



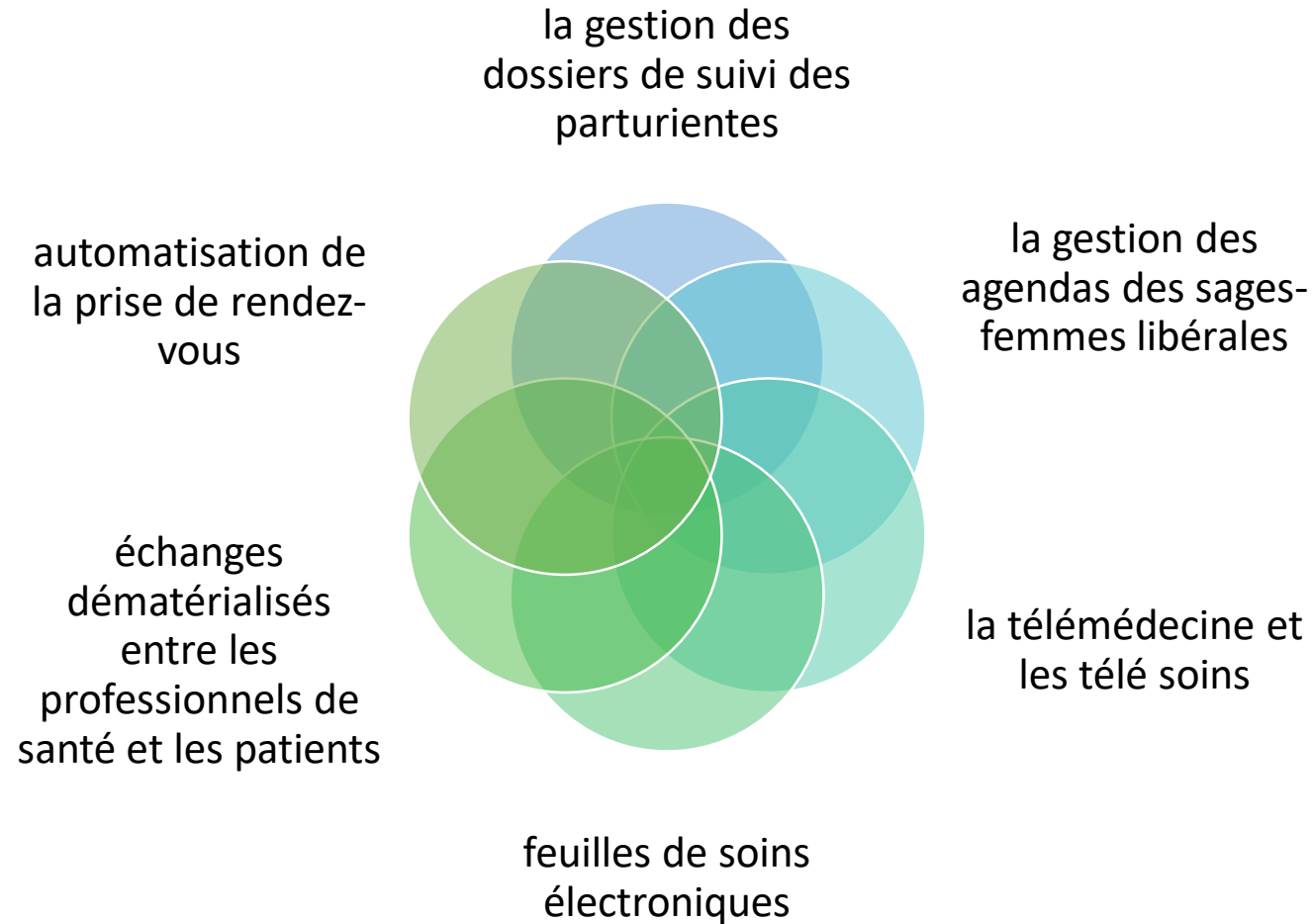
Cellule Cybersécurité Santé Nouvelle-Aquitaine

TOUS CONCERNÉS !

Professionnels libéraux et hospitaliers Acteurs des secteurs sociaux
et médico-sociaux Soignants et administratifs Fédérations et institutions

Suite à une orientation stratégique nationale forte, et sous l'impulsion de l'ARS NA, ESEA a créé la Cellule Cybersécurité santé NA qui a vu le jour en septembre 2021. Elle a pour mission **d'accompagner et de conseiller les acteurs de santé** de la région dans le renforcement de la sécurité de leur système d'information. Elle **coordonne et anime les actions collectives régionales** de cybersécurité en santé et propose également des actions de **sensibilisation** et de **formation spécifiques**.

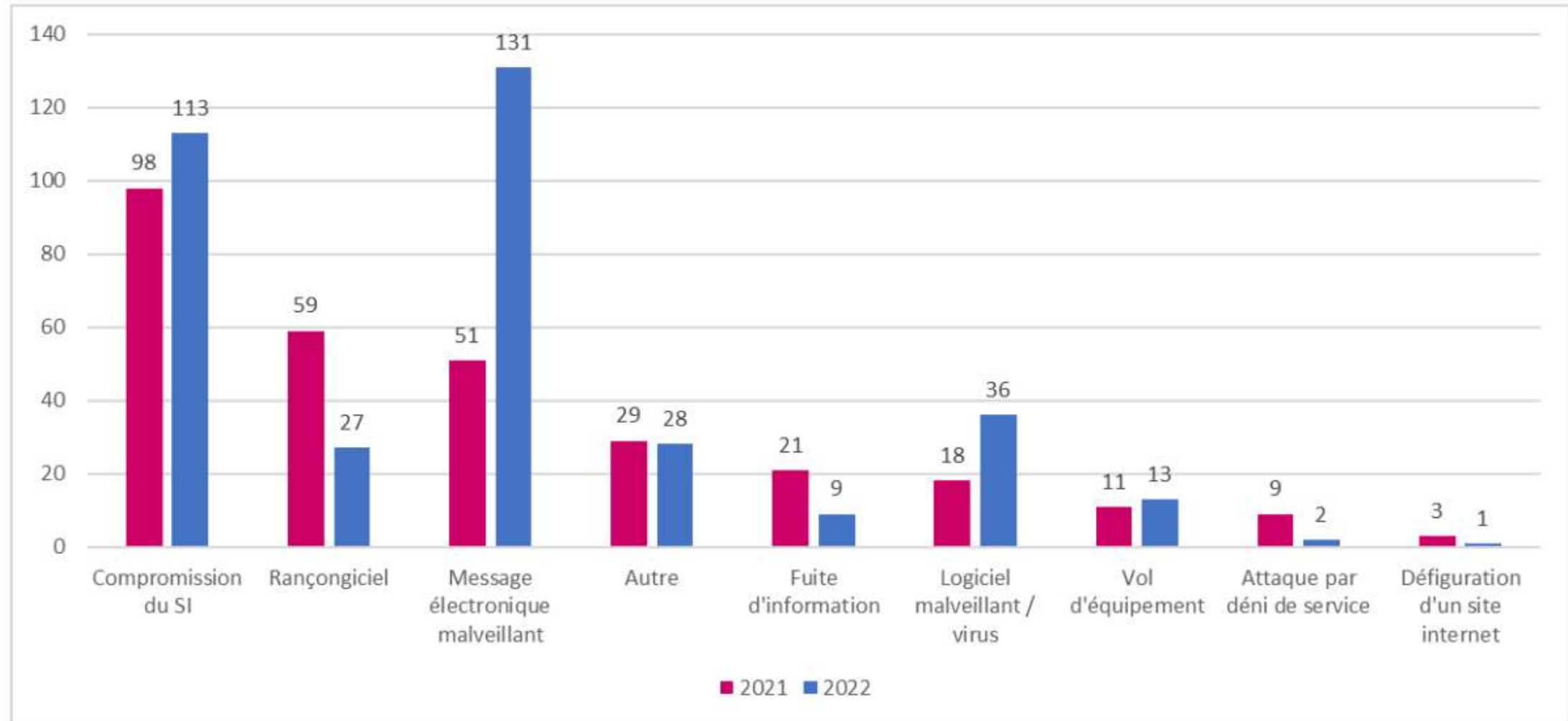
Les sages-femmes 2.0



Les risques les plus importants

- Systèmes biomédicaux paralysés
- Plateaux techniques indisponibles
- Données de programmation des soins détruites
- Systèmes de messageries en panne
- Données de gestion et de ressources humaines perdues
- Données personnelles de santé usurpées

CERT Santé : Les actes malveillants



Les modes opératoires des attaquants

La technique de l'hameçonnage (phishing)

L'exploitation de vulnérabilités sur des équipements qui n'ont pas été mis à jour

Les tentatives de récupération en testant un grand nombre de mots de passe (technique de brute force)

Panorama des cybermenaces

- Depuis la crise COVID :

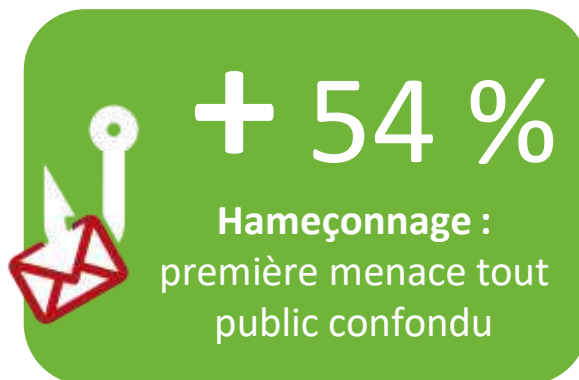
+ 500 %

de cyberattaques en milieu
médical depuis le COVID

66 %

des crises cybersécurité sont
dus à un rançongiciel

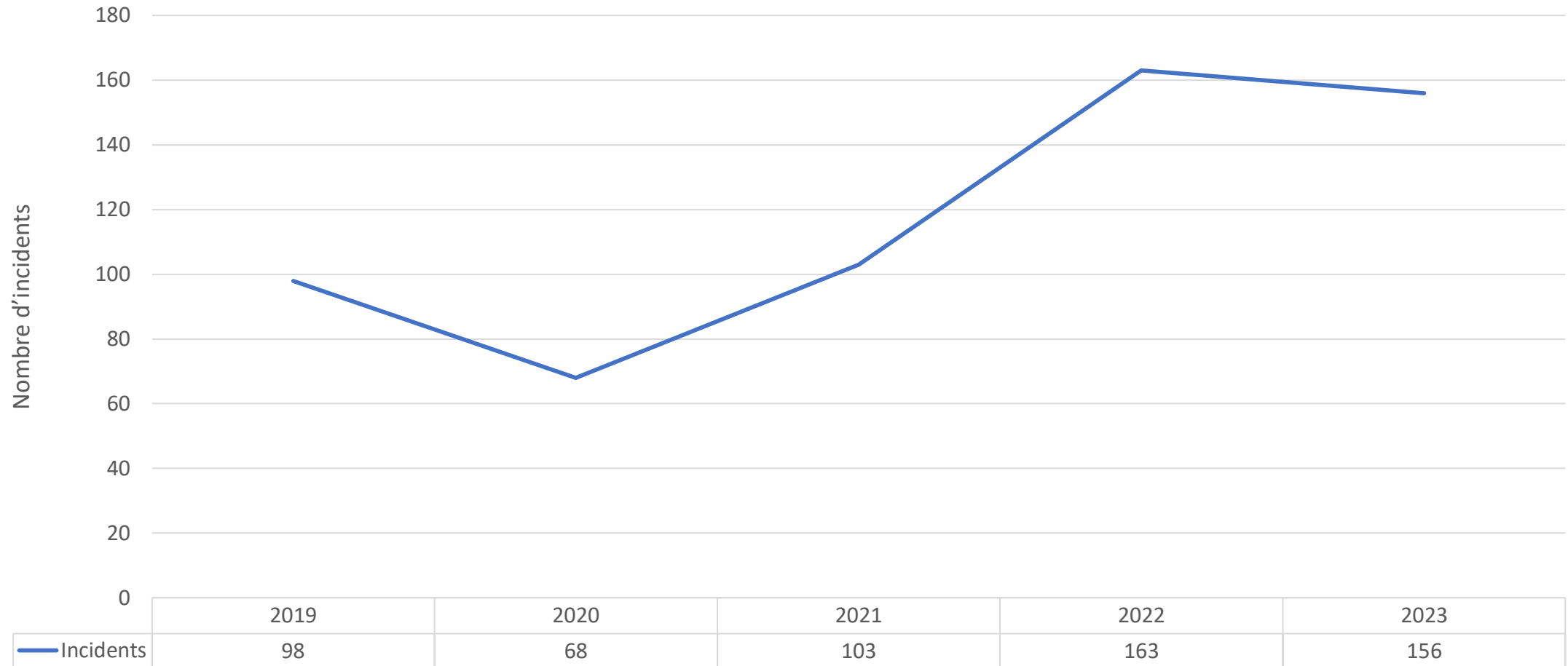
- En 2022, en demande d'assistance* :



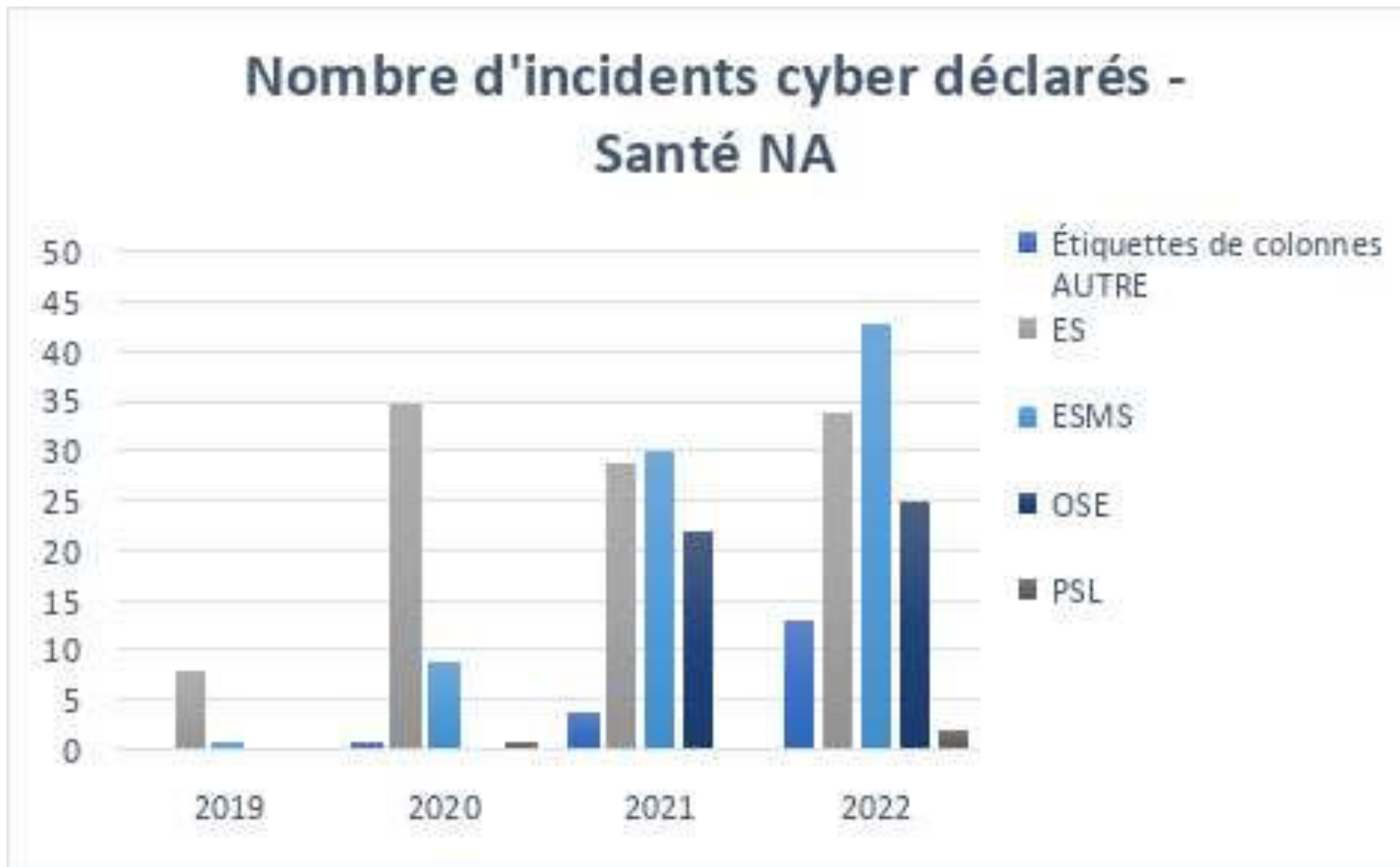
* Via le site cybermalveillance.gouv.fr

Statistiques en région Nouvelle-Aquitaine

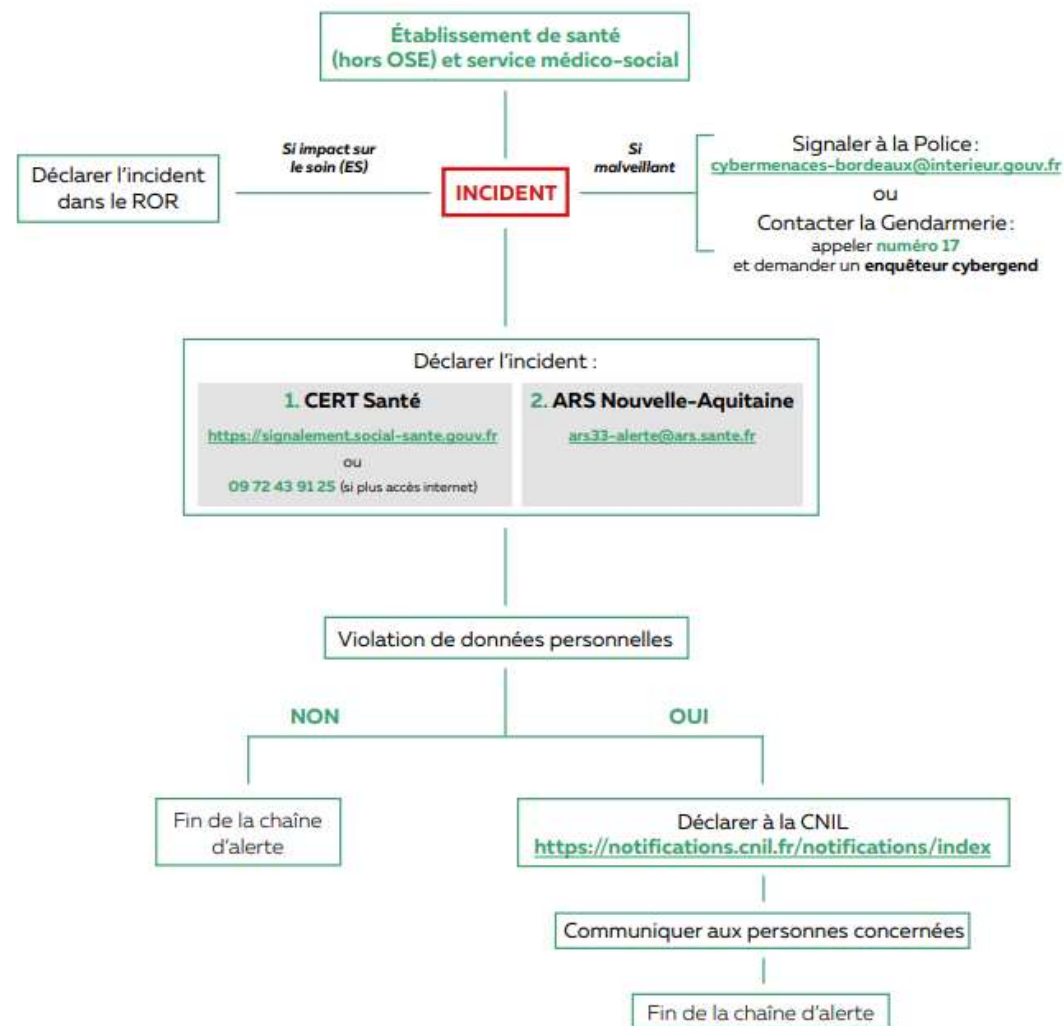
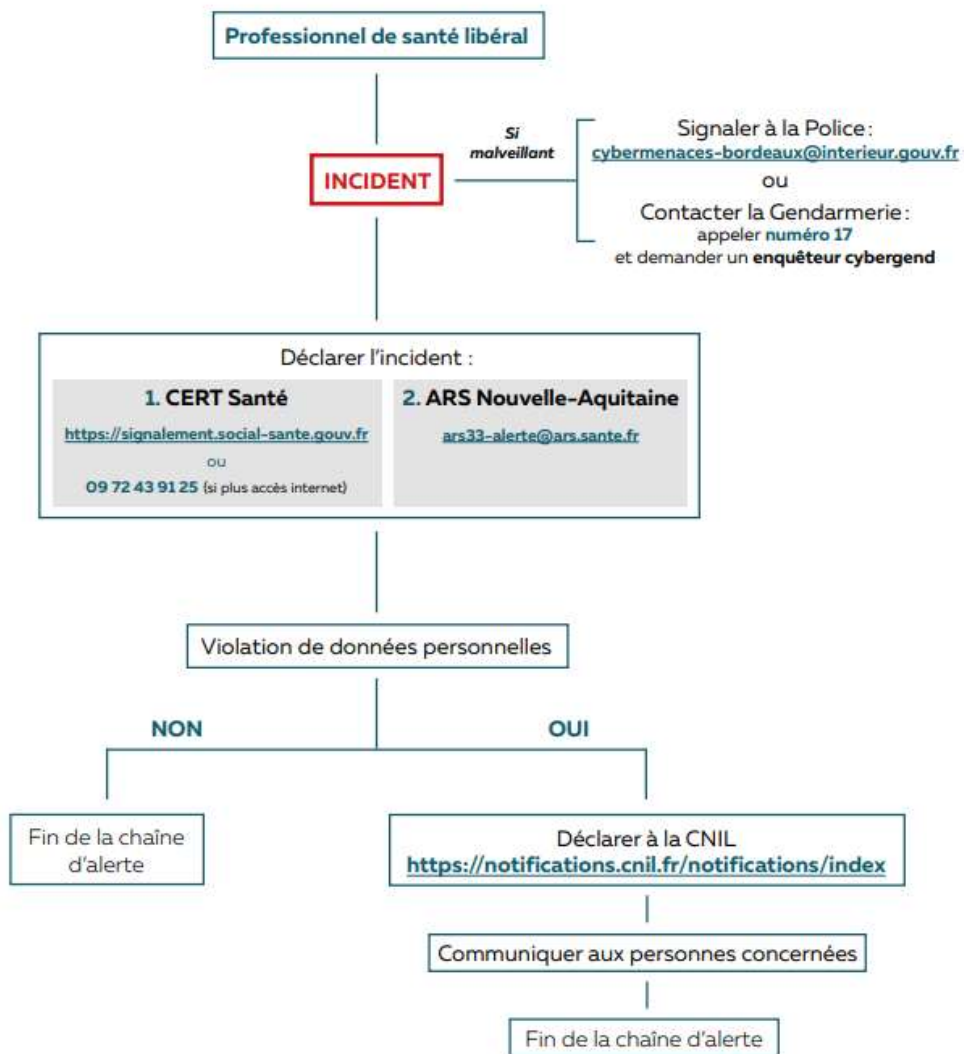
Statistiques en région Nouvelle-Aquitaine 2019 - 2023



Rappel des signalements pour les PSL



Chaînes d'alertes en cas d'incident



Les bonnes pratiques

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	26 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	5 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

- Un mot de passe par application
- 15 caractères minimum.
- Majuscules, minuscules, chiffres et caractères spéciaux
- Faire une phrase de passe simple qui vous parle plutôt qu'un mot de passe, ex : `Jeveux100KDO@nowel!`
- Bannir les chaînes de caractères (azerty, 123456...), les informations personnelles (prénoms, dates de naissances de proches...)
- Activer autant que possible la double authentification !
- Mettre en place un coffre fort de mot de passe, comme KeePass !

Que valent vos données personnelles

Prix en dollars (2023)



Carte de crédit

20 \$ à 60 \$



Comptes de paiements en ligne

1 \$ à 100 \$



Boîtes mails et comptes de réseaux sociaux

1 \$ à 65 \$



Dossiers médicaux ou informations médicales

1 \$ à 380 \$



Accès aux comptes bancaires

0,5% à 10 % de sa valeur



Comptes de jeux vidéo

1 \$ à 12 \$



Scan de carte d'identité, permis de conduire et passeport

1 \$ à 35 \$



Comptes de streaming

1 \$ à 10 \$



Cartes cadeaux

10 % à 50 % de sa valeur

*Sources : www.vpnmentor.com - www.expressvpn.com - www.lexpress.fr

Valeur financière - données de santé

Vos données de santé dérobées ont aussi une valeur financière

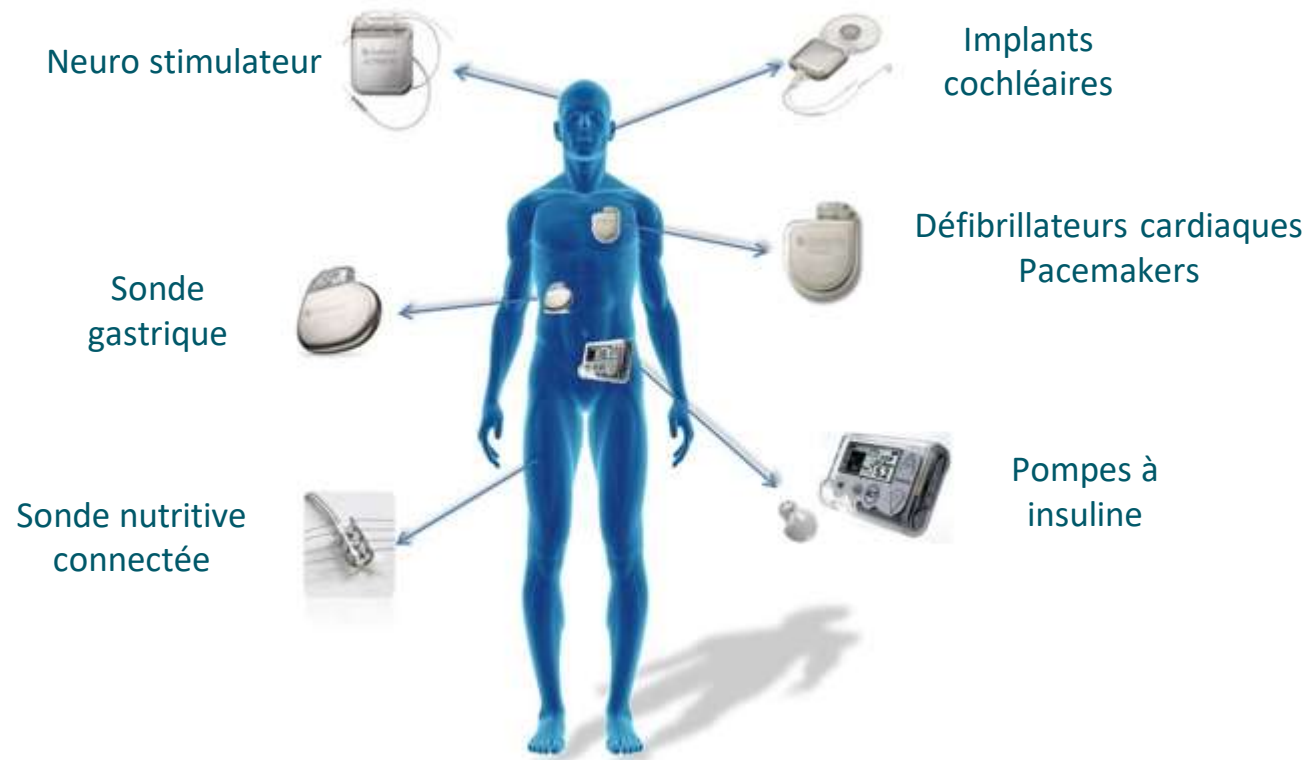


En 2022, au niveau mondial, « le potentiel des données de e-santé est estimé par les GAFAM à 7 100 milliards de dollars », selon Eugène Favier-Baron. Soit le PIB de la 4^{ème} puissance économique mondiale

*Source : www.mastermsi.fr/la-vente-de-donnees-de-sante-un-business-de-plus-en-plus-lucratif/

Le pouvoir de l'information...

IMPLANTS MEDICAUX CONNECTES EN MODE SANS CONTACT



Si on oublie notre corps, en moyenne, aux USA, en milieu hospitalier, 15 appareils connectés par chambre ; en France 6.

Il faut parfois moins de 3 minutes pour prendre le contrôle d'objets connectés courants.

Le cas de la maternité privée des Bluets



BFMTV
<https://www.bfmtv.com> › Paris Île-de-France

Paris: l'hôpital Pierre-Rouquès-Les Bluets victime d'une ...

18 oct. 2022 — L'hôpital Pierre-Rouquès-Les **Bluets**, dans le 12ème arrondissement de Paris, a été victime dans la nuit de dimanche d'une **cyberattaque**, ...

Siècle Digital
<https://siecledigital.fr> › Cybersécurité

Paris : la maternité Les Bluets victime d'une attaque informatique

20 oct. 2022 — La maternité parisienne des **Bluets** a publié un communiqué, lundi 17 octobre 2022, pour annoncer avoir subi une attaque informatique le dimanche ...

Le Parisien
<https://www.leparisien.fr> › paris-75 › a-paris-la-maternite...

À Paris, la maternité des Bluets victime d'une cyberattaque ...

19 oct. 2022 — Un piratage revendiqué et signé par « Vice Society », un groupe de hackers qui s'en est déjà pris au système informatique du **centre hospitalier** ...

TF1 Info
<https://www.tf1info.fr> › Nouvelles technologies

REPORTAGE - 10 jours après une cyberattaque, cette ...

21 oct. 2022 — L'hôpital Pierre Rouquès-Les **Bluets**, à Paris, a été victime d'une **cyberattaque**, dimanche 9 octobre. Les pirates ont prélevé des données, ...



L'accompagnement ESEA

La cellule Cybersécurité Nouvelle-Aquitaine

Sensibilisation

- Webinaires thématiques, cyber-mardi, ateliers, crise..

Information

- Veille technique et relai des dispositifs de soutien financier (AAP).

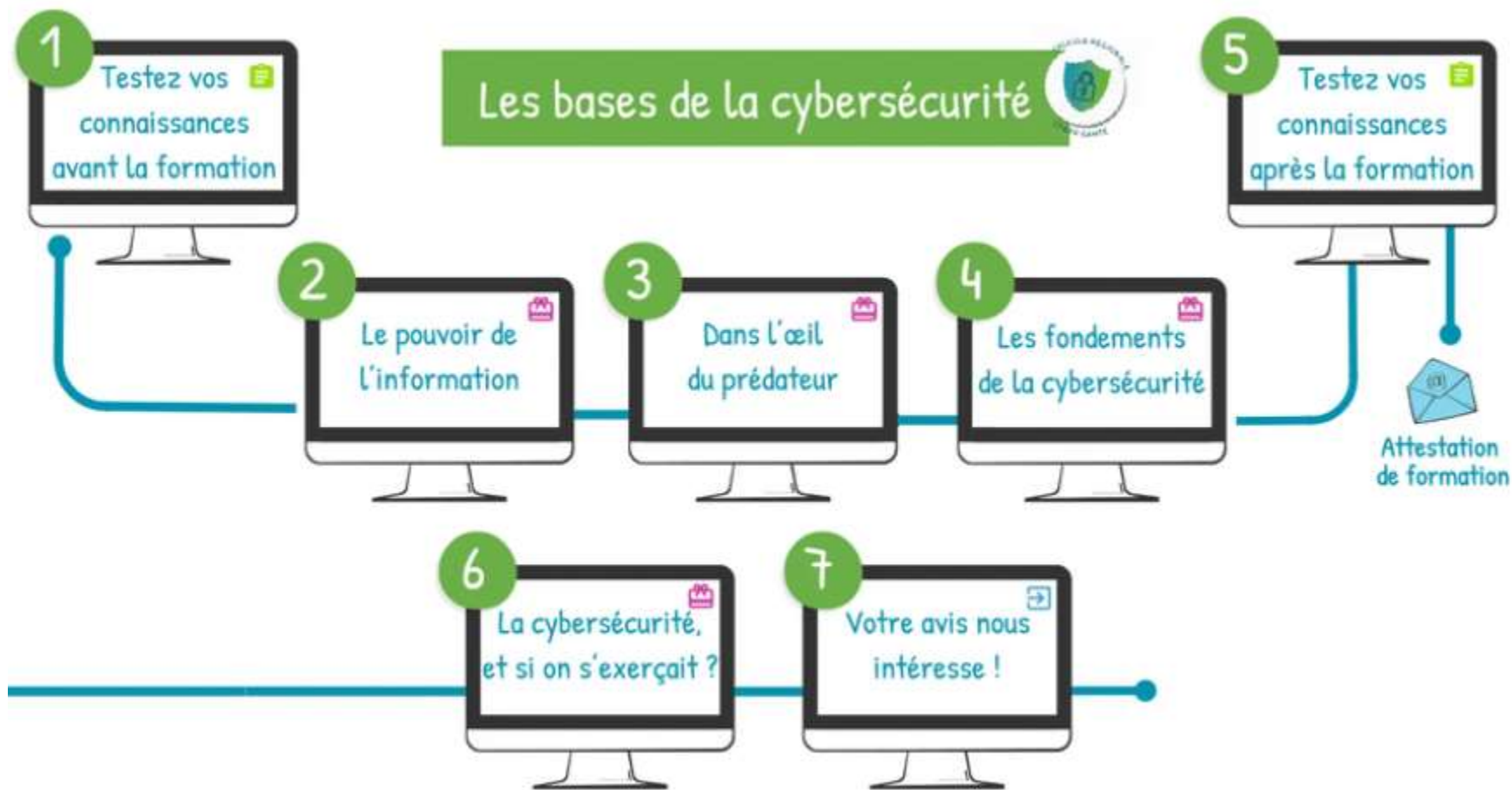
Formation

- Création et mise à disposition de contenus de formation numériques, mise à disposition d'outils pédagogiques personnalisables.

Aide à l'amélioration

- Conseils, exercices de crise, audits, outils, services (espace SSI, phishing), etc.

Présentation du parcours de formation





Merci pour
votre attention

- <https://www.esea-na.fr/programme/cybersecurite>
 - Formulaire de demande
- cybersecurite@esea-na.fr

Retrouvez nos actualités sur notre nouveau portail
www.esea-na.fr

et suivez-nous sur

