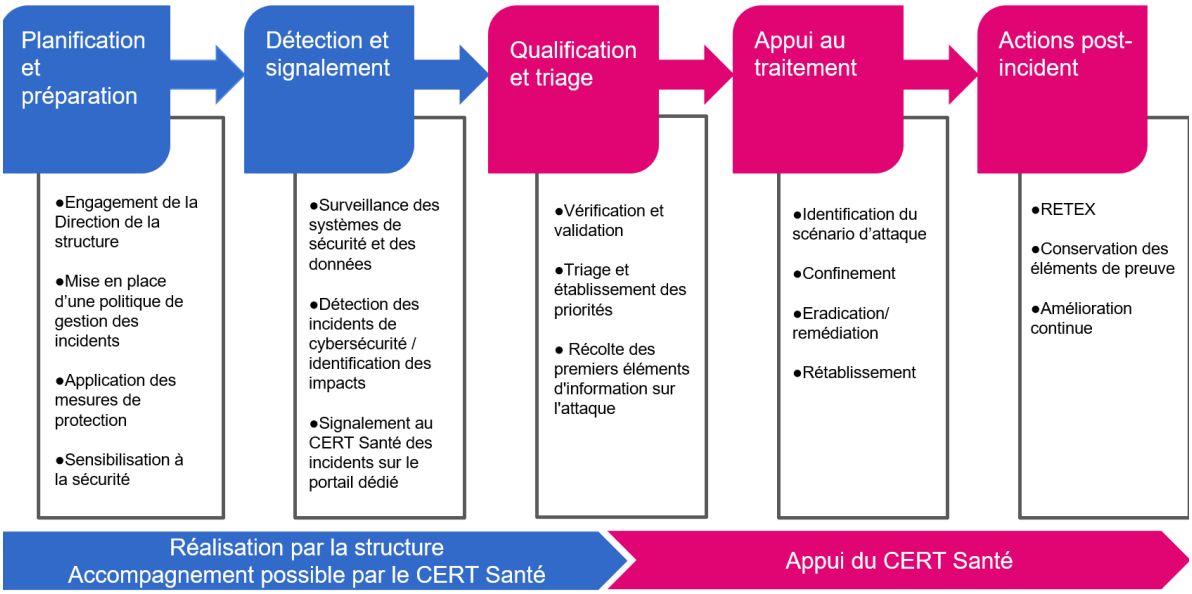
Accompagnement du CERT Santé dans la réponse à incident

Les étapes du processus de réponse à incident



Lors d'une demande d'accompagnement d'une structure, les experts du CERT Santé procèdent à **l'examen technique des causes** de l'incident.

Pour évaluer l'ampleur de l'incident, les **artefacts**[1] ou les **indicateurs** collectés dans le cadre de l'investigation initiale doivent être conservés. Ils peuvent être ensuite utilisés par le CERT Santé pour **identifier le scénario de compromission** et rechercher la présence de compromission sur tous les dispositifs sous la responsabilité de la structure impactée. Les indicateurs de compromission peuvent être partagés sur le MISP[2] de CERT Santé.

Une fois **l'éradication de la menace** achevée et la mise en place de **mesures de remédiation** permettant de se protéger contre une nouvelle attaque, les responsables informatiques de la structure **rétablissent le fonctionnement normal des systèmes** et confirment au CERT Santé que les systèmes fonctionnent normalement.

Lorsque les causes de l'incident et sa gestion peuvent contribuer à améliorer les actions de prévention et la réponse apportée par l'ensemble des structures de santé face à la menace de cybersécurité, le CERT Santé **rédige un RETEX** (Retour d'Expérience) qui sera publié sur l'espace membre du portail cyberveille[3] (dont l'accès est réservé aux seuls membres inscrits). Le RETEX permet aussi d'enrichir la base de connaissances du CERT Santé, de façon à mieux qualifier les incidents et accompagner les structures de santé.

A l'issue d'un incident majeur, il est recommandé de réaliser un **audit de son exposition sur Internet** (audit de cyber-surveillance) ainsi que de son infrastructure interne.

Pendant le traitement d'un incident, toutes les actions et prises de décision doivent être répertoriées dans un **journal de bord** pour être synthétisées ultérieurement dans le bilan de gestion de l'incident, voire un RETEX.

[1] Dans le domaine de l'investigation numérique, le terme Artefact désigne un type de données pouvant fournir des éléments permettant de retracer l'activité d'un système

[2] Malware Information Sharing Platform (CIRCL)

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

Accompagnement du CERT Santé dans la réponse à incident

Etapes de l'appui au traitement proposé par le CERT Santé

1 Prendre connaissance du système d'information et des impacts

Moyen opérationnel privilégié : entretien téléphonique / ou en télé/visioconférence - un CR de l'entretien est envoyé à la structure.

Ce qui est attendu de la structure : *description de son SI, architecture serveurs (SI métiers et support), interconnexions internes et externes, solutions de sécurité mises en place (antivirus, pare feu, proxy, etc, politique d'accès à distance (VPN, RDP) et description des services impactés (DPI, Biologie, radiologie, Biomédical, etc…)*

2 Proposer des mesures de confinement complémentaires

A l'issue de ce premier entretien, le CERT Santé peut proposer des mesures visant à réduire l'impact potentiel de la menace.

Quelques exemples : isolation de l'Active Directory, désactivation massive de comptes, fermeture des services permettant les communications depuis Internet (RDP, Webmail, VPN, ...), déconnexion des sauvegardes, etc.

3 Identifier le scénario complet de l'attaque

Il s'agit de recueillir toute information disponible (artefact) concernant les activités réalisées au cours des périodes précédant et suivant immédiatement l'incident en vue de déterminer l'ampleur et la gravité de l'attaque. Il est primordial de retrouver les indicateurs de compromission.

Moyen opérationnel privilégié : *Acquisition et analyse de journaux d'évènements et de preuves numériques. Le CERT Santé met à disposition de la structure un outil de prélèvement d'artefacts à partir d'un grand volume de données (y compris des données à caractère personnel) extraites des machines potentiellement compromises. La Cellule met également à disposition un scanner qui recherche les indicateurs de compromission sur un parc de machines.*

Ce qui est attendue de la structure : *vérification de l'étendue de la compromission, analyse ou fourniture de logs d'OS, des composants de sécurité (proxy, pare-feu, VPN, antivirus, etc…), courriels malveillants, messages de rançon, vérification de la configuration des composants de sécurité, recherche du « patient 0 » de l'attaque, réalisation d'un scan antiviral du parc …*

4 Proposer des mesures de remédiation

Proposer des mesures pour remédier et **prévenir une nouvelle attaque.**

Quelques exemples : désinfection des systèmes compromis, suppression des fichiers malveillants, correction des vulnérabilités exploitées, modification des mots de passe des comptes potentiellement impactés, filtrage d'URL et d'IP liées à une activité malveillante, etc....

Afin d'éviter une nouvelle compromission, la Cellule est aussi en mesure d'apporter un appui dans la remise en service progressive du SI.

5 Proposer des mesures d'amélioration

Proposer un **plan d'action** permettant à la structure de **renforcer sa résilience face à la cybermenace**

Quelques exemples : durcissement de la politique d'accès à distance au SI et de sa politique de mots de passe, installation/activation de nouvelles protections pour la messagerie (SPF (Sender Policy Framework) et DMARC (Domain-based Message Authentication), pour les environnements Windows (LAPS (Local Administrator Password Solution) et ASR (Automated system recovery)), améliorer les mesures de cloisonnement entre les services, mise en œuvre d'outils permettant de centraliser les logs et de mieux les exploiter, organiser des sensibilisations et communications internes au sujet des cybermenaces et bonnes pratiques à adopter, etc…

VERSION 1.1

04/08/2021