasi-certain / Facile	
R01	canal direct	Canal direct	Exfiltration des données via un canal direct	Vol de données de R&D	Faible	Faible	Très vraisemblable / modérée	
R03	Canal d'exfiltration depuis le prestataire informatique	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	Faible	Très élevée	Peu vraisemblable / Difficile	
R02	Vol sur le SI du laboratoire	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	Quasi-certaine	Modérée	Vraisemblable / Elevée	

Figure 4.28. Activité 4.2 : méthode expresse

Dans la méthode expresse, seule la table des scénarios opérationnels (4) est affichée, et permet de saisir des valeurs de probabilité de succès et de difficulté technique pour chaque scénario opérationnel. La vraisemblance est alors calculée automatiquement par l'application selon la Section 4.7.1, ou peut être renseignée manuellement.

Comme dans les autres méthodes, les boutons (2) et (3) permettent de recalculer les valeurs de vraisemblance en fonction des valeurs de probabilité de succès et de difficulté technique. Le bouton (2) ne recalcule que les valeurs qui n'ont pas été modifiées (c'est-à-dire les valeurs identiques aux valeurs calculées), alors que le bouton (3) permet de recalculer l'ensemble des valeurs, qu'elles aient été forcées par l'utilisateur ou non.

Méthode standard

La Figure 4.29 permet d'attribuer un niveau de vraisemblance élémentaire (probabilité de succès) à chaque action, afin de permettre à l'application de calculer le niveau résultant sur chaque mode opératoire technique, et d'inférer ensuite le niveau de vraisemblance globale du scénario.

	445-644.4.0				Scénarios opération	onnels		10 2 0
Évaluer	la vraisemblance de	s scéna	arios opérationnels					Méthode d'évaluation : Méthode Standard 💌
Méthode Sta	tandard C 2							Algorithme de calcul : Algorithme standard (vraisemblance = probabilité minimale) *
✓ Scénario:	os opérationnels 🚯 1							T 1 ¢
Référenc∉	Chemin d'attaque		Scénario opérationnel	Description of	pérationnelle	Scénario Stratégique	Vraisemblance	Iustification initiale
R01	canal direct	Canal dir	rect	Exfiltration des données via un	n canal direct	Vol de données de R&D	Peu vraisemblable / Difficile	
R02	Vol sur le SI du laboratoire	Vol sur le	e SI du laboratoire	Les données sont récupérées	sur le SI du laboratoire qui	Vol de données de R&D	Vraisemblable /	
R03	Canal d'exfiltration depuis le prestataire informatique	Canal d'e informat	exfiltration depuis le prestataire tique	Le concurrent crée un canal d' du prestataire informatique.	exfiltration passant par le SI	Vol de données de R&D	Vraisemblable / Elevée	
✓ Actions d	du scénario opérationnel : Cana	l direct	a 2	Un attaduant compromet rout	ji de maintenance utilise par		Ires	1
	Intitulé		Probabilité				Iustification	
Reconnaissa	ance externes sources ouverte	5	Faible Le	s méthodes actuelles d'OSINT perm	ettent d'agréger des connaissa	ances utiles pour mener à bien de	s attaques cyber	
Intrusion via	ia un canal d'accès préexistant		Très élevée					
Intrusion via	ia mail de hameçonnage sur se	rvice RH	Quasi-certaine					
Intrusion via	ia le site du CE (point d'eau)		Faible					
Reconnaissa site de Paris	ance interne réseaux bureautions	jue & IT	Très élevée					
< Contractions								• • • • • • • • • • • • • • • • • • •
✓ Modes op	pératoires du scénario opératio	onnel : Cana	al direct 🚯 3					1 0
Probabilit	ité Justification							Actions
Faible	Reconna	issance ext	ternes sources ouvertes -> Intrus	ion via un canal d'accès préexistant	Reconnaissance interne rése	eaux bureautique & IT site de Par	is -> Latéralisation vers	réseaux LAN et R&D -> Exploitation maliciel de collecte et d'exfiltration -> Création et maintien
Faible	Reconna	issance ext	ternes sources ouvertes -> Intrus	ion via mail de hameçonnage sur se	rvice RH -> Reconnaissance int	terne réseaux bureautique & IT si	te de Paris -> Latéralisa	tion vers réseaux LAN et R&D -> Exploitation maliciel de collecte et d'exfiltration -> Création et
Faible	Reconna	issance ext	ternes sources ouvertes -> Intrus	ion via le site du CE (point d'eau) -> F	leconnaissance interne réseau	ix bureautique & IT site de Paris -	> Latéralisation vers ré:	seaux LAN et R&D -> Exploitation maliciel de collecte et d'exfiltration -> Création et maintien d'u
Faible	Reconna	issance ext	ternes sources ouvertes -> Corru	otion d'un personnel de l'équipe de l	R&D -> Voler des informations			
Faible	Reconna	iissance ext	terne avancée -> Corruption d'un	prestataire d'entretien des locaux ->	 Clé USB piégée connectée sur 	r un poste de R&D -> Voler des in	formations	
•								•
✓ Graphe d	du scénario opérationnel : Cana	l direct 🛛 🤞	4					
			c	onnaitre	Rentrer	Trouver		Exploiter
			Recor	inaissance le avancée	OU trusion via un canal	Latéralisation vers réseaux LAN et R&D		tion maliciel de et d'exfluration
				d	accès préexistant			

Figure 4.29. Activité 4.2 : méthode standard

Dans la Figure 4.29, la table des scénarios opérationnels (1) permet de sélectionner le scénario opérationnel à afficher. La table des actions (2) permet de modifier la vraisemblance élémentaire (probabilité de succès) des actions, ainsi que de justifier le niveau choisi. Les modes opératoires calculés à partir du graphe défini dans Section 4.7.2 sont affichés dans la table des modes opératoires (3). La probabilité de succès des modes opératoires est calculée automatiquement à partir des niveaux de vraisemblance élémentaire (probabilité de succès) des actions. Il est possible de forcer un niveau de probabilité de succès des modes opératoires différent de celui calculé. Sélectionner un mode opératoire le fait ressortir dans le graphe (4). Le graphe affiché est similaire à celui de Section 4.7.2, mais les niveaux de vraisemblance élémentaire des actions sont affichés en plus.

Méthode avancée

La Figure 4.30 est très similaire à la méthode standard, mais permet d'évaluer les actions en termes de difficulté d'exploitation en plus d'une probabilité de succès.

Scénarios opérationnels									
Évaluer la vraisemblance des scénarios opérationnels Méthode d'évaluation : Méthode Avancée *									
Méthode ava	ncée C 2					Algorithme de calcul : Algorithme avancé standard (mode opératoire le plus vraisemblable) 🔻			
✓ Scénarios	opérationnels 🚯 1					T 1 4			
Référence '	 Chemin d'attaque 	Scénario opérationnel	Description opérationnelle	Scénario Stratégique	Vraisemblance	Justification initiale			
R01	canal direct	Canal direct	Exfiltration des données via un canal direct	Vol de données de R&D	Vraisemblable / Elevée	·			
R02	Vol sur le SI du laboratoire	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 / Elevée				
٤	Canal devilteration dancie la	Canal doublication donuis la	Le concurrent cree un canai		Verienselstelete /	۲ ۲			
✓ Actions du	scénario opérationnel : Canal dire	α 🖸 <mark>2</mark>				2 🕈			
Reconnaissar ouvertes Intrusion via préexistant Intrusion via sur service Ri Intrusion via	Inthité aisemblance ékherental Difficulté Difficulté justification * acconsistance extentes source ouvertes Fable Fable Les méthodes actuelles d'OSINT permettent d'agréger des connaissances utiles pour mener à bien des attaques cyber * intrusion via una d'ackes prédesistant Très élevé Fable * * intrusion via una de hanegronge sur service RH Quasientation Fable * *								
✓ Modes op	ératoires du scénario opérationnel	: Canal direct 🚯 3				1			
Probabilité Faible Faible Faible	Difficulté Vraisemblanc Élevée Peu vraisemblat Difficile Élevée Peu vraisemblat Difficile Peu vraisemblat Difficile	e Justifici	ation Recom R&D -> Recom LAN et Recom > Explo	naissance externes sources ouver Exploitation maliciel de collecte e naissance externes sources ouver R&D -> Exploitation maliciel de co naissance externes sources ouver pitation maliciel de collecte et d'ex	tes -> Intrusion via t d'exfiltration -> Cr tes -> Intrusion via ollecte et d'exfiltrati tes -> Intrusion via cfiltration -> Créatio	Actions Action			
Faible	Faible Modérée Vraisemblable / Vraisemblable / Reconnaissance externes sources ouvertes > Corruption d'un personnel de l'équipe de R&D > Voler des informations								
👻 Graphe du	scénario opérationnel : Canal dire	et 4							
		Recon	Connaitre naissance e avancée 2 2	Rentrer OU Intrusion via un canal d'accès préexistant	La rés	Trouver Exploiter Advalation vers Seaux LAN et R&D D Collecte et desfitzation Collecte at maintain Collection at maintain V			

Figure 4.30. Activité 4.2 : méthode avancée

Dans la Figure 4.30, la table des scénarios (1) est similaire à celle de la méthode standard. Sélectionner un scénario opérationnel dans la table des scénarios (1) permet d'évaluer la vraisemblance élémentaire et la difficulté technique des actions qui le composent depuis la table des actions (2). L'application est alors en mesure de calculer automatiquement une probabilité de succès pour les modes opératoires de la même façon que dans la méthode standard. Avec la méthode avancée, la même technique est utilisée pour calculer une difficulté technique des modes opératoires, et en déduire un niveau de vraisemblance pour chaque mode opératoire en utilisant la matrice de cotation définie dans la Section 4.7.1. L'application calcule ensuite la vraisemblance globale du scénario opérationnel à partir des vraisemblances des modes opératoires. L'utilisateur a donc à renseigner uniquement les valeurs de vraisemblance élémentaire (probabilité de succès) et de difficulté technique pour chaque action d'un scénario, et l'application en déduit les niveaux pour les modes opératoires et le scénario opérationnel. Il est toutefois possible à l'utilisateur de forcer des valeurs différentes de celles calculées à tous les niveaux.

Tout comme dans la méthode standard, le graphe (4) est similaire à celui défini dans Section 4.7.2, mais affiche cette-fois pour chaque action son niveau de vraisemblance élémentaire (probabilité de succès) (à gauche) et son niveau de difficulté technique (à droite).

4.8 Atelier 5 : Traitement du risque

L'atelier 5 est constitué de 3 activités et d'une page de configuration. L'activité 5.1 consiste à effectuer une synthèse des risques afin de permettre leur évaluation. L'activité 5.2 définit la stratégie de traitement des risques, avec le plan de traitement associé et les risques résiduels. L'activité 5.3 permet la définition du cadre de suivi des risques et des cycles opérationnels et stratégiques prévus.

4.8.1 Configuration de l'atelier 5

Le bouton (élément 3 de Figure 4.32 permet d'accéder à la configuration de l'atelier depuis n'importe laquelle de ses activités.



Figure 4.31. Page de configuration de l'atelier 5

Dans la Figure 4.31, la table des niveaux de risque (2) permet de définir les niveaux de risque existants, qui seront calculés en fonction de la gravité et de la vraisemblance selon la matrice de Farmer (3). Les autres éléments de la page (4, 5, 6, 7) servent à la définition des mesures de sécurité dans l'activité 5.2. La table des catégories de mesures de sécurité (4) permet de définir les catégories servant à classer les mesures de sécurité. Les statuts des mesures de sécurité (5) permettent de définir les statuts servant à suivre l'avancement de mise en œuvre des mesures de sécurité. Les complexités des mesures de sécurité. La table de configuration des échéances (7) permet d'attribuer une couleur spécifique à la date d'échéance des mesures de sécurité en fonction de la date renseignée comme échéance et de la date du jour. Une valeur négative signifie que la date d'échéance est antérieure à la date du jour (dans les délais), une valeur positive signifie que la date d'échéance est ultérieure à la date du jour (retard).

Le bouton (1) permet de revenir aux activités de l'atelier 5.

4.8.2 Activité 5.1 : Évaluation des risques

Figure 4.32 consiste à évaluer les risques identifiés dans les ateliers précédents.

Activitá E 4	Traitement du risque											
✓ Scénarios	venture realizations () 3											
Référence	Chemin d'attaque	Description	Gravité	risque initial								
R04	Compromission de l'outil de maintenance	Un attaquant compromet l'outil de maintenance utilisé le fournisseur de matériel afin de porter atteinte à la production des vaccins.	par Critique	Vraisemblable / Elevée	Majeur							
R05	Altération de l'étiquetage des vaccins	Les étiquettes des vaccins sont modifiées, afin d'empêt leur livraison correcte.	her Critique	Peu vraisemblable / Difficile	Imp	ortant						
R01	canal direct	Exfiltration des données via un canal direct	Majeur	Très vraisemblable / modérée	Ма	ijeur						
R03	Canal d'exfiltration depuis le prestataire informatique	Le concurrent crée un canal d'exfiltration passant par le du prestataire informatique	SI Majeur	Quasi-certain / Facile	Crit	tique						
R02	Vol sur le SI du laboratoire	Les données sont récupérées sur le SI du laboratoire qu délient une partie des données de R&D	ui Majeur	Impi	ortant							
∢ ❤ Cartograp	v caroorashie initiale du risoue 4											
				Vraiser	nblance							
Gravité	Peu vraisemi	blable / Difficile	Vraisemblable / Elevé	e	Très vraisemblable / modérée	Quasi-certain / Facile						
Critique	R05		R04									
Majeur			R02		R01	R03						
Important	tant											
Mineur	Mineur											
 Évènemen 	Evènements redoutés 5											

Figure 4.32. Activité 5.1

Dans Figure 4.32, les risques sont présentés dans la table des scénarios de risques (3) ainsi que dans la cartographie des risques (4). Les niveaux de risque et leur calcul sont définis dans la Section 4.8.1. La table des évènements redoutés (5) permet de montrer les évènements redoutés afin de visualiser ceux qui ne sont associés à aucun scénario, apparaissant en gras dans la table. Cette table est similaire à celle présente dans Section 4.3.3, et est cachée par défaut. Cliquer sur le titre de la table pour l'afficher.

Le bouton (1) permet d'exporter les données de l'atelier, et le bouton (2) permet d'accéder à la Section 4.8.1.

4.8.3 Activité 5.2 : Stratégie de traitement du risque et définition des mesures de sécurité

Figure 4.33 a pour objectifs la définition de la stratégie de traitement du risque et des mesures de sécurité.

Traitement du risque											2					
Décider de la stratégie de traitement du risque et définir les mesures de sécurité																
✓ Mesures d	e sécurité 🚯 1													۵		T ± ¢
Référence M02	Audit de sécurité technique e SI bureautique par un PASSI	Intitulé Entité respon é technique et organisationnel de l'ensemble du RSSI par un PASSI		ible és de mise eloût/Complexit Priorité		Statut À lancer	Statut Catégorie A lancer Gouvernance et anticip (dont audit)		Commentaire additionnel		Date d'échéance Description Audit de sécurité technique et organisationne de l'ensemble du S1 bureautique p.		sonne responsa iel 11 par		Charge estir 1	
 Mesures d 	e sécurité de l'écosystème 🚯	2														T±O
Référence ME01	Intitulé Réduire le risque de piégeage des équipements de maintenance utilisés sur le système industriel	Description Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site (permet de réduire la pénétration des fournisseurs de 3 à 2).		Risques associés Compromission de l'outil de maintenance		ntité responsable	Difficu	ultés de mise en œuvre	Coût/Complexit	Charge estin	Date d'écl	néance Prie	orité	Statut À lancer	Catégorie * Protection (Cloisonne MCS)	
ME02	Audit de sécurité et suivi du plan d'action interne	Audit de sécurité et suivi du plar	Canal d'exfiltration de puis le prestataire informatique			RSSI	Accepta par les p laborato	tion de la démarche prestataires et pires	++		26/09/2025			À lancer	et anticipatior	
Référence	Chemin d'attaque	Description	liveau de risque ini	ia N	tesures de l'écosu	stàme			Mesures de sécu	rité	crint	ion et analyse d	urisque rési	irovitá rás		raisemblance (
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.	Majeur	Réduire le ris de maintenar industriel Audit de sécu interne	des équipe système an d'action	Intégration ements dans les cor Mise en plat ayant lieu cl Audit de séc Renforceme Renforceme	stion d'une clause de parantie d'un niveau de sécurité satofalisant is contrats avec les prestataires et alboratorites n place d'une procédure de signalement de tout incident de sécurité lieu cheu prestataires ou un laboratorie de sécurité organisationnel des prestataires et laboratories clés rement de la sécurité du system inclustriel rement de la sécurité d'activité					a noque resa	Critiqu	ue	Peu vraisemt Difficile	
Cartographie initiale du risque 4 Cartographie initiale du risque 5																
Vraisemblance							Vraisemblance									
Gravité	Peu vraisemblable / Difficile	Vraisemblable / Elevée	Très vraisemblab	le / modérée	Quasi-certa	ain / Facile	Gravité	Peu v	raisemblable / Difficile R04	Vraisembla	ole / Elevée	Très vraisemb	lable / modérée		Quasi-certa	in / Facile
Critique	RUS	H04				Critique		R05			002					
Important		NJ2	RUT		KU		Important		NU2	R			05			
Mineur							Mineur									

Figure 4.33. Activité 5.2

Dans Figure 4.33, la table des mesures de sécurité (1) permet de définir les mesures de sécurité à implémenter. Ces mesures de sécurité peuvent être associées à des scénarios de risques, des Section 4.3.2, des exigences du Section 4.3.4 et des actions des Section 4.7.2. Les mesures de sécurité de l'écosystème définies dans Section 4.5.4 apparaissent dans la table des mesures de sécurité de l'écosystème (2). Elles peuvent être associées à des risques et à des exigences du Section 4.3.4.

Les risques résiduels peuvent être définis dans la table des risques résiduels (3). Il est nécessaire de définir la gravité et la vraisemblance résiduelles des risques depuis la table si celles-ci ne sont pas définies.

Une fois la cotation des risques résiduels effectuée, ceux-ci apparaissent sur la cartographie résiduelle des risques (5). Il est alors possible de changer la cotation en effectuant des glisser-déposer des risques dans la cartographie résiduelle des risques. La cartographie initiale du risque (4) est identique à celle de Section 4.8.2, et permet de visualiser l'évolution des risques avec les deux cartographies.

4.8.4 Activité 5.3 : Cadre de suivi des risques

Figure 4.34 vise à renseigner quelques éléments sur le suivi des risques.

Traitement du risque							
Activité 5.1 Activité 5.2 Activité 5.3					_		
Cadre de suivi des risques							
✓ Comité de suivi des risques			2	T	1 0		
Nom Fonction	Rôle						
John							
✓ Cycles stratégiques et opérationnels			2	T	1 0		
Type Nom	Date de début						
Stratégique Première version de l'étude 03/06/2024 Opérationnel Revue des risques 01/01/2025							
Stratégique Révision dans le cadre de 05/01/2026							
" I'homologation							

Figure 4.34. Activité 5.3

Dans Figure 4.34, la table du comité de suivi des risques (1) permet de renseigner les membres du comité de suivi des risques, en charge du suivi de l'évolution des risques et de l'application du plan de traitement. La table des cycles stratégiques et opérationnels (2) est similaire à celle précédente dans Section 4.3.1, et permet de définir les cycles opérationnels et stratégiques à venir.