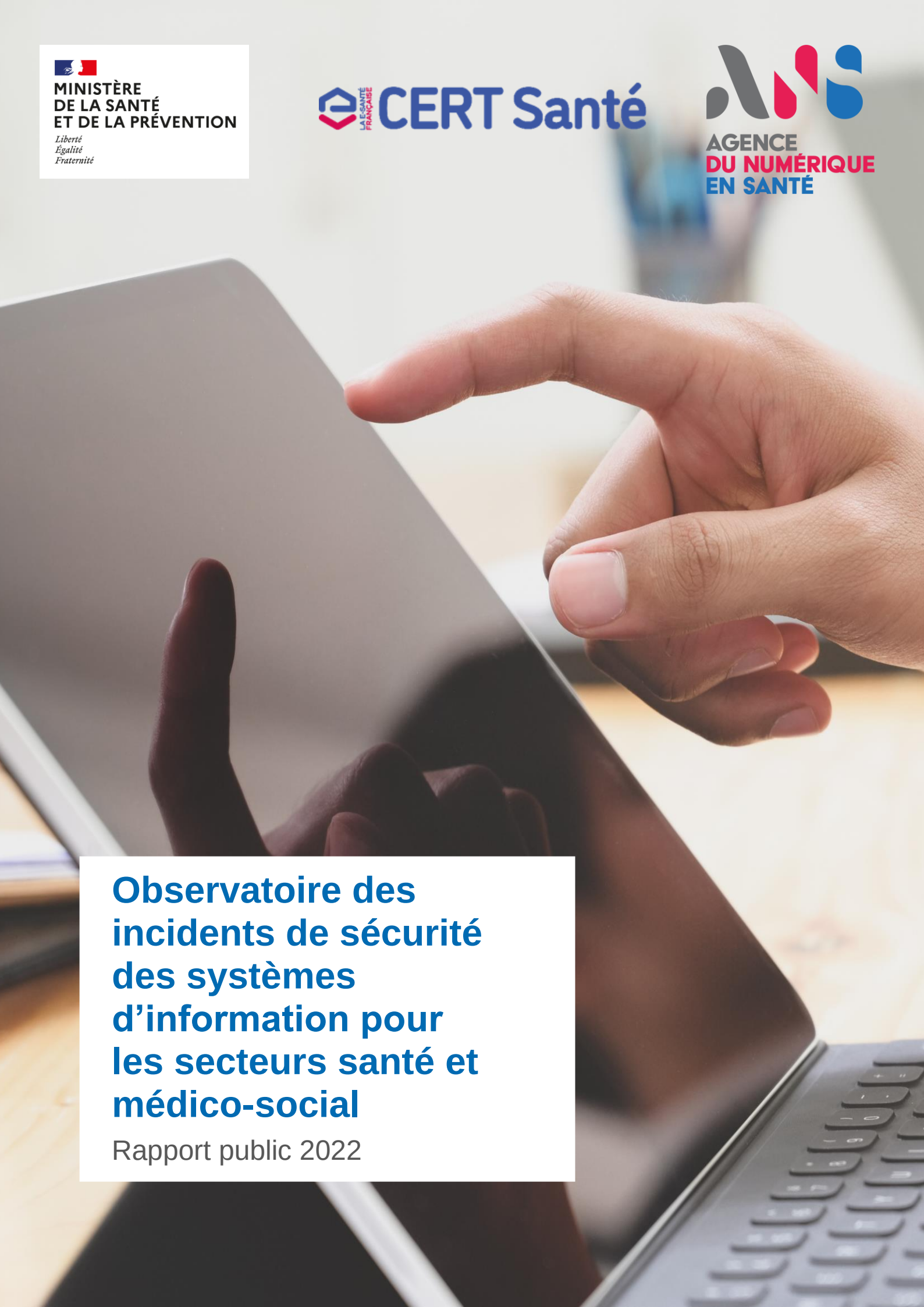
MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

CERT Santé

AGENCE
DU NUMÉRIQUE
EN SANTÉ



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

Rapport public 2022

SOMMAIRE

TABLE DES FIGURES

1 INTRODUCTION

L'année 2022 a encore été marquée par des attaques d'ampleur visant les établissements de santé (ES). Le ministère de la santé et de la prévention a proposé une action massive, collective et rapide pour contrer la menace cyber et s'est engagé dès décembre 2022 à élaborer et à mettre en œuvre rapidement un plan ambitieux de renforcement de la cybersécurité des ES, associé à un plan d'investissement pluriannuel : le programme CaRE (Cyber Accélération et Résilience des Etablissements). En appui à la DNS, l'ANS est fortement impliquée dans la conception et dans le déploiement à venir de ce programme qui rassemble et implique toutes les parties prenantes : au niveau national (ANSSI, ANS, DGOS, DNS et HFDS/FSSI), régional (ARS et GRADeS) et local (professionnels, établissements, industriels).

Malgré la baisse du nombre d'attaques par rançongiciel en 2022 (27 portées à la connaissance du CERT Santé), beaucoup d'entre elles ont encore eu un impact majeur sur les établissements. Ainsi 17 établissements ont été contraints de mettre en place un mode dégradé de fonctionnement qui a perduré plusieurs semaines voire plusieurs mois pour 4 d'entre eux.

Le CERT Santé est intervenu auprès de 97 établissements en 2022 concernant 103 incidents (en hausse de 26% par rapport à 2021). Son intervention a permis de stopper la progression d'une attaque et de renforcer les mesures de protection de l'établissement. Le CERT Santé obtient un excellent taux de satisfaction de 93%, recueilli auprès de ses bénéficiaires après la mise en œuvre des actions d'accompagnement.

En étendant son service de réponse à incident en heures non ouvrées dès octobre 2022, le CERT Santé s'est doté d'une capacité supplémentaire pour aider les établissements à neutraliser rapidement une cyber-attaque. L'astreinte du CERT Santé a déjà été sollicitée à huit reprises. Ce service sera étendu aux acteurs du médico-social en 2023.

Le portail du CERT Santé a fait peau neuve en 2022 (https://cyberveille-sante.gouv.fr/). Des améliorations significatives ont été apportées dans la présentation des contenus (vulnérabilités critiques, actualités et dossiers thématiques) et l'offre de service du CERT Santé y est présentée de façon détaillée. L'espace abonné du portail propose une nouvelle fonctionnalité de notification à fréquence régulière (défini par l'utilisateur) concernant les alertes et les bulletins d'actualités publiés sur une période donnée. Les abonnés peuvent ainsi être informés des nouvelles publications spécifiquement en lien avec leurs sujets d'intérêt.

Conscient de l'importance de sensibiliser et de préparer les directions à la gestion de crise liée à une attaque de cybersécurité, l'ANS et ses administrateurs ARS-GRADeS ont élaboré et mis à disposition des kits d'exercice de crise cybersécurité prêts à l'emploi et autoporteurs pour faciliter leur organisation. Ces kits sont adaptés à différents niveaux de maturité (débutant, intermédiaire et confirmé) mesurés grâce à une grille d'autoévaluation qui permet à tout établissement de sélectionner le niveau de kit approprié à son contexte.

En 2022, l'ANS a également enrichi le corpus de référentiels et de guides de la PGSSI-S et intégré les exigences de sécurité essentielles dans le programme SEGUR du numérique en Santé. Les éditeurs/hébergeurs doivent contribuer via leurs solutions au renforcement de la résilience des SI de santé vis-à-vis des menaces de cybersécurité.

L'ANS, partie prenante du programme CaRE, poursuit et fait évoluer ses activités de prévention en restant agile et à l'écoute des besoins de l'écosystème mais également au travers de la vague 2 du SEGUR du numérique en santé.

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

2.1 Contexte réglementaire et organisationnelle

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 depuis le 1er octobre 2017. 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 contexte réglementaire a évolué en 2022 avec la publication du décret n° 2022-715 du 27 avril 2022 (JORF n°0214 du 28 avril 2022) relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information. L'Agence du Numérique en Santé (ANS) désignée comme le groupement d'intérêt public (GIP) est renforcée dans son rôle d'acteur central dans la gestion des incidents. Elle est en charge de les qualifier, d'alerter les autorités compétentes et d'apporter un appui aux déclarants dans la réponse apportée aux incidents.

La nature des incidents à déclarer s'étend désormais aux incidents ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé et ceux qui sont susceptibles de toucher d'autres établissements et organismes ou services.

Le CERT Santé, porté par l'ANS, est le premier CERT sectoriel en France. Il a intégré en janvier 2021 l'Intercert FRANCE (anciennement InterCERT-FR), association loi 1901 qui constitue la première communauté de CSIRT[1] en France. En tant que membre de cette association, le CERT Santé bénéficie des retours d'expérience et de la coopération avec les autres CSIRT/CERT dans sa lutte contre les menaces de cybersécurité.

2.2 Présentation des activités

Le dispositif de traitement des signalements des incidents de sécurité des systèmes d'information constitue un élément clé 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 cyber sécurité.

Sa mise en œuvre opérationnelle s'appuie sur le CERT Santé de l'ANS qui a intégré l'InterCERT-FR en janvier 2021.

[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 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 des solidarités et 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), qui assure le pilotage du traitement en cas d'incident de sécurité majeur ;
    - 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 ;
    - aux agences sanitaires dans le cas d'un incident majeur impactant la prise en charge des patients ;
    - à l'ANSSI, en cas d'incident concernant une structure relevant de dispositifs spécifiques (OIV ou OSE), ou en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
    - à terme, à la CNIL en cas d'impact sur les données à caractère personnel.

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

- Mise à disposition de fiches réflexes (ex : maliciel, hameçonnage ou défiguration de site Web) ou de recommandations de mesures de remédiation correspondant à la nature de l'incident (ex : changement de mots de passe, mise en liste noire d'adresses de messagerie, blocage de protocoles) ;
- Proposition des mesures de confinement complémentaires au cours d'un premier entretien (fermeture des services permettant les communications depuis Internet (RDP, Webmail, VPN, ...), désactivation massive de comptes, etc…) ;
- Assistance à l'identification de la menace et le scénario complet de la compromission (acquisition 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…) ;
- Orientation vers un prestataire cyber dans le cas d'une demande d'intervention sur site.

Le CERT Santé propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité :

- Proposer et émettre 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) ;

- Proposer des solutions pour renforcer la sécurité (configuration des systèmes, solutions concrètes de sécurisation des sauvegardes, 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.

Mise en place d'une permanence 24/7

Depuis le 17 octobre, le CERT Santé étend son service de réponse à incident aux heures non ouvrées, soit 24h/24 et 7j/7. Une astreinte est mise en place pour accompagner les bénéficiaires du CERT Santé confrontés à un incident majeur ayant déjà affecté un ou plusieurs services numériques et contraignant l'établissement à mettre en place un mode dégradé de fonctionnement.

La personne d'astreinte au sein du service informatique ou de la DSI de l'établissement pourra contacter l'astreinte du CERT Santé en appelant le 09 72 43 91 25, accueil téléphonique du CERT Santé. Elle bénéficiera d'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 de son système d'information.

Animation de la communauté « cyberveille-santé »

Le portail cyberveille-santé dispose d'un salon Tchap au sein duquel les correspondants du CERT 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.

Alerte des structures sur la menace cyber

Au travers du portail cyberveille-santé dédié à la sécurité du numérique en santé, le CERT Santé, en coordination étroite avec le centre gouvernemental CERT-FR de l'ANSSI :

- Informe et alerte 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 (messages électroniques malveillants, rançongiciels, vols de données, etc…) ;
- Apporte un appui aux structures dans la gestion de la sécurité et des incidents (fiches réflexes, fiches pratiques, guides de bonnes pratiques).

Améliorer la sécurité de la messagerie

L'utilisation de courriels malveillants (technique de l'hameçonnage) est très développée par les attaquants pour chercher à compromettre un SI. Le CERT Santé propose aux structures de tester les règles de sécurité de leur serveur de messagerie avec un service en ligne. Ce service a pour but d'identifier les améliorations à apporter dans la configuration des règles de sécurité de la messagerie pour réduire le risque de manipulation de contenus malveillants par les utilisateurs. Il permet de vérifier que la politique de contrôle des messages et de leur contenu a pris en compte les principales menaces issues de l'émetteur, de métadonnées du message (en-tête, encodage, découpage en plusieurs parties, etc…), d'une pièce jointe (spam, virus, etc…), d'une URL (hameçonnage), etc. … Le service contient plus de 170 points de contrôle.

Les activités de prévention menées dans le cadre du service national de cyber-surveillance et de la veille proactive sont présentées en 5.1.

Intervention de l'ANS en cybersécurité au-delà du champ opérationnel

Depuis 2021, avec l'intégration des ARS et les GRADeS dans sa gouvernance, l'ANS propose des espaces d'échange, de partage et de travail collaboratif sur le volet de la cybersécurité entre l'échelon national et l'échelon régional.

En lien avec les nouvelles mesures de renforcement de la stratégie ministérielle de la cyber en santé, l'ANS a lancé un Groupe de Travail Territorial visant à rassembler FSSI, ARS/GRADeS, et experts cyber de l'ANS autour de la production d'un guide dédié de sensibilisation pour le secteur social et médico-social et la production de kits d'exercices de crise.

1. Kit d'exercice de crise

La réalisation d'exercices de crise cybersécurité au sein des établissements de santé et des structures médico-sociale est l'une des actions prioritaires du Plan de renforcement cybersécurité du ministère de la santé et de la prévention. Il y a donc une réelle nécessité de sensibilisation et de préparation de tous les acteurs du secteur (directions, métiers, DSI, etc.) aux risques cybersécurité dans leurs contextes particuliers à la gestion de crise. La direction générale de l'établissement doit être impliquée fortement dans ce type d'exercice au même titre que la DSI. Par ailleurs, les directeurs d'établissement classés OIV[2] ou OSE[3], tels que définis dans la déclinaison nationale de la directive NIS[4], sont pénalement responsables de la sécurité des SI. Il est donc primordial qu'ils soient préparés à ce type de crise.

Pour s'adapter au plus grand nombre de contextes, ces kits ont été éprouvés in situ dans des établissements de santé et structures médico-sociales informatisées de tailles et

[2] Opérateur d'Importance Vitale

[3] Opérateur de Services Essentiels

[4] NIS : Network and Information Security
Adoption de la directive Network and Information Security (NIS) : l'ANSSI, pilote de la transposition en France | Agence nationale de la sécurité des systèmes d'information

d'organisations différentes. Ainsi, les structures peuvent envisager une réalisation autonome des exercices ou opter pour une réalisation assistée par un prestataire externe.

Ces kits sont adaptés à différents niveaux de maturité (débutant, intermédiaire et confirmé) mesurés grâce à une grille d'autoévaluation qui permet à tout établissement de sélectionner le niveau de kit approprié à son contexte.

Chaque kit est prêt à l'emploi. Il a pour objectif de permettre à une structure de santé de découvrir la gestion de crise cybersécurité en condition réelle et de s'approprier des automatismes de gestion de crise cybersécurité afin de renforcer la résilience de leur structure et d'assurer au mieux la continuité des soins.

Il est divisé en trois parties :

1. Un kit participant – Ce kit comporte les règles du jeu, les fiches de bonnes pratiques, ainsi qu'un glossaire pour permettre aux participants de se familiariser avec les concepts de la cybersécurité. Il doit être partagé avec eux en amont de l'exercice ;

2. Un kit de communication – Ce kit permet de communiquer au mieux auprès des participants à l'exercice pour en expliquer la démarche et mobiliser les acteurs ;

3. Un kit animateur – Ce kit permet à tout animateur (interne ou externe) de pouvoir animer en autonomie l'exercice au sein de la structure. Découvrez-le en images à travers la vidéo de présentation présente dans le kit.

Attention : Il est conseillé que seule l'équipe animation puisse consulter ce kit animateur pour assurer la bonne tenue du test et ne pas biaiser la réussite de l'exercice.

L'ensemble de ces kits est disponible sur le portail cyberveille-santé au lien suivant : https://www.cyberveille-sante.gouv.fr/dossier-thematique/exercice-de-crise-cyber

Les exercices de crise sont aujourd'hui en cours de généralisation dans tous les établissements sanitaires, grâce à la mise à disposition des kits ANS et d'un financement dédié FIR de 10M€ fléché vers les ARS qui sont en charge du déploiement, avec le suivi et l'accompagnement de l'ANS.

2. Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) et gestion d'une identité numérique

L'article L. 1470-5 du code de la santé publique prévoit que l'ANS élabore, en concertation avec l'écosystème, des référentiels visant à garantir l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel par les services numériques en santé. Ces référentiels sont rendus opposables par arrêté du ministre en charge de la santé. Ils sont complétés par des guides de bonnes pratiques qui visent à accompagner l'ensemble des acteurs dans le renforcement de la sécurité de leurs systèmes d'information. L'ensemble de ces référentiels et guides constituent le corpus documentaire de la PGSSI-S.

Le référentiel d'identification électronique de la PGSSI-S est notamment devenu opposable le 28 mars 2022. Il introduit des exigences de sécurité pour garantir la sécurité des services numériques en santé décrits comme sensibles et notamment :

- Dès le 1er janvier 2023

- L'obligation de mise en œuvre de ProSanté Connect pour l'authentification des professionnels de santé ;
- La mise en œuvre, sauf exceptions décrites dans le document, d'un second facteur d'authentification pour la plupart des cas d'usages Que les ES devront mettre en œuvre un second facteur d'authentification ;

- A partir du 1er janvier 2026, les professionnels de santé devront posséder une identité numérique de niveau de garantie équivalent au niveau substantiel eIDAS (règlement d'exécution européen n°2015/1502).

3. Doctrine, maturité, référencement

Responsable de l'élaboration et de la promotion de la PGSSI-S, l'ANS se mobilise pour accompagner les acteurs dans leurs démarches de mise en conformité.
Ainsi dans le cadre du Ségur du numérique en santé, les exigences relatives aux dispositifs s'interfaçant avec Pro Santé Connect ou l'INS, sont vérifiées préalablement à leur référencement. Des exigences plus précises portant sur la sécurité des solutions utilisées sont également en train d'être finalisées pour une intégration dans la vague 2 du Ségur numérique.
Plus d'une cinquantaine d'exigences réparties en trois catégories sont ainsi prévues :

- Des exigences portant sur des thématiques de base de la sécurité des systèmes d'information telles que la gouvernance, les antivirus, la veille et les mises à jour de composants, la gestion des incidents, le contrôle des flux réseaux et applicatifs, la cryptographie et la gestion des secrets, les sauvegardes, etc. ;
- Des exigences portent sur la conformité au référentiel d'identification électronique de la PGSSI-S ;
- Enfin des exigences portent sur la gestion des identités et des accès et visent notamment à améliorer la gestion des comptes utilisateurs et des permissions ainsi que la compatibilité des solutions avec des annuaires et des solutions de type webSSO.

Des preuves seront demandées afin de valider la conformité des solutions candidates au référencement et un test d'intrusion devra être réalisé afin de valider un certain nombre de points de contrôles spécifiques.
Des travaux équivalents sont en cours pour les applications qui visent à intégrer le store Mon Espace Santé.

4. Positionnement de l'ANS dans le pilotage de la TF

L'ANS se positionne en appui de la DNS pour coordonner l'ensemble des parties prenantes (FSSI, DGOS, ANSSI, ANS, ARS/GRADeS, Fédérations hospitalières et médico-sociales) dans les travaux de la TF cyber lancée en décembre 2021, qui a pour objectif de concevoir et de mettre en œuvre le programme CaRE et un plan pluriannel massif.

Les productions et livrables seront présentés dans le rapport 2023.

.

3 Synthèse de l'activité en 2022

En 2022, le nombre total d'établissements ayant déclaré au moins un incident a augmenté de façon significative (+33%) malgré une baisse du nombre de signalements par rapport à 2021 (-19%). Cette baisse est principalement liée à l'absence d'incident ayant impacté la disponibilité des solutions métiers hébergées par des prestataires.

Le nombre d'interventions en appui technique a augmenté de 26% par rapport à 2021. Le CERT Santé a été sollicité à de nombreuses reprises pour aider à confiner les systèmes potentiellement compromis et récupérer l'ensemble des informations permettant une analyse des traces numériques laissées par les cyberattaquants et alimenter le dépôt de plainte. Il a fait le lien avec les autorités chargées de la lutte contre la cybercriminalité et a également accompagné des établissements à produire un plan de remédiation suite à une compromission importante du SI nécessitant la mise en œuvre de mesures de durcissement.

Grâce à la communauté des CSIRT de l'InterCERT France, et en particulier à sa coopération avec le CERT-FR dans la veille sur les menaces de cybersécurité impactant le secteur de la santé, le CERT Santé a pu être informé de plusieurs fuites d'identifiants et de compromissions de comptes (e-mail, VPN), ainsi que des campagnes de phishing concernant certains de ses bénéficiaires. Son intervention a permis aux établissements concernés d'identifier les activités malveillantes, de les neutraliser puis de renforcer ses moyens de protection.

Dans le cadre de compromissions majeures de SI, le CERT Santé a été amené à coordonner ses actions avec des prestataires cyber (PRIS[5] en particulier) mais également à conseiller ses bénéficiaires dans les choix/options techniques retenues par ces derniers. Ce service est particulièrement apprécié par les bénéficiaires qui sont souvent démunis dans le pilotage de prestataires spécialisés.

Le CERT Santé est intervenu auprès de 9 prestataires de solutions métier suite à l'identification de failles de sécurité 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 accompagné ces acteurs dans la correction des vulnérabilités ainsi que dans le renforcement de la sécurité de leur application et de leur infrastructure.

Le nombre d'incidents liés à une attaque par rançongiciel est en baisse de 49% par rapport à 2021 (dans son rapport annuel, le CERT-FR rapporte que le nombre d'incidents liés aux rançongiciels a diminué de 46% par rapport à 2021). Ces attaques ont cependant fortement impacté certains établissements les contraignant à mettre en place un mode dégradé de fonctionnement pendant plusieurs semaines voire plusieurs mois. Les établissements tels que les OSE ont bénéficié de l'appui de l'ANSSI, en particulier dans la phase de reconstruction de leur SI.

De nombreuses alertes sur des failles critiques concernant des services exposés sur Internet ont été publiées en 2022 (messagerie, accès VPN, serveurs web métier). Par ailleurs, le CERT Santé a alerté ses bénéficiaires concernant des compromissions de comptes d'accès (Messagerie, VPN, etc..). **Le nombre d'alertes transmises est de plus de 2100 soit une augmentation de 10% par rapport à 2021. 76 cas de compromission ont pu être**

[5] Prestataires de réponse aux incidents de sécurité

identifiées et le CERT Santé est intervenu à 20 reprises pour assister le bénéficiaire dans sa recherche de compromission et la mise en œuvre des mesures correctives.

4 OBSERVATOIRE DES SIGNALEMENTS

4.1 Chiffres clés pour la période 2021-2022

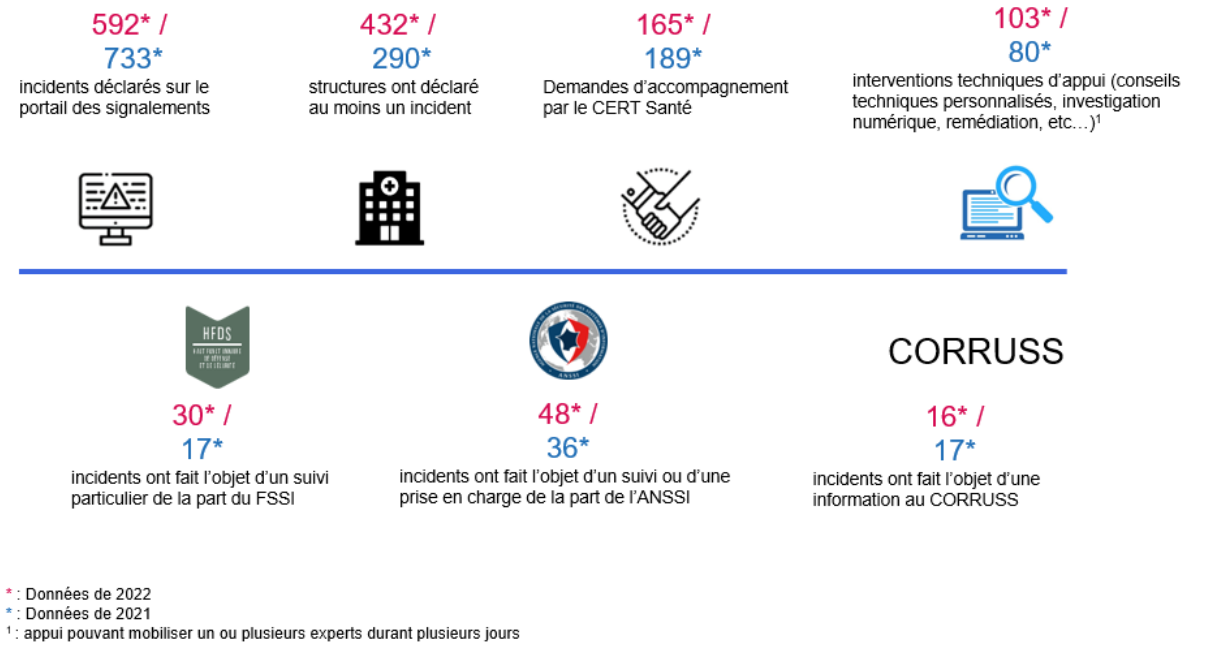


Figure 1 – Chiffres clés des signalements déclarés en 2021 et 2022

En coordination avec le CERT Santé, l'ANSSI et le FSSI sont intervenus directement au profit de 48 structures de santé, 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 à de nombreuses reprises auprès de prestataires sectoriels.

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

- Quarante établissements de santé publics, dont 29 opérateurs de services essentiels (OSE). Ces incidents étaient liés à des attaques par rançongiciel, des compromissions par des chevaux de Troie, des compromissions de comptes (AD, VPN ou messagerie), l'exploitation de vulnérabilités sur des équipements de sécurité ou des dysfonctionnements graves de systèmes critiques ;
- Cinq établissements de santé privés et un établissement et service médico-sociaux victimes de rançongiciels, de compromission de comptes (AD, VPN ou messagerie) et d'exploitation de vulnérabilités ;
- Un centre de radiothérapie et un centre le lutte contre le cancer victimes de rançongiciels.

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

- Trente établissements dont 11 OSE. Ces incidents étaient liés à des attaques par rançongiciels, à la compromission de SI et aux dysfonctionnements graves de systèmes critiques, et pertes du lien télécom.

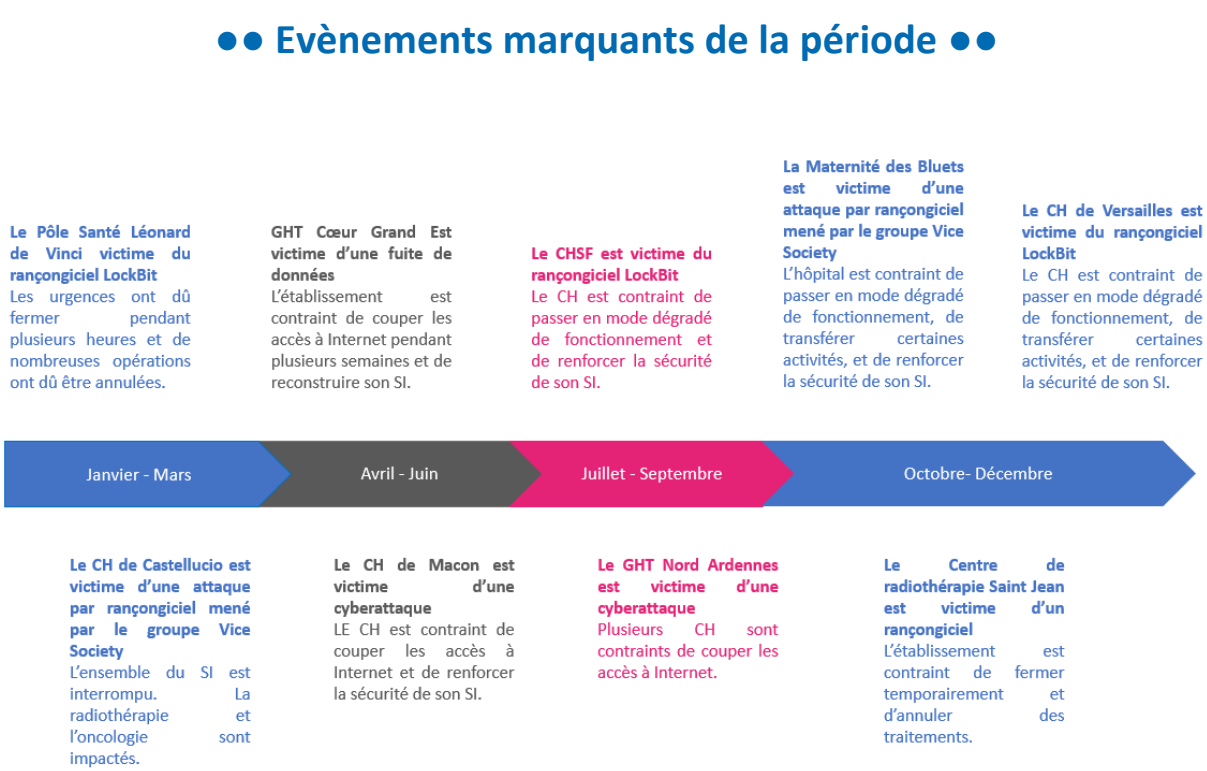


Figure 2 – Evènements marquants de l'année 2022

4.2 Informations générales sur les signalements

592 incidents ont été déclarés en 2022. Ce nombre est en baisse par rapport à 2021 (733). Pour mémoire, 396 incidents avaient été déclarés en 2020. Cette baisse est principalement liée à l'absence d'incidents ayant impacté les hébergeurs de solutions métiers. Elle peut également s'expliquer par le renforcement progressif des mesures de protection des accès qui avaient été ouverts massivement pendant la pandémie.

Toutefois, les incidents les plus importants sont beaucoup plus visibles et médiatisés. Nous constatons cependant 50% de déclarations d'incidents supplémentaires par rapport à 2020, la cybermenace est donc encore à un niveau élevé.

Parmi ces incidents, on compte des incidents « hors périmètre » (28). 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 (4).

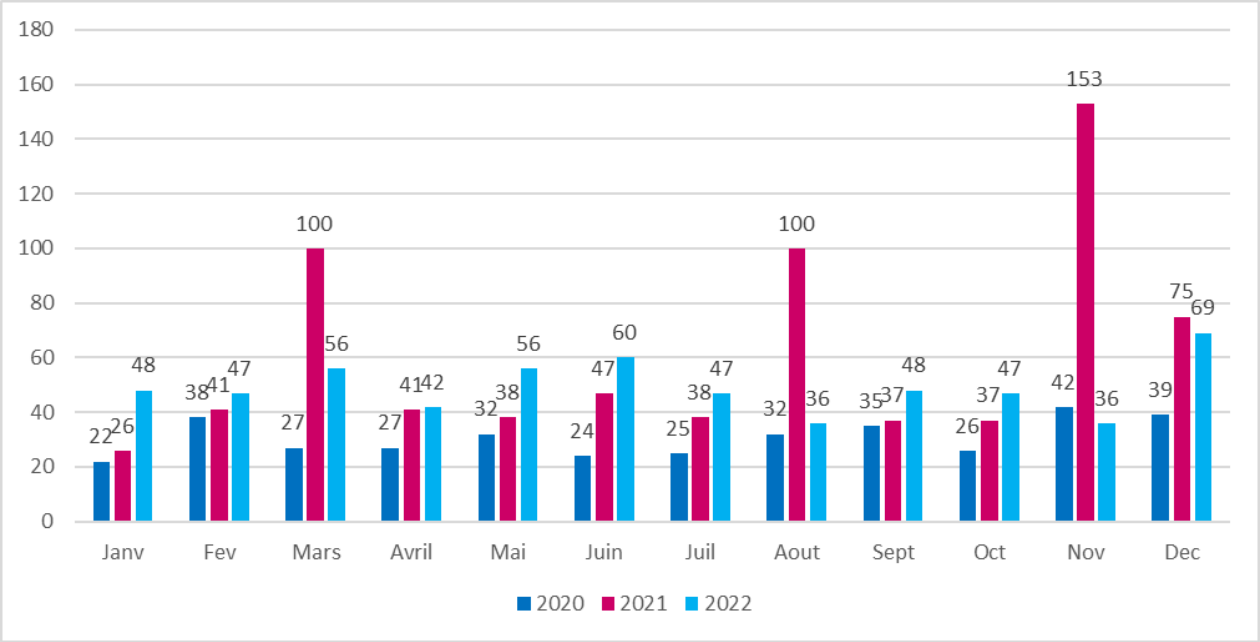


Figure 3 - Nombre de signalements par mois

La baisse relative des déclarations s'explique par l'absence d'incident ayant impacté les hébergeurs d'applications métier des bénéficiaires du CERT Santé. On compte en 2022 une moyenne de 49 déclarations par mois. Cela constitue une augmentation de 22% par rapport à 2021 si l'on ne tient pas des pics de déclaration des mois de mars, août et novembre 2021 qui correspondaient à l'incendie du data center d'OVH à Strasbourg, à un incident d'origine malveillante concernant un fournisseur de solutions métier pour ESMS et à une panne de l'hébergeur Mipih.

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

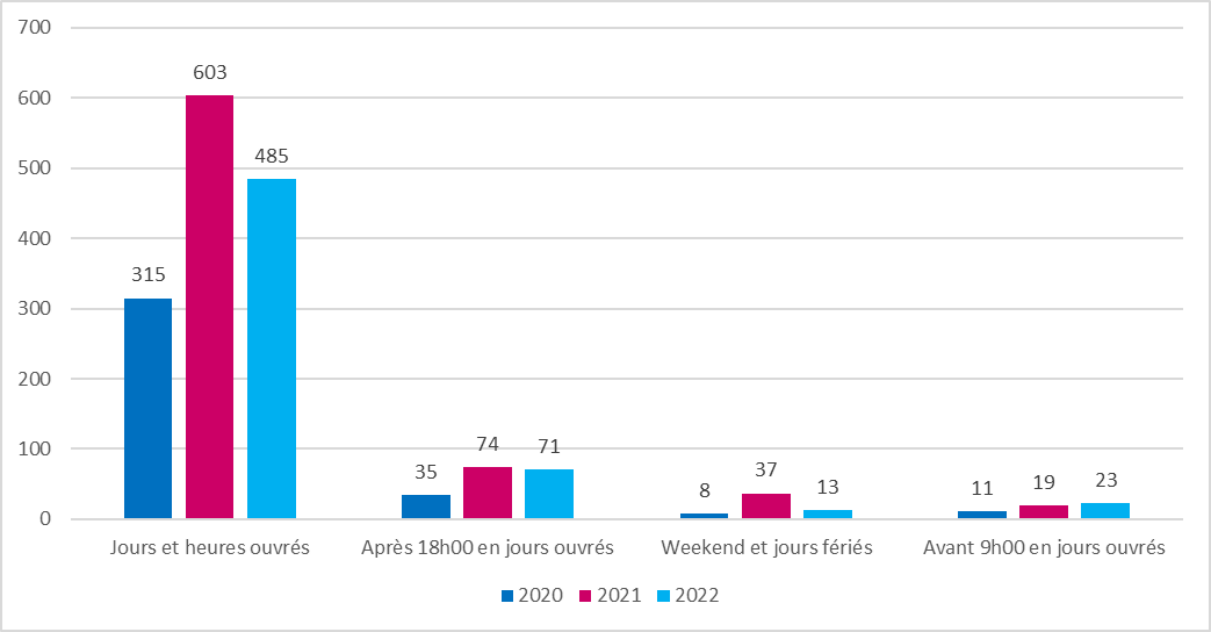


Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt

74% des signalements ont été effectués en heures et jours ouvrés (HO/JO) en 2022, entre 9h et 18h.

Ce sont principalement des structures publiques qui sont à l'origine des déclarations en HNO/JNO. Quarante-quatre demandes d'accompagnement ont été formulées durant ces périodes. Parmi celles-ci, vingt-trois structures (onze CH, neuf hôpitaux privés à but non lucratif, un hôpital privé, une association et un éditeur de logiciel) nécessitaient un appui suite à des attaques par rançongiciels entrainant une interruption du SI support de nombreux services de prise en charge des patients, à des compromissions de comptes AD ou de messagerie, ou à des exploitations de vulnérabilités. Onze demandes d'accompagnement en HNO/JNO ayant fait l'objet d'un appui technique se sont avérées être des faux-positifs. Elles ont été prises en charge rapidement par le CERT Santé à l'ouverture du service et quatre structures nécessitaient un accompagnement sur site au regard de l'ampleur du sinistre. Elles ont également bénéficié d'un appui de l'ANSSI et ont fait appel à un prestataire spécialisé dans la réponse à incidents et la reconstruction d'un SI post-incident pour les appuyer sur place.

Etat des incidents lors de leur signalement

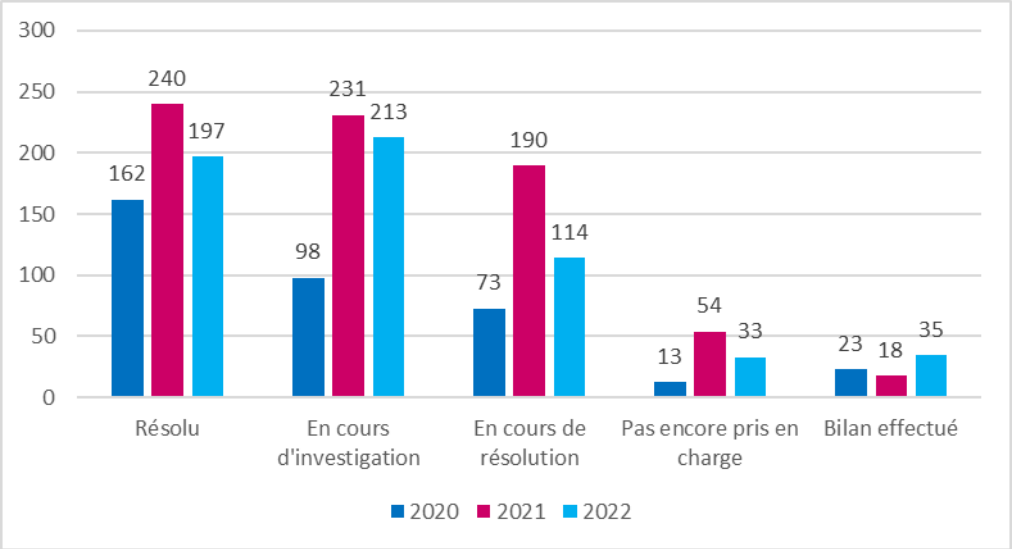


Figure 5 - Etat des incidents lors de leur signalement

En 2022, comme en 2021 et 2020, plus de la moitié des incidents sont résolus ou en cours de résolution par la structure avant leur déclaration.

Depuis 2019, le CERT Santé est davantage sollicité par les structures pour des actions d'investigation et la mise en place de mesures de remédiation. **Sur trois ans, cette part augmente chaque année, pour atteindre 36% en 2022**.

11 structures n'ont pas transmis d'informations complémentaires à la suite de leur déclaration malgré une demande de compléments d'information et/ou une proposition d'appui**. Ce chiffre est en baisse significative par rapport à 2021** (33).

29%

C'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2022**. Il est **en légère augmentation par rapport à 2021 (26%)**.

Les accompagnements sont en général demandés lors d'incidents ayant un impact important sur la structure ou bien lorsque la structure veut s'assurer qu'elle a bien entrepris l'ensemble des actions recommandées tant en matière d'investigation que de remédiation, voire d'amélioration de leur résilience face aux cyberattaques. **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●●

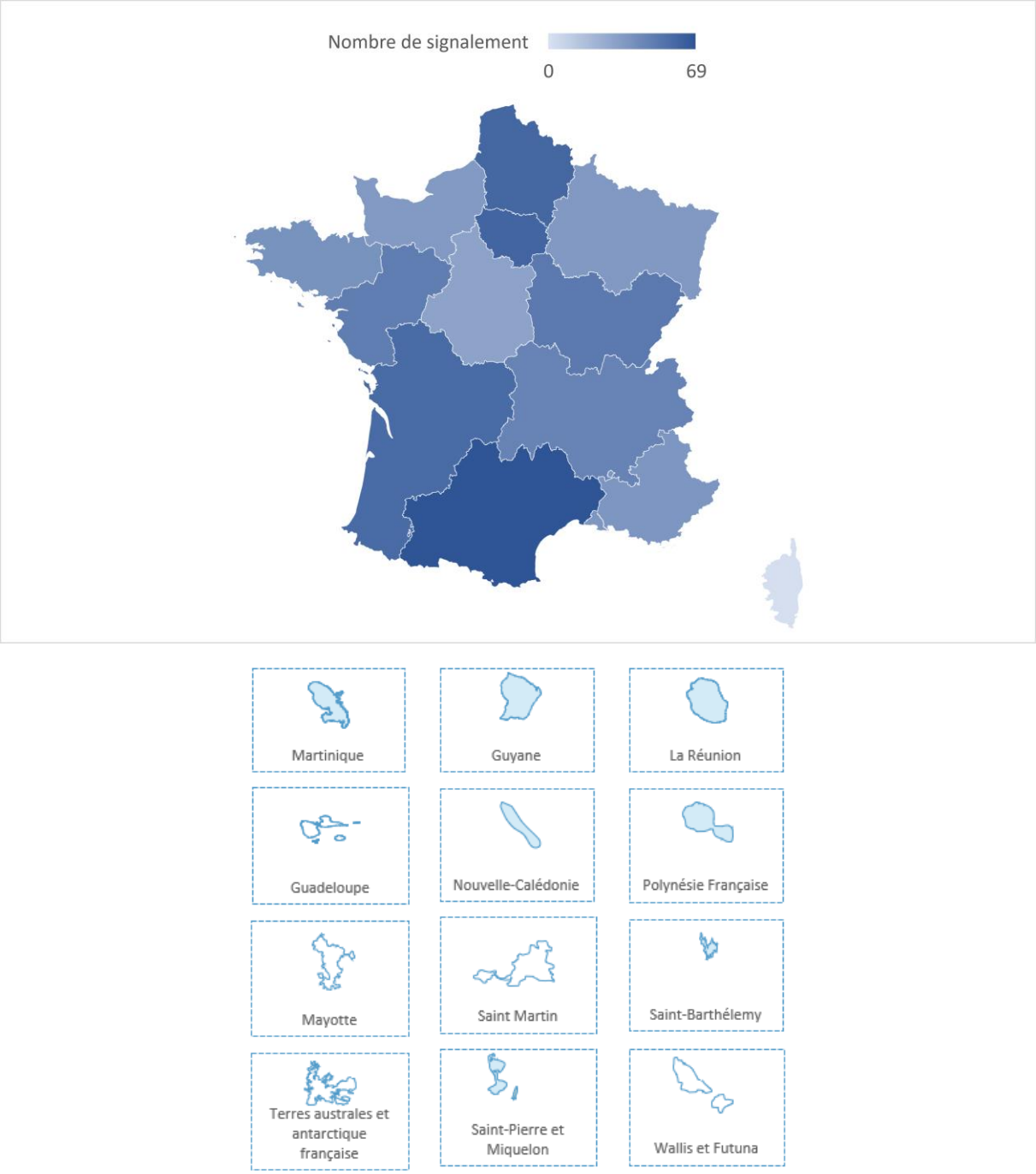


Figure 6 - Répartition des signalements par région

Les régions pour lesquelles le nombre de signalements est le plus important sont l'Occitanie, les Hauts-de-France et l'Ile-de-France avec 69 pour l'Occitanie, 61 pour l'Ile-de-France et 60 signalements pour les Hauts de France. Ces trois régions représentent à elles seules plus de 32% du total des signalements.

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

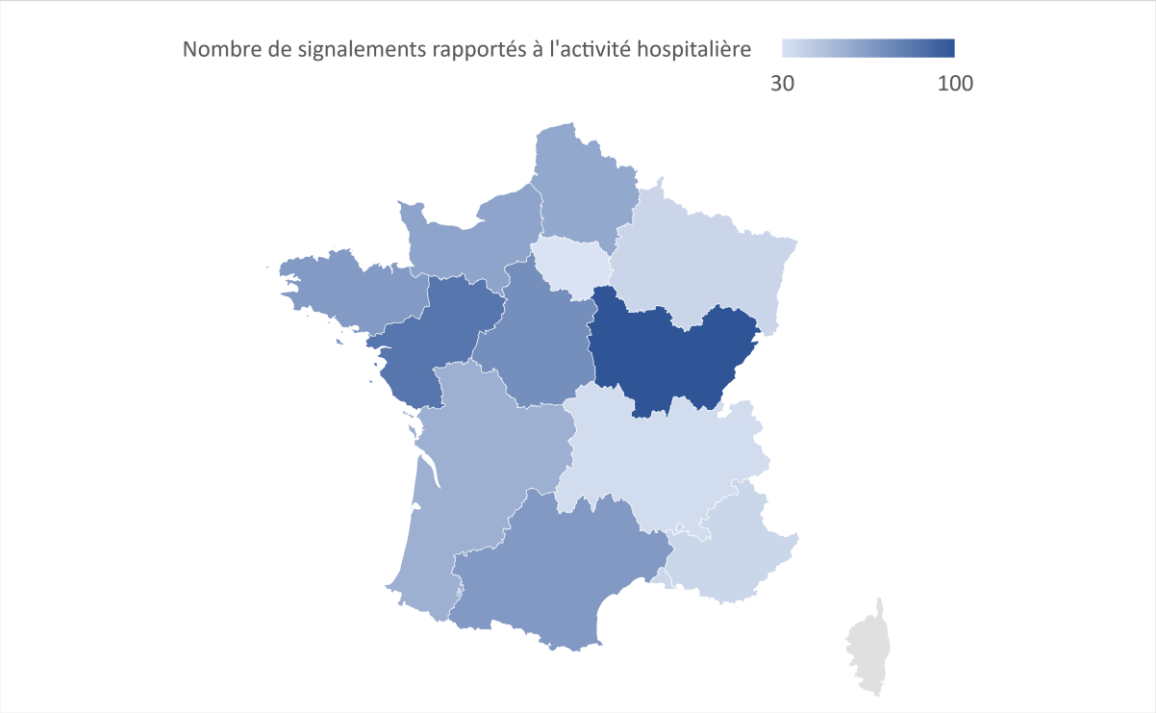


Figure 7 - Nombre de signalements rapporté à l'activité hospitalière des régions

Cette carte présente le ratio entre le nombre de signalements et l'activité hospitalière rapportée au niveau national : plus une région a un nombre de signalements élevé par rapport à son activité, 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 rapport à la métropole. La région avec le ratio le plus élevé (Bourgogne-Franche-Comté) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (4.5% de l'activité nationale), la région Bourgogne-Franche-Comté est en tête en matière de remontée des incidents. Les régions Pays de la Loire et Centre-Val de Loire arrivent en deuxième et troisième position. Les régions au sein desquelles les établissements déclarent le plus sont très actives dans la sensibilisation aux enjeux de cybersécurité et la promotion des services du CERT Santé.

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 continuer à faire de la pédagogie sur l'importance de déclarer ses incidents cyber, de faire la promotion des services du CERT Santé, 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

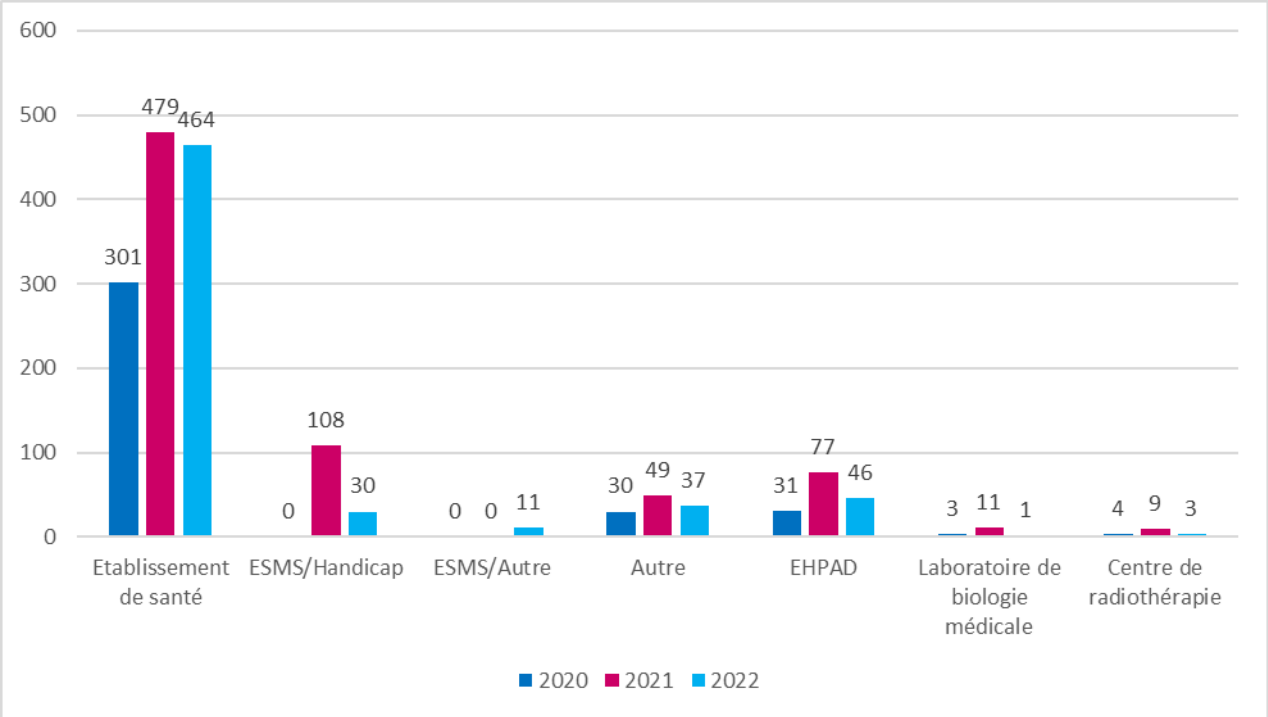


Figure 8- Répartition des signalements selon le type de structure

La grande majorité (78%) des incidents de sécurité est déclarée par les **établissements de santé** (voir détail figure 7).

●● Part des signalements comparée à la part des établissements de santé selon leur type ●●

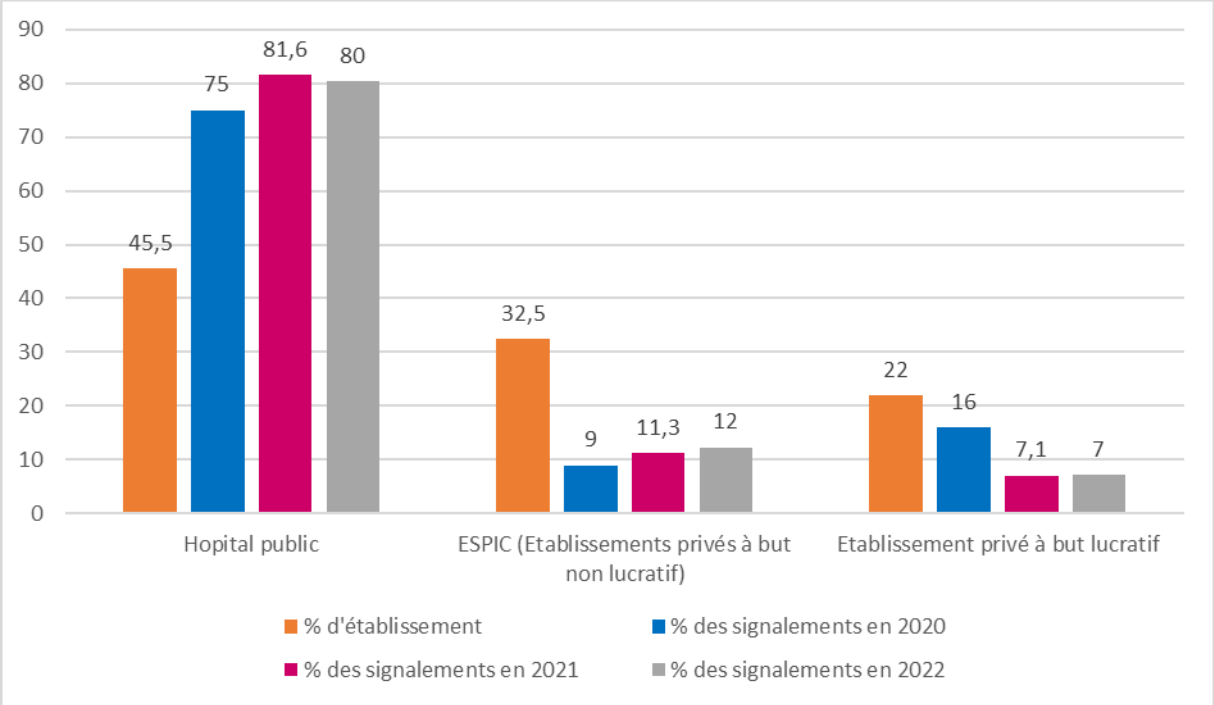


Figure 9 - Part des signalements comparée à la part des établissements selon leur raison sociale

La part des établissements dans la déclaration des incidents en 2022 est stable par rapport à 2021. **100 établissements référencés OSE** ont déclaré au moins un incident en 2022.

69 C'est le nombre de structures ayant déclaré plus de 2 incidents durant l'année 2022 sur 432 structures au total. 15 d'entre elles ont signalé au moins quatre incidents.

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

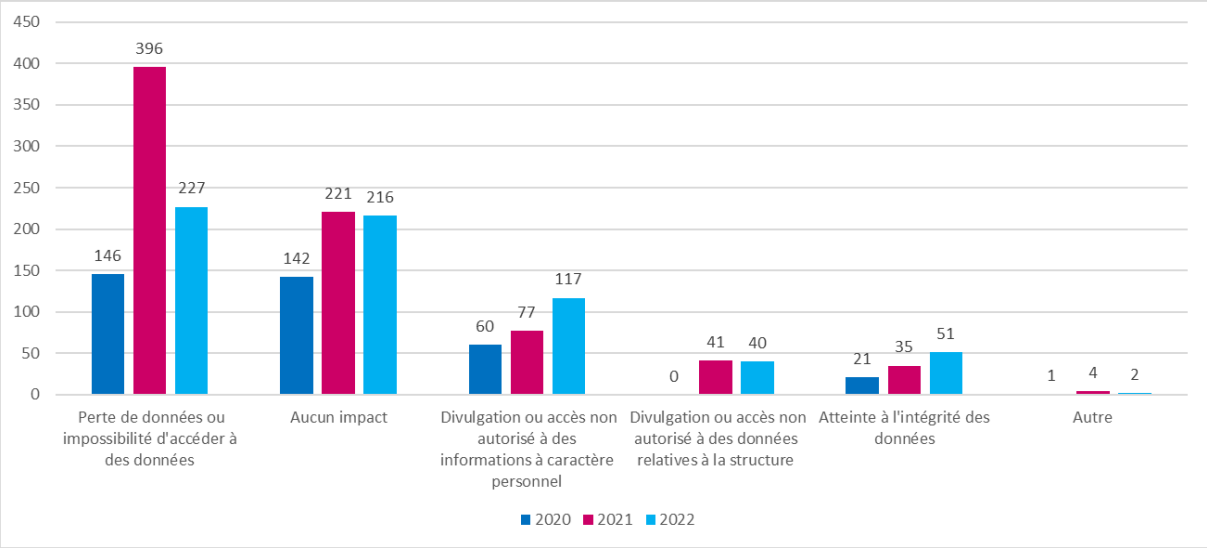


Figure 10- Répartition selon les types d'impact sur les données

Les incidents signalés en 2022, lors desquels tout ou partie des données des applications de la structure n'étaient plus accessibles ont fortement diminué par rapport à 2021. C'est principalement dû à l'absence d'incidents importants concernant les hébergeurs.

Pour 30% 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, la réception de fausses factures papiers ou bien encore des bugs applicatifs ou une perte de la ligne téléphonique.

Les incidents qui ont mené à la divulgation ou l'accès à des informations à caractère personnel ont augmenté par rapport à 2021 et représentent 18% des signalements. Elles sont dues en majeure partie à des vols d'identifiants de comptes d'accès à distance (VPN, RDP) et de messagerie (Webmail). Accessoirement, cette atteinte à la confidentialité des données peut être due à un vol d'équipement.

58% C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son organisation en 2022. Ce chiffre est en augmentation puisqu'il était de 35% en 2020 et de 38% en 2021.

39%

C'est le pourcentage de structures qui ont été contraintes de mettre en place en 2022 un **fonctionnement en mode dégradé** du système de prise en charge des patients (13% de moins qu'en 2021). 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 sur la période d'**une journée si on ne tient pas compte des structures impactées par les incidents majeurs provoqués par une attaque par rançongiciel. Concernant ces derniers, la mise en place d'un mode dégradé de fonctionnement a perduré plus d'un mois avec la nécessité dans les premiers jours d'organiser la prise en charge des patients dans les établissements voisins. 19%** des établissements ayant mis en place un mode dégradé ont subi une interruption du système de prise en charge des patients.

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

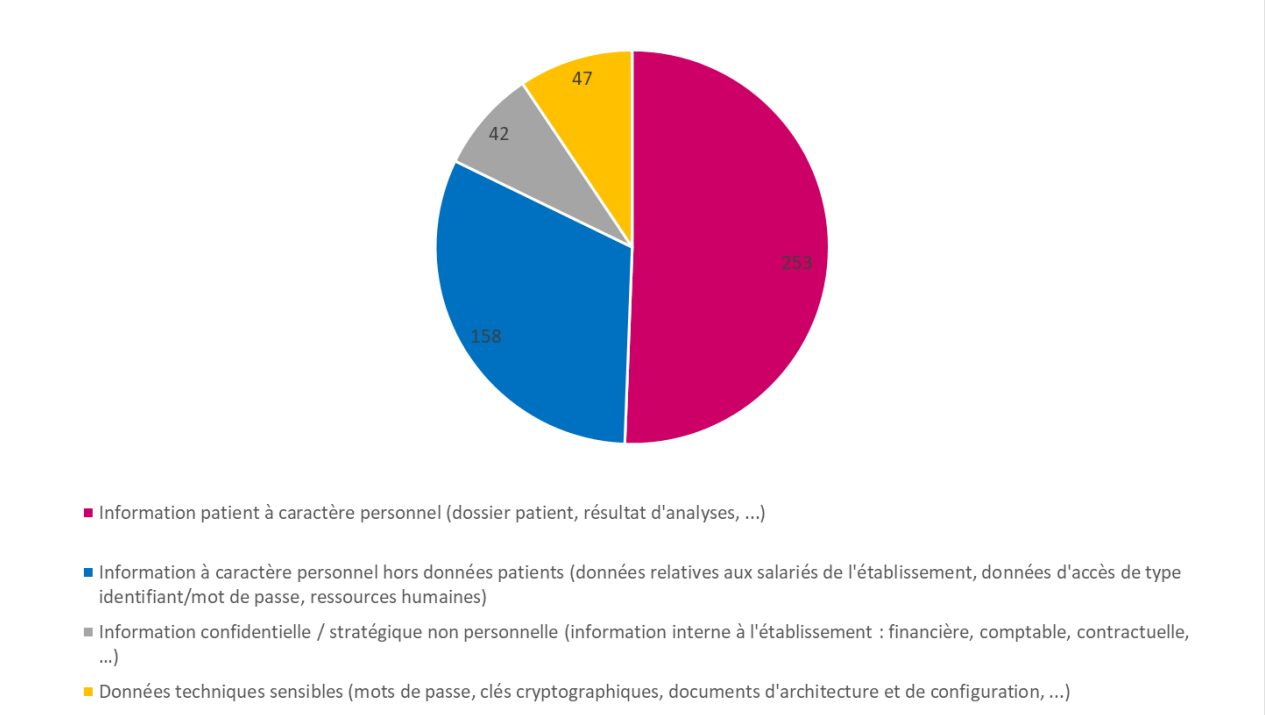


Figure 11 - Répartition selon les types de données impactées

63% 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.

46% 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, **43%** touchent des **données de santé à caractère personnel**, 22% des informations à caractère personnel hors données patient (principalement des identifiants de comptes utilisateur), 14% des données techniques sensibles et enfin 7% 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●●

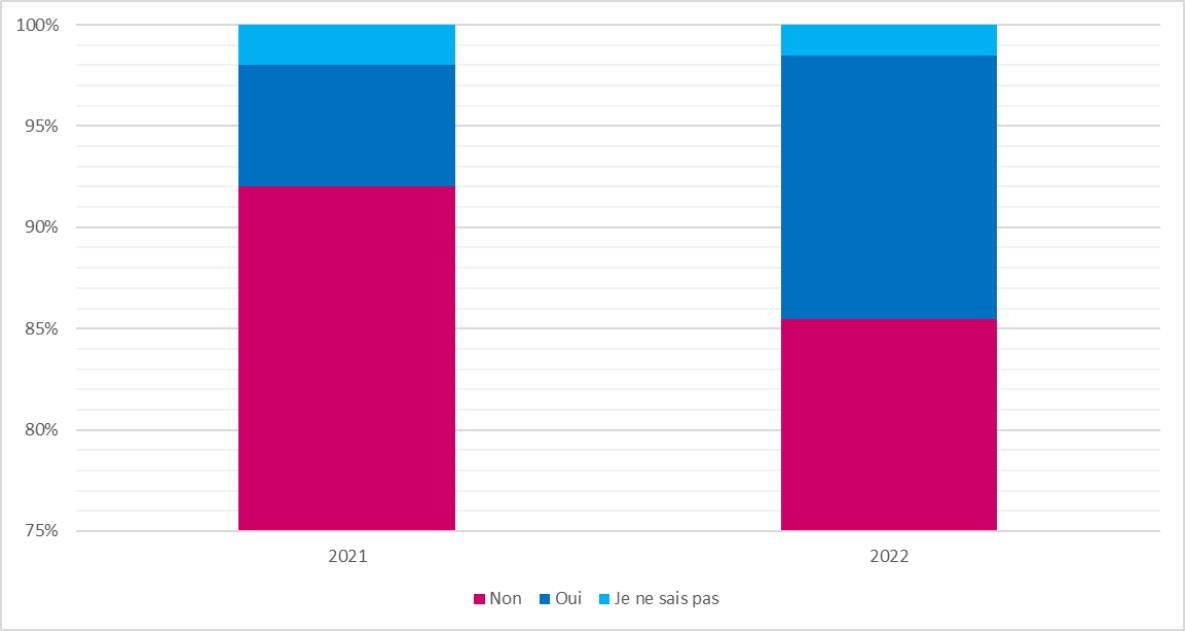


Figure 12 - Mise en danger potentielle des patients

Parmi les **76 mises en danger patient** de cette année 2022 (13% du nombre total d'incidents), **5** incidents ont entrainé une **mise en danger patient avérée**.

Concernant les 94% restants (71), correspondant à la part de mises en danger **potentielles** de patients, on retrouve principalement des incidents liés à l'interruption de services hébergés durant plusieurs jours ou du service téléphonique support du SAMU.

On distingue également les dysfonctionnements des logiciels de prescription/aide à la dispensation liés à des bugs ayant provoqués des erreurs dans les prescriptions et la délivrance des médicaments qui auraient pu entrainer une mise en danger des patients plus importante sans la vigilance des professionnels de santé et la mise en place de procédures permettant d'identifier les erreurs.

Pour rappel, le nombre de décès liés aux erreurs de prescriptions médicamenteuses reste très élevé (de l'ordre de plusieurs milliers). L'ANS, en partenariat avec l'ANSM notamment, a construit un référentiel unique interopérable du médicament pour réduire ces risques.

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

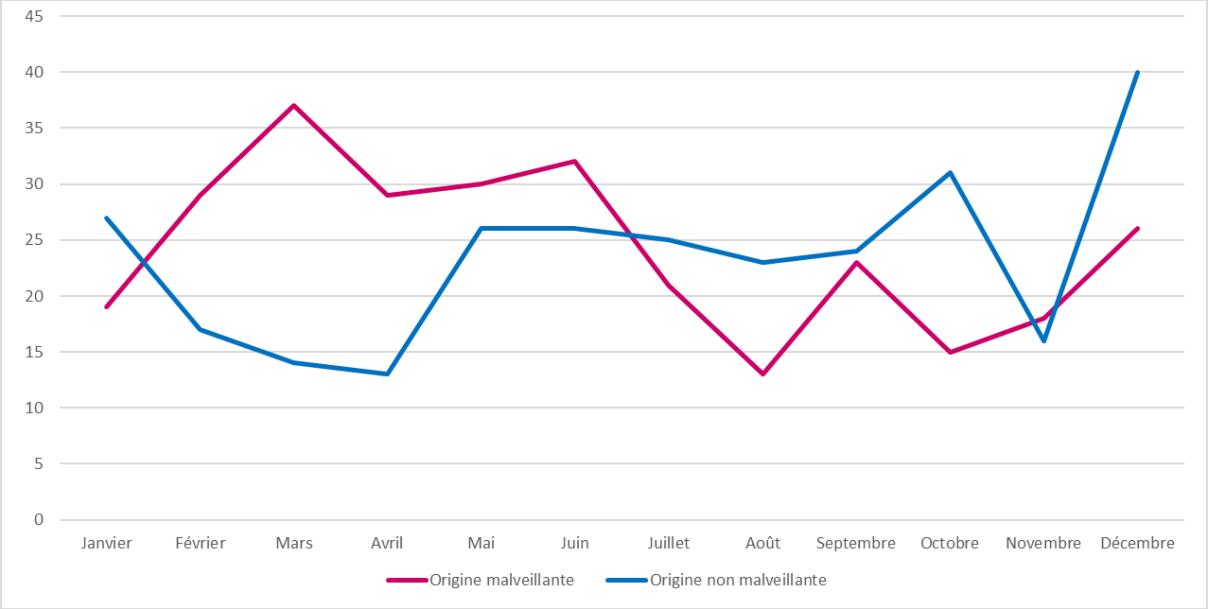


Figure 13 - Répartition selon le type d'incident

Parmi **les incidents déclarés, 50% sont d'origine malveillante et 50% d'origine non malveillante**. Dans l'analyse détaillée de ces deux catégories d'incidents, sont exclus les 26 signalements dits « Hors périmètre » n'ayant pas fait l'objet d'un traitement particulier.

Les actes malveillants

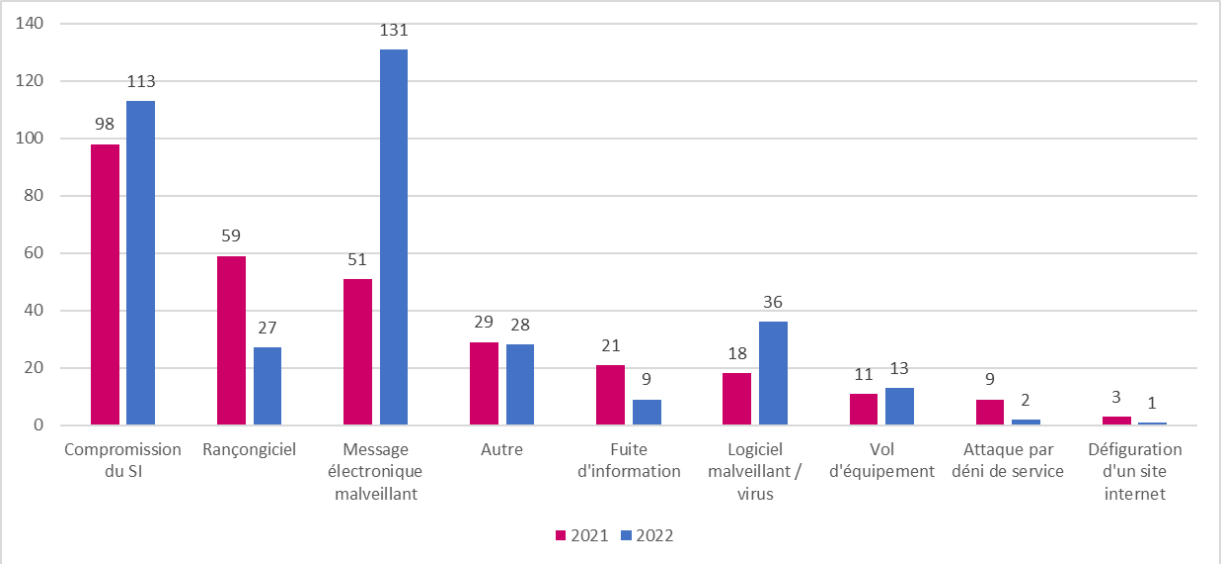


Figure 14 - Nombre d'incidents par type d'origine

L'année 2022 a été marquée 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. Une augmentation significative de la compromission de comptes de maintenance des solutions d'infrastructures et applicatives des structures a été observée.

Les attaquants récupèrent les identifiants selon trois modes opératoires : 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).

Les attaques par rançongiciels ont été plus nombreuses lors du premier trimestre et à partir du mois d'août, entrainant des sinistres majeurs pour certaines structures.

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).
- Enfin, son versement s'apparente à subventionner une organisation criminelle.

Pour rappel, le CERT Santé a publié une fiche rappelant les actions à mener lorsqu'une structure est victime d'un acte de cybermalveillance, en particulier le dépôt d'une plainte : https://www.cyberveille-sante.gouv.fr/dossier-thematique/face-une-menace

Pour renforcer la sécurité de son SI face à la menace rançongiciel et les conséquences d'une compromission majeure, le CERT Santé propose une démarche de durcissement du SI basée sur un support permettant de guider les opérationnels de la sécurité des SI. Il s'agit de mettre

en œuvre des solutions concrètes de sécurisation des sauvegardes, hyperviseurs, de l'administration, du cloisonnement réseau, etc. Présenté sous la forme de fiches et de questions, il permet d'identifier les mesures à mettre en œuvre et de prendre en compte leur mise en œuvre dans le temps. Les mesures préconisées sont basées sur les recommandations de l'ANSSI (un lien vers le guide et les numéros des recommandations concernés est précisé pour chaque mesure).

Le support méthodologique de la démarche a été publié sur GitHub ainsi qu'une vidéo de présentation (voir portail cyberveille-santé). Ils sont disponibles au lien suivant : https://www.cyberveille-sante.gouv.fr/les-services#accompagnement-dans-le-renforcement-de-la-securite-de-votre-si-184

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

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

Notons qu'une part des incidents (16%) relève de plusieurs qualifications. Par exemple, une attaque par rançongiciel, suite à la compromission d'un compte VPN lié 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 (emotet, trickbot) ou générer de la crypto-monnaie.

50% C'est le pourcentage des incidents qui ont une origine malveillante en 2022. Ce chiffre **a diminué de 2%** par rapport à 2021 et **10%** par rapport à 2020.

Evolution du nombre d'incidents d'origine malveillante

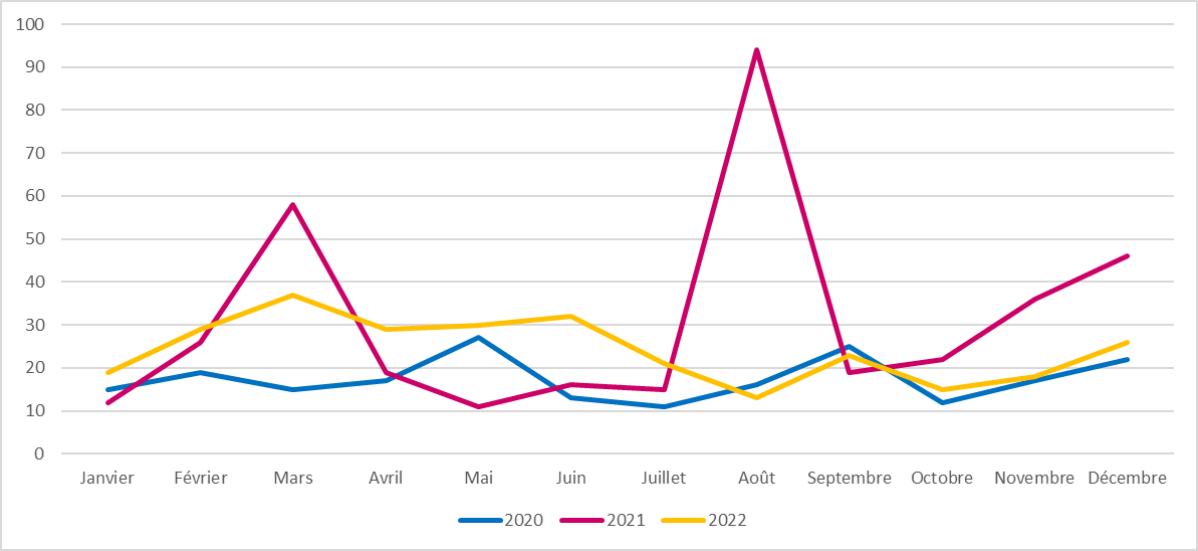


Figure 15 - Evolution du nombre d'incidents dont l'origine est malveillante

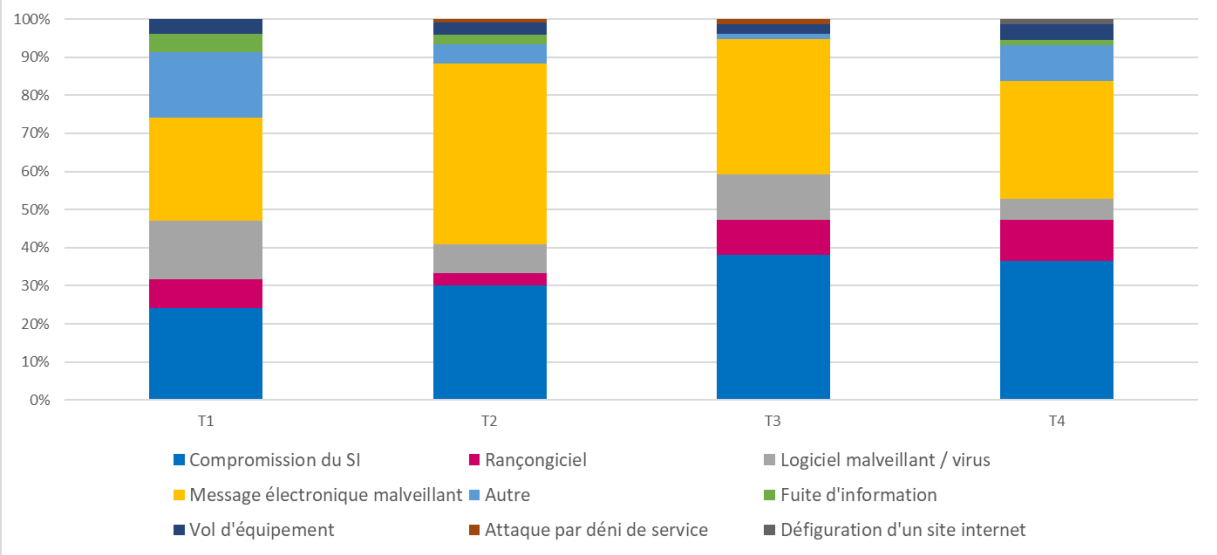


Figure 16 - Origine malveillante des incidents par trimestre

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 rançongiciels) et qui ont été identifiés au cours de l'année :

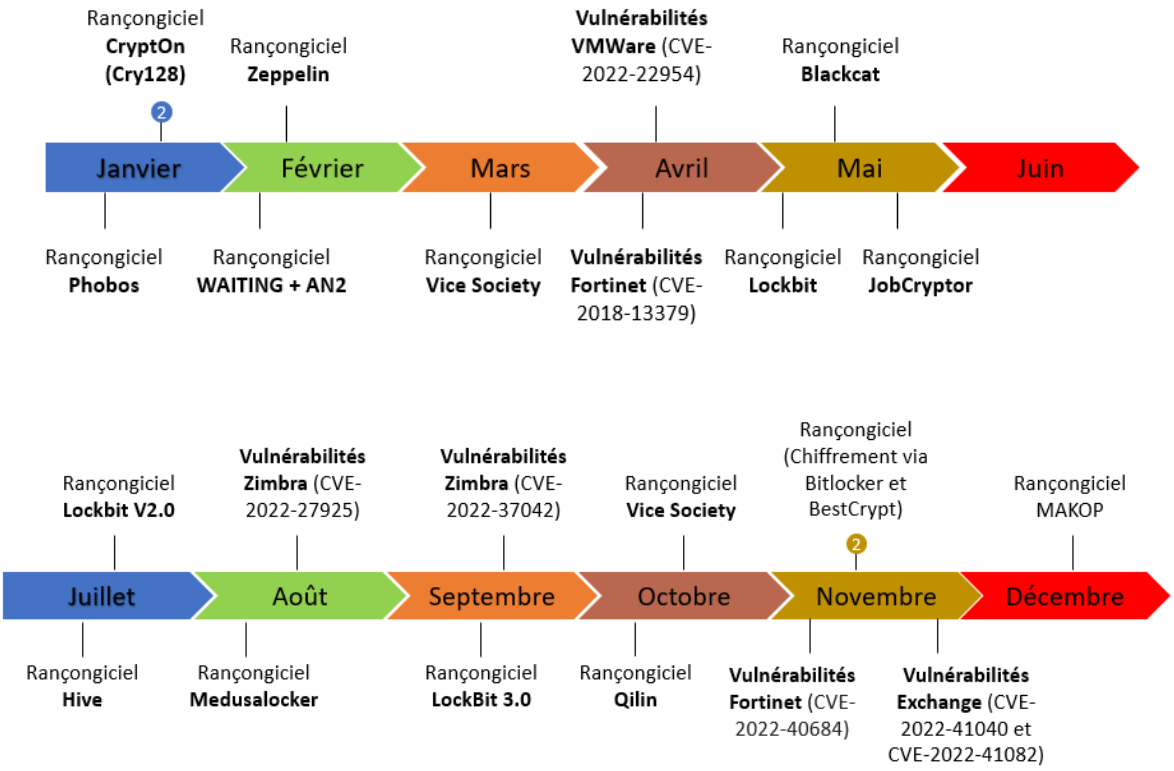


Figure 17 - Chronologie des cyber-menaces identifiées en 2022

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

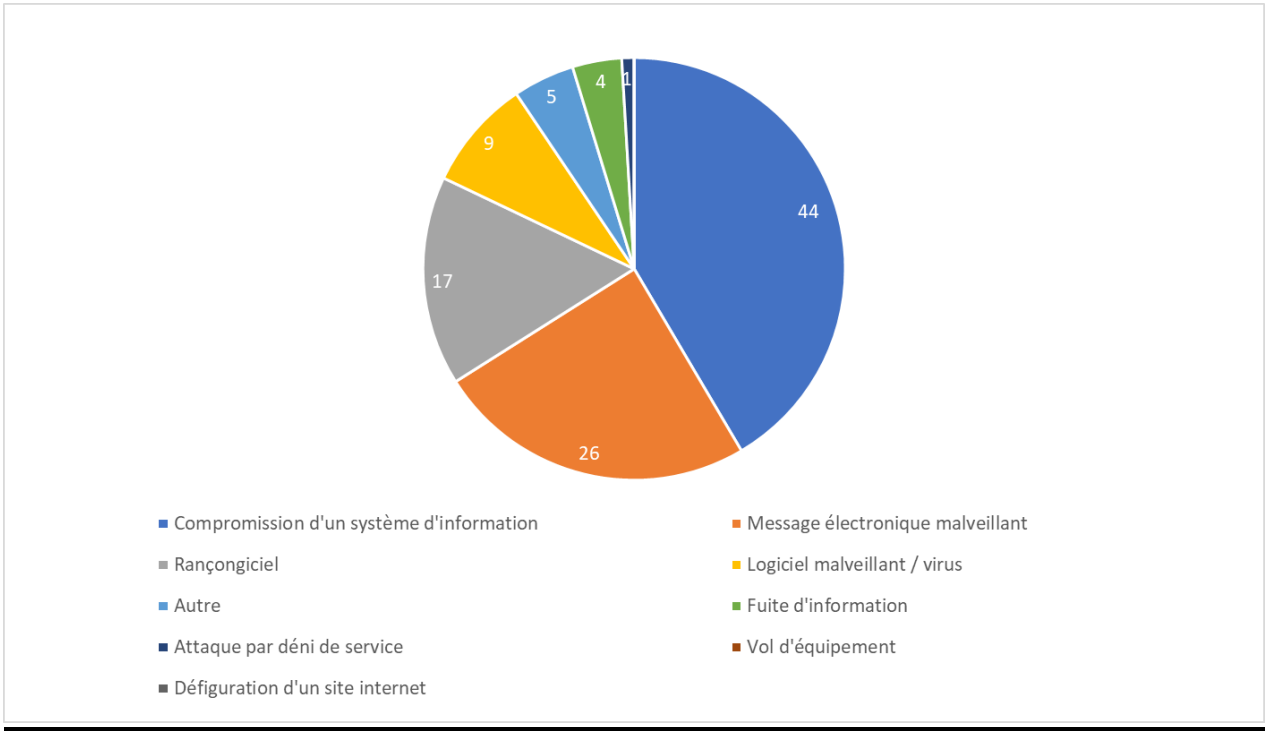


Figure 18 - Origine des incidents pour lesquels un appui technique a été apporté par le CERT Santé

●● Accompagnement global des structures de santé ●●

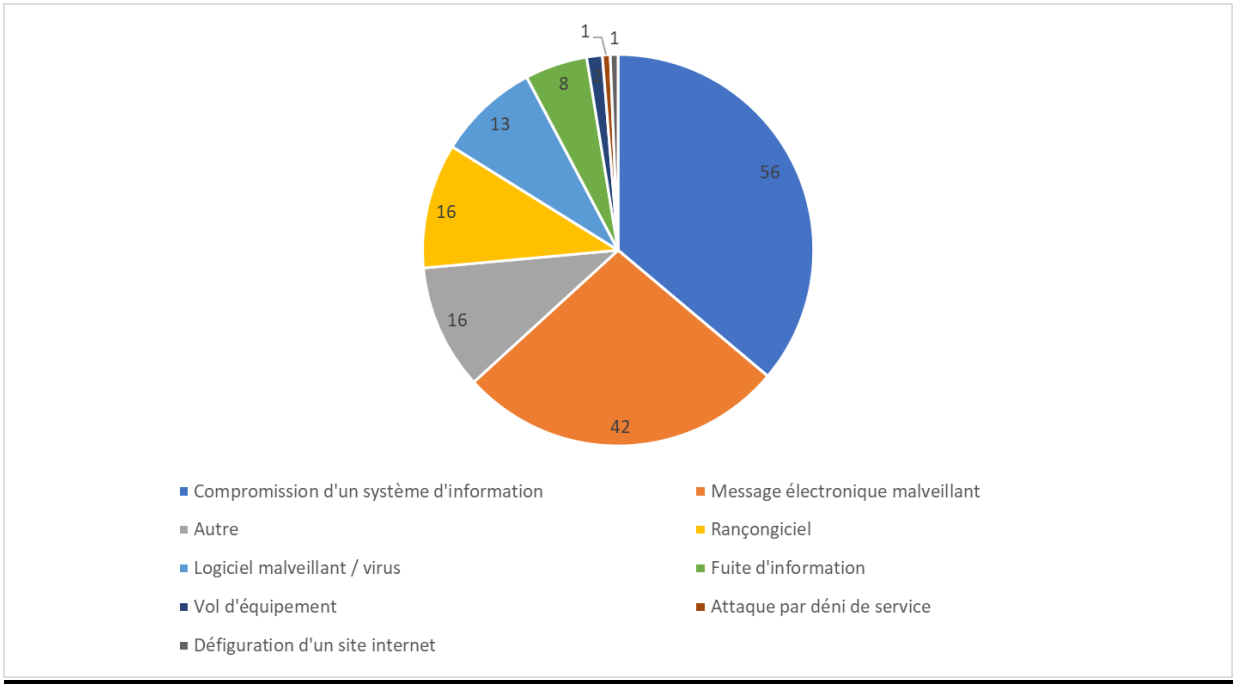


Figure 19 - Origine des incidents pour lesquels des recommandations ont été émises par le CERT Santé

Le nombre de déclarations d'incident pour lesquels une demande d'accompagnement est formulée est en baisse. Cependant, au prorata du nombre de signalements déclarés, les demandes d'accompagnement sont en hausse de 2%. Elles concernent généralement une demande d'appui pour identifier l'origine d'une compromission avérée ou potentielle du SI et la validation des mesures visant à endiguer la propagation de la menace et corriger les failles de sécurité. Ce sont les ES publics (59%) qui ont le plus sollicité le CERT Santé et en particulier les ES supports de GHT (29%).

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

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

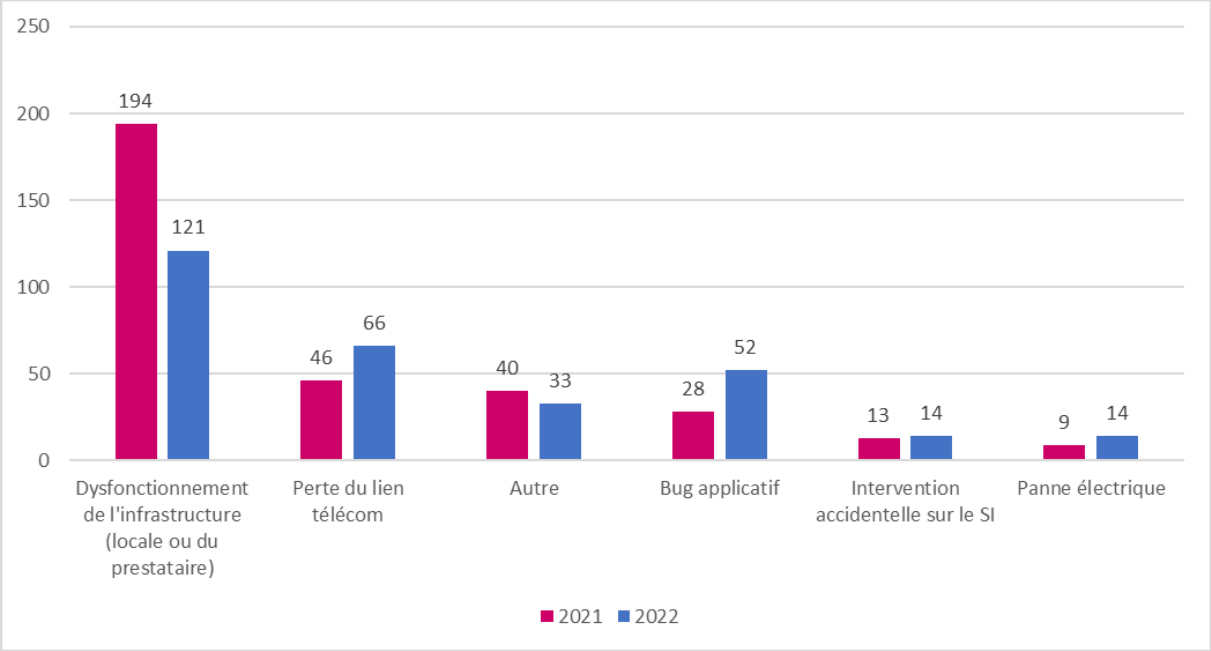


Figure 20 - Origine non malveillante des incidents

L'augmentation du nombre d'incidents ayant une origine non malveillante est principalement liée à des changements opérés sur le SI interne non maitrisés et à 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 41%**.

La **perte du lien télécom** est la deuxième source d'incident d'origine non malveillante (22%). 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.

Le nombre de déclarations lié à un **bug applicatif** (19%) est en augmentation par rapport à 2021. Dans une majorité 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.

Dans la catégorie « Autre » on retrouve principalement des déclarations de failles de sécurité 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.

50% C'est la part d'incident d'origine non malveillante en 2022, ce chiffre a augmenté de 2% par rapport à 2021 et de 10% par rapport à 2020.

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

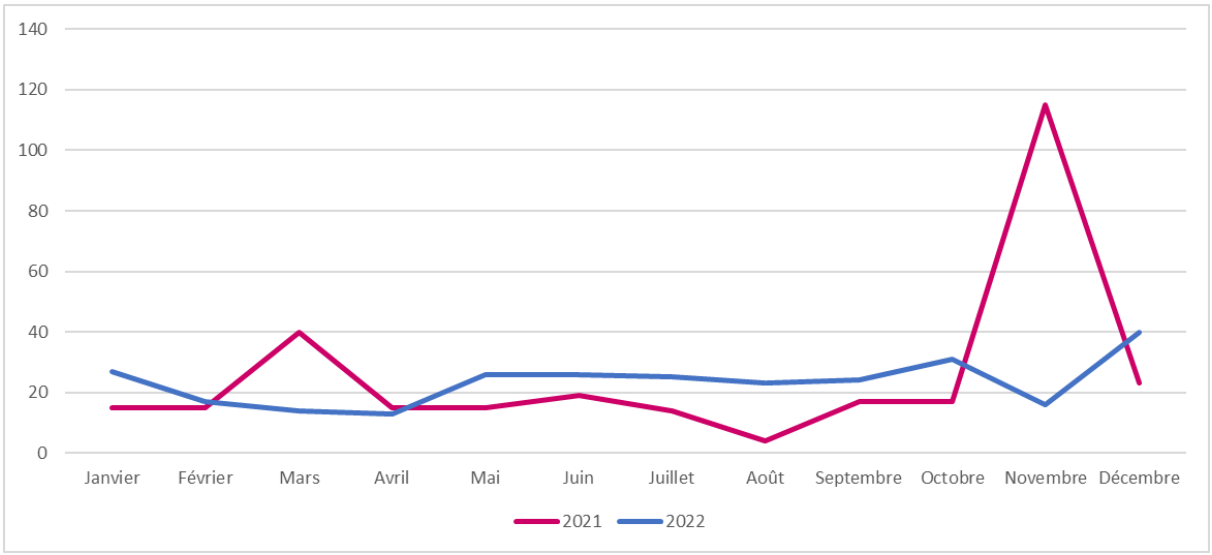


Figure 21 - Evolution du nombre d'incidents dont l'origine est non malveillante

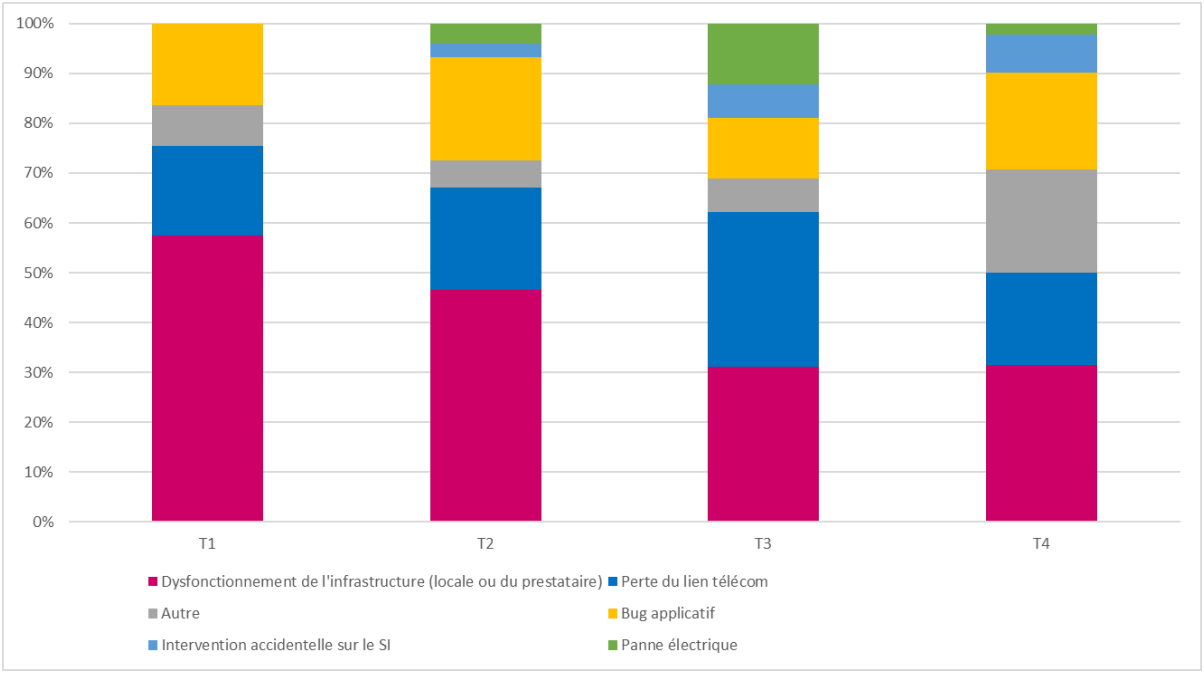


Figure 22 - Origine non malveillante des incidents par trimestre

4.3 Publication d'alertes sur le portail cyberveille-santé

En 2022, quinze alertes ont été publiées sur le portail cyberveille-santé concernant :

- Une campagne de messages malveillants visant à conduire la victime à télécharger des binaires dangereux pour le poste de travail et le reste du système d'information (TrickBot).

- Des vulnérabilités critiques :
  - **[3]** Vulnérabilité sur des systèmes Windows dont l'exploitation permet à un attaquant distant et non-authentifié d'exécuter du code arbitraire ou d'obtenir des privilèges plus élevés ;
  - **[2]** Vulnérabilité sur la messagerie Exchange dont l'exploitation permet à un attaquant possédant un accès authentifié au serveur Exchange de pouvoir exécuter du code arbitraire à distance ;
  - Vulnérabilité sur la suite Office (Follina) dont l'exploitation des vulnérabilités CVE-2022-30190 permet d'exécuter du code arbitraire à partir d'un fichier Word ou RTF ;
  - **[2]** Vulnérabilités sur la solution VPN Fortinet permettant à un attaquant non authentifié d'exécuter du code arbitraire depuis l'interface d'administration ou d'exécuter du code ou des commandes arbitraires via des requêtes spécifiquement conçues ;
  - Une vulnérabilité dans le portail utilisateur admin du pare-feu Sophos dont l'exploitation permet à un attaquant d'exécuter du code arbitraire sur le système ;
  - Vulnérabilités critiques dans la solution de sauvegarde Veeam dont l'exploitation permet à un attaquant distant et non-authentifié d'exécuter du code arbitraire ;
  - Vulnérabilités critiques sur l'agent Axeda présent sur de nombreux dispositifs médicaux dont l'exploitation permet à un attaquant d'accéder à une prise en main complète du système via des identifiants codés en dur dans le programme, un accès complet au système de fichiers et l'exécution de codes arbitraires ;
  - Vulnérabilités Citrix permet à un attaquant non-authentifié d'exécuter du code arbitraire à distance ;
  - Vulnérabilité sur le noyau linux dont l'exploitation permet à un attaquant distant et non authentifié, en envoyant des requêtes spécifiquement forgées, d'exécuter du code arbitraire avec les droits du noyau.
  - Vulnérabilités dans openSSL dont l'exploitation permet à un attaquant, en créant une adresse électronique spécialement forgée dans un certificat, d'exécuter du code arbitraire ou de provoquer un déni de service ;
  - Vulnérabilités dans Google Chrome dont l'exploitation permet à un attaquant distant, en persuadant une victime à consulter un site spécifiquement forgé, d'exécuter du code arbitraire, provoquer un déni de service ou de s'évader d'une sandbox.

5 OBSERVATOIRE DES VULNERABILITES

5.1 Service national cyber-surveillance

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

L'audit de cyber-surveillance est un service de diagnostic et d'évaluation de la sécurité du système d'information vis-à-vis d'Internet (service national de cyber-surveillance). Ce service de cyber-surveillance est :


Gratuit et mis à la disposition des établissements de santé (victime d'un acte de cyber-malveillance ou OSE) ;


Confidentiel (seul le RSSI de la structure concernée et les auditeurs ont accès aux résultats détaillés) ;


En grande partie automatisé (des phases de collecte et de tests jusqu'à la génération du rapport).

Le service de cyber-surveillance réalise un audit des domaines et sous-domaines des structures de santé exposés sur Internet déclarés par la structure de santé[6] afin de détecter d'éventuelles vulnérabilités.

L'audit se déroule en deux phases :

- Une phase passive consistant en la collecte d'informations à partir de sources ouvertes sur Internet ;
- Une phase active consistant en 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 ;
    - Le test des comptes avec des identifiants faibles et des identifiants par défaut ;
    - L'utilisation des scanneurs généralistes / spécifiques afin de détecter d'éventuelles erreurs de configuration et / ou de défauts de mise à jour.

Le rapport de cyber-surveillance fourni présente :

- Le périmètre de l'évaluation avec la liste des domaines et sous-domaines, avec une cartographie des systèmes détectés ;
- Une synthèse managériale permettant de prendre rapidement connaissance du niveau de sécurité constaté et de la typologie des vulnérabilités ;
- Une synthèse technique présentant :
    - les vulnérabilités détectées par niveau de criticité,
    - un plan d'actions de remédiation hiérarchisé ;
- Le détail des vulnérabilités identifiées avec pour chacune :
    - la criticité,

[6] A l'occasion de ce cadrage, le CERT Santé peut détecter des domaines ou sous domaines non déclarés par la structure

- le type de vulnérabilité (ou catégorie, telle que usurpation d'identité, défaut de configuration, …),
- le SI affecté,
- la description de la vulnérabilité,
- la recommandation associée en vue de sa correction.

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[7]. Ces informations permettent d'encadrer les audits de cyber-surveillance lorsqu'ils sont réalisés par des prestataires à la demande des structures.

En 2022, 113 audits ont été réalisés : quarante-cinq GHT (297 ES), cinquante établissements hospitaliers, deux ESMS, cinq ordres de professionnels de santé et deux GCS situés dans les DOM COM.

5.2 Service de veille proactive

Le CERT Santé a renforcé son activité de veille proactive au regard du nombre important de vulnérabilités critiques qui ont fait l'objet d'une publication en 2022. Ainsi afin de prévenir la compromission potentielle de SI au travers de l'exploitation de ces vulnérabilités, le CERT a alerté plus de 500 structures. Ces alertes ont principalement concerné l'environnement Windows (système d'exploitation, messagerie, suite Office) et des solutions d'accès à distance (VPN (Fortinet) ou bureau à distance (Citrix)).

Cette activité d'alerte est réalisée en étroite coopération avec le CERT-FR. Ainsi le CERT Santé a relayé une soixantaine d'alertes concernant des compromissions avérées ou potentielles de SI identifiées par l'ANSSI.

Vous trouverez ci-dessous un rappel des principales activités de surveillance du CERT Santé.

Serveurs identifiés dans des listes noires d'activités cyber-malveillantes

Ces machines compromises sont référencées dans des listes noires gérées par différentes communautés intervenant dans la lutte contre la cybercriminalité (firehol, MISP, DnsBL …).

Le CERT Santé récupère quotidiennement cette liste noire, compare les adresses IP avec celles du secteur santé puis alerte par message électronique le RSSI/ référent sécurité de la structure concernée le cas échéant en précisant le type d'activité malveillante (spam, tentative d'accès brute force, ...) et la liste noire référençant sa plage IP ou son nom de domaine.

Vulnérabilités critiques présentes sur des services exposés sur Internet

Grâce à la veille quotidienne sur les vulnérabilités critiques des composants utilisés par les structures de santé et la cartographie Internet des structures, le CERT Santé est en mesure d'alerter par message électronique le RSSI / référent sécurité des structures qui exposent un

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

service (accès à distance principalement) potentiellement vulnérable sur internet dès la publication de la vulnérabilité (CVE).

5.3 Constat et recommandations

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…). L'exploitation de certaines vulnérabilités peuvent permettre à un attaquant d'accéder par rebond à tout ou partie de leur système d'information avec parfois des privilèges élevés. Pour les structures ayant été auditées deux fois (principalement des CHU), on constate une réduction significative de la présence de ce type de vulnérabilités.

Les recommandations suivantes sont régulièrement communiquées aux structures :

- Réduire les surfaces 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 télé-administration reposant sur RDP ou d'autres protocoles. Il a ainsi été démontré la possibilité de prendre le contrôle total de serveurs ;

- Appliquer une politique de mot de passe suffisamment robuste afin d'éviter d'être la cible d'action malveillante depuis Internet (voir guide https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_s%C3%A9curit%C3%A9_mot_passe.pdf);

- Améliorer le suivi des correctifs : des structures de santé exposent sur internet des systèmes avec des composants obsolètes. Il est indispensable d'assurer une veille des composants exposés sur internet et de les mettre à jour suivant un processus éprouvé lorsque des correctifs sont disponibles. La priorité doit être donnée aux correctifs de sécurité correspondants à des vulnérabilités critiques afin de se prémunir au plus vite d'attaques cherchant à les exploiter ;

- 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 ;

- Renforcer les configurations et la sécurisation des accès : beaucoup de failles 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 ;

- Vérifier la suppression des failles web classiques (présentées dans le Top 10 OWASP[8]) : 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 failles référencées par l'OWASP s'il est correctement configuré ;

- 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.

[8] 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.

6 GLOSSAIRE

ANS	Agence du Numérique en Santé
ANSM	Agence Nationale de la Sécurité du Médicament et des produits de 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
Cryptovirus	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.
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 susceptibles 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 ministérielle au numérique en santé
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
HFDS	Haut Fonctionnaire de Défense et Sécurité
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.
RGPD	Règlement Général sur la Protection des Données

NOTES PERSONNELLES

Pour aller plus loin, rendez-vous sur :

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

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté Égalité Fraternité

CERT Santé

AGENCE DU NUMÉRIQUE EN SANTÉ