RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION **REMÉDIATION**

CYBERATTAQUES ET REMÉDIATION
LES CLÉS DE DÉCISION

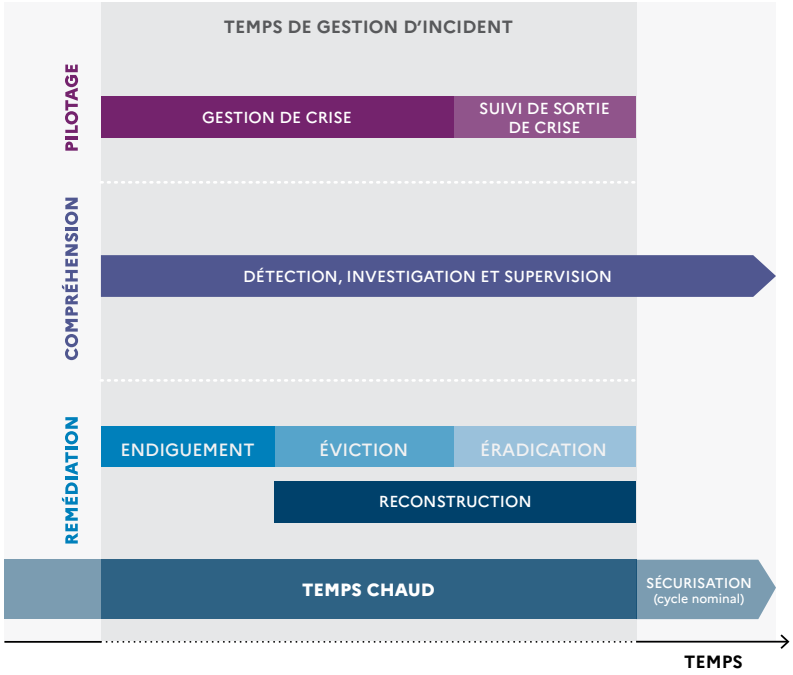
V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

L'ANSSI publie un ensemble de guides sur la remédiation, qui décrit les principes du pilotage et de la mise en œuvre d'une remédiation au sein d'une organisation affectée par un incident de sécurité.

La remédiation est, avec l'investigation, la communication et la gestion de crise, l'une des dimensions majeures de la reprise de contrôle suite à une attaque cyber (atteinte aux activités ou espionnage).

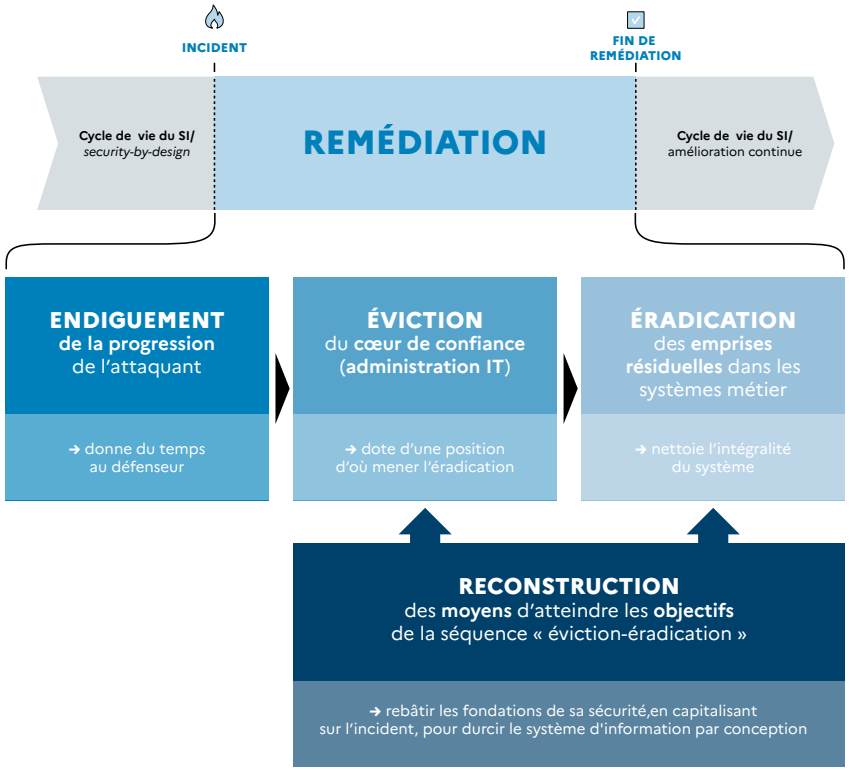
À la suite d'un incident majeur, la remédiation modifie durant plusieurs semaines voire plusieurs mois le cycle de vie du système d'information, et touche durant cette période de nombreux métiers.

Si la remédiation est bien pilotée, l'incident devient une opportunité d'amélioration significative de la résilience de l'organisme qui le subit. Décideurs, déterminez ces objectifs stratégiques et débloquez rapidement les moyens nécessaires.



DÉFINITIONS : LA SÉQUENCE « E3R »

La remédiation peut être séquencée suivant le diagramme « E3R » :



Le cœur de confiance est la brique centrale du système d'information, d'où l'attaquant est exclu de façon certaine et qui est indispensable pour mener les actions de remédiation. Sa reconstruction est une étape majeure. Son échec mène généralement à un cycle de compromission/remédiation qui peut s'étendre sur des mois voire des années.

V.0.0 – APPEL PUBLIC À COMMENTAIRES

BIEN CHOISIR SON PLAN DE REMÉDIATION : UN ENJEU VITAL ?

Les dégâts d'une attaque informatique peuvent se chiffrer en millions, voire en dizaines de millions d'euros. C'est pourquoi les orientations et les moyens donnés au pilotage de la remédiation sont déterminants pour l'avenir d'une organisation touchée.

Ce guide propose trois scénarios à arbitrer en fonction de l'urgence de redémarrage et des coûts induits par les dommages liés à l'attaque à long terme :

Scénario 1 - « Restaurer au plus vite des services vitaux »

Face à un péril immédiat pour votre organisation, un nombre restreint de services doivent impérativement être redémarrés. Toutefois, cette approche ne traitera ni les causes racines de l'incident, ni ne protégera d'une résurgence de l'attaque à moyen terme. La survie de votre organisation reste en question.

Scénario 2 - « Reprendre le contrôle du SI »

Vous privilégiez un retour le plus rapide possible à l'état de fonctionnement antérieur de la totalité du système d'information. Il n'est pas restructuré. Votre organisation reste à risque, tant que des changements substantiels n'auront pas été réalisés (protection de l'administration, détection…).

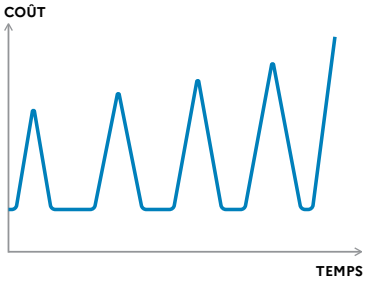
Scénario 3 - « Saisir l'opportunité pour préparer une maîtrise durable du SI »

Quitte à réaliser des changements majeurs dès la remédiation, vous transformez votre posture de sécurité. Vous choisissez d'investir durablement pour vous réapproprier le pilotage et la défense de votre système d'information. Cette approche permet d'adopter un modèle de sécurité proactif, plutôt que réactif.

LES COÛTS DE LA REMÉDIATION

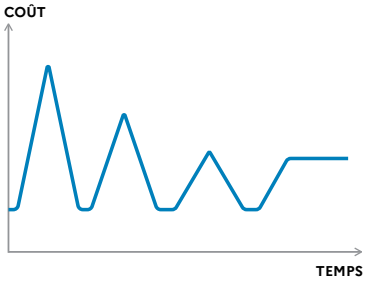
Les investissements réalisés en soutien du plan de remédiation sont déterminants. Ils conditionnent la manière dont l'activité normale va reprendre et dont la gestion de la sécurité sera ensuite assurée. Suivant le scénario choisi, l'étalement des coûts de la remédiation varie sur les moyen et long termes.

Scénario 1



Le redémarrage d'urgence des services vitaux est faiblement coûteux, mais les risques de résurgence sont élevés. D'autres remédiations ultérieures seront alors nécessaires, ce qui génère un coût total très élevé pour l'organisation.

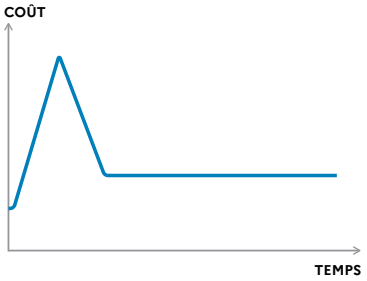
Scénario 2



L'état fonctionnel du SI est ramené à la situation précédant la compromission, dès la première remédiation. Néanmoins, le plan de sécurisation s'étalera sur la durée et aura à nouveau des impacts sur l'activité métier.

V.0.0 – **APPEL PUBLIC À COMMENTAIRES**

Scénario 3



Le coût de la première remédiation est élevé, mais elle constitue une opportunité majeure pour poser les bases d'une sécurité à l'état de l'art. À terme, cet investissement aura été très rentable. L'organisation maîtrise durablement sa sécurité.

SEPT RECOMMANDATIONS POUR RÉUSSIR SA REMÉDIATION

1. Pilotez dans la tempête

Sortez de l'immédiateté : se faire absorber par l'activité à la minute est un gouffre. Les incidents se gèrent en semaines et en mois. Prenez le temps de comprendre, de vous faire expliciter les options pour choisir.

2. Assumez des choix structurants

Tout vouloir traiter conduit à la dispersion des moyens et à l'échec. Seuls des décisions stratégiques fortes, une posture assumée et des engagements financiers concrets dans le traitement d'incident permettent des effets durables.

3. Fixez des objectifs stratégiques centrés sur les métiers

Les objectifs stratégiques que vous devez fixer conditionnent la fin du plan de remédiation, et dépendent de l'un des trois scénarios présentés précédemment. Ces objectifs se mesurent à la capacité des métiers à travailler. Ne vous laissez pas emporter dans les arbitrages de détails techniques, mais assumez la portée de leurs impacts sur l'activité de votre organisme.

4. Restez réactif

Une remédiation se joue contre une intelligence hostile. Les changements adverses peuvent nécessiter des adaptations. La partie ne se termine jamais.

5. Soyez flexible

La réalisation d'un plan de remédiation rencontre des obstacles. Vous devrez adapter les moyens, les priorités et les temporalités, tout en maintenant des objectifs clairs et constants. Adapter les actions en gardant le cap est un des arts majeurs du décideur.

V.0.0 – APPEL PUBLIC
À COMMENTAIRES

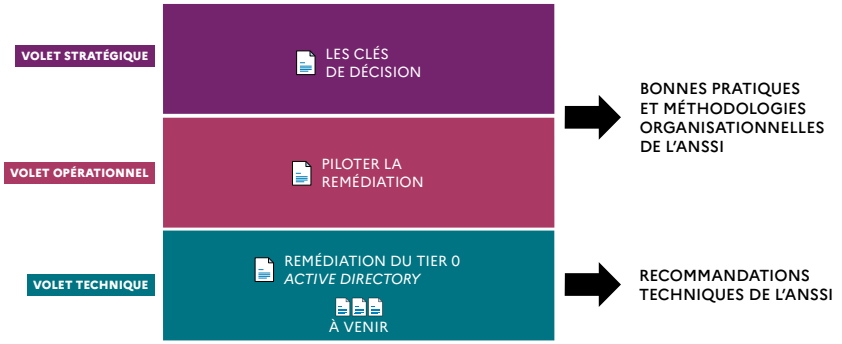
6. Gardez l'œil sur l'humain

Une fois un plan de remédiation lancé, votre rôle est fondamental dans le maintien du cap. Le leadership, la gestion du moral et de la fatigue dans la durée sont cruciaux dans l'exécution du projet.

7. Contemplez un horizon de long terme

Des investissements judicieux pendant la remédiation conditionnent la manière dont l'activité normale va reprendre et dont la gestion de la sécurité va être assurée. Un projet de remédiation réussi n'est pas un substitut à un plan de sécurisation dans la durée, mais il peut améliorer radicalement la gestion des risques cyber par une organisation.

STRUCTURE DU CORPUS DOCUMENTAIRE



POUR ALLER PLUS LOIN

Sur la base des éléments de ce document, vous avez fait le choix d'une option de remédiation. Vous devez désormais orienter vos équipes vers deux types de documentation :

- Les documents opérationnels (voir le volet *Cyberattaques et remédiation, piloter la remédiation*) s'adressent à vos RSSI, DSI et à vos équipes de pilotage de remédiation. Ils vous accompagneront dans la déclinaison des objectifs stratégiques en objectifs techniques. Ces document sont destinés à accompagner le pilotage opérationnel des opérations de remédiation à un incident de sécurité informatique. Ils apportent des outils opérationnels aux responsables des équipes techniques, pour gérer le projet de remédiation et ses intervenants.

- Les documents techniques (voir le volet *Cyberattaques et remédiation, la remédiation du Tier 0 Active Directory*) s'adressent à vos équipes d'exploitation. Ils détaillent les principaux axes de mise en œuvre à prendre en compte lors de la remédiation.

Ces documents accompagnent votre organisation dans les actions techniques à effectuer au cours de la remédiation, pour des technologies spécifiques (Tier 0 Active Directory…).

La remédiation consiste en la reprise de contrôle d'un système d'information compromis. Le volet stratégique, à savoir les orientations et les moyens donnés au pilotage de la remédiation, sont déterminants pour l'avenir d'une organisation touchée. Bien piloté, l'incident subi devient une opportunité d'amélioration significative.

La remédiation est l'une des dimensions majeures de la reprise de contrôle suite à une attaque cyber, avec l'investigation, la communication et la gestion de crise. C'est un travail qui commence dès l'endiguement de l'action adverse et qui peut s'étendre sur plusieurs mois.

Fruit d'une riche expérience dans l'accompagnement d'organisations victimes d'incidents de sécurité, l'ANSSI publie un corpus de guides sur la remédiation, décrivant les principes de son pilotage et de sa bonne mise en œuvre : le volet stratégique, le volet opérationnel et le volet technique.

Ce volet stratégique apportera les clés de décision nécessaires dans la détermination des objectifs et la sélection du plan de remédiation.

Version 0.0 – Avril 2023
Dépot légal : avril 2023
ISBN papier : 978-2-11-167136-2
ISBN numérique : 978-2-11-167137-9

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr