

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

Rapport public 2025

SOMMAIRE

1	Introduction	3
2	Dispositif de traitement des signalements des incidents de sécurité des systèmes d'information pour le secteur santé	5
2.1	Contexte réglementaire et organisationnel.....	5
2.2	Présentation des activités	5
3	Synthèse de l'activité en 2025	10
4	Observatoire des signalements.....	11
4.1	Chiffres clés pour la période 2024-2025.....	11
4.2	Informations générales sur les signalements	12
4.3	Publication d'alertes sur le portail cyberveille	35
5	Service national cybersurveillance	36
6	Veille proactive	37
7	Constat et recommandations	38
8	Glossaire.....	44

TABLE DES FIGURES

Figure 1 - Chiffres clés des signalements déclarés en 2024 et 2025	11
Figure 2 - Evènements marquants de l'année 2025	12
Figure 3 - Nombre de signalements par mois	13
Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt	14
Figure 5 - Etat des incidents lors de leur signalement	15
Figure 6 - Répartition des signalements par région	18
Figure 7 - Nombre de signalements rapporté à l'activité hospitalière par région	19
Figure 8 - Répartition des signalements selon le type de structure.....	20
Figure 9 - Part des signalements comparée à la part des établissements selon leur raison sociale	21
Figure 10 - Répartition selon les types d'impact sur les données.....	22
Figure 11 - Répartition selon les types de données impactées.....	24
Figure 12 - Mise en danger potentielle des patients.....	25
Figure 13 - Répartition selon le type d'incident	26
Figure 14 - Nombre d'incidents par type d'origine	27
Figure 15 - Evolution du nombre d'incidents dont l'origine est malveillante	30
Figure 16 - Origine malveillante des incidents par trimestre	30
Figure 17 - Chronologie des cybermenaces identifiées en 2025	31
Figure 18 - Origine des incidents pour lesquels un appui technique a été apporté par le CERT Santé.....	31
Figure 19 - Origine non malveillante des incidents	33
Figure 20 - Evolution du nombre d'incidents dont l'origine est non malveillante	34
Figure 21 - Origine non malveillante des incidents par trimestre.....	35

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. Au regard du nombre d'incidents déclarés en 2025, quasiment similaire à celui de 2024, et de la légère hausse du nombre d'établissements ayant déclaré au moins un incident, il apparaît que le secteur de la santé reste confronté à un niveau de menace élevé.

Cela est confirmé par le [Panorama de la cybermenace dressé par l'ANSSI](#), qui qualifie la menace de stable et persistante, avec 3 586 événements de sécurité pris en charge par l'autorité nationale en matière de cybersécurité et de cyberdéfense, dont 1 366 incidents confirmés. 10% d'entre eux ont concerné le secteur de la santé, faisant de ce dernier le troisième secteur le plus touché.

Au-delà de ces indicateurs globaux, il convient en premier lieu de noter que le nombre d'incidents ayant eu un impact majeur sur la continuité des soins et donc la prise en charge des patients poursuit sa baisse pour ce qui concerne les établissements de santé. Cette tendance résulte des efforts collectifs menés :

- Avec l'appui du programme CaRE, les établissements ont remédié aux principales faiblesses de leur surface exposée sur Internet et ont ainsi fermé des points d'entrée exploitables par les cyberattaquants. Ils ont également élevé le niveau de sécurité de leurs annuaires techniques rendant ainsi plus difficile la mise en œuvre de chaînes d'attaque reposant sur leur exploitation malveillante à des fins d'élévation des privilèges. La vigilance portée sur ces deux éléments du système d'information se poursuit au travers de la réalisation d'audits de Cybersurveillance (service mis à disposition par le CERT Santé) et d'audits ADS (service mis à disposition par l'ANSSI).
- Toujours dans le cadre de l'axe 4 du programme CaRE dédié à la sécurité opérationnelle des établissements, ces derniers travaillent depuis quelque mois à améliorer leur résilience en sécurisant leurs sauvegardes et en définissant les solutions et modes dégradés permettant la continuité de leurs activités en cas d'incident et notamment en cas d'indisponibilité de leurs systèmes d'information.
- La veille proactive opérée par le CERT Santé, qui permet notamment la détection au plus tôt des vulnérabilités majeures et des campagnes d'exploitation, bénéficie d'une automatisation croissante du traitement des alertes, d'une augmentation du nombre de bénéficiaires supervisés et d'une facilitation d'accès aux données pour ces derniers. Cette veille a un impact d'autant plus important qu'elle est complétée par les capacités des partenaires du CERT Santé (notamment l'ANSSI et les CSIRT régionaux) avec lesquels la collaboration a été renforcée en 2025.

Par ailleurs, il ressort que les établissements de santé présentent un niveau de préparation accru face aux crises d'origine cyber, en particulier grâce au déploiement d'exercices de gestion de crise, lesquels doivent désormais s'inscrire dans une démarche durable et récurrente. Cette analyse est corroborée par les résultats d'une étude conduite dans le cadre du Programme CaRE, à laquelle ont répondu près de 720 directeurs d'établissement, dont 79 % déclarent se considérer bien préparés ou, a minima, assez bien préparés.

Si le nombre d'incidents déclarés par les bénéficiaires du CERT Santé est globalement stable, ceux émanant d'établissements et services sociaux et médico-sociaux est en nette augmentation (+48%). Si l'on peut se satisfaire d'une meilleure connaissance de la chaîne d'alerte par les structures de ce secteur, le contexte de transformation numérique accélérée associée à cette forte hausse montrent la nécessité de la mise en place d'un soutien des démarches de prévention et d'accompagnement dans l'élévation du niveau de sécurité.

Si le nombre d'incidents liés aux rançongiciels est en baisse (-30%), l'année 2025 a mis en exergue que les fuites de données constituent aujourd'hui l'un des risques les plus préoccupants pour le secteur de la santé. Ces incidents peuvent conduire à la revente ou à la divulgation de dossiers médicaux, de résultats d'analyse ou de données administratives, avec des conséquences graves en matière de confidentialité et de confiance des patients. L'immense majorité des incidents de ce type constatés par le CERT Santé avaient pour origine la compromission du compte d'un professionnel de santé ou d'un prestataire. Que ce soit par des infostealers^{OBJ}, par hameçonnage ou par manque de robustesse des mots de passe, la répétition de ce type de compromission montre la nécessité de sécuriser les accès distants aux systèmes d'information, de s'appuyer sur une identité numérique fiable et maîtrisée et de généraliser l'usage de l'authentification multi-facteurs. C'est tout l'enjeu de la deuxième version du Référentiel d'Identification Electronique dont le déploiement dans les mois à venir est porté par le projet HospiConnect.

L'analyse des indicateurs présentés dans cet observatoire rappelle que, grâce au travail déjà accompli, la dynamique est engagée. Malgré un niveau de cybermenace qui reste élevé, les actions collectives mises en place depuis plusieurs années permettent d'y apporter une meilleure réponse. Cependant les efforts doivent être poursuivis, surtout dans un contexte d'aggravation des tensions géopolitiques mondiales pouvant entraîner le franchissement d'un nouveau palier de la menace.

Collectivement, poursuivons l'effort avec la même énergie pour renforcer durablement la cybersécurité du système de santé.

Bonne lecture !

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 d'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 CSIRT¹ 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 chargé de la Santé en coordination étroite avec les autorités gouvernementales en charge de la cybersécurité.

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

¹ Computer Security Information Response Team

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 consistent à :

- ▶ traiter le signalement sur le portail des signalements des événements 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 chargé de la santé et/ou les autorités compétentes de l'Etat selon la nature 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 Directory², désactivation massive de comptes, etc.) ;
- ▶ assistance à l'identification de la menace et du scénario complet de la compromission (collecte et analyse de journaux d'événements 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) ;

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

- ▶ 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 traitement des incidents reste la responsabilité des structures déclarantes.

Le CERT Santé propose également un accompagnement dans les phases d'identification et de déploiement de mesures de sécurité (notamment dans le cadre d'une procédure de durcissement post-incident) :

- ▶ proposition et fourniture d'un avis sur les 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.

Permanence 24/7

Le CERT Santé assure un service de réponse à incident accessible 24h/24 et 7j/7. Pendant les heures non ouvrées, 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](#) 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, de technologies de santé ou de 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.).

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. Ce service national 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 scanners 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 cyberveille³.

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.

³ <https://cyberveille-sante.gouv.fr/cybersurveillance>

3 Synthèse de l'activité en 2025

Le nombre total d'incidents déclarés (764 signalements) a légèrement augmenté par rapport à 2024 (749). Le nombre d'établissements (606) ayant déclaré au moins un incident est en augmentation de 9% par rapport à 2024. Cela est lié à l'augmentation significative (+50%) du nombre d'établissements et service médico-sociaux ayant déclaré au moins un incident. 71 établissements ont bénéficié d'un appui technique de la part du CERT Santé (contre 75 en 2024).

La compromission du SI est la menace la plus importante en 2025. Il est intéressant de noter que le nombre d'incidents lié aux rançongiciels est en baisse de 30% par rapport à 2024. Ils concernent majoritairement des établissements et services médico-sociaux. Ces établissements ont été contraints de mettre en place un mode de fonctionnement dégradé qui a pu s'étendre sur plusieurs semaines.

Le nombre d'incidents ayant un impact sur la prise en charge des patients est en augmentation par rapport à 2024 (de 24%). En effet, 288 signalements reçus en 2025 indiquent que les établissements ont été contraints de passer en mode dégradé ou d'interrompre la prise en charge des patients soit 38% des signalements reçus. Seuls 25% 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.

Le nombre d'incidents majeurs poursuit sa baisse (2 en 2025 contre 3 en 2024).

Enfin, l'ANS est intervenue en 2025 auprès de 9 prestataires de solutions métier suite à l'identification de vulnérabilités présentes sur des serveurs exposés sur Internet. Ces vulnérabilités ont été remontées majoritairement par des établissements de santé mais également par l'ANSSI ou dans le cadre d'un audit de cybersurveillance. L'ANS réalise un suivi régulier de l'avancement du développement des correctifs et de leur déploiement par les éditeurs concernés.

4 OBSERVATOIRE DES SIGNALEMENTS

4.1 Chiffres clés pour la période 2024-2025

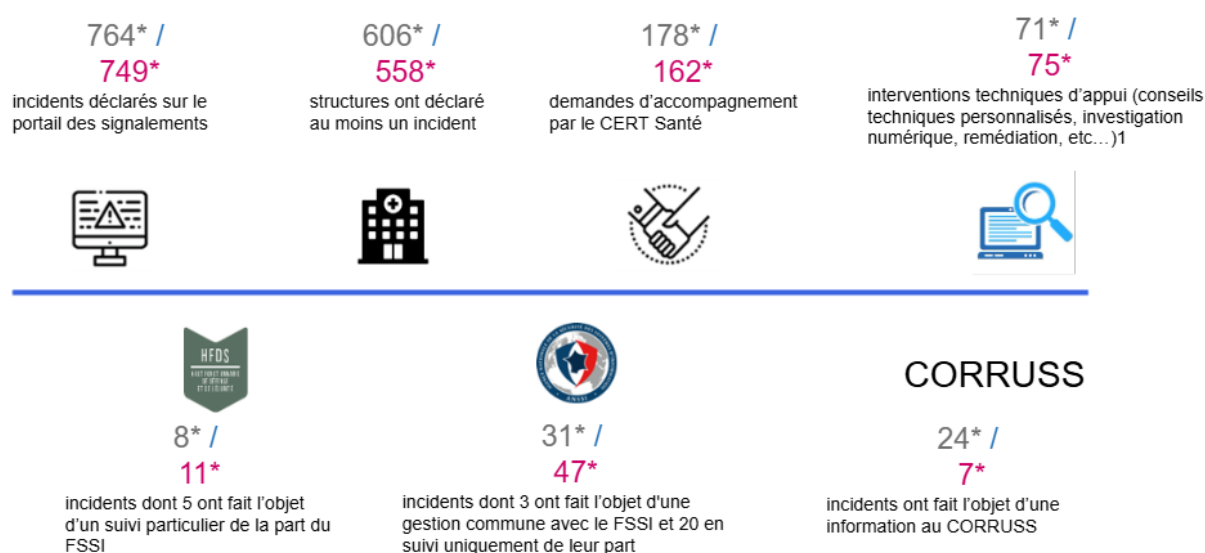


Figure 1 - Chiffres clés des signalements déclarés en 2024 et 2025

En coordination avec le CERT Santé, l'ANSSI et le FSSI sont intervenus directement au profit de 30 établissements dans le cadre du suivi de la gestion d'un incident ou l'appui à la réponse. Certaines structures ont bénéficié de plusieurs interventions. Le FSSI est intervenu auprès de certains prestataires sectoriels.

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

- 18 établissements de santé publics, dont 9 opérateurs de services essentiels (OSE), victimes de rançongiciel, de compromissions de comptes (AD, VPN ou messagerie) ou de fuites de données ;
- 4 EHPAD, deux établissements de santé privés, deux laboratoires de biologie médicale et un établissement de service médico-social victimes de rançongiciels, de compromission de comptes (AD) et de fuites de données.

Pour le FSSI du ministère, il s'agit de :

- 8 établissements dont 3 OSE. Ces incidents étaient liés à des attaques par rançongiciel, exfiltration de données et Faux Ordres de Virement Bancaire (FOVI).

●● Evènements marquants de la période ●●

La FEDERATION ADMR DU CALVADOS est victime du rançongiciel RansomHub entraînant un chiffrement de ses données. L'établissement a été contraint de fonctionner en mode dégradé pendant plusieurs jours.

Les Laboratoires de Biologie Médicale CERBALLIANCE Provence-Azur et Alpes Durance sont victimes d'une intrusion. Des "milliers de données" administratives de patients (noms, prénoms, adresses mail et numéro de téléphone) sont exfiltrées.

Le CHD STELL est victime d'une attaque par le rançongiciel du groupe RansomHub. L'établissement a été contraint de fonctionner en mode dégradé pendant plusieurs jours.

Le groupe INOVIE LABOSUD a été victime d'une intrusion. Un tiers illégitime accède potentiellement à des données à caractère personnel de plusieurs millions de personnes.

De nombreux établissements sont victimes de l'interruption de service du logiciel médical WEDA à la suite d'une cyberattaque ayant touché l'éditeur. Les établissements ont été contraints de fonctionner en mode dégradé pendant plusieurs jours.



L'AFAPEI SUD ALSACE est victime d'un incident de cybersécurité entraînant un chiffrement de ses données. L'établissement a mis en œuvre son plan de gestion de crise, permettant un retour progressif à la normale et un renforcement de son dispositif de sécurité.

Le CH de PEZENAS est victime d'une attaque par le rançongiciel Makop. L'établissement a été contraint de fonctionner en mode dégradé pendant plusieurs jours et une partie des sauvegardes a été touchée.

Les GRADEs ont subi une compromission de comptes de professionnels de santé, entraînant une fuite de données. L'accès à certains outils régionaux a été coupé pendant plusieurs jours.

Le Centre Médico-Psychopédagogique de Chennevières-sur-Marne est victime d'une attaque par rançongiciel du groupe Lockbit Black. L'établissement a été contraint de fonctionner en mode dégradé pendant plusieurs jours.

Figure 2 - Evènements marquants de l'année 2025

4.2 Informations générales sur les signalements

764 incidents ont été déclarés en 2025. Ce nombre est en augmentation par rapport à 2024 (749). Pour mémoire, 581 incidents avaient été déclarés en 2023.

Parmi ces incidents, on compte des incidents « hors périmètre » (41 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 (2).

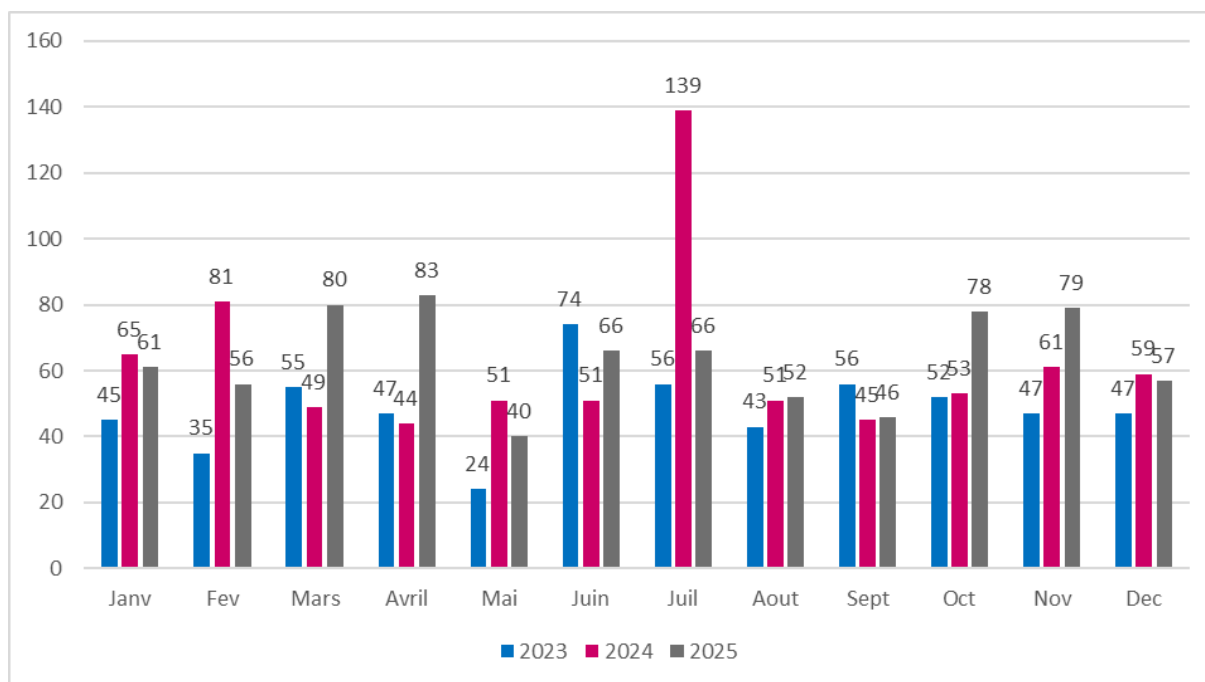


Figure 3 - Nombre de signalements par mois

On compte en 2025 une moyenne de 64 déclarations par mois (62 en 2024).

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

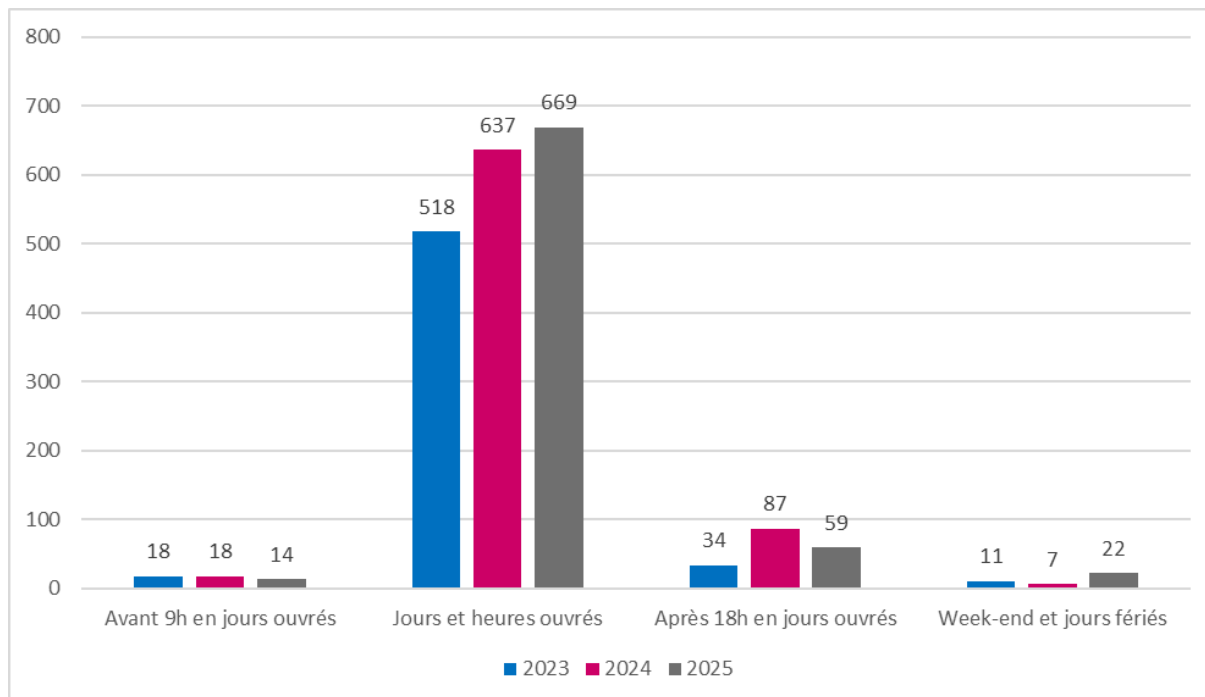


Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt

87% des signalements ont été effectués en heures et jours ouvrés (HO/JO) en 2025, en augmentation de 5% par rapport à 2024. On constate une baisse significative de la part des incidents déclarés après 18h en jours ouvrés. La part des incidents déclarés entre 18h et 18h30 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. 31 demandes d'accompagnement ont été formulées durant ces périodes. Parmi celles-ci, huit structures (trois établissements de santé publics, un établissement de santé privé à but non lucratif, un établissement de santé privé lucratif et trois ESMS) nécessitaient un appui pour donner suite à des attaques par rançongiciel entraînant un fonctionnement dégradé des activités support ou du système de prise en charge des patients, à des compromissions du SI ou à une attaque par brute force.

16 incidents ont été pris en charge en 2025 par l'**astreinte du CERT Santé** suite à un appel téléphonique en HNO (en baisse de plus de 54% par rapport à 2024). 5 ont fait l'objet d'un appui technique en heures ouvrées (4 en 2024).

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.

●● Etat des incidents lors de leur signalement ●●

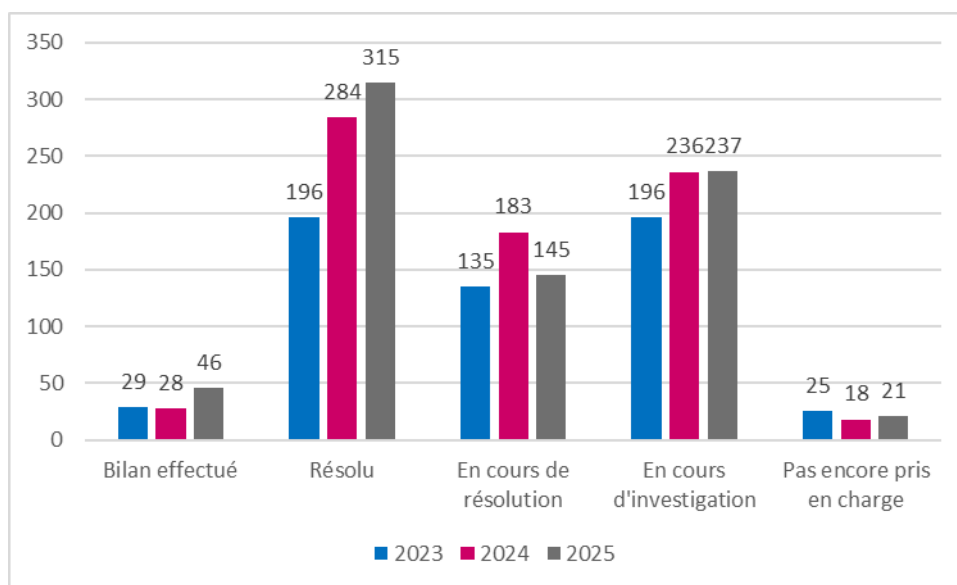


Figure 5 - Etat des incidents lors de leur signalement

Les incidents déclarés dans un état résolu est en constante évolution. En 2025, plus de la moitié (60%) 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 est similaire à l'année précédente soit **31%**.

20 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 baisse rapport à 2024. 55% de ces incidents étaient potentiellement**

d'origine malveillante (rançongiciel, compromissions du SI (AD ou messagerie, vol d'équipement, défacement de site, fuite d'information) contre 35% en 2024.

C'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2025**. Il est **très légèrement supérieur à celui de 2024 (22%)**.

23%

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, etc.) et ne sont pas suffisamment réactifs dans la mise en place de solutions de remédiation.

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

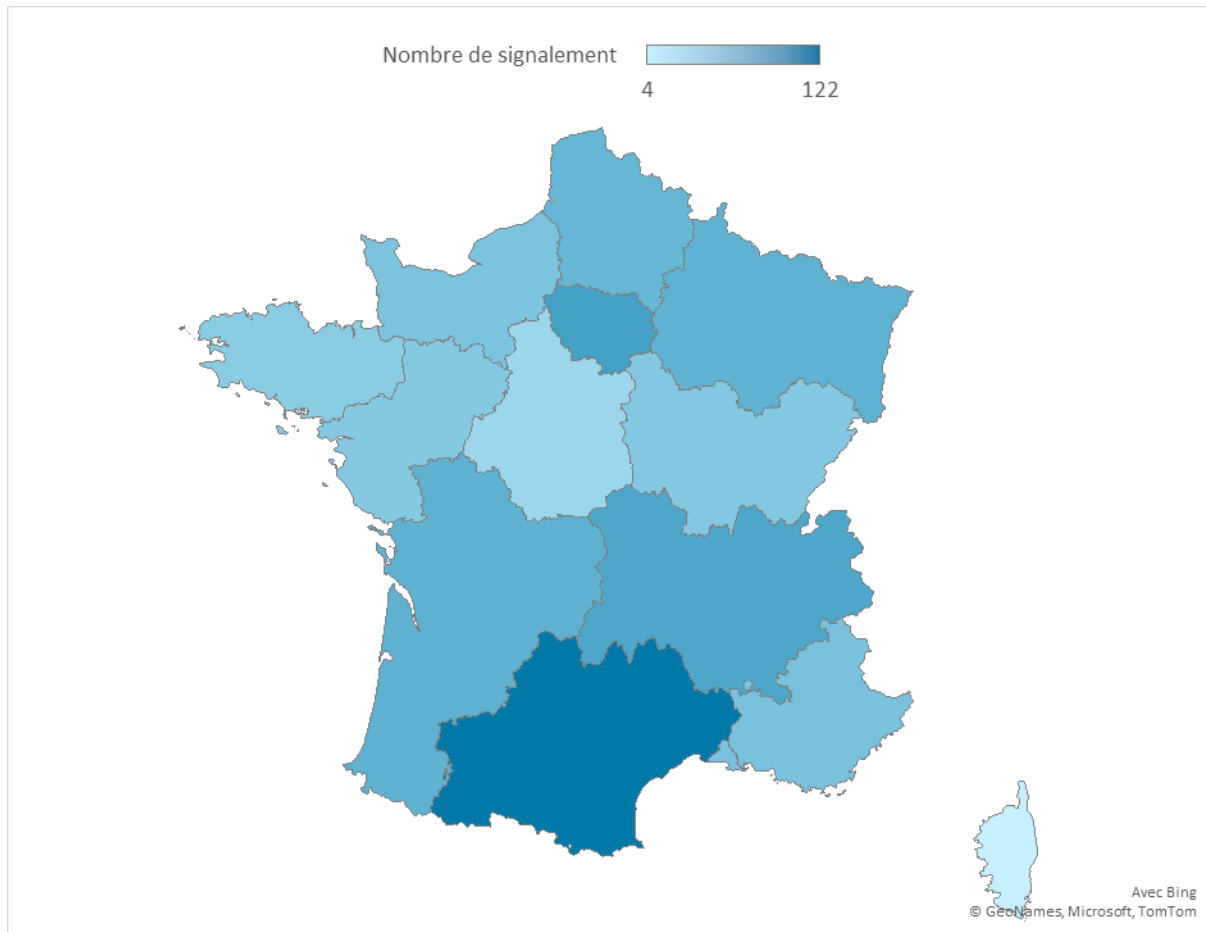




Figure 6 - Répartition des signalements par région

Les régions pour lesquelles le nombre de signalements est le plus important sont l'Occitanie (122), l'Île-de-France (82) et l'Auvergne-Rhône Alpes (76). Ces trois régions représentent à elles seules plus de 37% du total des signalements.

●● Nombre de signalements rapporté à l'activité hospitalière par région ●●

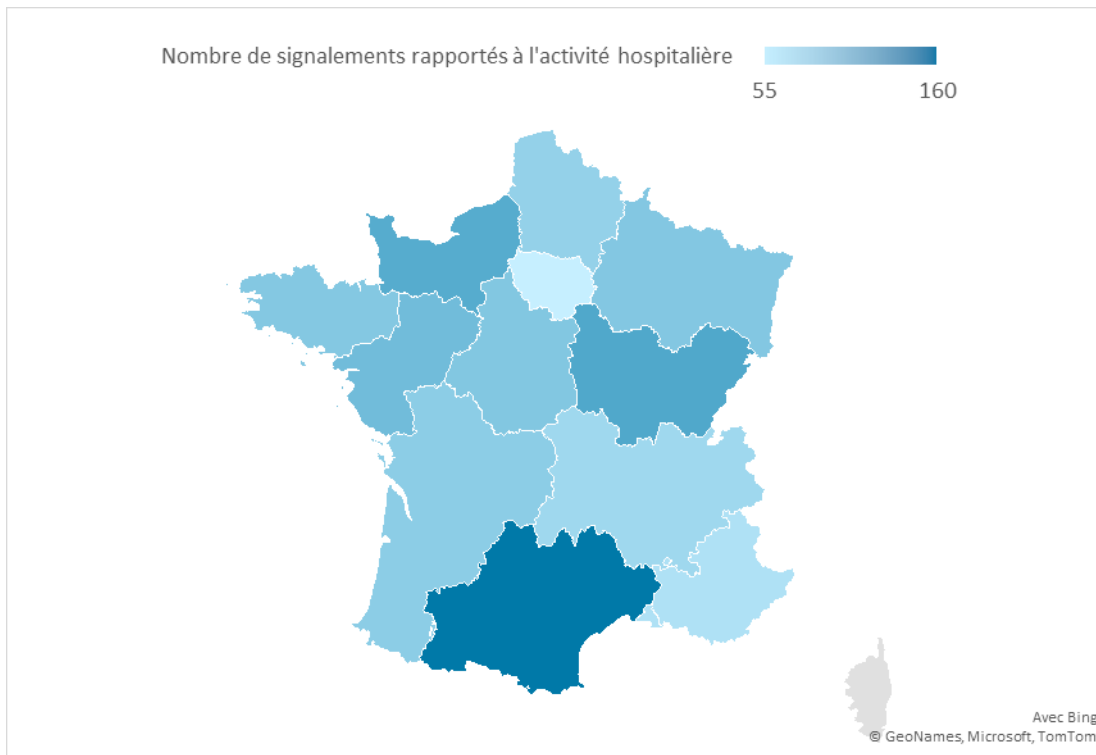


Figure 7 - Nombre de signalements rapporté à l'activité hospitalière par région

Cette carte présente le ratio entre le nombre de signalements et l'activité hospitalière rapportée au niveau national⁴ : 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 en raison du faible taux d'activité hospitalière par rapport à la métropole. La région avec le ratio le plus élevé (Occitanie) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (9% de l'activité nationale), la région Occitanie est largement en tête en matière de remontée des incidents. La région Bourgogne-Franche-Comté arrive en deuxième position et la région Normandie en troisième.

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

⁴ Instruction N° DGOS/PF5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme HOP'EN

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.

●● Répartition des signalements selon le type de structure ●●

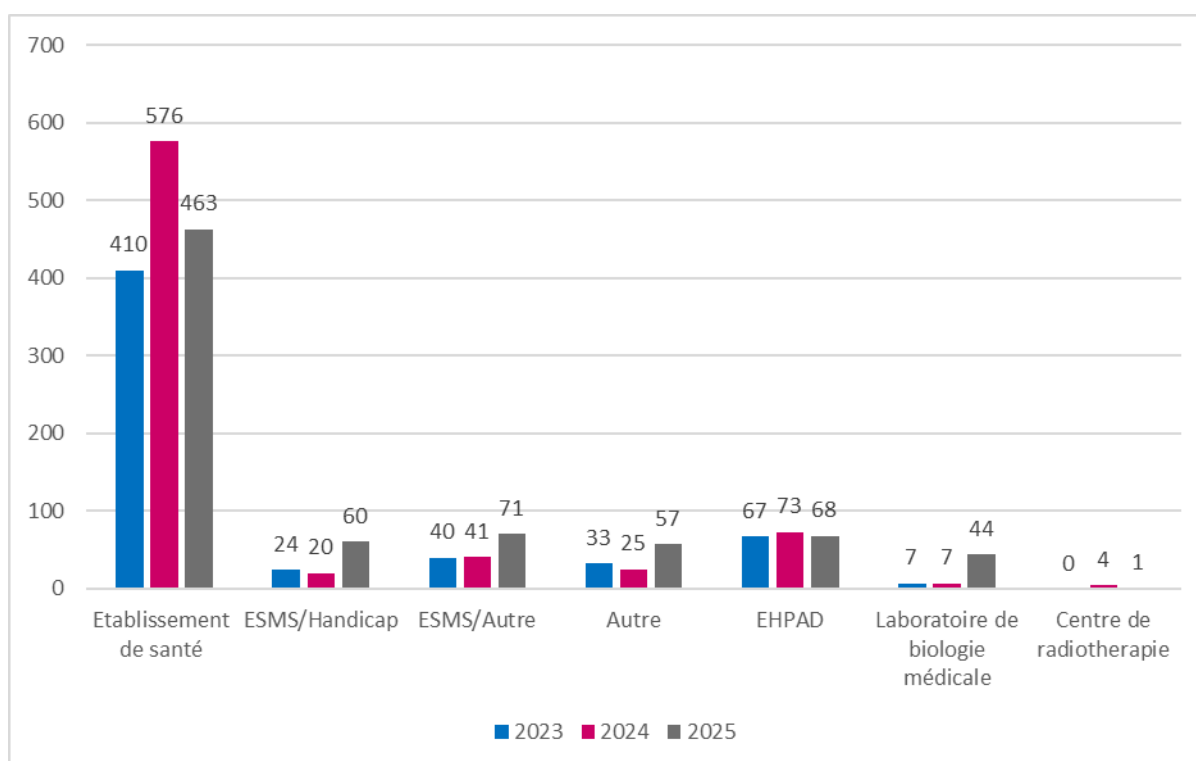


Figure 8 - Répartition des signalements selon le type de structure

Malgré une baisse de 20%, la majorité (61%) des incidents de sécurité est toujours déclarée par les **établissements de santé** (voir détail figure 8). On note une augmentation significative des déclarations des ESMS (+48%) et des laboratoires de biologie médicale (principalement des groupes). Cette dernière catégorie a été fortement impactée par des cyberattaques ayant entraîné une fuite de données.

●● 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) ●●

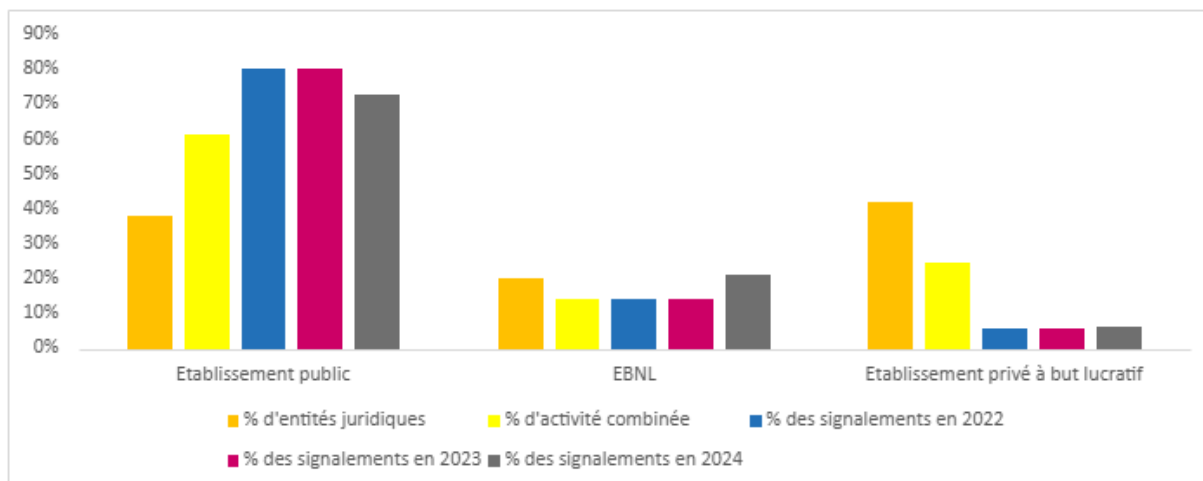


Figure 9 - Part des signalements comparée à la part des établissements selon leur raison sociale

Les parts des types d'établissements dans la déclaration des incidents en 2025 sont stables par rapport à 2024. Les établissements de santé publics déclarent toujours le plus d'incidents (78%) alors qu'ils ne sont que 38% 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 ;
- ils représentent une plus grande activité hospitalière (61% de l'activité combinée), 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.

115 établissements désignés OSE ont déclaré au moins un incident en 2025.

93

C'est le nombre de structures ayant déclaré plus de 2 incidents durant l'année 2025 sur 606 structures au total. Parmi elles, il y avait une très grande majorité d'établissements de santé (68). 8 établissements de santé ont signalé au moins quatre incidents.

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

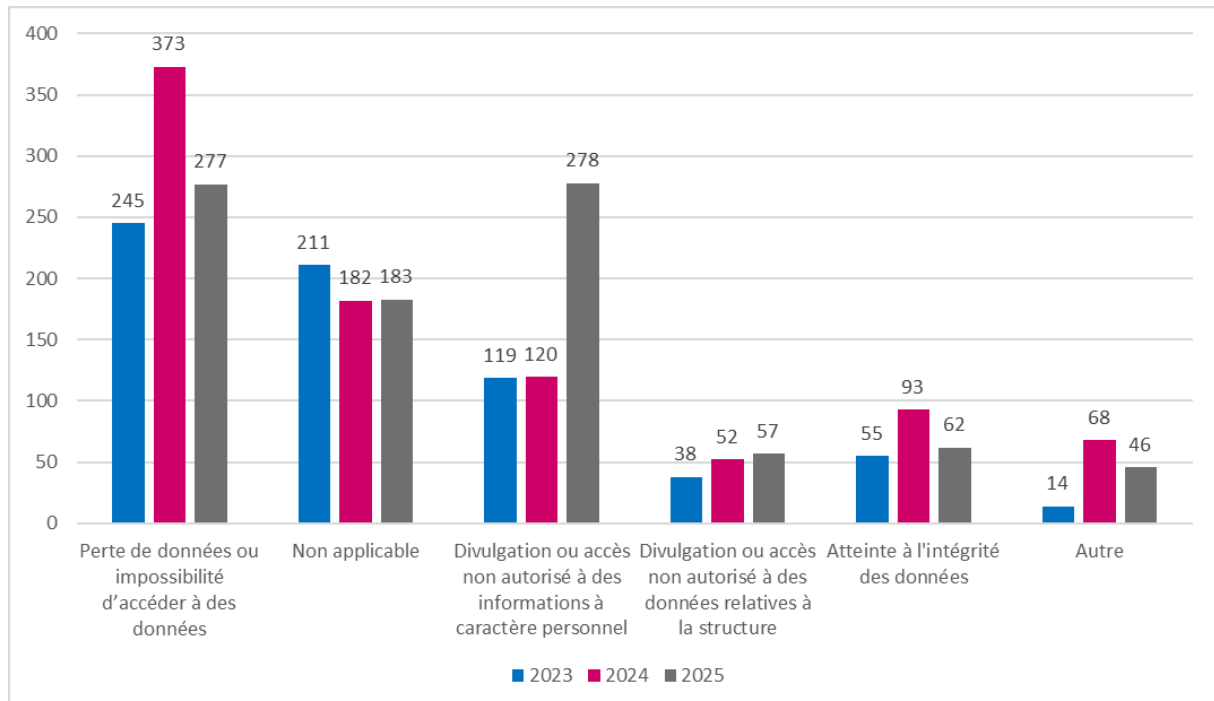


Figure 10 - Répartition selon les types d'impact sur les données

Le nombre d'incidents entraînant une divulgation ou un accès non autorisé à des données à caractère personnel a connu une forte augmentation en 2025 (plus du double de 2024). La première origine est l'accès illégitime aux plateformes en ligne suite à la compromission d'un ou plusieurs comptes d'accès ou l'exploitation d'une vulnérabilité (logicielle ou liée à une mauvaise configuration). La deuxième cause importante est la compromission de comptes de messagerie suite à un vol d'authentifiants par l'hameçonnage, le harponnage ou la recherche de mot de passe par force brute. Les incidents signalés où tout ou une partie des données des applications de la structure étaient devenues inaccessibles ont diminué de 26% par rapport à 2024. Il s'agit également d'incidents chez les fournisseurs de logiciels métier (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.

50%

C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2025. Ce chiffre est en légère baisse par rapport à 2024 et 2023.

49%

C'est le pourcentage de structures qui ont été contraintes de mettre en place en 2025 un **fonctionnement en mode dégradé** du système de prise en charge des patients (20% de plus qu'en 2024).

Ce mode dégradé dépend de la nature de l'incident et des procédures mises en place dans les structures : application du plan de continuité d'activité, 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. 20% des établissements ayant eu recours au mode dégradé ont subi une interruption du système de prise en charge d'un patient.

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

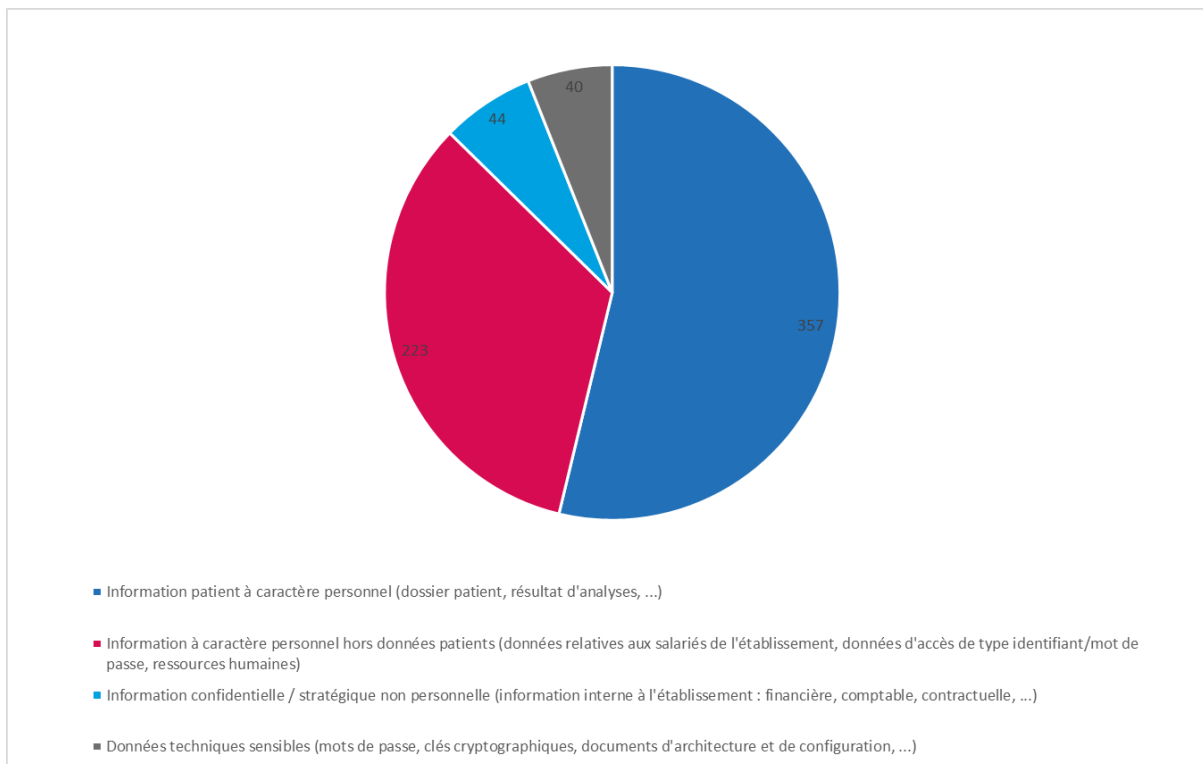


Figure 11 - Répartition selon les types de données impactées

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.

21% 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, **54%** touchent des **données de santé à caractère personnel**, 34% des informations à caractère personnel hors données patient (principalement des identifiants de comptes utilisateur), 6% des données techniques sensibles et enfin 6% des informations confidentielles ou stratégiques. Les données à caractère personnel sont donc toujours les premières atteintes par les incidents de sécurité déclarés. Ces chiffres sont stables par rapport à 2024.

●● Mise en danger potentielle des patients ●●

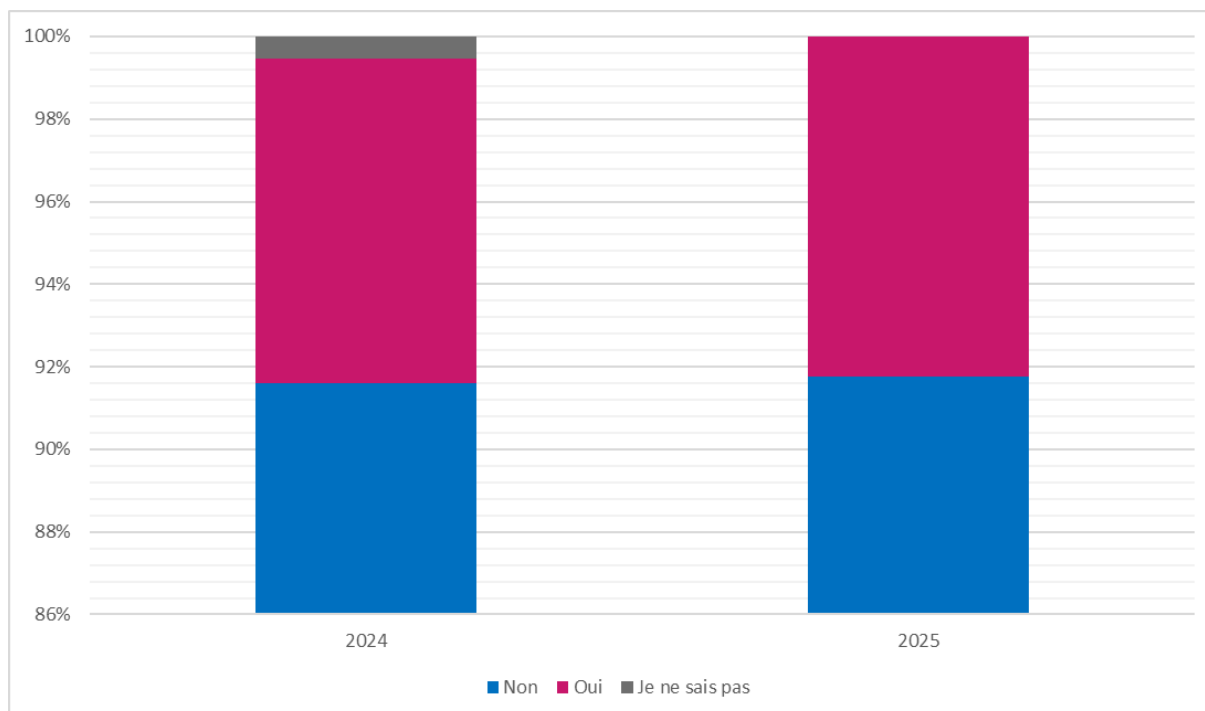


Figure 12 - Mise en danger potentielle des patients

Parmi les **63 mises en danger patient potentielles** recensées en 2025 (8% du nombre total d'incidents), **8 incidents ont entraîné une mise en danger patient avérée**.

Les 55 incidents restants, correspondant à la part des mises en danger potentielles de patients, ont été attribués à diverses causes. Il s'agit notamment d'incidents de cybersécurité impactant des fournisseurs, 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 d'origine malveillante ou non malveillante ●●



Figure 13 - Répartition selon le type d'incident

Parmi **les incidents déclarés, 400 sont d'origine malveillante** (+22% par rapport à 2024) **et 323 d'origine non malveillante**. Dans l'analyse détaillée de ces deux catégories d'incidents, sont exclus les 41 signalements dits « Hors périmètre » n'ayant pas fait l'objet d'un traitement particulier (contre 22 en 2024). Lorsqu'un incident d'origine malveillante concerne un prestataire d'un service numérique ayant impacté plusieurs structures déclarant l'incident et ses impacts en termes de disponibilité du service, il est comptabilisé dans les statistiques comme un unique incident d'origine malveillante.

Les actes malveillants

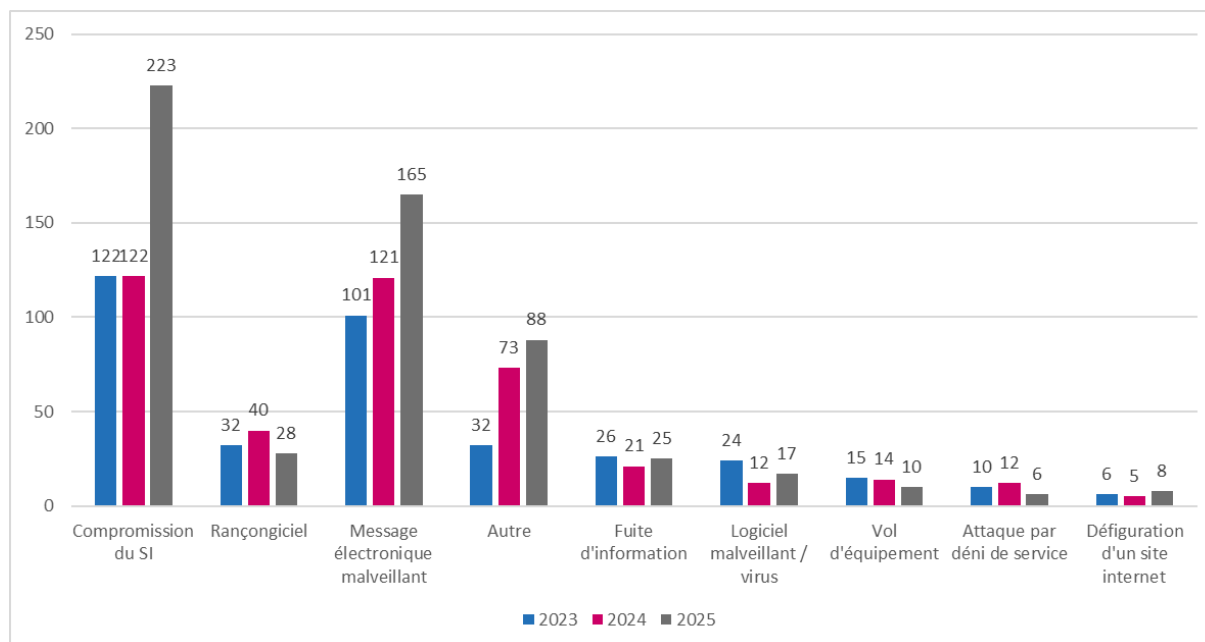


Figure 14 - Nombre d'incidents par type d'origine

L'année 2025 a été marquée, comme 2024, par une forte activité malveillante relative au vol d'identifiants (login – mot de passe) : comptes de messagerie, comptes d'accès à distance, comptes utilisateurs ou de maintenance d'applications métier. L'activité des infostealers⁵ et d'hameçonnage constitue toujours les menaces de vol les plus importantes.

Sur les 28 attaques par rançongiciels répertoriées tout au long de l'année, 12 ont impacté plusieurs serveurs de l'établissement (pour certains les contrôleurs de domaines ont également été touchés), 12 ont impacté un seul serveur et 4 concernaient uniquement un poste de travail. Deux incidents concernaient des prestataires et ont entraîné 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 précédées par une exfiltration d'informations confidentielles ou sensibles.

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 plus de 120 bénéficiaires du CERT Santé

⁵ Logiciel malveillant s'infiltrant sur le système de la victime pour voler des données

ont été alertés concernant l'exposition d'un service numérique potentiellement vulnérable.

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 bancaire par mail et par téléphone des services administratifs. Les fraudes au président et les tentatives de FOVI par usurpation d'identité sont en augmentation.

Notons que la moitié des incidents (50%) relève de plusieurs types de malveillance. Par exemple, une attaque par rançongiciel, suite à 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 compromission du SI a fait l'objet d'une analyse particulière. En effet, ont été distingués pour ce type d'incidents les différents vecteurs de compromission des SI : AD, VPN, Messagerie, ou Autre.

Les compromissions via un accès VPN représentaient 5%, par l'AD 8%, les compromissions de messagerie 50%, et enfin, la catégorie Autre 25% (comptes applicatifs ou de maintenance).

A nouveau, plusieurs types de compromissions peuvent être pertinents.

Les vecteurs de compromission majoritaires pour les incidents à criticité significative ou importante est la compromission par l'accès VPN (40%) et un compte AD (33%).

La catégorie « Logiciel malveillant / virus » correspond principalement à des logiciels collectant et exfiltrant des données à caractère personnel ou exécutant un navigateur avec un moteur de recherche malveillant.

53%

C'est le pourcentage des incidents qui ont une origine malveillante en 2025. Ce chiffre **est en forte hausse** comparé à l'année précédente.

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

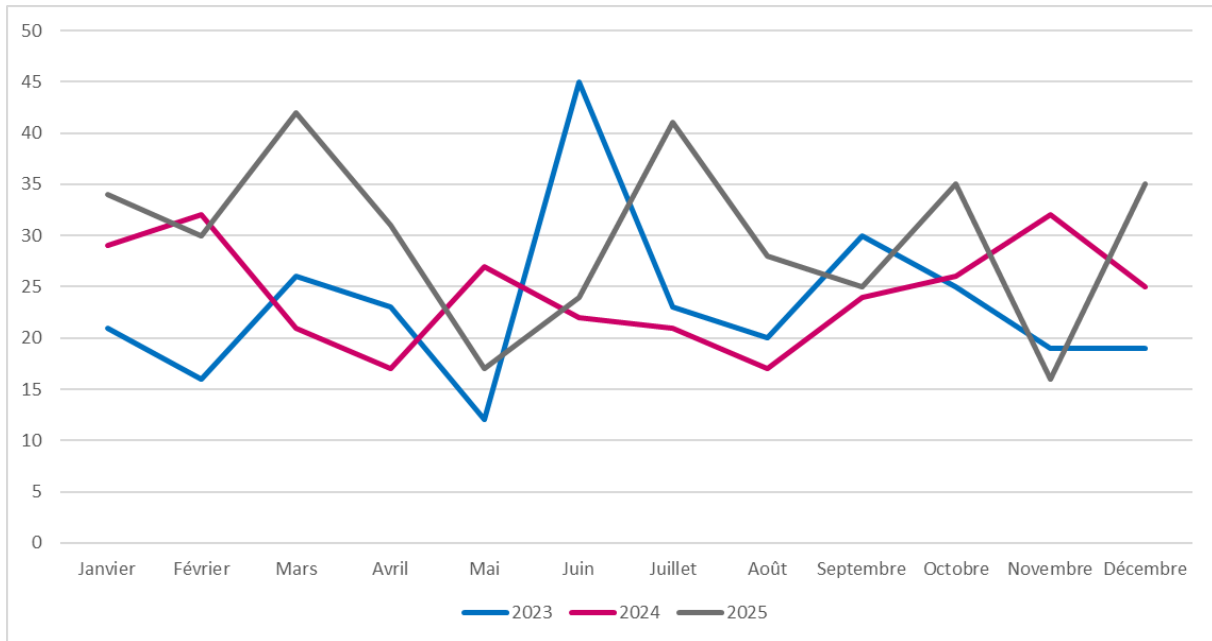


Figure 15 - Evolution du nombre d'incidents dont l'origine est malveillante

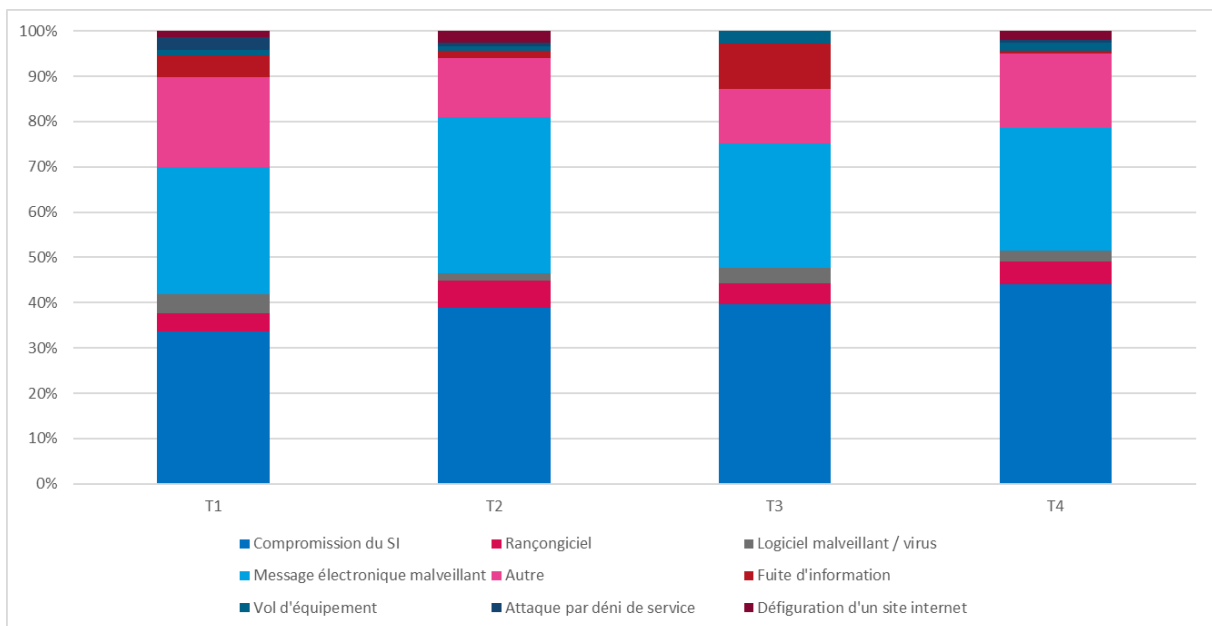


Figure 16 - Origine malveillante des incidents par trimestre

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 :

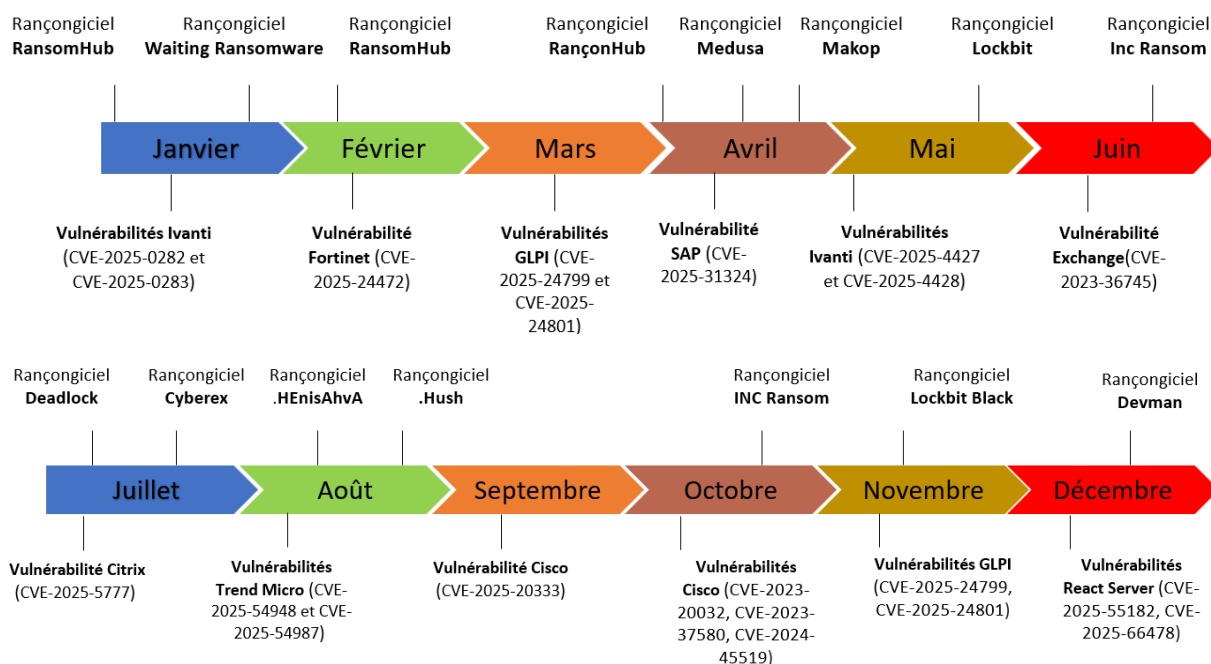


Figure 17 - Chronologie des cybermenaces identifiées en 2025

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

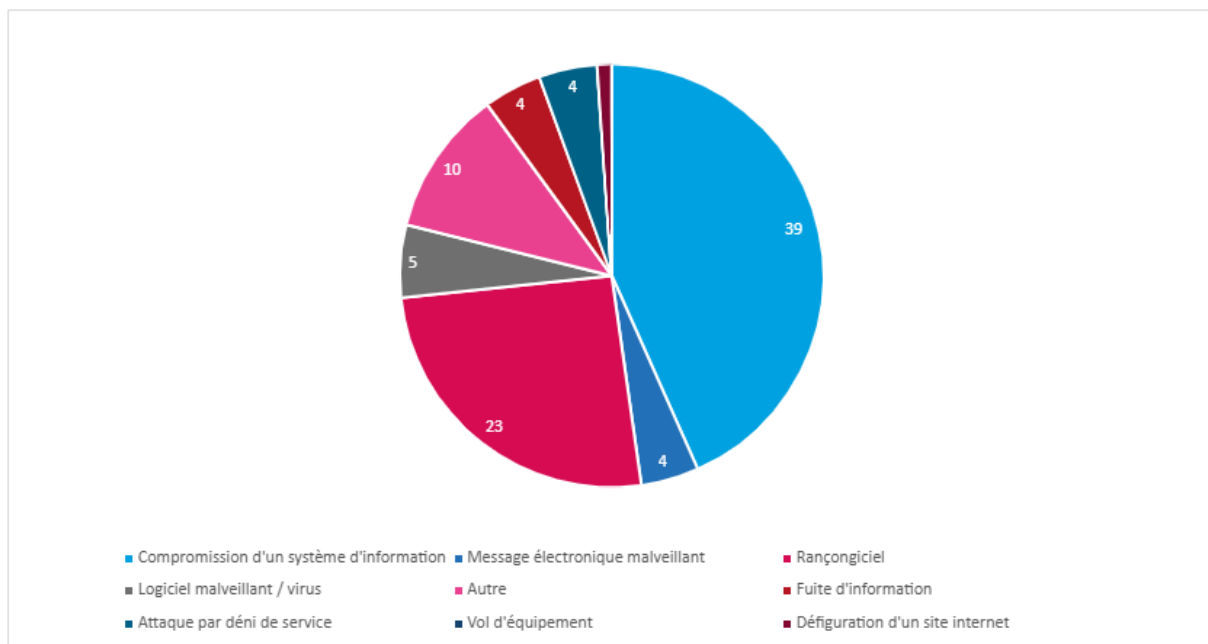


Figure 18 - Origine des incidents pour lesquels un appui technique a été apporté par le CERT Santé

Le nombre de déclarations d'incident assorties d'une demande d'accompagnement a augmenté en 2025. Il y a eu au total 194 demandes d'accompagnement, soit 25% des incidents signalés. Ce sont les ESMS (44%) 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 71 accompagnements techniques réalisés par le CERT Santé, 6 constituaient une levée de doute face à un faux positif, soit 8% 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, de la documentation de l'ANSSI, aux conseils plus techniques comme la mise en place de durcissement de systèmes, etc.

Neuf établissements (cinq établissements sanitaires, trois ESMS et un groupe de laboratoires) ont sollicité un prestataire externe de réponse à incidents pour une assistance dans la gestion de l'incident. Six d'entre eux ont fait appel à un prestataire avant de faire la déclaration au CERT Santé, en particulier pour rechercher l'origine de la compromission. Deux interventions ont été réalisées dans le cadre d'un contrat d'assurance cyber.

Le neuvième a contractualisé avec un PRIS sur la recommandation du CERT FR et du CERT Santé. Le prestataire a principalement contribué à la reconstruction du système d'information de l'établissement qui a été fortement impacté par une attaque par rançongiciel.

Des prestations de SOC ou des solutions de détection des activités malveillantes (type EDR) au sein des établissements ont permis de bloquer des activités qui auraient pu avoir un impact important sur la sécurité et l'intégrité du système d'information : détection et blocage d'un rançongiciel, d'un mouvement latéral, infostealer, vers ou virus, spyware/grayware et hameçonnage.

Les signalements d'origine non malveillante

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

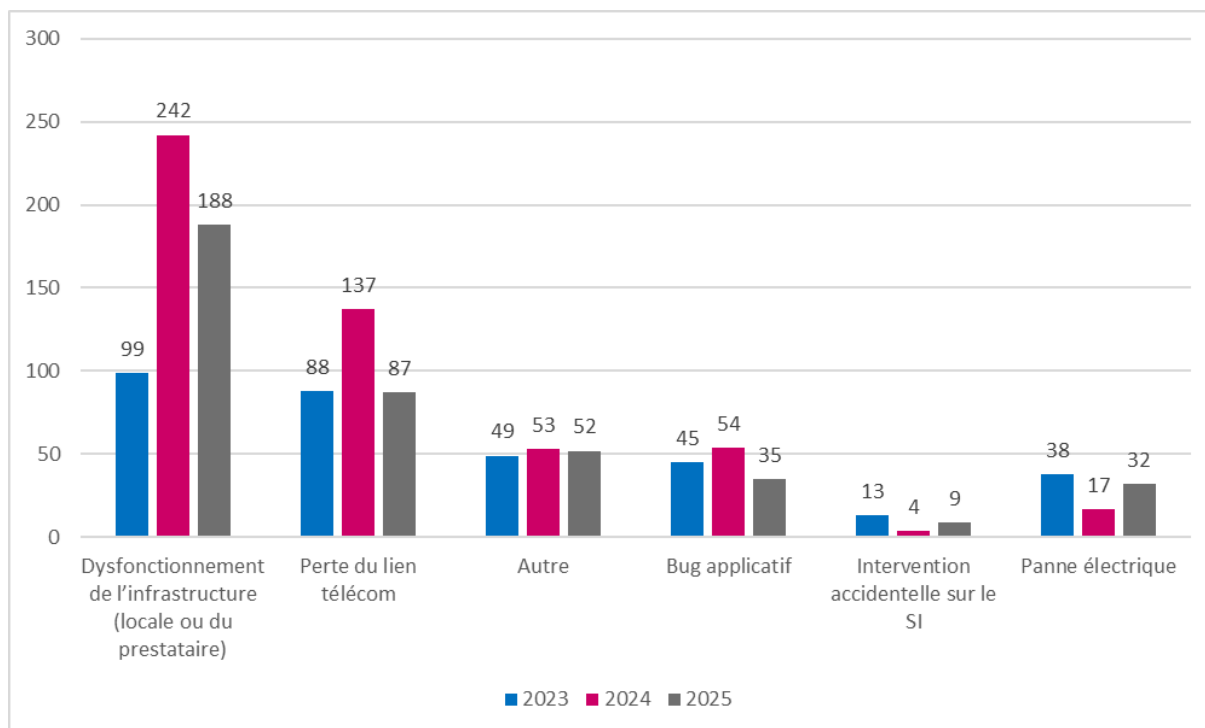


Figure 19 - Origine non malveillante des incidents

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 58%**. On compte, parmi ces cas, 75% de dysfonctionnements du côté des prestataires contre 25% de dysfonctionnements de l'infrastructure locale.

La perte du lien télécom est la deuxième source d'incident d'origine non malveillante (27%). Cette perte peut fortement impacter le fonctionnement des activités métier des établissements, en particulier ceux disposant d'un service d'urgences ou un SAMU. Ce type d'incident est généralement traité en priorité par les opérateurs.

Même s'ils sont en diminution de 27% par rapport à 2024, (de 27%), ces deux types d'incidents représentent toujours une part significative des incidents d'origine non malveillante (85%).

Le nombre de déclarations lié à un **bug applicatif** (11%) est en baisse par rapport à 2024. 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.

Sur les 52 incidents liés à un bug, seuls 5 établissements ont bénéficié d'une intervention de l'éditeur de la solution pour développer un correctif.

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 événements informatiques à l'origine de comportements imprévus de systèmes mais qui se sont révélés être des « faux positifs » après une investigation du CERT Santé.

47%

C'est la part d'incident d'origine non malveillante en 2025 des incidents, ce chiffre est en forte baisse par rapport à 2024.

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

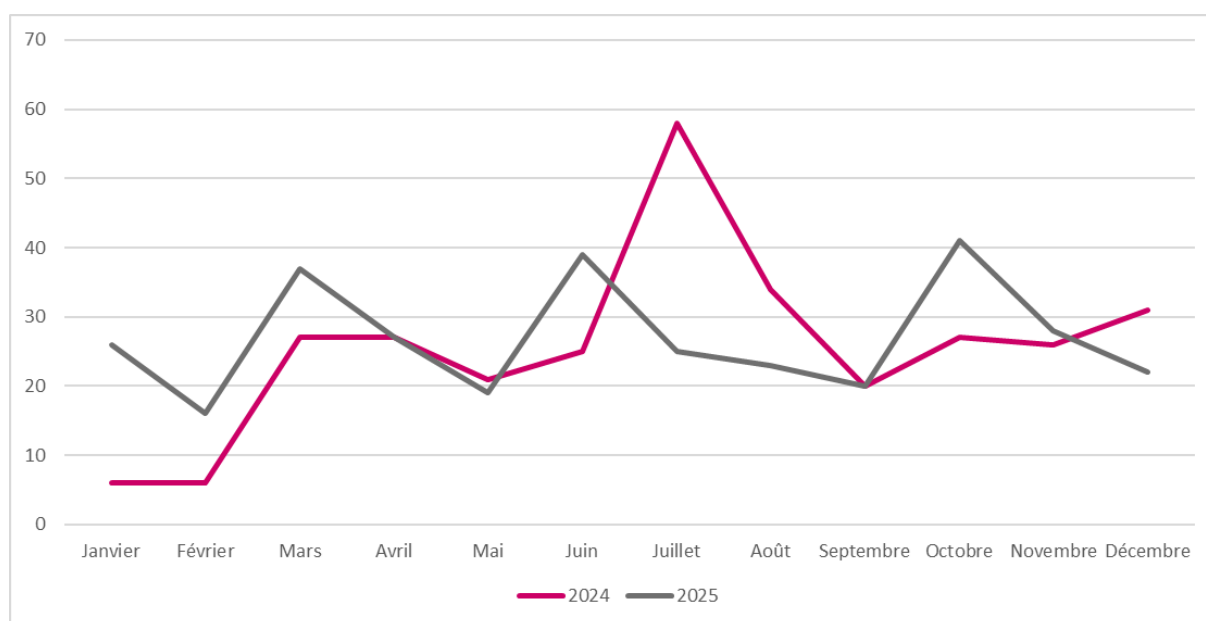


Figure 20 - Evolution du nombre d'incidents dont l'origine est non malveillante

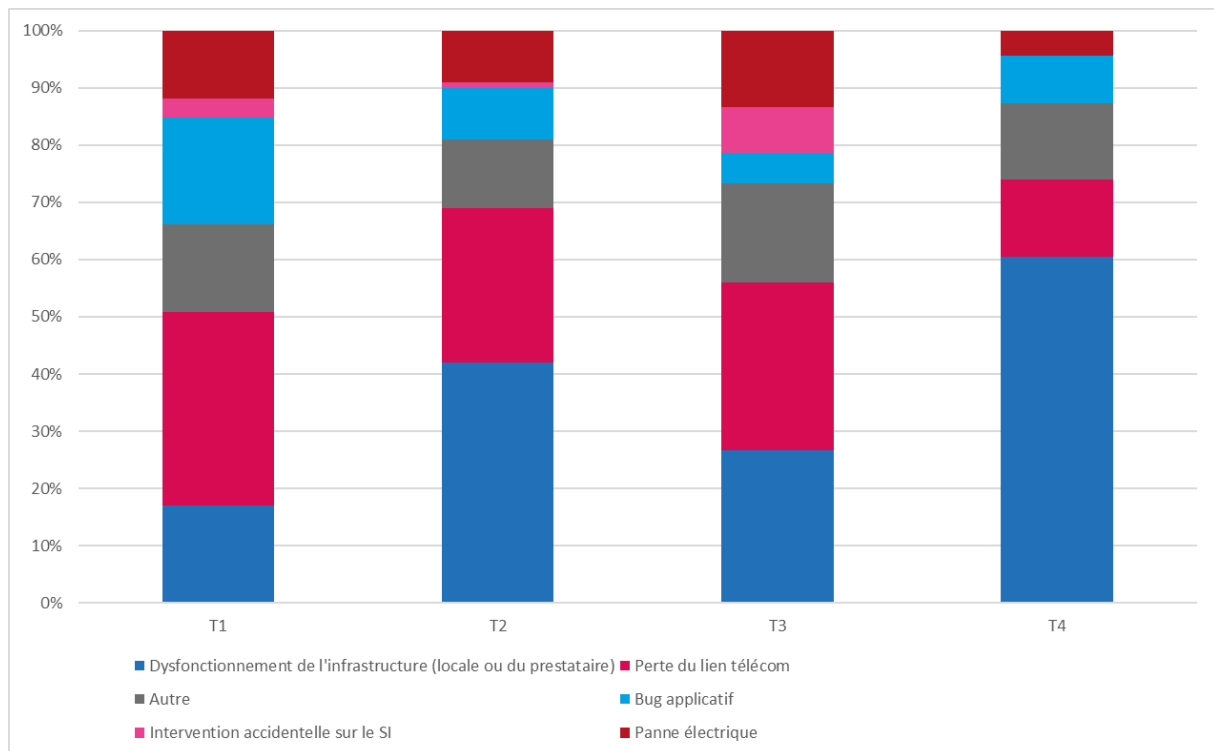


Figure 21 - Origine non malveillante des incidents par trimestre

4.3 Publication d'alertes sur le portail cyberveille

En 2025, 121 alertes ont été publiées sur le portail cyberveille (134 en 2024) parmi lesquelles des vulnérabilités critiques activement exploitées concernant :

- 4 vulnérabilités sur les solutions Cisco permettant à un attaquant non authentifié et selon différents modes opératoires d'exécuter du code arbitraire avec des privilèges root ;
- 4 vulnérabilités sur les solutions VPN Fortinet permettant à un attaquant non authentifié et selon différents modes opératoires d'exécuter du code arbitraire ;
- 5 vulnérabilités sur l'environnement Windows permettant à un attaquant selon différents modes opératoires d'exécuter du code arbitraire avec des privilèges SYSTEM ;
- 3 vulnérabilités sur les solutions VPN Ivanti permettant à un attaquant non authentifié et selon différents modes opératoires d'exécuter du code arbitraire ;
- 3 vulnérabilités sur les solutions d'accès à distance Citrix permettant à un attaquant non authentifié et selon différents modes opératoires d'exécuter du code arbitraire ou de récupérer les informations de connexion d'une session active.

5 SERVICE NATIONAL CYBERSURVEILLANCE

Le nombre d'audits réalisés a fortement diminué en 2025. De nombreux audits de l'exposition sur Internet des établissements ont en effet été réalisés par des industriels au travers du programme CaRE selon le cahier des charges élaboré par le CERT Santé.

Ainsi en 2025, 144 audits ont été réalisés : 111 CH membres de 34 GHT (pour 19 GHT, plus de 50% des ES ont été audités), 22 établissements sanitaires hors GHT, 7 ESMS, trois GRADeS et une maison de santé.

Parmi les 111 établissements appartenant à des GHT, 22 exposaient un système avec au moins une vulnérabilité critique (obsolescence d'un composant avec un score CVSS⁶ supérieure ou égal à 9) et 46 avec au moins une vulnérabilité haute (exposition d'un service de gestion du SI sur internet).

Le service est toujours très apprécié par les bénéficiaires du CERT Santé. Parmi ceux qui ont répondu au questionnaire de satisfaction qui leur a été envoyé à l'issue de l'audit, 86% étaient satisfaits ou très satisfaits concernant le processus de commande des audits et par le contenu du rapport d'audit délivré à la suite de sa réalisation.

⁶ Common Vulnerability Scoring System (CVSS) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables.

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 582 structures en 2025. 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 nombre significativement plus important de structures alertées en 2025 (45% de plus qu'en 2024) s'explique par l'introduction d'un service de recherche de fuite d'identifiants concernant un grand nombre d'établissements.

Le CERT Santé a relayé plus de 64 alertes concernant des compromissions avérées ou potentielles de SI identifiées par l'ANSSI.

Sur l'ensemble des alertes envoyées par le CERT Santé, 60 concernaient des compromissions avérées de comptes ou d'applications (BAL, VPN, comptes applicatifs, Exploit). La très grande majorité concernait des comptes de messagerie (56).

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, s'est poursuivie en 2025.

Si cette dynamique est réelle, il est indispensable qu'elle se poursuive dans les prochains mois, en raison du risque de franchissement d'un nouveau palier de la cybermenace dans un contexte d'aggravation des tensions géopolitiques mondiales, et permette d'adresser des sujets majeurs tels que la sécurisation des accès distants et la généralisation de l'authentification multi-facteurs.

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.

Maitriser les systèmes exposés

- ▶ Réduire la surface d'attaque en désactivant les comptes, protocoles et services qui ne sont pas indispensables : certaines structures de santé auditées exposent un grand nombre de services numériques sur Internet y compris des services de téléadministration 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 OWASP⁷) : 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 (boîtiers VPN, fermes RDS ou de virtualisation, routeurs d'interconnexion, etc.). Ils doivent faire l'objet d'une attention particulière

⁷ 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.

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.
- ▶ 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.

Il est indispensable de poursuivre la réalisation de scans à fréquence régulière, comme cela avait été introduit par le Domaine 1 du programme CaRE, pour maintenir une surveillance continue et s'assurer de l'absence de vulnérabilité critique.

Mettre en place une authentification double facteur

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 multi-facteur 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 multi-facteur 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 d'Identification Electronique version 2 définit des exigences sur les connexions à des services numériques traitant des données de santé et les schémas d'identification électronique associés. Il sera rendu opposable courant 2026 et le

respect des exigences correspondantes sera donc obligatoire pour les acteurs concernés. L'objectif du projet HospiConnect est d'accélérer le déploiement des exigences de ce référentiel et ainsi de réduire les risques d'usurpation de l'identité numérique des professionnels pour l'accès aux services numériques en santé. Il est intégré au Programme CaRE dans le cadre de son 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 patches de sécurité.
- ▶ Pour la réplication, appliquer la règle de sauvegarde en système 3-2-1⁸.

Le Domaine 2 du programme CaRE vise le renforcement de la stratégie de continuité et de reprise d'activité. Il intègre des exigences liées à la gestion des sauvegardes (architecture, supervision, immuabilité, authentification, etc.) et à leur restauration en cas de crise.

⁸ <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 cybersécurité⁹ 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 avec un renouvellement obligatoire tous les 1 à 3 ans (sauf connaissance de fuite).

⁹ <https://esante.gouv.fr/strategie-nationale/cybersecurite/axe-1>

- ▶ 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 multi-facteur et aux mots de passe¹⁰ [.](#)

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. Si le domaine 1 du programme CaRE visait à atteindre un premier niveau de remédiation suite à la mise en œuvre bimestrielle d'un audit ADS de l'ANSSI¹¹, il convient de poursuivre le durcissement des AD.

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 maîtrisant 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 boîte déclarée (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

¹⁰ <https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe>

¹¹ <https://esante.gouv.fr/strategie-nationale/cybersecurite#content-38127>

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.¹²

¹² <https://cyber.gouv.fr/publications/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation>

8 GLOSSAIRE

AD	Active Directory
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
CH	Centre Hospitalier
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.
CORUSS	Centre opérationnel de réception et de régulation des urgences sanitaires et sociales
CVSS	Common Vulnerability Scoring System
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 cyberspace 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.
DDoS	Deni de service distribué (Distributed Denial of Service)
DGS	Direction Générale de la Santé
DNS	Délégation ministérielle au numérique en santé
DPI	Dossier Patient Informatisé
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.
FOVI	Faux Ordres de Virement
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	<p>Forme d'extorsion imposée par un code malveillant sur un utilisateur du système.</p> <p>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.</p>
RSSI	Responsable de la Sécurité des Systèmes d'information
SI	Système d'Information
SOC	Centre des Opérations de Sécurité (Security Operations Systems)
VPN	Réseau privé virtuel (Virtual Private Network)

NOTES PERSONNELLES

Pour aller plus loin, rendez-vous sur :



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

Pour prendre contact :



- ➔ au sein du Ministère de la Santé, des Familles, de l'Autonomie et des Personnes handicapées :
ssi@sg.social.gouv.fr
- ➔ au sein de l'Agence du Numérique en Santé :
cyberveille@esante.gouv.fr