19 Novembre 2024 | Hospices Civils de Lyon
Groupement Hospitalier Est

# JOURNÉE RÉGIONALE CYBERSÉCURITÉ

GCS Sara
la santé connectée

HCL
HOSPICES CIVILS DE LYON

TOUS CYBER VIGILANTS

# Audit d’exposition internet

TOUS CYBER VIGILANTS

1 Où en somme-nous ?

2 La détection par AlgoLightHouse

3 Comment accélérer la remédiation ?

TOUS CYBER VIGILANTS

1

# Où en somme-nous ?

# Rappel des objectifs

1

Auditer l'exposition internet en continu

Soutenir le programme CaRE

Etendre le service au-delà de CaRE

**Solution AlgoLightHouse pour une durée de deux ans**

# Rappel du planning

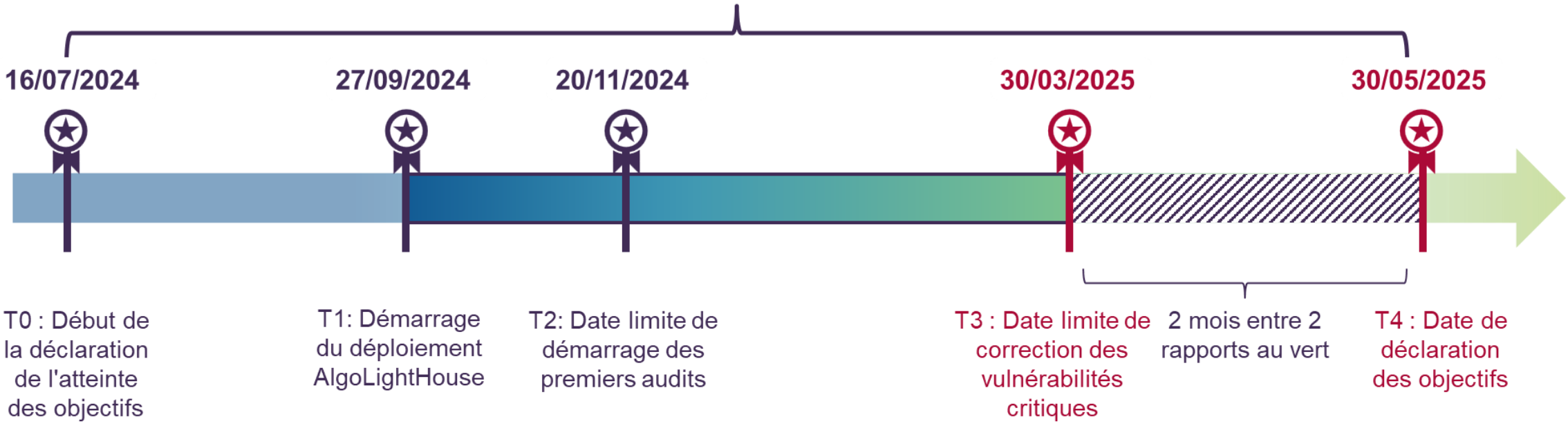
1

## Conditions et seuils d'éligibilité :

- Utilisation d'une plateforme d'audit industrielle **conforme** au *cdc* ANS v1.0
- 2 mois entre rapports ET 2 rapports successifs **au vert**
- Dernier audit **1 mois maximum** avant la déclaration des objectifs

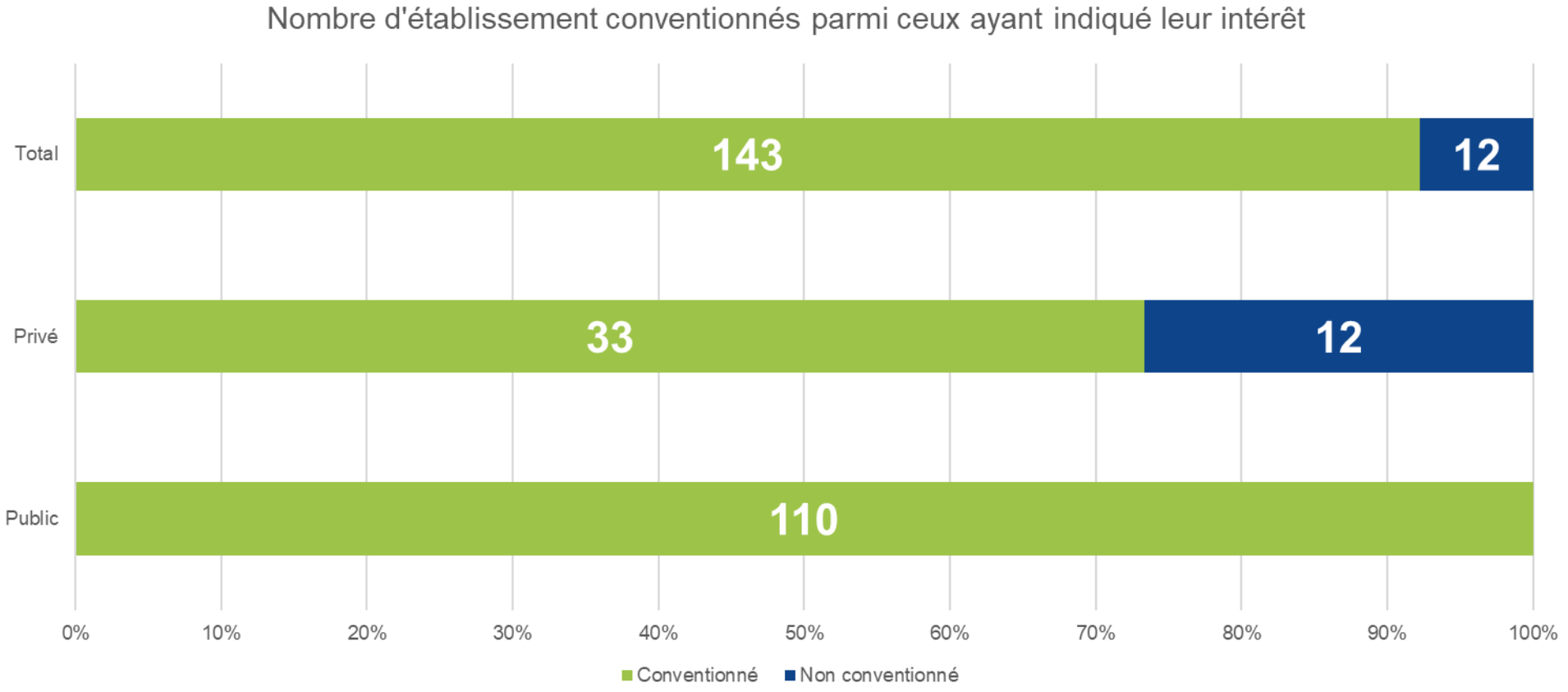
### Rapport vert selon ANS

« Aucune vulnérabilité publique de niveau critique (CVE supérieur ou égal à 9) ou risque critique lié aux services exposés ou vulnérabilité publique de niveau haute avec un score CVSS entre 7 et 9 n'ayant pas été identifié lors du précédent audit. »



# Etablissements conventionnés

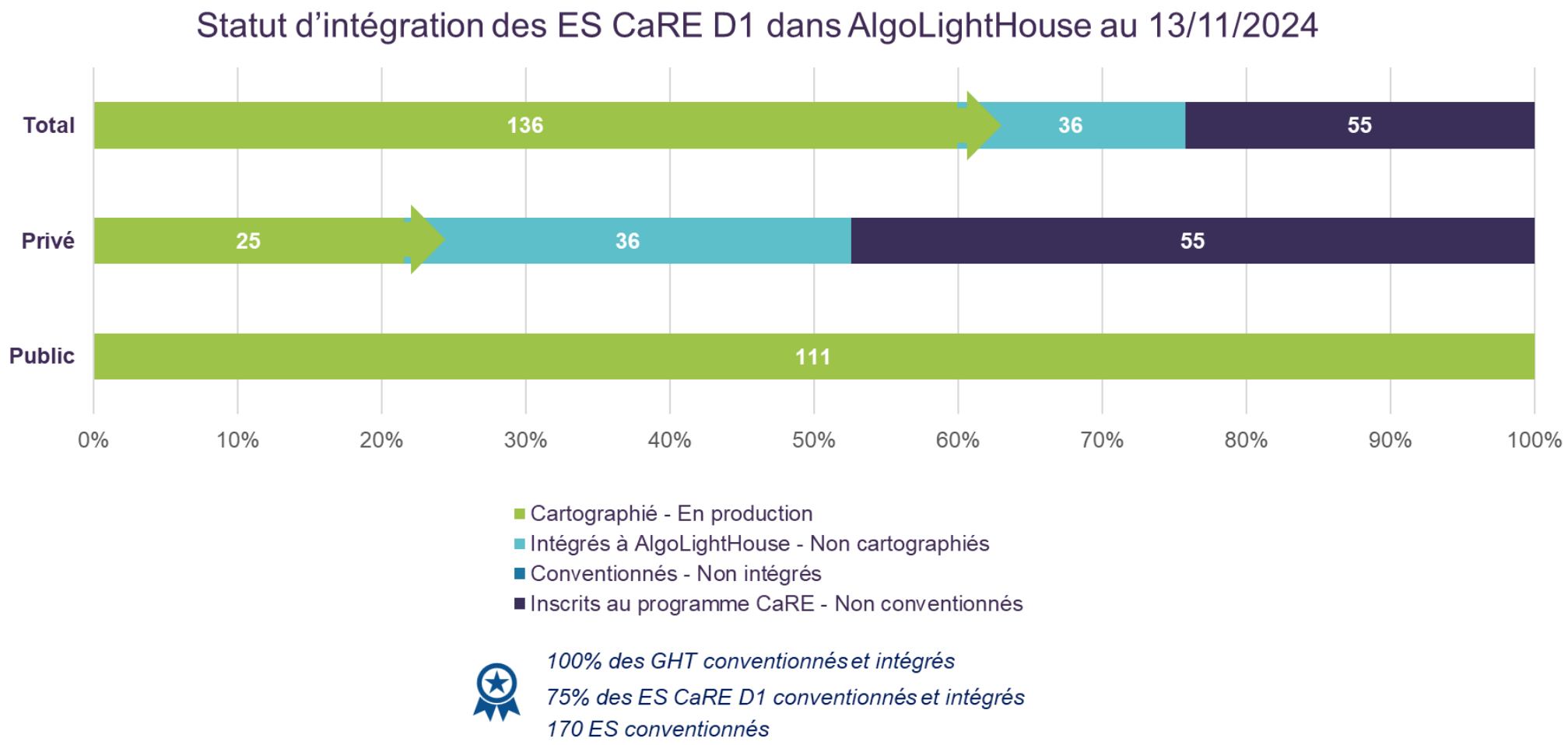
1




*92% des établissements intéressés conventionnés*
*+ 28 établissements supplémentaires*

# Statistiques sur la phase d'intégration

1



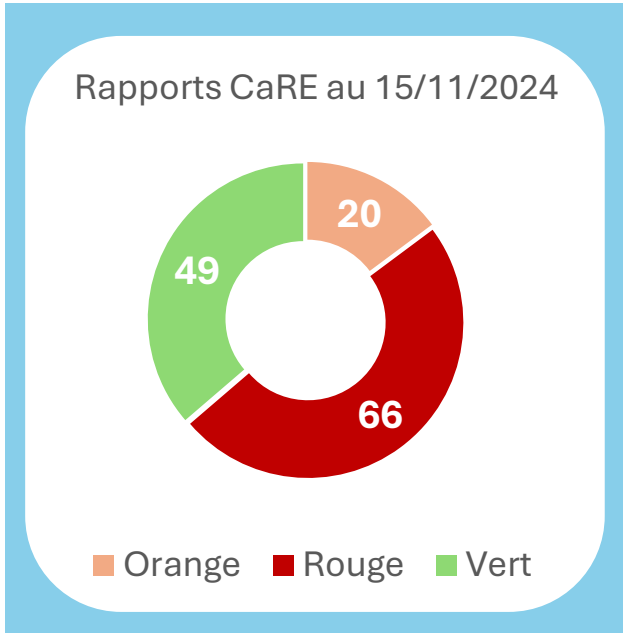

*100% des GHT conventionnés et intégrés*

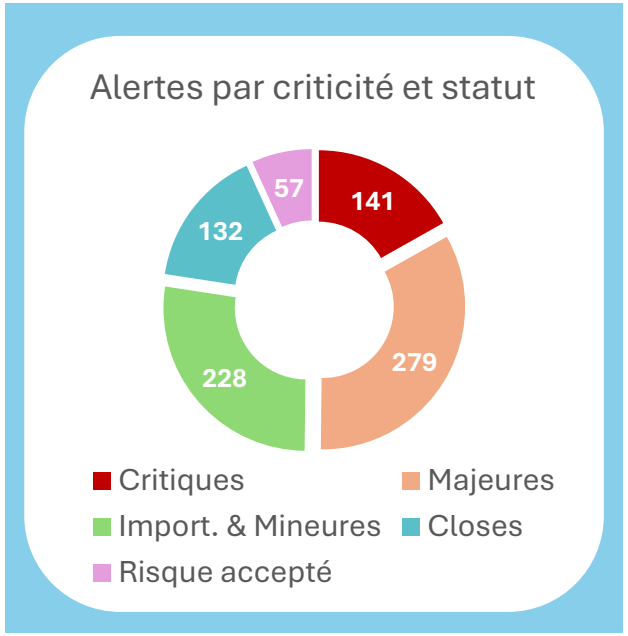
*75% des ES CaRE D1 conventionnés et intégrés*

*170 ES conventionnés*

# Objectifs CaRE






**Questionnaire d'évaluation AlgoLightHouse**

Première analyse à partir du 30 novembre

Domaines surveillés
**2449**

IP surveillées
**2783**

TOUS CYBER VIGILANTS

2

# La détection par AlgoLightHouse

# Qui sommes-nous ?

2

**Cabinet-conseil** cybersécurité **indépendant**

Implanté également au Campus Cyber

**Accompagnement SSI**

Auditer | Conseiller | Surveiller

**Réagir (CERT depuis 2016)**

**Équipe à taille humaine**

50 collaborateurs

algoLightHouse by algosecure

**De l'expertise**

Des certifications et qualifications au niveau entreprise et collaborateurs

ISO 27001 BUREAU VERITAS Certification

VISA DE SÉCURITÉ

**De la passion**

Une forte implication dans les communautés cyber : clubs cyber/digital, MLSSI

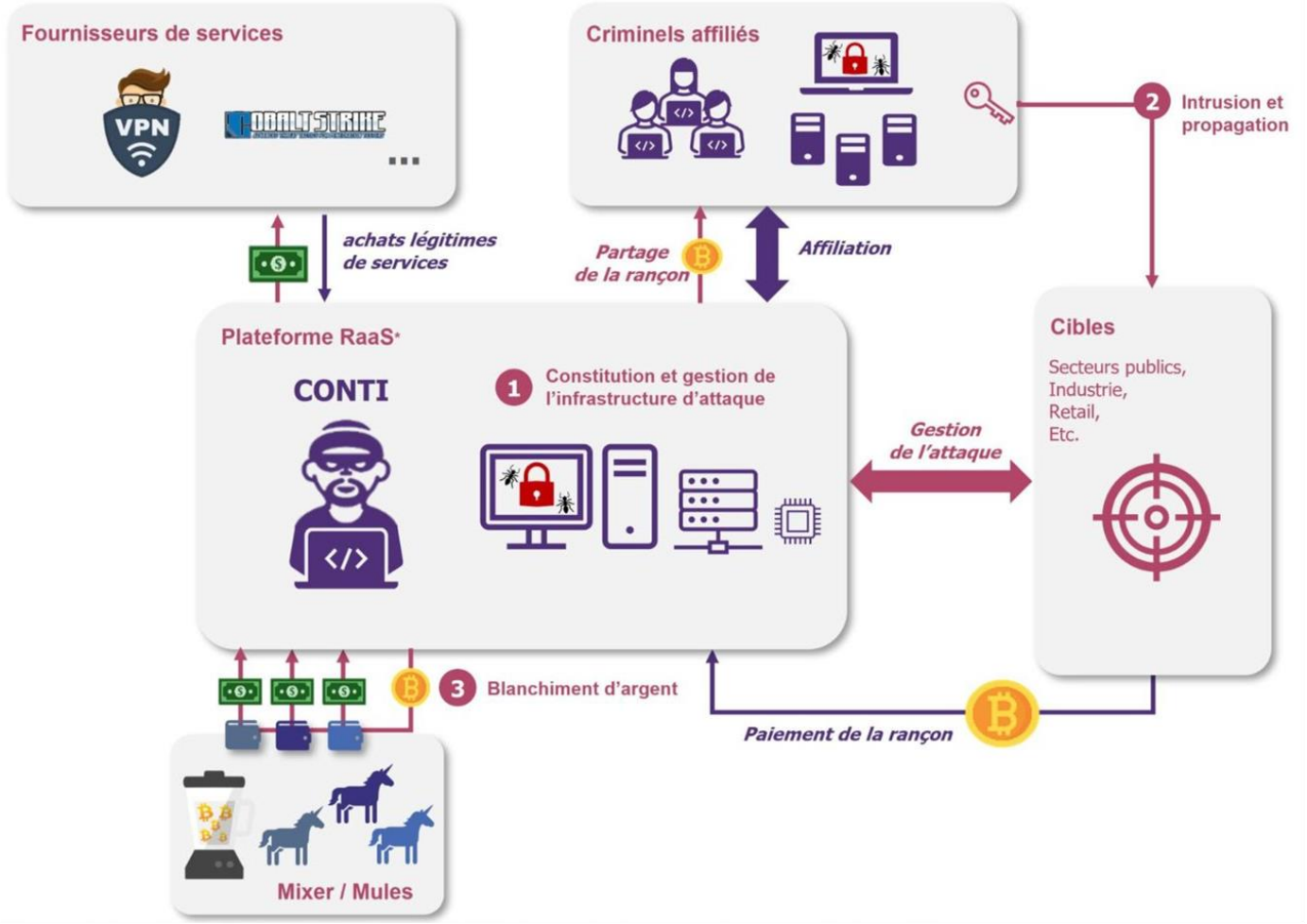
HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

MLSSI Les Matinées Lyonnaises de la SSI

# Écosystème cybercriminel

2

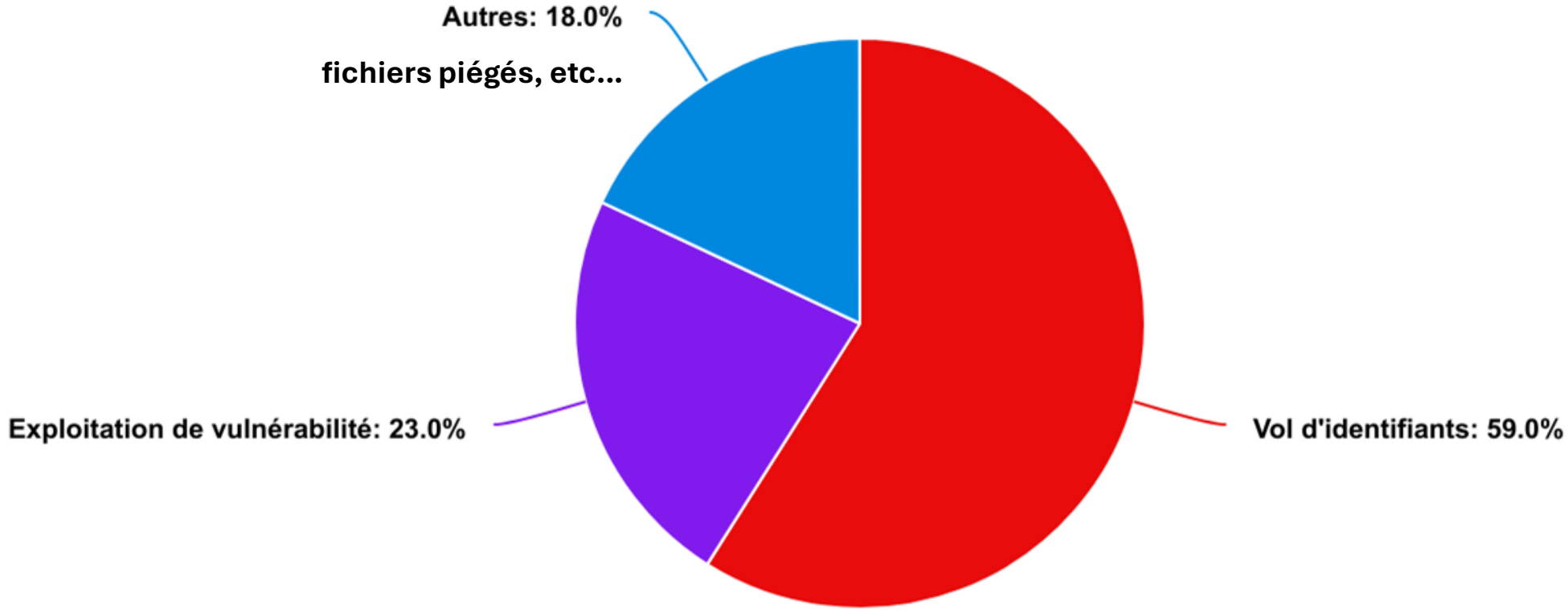
**Organisation huilée :**
Info-stealers, développeurs, mules, chercheurs de vecteurs d'attaque, ...




source : riskinsight-wavestone.com

# Les principaux vecteurs d'intrusion

2

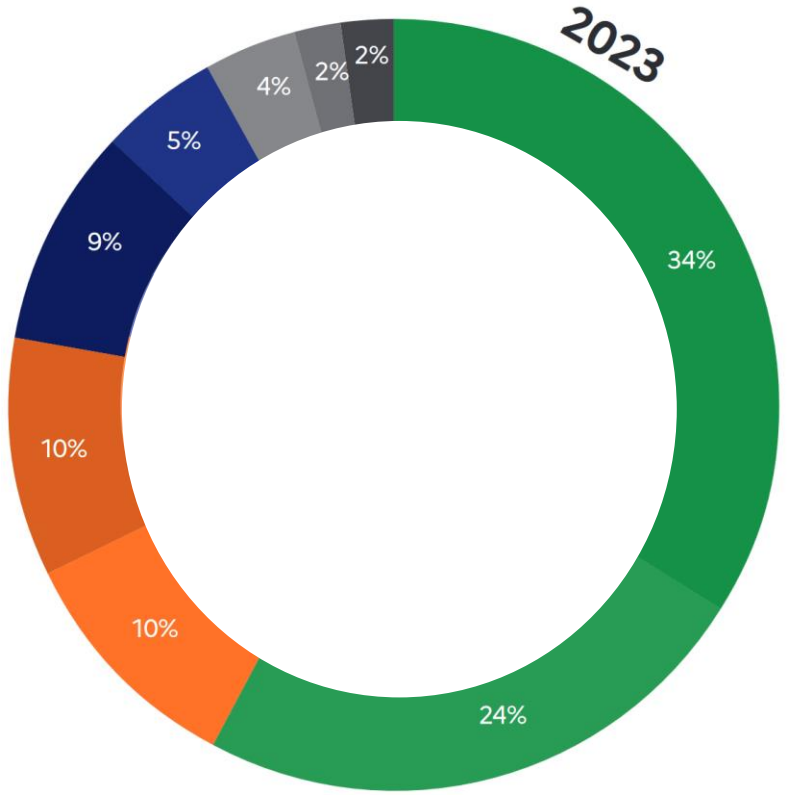


# Victimologie des criminels

2

→ **Répartition des victimes d'attaque par rançongiciel**

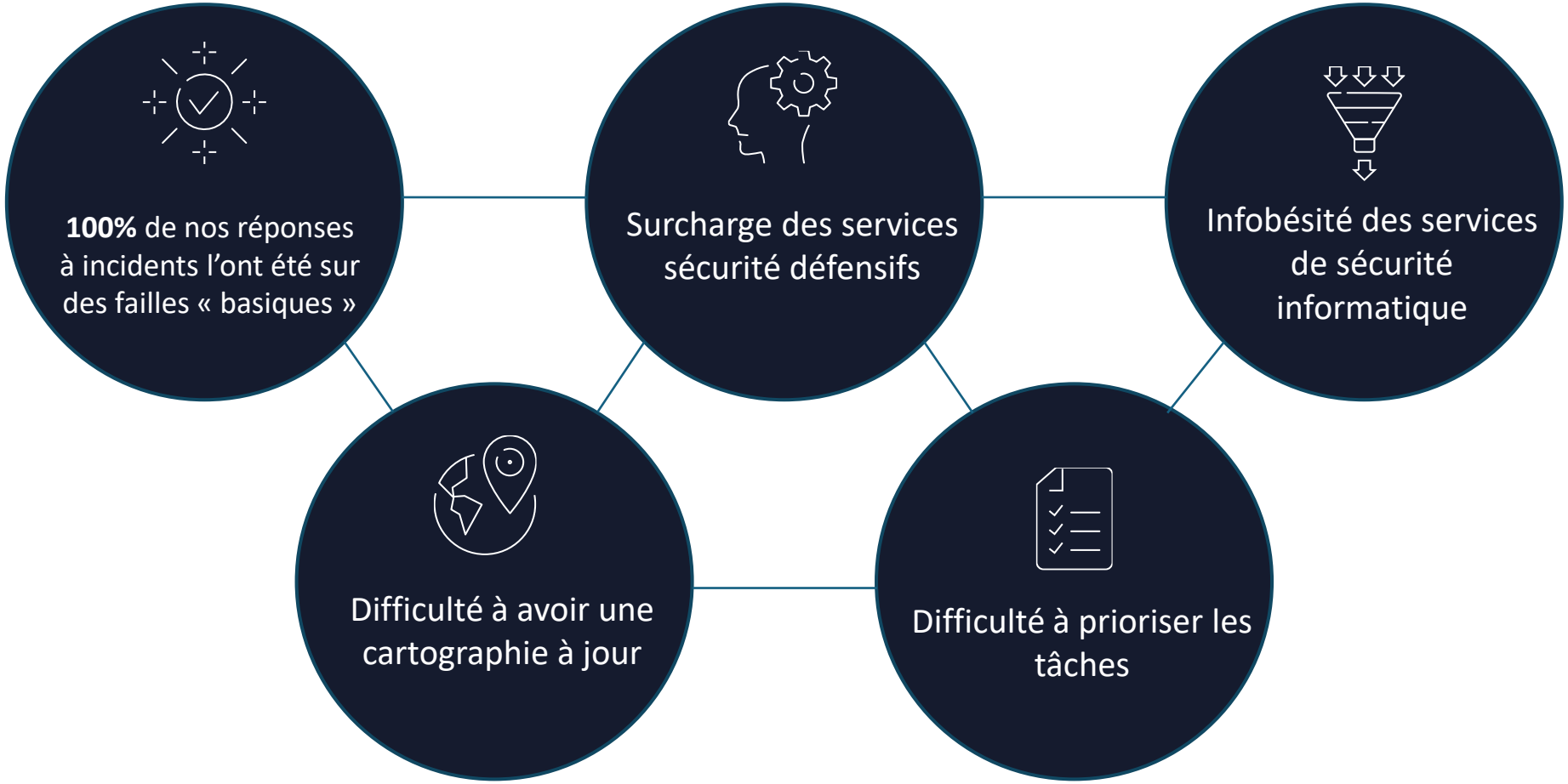
- TPE/PME/ETI
- Collectivité territoriale/locale
- Entreprise stratégique
- Établissement de santé
- Association
- Établissement d'enseignement supérieur
- EPA, EPIC
- Ministère
- Autre




source: ANSSI, panorama de la cybermenace 2023

# Constats AlgoSecure

2



# Les piliers AlgoLightHouse

2

### Audit externe et cartographie en continu

Identifie les points d'accès non sécurisés, **réduisant ainsi le risque d'intrusions et de pertes de données sensibles.**

Maintient une cartographie et une vision de son périmètre exposé à jour, notamment pour connaître les **potentiels points d'entrées exploitable par un attaquant** et anticiper cela.

### Veille et recherche OSINT

Essentiel pour maintenir un niveau de sécurité optimal.

Surveille de manière proactive le périmètre de l'entreprise et les personnes exposées.

Cette vigilance facilite la détection précoce de potentielles **fuites d'informations sensibles** et aide à atténuer les risques de cyberattaques ciblées.

### Analyse humaine et expertise

Les équipes de surveillance intègrent des analystes offensifs dotés d'un regard affuté.

Chaque alerte remontée est **vérifiée et évaluée par des experts.**

### Feuille de route SSI

Les alertes sont associées à des **commentaires et des actions de remédiation** (si nécessaire).

Les actions de remédiations sont priorisées.

Une phase de test et vérification est prévue pour s'assurer des corrections.

# Exigences du Programme CaRE

2

## Alertes Critiques

- Ports sans chiffrement natif
- Ports sensibles ou d'administration
- Ports de bases de données
- Chemins critiques exposés

(.env, backups, .git, phpMyAdmin)

- Vulnérabilités CVSS ≥ 9
- Certificats SSL vulnérables à Heartbleed

## Alertes Majeures

- Autres ports sensibles
- Chemins sensibles exposés (.htaccess, ...)
- Vulnérabilités CVSS ≥ 7
- Certificats SSL expirés ou protocoles vulnérables

## Alertes Importantes

- Autres chemins sensibles exposés (package.json, ...)
- Vulnérabilités CVSS ≥ 5
- Chaîne de confiance brisée des certificats SSL

# Exigences du Programme CaRE

2

Echelle de criticité ≠ ANSSI

| ↓ Impact Exploit. → | Très difficile | Difficile | Modérée | Facile |
|---|---|---|---|---|
| Mineur | Mineur | Mineur | Important | Majeur |
| Important | Mineur | Important | Important | Majeur |
| Majeur | Important | Majeur | Majeur | Critique |
| Critique | Important | Majeur | Critique | Critique |

# Typologie des alertes fréquentes

2

- Chemins sensibles exposés (phpMyAdmin et phpinfo)
- Directory Listing (notamment configurations)
- Ports d'administration (SSH) exposés sans restriction IP

Alertes identifiées parmi
2 705 domaines et 2 841 IPs en surveillance

# Alertes mais surtout Cartographie

2

- Vision sur l'ensemble du périmètre
- Identifier rapidement les responsables des actifs

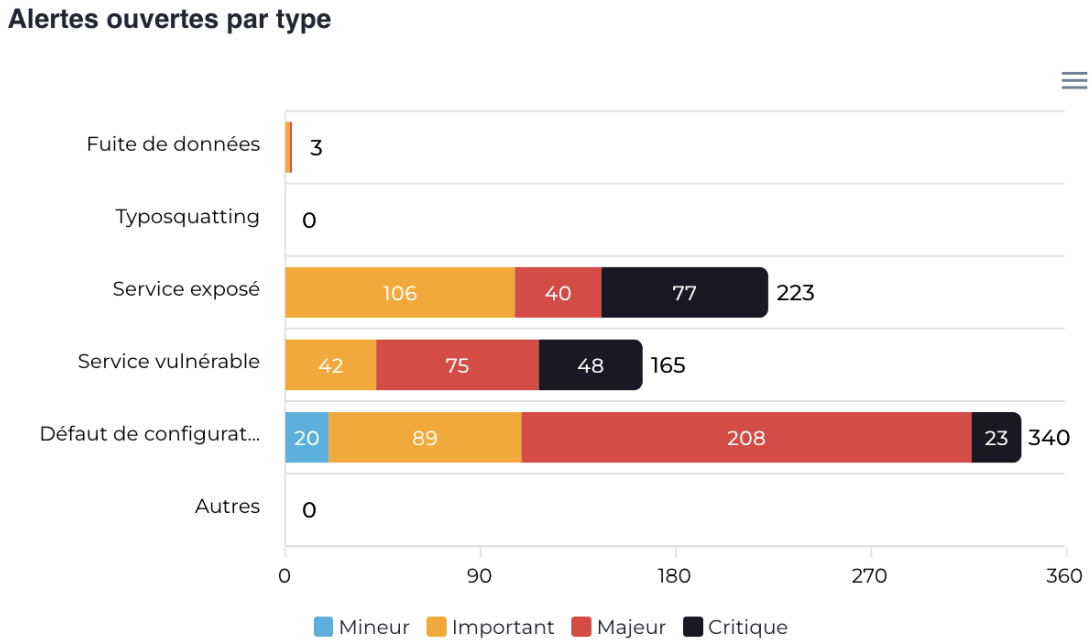
**En moyenne, temps de résolution < 5 jours**

Autres acteurs de la pharmaceutique ~ 9 jours

Équipe dédiée pour des **questions** et des **re-tests** :

- 501 messages de support
- 111 e-mails à support@algolighthouse.fr

# Quelques statistiques





**Dont 4 incidents critiques avec déclanchement d'appels téléphoniques**

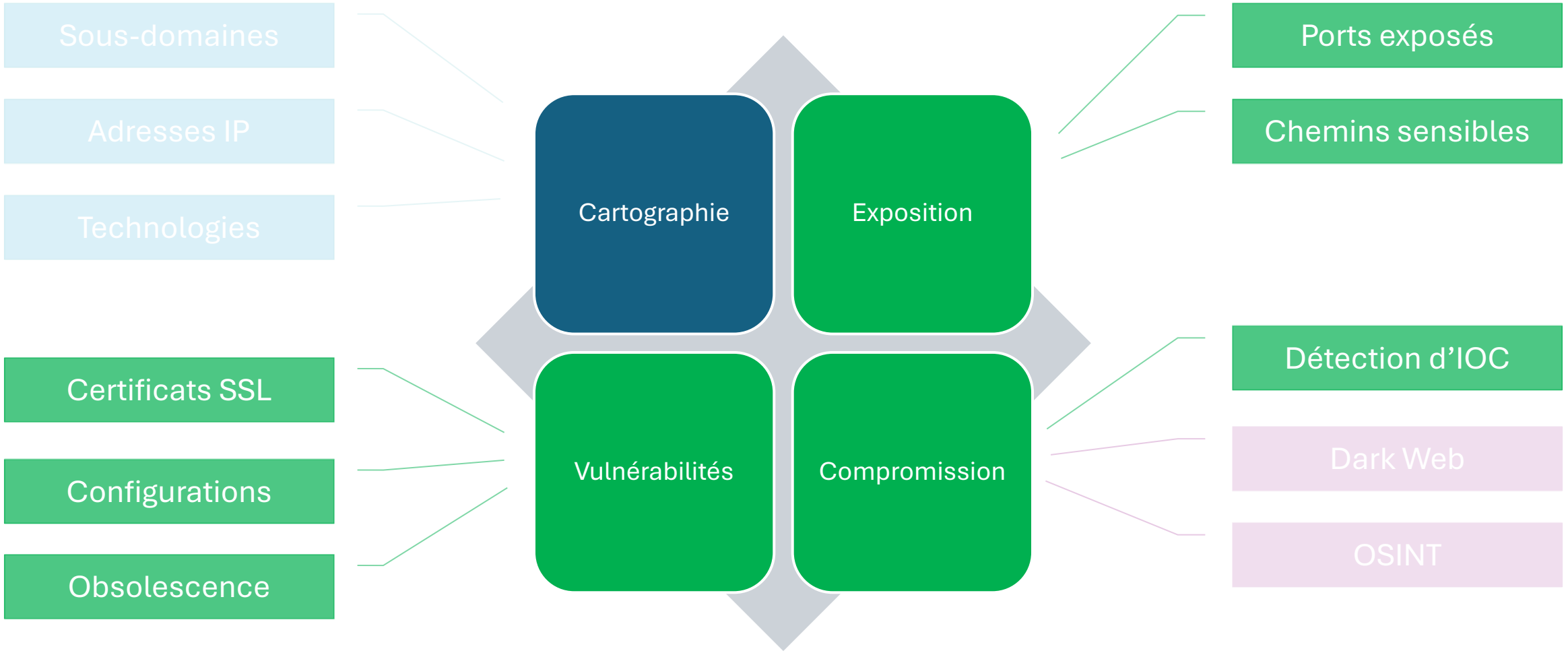
TOUS CYBER VIGILANTS

3

# Comment accélérer la remédiation?

# Comment gérer les résultats des audits ?

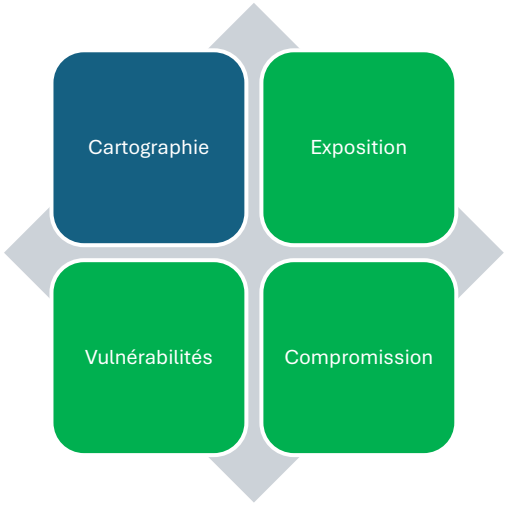
3



# Reflexe numéro 1 – Réduire l'exposition

3

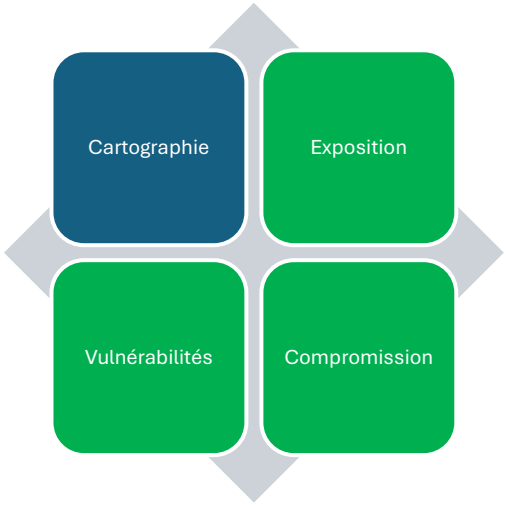
**Est-il nécessaire d'exposer ce domaine ou cette IP ?**

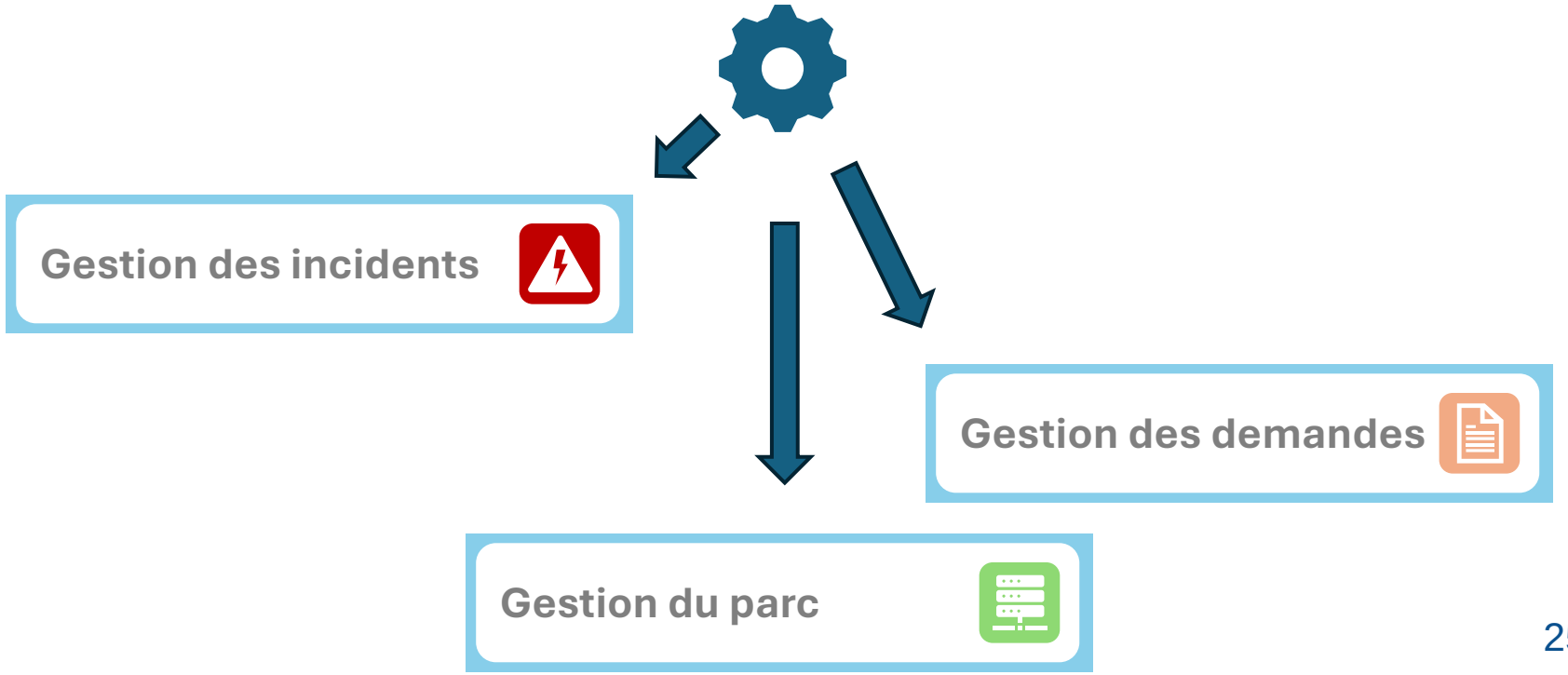



# S’appuyer sur les processus existants

3

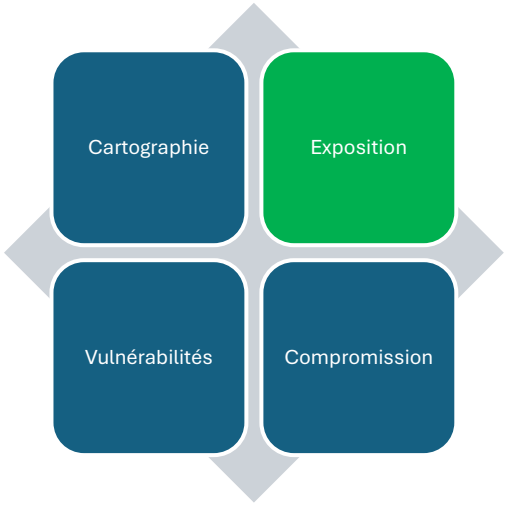
## Quel est le processus le plus efficace ?



# Ports exposés et chemins sensibles

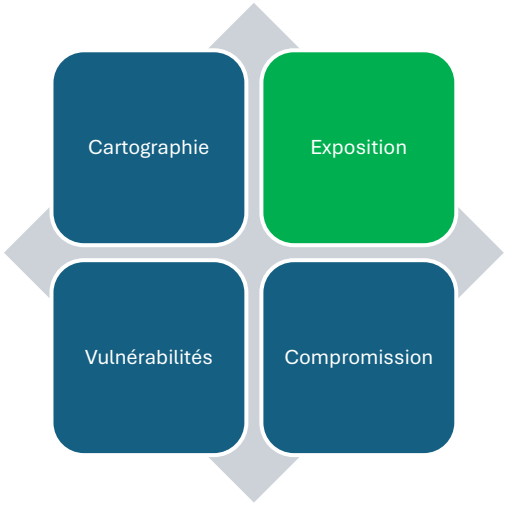
3




1. Est-il possible de ne plus les exposer ?
2. Est-il possible de restreindre l'exposition ?
3. D'autres mesures de sécurité ?

# Ports exposés

3




Ports exposés

## Ports des interfaces d'administration

- Restreindre au réseau interne ou VPN d'administration
- Restreindre à certaines IP externes précises
- Utiliser un bastion

## Ports non chiffrés

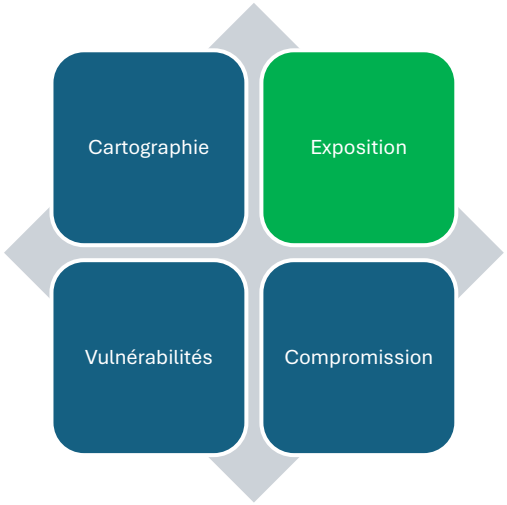
- Remplacer par des ports chiffrés
- Rediriger vers des ports chiffrés
- Restreindre depuis certaines IP externes précises

## Ports de bases de données

- Restreindre depuis le réseau interne ou VPN d'administration
- Restreindre depuis certaines IP externes précises
- Utiliser un bastion

# Chemins sensibles






Chemins sensibles

## Interfaces d'administration

- Restreindre au réseau interne ou VPN d'administration
- Restreindre à certaines IP externes précises
- Utiliser un bastion

## Données et fichiers confidentiels

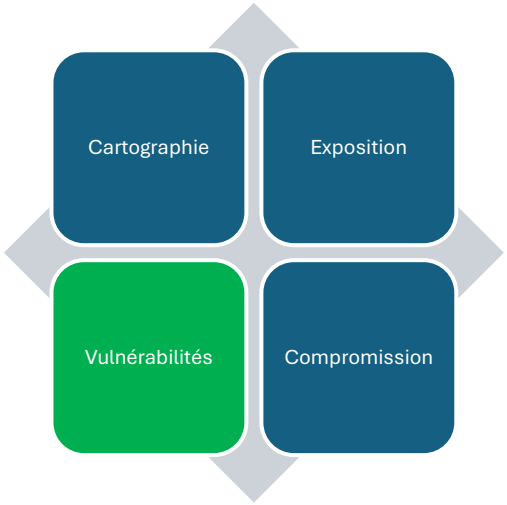
- Evaluer la criticité et confidentialité
- Supprimer ou déplacer la donnée
- Restreindre l'accès

## Pages d'authentification publiques

- Mettre en place du MFA
- Sécuriser l'authentification (ex. anti-brute force)
- Surveiller les connexions

# Gérer les vulnérabilités

3




## Obsolescence

- Mettre en place un processus de mise à jour
- Supprimer les composants non nécessaires
- Ne pas exposer de composants obsolètes

## Vulnérabilités liées à une configuration

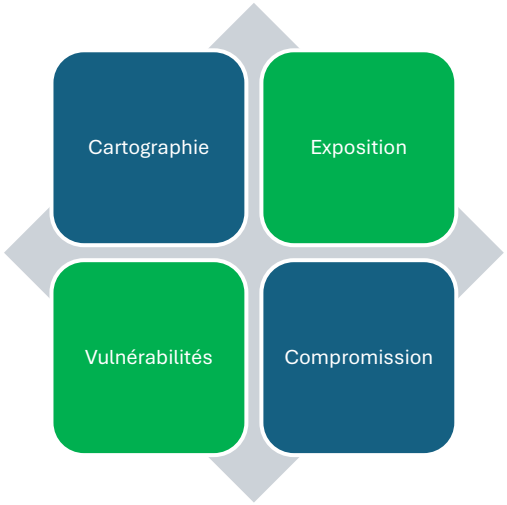
- Déterminer quelle équipe peut la gérer
- Supprimer les composants non nécessaires
- Ne pas exposer de composants vulnérables

## Certificat SSL

- Gérer l'expiration des certificats SSL
- Utiliser des protocoles robustes

# Réduire la surface exposée en amont

3

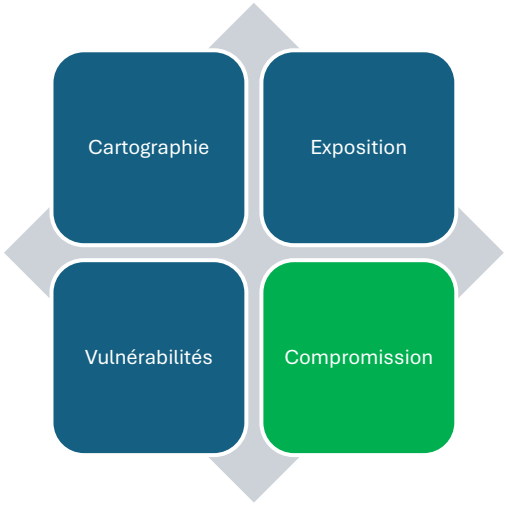



Intégrer la démarche dans le processus de changement

- Exposer uniquement les IP et domaines nécessaires
- Appliquer la même démarche pour les ports
- Ne déployer que les composants nécessaires
- Gérer les interfaces d'administration
- Gérer ses certificats SSL
- Gérer les mises à jour de son parc

# Et en cas d'IOC ?






Détection d'IOC

Ouvrir immédiatement un incident de sécurité

- Déclencher son équipe de réponse à incident
- Isoler l'élément compromis
- Contrôler la présence de l'IOC sur le reste du SI
- Prévenir le CERT Santé

GCS Soara
la santé connectée

HCL
HOSPICES CIVILS
DE LYON