AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Présentation de l'activité « Réponse aux incidents de sécurité » du CERT Santé

LA E-SANTÉ FRANÇAISE

Mars 2023

TLP : CLEAR

Qu'est ce qu'un incident de sécurité ?

Un incident de sécurité est une violation intentionnelle et/ou inattendue, portant atteinte à la disponibilité, la confidentialité ou l'intégrité d'une ressource (ex. données de santé, un système d'information) d'une organisation.

Règlementation relative au signalement des incidents de sécurité

- Article L1111-8-2 du Code de la Santé Publique Les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information.
- Le décret n°2022-715 du 27 avril 2022 décrit les conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information.

Qu'est ce que la réponse à incident ?

Dans le cas où le dysfonctionnement d'une ressource a été détectée, l'organisme a la responsabilité de réagir rapidement et de manière efficace.

La réponse à incident est le processus de réaction mis en place par une organisation afin de :

- Gérer l'incident en cours (au niveau opérationnel et technique)
- Limiter les dommages (avec si besoin un confinement)
- Assurer la continuité des activités les plus critiques

Les étapes du processus de réponse à incident

1. Qualification
2. Confinement
3. Investigation
4. Remédiation
5. Durcissement

En fonction du contexte, ces étapes peuvent être réalisées simultanément

Les grandes étapes de la réponse à incident

QUALIFICATION

1

Réaliser une première **évaluation d'un incident** et de ses impacts avérés ou potentiels, et de le partager si nécessaire

CONFINEMENT

2

Partager un ensemble de recommandations pour **isoler une partie du SI** en cas d'incident de cybersécurité

INVESTIGATION

3

Rechercher les origines et les modalités d'une attaque informatique, ainsi que les éléments du SI qui sont compromis

REMEDIATION

4

Mettre en place les premières mesures permettant de sécuriser à nouveau le système d'information afin de bloquer l'attaquant

En fonction du contexte, ces étapes peuvent être réalisées simultanément

DURCISSEMENT

5

Renforcer la sécurité afin d'**être plus résilient face** à la menace cyber existante

Accompagnement optionnel et dépendant du niveau de sécurité du SI

En fonction de la criticité de l'incident et du diagnostic défini, le CERT Santé peut éventuellement accompagner sur la reconstruction du système d'information compromis

Qu’est ce qu’un CERT ?

Parfois l’organisation ne possède pas la maturité cyber ou les ressources en interne pour répondre efficacement face à une attaque.
C'est là que les sapeurs-pompiers de la cybersécurité interviennent : le CERT* ou le CSIRT**

Le CERT est un organisme composé d’experts en sécurité informatique chargés d’intervenir pour apporter un appui technique dans la réponse à incident auprès d’un référent en sécurité (ex. RSSI)

*Le CERT (pour Computer Emergency Response Team) est une marque commerciale enregistrée et déposée par l’Université Carnegie Mellon (États-Unis)
**Appellation pour Computer Security Incident Response Team

Les acteurs potentiels de la réponse à incident

Le signalement des incidents de sécurité des SI est obligatoire depuis le 1er oct. 2017

Acteur(s) privé(s) sous contrat

PRESTATAIRE(S)
Cyber (PRIS*) / Informatique

Bénéficiaires (Etablissements de santé & ESMS)

Acteurs étatiques

CERT Santé

CERT-FR

*appellation pour Prestataires de Réponse aux Incidents de Sécurité

Le CERT Santé ?

Vous êtes :

Etablissement de santé

ou

Etablissement et service médico-social

ou

Centre de radiothérapie

ou

Laboratoire de biologie médicale

Le CERT Santé est l'interlocuteur privilégié auprès duquel déclarer votre incident de sécurité. Les équipes du CERT Santé sont au service de l'écosystème des secteurs de la santé et du médico-social afin d'apporter un appui technique à distance sur les différentes étapes de la réponse à incident, allant même jusqu'à l'accompagnement à la reconstruction du système d'information.

Le signalement des incidents de sécurité des SI est obligatoire depuis le 1er oct. 2017

Les étapes de l'appui à la réponse à incident proposé par le CERT Santé

Le périmètre d'intervention du CERT Santé

1 Qualification

Actions réalisées systématiquement

Prise de contact suite à la déclaration d'un incident afin d'**identifier les risques** et diffusion d'une **alerte vers les autorités compétentes** de l'État selon la nature de l'incident.

2 Confinement

Préconisation de mesures de confinement afin d'**empêcher la propagation de l'activité malveillante**

3 Investigation*

Actions réalisées selon les cas et la criticité des actes de cyber-malveillance

Mise à disposition d'outils de recherche de compromission et d'investigation afin d'analyser les résultats et d'**identifier le scénario de compromission**

4 Remédiation*

Proposition d'un plan d'actions pour **protéger le SI contre une nouvelle attaque** et relancer les services numériques essentiels

5 Durcissement**

Actions réalisées selon les cas et la criticité des actes de cyber-malveillance

Envoi d'un rapport de gestion de l'incident contenant des **recommandations complémentaires pour renforcer le SI** (au-delà de la réponse à incident)

* En fonction du contexte, ces étapes peuvent être réalisées simultanément
** Optionnel - Dépend de la criticité de l'incident

Comment solliciter le CERT Santé en cas d'incident ?

EN HEURES OUVRÉS (HO)

Déclarez votre incident en heures ouvrées (9h-18h du lundi au vendredi) sur le **portail de signalement des évènements sanitaires indésirables** (interface professionnel de santé) - **signalement.social-sante.gouv.fr** - via un formulaire de déclaration.

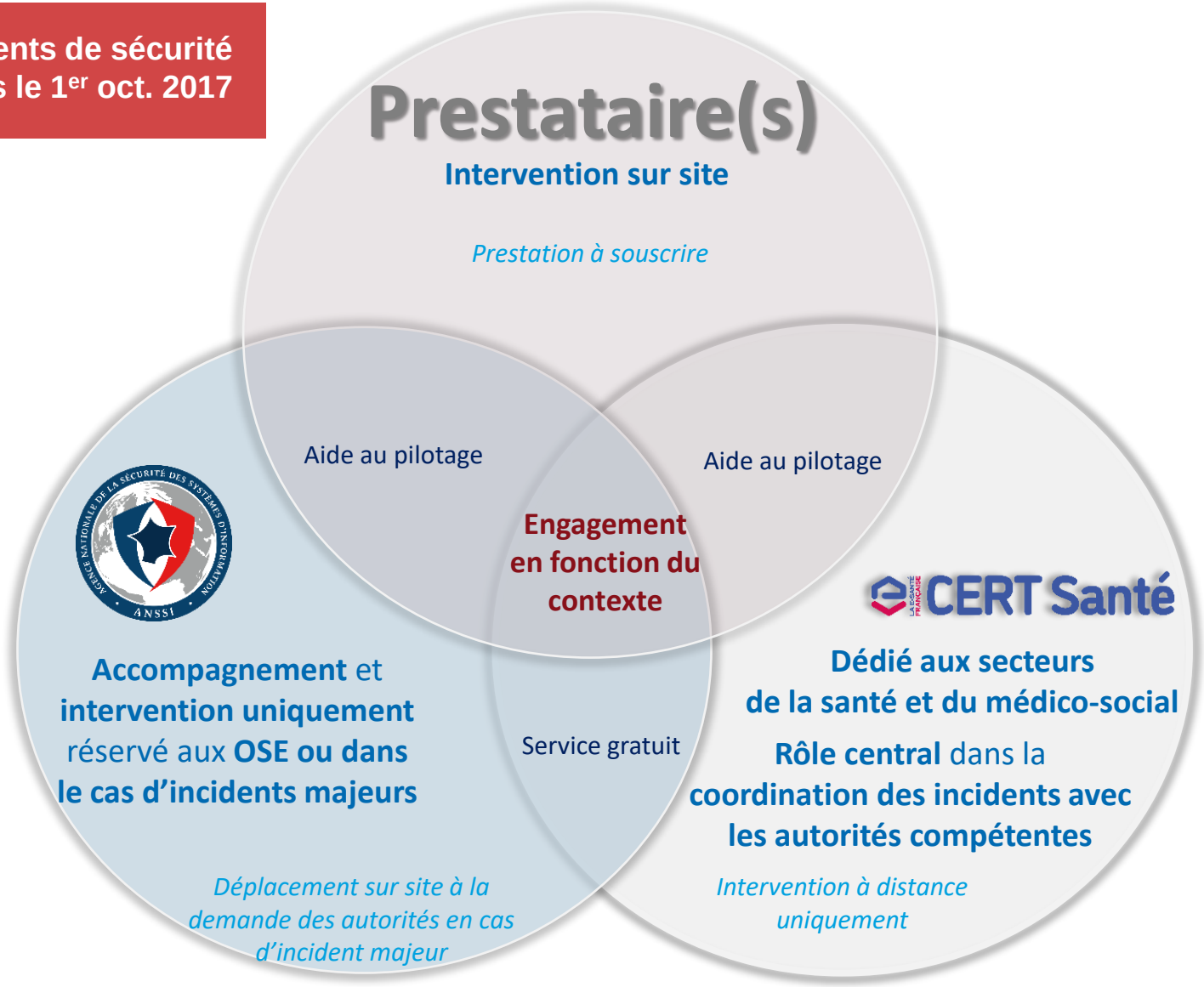
EN HEURES NON OUVRÉS (HNO)

En cas d'incident majeur, contactez le CERT Santé par téléphone au **09 72 43 91 25** ou par mail à l'adresse **cyberveille@esante.gouv.fr**

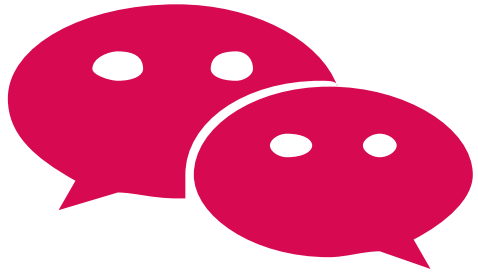
Le CERT Santé **priorise ses interventions** selon la nature de l'établissement et des impacts sur la prise en charge des patients.

Les différents acteurs de la réponse à incident

Le signalement des incidents de sécurité des SI est obligatoire depuis le 1er oct. 2017



Comment nous contacter ?



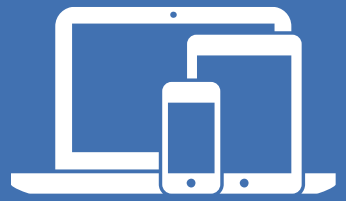
Une question ? Un besoin ?

L'envie de partager et de contribuer au développement du CERT Santé ?

cyberveille@esante.gouv.fr

AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici



esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante

Le CERT-FR ?

Vous êtes un établissement de santé ?
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) est un appui pour le CERT Santé dans la coordination de la réponse à incident.

Vous êtes un OSE* ?
Lorsqu'un incident est qualifié de majeur, le CERT-FR peut de manière exceptionnelle déployer des équipes sur le terrain et accompagner ces structures dans le cadre de la réponse à incident.

Le périmètre d'intervention du CERT-FR

QUALIFICATION › CONFINEMENT › INVESTIGATION › REMEDIATION › DURCISSEMENT

En fonction du contexte, ces étapes peuvent être réalisées simultanément

*appellation pour Opérateur de Service Essentiel

Le PRIS?

Le Prestataire de Réponse aux incidents de Sécurité (PRIS) atteste d'un savoir-faire et de compétences conformes au référentiel établit par l'ANSSI en matière de réponse aux incidents de sécurité.
Le PRIS est soumis à un contrat. Il n'intervient que sur les aspects techniques de la réponse à incident.

Le périmètre d'intervention du PRIS

QUALIFICATION > CONFINEMENT > INVESTIGATION > REMEDIATION

En fonction du contexte, ces étapes peuvent être réalisées simultanément