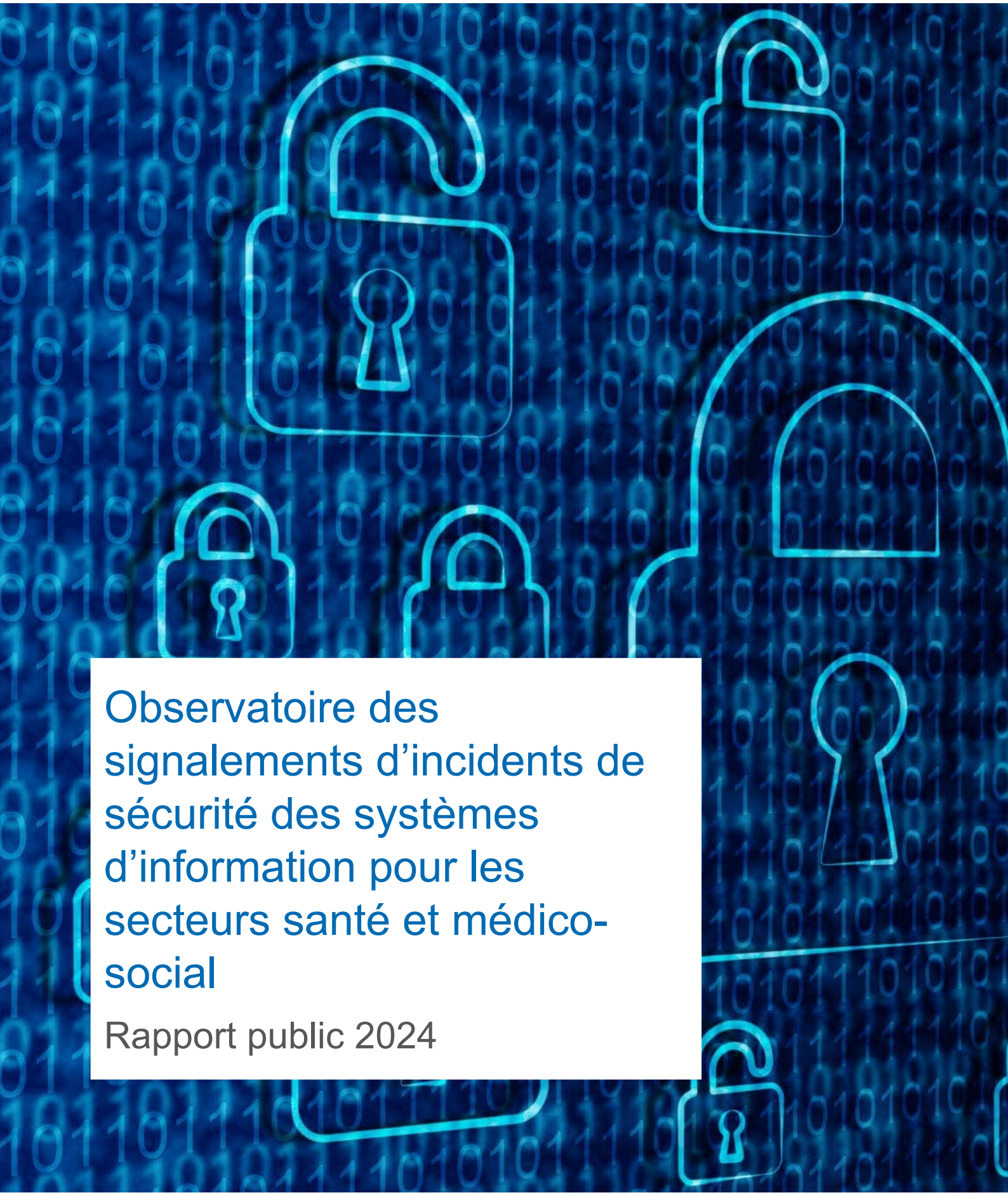
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

CERT Santé



Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social

Rapport public 2024

SOMMAIRE

TABLE DES FIGURES

1 INTRODUCTION

L'observatoire du CERT Santé permet chaque année de partager l'évolution de la menace cyber et la qualité de la réponse collective. Si l'année 2024 a été marquée par une augmentation significative du nombre de signalements, le principal constat réside dans la poursuite de la baisse du nombre d'incidents ayant eu un impact majeur sur la continuité des soins.

Ces deux tendances, au premier abord antagonistes, traduisent deux réalités opérationnelles :

- la chaine d'alerte est connue par de plus en plus d'établissements, et notamment ceux du secteur médico-social ;
- même s'il reste amplement perfectible, le niveau de sécurité des établissements de santé s'est amélioré ces derniers mois.

A notre sens, cette amélioration est multifactorielle :

- Les établissements de santé connaissent mieux les faiblesses de la partie exposée de leurs systèmes d'information et y remédient.
  La possibilité donnée par l'ANSSI à tous les établissements de santé d'utiliser son service SILENE, les nombreux audits de Cybersurveillance délivrés par le CERT Santé ou encore les audits de surface réalisés dans le cadre du Domaine 1 du programme CaRE ont permis d'identifier les vulnérabilités exposées qui constituent autant de portes d'entrée potentielles pour les cyberattaquants. Un grand nombre d'entre elles auront ainsi été corrigées par les équipes informatiques des établissements en s'appuyant pour partie sur l'incitation budgétaire apportée par le premier appel à financement CaRE ;

- Les établissements commencent à s'exercer face au risque cyber.
  La réalisation massive d'exercices de crise par les établissements de santé a permis à leurs équipes de se familiariser avec les procédures à suivre en cas d'attaque. Cela améliore leur capacité à réagir rapidement et efficacement, minimisant ainsi les impacts sur les opérations hospitalières ;

- Le CERT Santé a amélioré sa veille pro-active.
  La veille pro-active menée par le CERT Santé a fortement évolué en 2024, autant sur son efficience que sur son périmètre. Elle concerne à présent les vulnérabilités majeures, les campagnes d'exploitation ou encore les fuites d'identifiants et le délai d'alerte a été grandement diminué. Ces efforts seront poursuivis en 2025.

- Le CERT Santé s'est investi particulièrement dans le champ de la prévention, dans un contexte de surexposition de la France à l'occasion de l'organisation des JOP de Paris : animation de webinaires de sensibilisation, organisation d'exercices de gestion de crise et réalisation d'audits de l'exposition sur Internet.

Si l'on peut se réjouir de cette tendance, le CERT Santé continue de constater auprès des établissements de santé et médico-sociaux qu'il accompagne dans la réponse à incident, des manques récurrents :

- la carence en cartographie des systèmes d'information qui rend complexe la prise de décision en cas de crise du fait d'une absence de visibilité sur les impacts de celle-ci ;
- des faiblesses en matière de gestion des droits d'administration sur les différentes briques constituantes des systèmes d'information ;
- une protection des sauvegardes insuffisante au regard de l'importance de son rôle de dernier rempart ;
- une insuffisante sécurisation et surveillance des accès distants aux systèmes d'information ;
- l'absence de documentation des processus de continuité d'activité permettant aux métiers de délivrer les soins en conditions dégradées ;
- l'usage de moyens d'authentification inadaptés aux enjeux de sécurité portés par les systèmes d'information auxquels ils permettent d'accéder ;
- une mauvaise identification du responsable du maintien en conditions de sécurité de certains équipements, en résulte l'exposition de vulnérabilités ;
- le manque de compétences informatiques internes dans les établissements de petite taille constitue un frein dans la bonne compréhension de la menace sur la sécurité des systèmes d'information par leurs dirigeants et dans la capacité à mettre en œuvre rapidement et correctement les mesures de confinement qui s'imposent. Pour ces établissements, l'adossement à une structure suffisamment dimensionnée ou encore le déploiement de ressources compétentes via mutualisation semblent indispensables.

Les attaques par rançongiciel, principalement à des fins d'extorsion, ont continué à mobiliser le CERT Santé en 2024 avec un nombre d'incidents de ce type comparable à l'année passée. Le déploiement de ces rançongiciels est souvent liée à l'utilisation d'infostealers dans les chaînes d'infection. Déployés massivement, ces programmes malveillants permettent de voler des identifiants sur le poste de travail de la victime. Ces derniers sont ensuite revendus sur des forums ou par le biais de canaux de communications privés, puis réutilisés par d'autres attaquants. De nombreux

mécanismes incitant les utilisateurs à installer ce type de programme ont été découverts en 2024, menant à une forte augmentation du risque lié à ce vecteur de compromission.

Si le travail à mener est encore très important, les efforts collectifs commencent à payer.

Bonne lecture.

L'équipe du CERT Santé

2 DISPOSITIF DE TRAITEMENT DES SIGNALEMENTS DES INCIDENTS DE SECURITE DES SYSTEMES D'INFORMATION POUR LE SECTEUR SANTE

2.1 Contexte réglementaire et organisationnel

En application de l'article L. 1111-8-2 du code de la santé publique, les établissements de santé, les hôpitaux des armées, les centres de radiothérapie et les laboratoires de biologie médicale doivent déclarer leurs incidents de sécurité des systèmes d'information à l'Agence du numérique en Santé (ANS). Depuis le 18 novembre 2020, cette obligation a été étendue aux établissements médico-sociaux par ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé (ARS).

Le décret d'application n°2022-715 du 27 avril 2022 précise le rôle et les missions de l'ANS, en particulier son périmètre d'intervention en matière d'appui à la réponse à incident et les actions de prévention.

Ces missions sont portées au sein de l'ANS par le CERT Santé, premier CERT sectoriel en France ayant intégré en janvier 2021 l'InterCERT FRANCE. L'InterCERT FRANCE est une association loi 1901 qui constitue la première communauté de CSIRT[1] en France. Le CERT Santé coopère avec les autres CSIRT/CERT dans l'analyse des menaces de cybersécurité et partage ses retours d'expérience. Il bénéficie régulièrement de l'activité de veille des membres de la communauté (indicateurs de compromission, fuite d'identifiants, etc…).

2.2 Présentation des activités

Le dispositif de traitement des signalements des incidents de sécurité des systèmes d'information constitue un élément important de la stratégie d'amélioration du niveau de sécurité numérique du secteur santé portée par le ministère des solidarités et de la santé, en coordination étroite avec les autorités gouvernementales en charge de la cybersécurité.

[1] Computer Security information Response Team

Sa mise en œuvre opérationnelle s'appuie sur le CERT Santé de l'Agence du Numérique en Santé depuis sa création en 2017.

Mise à disposition d'un portail de signalement et proposition d'un appui

L'accompagnement et l'appui mis en place par le CERT Santé dans le cadre de leur signalement consiste à :

- Traiter le signalement sur le portail des signalements des évènements sanitaires indésirables et notifier au déclarant sa prise en compte ;
- Analyser et qualifier le signalement pour le compte des autorités compétentes ;
- Apporter, si besoin, un accompagnement dans le traitement de l'incident de sécurité des systèmes d'information ;
- Diffuser une alerte vers le ministère de la santé et de l'accès aux soins et/ou les autorités compétentes de l'Etat selon la nature de l'incident :
    - la Délégation au Numérique en Santé, pour assurer la communication et l'information du cabinet ministériel sur l'avancement de la gestion de l'incident ;
    - le fonctionnaire de sécurité des systèmes d'information des ministères sociaux (FSSI) pour assurer la cohérence des actions de remédiation menées à l'échelle locale par les bénéficiaires avec les procédures définies au niveau national, ainsi que la qualité des services rendus par les éventuels PRIS ou prestataires mobilisés ;
    - la direction générale de la santé (DGS) via le CORRUSS (Centre opérationnel de réception et de régulation des urgences sanitaires et sociales), dans le cas d'un incident ayant un impact sanitaire ;
    - à l'ANSSI, en cas d'incident concernant une structure relevant de dispositifs spécifiques (Opérateur de Service Essentiel, ou en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs.

Le CERT Santé apporte son appui aux structures dans le cadre de la réponse à un incident :

- proposition des mesures de confinement complémentaires au cours d'un premier entretien (isolation des sauvegardes, restriction des flux entrants/sortants, isolation de l'Active Directory[2], désactivation massive de comptes, etc…) ;

[2] L'**Active Directory** (**AD**) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

- assistance à l'identification de la menace et du scénario complet de la compromission (Collecte et analyse de journaux d'évènements et de preuves numériques, analyse de codes malveillants, de fichiers infectés, recherche du « patient 0 » de l'attaque, etc…) ;
- proposition de mesures de remédiation adaptées (désinfection des systèmes compromis, suppression des fichiers malveillants, correction des vulnérabilités exploitées, etc…) et mise à disposition de fiches réflexes (ex : rançongiciel, compromission de comptes de messagerie, DDoS) ;
- orientation vers un prestataire cyber, principalement dans le cas d'un incident majeur nécessitant une reconstruction partielle ou totale de l'architecture de sécurité du SI.

Le CERT Santé propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité (notamment dans le cadre d'une procédure de durcissement post-incident) :

- Proposition et fourniture d'un avis sur des plans d'action sécurité
  - priorisation des mesures proposées (ex : renforcer le cloisonnement réseau du SI support d'activités de soins vitaux) ;
  - propositions pour améliorer la sécurité du SI (ex : utilisation d'une application pour l'administration locale ou pour limiter l'exploitation de vulnérabilités).
- Proposition de solutions pour renforcer la sécurité (configuration des systèmes, solutions concrètes de sécurisation des sauvegardes, des hyperviseurs, de l'administration, du cloisonnement réseau, etc.) basées sur les guides de l'ANSSI.

Le traitement des incidents reste la responsabilité des structures déclarantes.

Permanence 24/7

Depuis octobre 2022, le CERT Santé a étendu son service de réponse à incident aux heures non ouvrées et est **donc accessible 24h/24 et 7j/7**. Sur cette plage horaire, une astreinte est joignable au 09 72 43 91 25 pour apporter un appui dans la qualification de l'incident et la mise en œuvre de mesures permettant de stopper la propagation d'une activité malveillante au sein du système d'information d'un bénéficiaire du CERT Santé.

Publication d'alertes sur la menace cyber et partage de bonnes pratiques

Au travers du portail cyberveille-santé dédié à la sécurité du numérique en santé, le CERT Santé :

- informe les structures de santé concernant des vulnérabilités ou des dysfonctionnements majeurs de dispositifs médicaux, des technologies de santé ou des technologies standards (système d'exploitation, suite bureautique, base de données, etc.) ;
- alerte les structures de santé concernant des actes de cyber-malveillance en cours de réalisation (campagne de messages électroniques malveillants, vols de données, etc.) ;
- apporte un appui méthodologique aux structures dans la gestion de la sécurité et des incidents (mise à disposition de fiches réflexes, de fiches pratiques et de guides de bonnes pratiques).

Veille proactive

Depuis 2020, le CERT Santé alerte en direct par message électronique les établissements de santé (ES) ou les établissements et services médico-sociaux (ESMS) concernant :

- la présence d'une ou plusieurs vulnérabilités critiques sur leur(s) outil(s) et système(s) exposé(s) sur Internet et faisant l'objet de campagne d'exploitation ;
- la compromission potentielle ou avérée de comptes de messagerie ou de comptes d'accès à distance sur des machines exposées sur Internet ;
- les services sensibles exposés sur Internet (RDP, DICOM, etc.).

Cette activité d'alerte est réalisée en étroite coopération avec le CERT-FR de l'ANSSI. Pour les machines concernées, ces alertes précisent l'adresse IP, le nom de domaine et le ou les services.

Service de cybersurveillance

L'audit de cybersurveillance est un service de diagnostic et d'évaluation de la sécurité du système d'information vis-à-vis d'Internet (service national de cybersurveillance). Le service de cybersurveillance consiste en un audit des domaines et sous-domaines exposés sur Internet déclarés par la structure

Le service de cybersurveillance permet, pour un périmètre de domaines exposés sur Internet défini, de :

- cartographier et déterminer la surface d'attaque d'un système d'information ;

- détecter de manière pro-active les vulnérabilités qui affectent le système d'information.

L'audit se déroule en deux phases :

- la collecte d'informations à partir de sources ouvertes sur Internet ;
- la réalisation d'un audit de chacun des domaines du système d'information de la structure. Cette phase comprend :
  - une cartographie des services et des ressources accessibles ;
  - l'utilisation de scanneurs généralistes / spécifiques afin de détecter d'éventuelles erreurs de configuration et / ou des défauts de mise à jour ;
  - le test des comptes avec des identifiants faibles et des identifiants par défaut.

Une fois le diagnostic réalisé, un rapport d'audit est fourni à la structure auditée dans des délais courts afin de lui permettre de rapidement mettre en place les éventuelles mesures de remédiation.

Le périmètre de l'audit ainsi que les attendus du rapport sont présentés sur le portail cyberveille-santé[3].

Animation de la communauté « CERT Santé »

Le CERT Santé anime un salon Tchap au sein duquel les RSSI, les DSI et les acteurs étatiques de la cybersécurité en santé peuvent échanger entre eux sur :

- l'état de la menace ;
- des bonnes pratiques et la mise en œuvre de solutions ;
- les actions ministérielles visant à encadrer et à accompagner les acteurs dans la mise en œuvre de la sécurité numérique.

Cet espace sécurisé a vocation à faciliter les échanges autour de la cybersécurité entre les acteurs du secteur santé.

Améliorer la sécurité de la messagerie

L'utilisation de courriels malveillants (technique de l'hameçonnage par exemple ou pièce jointe malveillante) est très développée par les attaquants pour chercher à compromettre un SI. Ainsi, dans le cadre des actions de prévention en vue des JOP de Paris, le CERT Santé a audité 184 établissements impliqués dans cet évènement en leur proposant un service de contrôle automatique des règles de sécurité de leurs serveurs de messagerie.

[3] https://cyberveille-sante.gouv.fr/cybersurveillance

3 Synthèse de l'activité en 2024

Le nombre total d'incidents déclarés (749 signalements) a fortement augmenté par rapport à 2023 (581). Cette augmentation est principalement dû à des incidents d'origine non malveillante comme le dysfonctionnement de solutions largement déployées (CrowdStrike Falcon) mais également à des incidents d'origine malveillante impactant certains prestataires de services métier communs à plusieurs établissements.

Parmi les 558 établissements ayant déclaré au moins un incident, soit une augmentation de 21% du nombre de déclarants par rapport à 2023, 75 ont bénéficié d'un appui technique de la part du CERT Santé.

Le ratio plus faible des incidents d'origine malveillante (44%) malgré l'augmentation du nombre d'incidents déclarés peut être expliqué par les éléments suivants :

- La sécurité de l'exposition sur internet des établissements de santé qui progresse (une forte impulsion a été donnée[4] par le programme CaRE dans le cadre du Domaine D1) ;
- Une bonne prise en compte des alertes transmises en direct par mail par le CERT Santé, en particulier lorsque des fuites d'identifiants de comptes à distance ont été identifiées.

La menace rançongiciel reste la plus importante en 2024 en termes d'impact sur le SI. Le nombre d'incidents lié à cette menace est en hausse de 28% par rapport à 2023 et concerne majoritairement des ES publics et des ESMS. Le chiffrement des données était régulièrement précédé d'une exfiltration faisant l'objet d'une mise en vente sur Internet. Ces établissements ont été contraints de mettre en place un mode de fonctionnement dégradé qui a pu s'étendre sur plusieurs semaines.

- une plus grande activité hospitalière avec un nombre important d'interconnexions avec l'extérieur impliquant une plus grande exposition ;
- les établissements de santé publics étant mieux sensibilisés à la déclaration des incidents d'origine cyber que les établissements privés, il est possible que le nombre d'incidents les concernant soit plus proche de la réalité, comparé aux établissements privés.

[4] Arrêté du 18 mars 2024 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé - Fonction « Annuaires techniques et exposition sur internet » - Légifrance (legifrance.gouv.fr)

Le nombre d'incidents ayant un impact sur la prise en charge des patients est en augmentation par rapport à 2023 (de 13%). En effet, 230 signalements reçus en 2024 indiquent que les établissements ont été contraints de passer en mode dégradé ou d'interrompre la prise en charge des patients soit 31% des signalements reçus. Seuls 19% de ces incidents ont une origine malveillante, les 3 causes principales étant la perte de lien télécom, un bug applicatif généralement sur le DPI ou un dysfonctionnement de l'infrastructure locale ou du prestataire.

L'année 2024 a également été marquée par une diminution du nombre d'incidents majeurs.

Ceci peut s'expliquer comme suit :

- un service de veille pro-active du CERT Santé plus efficace avec l'envoi d'alertes dans des délais très courts suite au lancement de la campagne d'exploitation ;
- un plus grand nombre d'établissements a réalisé un audit de l'exposition sur Internet et réduit sa surface d'attaque ;
- de nombreux établissements de santé ont réalisé en 2024 des exercices de crise[5] ;
- une capacité organisationnelle et technique des établissements de santé à réagir plus vite, dès la détection qui s'illustre par : des points de contact dans la plupart des établissements, des équipes opérationnelles, et une capacité à mettre à jour les infrastructures dans des délais très courts.

Enfin, le CERT Santé est intervenu en 2024 auprès de 4 prestataires de solutions métier à la suite de l'identification de vulnérabilités présentes sur des serveurs exposés sur Internet. Ces vulnérabilités ont été identifiées soit lors d'un audit de cybersurveillance, soit lors de la réponse à un incident. Le CERT Santé a pu accompagner certains éditeurs dans la correction des vulnérabilités ainsi que dans le renforcement de la sécurité de leur application et de leur infrastructure.

4 OBSERVATOIRE DES SIGNALEMENTS

4.3 Chiffres clés pour la période 2023-2024

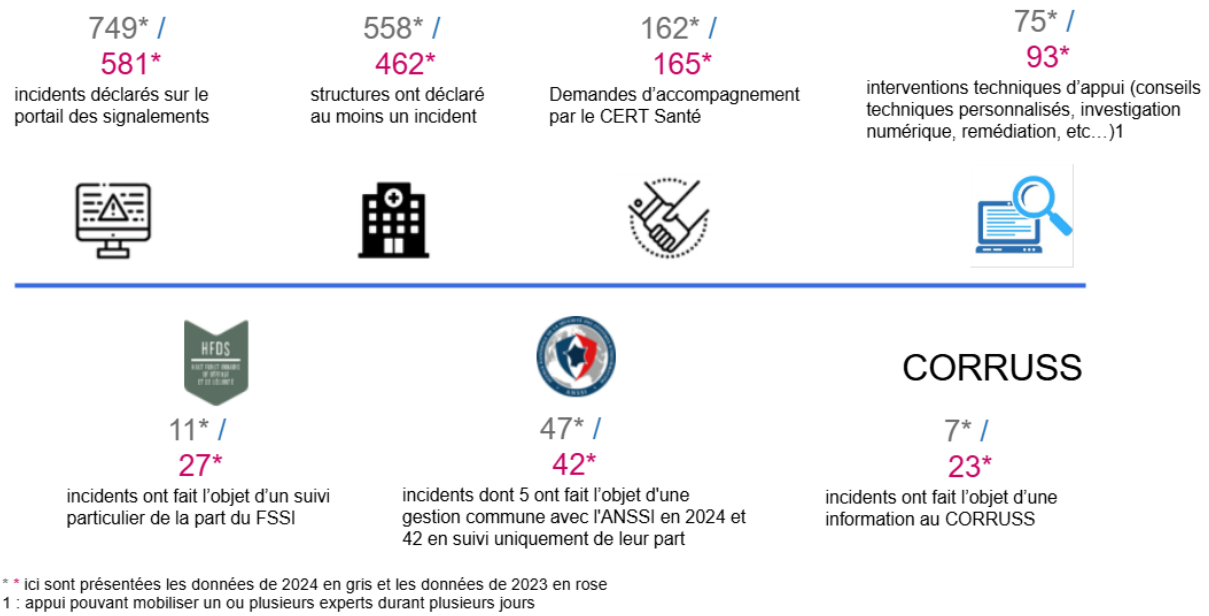


Figure 1 – Chiffres clés des signalements déclarés en 2023 et 2024

En coordination avec le CERT Santé, l'ANSSI et le FSSI sont intervenus directement au profit de 49 établissements, dans le suivi de la gestion d'un incident ou l'appui à la réponse. Certaines structures ont bénéficié de plusieurs interventions et le FSSI est intervenu auprès de certains prestataires sectoriels.

Pour **l'ANSSI** il s'agit de :

- Vingt-sept établissements de santé publics, dont 14 opérateurs de services essentiels (OSE). Ces incidents étaient liés à des attaques par rançongiciel, des compromissions de comptes (AD, VPN ou messagerie), l'exploitation de vulnérabilités sur des équipements de sécurité ou des dysfonctionnements graves de systèmes critiques ;
- Quinze établissements de santé privés, trois établissements de service médico-sociaux et deux autres types de structure victimes de rançongiciels, de compromission de comptes (AD, VPN ou messagerie), de dysfonctionnements d'infrastructures, de perte de lien télécom et de défiguration de site.

Pour le FSSI, il s'agit de :

- neuf établissements dont 3 OSE. Ces incidents étaient liés à des attaques par rançongiciel, DDoS, exfiltration de données et au dysfonctionnement d'un système critique.

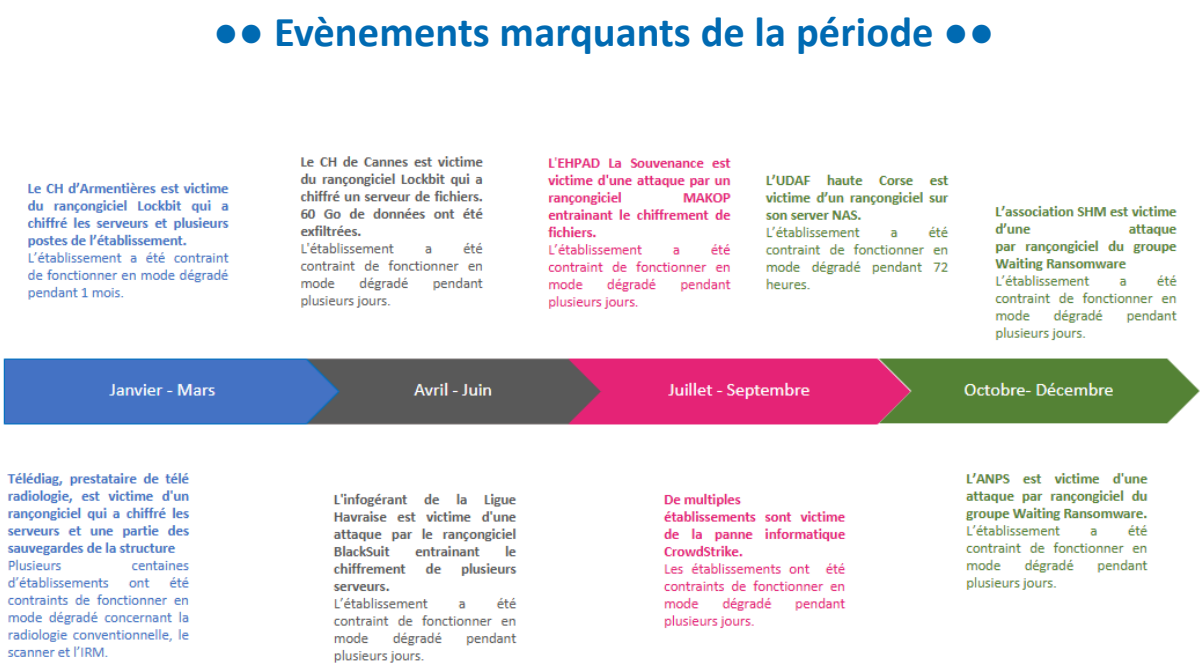


Figure 2 – Evènements marquants de l'année 2024

4.4 Informations générales sur les signalements

749 incidents ont été déclarés en 2024. Ce nombre est en forte augmentation par rapport à 2023 (581). Pour mémoire, 591 incidents avaient été déclarés en 2022.

Parmi ces incidents, on compte des incidents « hors périmètre » (22 au total). La majorité des incidents non traités par le CERT Santé sont des incidents ne concernant pas un système d'information support d'une activité sanitaire ou médico-sociale. On comptabilise également dans cette catégorie les exercices de crise cyber qui intègrent une déclaration de l'incident au CERT Santé (12).

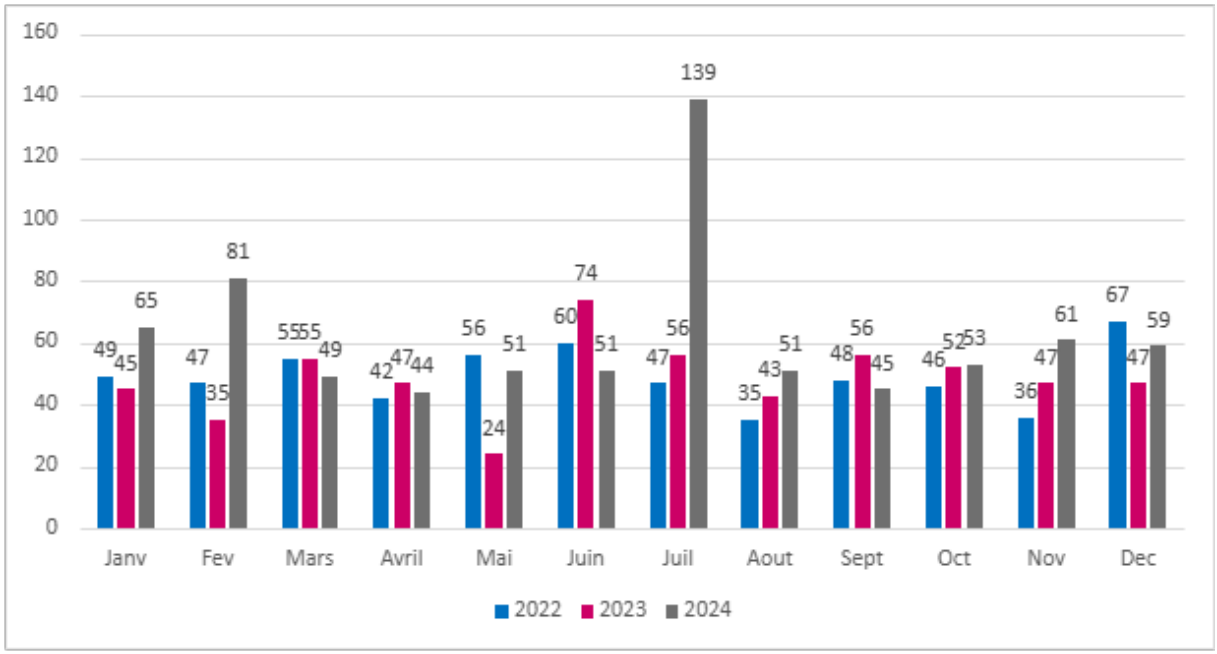


Figure 3 - Nombre de signalements par mois

On compte en 2024 une moyenne de **62 déclarations par mois** (48 en 2023).

●● Répartition des signalements selon l'horaire et le jour de leur dépôt ●●

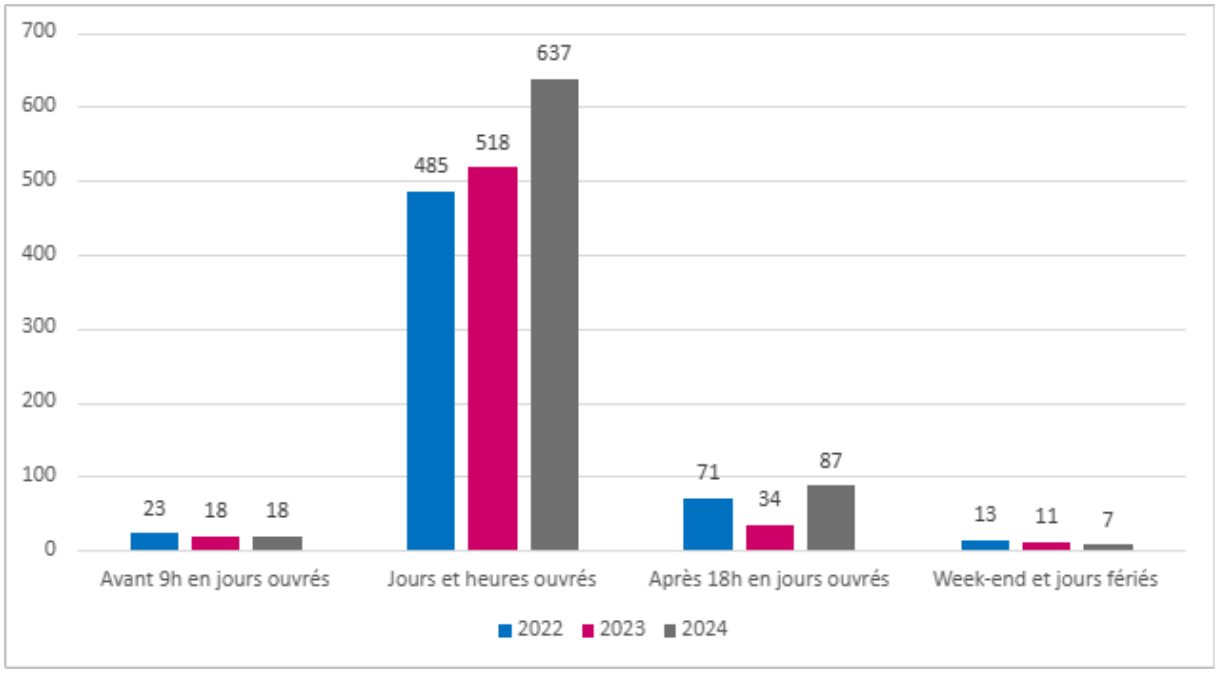


Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt

85% des signalements ont été effectués en heures et jours ouvrés (HO/JO) en 2024, entre 9h et 18h, en légère baisse (7%) par rapport à 2023. On constate une augmentation significative de la part des incidents déclarés après 18h en jours ouvrés. La part des incidents déclarés entre 18h et 18h30, comme en 2023, est toujours supérieure à celle des incidents déclarés après 20h.

Ce sont principalement des structures publiques qui sont à l'origine des déclarations en HNO/JNO sur le portail des signalements. Dix-neuf demandes d'accompagnement ont été formulées durant ces périodes. Parmi celles-ci, sept structures (un établissement de santé public, un établissement de santé privé d'intérêt collectif (ESPIC), un établissement de santé non PSPH, deux ESMS et deux EHPAD) nécessitaient un appui à la suite d'attaques par rançongiciel entraînant un fonctionnement dégradé des activités support ou du système de prise en charge des patients, à des compromissions de comptes AD ou de messagerie, ou à des exploitations de vulnérabilités.

35 incidents ont été pris en charge en 2024 par **l'astreinte du CERT Santé** à la suite d'un appel téléphonique en HNO. 4 ont fait l'objet d'un appui technique en heures ouvrées.

Il est nécessaire de prendre en compte que la déclaration formelle d'un incident au CERT Santé n'est néanmoins pas toujours opérée par le même service que celui responsable de sa détection. Aussi, il n'y a pas de corrélation directe entre l'horaire de détection d'un incident et celui de sa déclaration.

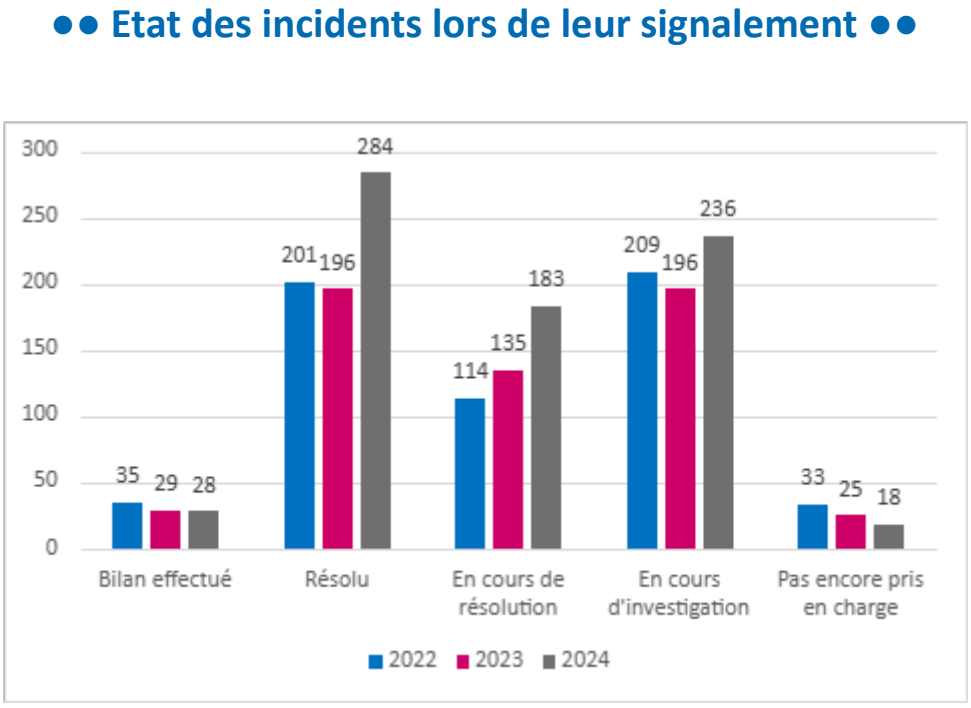


Figure 5 - Etat des incidents lors de leur signalement

En 2024, plus de la moitié des incidents sont résolus ou en cours de résolution par la structure avant leur déclaration. La part des incidents pour lesquels le CERT Santé a été sollicité pour des actions d'investigation et d'aide à la remédiation a également augmenté cette année, pour atteindre **31%.**

32 structures n'ont pas transmis d'information complémentaire à la suite de leur déclaration, malgré une demande de compléments et/ou une proposition d'appui**. Ce chiffre est en augmentation rapport à 2023**. **35% de ces incidents étaient**

potentiellement d'origine malveillante (compromission de boites de messagerie ou exploitation de vulnérabilités) contre 20% en 2023.

22%

C'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2024**. Il est **inférieur à celui de 2023**.

Un accompagnement est demandé lors d'incidents ayant un impact important sur l'activité de la structure ou lorsqu'un évènement remonté par les équipements de sécurité du SI laisse présager une compromission potentielle. La structure veut s'assurer qu'elle a bien entrepris l'ensemble des actions recommandées tant en matière d'investigation que de remédiation. **La principale demande d'appui concerne la gestion des attaques virales et la compromission des systèmes**.

De nombreuses structures sollicitent le CERT Santé pour intervenir auprès de prestataires lorsque ces derniers sont à l'origine de l'incident (panne réseau, dysfonctionnement applicatif) et ne sont pas suffisamment réactifs dans la mise en place de solutions de remédiation.

●● Répartition des signalements selon la localisation de la structure●●

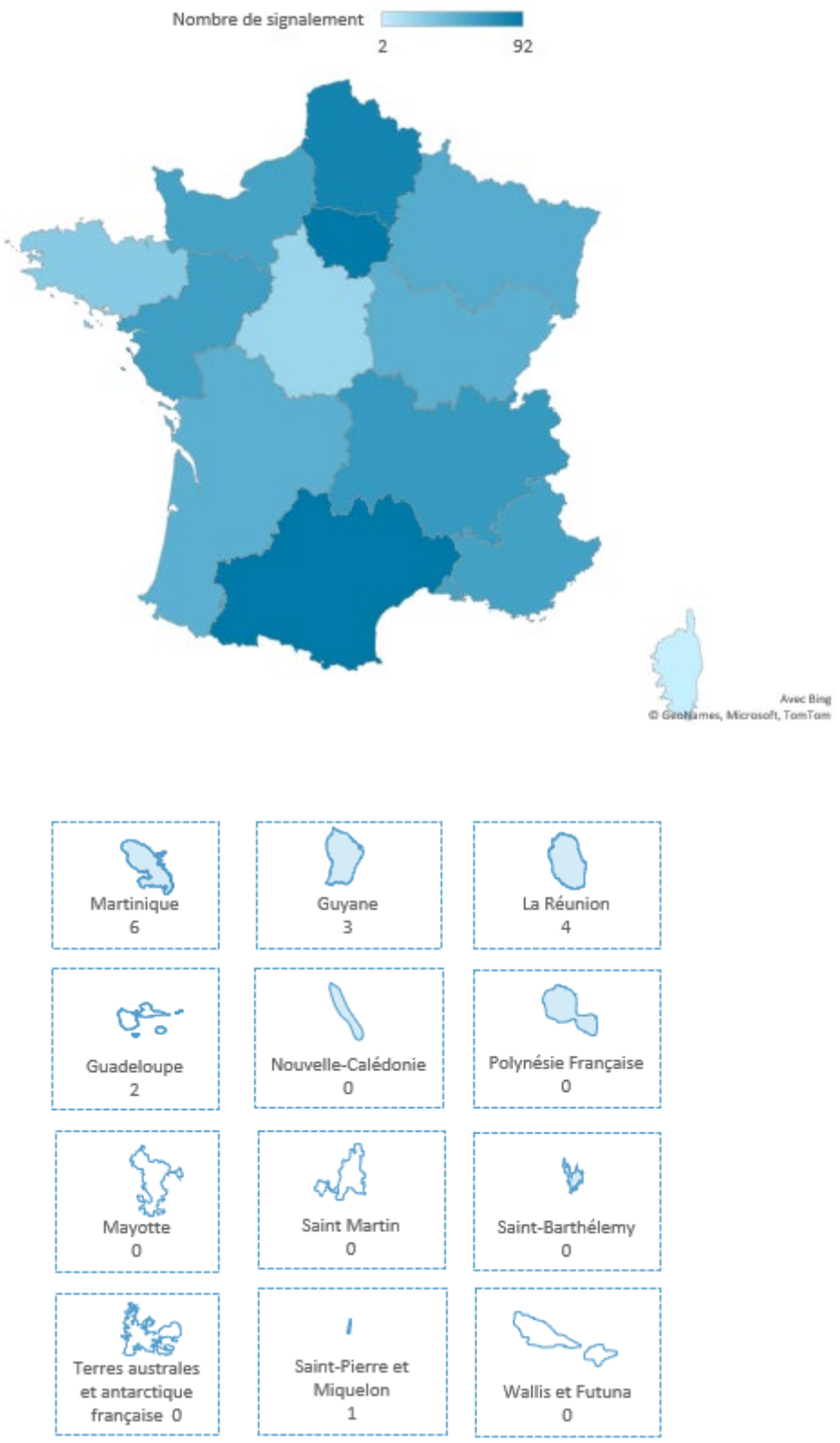


Figure 6 - Répartition des signalements par région

Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social (2024)

Les régions pour lesquelles le nombre de signalements est le plus important sont l'Occitanie (92), l'Ile-de-France (91) et les Hauts-de-France (83). Ces trois régions représentent à elles seules plus de 36% du total des signalements.

●● Nombre de signalements rapporté à l'activité hospitalière des régions ●●

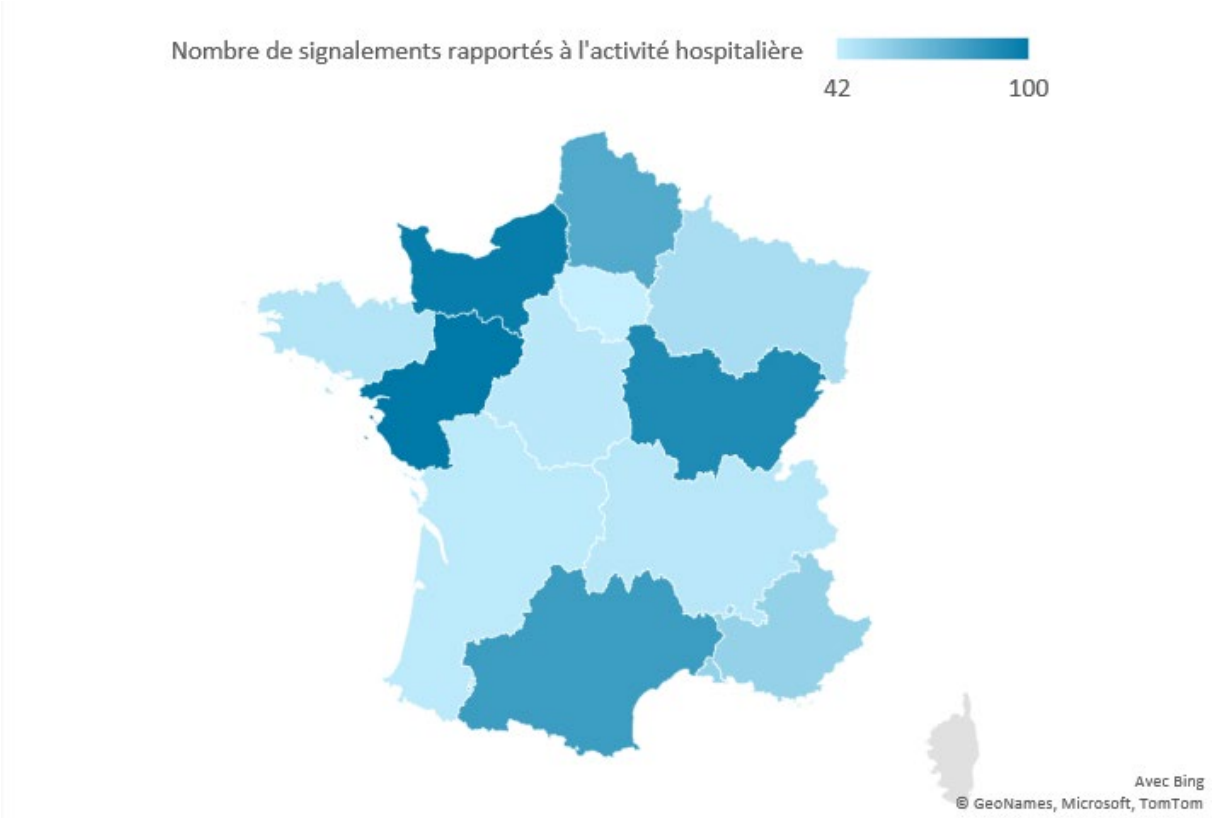


Figure 7 - Nombre de signalements rapporté à l'activité hospitalière des régions

Cette carte présente le ratio entre le nombre de signalements et l'activité hospitalière rapportée au niveau national[6] : plus une région a un nombre de signalements élevé par rapport à son activité sanitaire, plus celle-ci est foncée. Les DOM-COM n'ont pas été pris en compte dans cette analyse à cause du faible taux d'activité hospitalière par

[6] INSTRUCTION N° DGOS/PF5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme HOP'EN - Légifrance

rapport à la métropole. La région avec le ratio le plus élevé (Pays de la Loire) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (5,1% de l'activité nationale), la région Pays de la Loire est en tête en matière de remontée des incidents. La région Normandie arrive en deuxième position. La région Bourgogne-Franche-Comté arrive en troisième position.

En revanche, la région Ile de France déclare peu d'incidents au regard du nombre d'établissements hospitaliers situés sur ce territoire de santé.

Il est nécessaire de rappeler à toutes les structures de santé l'obligation de déclaration des incidents de sécurité, en particulier dans les régions où le nombre de signalements rapporté à l'activité hospitalière est faible.

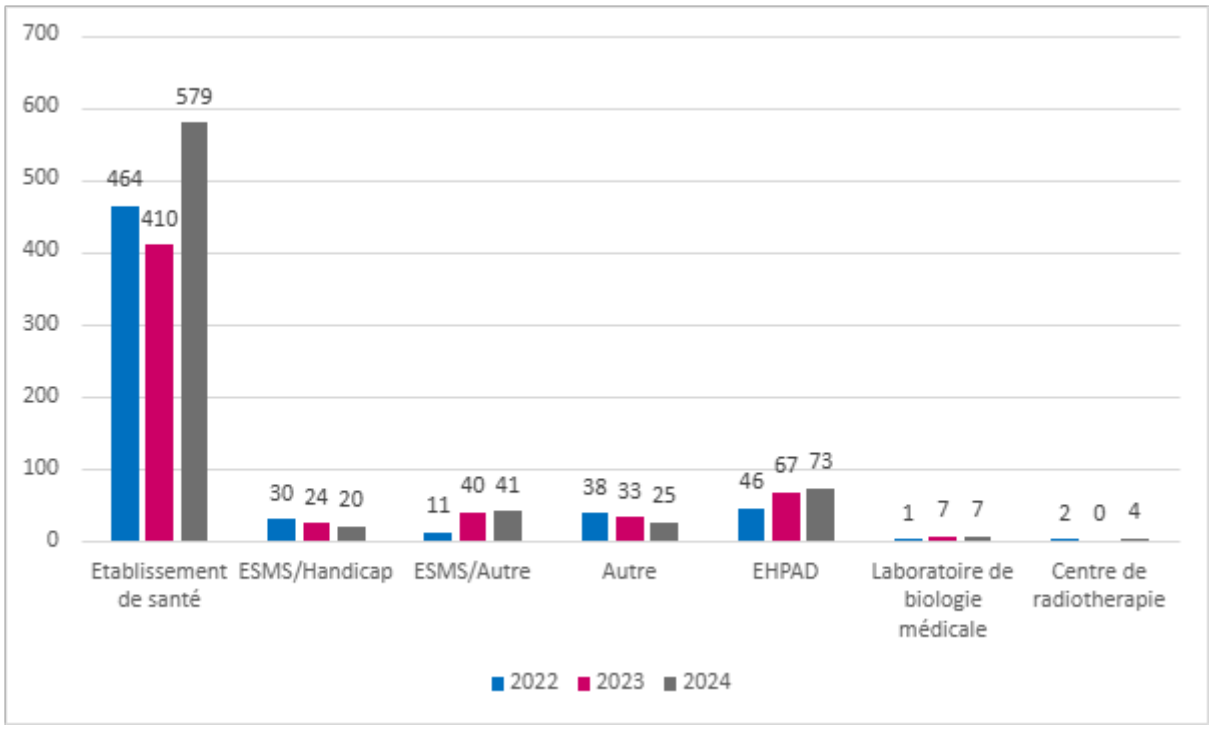


Figure 8- Répartition des signalements selon le type de structure

La grande majorité (77%) des incidents de sécurité est déclarée par les **établissements de santé** (voir détail figure 8).

●● Part des signalements comparée à la part des établissements de santé selon la nature de la personne morale (nombre d'entités juridiques et activité combinée) ●●

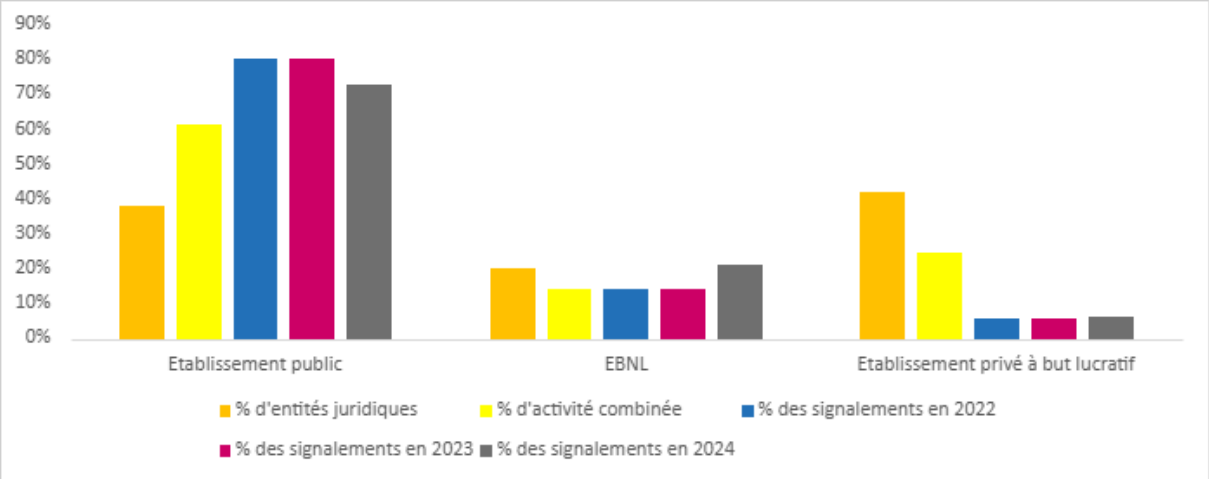


Figure 9 - Part des signalements comparée à la part des établissements selon leur raison sociale

10

Les parts des types d'établissements dans la déclaration des incidents en 2024 sont stables par rapport à 2023. Les ES publics déclarent toujours le plus d'incidents (73%) alors qu'ils ne sont que 35% des entités juridiques. Ce constat peut être expliqué comme suit :

- les établissements de santé publics sont régulièrement sensibilisés à la déclaration des incidents d'origine cyber ;
- une plus grande activité hospitalière (61% de l'activité combiné), avec environ 70% du personnel hospitalier, portant beaucoup de collaborations (aspect universitaire, etc) et donc avec un nombre important d'interconnexions avec l'extérieur impliquant une plus grande exposition sur Internet.

77 établissements **désignés OSE** ont déclaré au moins un incident en 2024.

29 C'est le nombre de structures ayant déclaré plus de 2 incidents durant l'année 2024 sur 558 structures au total. Parmi elles, il y avait 27 établissements de santé et 2 établissements et services médico-sociaux. 15 établissements de santé ont signalé au moins 4 incidents.

●● Répartition des déclarations selon le type d'impact sur les données ●●

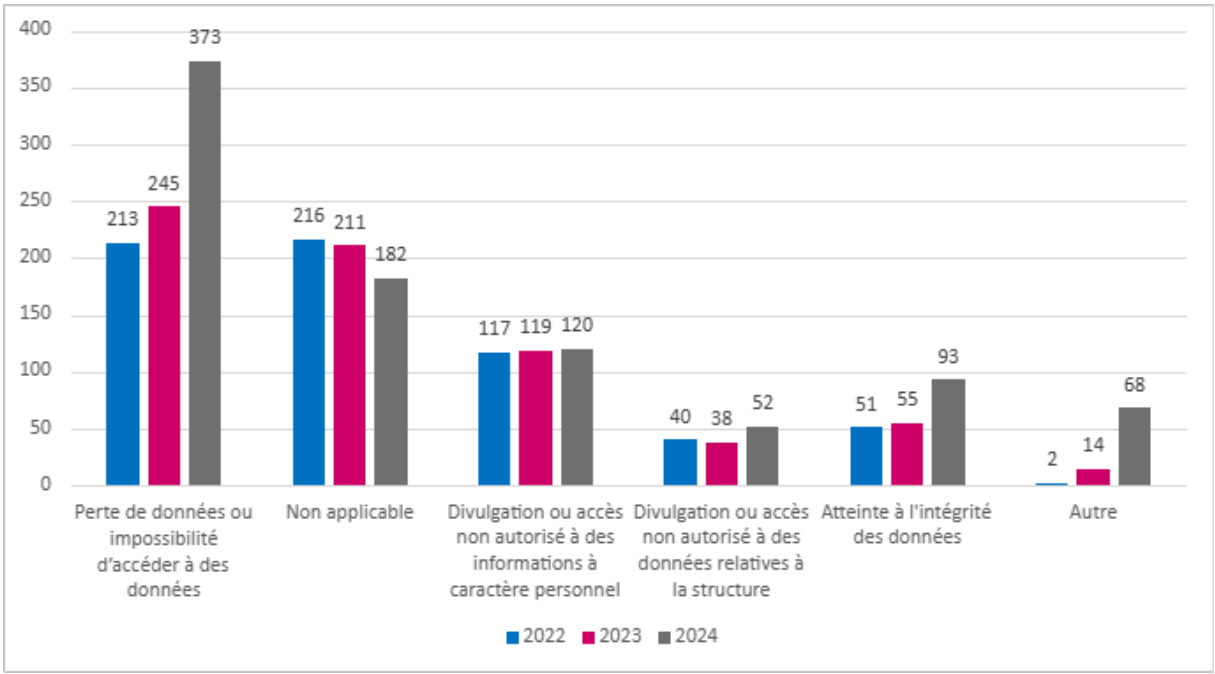


Figure 10- Répartition selon les types d'impact sur les données

En 2024, les incidents signalés où tout ou une partie des données des applications de la structure étaient devenues inaccessibles ont augmenté de 52% par rapport à 2023, principalement en raison d'incidents chez les fournisseurs de logiciels (Crowd Strike), fournisseurs de DPI mais également des cas fréquents de coupures de liens télécoms (qui concernent souvent des incidents côté FAI).

Pour 24% des signalements, les structures assurent qu'il n'y a eu aucun impact sur les données. On retrouve alors des incidents ayant pour origine des tentatives d'hameçonnage ou d'intrusion sur le SI, des attaques par ingénierie sociale ou bien encore des bugs applicatifs ou une perte du lien télécom.

De plus, le taux de divulgation ou d'accès non autorisé à des informations à caractère personnel et données relatives à la structure est resté stable par rapport à l'année précédente. Parmi ces cas, la majorité implique le vol d'authentifiant par des pratiques telles que l'hameçonnage, le harponnage ou la recherche de mot de passe par force brute, entraînant une compromission des comptes de messagerie et Active Directory, souvent utilisés pour des campagnes d'hameçonnage ultérieures, des tentatives de latéralisation ou d'élévation de privilèges. On observe une augmentation des cas de

fuite d'informations à la suite de l'exploitation de vulnérabilités sur des équipements exposés sur Internet ou par exfiltration de données lors d'attaques par rançongiciel.

51 % **C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2024. Ce chiffre est en légère baisse par rapport à 2023 et 2022.**

42 %

C'est le pourcentage de structures qui ont été contraintes de mettre en place en 2024 un **fonctionnement en mode dégradé** du système de prise en charge des patients (10% de plus qu'en 2023).

Ce mode dégradé dépend de la nature de l'incident et des procédures mises en place dans les structures : application du plan de continuité, utilisation du mode de fonctionnement papier pour gérer les patients, utilisation d'un poste dédié, mise en place de solutions de contournement pour prendre en compte les dysfonctionnements des logiciels de prescription, etc.

En moyenne, le mode dégradé a été mis en œuvre par les structures de santé pendant **une journée** mais certains établissements ont été confrontés à cette situation pendant plusieurs jours. **8%** des établissements ayant mis en place un mode dégradé ont subi une interruption du système de prise en charge d'un patient.

●● Répartition des déclarations selon le type de données impactées●●

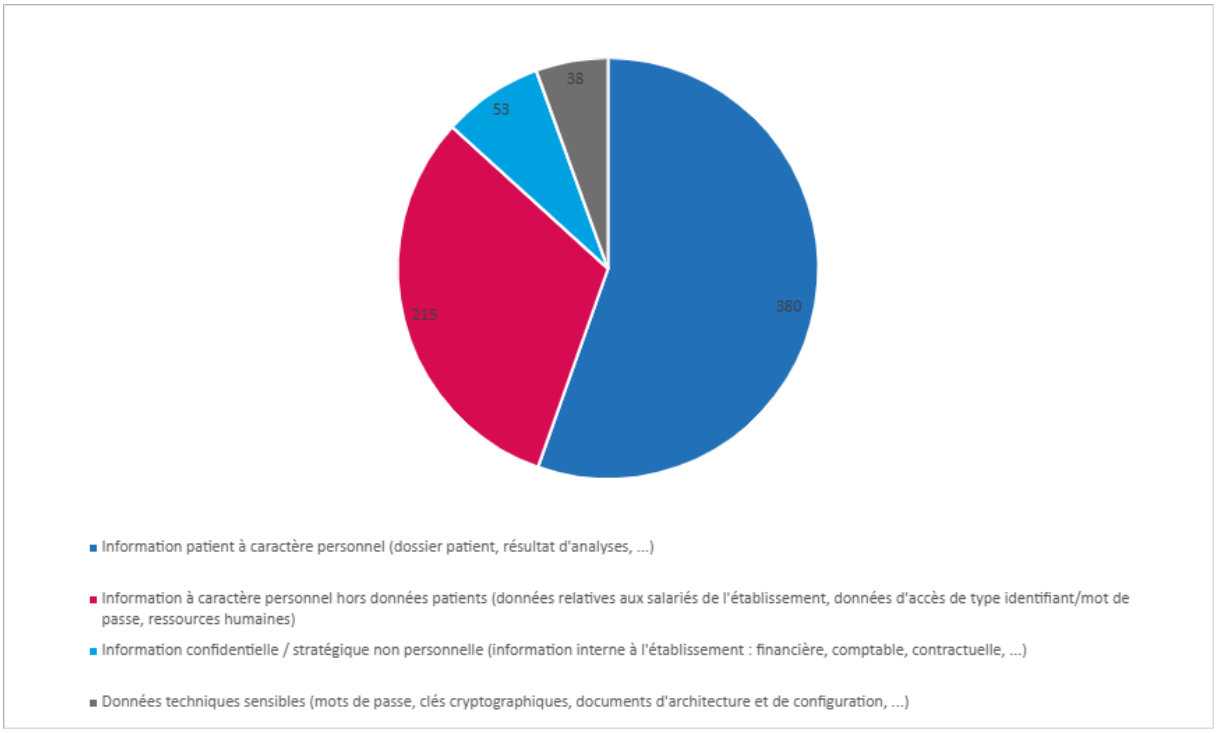


Figure 11 - Répartition selon les types de données impactées

76% C'est le pourcentage de structures indiquant que **l'incident a eu un impact sur des données**, qu'elles soient à caractère personnel, techniques ou relatives au fonctionnement de la structure.

22% des incidents impactant des données touchent **plus d'une catégorie de données** parmi les quatre catégories décrites dans le graphique ci-dessus.

C'est ainsi que parmi les incidents impactant des données, **55%** touchent des **données de santé à caractère personnel**, 31% des informations à caractère personnel hors données patient (principalement des identifiants de comptes utilisateur), 6% des données techniques sensibles et enfin 8% des informations confidentielles ou stratégiques. Les données à caractère personnel sont donc les premières atteintes par les incidents de sécurité déclarés.

●● Mise en danger potentielle des patients●●

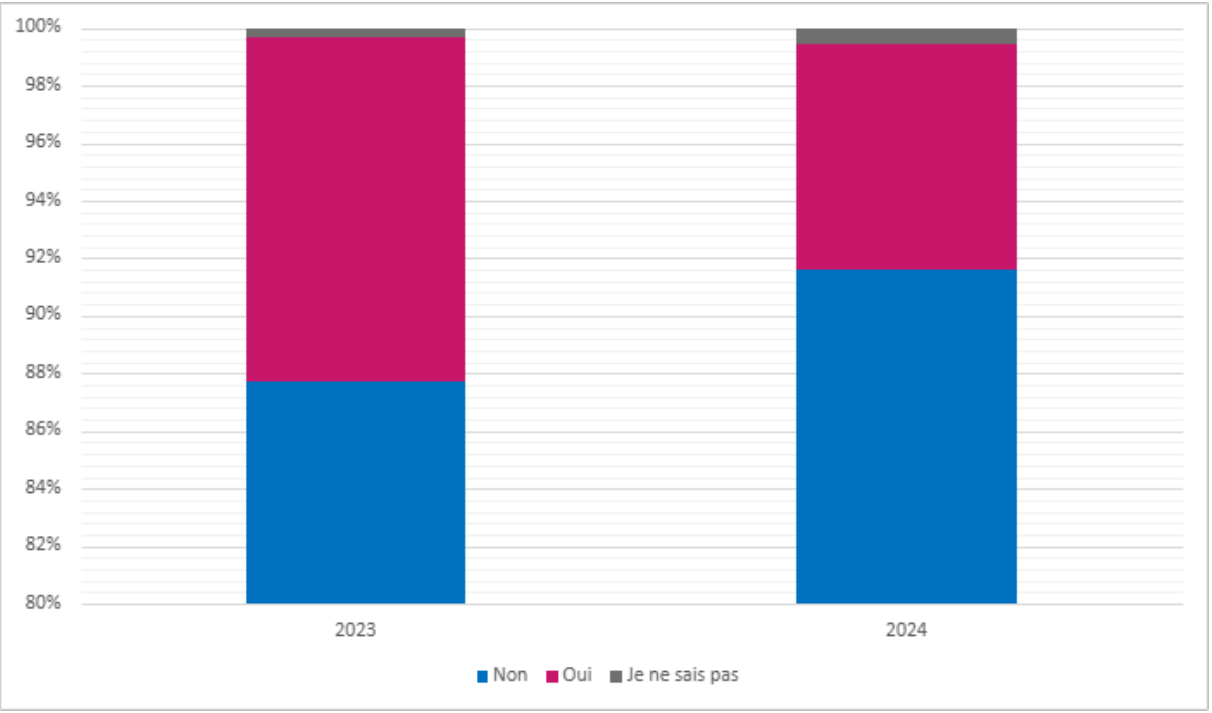


Figure 12 - Mise en danger potentielle des patients

Parmi les **59 mises en danger patient potentielles** de cette année 2024 (8% du nombre total d'incidents), **trois incidents ont entrainé une mise en danger patient avérée**.

Les 56 incidents restants, correspondant à la part des mises en danger potentielles de patients, ont été attribués à diverses causes. Il s'agit notamment d'attaques par rançongiciel, de coupures de courant ou de liens télécom, ainsi que de pannes d'équipement. Ces incidents ont eu un impact direct sur la disponibilité des services de santé, entraînant des interruptions prolongées de l'accès à des services hébergés, des perturbations du service téléphonique du SAMU et des dysfonctionnements des logiciels de prescription/aide à la dispensation.

Ces situations ont engendré des risques plus ou moins accrus pour la sécurité des patients, mettant en évidence la nécessité de mesures préventives et d'une gestion proactive des incidents pour garantir la continuité des soins.

En outre, les dysfonctionnements des logiciels de prescription/aide à la dispensation, attribués à des bugs logiciels, ont été identifiés comme une cause supplémentaire d'incidents de mise en danger patient. Heureusement, la vigilance des professionnels de santé et la mise en place de procédures de détection d'erreurs ont contribué à limiter l'impact de ces incidents sur la sécurité des patients.

●● Répartition des signalements à origine malveillante ou non malveillante ●●

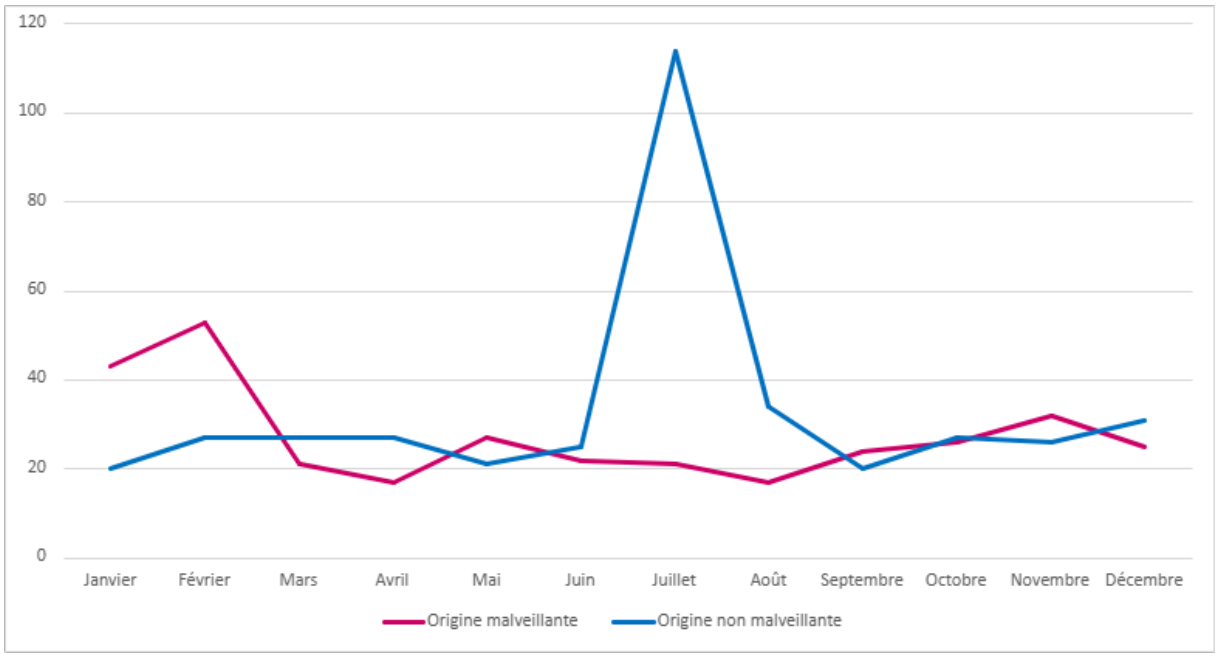


Figure 13 - Répartition selon le type d'incident

Parmi **les incidents déclarés, 328 sont d'origine malveillante et 399 d'origine non malveillante**. Dans l'analyse détaillée de ces deux catégories d'incidents, sont exclus les 22 signalements dits « Hors périmètre » n'ayant pas fait l'objet d'un traitement particulier (contre 24 en 2023).

Les actes malveillants

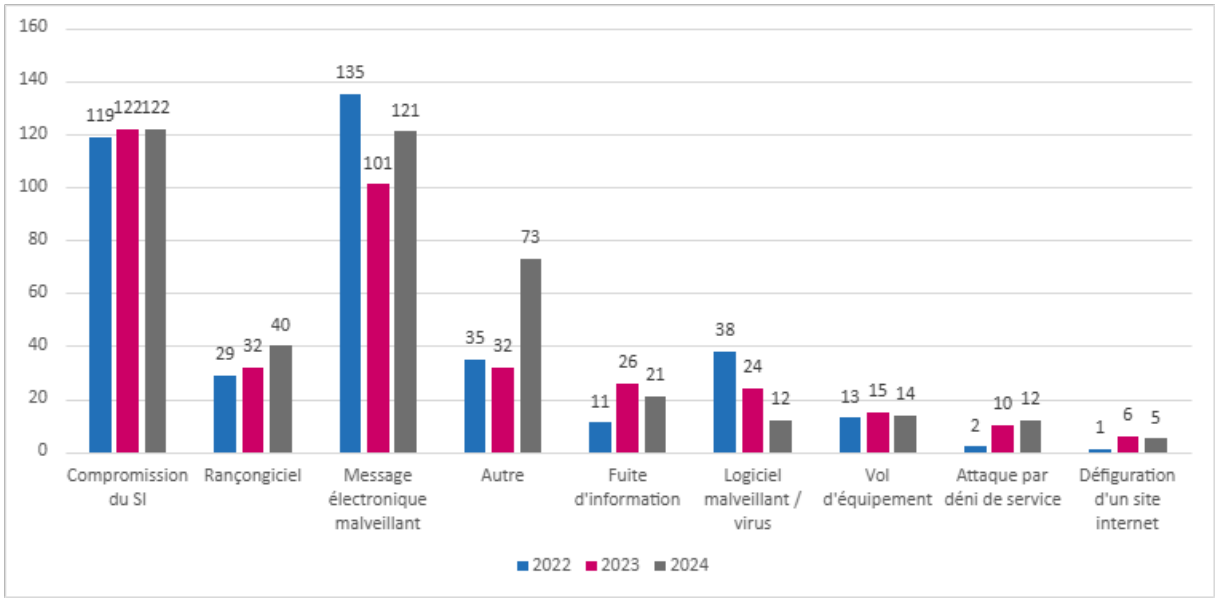


Figure 14 - Nombre d'incidents par type d'origine

L'année 2024 a été marquée, comme 2023, par une forte activité malveillante relative au vol d'identifiants (login – mot de passe) de comptes de messagerie et de comptes d'accès à distance. Le vol d'identifiants par infostealer[7] s'est développé.

Les attaquants récupèrent les identifiants selon les modes opératoires suivants : sur Internet (Internet clandestin, messagerie instantanée, etc.), par la technique de l'hameçonnage (phishing), l'exploitation de vulnérabilités sur des équipements qui n'ont pas été mis à jour et les tentatives de récupération en testant un grand nombre de mots de passe (technique de brute force).

Sur les 40 attaques par rançongiciels répertoriées tout au long de l'année, 4 ont impacté plusieurs serveurs de l'établissement (pour certains les contrôleurs de domaines ont également été touchés), 18 ont impacté un seul serveur et 16 concernaient uniquement un poste de travail. Deux incidents concernaient des prestataires et ont entrainé l'interruption des services (sans propagation de la compromission).

Certaines de ces attaques ont causé des dysfonctionnements critiques au sein des établissements victimes à cause de la perte massive de données et ont été parfois

[7] Logiciel malveillant s'infiltrant sur le système de la victime pour voler des données

précédées par une exfiltration d'informations confidentielles ou sensibles (en baisse par rapport à 2023).

Il convient cependant de souligner l'impact significatif de l'intervention proactive du CERT Santé dans la prévention de l'exploitation de vulnérabilités permettant d'obtenir un premier accès au SI de la victime.

Ainsi, dans le cadre d'un accompagnement technique, plusieurs attaques ont été prises en charge dès leur phase initiale d'infiltration ou bien neutralisées avant la compromission de composants critiques du SI tels que l'Active Directory.

L'intervention rapide du CERT Santé à la suite des signalements d'activités malveillantes en cours de réalisation sur le SI des victimes a permis de les neutraliser. Le CERT Santé a pu conseiller la structure et ainsi stopper toute progression des attaques vers d'éventuelles étapes de chiffrement ou de propagation au sein du système d'information pouvant impacter plus largement l'Active Directory et des services numériques critiques.

Cette intervention proactive a permis de protéger les données critiques des établissements de santé, préservant ainsi l'intégrité et la continuité opérationnelle de leurs systèmes d'information.

En conséquence, ces actions ont évité des perturbations majeures pouvant compromettre le bon fonctionnement des systèmes d'information, voire les paralyser, ainsi que la nécessité de recourir à des solutions de récupération de données.

Il est rappelé la recommandation gouvernementale de ne jamais payer de rançon :

- Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux ;
- Le paiement de la rançon n'empêchera pas l'entité d'être à nouveau la cible de cybercriminels ;
- L'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus (exemple : un fichier de base de données) ;
- En outre, son versement s'apparente à subventionner une organisation criminelle ;
- Enfin, les sociétés assistant la victime dans le paiement de la rançon peuvent être poursuivies pénalement en France sur le fondement de la complicité d'atteinte au Système de Traitement Automatique de Données et de Blanchiment ;
- En cas de prise de contact avec les auteurs, il est fortement recommandé de le faire avec l'assistance d'un service de police spécialisé, qui dispose d'un cadre légal pour ce faire.

Les fuites d'information concernent des identifiants de connexion (principalement à des VPN ou des comptes de messagerie) et des données de santé à caractère personnel.

La catégorie « Autre » concerne principalement des tentatives d'escroquerie par mail et par téléphone qui n'ont pas abouti.

Notons qu'une part des incidents (42%) relève de plusieurs qualifications. Par exemple, une attaque par rançongiciel, à la suite de la compromission d'un compte VPN liée à des identifiants en vente sur Internet relève des catégories suivantes : « fuite de données », « compromission de SI » et « rançongiciel ».

La catégorie « Logiciel malveillant / virus » correspond aux codes malveillants pouvant être utilisés pour exfiltrer des données, perturber le fonctionnement des machines, déployer des rançongiciels (exemple : QakBot démantelé en août 2023 opérant en tant qu'infostealer et associé à des activités de botnet) ou générer de la crypto-monnaie.

44% C'est le pourcentage des incidents qui ont une **origine malveillante** en 2024. Ce chiffre **est en baisse** comparé à l'année précédente.

●● Evolution du nombre d'incidents d'origine malveillante ●●

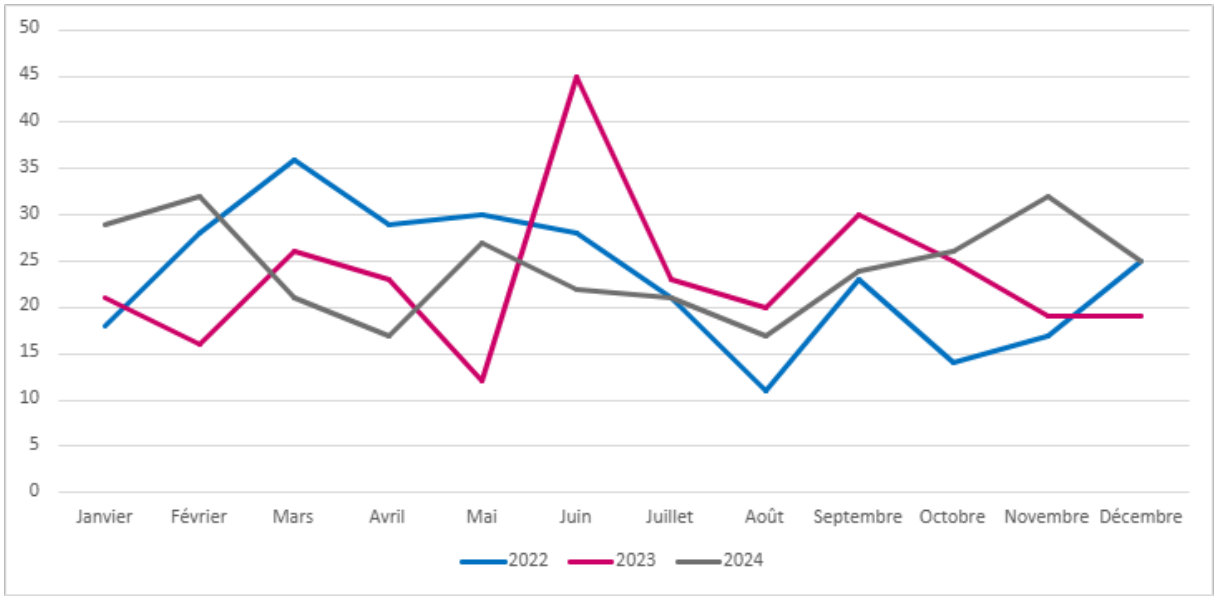


Figure 15 - Evolution du nombre d'incidents dont l'origine est malveillante

.

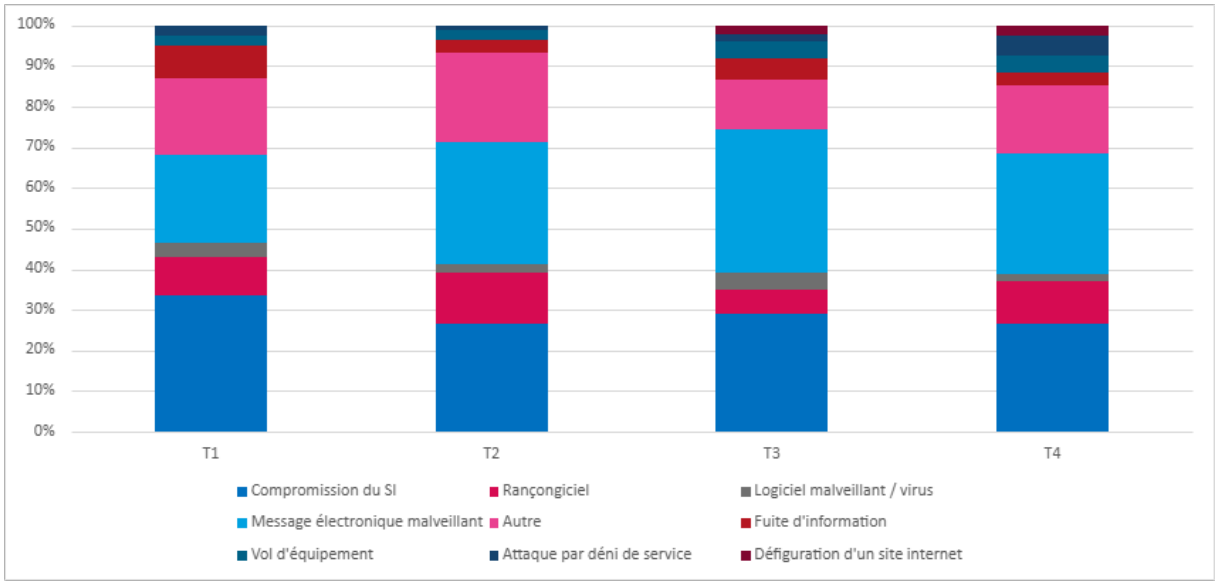


Figure 16 - Origine malveillante des incidents par trimestre

La frise chronologique suivante présente les rançongiciels et les principales vulnérabilités ayant fait l'objet d'une exploitation (mais sans lien avec les attaques par rançongiciel) qui ont été identifiés au cours de l'année :

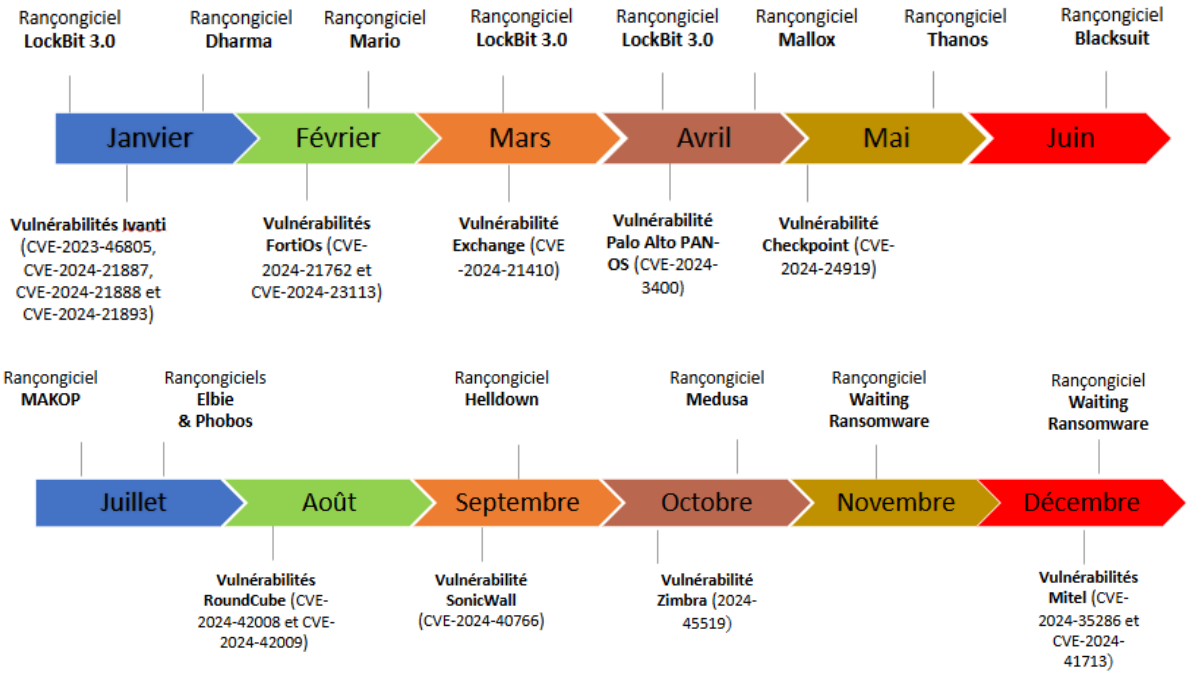


Figure 17 - Chronologie des cyber-menaces identifiées en 2024

●● Appui technique pour la résolution d'un incident ●●

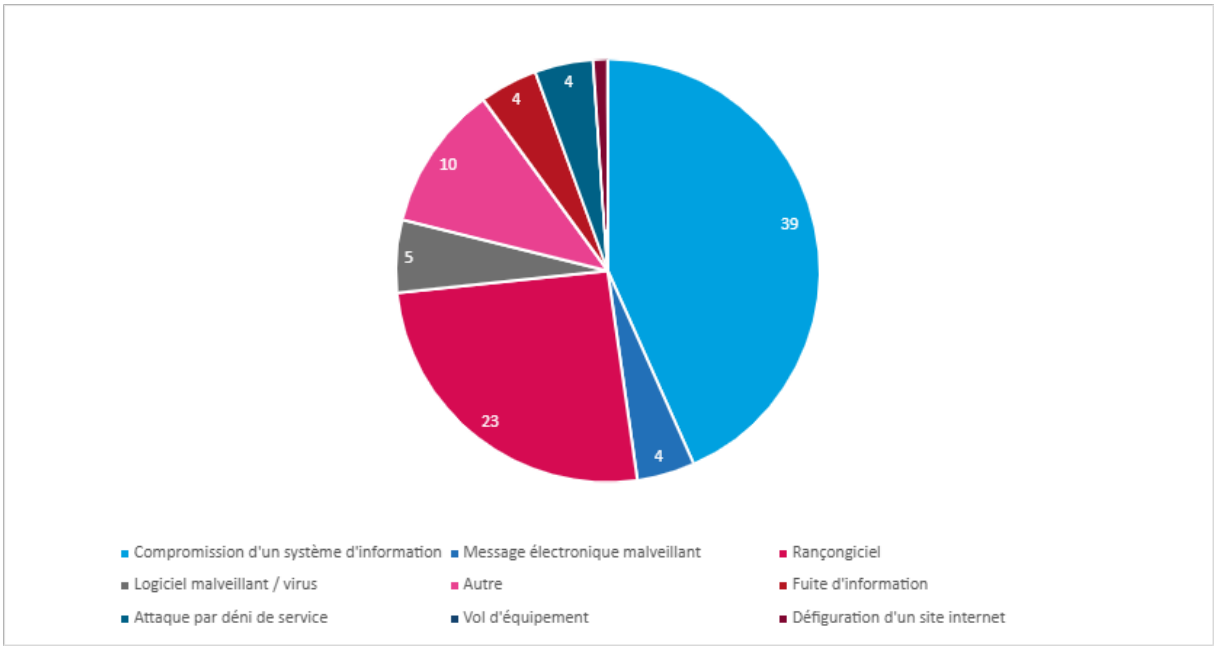


Figure 18 - Origine des incidents pour lesquels un appui technique a été apporté par le CERT Santé

Le nombre de déclarations d'incident pour lesquels une demande d'accompagnement est formulée a très légèrement baissé en 2024. Il y a eu au total 162 demandes d'accompagnement, soit 22% des incidents signalés. Ce sont les ES publics (51%) qui ont le plus sollicité le CERT Santé. Ces demandes concernent généralement une demande d'appui pour confiner des services compromis, identifier l'origine d'une compromission avérée ou potentielle du SI et valider des mesures visant à endiguer la propagation de l'attaque et corriger les vulnérabilités.

Parmi les 75 accompagnements techniques réalisés par le CERT Santé, 8 constituaient une levée de doute face à un faux positif, soit 11% des cas.

Dans le cadre **de l'accompagnement des structures de santé**, des recommandations ont été émises par le CERT Santé afin, notamment, de permettre aux structures d'améliorer la sécurité de leur SI. Ces recommandations sont **adaptées à la taille de la structure ainsi qu'au niveau de technicité du déclarant et des équipes de la structure**.

Elles sont donc **variées** et peuvent aller de l'envoi des fiches et guides du portail cyberveille-santé, de la documentation de l'ANSSI, aux conseils plus techniques comme la mise en place de durcissement de systèmes, etc.

Les signalements d'origine non malveillante

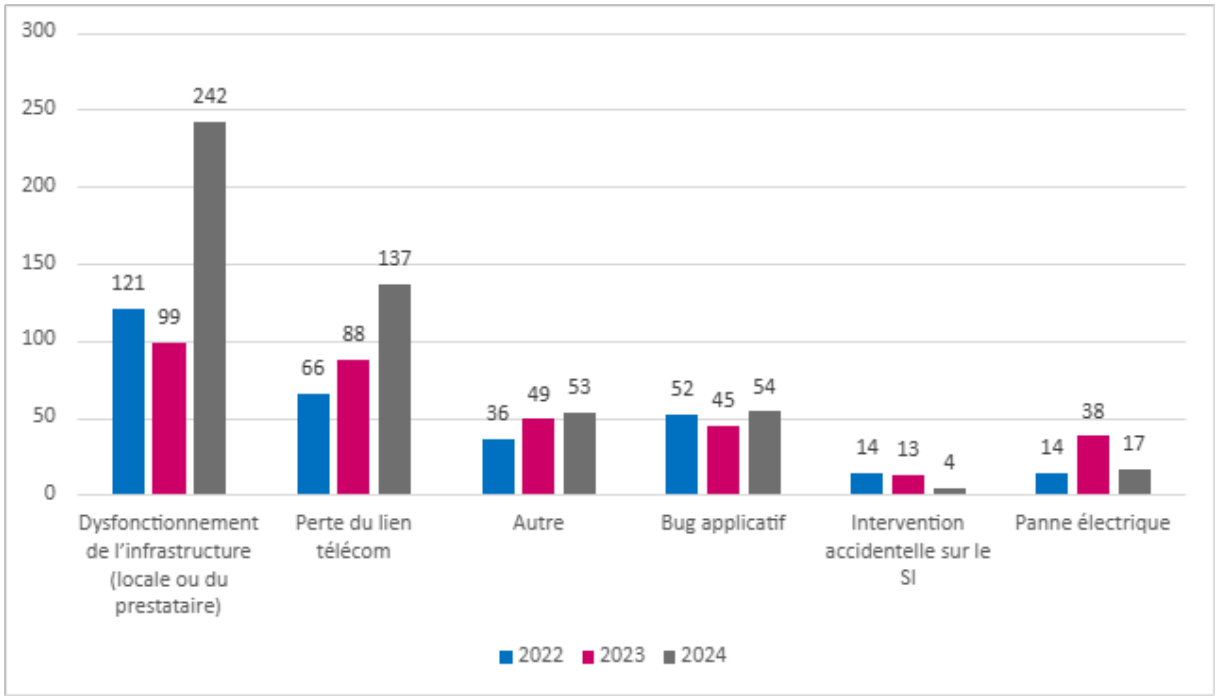


Figure 19 - Origine non malveillante des incidents

Le nombre d'incidents ayant une origine non malveillante est principalement lié à des mises à jour problématiques et des incidents issus des hébergeurs ou prestataires de solutions métier en mode SaaS. Cela a provoqué des interruptions prolongées de service ou des applications hébergées. **La part d'origine non malveillante et liée à un dysfonctionnement de l'infrastructure est de 38%.** On compte, parmi ces cas, 59% de dysfonctionnements du côté des prestataires contre 41% de dysfonctionnements de l'infrastructure locale.

La **perte du lien télécom** est la deuxième source d'incident d'origine non malveillante (34%). Cette perte peut fortement impacter le fonctionnement des activités métier des structures de santé, en particulier les structures disposant d'un service d'urgences ou un SAMU. Ce type d'incident est généralement traité en priorité par les opérateurs.

On observe qu'en 2024, ces deux types d'incidents représentent une part nettement plus significative qu'en 2023. Ce phénomène peut être dû à l'augmentation globale du nombre d'incidents déclarés cette année, mais pourrait également provenir d'une communication plus claire vis à vis du traitement de ce type d'incidents par les

établissements de santé, qui ne notifiaient pas systématiquement le CERT Santé lors d'une telle occurrence.

Le nombre de déclarations lié à un **bug applicatif** (14%) est en légère augmentation par rapport à 2023. Dans 46 % des cas, les éditeurs ont apporté des correctifs dans des délais compatibles avec la mise en place temporaire de mesures de vigilance exceptionnelles pour éviter de commettre des erreurs dans la prise en charge des patients. Il arrive toutefois régulièrement que certains bugs applicatifs persistent dans le temps. Bien que ce cas reste minoritaire, voire marginal, il peut causer des désagréments aux établissements de santé dans leurs tâches quotidiennes. Dans de rares situations, le CERT Santé se positionne en tant qu'intermédiaire entre l'éditeur et l'établissement de santé, voire les potentielles parties prenantes qui pourraient avoir voix au chapitre, afin de faire avancer les choses et apporter un réel appui aux établissements de santé afin de réduire le temps d'indisponibilité de leurs outils.

Dans la catégorie « Autre » on retrouve principalement des déclarations de vulnérabilités qui n'ont pas fait l'objet d'une exploitation par un acteur malveillant mais également des évènements informatiques à l'origine de comportements imprévus de systèmes mais qui se sont révélés être des « faux positifs » après une investigation du CERT Santé.

56% C'est la part d'incidents d'origine **non malveillante** en 2024 des incidents, ce chiffre est **en hausse** par rapport à 2023.

●● Evolution des incidents d'origine non malveillante ●●

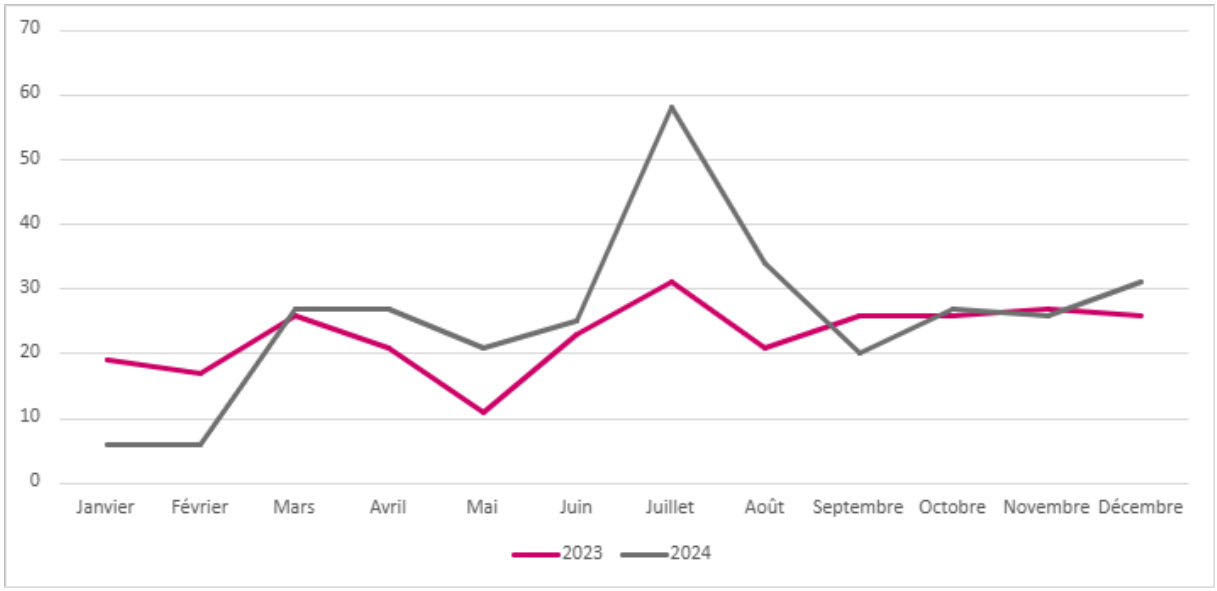


Figure 20 - Evolution du nombre d'incidents dont l'origine est non malveillante

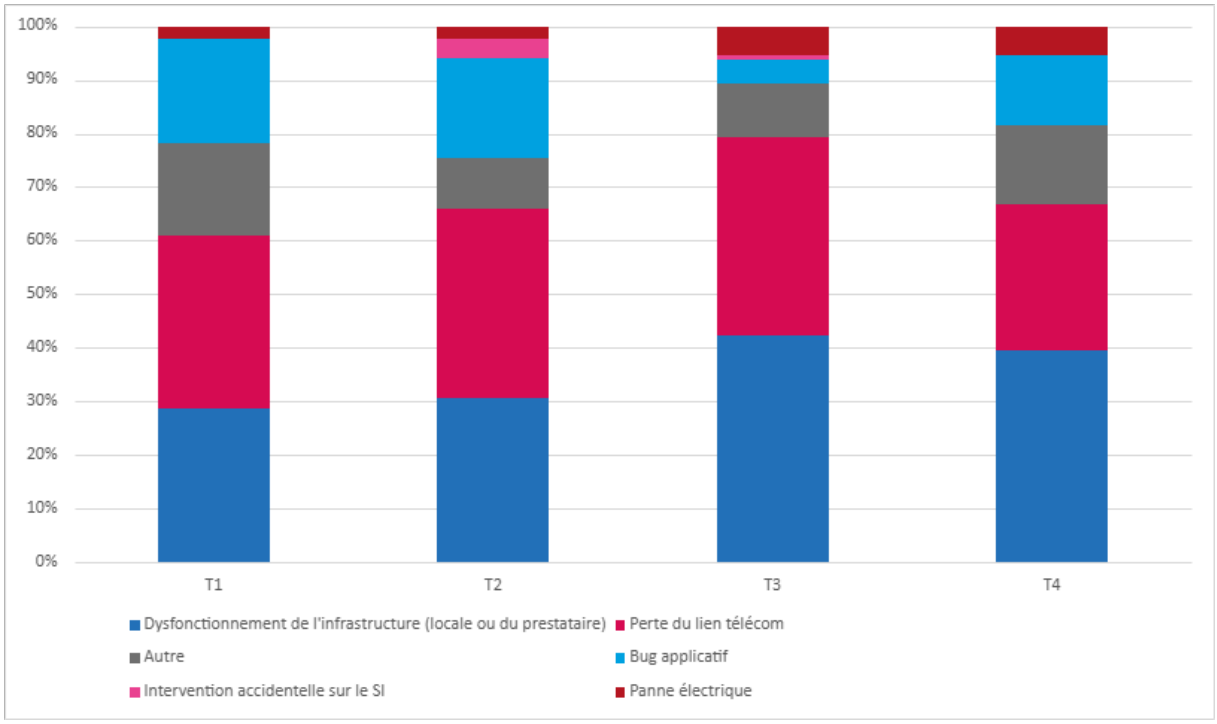


Figure 21 - Origine non malveillante des incidents par trimestre

4.5 Publication d’alertes sur le portail cyberveille-santé

En 2024, **134 alertes ont été publiées sur le portail cyberveille-santé** (105 en 2023) parmi lesquelles des vulnérabilités critiques activement exploitées concernant :

- 4 vulnérabilités sur les solutions VPN Fortinet permettant à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d’exécuter du code arbitraire ;
- 1 vulnérabilité sur le système d’exploitation des pare-feu Palo Alto permettant à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, d’exécuter du code arbitraire avec les privilèges root ;
- 1 vulnérabilité sur la solution VPN Ivanti permettant à un attaquant non authentifié d'exécuter du code arbitraire.

5 SERVICE NATIONAL CYBERSURVEILLANCE

Dans le cadre du plan de renforcement cyber du ministère, les audits de cybersurveillance ont été prioritairement orientés vers les groupements hospitaliers de territoire (GHT).

En 2024, **461 audits ont été réalisés** : 329 CH membres de 65 GHT (pour 50 GHT, plus de 50% des ES ont été audités), 111 établissements sanitaires, 19 ESMS et 2 GRADeS.

Parmi les établissements sanitaires, 104 ont été audités au titre de leur désignation comme établissement prioritaire pour les Jeux Olympiques et Paralympiques.

6 VEILLE PROACTIVE

Le CERT Santé a poursuivi son activité de veille proactive. Ainsi, afin de prévenir la compromission potentielle ou avérée de SI au travers de l'exploitation de vulnérabilités connues, **le CERT a alerté plus de 400 structures en 2024**. Ces alertes ont principalement concerné des solutions d'accès à distance (VPN - Fortinet, Ivanti -, pare-feux - Palo Alto, CheckPoint - ou de messagerie - Exchange, Zimbra -) et l'environnement Windows (messagerie, suite Office). On compte parmi ces structures une dizaine d'acteurs de l'écosystème (institutionnels, hébergeurs et éditeurs).

Le CERT Santé a **relayé plus de 120 alertes** concernant des compromissions avérées ou potentielles de SI identifiées par l'ANSSI.

Sur l'ensemble des alertes envoyées par le CERT Santé, 66 concernaient des compromissions avérées de comptes ou d'applications (BAL, VPN, comptes applicatifs, Exploit). Environ un tiers concernaient des comptes de messagerie.

7 CONSTAT ET RECOMMANDATIONS

Comme évoqué dans le paragraphe introductif, l'amélioration du niveau de sécurisation des systèmes d'information hospitaliers constatée par le CERT Santé en 2024 est significative.

Cette amélioration a notamment été induite par **le programme CaRE** qui, comme le souligne la Cours des comptes dans son [8] de début 2025 relatif à la sécurité informatique des établissements de santé, a permis de prendre "acte de l'urgence avec laquelle il convient de mettre à disposition des hôpitaux un certain nombre de protections techniques, face à un accroissement quantitatif et qualitatif de la cyber-malveillance, en particulier des rançongiciels".

Cette dynamique doit se poursuivre dans les prochains mois et permettre aux établissements de mieux anticiper la crise, de mieux protéger leurs données via des sauvegardes intègres, de mieux **protéger les accès distants à leur système d'information** ou encore de **déployer une identification et une authentification adaptées** aux enjeux portés par les services numériques sensibles au travers des Domaines 2 et 3 du programme et de **la démarche HospiConnect**.

En effet, les structures qui ont été auditées ou alertées exposent souvent trop de ressources sur Internet et ne portent pas suffisamment d'attention à la sécurisation de leurs services (portail Web, accès à distance, etc.).

Les établissements de santé et médico-sociaux que le CERT Santé a accompagné dans la réponse à incident présentaient parfois des faiblesses en matière de gestion des droits d'administration et de protection des sauvegardes.

En 2025, une grande majorité des établissements seront contraints **d'élever leur niveau de sécurité** dans le cadre de la mise en œuvre de **la réglementation NIS 2**. Les exigences couvrent toutes les dimensions de la cybersécurité (organisationnelle et technique).

Le CERT Santé rappelle ci-dessous quelques bonnes pratiques afin d'améliorer la résilience des établissements vis-à-vis des menaces cyber les plus importantes comme les attaques par rançongiciel.

<u>Maitriser les systèmes exposés</u>

- Réduire la surface d'attaque en désactivant les comptes, protocoles et services qui ne sont pas indispensables : certaines structures de santé auditées exposent

[8] https://www.ccomptes.fr/sites/default/files/2024-12/20250103-S2024-1456-La-securite-informatique-des-etablissements-de-sante.pdf

un grand nombre de services numériques sur Internet y compris des services de télé-administration reposant sur RDP ou d'autres protocoles.

- Renforcer les configurations et la sécurisation des accès : beaucoup de vulnérabilités détectées lors des audits concernent une mauvaise configuration des protocoles utilisés (par exemple le protocole SSL/TLS utilisé dans le cadre d'échanges chiffrés https) ou une divulgation d'informations sensibles. L'ensemble de ces vulnérabilités peut être corrigé assez simplement par la mise en œuvre de bonnes pratiques de configuration.

- Vérifier la suppression des vulnérabilités web classiques (présentées dans le Top 10 OWASP[9]) : se conformer aux bonnes pratiques de développement (par exemple le contrôle des saisies utilisateur). Il peut également être mis en œuvre un web application firewall (WAF) qui bloquera l'essentiel des tentatives d'exploitation des vulnérabilités référencées par l'OWASP s'il est correctement configuré.

- Mettre à jour les équipements (boitiers VPN, fermes RDS ou de virtualisation, routeurs d'interconnexion, etc.). Ils doivent faire l'objet d'une attention particulière et d'une réactivité adéquate face à la menace. En effet, des vulnérabilités critiques sont souvent utilisées par les attaquants pour se connecter sur un système d'information dans les quelques jours, voire heures, après la publication d'une alerte. Il est nécessaire de se tenir informé des nouvelles vulnérabilités sur les équipements déployés, particulièrement les équipements exposés sur internet. Il en va de même pour les équipements constituant l'infrastructure interne, qui peuvent faciliter l'action d'un attaquant déjà infiltré sur le réseau privé.

- Inclure un engagement du prestataire (DPI, Gestion des activités de biologie médicales, gestion des activités de radiologie, etc…) sur le maintien en conditions de sécurité de son infrastructure : de nombreuses vulnérabilités critiques ont été ainsi découvertes sur des systèmes gérés par des tiers externes. Lors de la contractualisation d'une prestation avec un tiers, il est essentiel d'inclure des engagements sur le maintien en conditions de sécurité ainsi que la possibilité de réaliser des audits.

[9] Le Top 10 OWASP est un document de sensibilisation standard pour les développeurs et la sécurité des applications Web. Il représente un large consensus sur les risques de sécurité les plus critiques pour les applications Web.

- De plus, dans le cadre de cet engagement, un cadrage clair des solutions de télémaintenance et des conditions d'accès à distance doit être mis en place.

Le premier appel à financement (« Domaine 1 ») du programme CaRE pour les établissements de santé vise le renforcement de leur niveau de sécurité en maitrisant leur exposition. Le scan réalisé tous les deux mois doit être poursuivi de maintenir une surveillance continue et de s'assurer de l'absence de vulnérabilité critique.[10]

Mettre en place une authentification double facteur sur les applicatifs exposés et critiques :

La récupération des mots de passe par force brute, par phishing ou par infostealing est grandissante. Le CERT Santé constate de plus en plus que des attaquants accèdent initialement aux systèmes avec des identifiants valides récupérés par les méthodes précitées dans les cas de compromissions, principalement sur les passerelles VPN et applicatifs exposés.

- Activer l'authentification multifacteur basée sur le temps (mot de passe changeant toutes les X secondes, nommé TOTP). Ainsi pour accéder au système, l'attaquant devrait en plus de posséder le couple identifiant / mot de passe valide, posséder ce second facteur d'authentification. Le multifacteur par mail est un compromis qui ne couvre pas correctement le risque de vol d'identifiants, les utilisateurs ayant souvent les mêmes identifiants pour leur boîte mail.

Le référentiel sur l'identification électronique définit des exigences sur les connexions à des services numériques traitant des données de santé (mots de passe robustes, authentification multi-facteurs et utilisation d'informations d'identification des utilisateurs vérifiées et issues des répertoires de référence - INS, RPPS, FINESS -. Il décrit des paliers successifs à atteindre, entre le 1er juin 2022 et le 31 décembre 2025. Il est opposable et le respect des exigences correspondantes est obligatoire pour les acteurs concernés[11]. Dans ce contexte, l'objectif de l'appel à projet HospiConnect[12] est d'accélérer le déploiement des exigences du référentiel d'identification électronique et de réduire les risques d'usurpation de l'identité numérique des professionnels de

[10] https://esante.gouv.fr/strategie-nationale/cybersecurite/axe-4#content-48279

[11] https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire?field_thematique_pgssi_target_id%5B745%5D=745

[12] https://esante.gouv.fr/strategie-nationale/cybersecurite/axe-4#content-48993

santé pour l'accès aux services sensibles. Il est intégré au Programme CaRE dans le cadre de l'axe 4 "Sécurité opérationnelle".

Sécuriser ses sauvegardes

Dans de nombreux incidents liés à une attaque par rançongiciel, les ES n'ont pas pu exploiter les sauvegardes qui étaient chiffrées. La présence de sauvegardes intègres aurait permis de diminuer sensiblement le délai de reprise d'activité.

- Identifier les données critiques et réaliser des sauvegardes automatiques et récurrentes, si possible de façon sécurisée (chiffrement des sauvegardes).

- S'assurer de la restriction d'accès aux sauvegardes en :
  - privilégiant un accès avec un compte d'administrateur local avec une authentification à deux facteurs, ce compte n'étant pas référencé dans l'Active Directory ;
  - restreignant l'accès aux composants d'administration aux seules adresses IP des rebonds ou postes autorisés (que cela soit l'interface d'administration de la sauvegarde ou l'administration du serveur qui l'héberge) ;
  - veillant à ce que l'utilisateur qui lance l'agent de sauvegarde sur les différentes machines n'a pas d'accès sur l'interface d'administration de l'application de sauvegarde ni de droit de suppression/modification des anciennes sauvegardes.

- Veiller à ce que les outils liés à la sauvegarde soient à jour avec les derniers patchs de sécurité.
- Pour la réplication, appliquer la règle de sauvegarde en système 3-2-1[13].

Le deuxième appel à financement (« Domaine 2 ») du programme CaRE pour les établissements de santé vise le renforcement de la stratégie de continuité et de reprise d'activité. Il intègre des exigences liées à la gestion des sauvegarde (architecture, supervision, immuabilité, authentification, etc.) et à leur restauration en cas de crise.

[13] https://www.it-connect.fr/sauvegarde-quest-ce-que-la-regle-du-3-2-1/

Se préparer à un incident cyber

- Organiser des exercices de gestion de crise cybersécurité[14] proches des conditions réelles afin de s'approprier des automatismes et d'assurer au mieux la continuité des soins en cas d'incident.

- Etablir et tester des plans de continuité et de reprise d'activité.

- Réaliser régulièrement des tests de restauration de ses sauvegardes afin de disposer de sauvegardes opérationnelles. Il est recommandé de consigner les résultats de ces tests dans un document unique de suivi dans lequel se trouvera le statut des restaurations, la réévaluation éventuelle du périmètre critique à sauvegarder et le statut sur les risques identifiés.

Maintenir la cartographie de son SI à jour

- Créer, maintenir et mettre à jour une cartographie du système d'information

Cette cartographie référence l'architecture réseau, les flux de sécurité, la liste la plus exhaustive possible des applicatifs et leurs versions déployées. Cette cartographie permet de réagir plus rapidement pour isoler des parties du réseau en cas d'attaque ou de participer au diagnostic lors de dysfonctionnements quelle que soit leur origine.

Gestion des comptes

Les règles de gestion de mot de passe définies par l'ANSSI ou la CNIL ne sont pas toujours appliquées (politiques de mot de passes trop simples - 6 à 8 caractères - acceptant les mots courants, les motifs prévisibles et des informations personnelles publiques).

- Avoir un mot de passe de 12 caractères, avec lettres (majuscules et minuscules), chiffres et caractères spéciaux pour les utilisateurs non privilégiés. Lorsque ces règles sont appliquées, il n'est pas nécessaire d'imposer l'expiration du mot de passe pour les comptes utilisateurs de l'Active Directory.

- Avoir un mot de passe de 16 caractères, avec lettres (majuscules et minuscules), chiffres et caractères spéciaux pour les utilisateurs à privilèges et administrateurs

[14][14] https://esante.gouv.fr/strategie-nationale/cybersecurite/axe-1

avec un renouvellement obligatoire tous les 1 à 3 ans (sauf connaissance de fuite).

- Utiliser un gestionnaire de mots de passe. C'est obligatoire pour la population des administrateurs et recommandé pour les utilisateurs. La non-connaissance d'autre mot de passe que le mot de passe maître du coffre-fort est un réel atout pour la sécurité du SI.

Pour en savoir plus, nous vous recommandons la lecture de la partie «4 - Facteur de connaissance » du guide de l'ANSSI : Recommandations relatives à l'authentification multifacteur et aux mots de passe[15].

L'annuaire Active Directory (AD) est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information (SI) Microsoft. L'obtention de privilèges élevés sur l'AD entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI. Il est donc primordial de réaliser un cloisonnement logique des ressources de l'AD pour réduire ce risque. Une des dimensions de ce cloisonnement est la restriction de l'utilisation de comptes à privilège et des différents niveaux d'administration proposés par cette technologie. Le «Domaine 1» du programme CaRE vise à atteindre un premier niveau de remédiation suite à la mise en œuvre bimestrielle d'un audit ADS de l'ANSSI[16].

Savoir être réactif :

- Systèmes exposés, systèmes critiques, les vulnérabilités sont exploitées sous quelques jours voire heures ;
  Importance d'avoir la capacité de mettre à jour ces systèmes dans des délais très courts (équipes, procédures, etc.), voire de savoir déconnecter certains systèmes temporairement en maitrisant les impacts ;

- Importance aussi de suivre les alertes du CERT-Santé, i.e. de disposer en établissement d'un point de contact qui relève très régulièrement la boite déclarée

[15] https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

[16] https://esante.gouv.fr/strategie-nationale/cybersecurite#content-38127

(cela a déjà permis d'arrêter des attaques après le premier niveau de compromission).

Mettre en place un système de journaux centralisé

Lors d'attaques, les journaux d'évènements sont un bon moyen pour comprendre ce qu'il s'est passé et pour définir le périmètre compromis. La journalisation est également importante pour permettre de détecter les premiers signaux d'une attaque en cours en permettant d'obtenir les traces liées aux actions des attaquants.

- Centraliser des journaux de logs de qualité et remonter des alertes automatiques basées sur des évènements anormaux (scan réseau / tentatives de force brute / désactivation d'antivirus, etc.) peut être un réel atout pour détecter et endiguer une attaque en cours.

- Analyser régulièrement les journaux de ses équipements périmétriques : installer un correctif pour une vulnérabilité critique sur un composant exposé sur Internet n'est pas la garantie d'être protégé contre une exploitation antérieure, il faut également analyser ses journaux pour vérifier si elle a été exploitée et, en cas de doute, renouveler l'ensemble de ses comptes.

- Assurer un délai de rétention suffisant sur les équipements concernés, conformément aux recommandations de l'ANSSI.[17]

[17] https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation

8 GLOSSAIRE

ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
ARS	Agence Régionale de Santé
CERT	Computer Emergency Response Team
Code malveillant	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau. Remarques : Les virus ou les vers sont deux types de codes malveillants connus.
CORRUSS	Centre opérationnel de réception et de régulation des urgences sanitaires et sociales
Cybermalveillance	La cybermalveillance recouvre toute activité criminelle réalisée par le biais d'Internet et des technologies du numérique. Elle englobe toute forme de malveillance effectuée à l'aide de l'informatique, d'équipements électroniques et des réseaux de télécommunication.
Cybersécurité	État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.
DGS	Direction Générale de la Santé
DNS	Délégation au numérique en santé
DSI	Directeur des Systèmes d'Information
ES	Etablissement de Santé
ESMS	Etablissement et Service Médico-Social
Forensique	L'analyse forensique en informatique signifie l'analyse d'un système informatique après avoir été victime d'une cyberattaque.
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HO/JO	Heures Ouvrées / Jours Ouvrés
HNO/JNO	Heures Non Ouvrées / Jours Non Ouvrés
LDAP	Lightweight Directory Access Protocol

Phishing	Hameçonnage - Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.
PRIS	Prestataire de Réponse aux Incidents de Sécurité
Rançongiciel	Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.
RSSI	Responsable de la Sécurité des Systèmes d'information
SI	Système d'Information

NOTES PERSONNELLES

Pour aller plus loin, rendez-vous sur :

- le site du Ministère du Travail, de la Santé, des Solidarités et des Familles : sante.gouv.fr
- le site de l'Agence du Numérique en Santé : esante.gouv.fr
- le portail cyberveille : cyberveille-sante.gouv.fr/

Pour prendre contact :

- au sein du Ministère chargé de la Santé :
  ssi@sg.social.gouv.fr
- au sein de l'Agence du Numérique en Santé :
  cyberveille@esante.gouv.fr

MINISTÈRE
DU TRAVAIL, DE LA SANTÉ,
DES SOLIDARITÉS
ET DES FAMILLES
Liberté
Égalité
Fraternité

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici