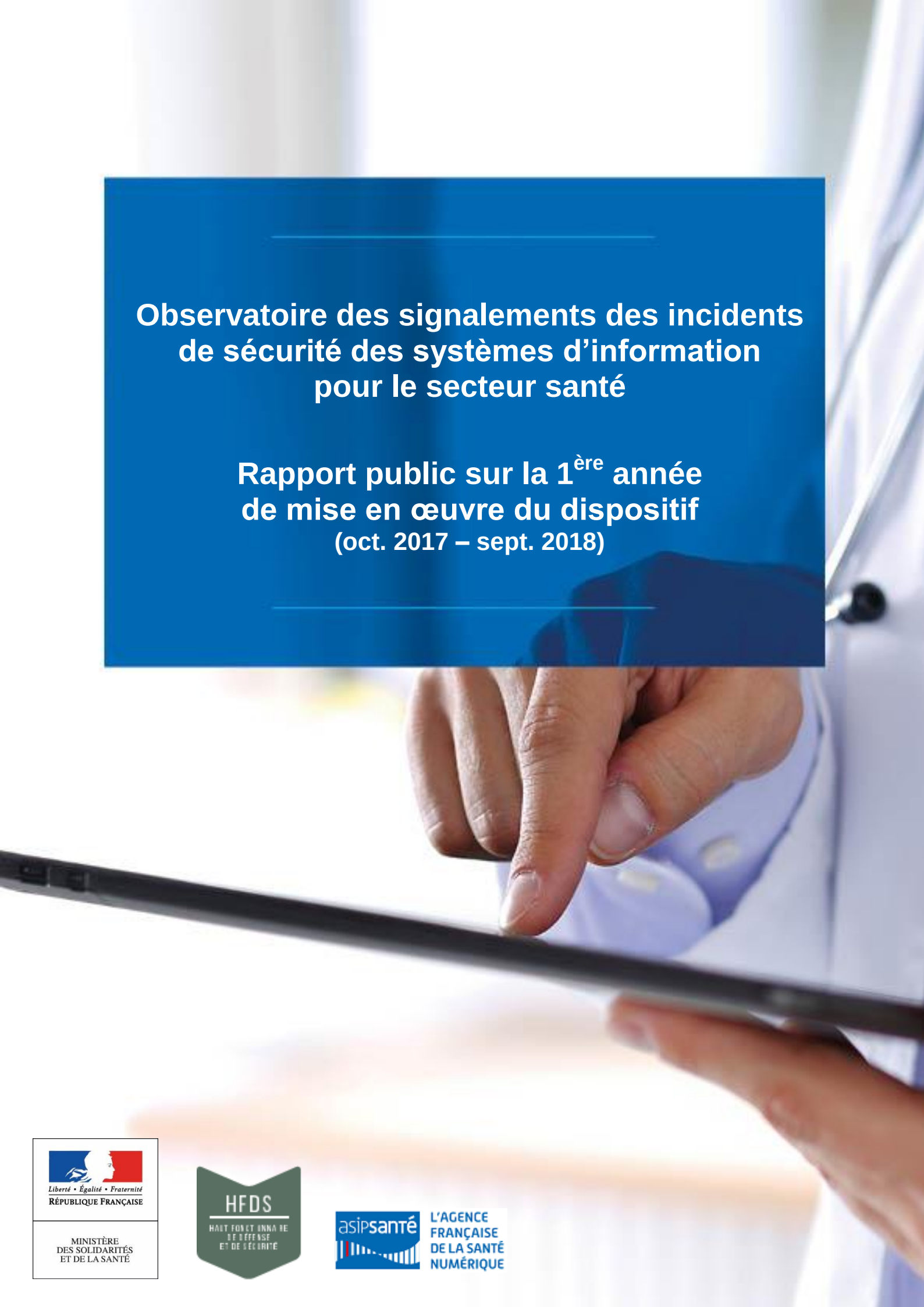


Observatoire des signalements des incidents de sécurité des systèmes d'information pour le secteur santé

Rapport public sur la 1ère année de mise en œuvre du dispositif

(oct. 2017 – sept. 2018)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

HFDS
HAUT FONCTIONNAIRE
DE DÉFENSE
ET DE SÉCURITÉ

asipsanté
L'AGENCE
FRANÇAISE
DE LA SANTÉ
NUMÉRIQUE

SOMMAIRE

1 Introduction 4
2 Dispositif de traitement des signalements des incidents de sécurité des systèmes d'information pour le secteur santé 5
2.1 Contexte réglementaire 5
2.2 Présentation des activités 5
3 Temps forts de la montée en puissance du dispositif 8
4 Traitement des signalements 9
4.1 Chiffres clés pour la période du 1er octobre 2017 au 30 septembre 2018 9
4.2 Informations générales sur les signalements 10
4.3 Nature des signalements 15
4.4 Incidents notables ayant fait l'objet d'un retour d'expérience anonymisé 19
5 Glossaire 20

TABLE DES FIGURES

Figure 1 - Nombre de signalements par mois 10
Figure 2 - Etat des incidents lors de leur signalement 11
Figure 3 - Etat actuel des incidents signalés 11
Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt 12
Figure 5 - Nombre de signalements rapporté à l'activité hospitalière des régions 13
Figure 6 - Répartition des signalements par région 13
Figure 7 - Répartition des signalements selon le type de structure 14
Figure 8 - Part des signalements comparée à la part des établissements selon leur raison sociale . 14
Figure 9 - Nombre d'incidents par type d'origine 15
Figure 10 - Répartition selon les types d'impact sur les données 16
Figure 11 - Evolution du nombre d'incidents dont l'origine est malveillante / non malveillante 17
Figure 12 - Mise en danger potentielle des patients 17
Figure 13 - Origine non malveillante des incidents par trimestre 18
Figure 14 - Origine malveillante des incidents par trimestre 18

1 INTRODUCTION

Le ministère des solidarités et de la santé a mis en place depuis le 1er octobre 2017 un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information. Au cours de cette première année d'activité, plus de 300 incidents ont été remontés au ministère et une quarantaine de demandes d'accompagnements ont été formulées. En effet, au-delà de l'obligation de déclaration par les structures de santé, le ministère propose un service d'appui aux structures de santé dans le cadre du traitement des incidents mais aussi en vue d'améliorer leur capacité à se protéger contre les menaces cyber.

Afin de bénéficier pleinement de cet appui, je vous invite à déclarer systématiquement vos incidents de sécurité des systèmes d'information. Le ministère veille à strictement préserver la confidentialité concernant les déclarants et les données relatives aux incidents car elle est garante de la confiance de l'ensemble des acteurs dans le dispositif.

Complémentaire à la remontée des incidents, le portail cyberveille-santé dédié à la sécurité numérique dans le secteur santé joue un rôle central dans l'information des acteurs opérationnels de la sécurité : il publie quotidiennement des informations sur les vulnérabilités présentes au sein des systèmes d'information et diffuse régulièrement des alertes sur des menaces sectorielles. Ainsi, de nombreux établissements de santé ont été informés durant l'été 2018 de campagnes massives de messages électroniques malveillants visant à récupérer des informations confidentielles.

En proposant un espace sécurisé, le portail cyberveille-santé est le moyen privilégié pour échanger : il doit favoriser la coopération et l'entraide entre les acteurs (ministère, ARS et structures de santé), afin de mieux faire connaitre les impacts des différentes menaces de cybersécurité à l'ensemble du secteur et permettre aux structures les plus vulnérables d'améliorer leur résilience aux incidents de sécurité.

Vos retours permettront aussi d'orienter la politique du ministère en matière de sensibilisation et d'accompagnement du secteur dans le domaine de cybersécurité.

Le dispositif étant dans sa première année de fonctionnement, il est encore en phase de montée en charge. Les indicateurs qui sont présentés dans ce rapport révèlent les premières tendances et feront très certainement l'objet d'une évolution sensible dans le futur.

La secrétaire générale des ministères sociaux,
Haut fonctionnaire de défense et de sécurité

Sabine Fourcade

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

2.1 Contexte réglementaire

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.

Dans le cadre de la mise en application du décret n° 2016-1214 du 12 septembre 2016 (JORF n°0214 du 14 septembre 2016) relatif aux conditions de traitement des incidents graves de sécurité des systèmes d'information du secteur santé, l'ASIP Santé est désignée comme le groupement d'intérêt public (GIP) en charge d'apporter un appui au traitement des incidents de sécurité des systèmes d'information.

L'arrêté d'application du 30 octobre 2017 relatif aux modalités de signalement et de traitement des incidents précise le rôle des agences régionales de santé (ARS) et de l'ASIP Santé dans le traitement des signalements et l'accompagnement des structures.

2.2 Présentation des activités

Dans le cadre du dispositif de traitement des signalements des incidents de sécurité des systèmes d'information de santé, la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) propose un accompagnement et un appui aux structures de santé dans le cadre du traitement de leur incident ainsi qu'un portail de veille et d'échange.

Le traitement des incidents SI

Le traitement des incidents est de la responsabilité des structures de santé. L'accompagnement et l'appui mis en place par la cellule ACSS dans le cadre de leur signalement consiste à :

- récupérer 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 de l'ARS compétente ;
- apporter, si besoin, un accompagnement dans le traitement de l'incident de sécurité des systèmes d'information ;
- informer le fonctionnaire de sécurité des systèmes d'information (HFDS/FSSI), qui assure le pilotage du traitement en cas d'incident de sécurité majeur (incident de niveau « significatif ») ;
- diffuser une alerte à 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 ;

- le cas échéant, diffuser une alerte vers les autorités compétentes de l'Etat selon la nature de l'incident :
  - à l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
  - aux agences sanitaires dans le cas d'un incident majeur dans la prise en charge des patients ;
  - à la CNIL en cas de fuite massive de données.

Afin d'accompagner les structures de santé dans le cadre de cette nouvelle obligation, conformément à l'article 5 de l'arrêté du 30 octobre 2017, il a été mis à leur disposition :

- un espace dédié aux déclarations au sein du portail de signalement des évènements sanitaires indésirables,
- un portail d'information (https://www.cyberveille-sante.gouv.fr) contribuant à informer les acteurs sur le dispositif de traitement des signalements, publiant des informations et de la documentation permettant d'améliorer la gestion de la sécurité au quotidien et proposant un espace sécurisé dédié aux échanges entre les acteurs de la sécurité au sein des structures de santé.

La veille sur l'actualité de la sécurité des SI et sur les menaces propres au secteur de la santé

Le portail **cyberveille-sante.gouv.fr** est animé quotidiennement pour assurer la publication :

- de bulletins de sécurité sur les technologies standards (émergence de menaces, méthodologies d'attaques innovantes, nouvelles vulnérabilités) et spécifiques au secteur santé (incidents de sécurité, nouvelles vulnérabilités) ;
- d'alertes de sécurité et de recommandations pour se protéger des menaces en cours sur la page d'accueil du portail - un flux RSS permet d'en être informé ;
- de documents d'appui à la gestion de la sécurité et des incidents (fiches réflexes, fiches pratiques, guides de bonnes pratiques).

L'animation de la communauté cyberveille-santé

Le portail cyberveille-santé dispose également d'un espace sécurisé au sein duquel les correspondants cyberveille-santé de la cellule ACSS peuvent échanger entre eux sur :

- des retours d'expérience sur le traitement d'incidents rencontrés et des indicateurs sur les actes de cybermalveillance ;
- les bulletins de sécurité ou les documents publiés sur le portail ;
- 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 de faciliter les échanges autour de la cybersécurité entre les acteurs du secteur santé.

Le dispositif apporte son appui aux structures dans le cadre de la résolution d'un incident :

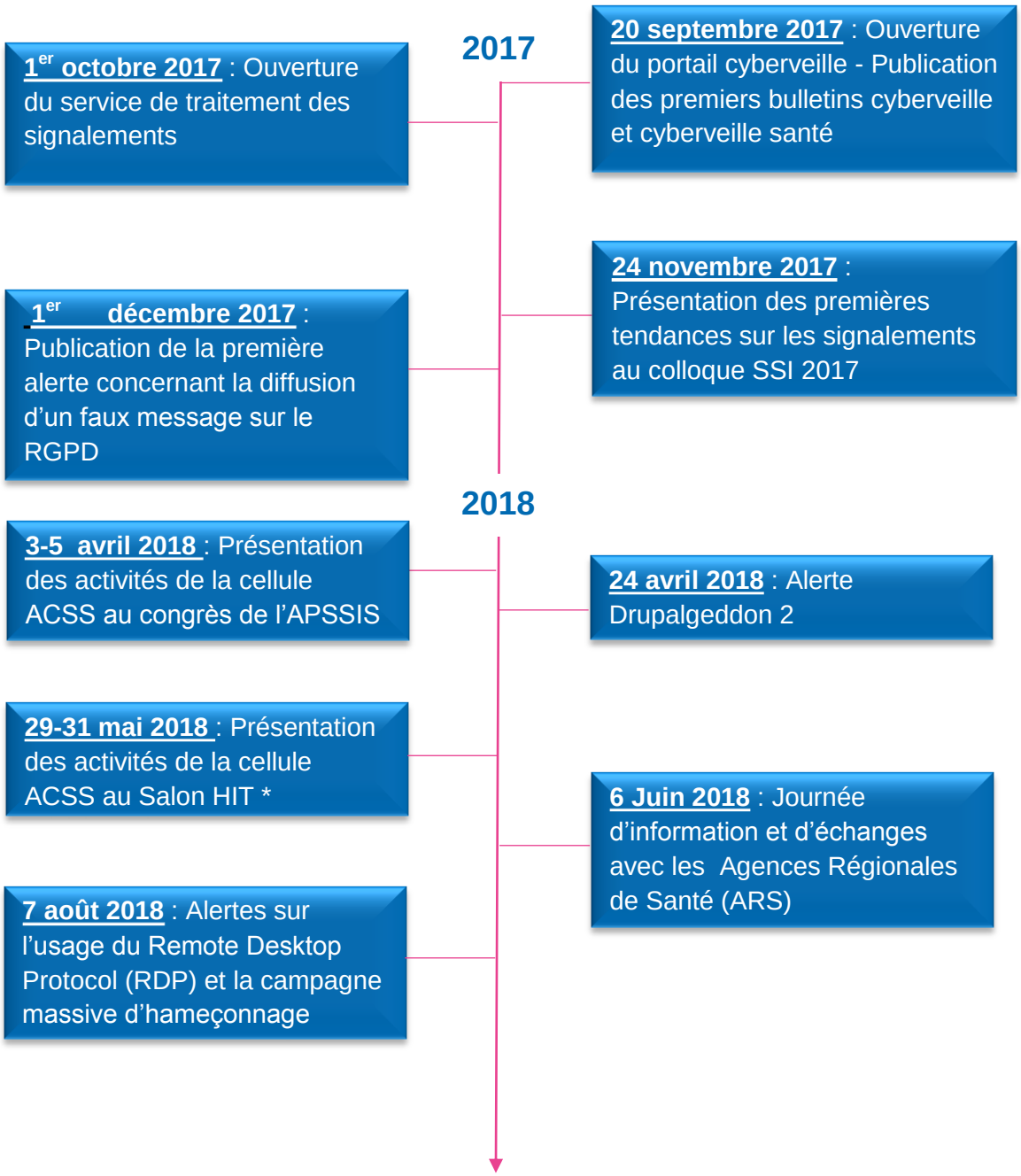
- orientation vers un prestataire de proximité référencé par le GIP cybermalveillance.gouv.fr dans le cas d'une demande d'intervention sur site ;
- communication d'une fiche réflexe (ex : phishing, cryptovirus, code malveillant ou défiguration de site Web) ou de recommandations de mesures de remédiations correspondants à la nature de l'incident (ex : changements de mots de passe, mise en liste noire d'adresses de messagerie, blocage de protocoles).

La cellule ACSS propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité :

- évaluation technique des plans d'action sécurité :
  - Priorisation des mesures proposées (ex : renforcer le cloisonnement réseau du SI support d'activités de soins vitaux) ;
  - Proposition pour améliorer la sécurité du SI (ex : utilisation d'une application pour l'administration locale ou pour limiter l'exploitation de vulnérabilités)
- rappel des bonnes pratiques d'administration et de développement (ex : promotion des guides de l'ANSSI sur la configuration d'un domaine Active Directory[1] ou la conception d'application web).

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

3 TEMPS FORTS DE LA MONTEE EN PUISSANCE DU DISPOSITIF



* Paris Healthcare Week

4 TRAITEMENT DES SIGNALEMENTS

4.1 Chiffres clés pour la période du 1er octobre 2017 au 30 septembre 2018

319

incidents déclarés sur le portail des signalements

41

demandes d'accompagnement

6

incidents « significatifs » ont fait l'objet d'un suivi particulier de la part du FSSI

3

incidents ont été pris en charge par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

13

incidents ont été communiqués à l'Agence Nationale de la Sécurité du Médicament et des produits de santé (ANSM)

3

incidents ont fait l'objet d'une alerte à la DGS/ CORRUSS.

319 incidents ont été déclarés sur le portail des signalements. On distingue des pics de signalements suite aux actions de communication menées par le FSSI des ministères sociaux et l'ASIP Santé ainsi qu'au moment de la publication d'alertes sur le portail cyberveille-santé. On estime que le nombre d'incidents déclarés correspond à 20% des incidents réels auxquels sont confrontées les structures de santé.

Les incidents qui ont nécessité une prise en charge par l'ANSSI concernaient des CHU ou gros CH ne disposant pas de suffisamment de compétences pour analyser l'origine malveillante de leurs incidents. Après analyse, ces incidents, s'ils ont perturbé le fonctionnement de l'établissement, n'ont pas eu d'incidence sanitaire.

Trois incidents dont l'origine n'était pas malveillante (bugs informatiques sur des logiciels de prescription, interruption brutale de moyens de transmission des données) ont entrainé des effets indésirables sur quelques patients (moins de 10 patients).

Les 3 alertes transmises à la DGS/CORRUSS concernaient :

- un incident d'origine malveillante impactant les activités cliniques, médico-techniques et techniques d'un CH (crypto-virus chiffrant les données et les rendant inaccessibles à leurs utilisateurs légitimes) ;
- deux bugs logiciels ayant entrainé la production de prescriptions erronées.

4.2 Informations générales sur les signalements

Depuis son lancement officiel, en octobre 2017, la cellule ACSS a enregistré un total de 319 signalements, en date du 30 septembre 2018 (moyenne de 27 signalements par mois). Les deux mois les plus chargés ont été juillet et août car de très nombreux établissements de santé ont été touchés par plusieurs campagnes d'hameçonnage à l'échelle nationale.

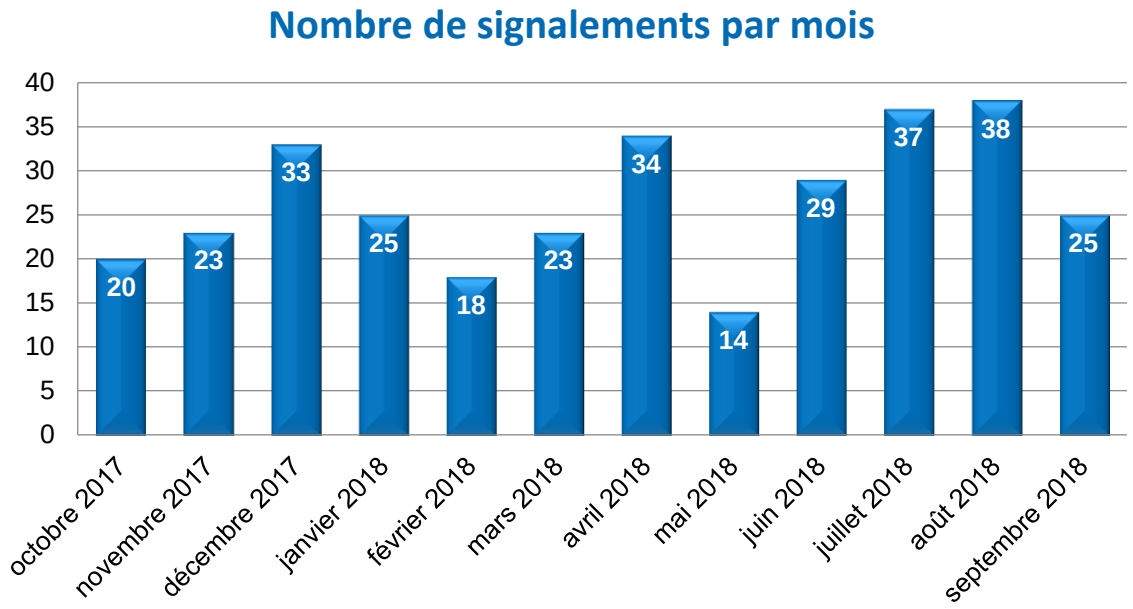


Figure 1 - Nombre de signalements par mois

Parmi l'ensemble des signalements, 38 n'entraient pas directement dans le champ d'application du décret n° 2016-1214 du 12 septembre 2016. Il s'agit principalement de déclarations réalisées par des établissements d'hébergement pour personnes âgées dépendantes. Lorsque ces signalements concernaient des incidents provoqués par des actes de cybermalveillance, une attention particulière a été portée pour veiller à la bonne mise en œuvre des mesures de remédiation.

Plusieurs structures qui n'avaient pas connaissance du dispositif ont finalement signalé leur incident à la suite d'un rappel effectué par leur ARS ou le FSSI. Il est prévu de relancer des actions de promotion du dispositif à l'occasion de la publication de ce rapport.

Etat des incidents lors de leur signalement

Dans plus de la moitié des cas, l'incident est déjà résolu lors de sa déclaration par la structure. Dans presque 15 % des cas, l'origine de l'incident n'a pas encore été identifiée (en cours d'investigation).

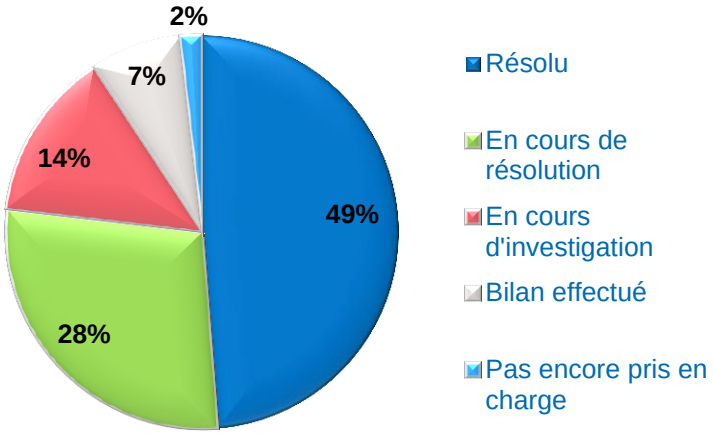


Figure 2 - Etat des incidents lors de leur signalement

Etat actuel des incidents signalés

93% des incidents ont été résolus. Les 7% restants correspondent à des signalements toujours en cours de traitement ou à des signalements d'incidents, évalués au niveau « grave », non résolus, pour lesquels la structure n'a apporté aucune réponse relative au traitement**.**

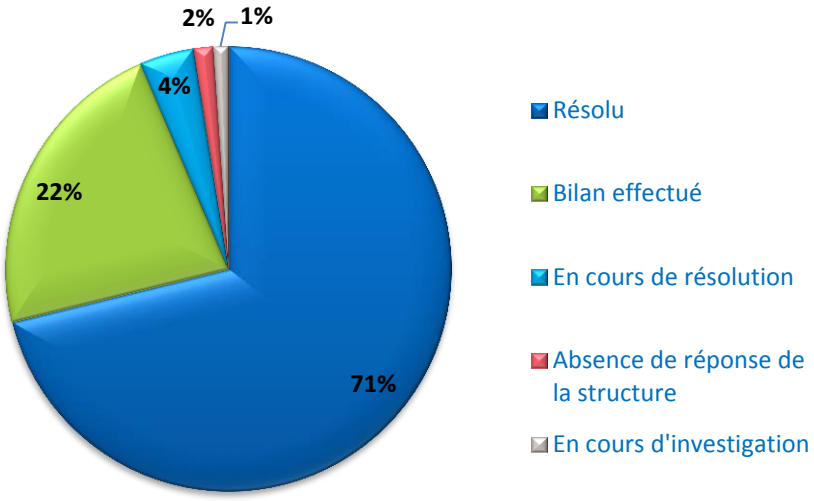


Figure 3 - Etat actuel des incidents signalés

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

85% des signalements sont effectués en jours et heures ouvrés, entre 9h et 18h. Les incidents déclarés en dehors de cette période ne constituaient pas des incidents majeurs et n'ont pas nécessité une intervention du FSSI.

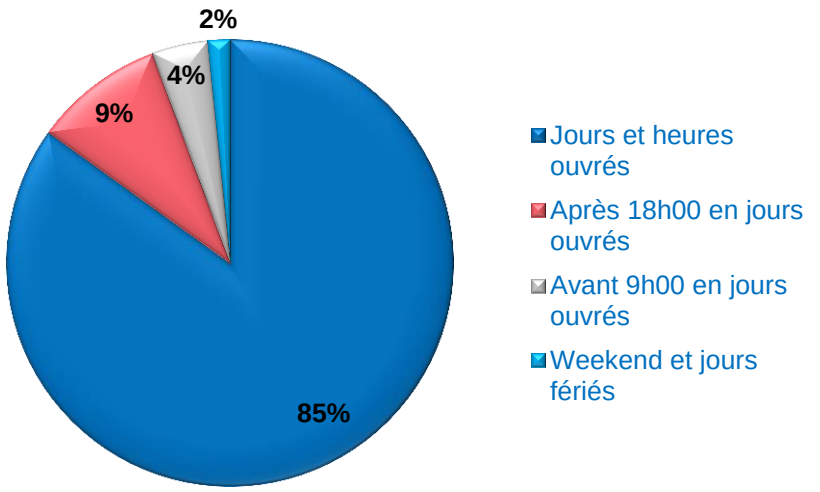


Figure 4 - Répartition des signalements selon l'horaire et le jour de leur dépôt

Les régions pour lesquelles le nombre de signalement est le plus important sont l'Île-de-France et l'Occitanie avec respectivement 40 et 41 signalements. Ces deux régions représentent à elles seules plus de 25% du total des signalements.

L'ensemble des régions a déclaré au moins un incident

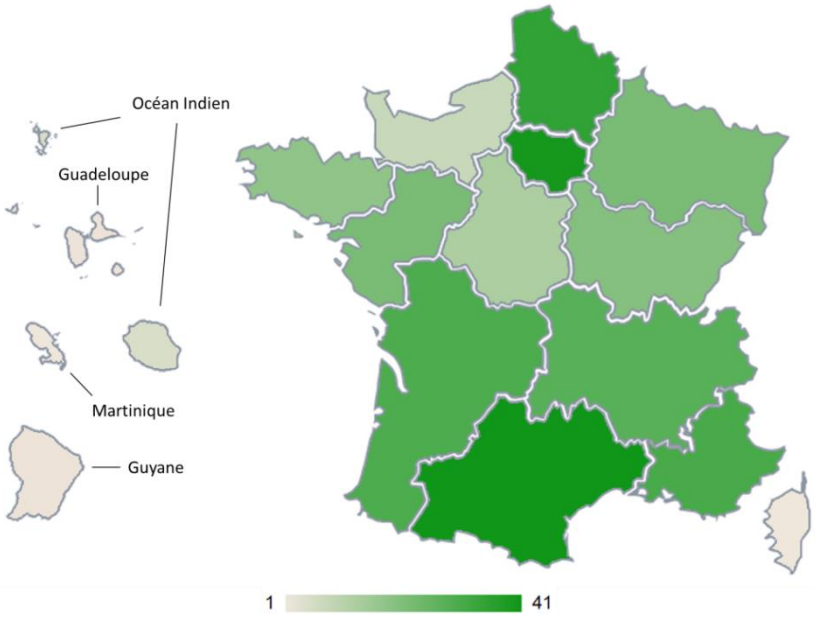


Figure 6 - Répartition des signalements par région

15 % C'est le pourcentage de signalements pour lesquels est demandé un accompagnement de la cellule ACSS. Les accompagnements sont en général demandés lors d'incidents ayant un impact important sur la structure.

La figure 6 présente le ratio entre le nombre de signalement et l'activité hospitalière rapportée au niveau national : plus une région a un nombre de signalement 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 ce ratio le plus élevé (Occitanie) est utilisée en tant qu'indice 100.

Au regard de son activité hospitalière (9% de l'activité nationale presque moitié moins que l'Île-de-France), l'Occitanie est en tête en matière de remontée des incidents. Il est à noter que la région Occitanie a participé activement à la définition et la mise en place du dispositif national de signalement des incidents.

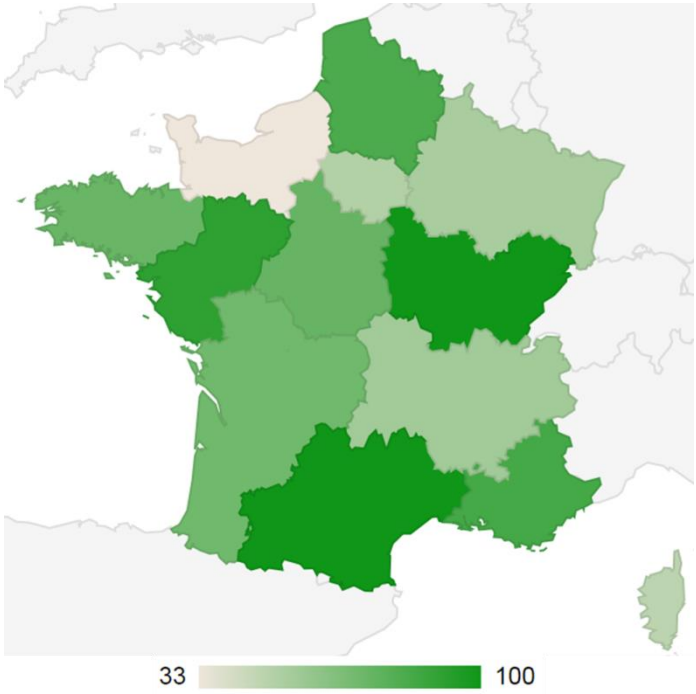


Figure 5 - Nombre de signalements rapporté à l'activité hospitalière des régions

Répartition des signalements selon le type de structure

La majorité des signalements sont déclarés par les établissements de santé. Ceux-ci représentent plus de 86% de la répartition. La catégorie « Autres » correspond principalement à des déclarations réalisées par des EHPAD.

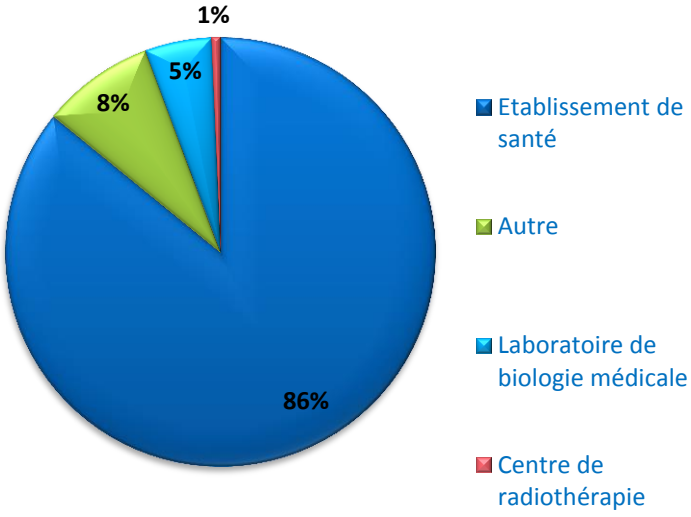
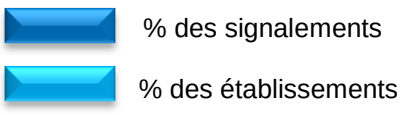


Figure 7 - Répartition des signalements selon le type de structure

Part des signalements comparée à la part des établissements selon leur type

Les établissements publics de santé sont majoritaires dans le paysage hospitalier : ils représentent près de la moitié des établissements de santé. Ce sont eux qui signalent le plus d'incidents : 75% du total.



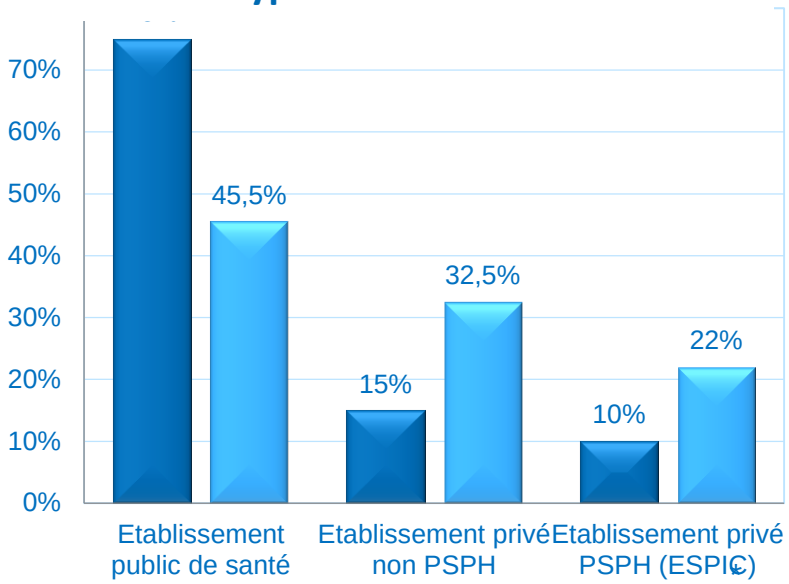


Figure 8 - Part des signalements comparée à la part des établissements selon leur raison sociale

**PSPH : Participant au Service Public Hospitalier / *ESPIC Etablissement de Santé Privé d'Intérêt Collectif*

4.3 Nature des signalements

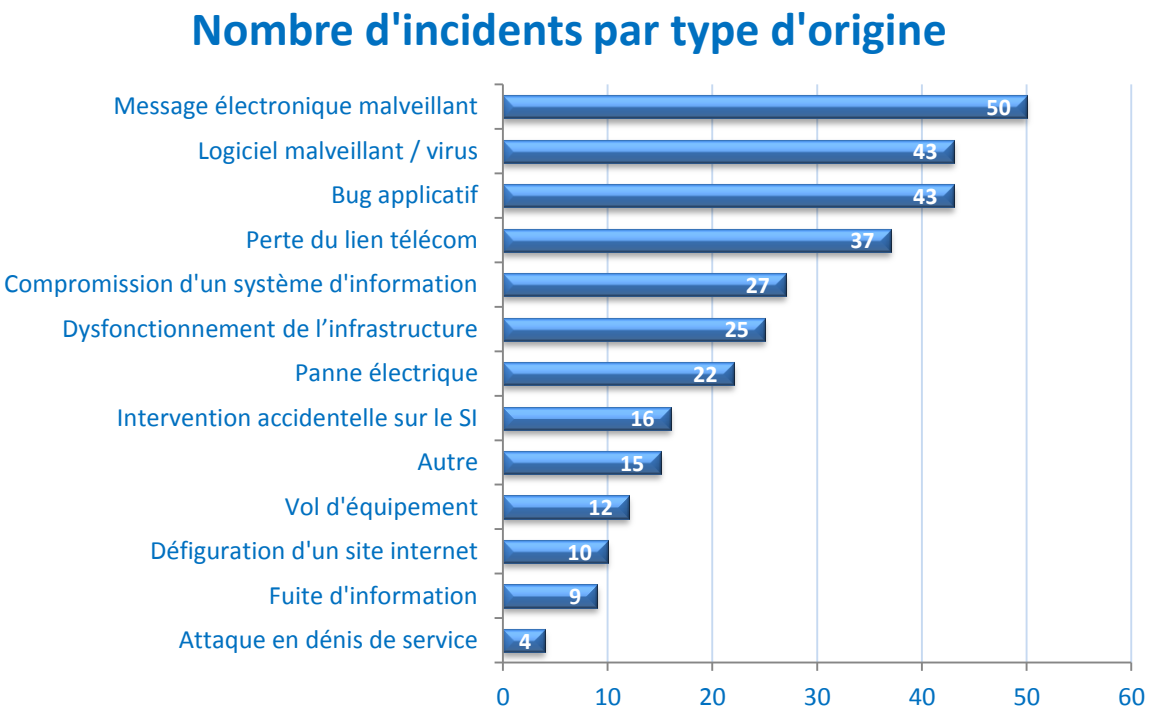


Figure 9 - Nombre d'incidents par type d'origine

La messagerie électronique reste le vecteur le plus important de la menace de cybersécurité dans les structures de santé. Le manque de vigilance ou la méconnaissance des techniques d'attaque permettent à des pirates de récupérer des identifiants de comptes de messagerie ou de déployer des rançongiciels au sein des systèmes d'information des structures de santé. La mise en œuvre de cette attaque a provoqué un grand nombre d'incidents au cours de l'été 2018. Ciblant particulièrement les structures de santé, les pirates ont exploité la compromission de comptes de messagerie de salariés de structures de santé, usurpant leur identité, pour attaquer d'autres structures de santé.

La catégorie « Autre » correspond principalement à des incidents malveillants de divers types, tels que des actes d'ingénierie sociale (tentatives d'escroquerie par téléphone ou par fax) visant à récupérer des informations confidentielles ou facturer des services.

47% C'est le pourcentage des incidents qui ont une origine malveillante, avec comme principaux vecteurs de déclenchement, les messages électroniques malveillants et les logiciels malveillants / virus.

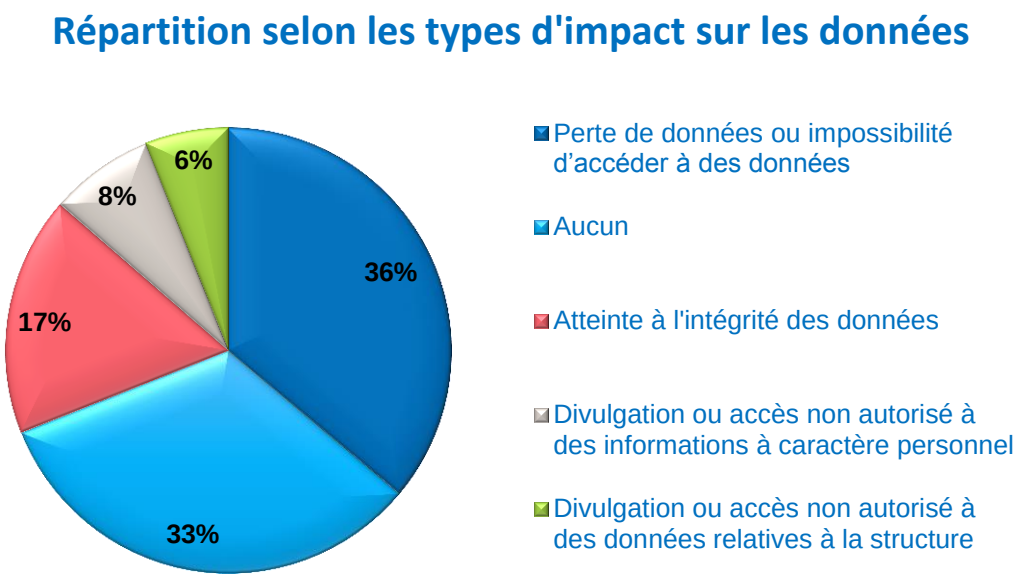


Figure 10 - Répartition selon les types d'impact sur les données

Pour plus d'un tiers des incidents signalés, tout ou partie des données présentes sur le SI de la structure n'étaient plus accessibles. Lorsque l'origine de l'incident est malveillante, ceci est principalement dû à l'activation «accidentelle» d'un cryptovirus qui chiffre les données présentes sur les machines auxquelles il peut accéder au travers du réseau. Ces codes malveillants sont déclenchés soit par l'activation d'un exécutable provenant d'un mail d'hameçonnage, soit par la compromission du système d'information lié à une intrusion d'un attaquant.

Les plus petites structures, celles ne disposant pas d'un service informatique en particulier et devant faire appel à un prestataire spécialisé, sont fortement impactées par cette menace qui peut entrainer une perte d'activité de plusieurs jours, une perte irréversible des données et une mise en danger potentielle des patients.

Lorsqu'une violation de données à caractère personnel a été constatée, la cellule ACSS a rappelé la nécessité de la notifier à la CNIL.

Par ailleurs, pour un autre tiers des signalements, la structure assure qu'il n'y a eu aucun impact.

Les dysfonctionnements des logiciels de prescription/aide à la dispensation liés à des bugs ayant provoqué des erreurs dans les prescriptions et la délivrance des médicaments auraient pu entrainer une mise en danger des patients sans la vigilance des professionnels de santé et la mise en place de procédures de fonctionnement dégradé.

La proportion entre ces incidents malveillants et les incidents non malveillants reste constante jusqu'au mois de juin 2018. Les structures ont particulièrement été touchées les mois de juillet et d'août 2018 par la réception de messages électroniques malveillants. Ceci s'est accompagné d'un accroissement du déploiement de logiciels malveillants sur la même période.

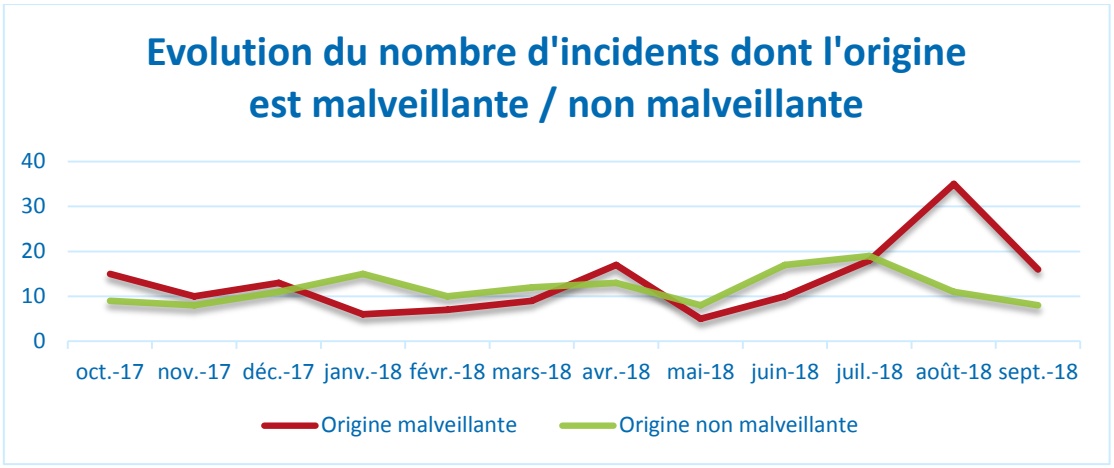


Figure 11 - Evolution du nombre d'incidents dont l'origine est malveillante / non malveillante

49%

C'est le pourcentage de structures qui ont été contraintes à mettre en place un fonctionnement dégradé du système de prise en charge des patients. Celui-ci dépend de la nature de l'incident et des procédures mises en place dans les structures : application du plan de continuité, utilisation du papier pour gérer les patients, mise en place de solutions de contournement pour prendre en compte les dysfonctionnements des logiciels de prescription, etc...

Mise en danger potentielle des patients

Sur les 11% des cas de « Mise en danger patient » potentielle, seuls 3 ont entrainé une mise en danger patient avérée (dose de radioactivité trop importante, administration d'un composant provoquant une allergie, absence de traitement pendant une journée). Ces conséquences sur la prise en charge des patients sont dues à des :

- bugs sur des logiciels de prescription et d'aide à la dispensation impactant l'intégrité des prescriptions et des dispensations ;
- bugs sur des logiciels de dossier patient informatisé ;
- pertes ou des dégradations des liens télécom (voix, données) nuisant à la prise en charge des patients.

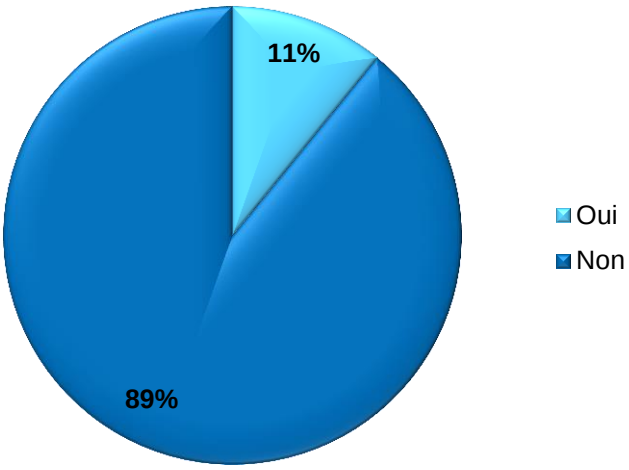


Figure 12 - Mise en danger potentielle des patients

31%

C'est le pourcentage de structures indiquant qu'il n'y a eu aucun impact sur son fonctionnement.

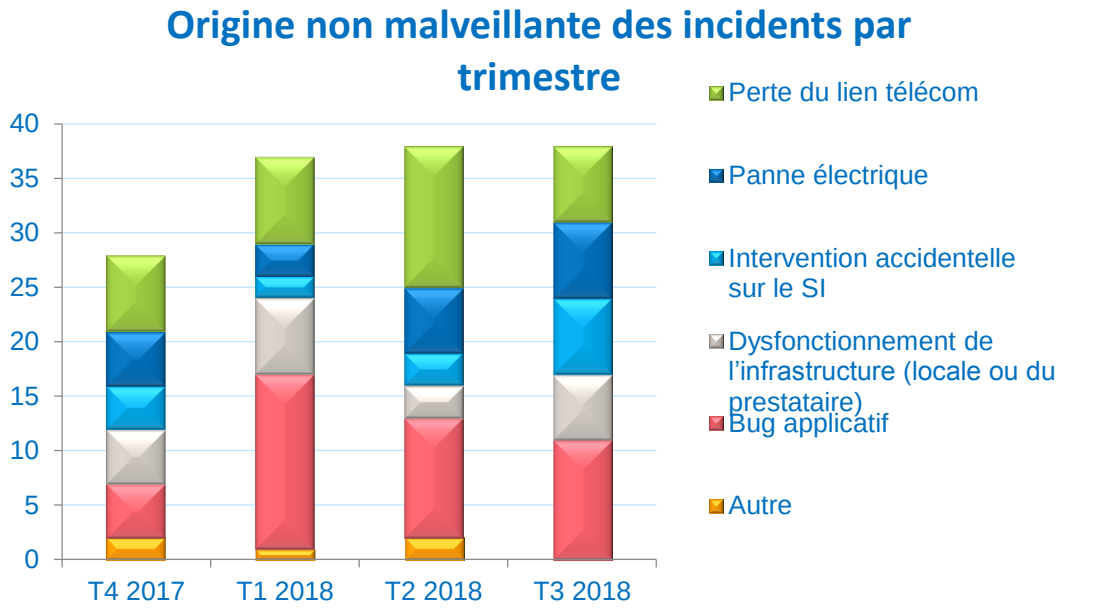


Figure 13 - Origine non malveillante des incidents par trimestre

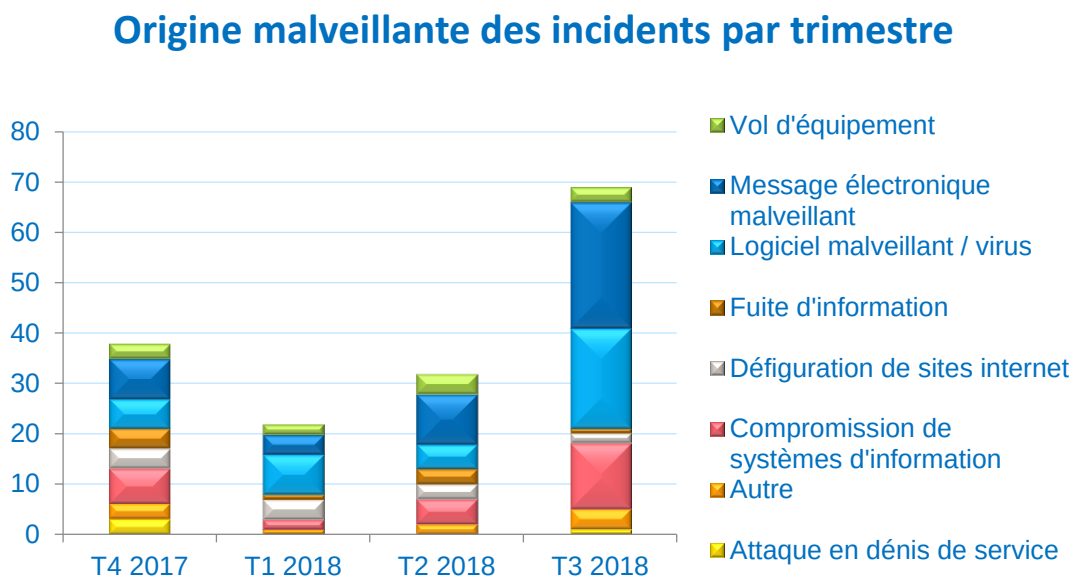


Figure 14 - Origine malveillante des incidents par trimestre

4.4 Incidents notables ayant fait l'objet d'un retour d'expérience anonymisé

Plusieurs incidents déclarés ont fait l'objet d'un retour d'expérience publié sur l'espace sécurisé du portail. Ces retours d'expérience ont permis de faire la lumière sur le mode opératoire de certaines attaques et de présenter les mesures de remédiation à mettre en œuvre en cas d'incident.

Parmi ces incidents, on peut signaler :

- une attaque par rançongiciel qui a contraint un centre de radiothérapie à arrêter son activité pendant deux jours et demi ;
- une intrusion suivie du déploiement de mineurs de crypto-monnaie qui a impacté la disponibilité des applications d'un CH pendant trois mois ;
- une attaque virale par un maliciel de type « wannacry » qui a impacté les activités cliniques, médico-techniques et techniques d'un CH, l'obligeant à délester des urgences vers une autre structure.

Ces incidents ont permis de rappeler l'importance de :

- la sensibilisation des utilisateurs aux messages malveillants et aux tentatives d'hameçonnage ;
- la gestion rigoureuse des mises à jour de sécurité et d'un renforcement des mesures de cloisonnement réseau concernant les SI supports des activités de soins vitaux ;
- la conservation d'un mode de sauvegarde hors-ligne et la réalisation de tests réguliers.

5 GLOSSAIRE

ACSS	Accompagnement Cybersécurité des Structures de 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
ASIP Santé	Agence des Systèmes d'Information Partagée de Santé
CERT	« Computer Emergency Response Team » (CERT - centre d'alerte et de réaction aux cyber-attaques)
CMSI	Chargé de Mission Systèmes d'Information au sein des ARS
CNIL	Commission Nationale de l'Informatique et des Libertés
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
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et Sécurité
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.
RDP	Remote Desktop Protocol – protocole Windows de connexion à distance
RGPD	Règlement Général sur la Protection des Données
RSS	Un flux RSS (RSS est le sigle pour Really Simple Syndication) est un flux au format XML permettant à ses abonnés de récupérer automatiquement une partie (titre ou extrait) ou la totalité d'un article nouvellement créé.

NOTES PERSONNELLES

Pour aller plus loin, rendez-vous sur :

- le site du Ministère des Solidarités et de la Santé : solidarites-sante.gouv.fr
- le site de l'ASIP Santé : esante.gouv.fr
- le portail cyberveille : cyberveille-sante.gouv.fr/

Pour prendre contact :

- au sein du Ministère : ssi@sg.social.gouv.fr
- au sein de l'ASIP Santé : cyberveille@sante.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE CHARGÉ DE LA SANTÉ

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE