

**RESEARCH & TECHNOLOGY**

Campus Polytechnique

1, avenue Augustin Fresnel

91767 Palaiseau cedex France

Tel : +33 (0)1 69 41 55 00

Fax : +33 (0)1 69 41 59 69

[www.thalesgroup.com](http://www.thalesgroup.com)

## RAPPORT / DOCUMENT TECHNIQUE

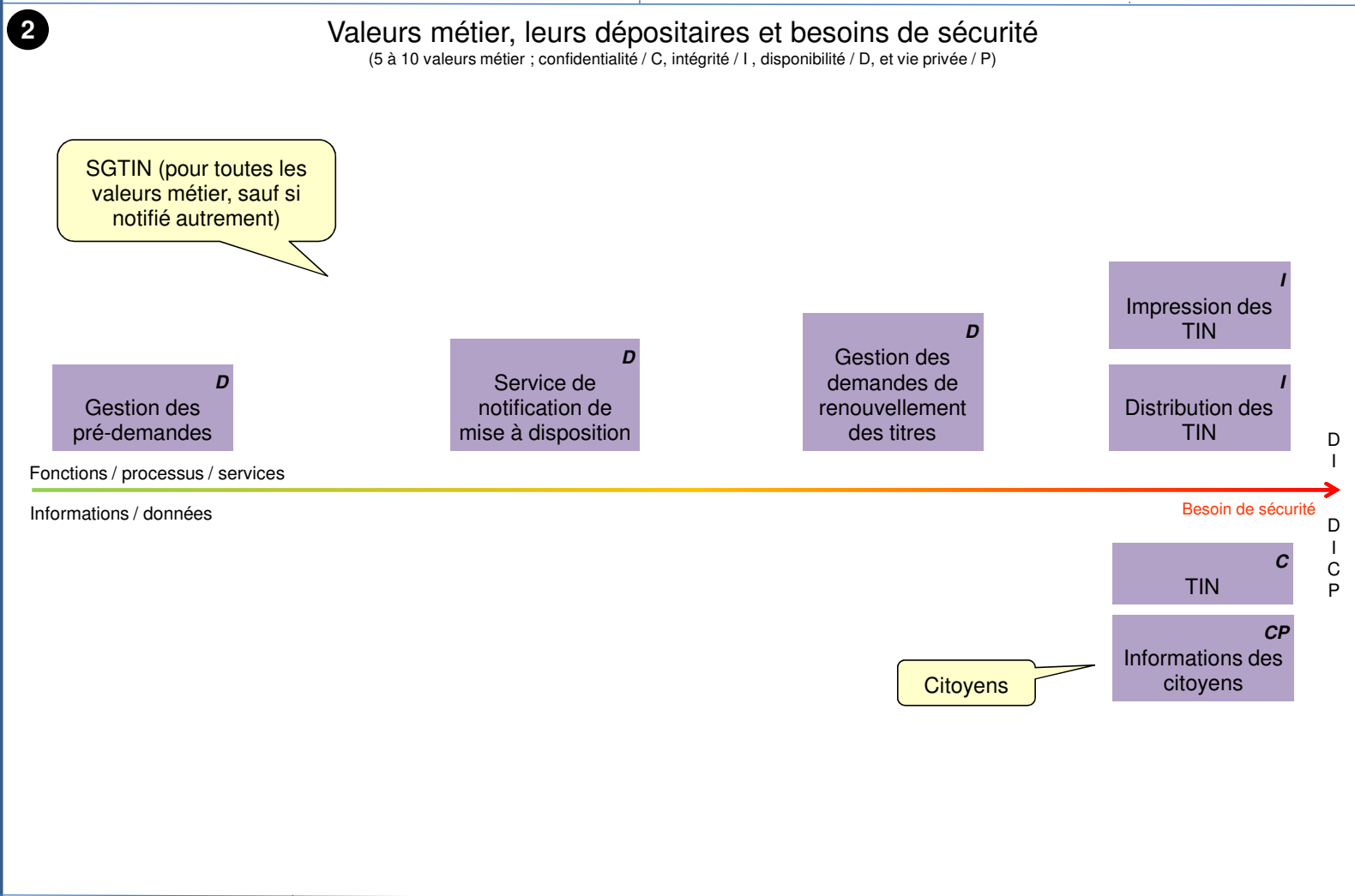
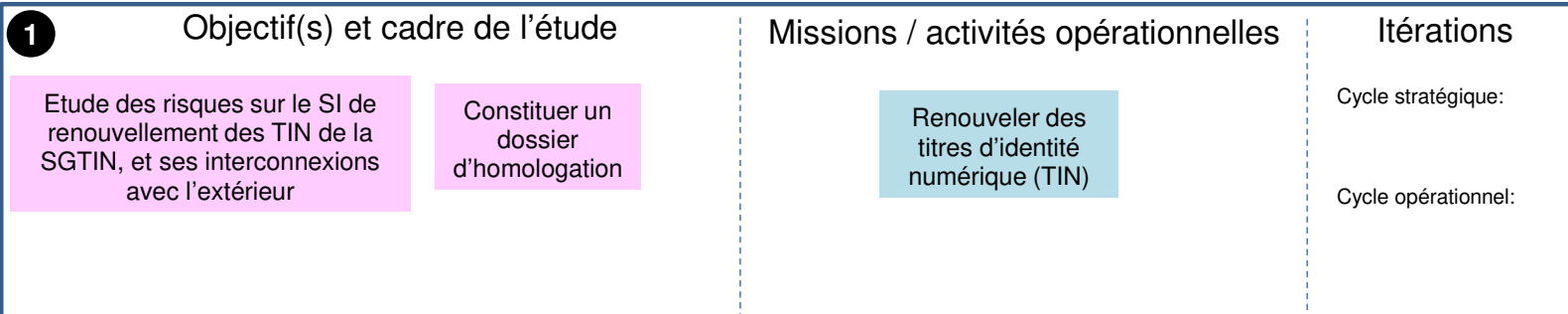
# RENOUVELLEMENT D'UN TITRE D'IDENTITÉ NUMÉRIQUE

## RAPPORT D'ANALYSE DE RISQUES DE CYBERSÉCURITÉ

FORMATEUR EBIOS - RISK MANAGER: STÉPHANE PAUL

NOMS DES STAGIAIRES: XXX, YYY, ZZZ

	- le :	A le :	B le :	C le :	D le :
Etabli par Signature					
Approuvé par Signature					



- ### 3
- Normes, standards:
- ANSSI hygiène de base
  - ANSSI PSSIE
  - CIS Controls
  - ISA/IEC 62443-3-3
  - ISO 27002
  - NIST SP800-53
  - EUROCAE ED-202A
  - Référentiel Général de Sécurité

### Référentiels de sécurité

(i.e., normes applicables, éventuellement avec limitations)

Autres sources:

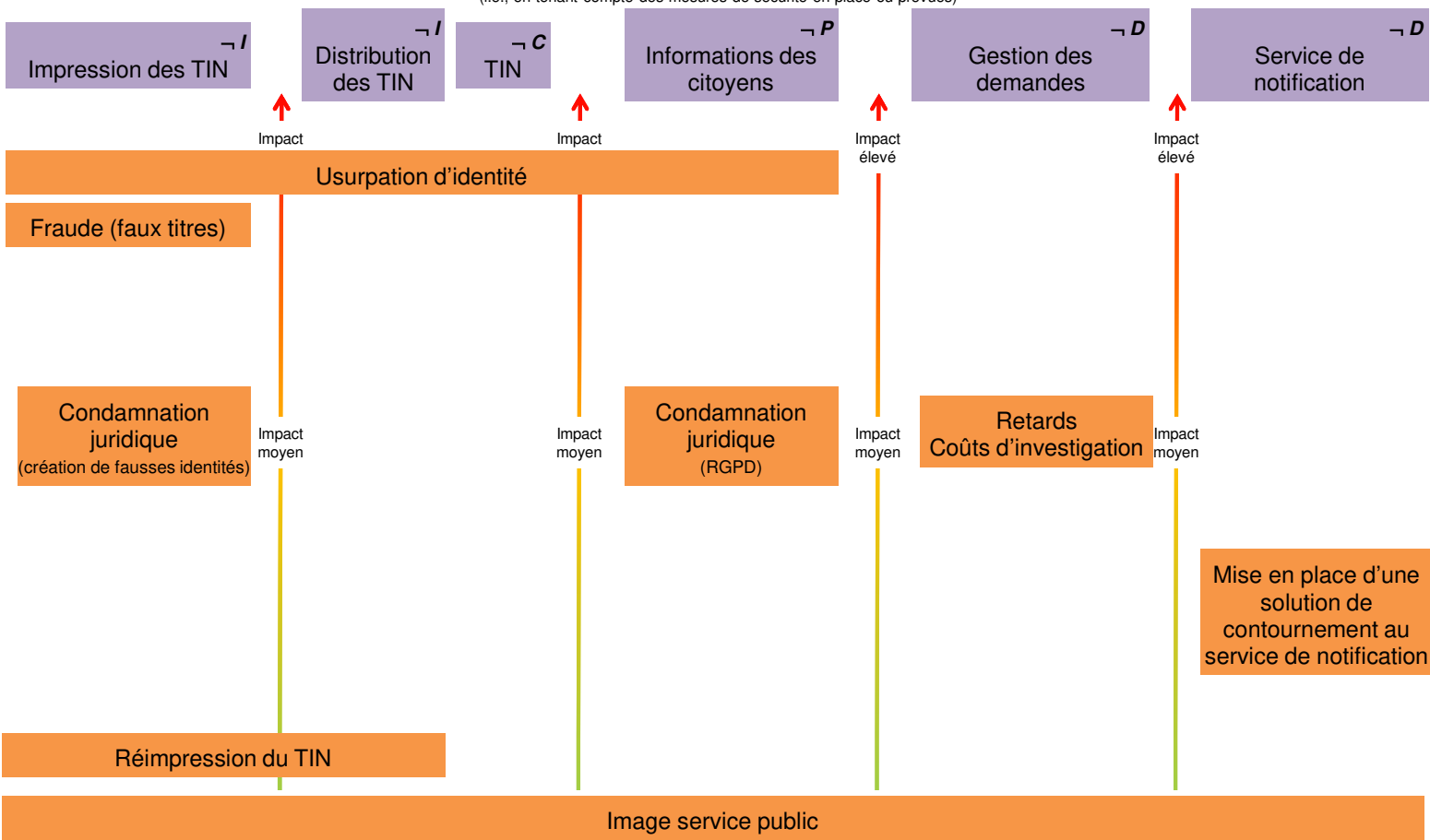
{OPEN}

- ### Abréviations
- **Autorité Nationale de Gestion des TIN**
  - **Réseau Interministériel de l'État**
  - **Société de Gestion des Titres d'Identité Numérique**
  - **Titres d'Identité Numérique**

## Evénements redoutés, impacts et sévérité

(i.e., en tenant compte des mesures de sécurité en place ou prévues)

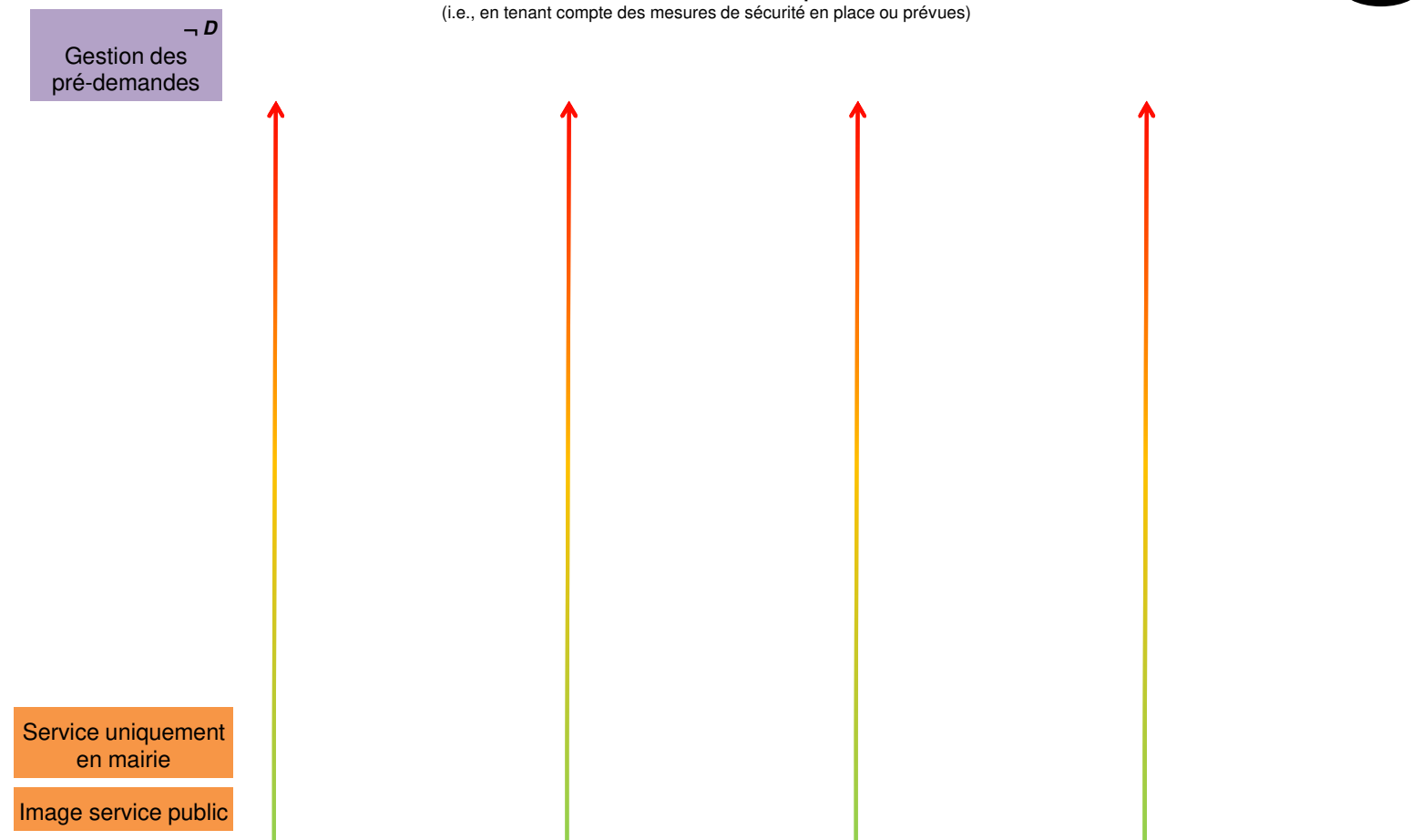
2a



## Evénements redoutés & impact/sévérité

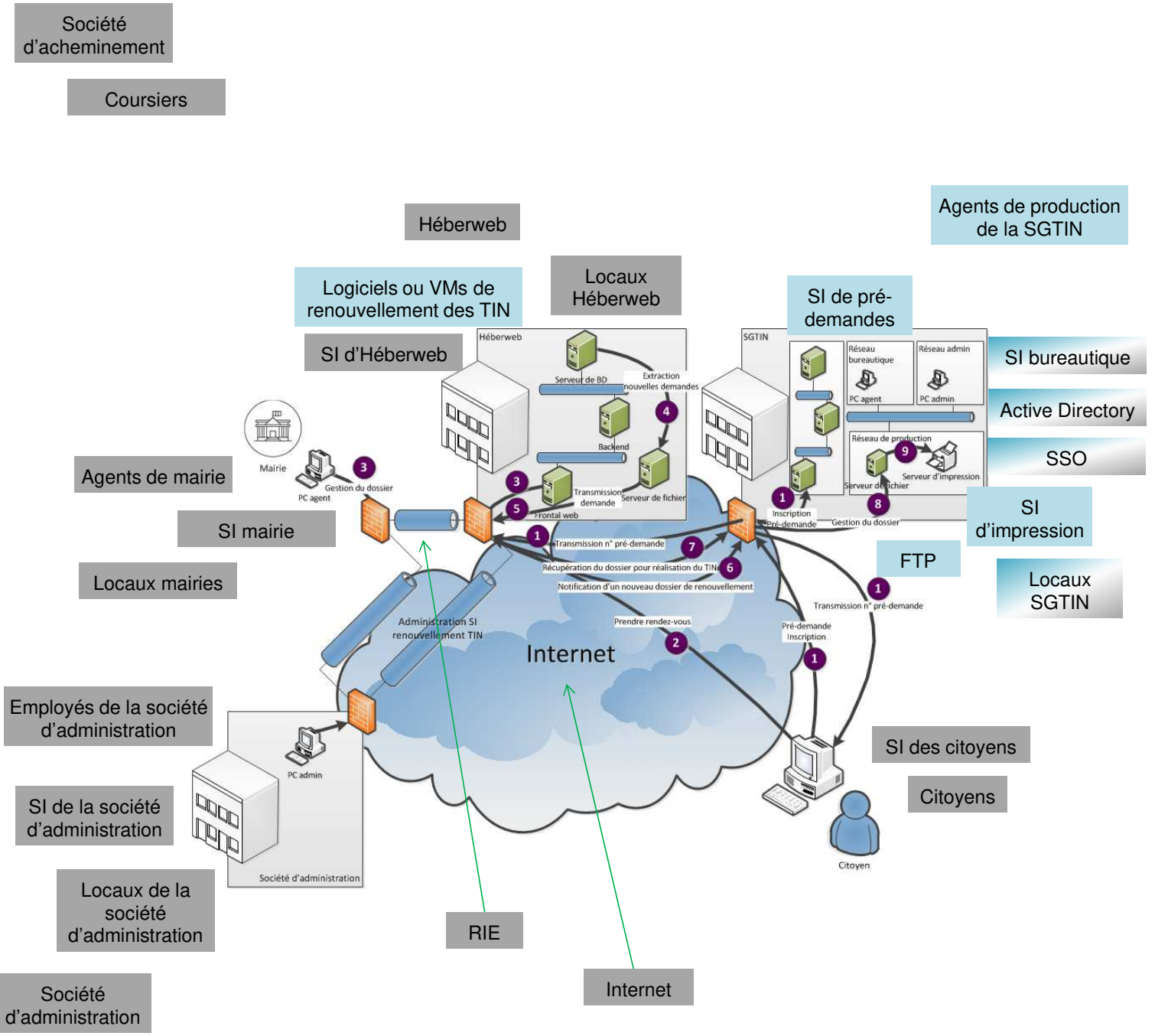
(i.e., en tenant compte des mesures de sécurité en place ou prévues)

2b



4

## Principaux biens support



5

## Analyse de conformité

(penser à exploiter les fragilités recensées dans les scénarios de l'atelier 4)



Validation des données en entrée  
(en provenance d'HerberWeb)

Communication WAN sécurisée

Contrôle d'accès strict au répertoire propre à l'activité de renouvellement des TIN

Non implémentée

Non implémentée

Gestion des incidents (audits)

Partitionnement des activités de renouvellement des TIN et des autres activités

Partiellement implémentée

Partiellement implémentée

Authentification via SSO et AD

Partitionnement en 3 couches

Pare-feu

Segmentation réseaux (pré-demandes, impression)

Complètement implémentée

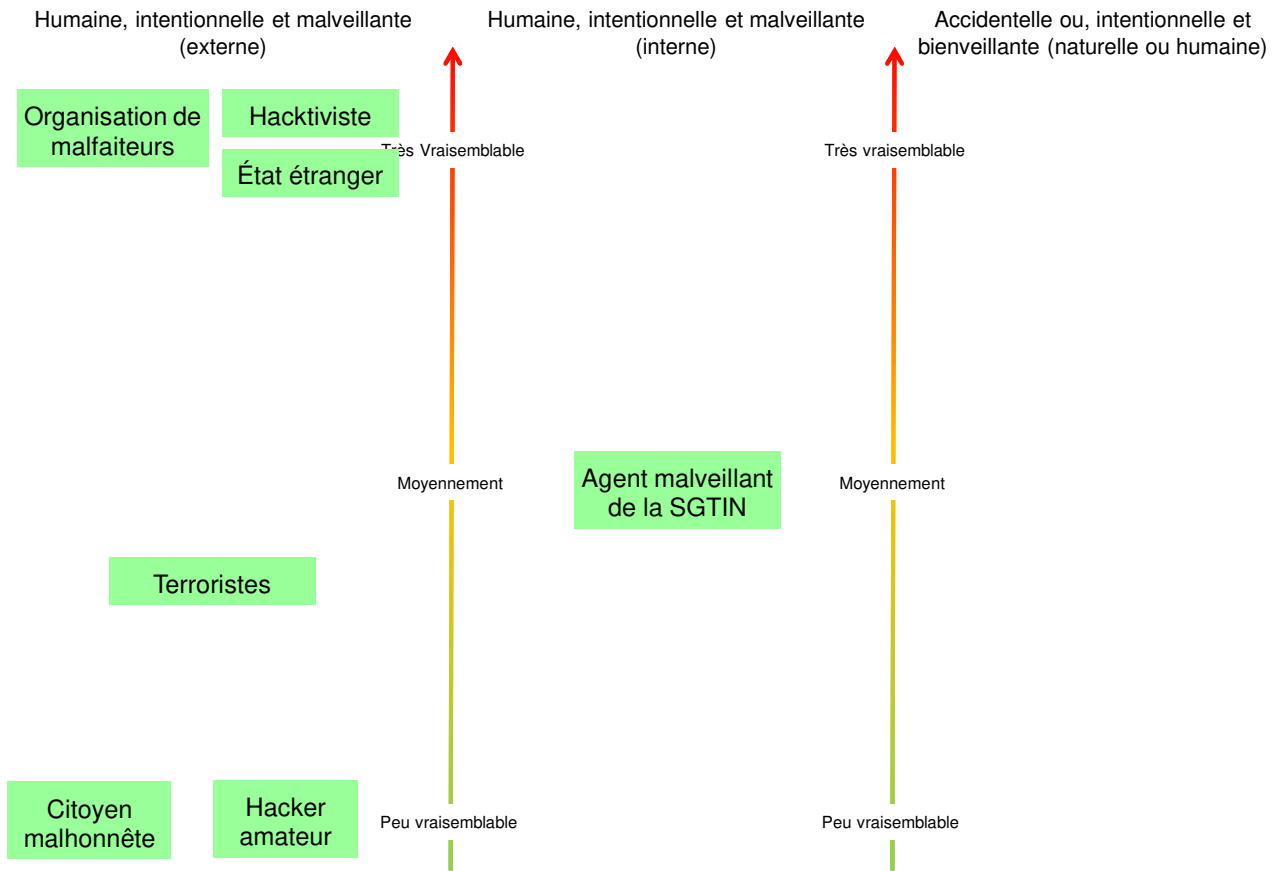
Complètement implémentée

## SR exclus

### Source de risque, suivant la vraisemblance de passage à l'acte

(considérer motivation, privilèges, chemins d'attaques plus faciles, variété des type de sources...; ≠ succès d'attaque)

1

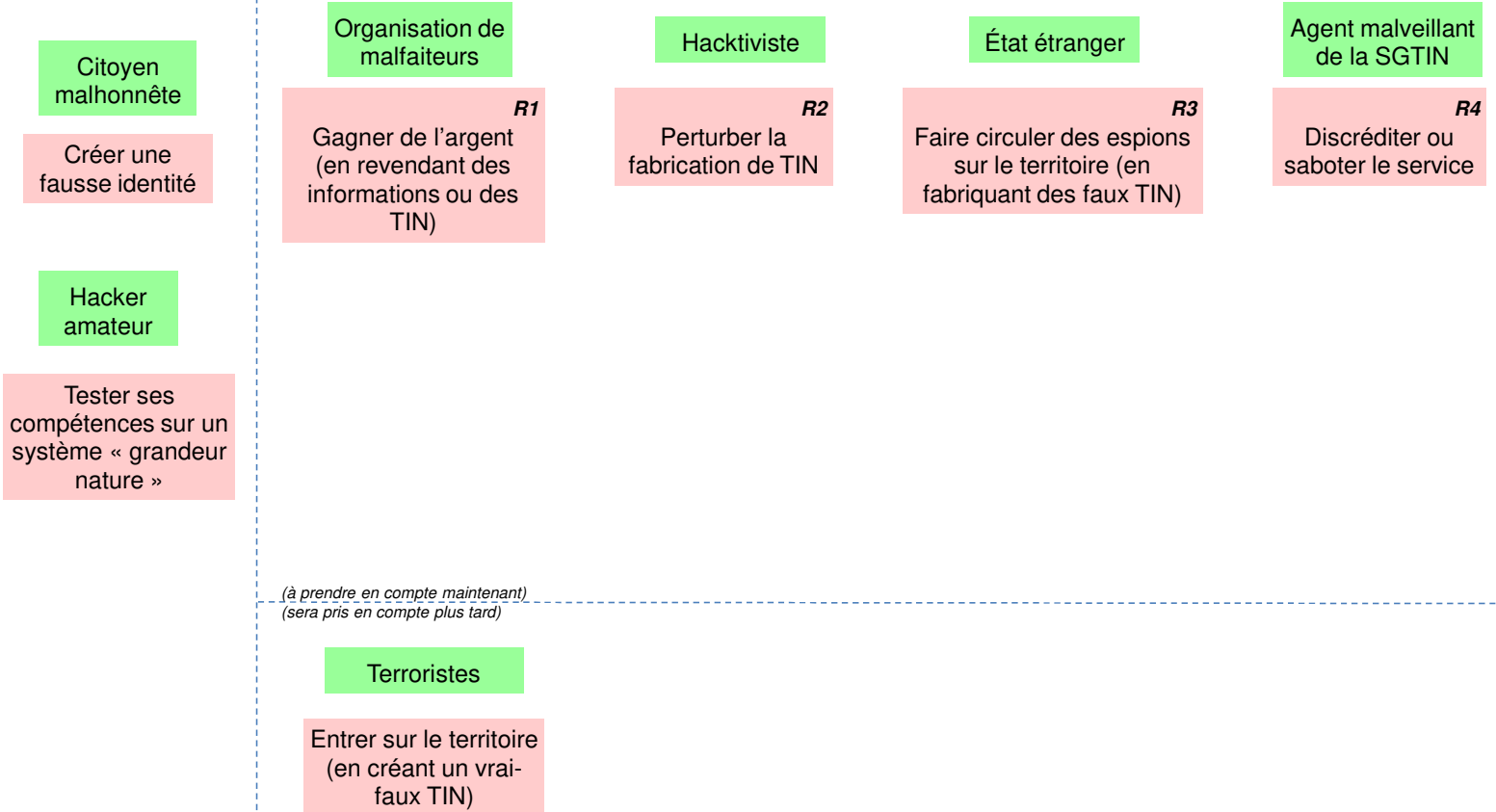


## Couples {SR, OV} exclus

### Couples {Source Risque, Objectifs Visés} retenus

(i.e., en tenant compte des mesures de sécurité existantes et des besoins de sécurité)

2

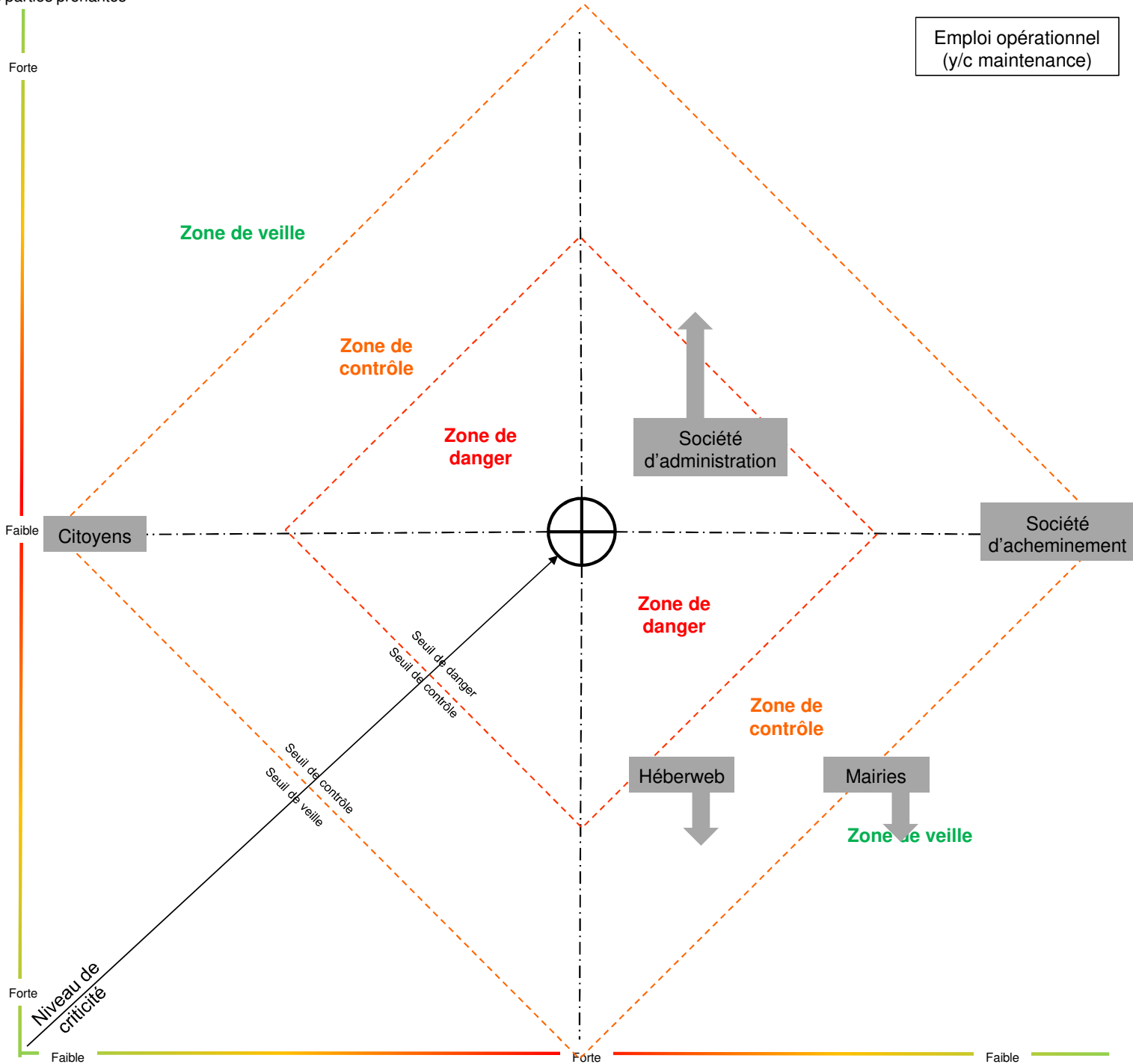


1

## Cartographie de la dangerosité de l'écosystème

(i.e., dépendance vis-à-vis des parties prenantes sous-traitants, maturité des sous-traitants...)

Emploi opérationnel  
(y/c maintenance)



Exposition du système  
aux parties prenantes

3

## Mesures de sécurité à appliquer sur l'écosystème

(les flèches grises indiquent l'évolution de la criticité des parties prenantes après applications des mesures)

Sources:

- ANSSI hygiène de base (standard)
- ANSSI hygiène de base (renforcé)
- ANSSI PSSIE
- CIS Controls
- ISA/IEC 62443-3-3 (SL1)
- ISA/IEC 62443-3-3 (SL2)
- ISA/IEC 62443-3-3 (SL3)
- ISA/IEC 62443-3-3 (SL4)
- ISO 27002
- NIST SP800-53 (low)
- NIST SP800-53 (moderate)
- NIST SP800-53 (high)

Il est proposé de mettre en œuvre sur la Société d'Administration, la Mairie et Héberweb toutes les mesures non implémentées relevées lors de l'audit (cf. planche 5)

3a

## Mesures de sécurité existantes de l'écosystème

### Héberweb

Contrôle d'accès strict aux zones d'hébergement

Cahier d'émargement visiteurs

MCS équipements de sûreté environnementale (refroidissement, protection incendie, protection électrique)

MCS équipements du SI (parc homogène et à jour)

Pare-feu

ISO 27001:2013

Partitionnement en 3 couches

### Société d'administration

HTTPS

SSL v3.0

ISO 9001:2015

Authentification SSH simple par mot de passe

Pare-feu

*Pas clair*

↓  
Sécurisation de la télé-administration (TeamViewer)

### Mairies

Charte informatique

Pare-feu

### Société d'acheminement

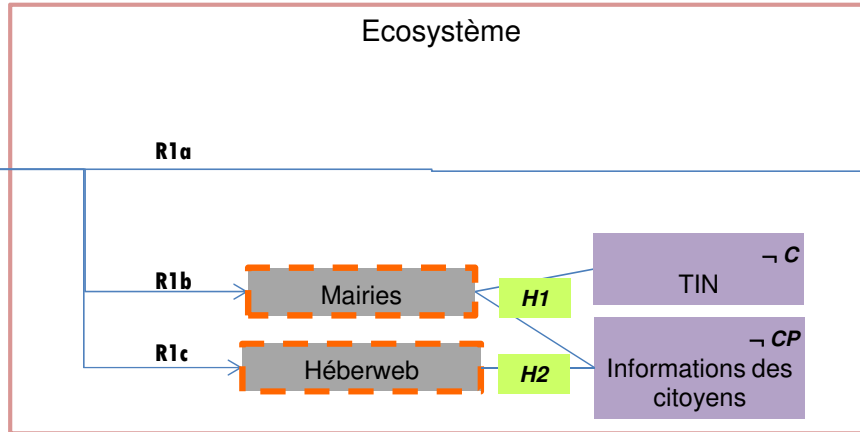
### Citoyens

Sévérité: Critique

{Source de risque ;  
Objectif visé}

Organisation de  
malfaiteurs

**R1**  
Gagner de l'argent  
(en revendant des  
informations ou des  
TIN)



Système

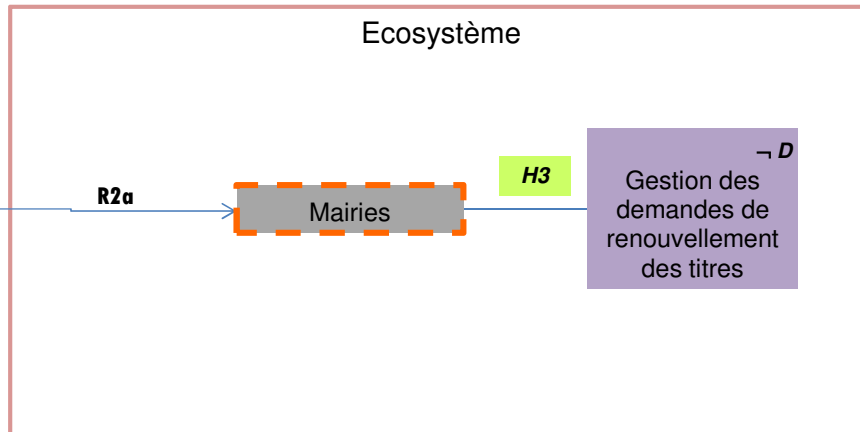
Informations des  
citoyens <sup>CP</sup>

Sévérité: Important

{SR ; OV}

Hacktiviste

**R2**  
Perturber la  
fabrication de TIN



Système

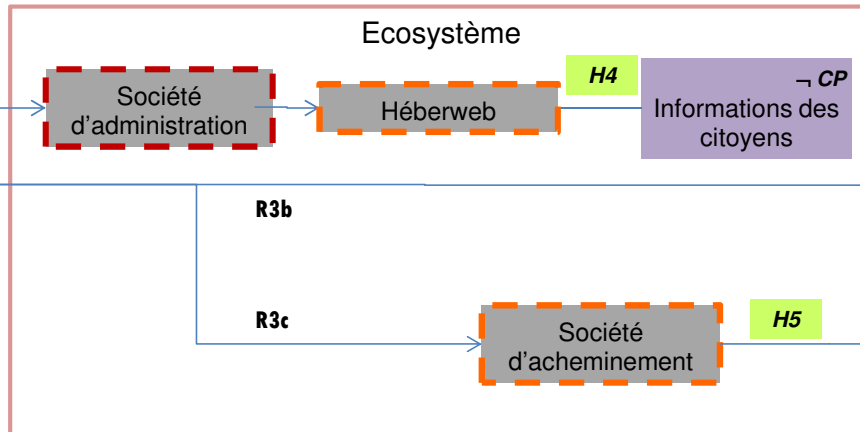
Gestion des  
demandes de  
renouvellement  
des titres <sup>D</sup>

Sévérité: Critique

{SR ; OV}

État étranger

**R3**  
Faire circuler des espions  
sur le territoire (en  
fabriquant des faux TIN)



Système

Impression des  
TIN <sup>I</sup>

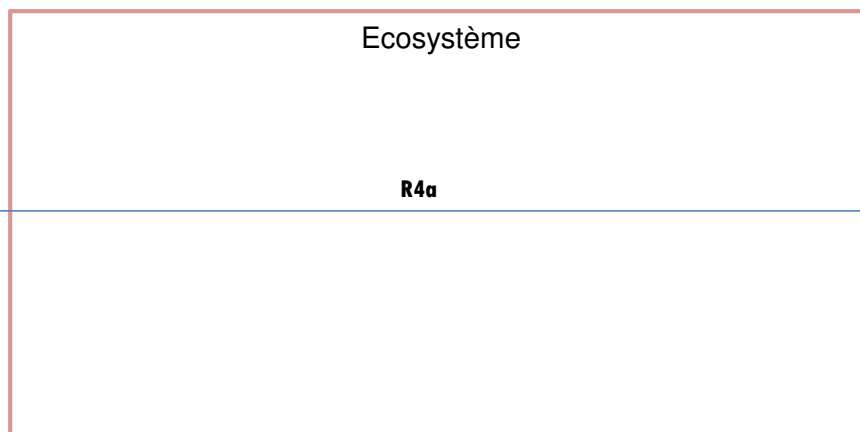
Distribution des  
TIN <sup>I</sup>

Sévérité: Mineur

{SR ; OV}

Agent malveillant  
de la SGTIN

**R4**  
Discréditer ou  
saboter le service

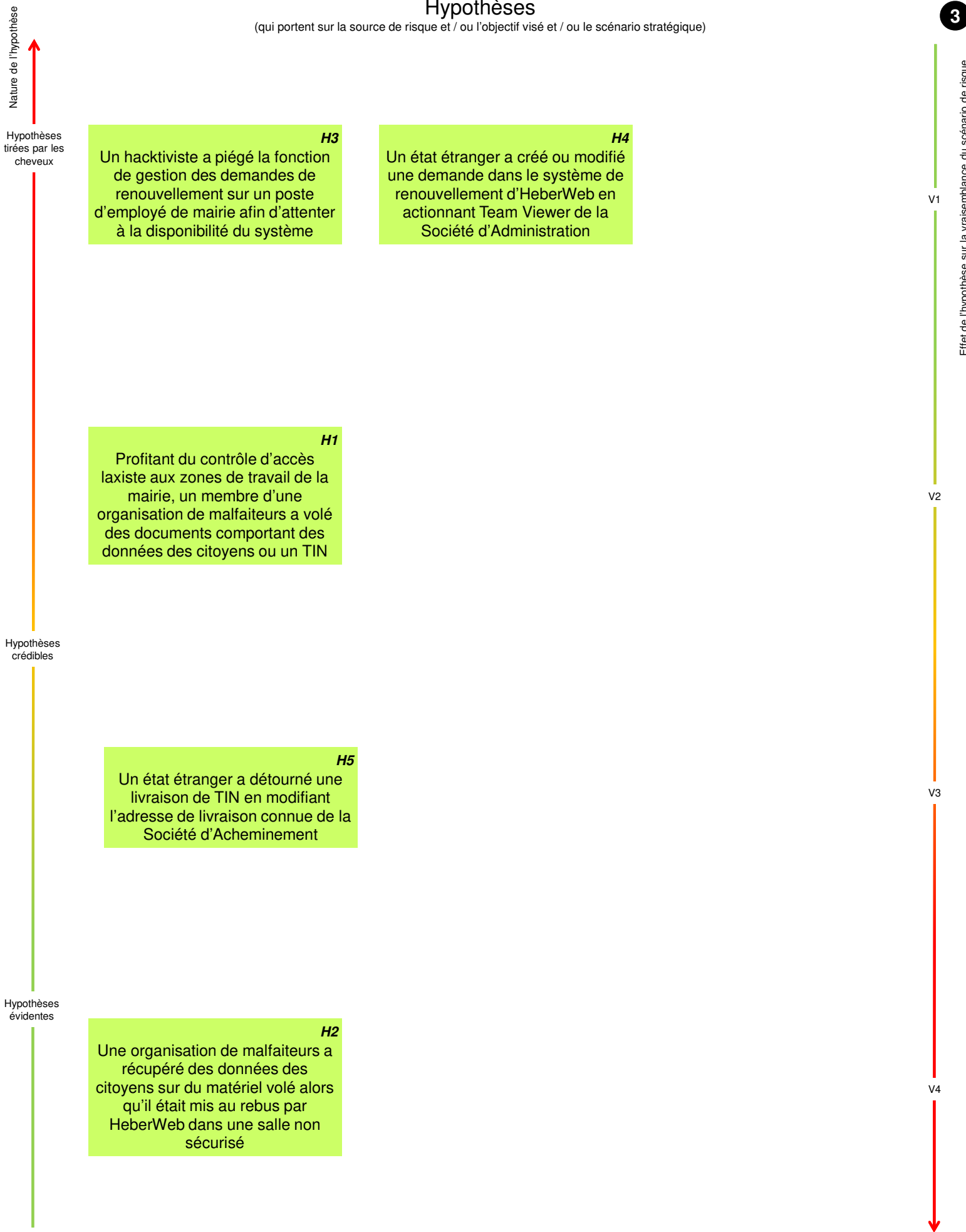


Système

Gestion des  
pré-demandes <sup>D</sup>

## Hypothèses

(qui portent sur la source de risque et / ou l'objectif visé et / ou le scénario stratégique)



3a

Héberweb

H2

Gestion de l'acquisition, de la maintenance et de la fin de vie des équipements informatiques

Local de stockage sécurisé

Procédure de renvoi au fournisseur (dont effacement sécurisé)

Société d'administration

H4

Partitionnement des réseaux bureautique et d'administration du SI

MCS équipements du SI (parc homogène et à jour)

NetBIOS et SMB correctement configurés (ports 137, 139 et 445)

Politique de mots de passe forts et tentatives limitées (pour agents de mairies)

Mairies

H1

Contrôle d'accès strict aux zones de travail

H3

Principe de moindre privilège (l'agent n'est pas administrateur de son poste)

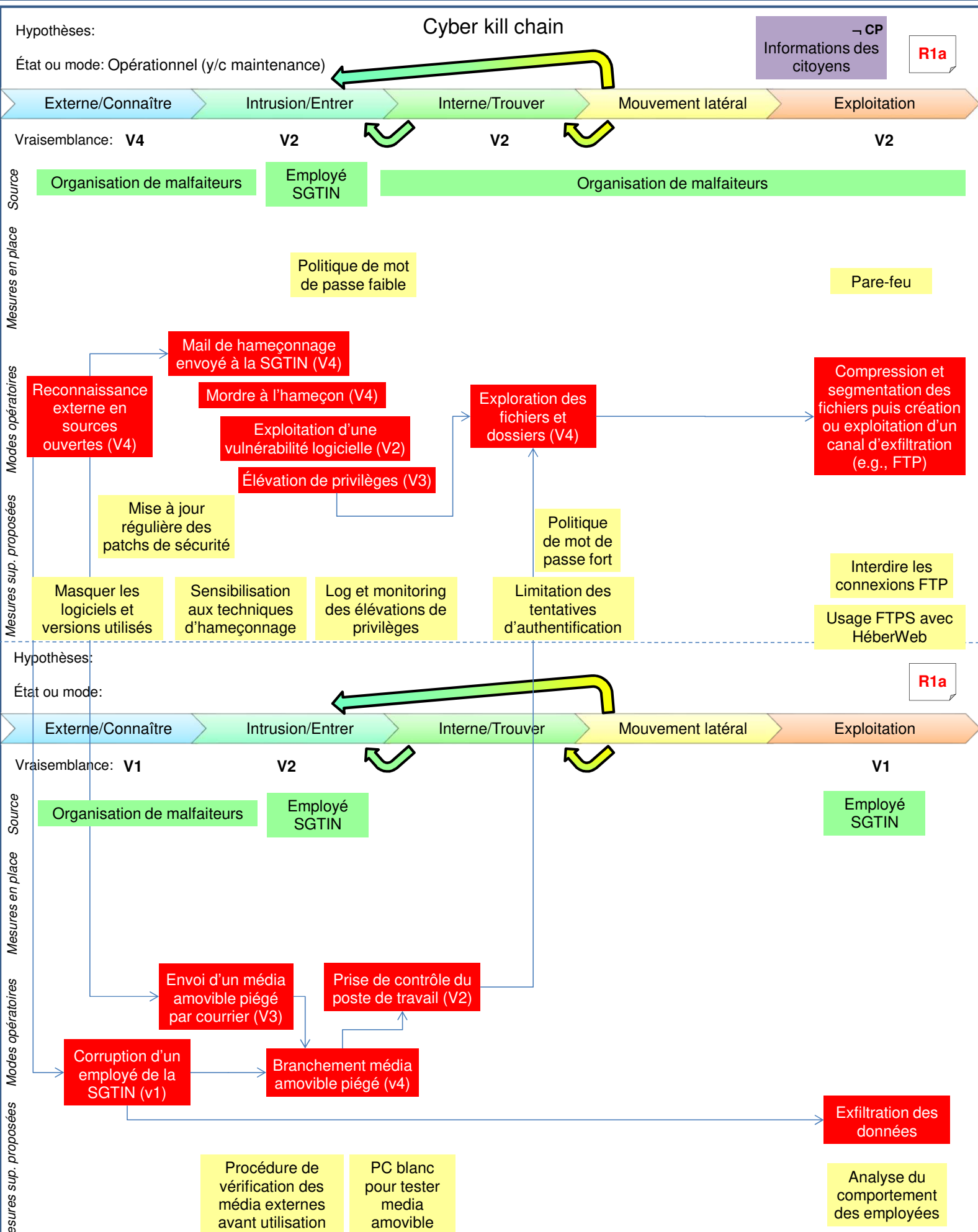
Partitionnement des réseaux bureautique et de renouvellement des TIN

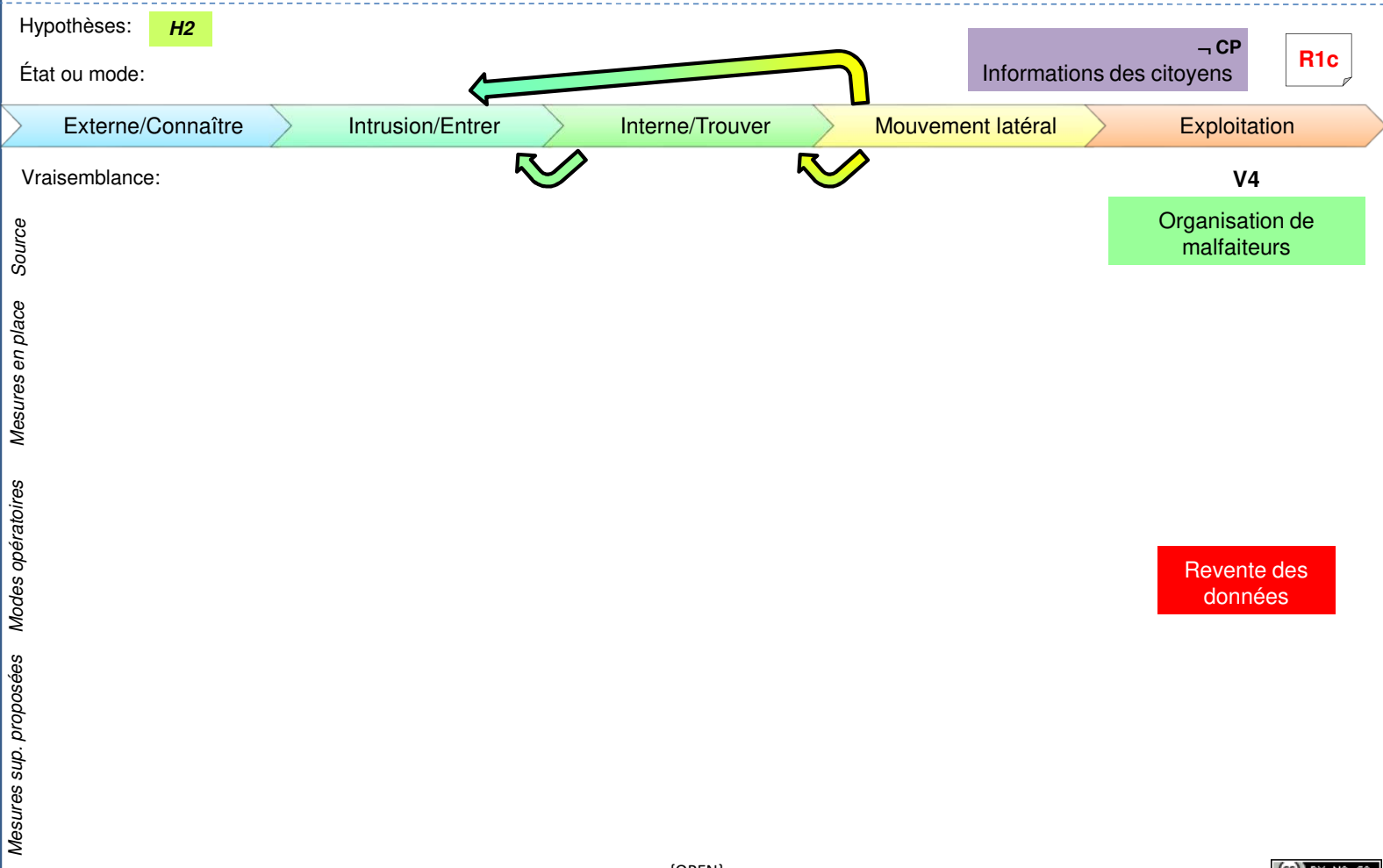
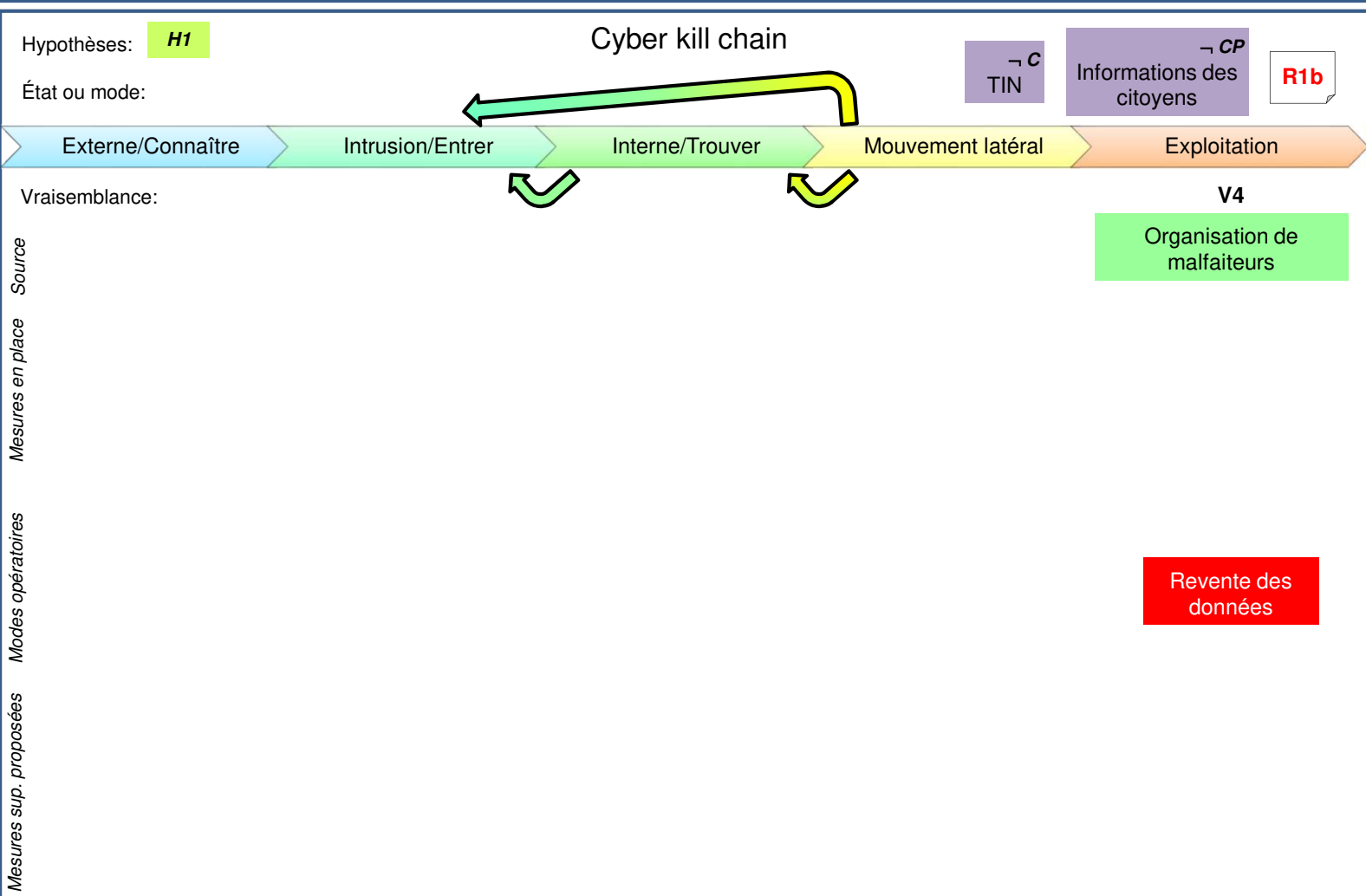
Chiffrement des données

Société d'acheminement

H5

Citoyens





## Liste des scénarios de risque

(inclure la source de risque, la valeur métier, l'événement redouté, les impacts, la sévérité, les biens supports critiques, les vulnérabilités exploitées, la vraisemblance)

N°	Description du scenario de risque	Responsable	Commentaires
R1a	Il est vraisemblable (V2) que, pour faire de l'argent, une organisation de malfaiteurs vole des données des citoyens à la SGTIN, par hameçonnage, envoi d'une clé piégée et/ou corruption de personnel, et les revend, permettant une usurpation critique d'identité (G4).	SGTIN	
R1b	Il est peu vraisemblable (V2) que, profitant du contrôle d'accès laxiste aux zones de travail de la mairie, un membre d'une organisation de malfaiteurs vole des documents comportant des données des citoyens ou des TIN et les revende pour faire de l'argent, permettant une usurpation critique d'identité (G4).	SGTIN	
R1c	Il est certain (V4) qu'une organisation de malfaiteurs puisse récupérer des données des citoyens sur du matériel volé alors qu'il était mis au rebus par HeberWeb dans une salle non sécurisé, et les revende pour faire de l'argent, permettant une usurpation critique d'identité (G4).	SGTIN	
R2a	Un hacktiviste piège la fonction de gestion des demandes de renouvellement sur un poste d'employé de mairie, afin d'attenter à la disponibilité du système.	SGTIN	
R3a	Un état étranger crée ou modifie une demande dans le système de renouvellement (HeberWeb) en actionnant Team Viewer (Société d'Administration) pour usurper une identité.	SGTIN	
R3b	Un état étranger fait imprimer de vrai-faux TIN en corrompant un utilisateur de SGTIN pour usurper une identité.	SGTIN	
R3c	Un état étranger détourne une livraison de TIN pour usurper une identité.	SGTIN	
R4a	Un agent malveillant SGTIN perturbe la disponibilité du SI SGTIN, grâce à ses droits d'accès, pour nuire à la réputation de la SGTIN.	SGTIN	

## Echelles de risque

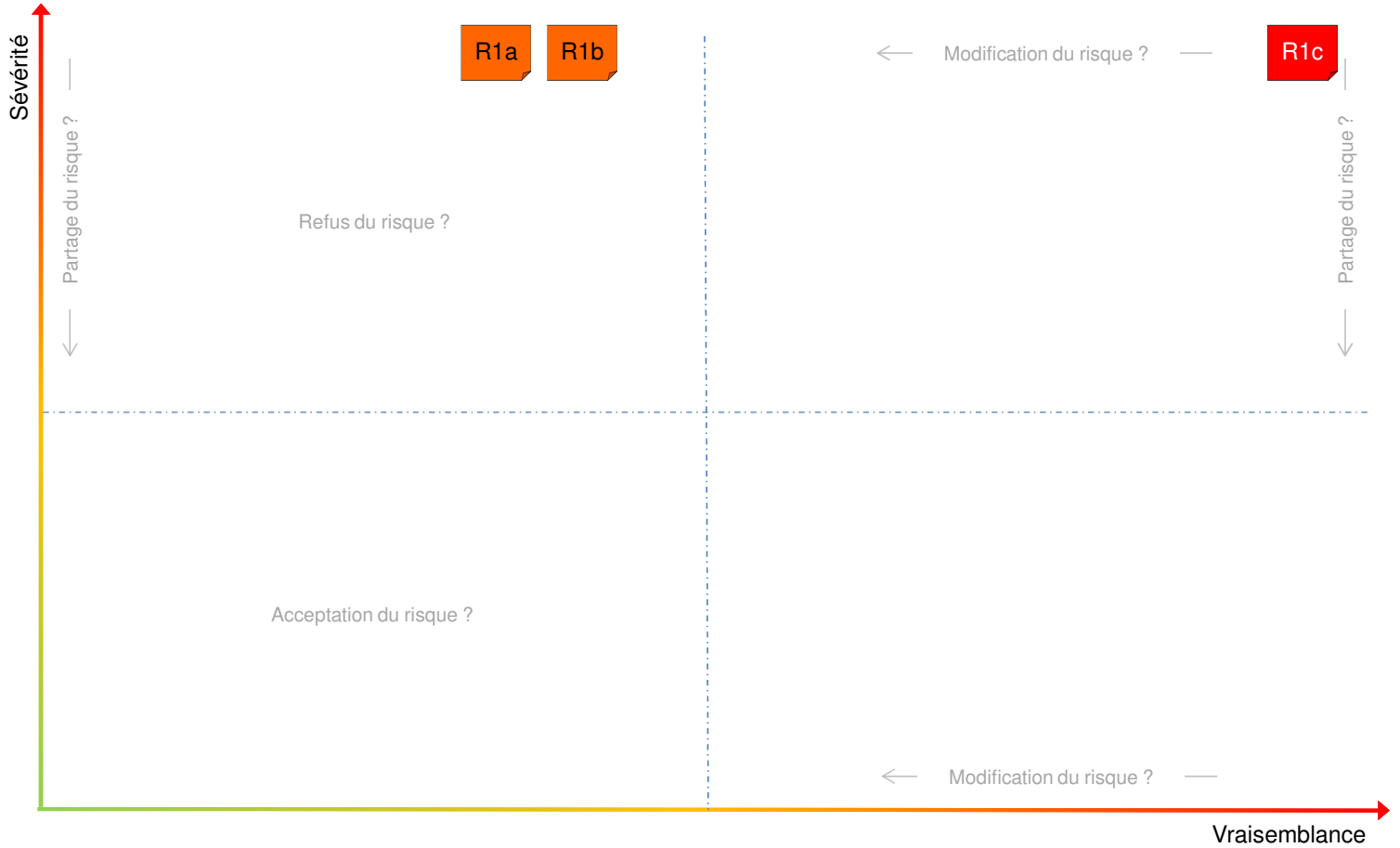
Sévérité / Gravité
G1 • Mineur
G2 • Significatif
G3 • Important
G4 • Critique

Vraisemblance
V1 • Peu vraisemblable
V2 • Vraisemblable
V3 • Très vraisemblable
V4 • Certain ou déjà produit

Niveau de risque	Acceptabilité du risque
Faible	Acceptable en l'état
Moyen	Tolérable sous contrôle
Elevé	Inacceptable

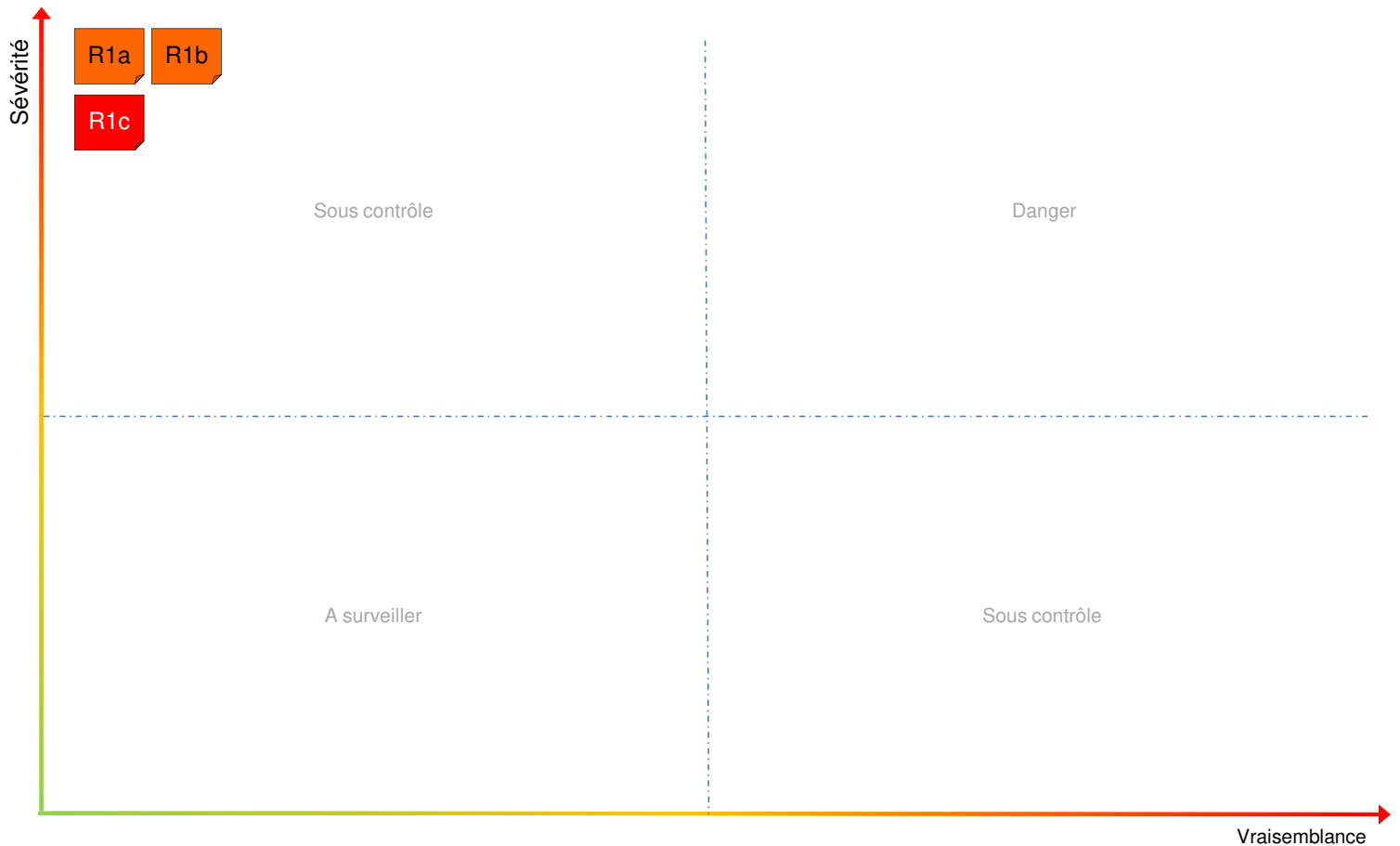
## Synthèses des risques initiaux

1



## Risques résiduels

3



## Objectifs de sécurité

(i.e., options de traitement de l'ISO 27005)

Risque accepté :

Risque modifié :

Risque refusé :

Risque partagé :

R1a

Masquer les logiciels et versions utilisés

Mise à jour régulière des patches de sécurité

Sensibilisation aux techniques d'hameçonnage

Log et monitoring des élévations de privilèges

Limitation des tentatives d'authentification

Politique de mot de passe fort

Station blanche pour tester le contenu des clefs USB avant connexion au SI

R1b

Contrôle d'accès strict aux zones de travail

R1c

Procédure de renvoi au fournisseur (dont effacement sécurisé)

Local de stockage sécurisé

Gestion de l'acquisition, de la maintenance et de la fin de vie des équipements informatiques

## Liste des scénarios de risque

(inclure la source de risque, la valeur métier, l'événement redouté, les impacts, la sévérité, les biens supports critiques, les mesures de sécurité, les vulnérabilités exploitées, la vraisemblance)

N°	Description du scenario de risque	Responsable	Commentaires
RR1	Sachant que les personnel de la SGTIN est sensibilisé aux techniques d'hameçonnage, qu'il existe une procédure de passage en station blanche pour les clefs USB et qu'il existe un politique de mots de passe fort, il est peu vraisemblable (V1) que, pour faire de l'argent, une organisation de malfaiteurs réussisse à voler des données des citoyens à la SGTIN, par hameçonnage, envoi d'une clé piégée et/ou corruption de personnel, et les revende, permettant une usurpation critique d'identité (G4).		
RR2	Sachant qu'il existe un contrôle d'accès strict aux zones de travail de la mairie, il est peu vraisemblable (V1) qu'un membre d'une organisation de malfaiteurs vole des documents comportant des données des citoyens ou des TIN et les revende pour faire de l'argent, permettant une usurpation critique d'identité (G4).		
RR3	Sachant qu'HeberWeb gère correctement l'acquisition, la maintenance et de la fin de vie des équipements informatiques, notamment en les stockant dans un local sécurisé, il est peu vraisemblable (V1) qu'une organisation de malfaiteurs puisse récupérer des données des citoyens sur du matériel volé alors qu'il était mis au rebus par HeberWeb, et les revende pour faire de l'argent, permettant une usurpation critique d'identité (G4).		
RR4			
RR5			
RR6			
RR7			
RR8			
RR9			

- L'objectif de cette étude est une évaluation des risques en vue de l'homologation du système de renouvellement des Titres d'Identité Numérique (TIN)
- Sept valeurs métiers ont été identifiées. Parmi les plus importantes figurent l'impression et la distribution des TIN, qui doivent être intègres, ainsi que les données des citoyens et les TIN eux-mêmes, qui doivent être confidentiels. La violation des exigences de sécurité concernant ces actifs pourrait entraîner des fraudes et des usurpations d'identité, dont la gravité est critique. Ensuite, la gestion des demandes de renouvellement, le service de notification des TIN et la gestion des pré-demandes sont également importants. Toutes ces fonctions doivent être disponibles, allant respectivement d'une haute disponibilité à « faire au mieux ». La violation des exigences de sécurité concernant ces actifs pourrait entraîner des conséquences graves, notamment des retards, des coûts d'enquête et l'activation de solutions de secours. Enfin, des préoccupations liées à la confidentialité des données des citoyens et au respect de leur vie privée existent également.
- Notre hypothèse est que le seul rôle de la Société de Gestion des TIN (SGTIN) est de renouveler les TIN. Sur la base de cette hypothèse, les trois systèmes informatiques suivants de la SGTIN constituent le cœur du système étudié : le système bureautique, le système de gestion des pré-demandes et le système de production / impression. De plus, nous pouvons supposer que la SGTIN fournit le logiciel de renouvellement des TIN, hébergé chez HeberWeb et accessible via Internet par les employés de la mairie. Au-delà des actifs informatiques, il est possible d'identifier les employés de la SGTIN et les locaux de la SGTIN comme des biens support humains et d'infrastructure.
- Les audits réalisés sur HeberWeb, la Société d'Administration Technique (SAT), les mairies et la SGTIN ont montré qu'un certain nombre de mesures de sécurité sont déjà en place, mais qu'il existe des vulnérabilités résiduelles importantes, principalement liées à des politiques de sécurité inappropriées, une mauvaise configuration et des solutions techniques obsolètes (par exemple, FTP, SSL v3.0).
- Trois sources de risques ont une forte probabilité d'attaquer le système étudié : une organisation criminelle pourrait voir une opportunité lucrative (R1), un État étranger pourrait vouloir fournir de faux TIN pour ses espions (R3) et un hacktiviste pourrait vouloir perturber la fabrication des TIN pour des raisons idéologiques (R2). Nous avons également retenu un employé mécontent comme origine potentielle d'un risque en raison des privilèges élevés que cet initié détient sur le système (R4)
- Les interconnexions du système étudié sont assez nombreuses, directement avec les citoyens et HeberWeb, et indirectement avec les mairies et la SAT. L'analyse de l'écosystème montre que la SAT se trouve dans la zone de danger, essentiellement en raison de la mauvaise maintenance et configuration de la sécurité des équipements. Toutes les autres parties intéressées se trouvent dans la zone de contrôle, avec une attention particulière pour HeberWeb, essentiellement à cause de la mauvaise gestion de la fin de vie des équipements informatiques.
- Nous supposons qu'une organisation criminelle ou un État étranger pourrait attaquer directement le système étudié (R1a, R3a) ou passer par la mairie (R1b, R3b), ou par HeberWeb (R1c, R3c). En revanche, nous supposons que le hacktiviste préférerait attaquer par les mairies (R2a), tandis que bien sûr, l'employé malveillant attaquerait directement le système (R4a). Compte tenu de ces scénarios stratégiques, il est recommandé de mettre en œuvre toutes les recommandations des audits. Les corrections suggérées dans les audits devraient améliorer considérablement l'état de la cybersécurité de la SAT, HeberWeb et des mairies.
- L'analyse du chemin d'attaque direct de l'organisation criminelle (R1a) montre que la SGTIN est vulnérable au phishing, aux malwares sur supports mobiles, et dans une moindre mesure, à la corruption. Il a été évalué qu'il est vraisemblable que des malwares pourraient profiter des mauvaises pratiques de maintenance de sécurité pour exploiter une vulnérabilité logicielle, permettant ainsi à l'organisation criminelle d'obtenir des privilèges et d'exfiltrer des données sensibles. De nombreuses mesures de sécurité à faibles coûts ont été proposées pour modifier le risque, notamment la formation de sensibilisation à la cybersécurité, une meilleure maintenance et de meilleures politiques de sécurité. Avec ces mesures, R1a devrait devenir plutôt peu vraisemblable.
- ...