# Retour d'expérience

# EBIOS Risk Manager

CLUBEBIOS

CLUBEBIOS

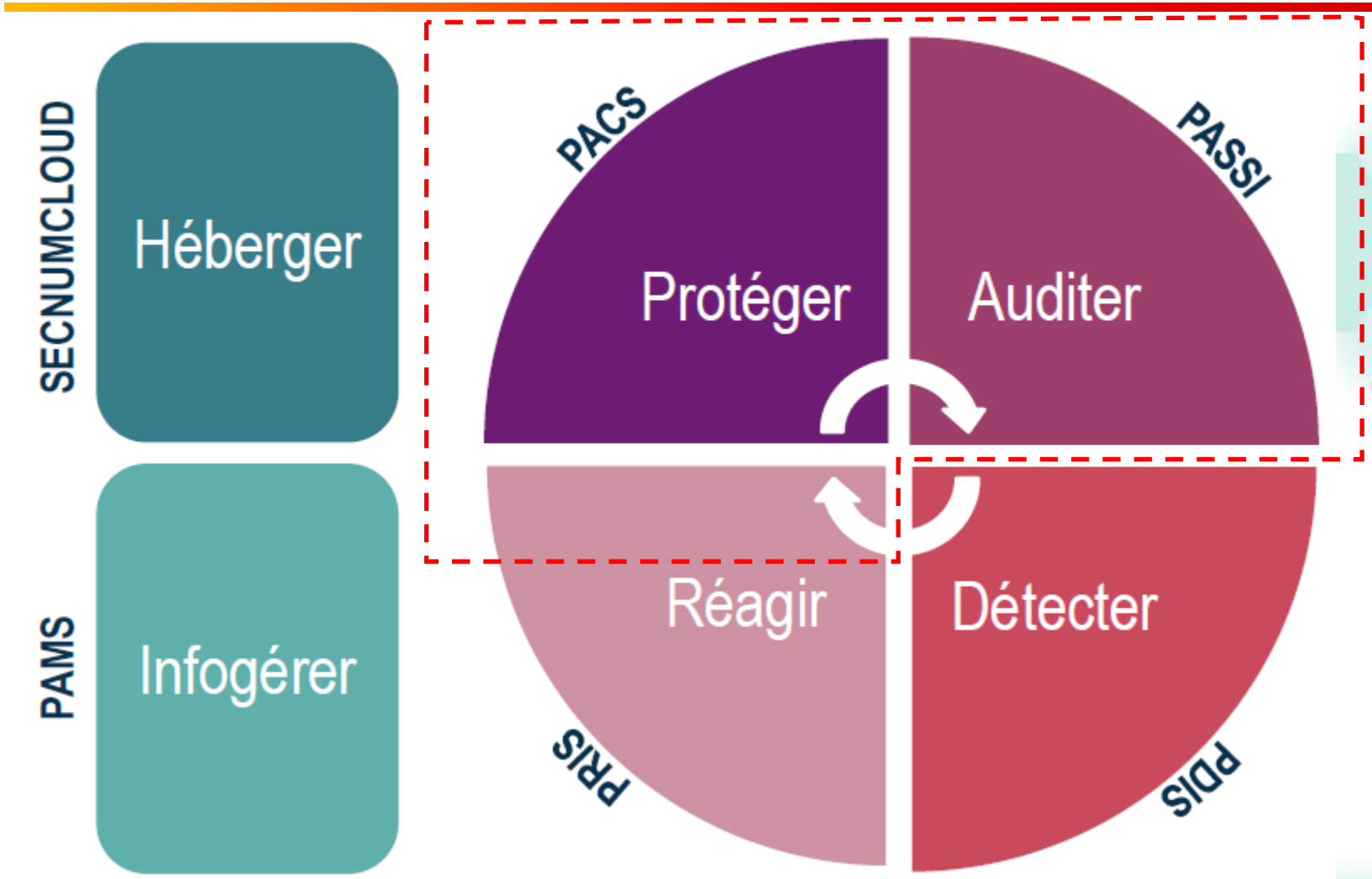
# RETEX EBIOS Risk Manager – ALL4TEC

## Centre d'Expertise Aérienne Militaire / EM Cyber

Vincent GUILLOT – Claire DÉNIEL

*rédacteur et relecteur d'analyse de risques opérationnels d'origine cyber*

# Centre d'expertise aérienne militaire / EM CYBER




MINISTÈRE DES ARMÉES
*Liberté Égalité Fraternité*

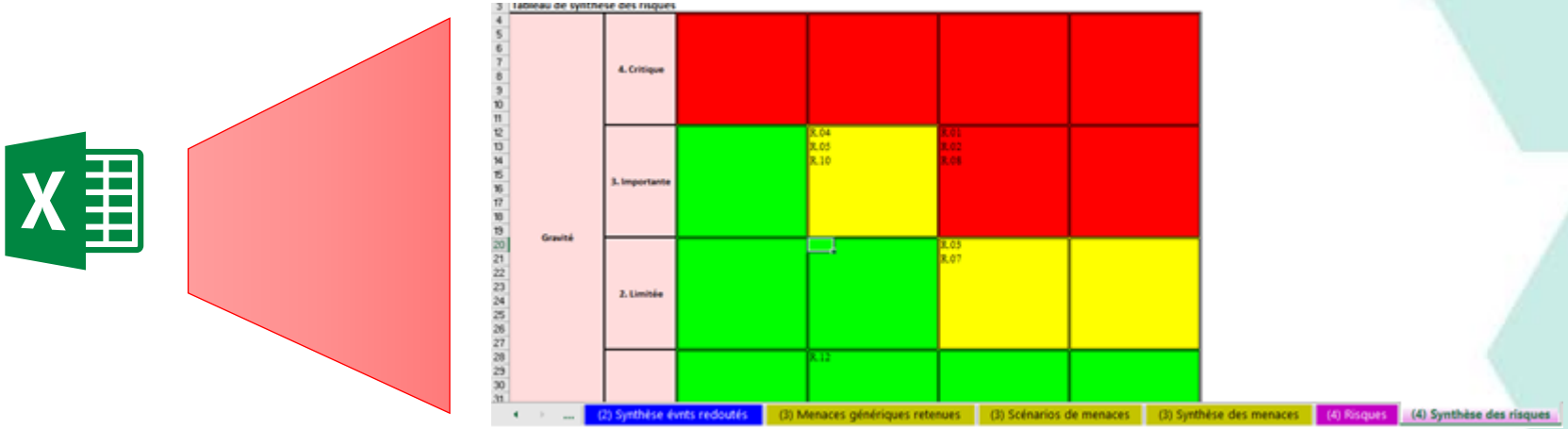
ARMÉE DE L'AIR & DE L'ESPACE

CEAM

**EM CYBER**

# Avant EBIOS Risk Manager

- Différentes expériences
  - EBIOS
  - approche capacitaire
  - attaque/défense
- Développement interne d'un outil pour EBIOS 2010




- Accueil favorable de la nouvelle méthode et d'un outil labellisé

# Premières impressions sur EBIOS Risk Manager

- évolution du paradigme
- littérale et visuelle
- menaces
- itération
- modularité

- périmètre/écosystème/partie prenante/cartographie
- socle de sécurité
- modélisation de scénarios opérationnels
- production hétérogène, rédaction de FEROS et d'APRI
- adhérence outil/méthode
- formation, pratique et confrontation entre praticiens

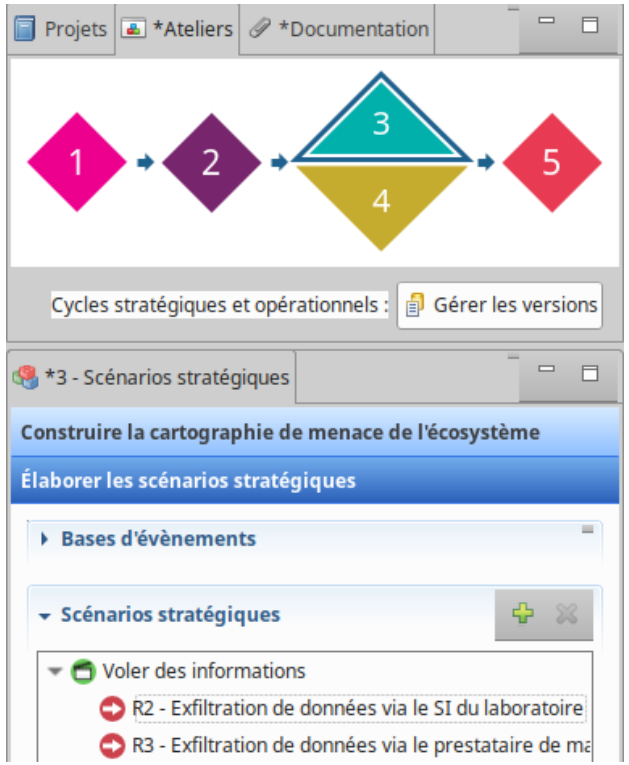
- impact organisation : RH (métier, cyber, rens., etc.), méthode et livrables
- classification
- outil indispensable

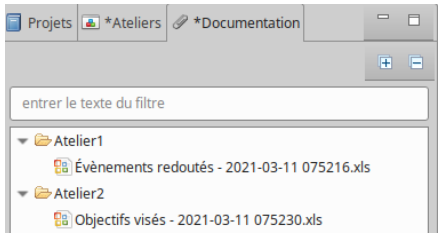
# Recherche d'outillage labellisé

- Etude du cahier des charges de l'ANSSI
- Prises de contact avec les éditeurs
- « Webinaires » et/ou mise à disposition de version « beta » d'évaluation
- Etude des fonctionnalités et des prérequis techniques des solutions disponibles

Recherche effectuée sur plusieurs mois au travers de la réalisation d'une analyse de risques « 5 ateliers » avec l'aide de version « Beta » ce qui a permis d'effectuer un benchmark exhaustif et concret.

# Benchmarking / Choix de la solution ALL4TEC




**Logiciel :**

- interface user friendly => pas besoin de consulter un manuel
- découpage en atelier et sous atelier selon le guide méthodologique
- respect strict de la terminologie EBIOS Risk Manager
- saisie « double entrée » : simple et intuitive tout au long des ateliers
- personnalisation aisée des tableaux
- système simple pour l'export/stockage des tableaux et schémas
- module d'élaboration et de cotation des scénarios intuitifs

**Déploiement et MCO/MCS :** simple à installer et soutenir (JAVA), multi OS, peu gourmande (cf. utilisation poste nomade)

**Disponibilité / écoute des équipes**

**Amélioration continue du produit :** correction des bug et intégration des RETEX

# RETEX sur la méthode et le logiciel

## Atelier 1 : Périmètre technique

**Interface intuitive :** saisie, export, mise en forme tableau rapide (initiale, itérations)

Contenu de la base de valeurs métier

*Glisser des colonnes ici pour grouper les lignes*

| | ✓/☐ | Abrév. | Nom | Description |
|---|---|---|---|---|
| 1 | ☑ | P.01 | Recherche & Développement (R&D) | Activité de recherche et développement des vaccins nécessitant :<br>• l'identification des antigènes ;<br>• la production des antigènes (vaccin vivant atténué, inactivé, s inactivation, filtration, stockage ;<br>• l'évaluation préclinique ;<br>• le développement clinique. |
| 2 | ☑ | P.02 | Fabriquer des vaccins | Activité consistant à réaliser :<br>• le remplissage de seringues (stérilisation, remplissage, étiqu<br>• le conditionnement (étiquetage et emballage). |
| 3 | ☑ | I.01 | Traçabilité et contrôle | Informations permettant d'assurer le contrôle qualité et la libérati aseptique, conditionnement, libération finale...) |

**Evolution :** définition des **besoins de sécurité** des valeurs métiers en lien avec les Evénements redoutés

**Schéma fonctionnel :** couverture et lien entre Métiers/SI et ajustement de la granularité => importer schéma

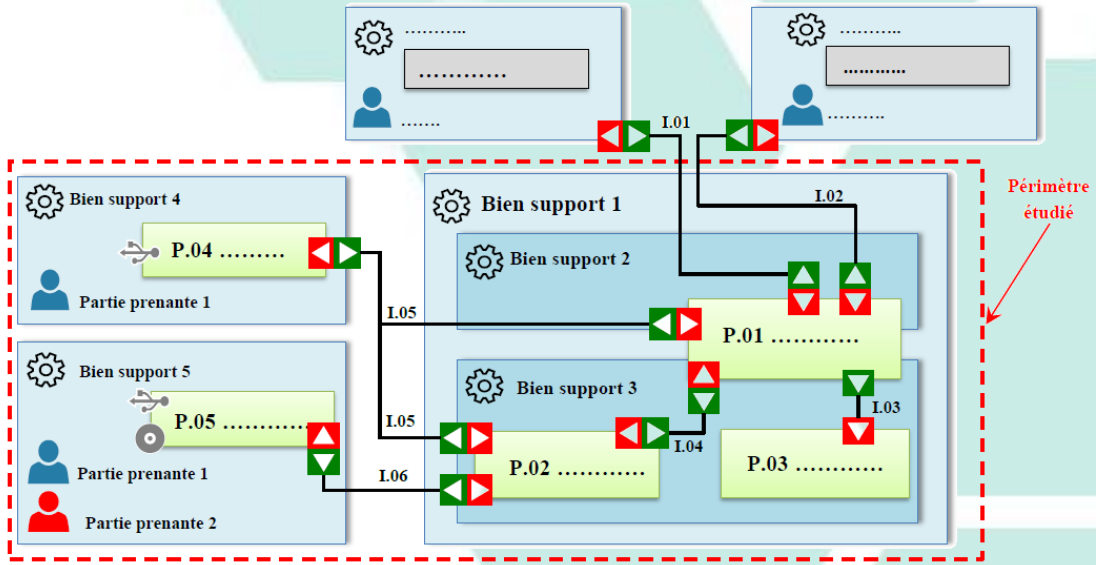



*Figure 1: Architecture fonctionnelle*

**Périmètre :**

système & écosystème ⇔ BS & PP de rang 1 à n

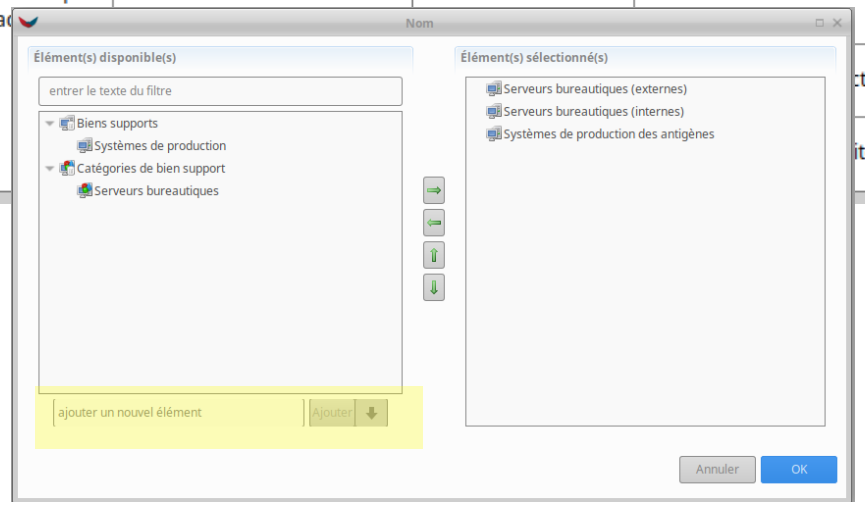
# RETEX sur la méthode et le logiciel

## Atelier 1 : synthèse du périmètre

Identification des missions de l'objet étudié

*Glisser des colonnes ici pour grouper les lignes*

| | ✓/☐ | Mission | Valeurs métier | | | Biens supports | | |
|---|---|---|---|---|---|---|---|---|
| | | | Nom | Nature | Responsables | Nom | Catégories | Responsables |
| 1 | ☑ | Identifier et fabriquer des vac | Recherche & Développement (R&D) | Processus | Pharmacien | Serveurs bureautiques (externes) | Serveurs bureautiques | Laboratoires |
| 2 | | | | | | Serveurs bureautiques (internes) | Serveurs bureautiques | DSI |
| 3 | | | | | | Systèmes de production des antigènes | | Laboratoires |
| 4 | | | | | tion | Systèmes de production | | DSI<br>Fournisseurs de matériel |
| 5 | | | | | ité | Serveurs bureautiques (internes) | Serveurs bureautiques | DSI |




**Saisie « double entrée » avec « alerte » :**

- base de données : initiale
- tableau de synthèse : initiale et/ou mise à jour

# RETEX sur la méthode et le logiciel

## Atelier 1 : Socle de sécurité

Plan d'amélioration continue de la sécurité

*Glisser des colonnes ici pour grouper les lignes*

| | Réf. | Référentiel | Mesure de sécurité | Type | Éléments associés | Scénarios de risque associés | Responsables | Freins et diffi |
|---|---|---|---|---|---|---|---|---|
| 1 | M1 | Référentiel de sécurité BIOTECH | Sensibilisation renforcée au hameçonnage par un prestataire spécialisé | Gouvernance | | R1 - Exfiltration de données via le SI de la R&D | RSSI | Validation du CHSCT |
| 2 | M2 | Référentiel de sécurité BIOTECH | Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI | Gouvernance | F3 - Prestataire informatique | R1 - Exfiltration de données via le SI de la R&D<br>R5 - Modification de l'étiquetage | RSSI | |

**Cas d'utilisation :**

- 1er cas « Projet » : définition/expression du besoin « FEROS » => socle de sécurité théorique
- 2eme cas « En Service » : socle de sécurité théorique et pratique (cf. audit)

  => Niveau de granularité pas forcément identique entre les deux besoins

**Périmètre du socle de sécurité :** Système / BS vs Ecosystème / PP => répétition ateliers 1 & 3 impact sur rapport global

**Logiciel :**

- Interface intuitive et couvre tous les besoins
- Rapport global : deux exports / tableaux

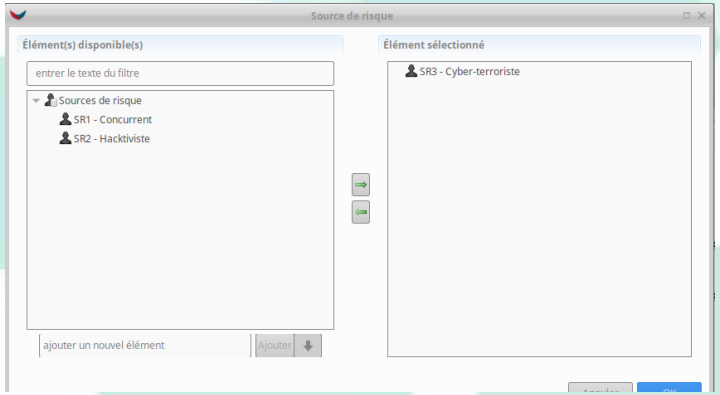
# RETEX sur la méthode et le logiciel

## Atelier 2 : Sources de risques / Objectifs Visés

Évaluation des couples source de risque / objectif visé

*Glisser des colonnes ici pour grouper les lignes*

| | Identification | | Cotation | | | Évaluation de la pertinence | | |
|---|---|---|---|---|---|---|---|---|
| | Source de risque | Objectif visé | Motivation | Ressources | Activité | Pertinence proposée | Pertinence retenue | Retenu |
| 1 | SR1 - Concurrent | OV1 - Voler des informations | +++ | +++ | +++ | 3. Élevée | 3. Élevée | ☑ |
| 2 | SR2 - Hacktiviste | OV2 - Saboter la campagne nationale de vaccination | ++ | + | ++ | 1. Faible | 2. Moyenne | ☑ |
| 3 | SR2 - Hacktiviste | OV3 - Divulguer des informations sur les tests animaliers | ++ | + | + | 1. Faible | 1. Faible | ☐ |




**Sources de risques :**

- Catégories : ajustées à l'étude
- Granularité : bon niveau exploitable
- Evaluation :
  - critère « activité » difficile à juger
  - « caractérisation » et motivation/opportunité plus pertinentes

**Objectifs visés :**

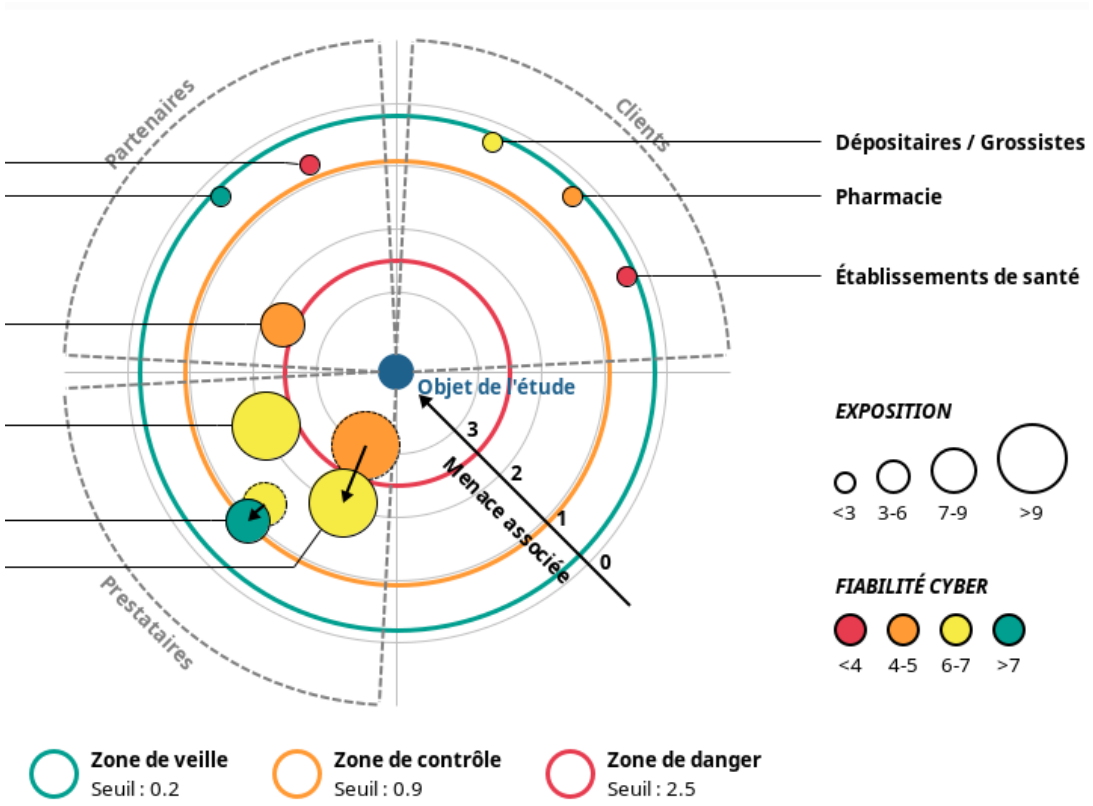
- Catégories : ajustées à l'étude
- Granularité : bon niveau exploitable

Description : Métier / informatique => impacts OPS / TECH (cf. ER) => préparation scénarios (itération entre ateliers)

**Choix des** SR/OV retenus en fonction des modes opératoires et des ressources

# RETEX sur la méthode et le logiciel

## Atelier 3 : Cartographie menace numérique / Partie prenante




**Description :** bien penser organisation & systèmes, notamment amont et ceux qui traitent une partie des VM

**Formalisation / évaluation** :
Granularité / exhaustivité (cf. description) ⇔ évaluation « catégorie »

**Définition des seuils/zones :**
« veille », « contrôle » et « danger »

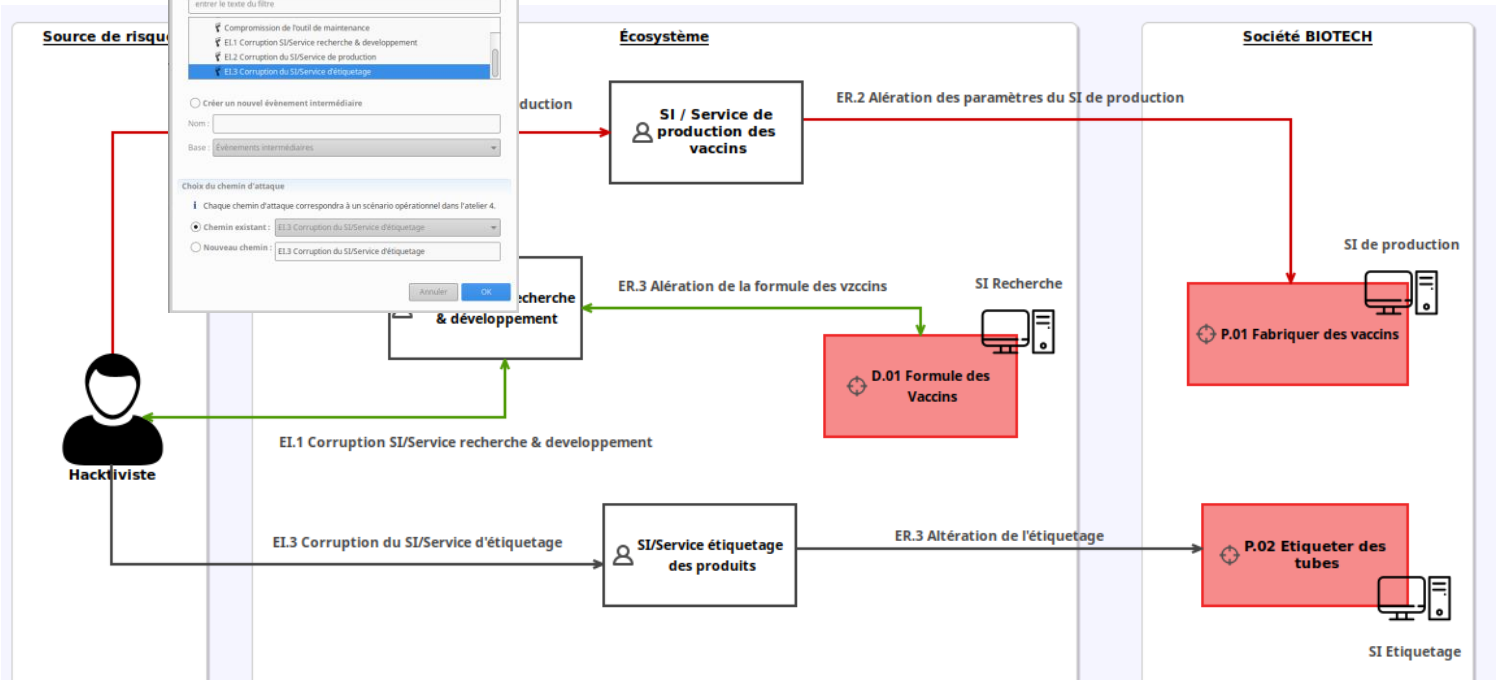
**Représentation « après mesure »:**
Apprécié sous réserve de la granularité et des seuils

**Définitions :**
Modification de la définition « pénétration » pour prendre en compte la notion d'accessibilité au BS et aux VM.

**Mesures de sécurité sur l'écosystème :**
Jusqu'à quel rang de partie prenante ?

# RETEX sur la méthode et le logiciel

## Atelier 3 : scénarios stratégiques




**Pré requis :** réflexion OV ⇔ VM / ER (cf. formation ANSSI)

**Nombreuses itérations :**
A/R entre ateliers 3 et 2: couverture / granularité

**Représentation des « BS » :**
Associés aux VM ou PP (cf. OV, ER et scénarios OPS)

**Mesures de sécurité :**
Répétition ateliers 1 & 3
socle de sécurité exigeant => peu/pas d'évolution

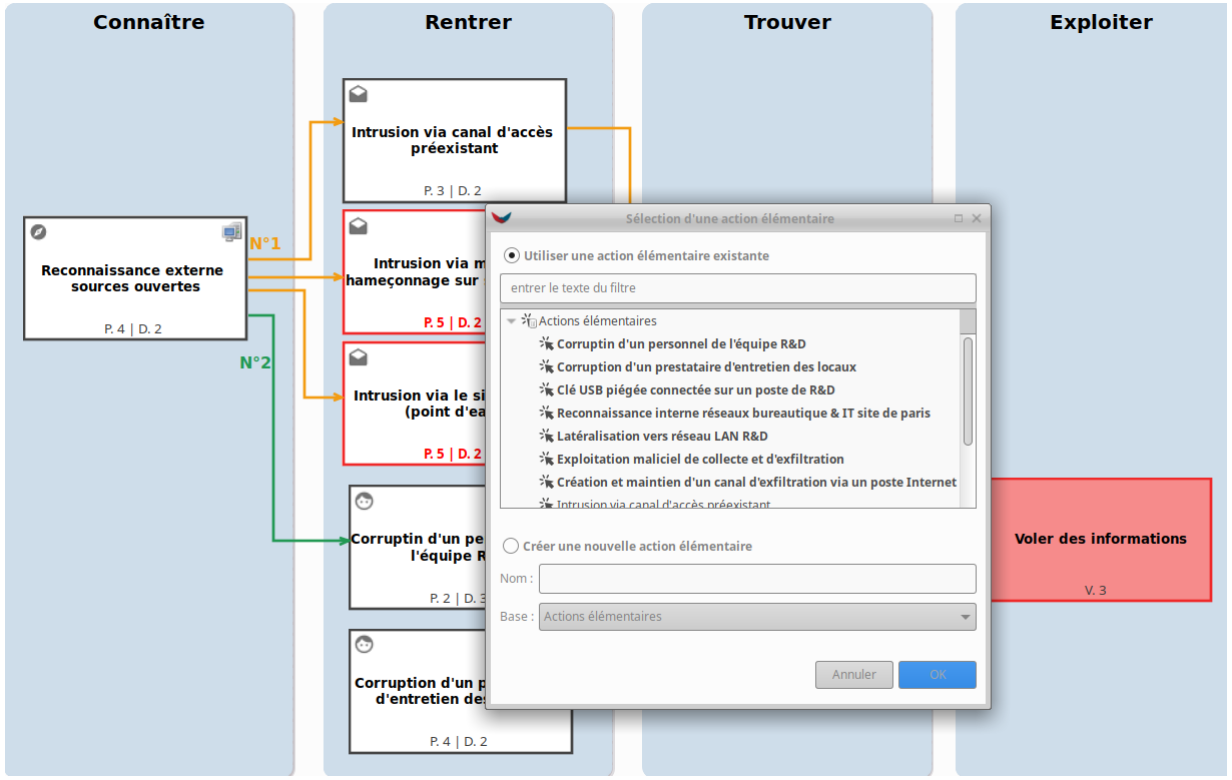
**Interface :** intuitive avec de nombreuses options de personnalisation

**Evolution prise en compte :** représentation des BS

**Amélioration :** personnalisation extrémités des flèches + possibilité d'ajouter une zone source de risques à droite

# RETEX sur la méthode et le logiciel

## Atelier 4 : modélisation/cotation des scénarios OPS « méthode avancée »




**Actions élémentaires :**
- granularité entre livret ANSSI et MITRE
- possibilité de zoom : sur certaines parties (PENTEST, …)

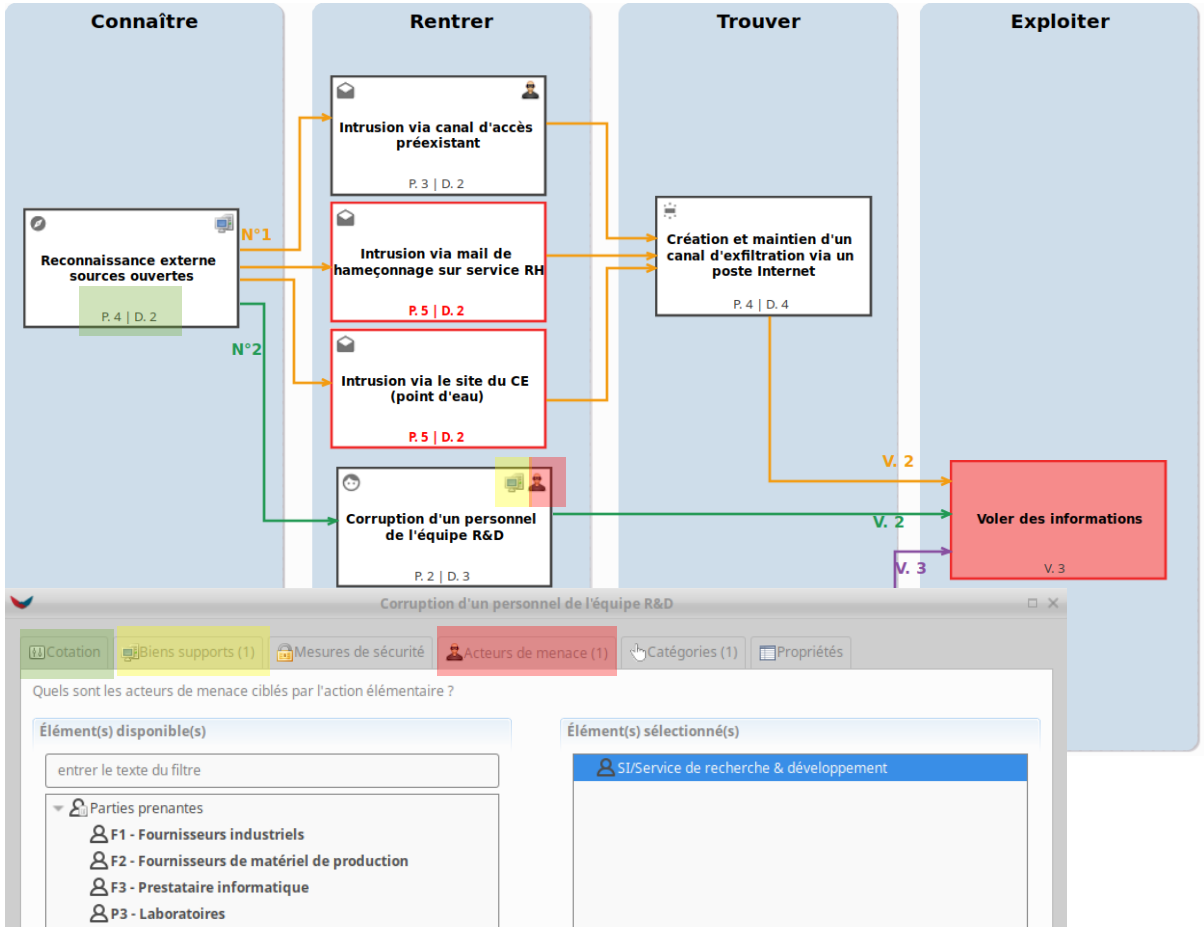
**Formulation :**
- différents niveaux de lecteur (cf. rapport final)
- personnalisée à l'étude : « rentrer » => Partie Prenante , « exploiter » => mention OS, …

**Lien OV, Valeur Métier et SI :**
- libellé de l'« action n-1 » fait mention de la ou les VM concernées

**Logiciel (rédacteur / relecteur):**
- indispensable pour réaliser ce type de schéma (ajout/modif.)
- système de fenêtre intuitive et possibilité de personnalisation
- système de suivi des versions : circuit « visa / relecture »

# RETEX sur la méthode et le logiciel

## Ateliers 4 / 5 : identification des mesures complémentaires




**Parcours des différents chemins**

Identifier pour chaque action élémentaire :

- biens supports
- parties prenantes

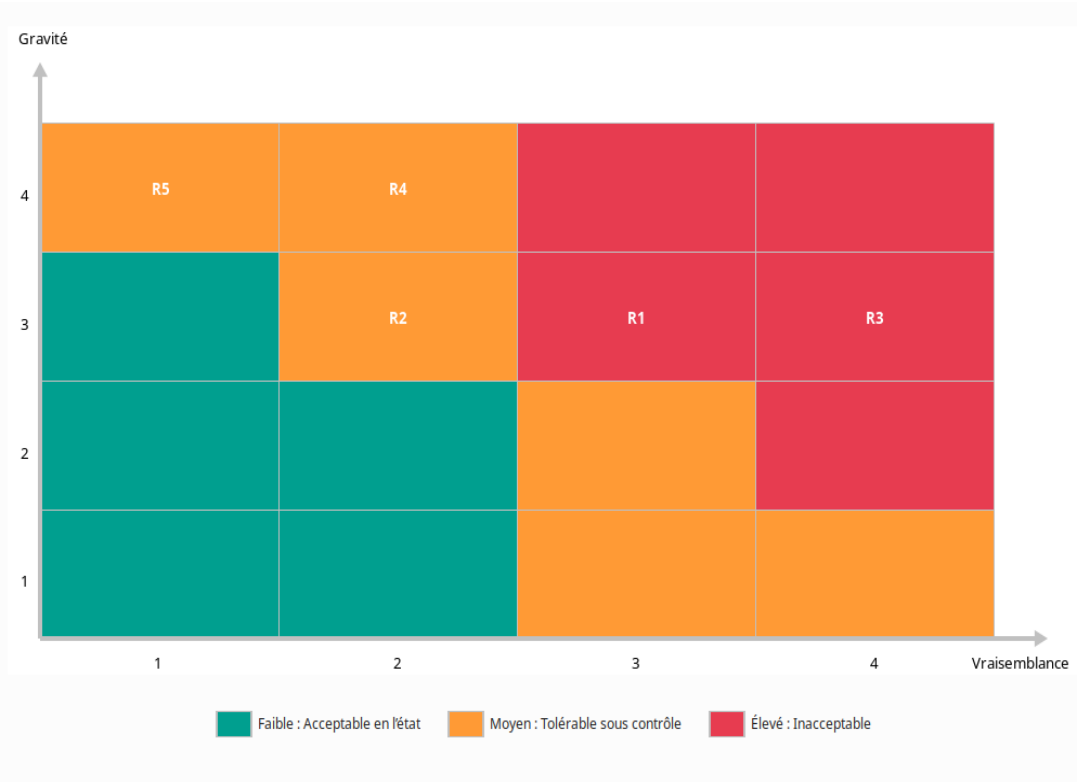
=> mesures de sécurité complémentaires

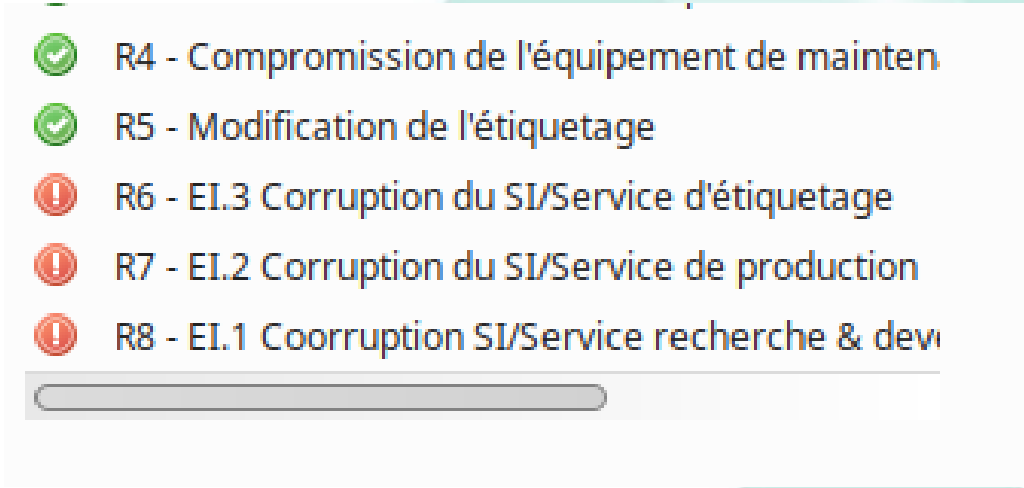
**Logiciel :**

- interface intuitive
- saisie double « entrée » (cf. ajout, correction, …)

# RETEX sur la méthode et le logiciel

## Atelier 5 : cartographie des risques




**Logiciel :**

- Affichage tronqué
- Rapport / export : point à améliorer

# RETEX sur la méthode et le logiciel

## Atelier 5 : Plan d'Amélioration Continue de la sécurité (PACS)

Plan d'amélioration continue de la sécurité

*Glisser des colonnes ici pour grouper les lignes*

| | Réf. | Référentiel | Mesure de sécurité | Type | Éléments associés | Scénarios de risque associés | Responsables | Freins et difficultés de mis |
|---|---|---|---|---|---|---|---|---|
| 1 | M1 | Référentiel de sécurité BIOTECH | Sensibilisation renforcée au hameçonnage par un prestataire spécialisé | Gouvernance | | R1 - Exfiltration de données via le SI de la R&D | RSSI | Validation du CHSCT indispensable |
| 2 | M2 | Référentiel de sécurité BIOTECH | Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI | Gouvernance | F3 - Prestataire informatique | R1 - Exfiltration de données via le SI de la R&D<br>R5 - Modification de l'étiquetage | RSSI | |

**Recensement :**

- Socle réglementaire adapté au projet (besoins de sécurité et technologie)
- Mesures complémentaires identifiées lors de l'analyse

**Couverture :**

- Éléments associés : PP, BS et VM
- Scénarios de risques

**Suivi de la mise en œuvre :**

- Freins, et coût des mesures
- Priorisation des mesures, ….

**Logiciel :**

- Interface intuitive et couvre tous les besoins
- Rapport global : deux exports / tableaux

# RETEX sur la méthode et le logiciel

## Atelier 5 : Plan d'Amélioration Continue de la sécurité (PACS)

Plan d'amélioration continue de la sécurité - Matrice

| Scénarios de risque \ Mesures de sécurité | | Référentiel de sécurité BIOTECH | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | M1 - Sensibilisation renforcée au hameçonnage par un prestataire spécialisé | M2 - Audit de sécurité technique et organisation... de l'ensemble du SI bureautique par un PASSI | M3 - Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires | M4 - Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire | M5 - Audit de sécurité organisation... des prestataires et laboratories clés. Mise en place et suivi des plans d'action consécutifs | M6 - Limitation des données transmises aux laboratoires au juste besoin | M7 - Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonneme... | |
| Voler des informations | R2 - Exfiltration de données via le SI du laboratoire | | | ✔ | ✔ | ✔ | ✔ | | |
| | R3 - Exfiltration de données via le prestataire de maintenance informatique | | | ✔ | ✔ | ✔ | | ⛔ | |
| | R1 - Exfiltration de données via le SI de la R&D | ✔ | ✔ | | | | | 🔄 | |
| Saboter la campagne nationale de vaccination | R4 - Compromission de l'équipement de maintenance | | | ✔ | ✔ | ✔ | | | |
| | R5 - Modification de l'étiquetage | | ✔ | | | | | | |
| | R6 - EI.3 Corruption du SI/Service d'étiquetage | | | | | | | | |
| | R7 - EI.2 Corruption du SI/Service de production | | | | | | | | |

**Vue couverture**

- vue globale synthétique appréciée

**Logiciel :**

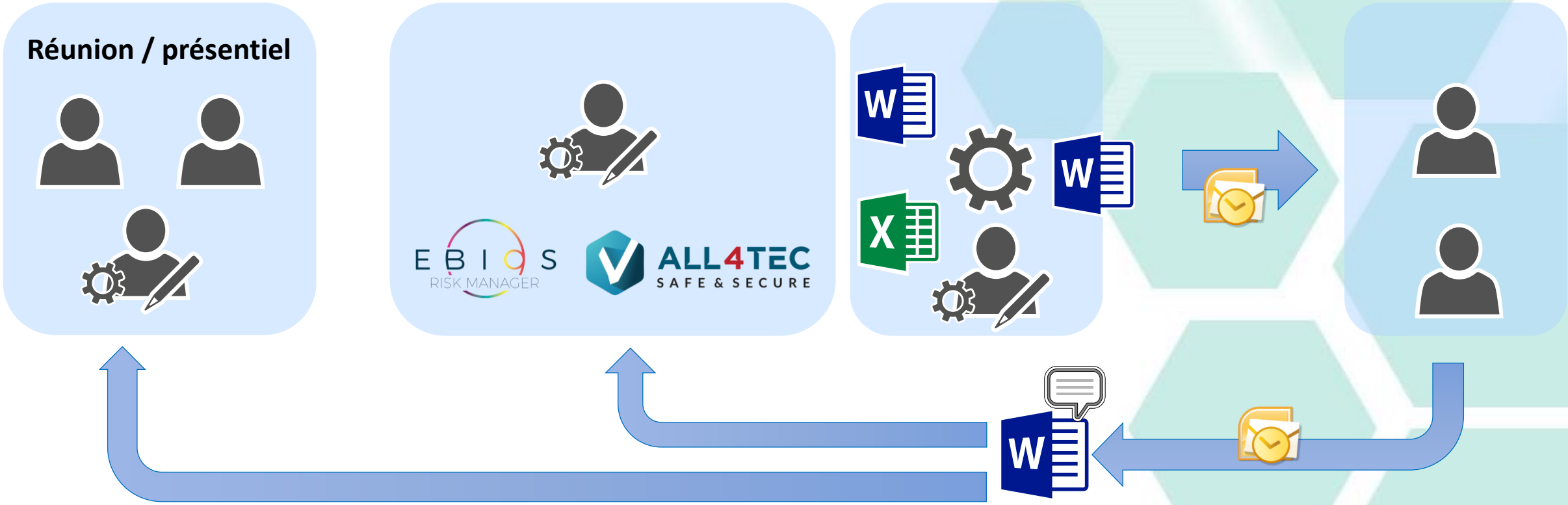
- automatisation 🙂

*Axes d'amélioration :*

- inverser colonnes et lignes : rapport final
- icones « état d'application » :
  - en cours ⛔
  - non appliqué 🔄

# RETEX sur la méthode et le logiciel

## Rapport global/final



# Conclusion

## Axes de travail

- Méthode :
  - socle de sécurité
  - scénarios opérationnels
  - travail collaboratif et itérations
  - FEROS et APRI
  - 02 équipes (ateliers 1&5 vs ateliers 2,3&4)
- Logiciel
  - Rapport Word / Modèle : version 2.3.0
  - Pratique relecture et suivi des versions

## Perspectives

vers une utilisation du logiciel pour d'autres activités et livrables ?

- homologation : export des schémas (cartographie de la menace numérique, scénarios, cartographie des risques)
- audit : compte rendu, préparation test d'intrusion

# Merci pour votre attention

CLUBEBIOS

CLUBEBIOS

Site : https://club-ebios.org
Twitter : @club_ebios
LinkedIn : https://fr.linkedin.com/company/club-ebios