RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

IL FAUT RÉINVENTER LA REMÉDIATION

JSSI 2023

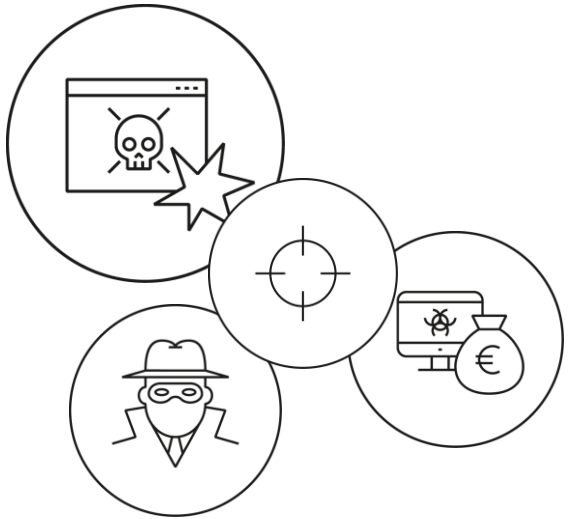
LA REMÉDIATION EN 2023

La remédiation en 2023

La situation

Un incident commence : une détection, une dysfonction, ou même une notification.

- Vous devez organiser la réponse
- Vous ne connaissez pas encore l’ampleur de l’incident
- L’objectif ou les objectifs des attaquants sont inconnus
- Toute la dette technique tombe sur la DSI
- Et, pourtant, vous devez déjà envisager la sortie



La remédiation en 2023

Un témoignage exemplaire

Partage du CH de Dax:

- Février 2021 :
  - Piratage du SI suivi de chiffrement
- Récupération d'un cœur de confiance : 10 jours
  - Avec le support d'OCD et de l'ANSSI
- Remise en production des sauvegardes : 2 à 3 mois
- Après 6 mois
  - Majorité des fonctions restaurées
  - Mais précaires
- Après 1 an
  - Toujours pas de stabilisation complète
  - Certaines fonctions irrécupérables
  - Retard métier considérable à rattraper

https://aime-et-partage.anap.fr/fileadmin/user_upload/page_aime_et_partage/CH_Dax/Cyberattaque-CH-DAX.pdf

La remédiation en 2023

La persistance n’est pas un mythe

- Certains adversaires restent en se sachant détectés
- Et recherchent en permanence de nouveaux accès
- Sur les grands SI retrouver toutes les emprises adverses est une gageure
- La surface exposée de la plupart des organisations est massive

Echouer sa remédiation, c’est l’assurance d’être recompromis.

La remédiation en 2023

Les constats

- L’ampleur des compromissions, voire des destructions sont insupportables
- La reprise de contrôle et la reconstruction sont improvisées.
- Les coûts de rétablissement surpassent toutes prévisions
- Les re-compromissions sont fréquentes.

Il faut faire mieux.

QUI SOMMES NOUS ?

Qui sommes nous ?

Les intervenants

Christophe Renard	Sous-direction opérations, Division Réponse, en charge du pilotage de la remédiation à l'ANSSI
Giacomo Martinelli	Sous-direction expertise, Division Industrie et Technologies, en charge des prestataires de cybersécurité

Qui sommes nous ?

Politique industrielle : les objectifs de l'agence

« Concevoir, développer et mettre en œuvre
la politique industrielle et technologique de l'agence. »

Connaître

- ✓ Maintenir la connaissance de l'offre privée, des technologies et de l'innovation, et identifier les sujets d'intérêt.
- ✓ Comprendre le marché et les besoins de sécurité.

Orienter

- ✓ Proposer et planifier la politique industrielle de l'agence et les priorités de développement technologique.
- ✓ Contribuer à l'influence française auprès des institutions européennes et en normalisation.

Intervenir

- ✓ Travailler avec l'industrie du numérique sur les enjeux de sécurité.
- ✓ Promouvoir les positions de l'agence dans les relations avec l'écosystème.

Qui sommes nous ?

Traitement d'incidents à l'ANSSI

- **CERT-FR / Sous Direction Opérations**
  - Une activité constante
    - ~1000 incidents suivis par an
    - Une vingtaine d'opérations
  - Victimes allant de l'OIV
    - À la PME sensible
    - En passant par les ministères
  - Majoritairement de l'espionnage
    - Mais aussi de la cybercriminalité
    - Et tous les incidents hors normes
  - Un acteur intégré à l'écosystème
    - En suivi sur la plupart des incidents
    - Traitement par des PRIS ou équivalents
    - Et toujours en collaboration avec les victimes et leurs sous-traitants

POURQUOI RÉINVENTER LA REMÉDIATION ?

Pourquoi réinventer la remédiation ?

De quoi parle-t-on ?

Remédier

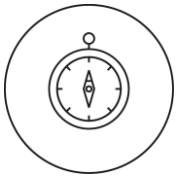
Emprunté au latin *remediare*, « guérir » et *remedium*, « remède, médicament. Au figuré: « préservatif, expédient ». Dérivé de *mederi* « soigner, corriger, traiter par des remèdes appropriés ».

- **1174** « ce qui est employé pour supprimer ou guérir un mal quelconque » (Garnier de Pont-Sainte-Maxence)
- **1281** « porter remède » (Règlement de l'Echevinage d'Amin pour la corporation des bouchers).
- **1355** « combattre un mal quelconque » (Besuire, Tite-Live)

Pour nous:

- Projet de reprise de contrôle d'un système d'information compromis.
- Séquence d'actions qui mène d'un état subi vers un état désiré.
- Un travail qui commence dès l'endiguement de l'action adverse et qui peut s'étendre sur plusieurs mois.

Pourquoi réinventer la remédiation ?



Objectifs de la remédiation

Assurer la survie de l'organisation

- En rétablissant les fonctions métiers essentielles
- En suivant des priorités stratégiques
- Avec le moins de perte possible en service, en données
- En protégeant employés, clients et partenaires

Reprendre le contrôle du SI

- En évinçant l'adversaire d'un cœur de confiance
- En s'assurant que ses emprises soient nettoyées
- En diminuant ses possibilités de retour
- En gardant les futurs incidents sous contrôle

Retourner à la normale

- Pour que les métiers puissent travailler
- Pour que la DSI reprenne ses projets
- Pour que les clients et partenaires aient confiance

Les priorités et les choix stratégiques varient
➔ il faut un cadre, pas une liste d'action fermée.

La doctrine

L'existant

- ISO-27035 – réponse aux incidents
  - chapitre 11 : *Incident containment, eradication and recovery opérations*
  - Quelques suggestions d'actions concrètes mais pas de stratégie
- ISO 22301 – continuité
  - Trop haut niveau pour guider les actions techniques
- ISO-27031 – préparation du SI à la continuité
  - Centré sur la préparation
- NIST SP 8000-61 rev 2
  - 3.3 : *containment eradication and recovery*
  - Peu de détails, si ce n'est l'admonission à phaser
- FIRST CSIRT Service Framework
  - *6.4 Mitigation and recovery*
  - Plus d'idées sur la structure

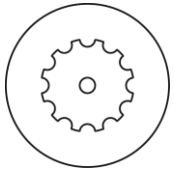
La littérature sur la résilience insiste sur la préparation plutôt que l'exécution

La doctrine

Conséquences du manque de doctrine

- Improvisation de plans
  - Manque de systématisme
  - Pilotage par les moyens plutôt que les objectifs
- Éparpillement des objectifs
  - Concentration sur des objectifs inadéquats
  - En particulier autour de ce qu'on sait faire
  - Plutôt que ce qui est nécessaire
  - Optimisme excessif sur la faisabilité
- Objectifs inflexibles
  - Les blocages ne remontent pas
  - Manque d'arbitrage
- Défaut de pilotage technique
  - La synchronisation se fait de façon *ad hoc*
  - Les choix techniques sont arbitrés aléatoirement

La doctrine



Conséquence du manque de méthode

- Recherche de solutions miracle

  « On déploie un EDR et c'est résolu non ? »

- Défaut de validation métier des restauration de service

  « Si c'est vert dans Nagios, ça marche ! »

- Manque d'anticipation sur les actions de restauration

  « Il suffit de tout restaurer sur un NAS et ensuite on déplace les 30To vers le SAN dans la journée »
  « Les données sont restaurées, la base va redémarrer ! »

- Problèmes de resynchronisation entre le restauré et le transitoire

  « On a tout dans le cloud, ça va repartir tout seul ! »

  - « C'est normal les listes de comptes et mots de passe sur le partage O365 ? »

- Oubli d'actions

  « Qui était chargé de changer les mots de passe sur l'hyperviseur déjà ? »
  « Pourquoi la synchronisation des DC se fait pas ? Qui a bloqué les RPC sur le pare-feu ? »

- Le savoir faire part avec les intervenants externes

  « Comment on accède à …. maintenant ? »

L’expertise en remédiation

Rôle des intervenants en réponse à incidents

Lors d’un incident de sécurité, plusieurs acteurs externes peuvent intervenir

Les prestataires PRIS	Prestations en investigation qualifiées par l’ANSSI (recherche d’indicateurs de compromission, investigations sur périmètre restreint et large périmètre)
Les prestataires de conseil en gestion de crise	Accompagnement à l’organisation des cellules de crise, communication de crise coordination des différents chantiers (réponse à incident, reprise d’activité…), gestion des relations avec les institutions, gestion des moyens RH/logistiques/financiers…
Les prestataires d’administration système	Accompagnement à la construction du SI et du réseau, infogérance, configuration des composants du SI
Les prestataires spécialisés sur des actions techniques particulières	Prestataires ou fournisseurs de solutions en gestion des identités, en restauration de données perdues

L’expertise en remédiation

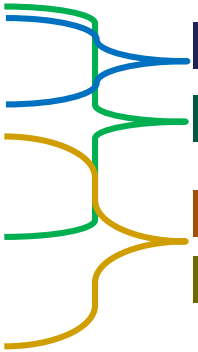
Etat de l’offre actuelle

Les acteurs de la réponse incident se positionnent déjà sur la remédiation…

Offre en appui au pilotage de la remédiation

Aide à la reconstruction du SI en environnement compromis

Aide à l’exécution d’actions techniques spécifiques : nettoyage et reconstruction du Tier 0 AD, restauration de données,…



Prestataires de conseil en gestion de crise

Prestataires PRIS

Prestataires d’administration système

Prestataires spécialisés

…mais il existe peu d’acteurs en mesure d’offrir un accompagnement sur toutes les dimensions de la remédiation

Pratiques peu unifiées

Offre dispersée

Niveau d’expertise et vocabulaires peu homogènes

L’expertise en remédiation

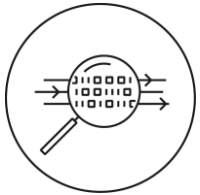
Conséquences des confusions sur les intervenants

Les rôles et acteurs ne sont pas clairement identifiés

- Il en résulte une confusion dans les traitements
- Certaines fonctions ne sont pas tenues
- Les actions ne sont pas suffisamment coordonnées
- Absence de visibilité sur les prestations à commander

Impacts	
	• **Inefficacité**
	• **Improvisation**
	• **Démoralisation**

L'expertise en remédiation



Conséquences de la non reconnaissance d'un domaine d'expertise

- Sous-estimation de la complexité
  - *« Il n'y a qu'à réinstaller les Citrix, qu'on avait mis 3 mois à faire marcher… »*
  - *« Habituellement on met 3 jours, là avec un peu d'effort on devrait avoir terminé dans la journée… »*
- Problèmes de sécurité opérationnelle
  - *« Oui, je me connecte à l'appel vidéo depuis mon poste sur le SI compromis… »*
  - *« On vous a mis tous les mots de passe dans un Excel sur le partage de fichier… »*
  - *« …On stocke tout dans le cloud, c'est safe…Oui c'est authentifié sur l'ADFS... »*
- Sous-estimation de l'attaquant
  - *« Mon antivirus a supprimé plein de webshells sur mon OWA dans la journée, ça reste sous contrôle… »*
  - *« On a désactivé le compte compromis, fin de l'incident… »*
  - *« L'antivirus a effacé le Mimikatz sur le contrôleur de domaine, donc pas d'impact sur l'AD… »*
  - *« L'application est sous Linux, au moins elle est protégée… »*
- Solutions aux conséquences hasardeuses
  - *« Il suffit d'installer un nouvel AD, et d'y réimporter tous les utilisateurs avec les mêmes noms… »*
  - *« Pas besoin de faire une recherche de compromission, on va restaurer les machines à une date antérieure aux premières activités… »*
  - *« On a éteint toutes les VMs juste avant le chiffrement, on a juste à les redémarrer en même temps…*

TRAVAUX DE L’ANSSI

Travaux de l’ANSSI

Dispositif

Un groupe de travail au sein de l’ANSSI	Mobilisation de l’intégralité des experts de l’ANSSI sur toutes les dimensions de la remédiation (pilotage, actions techniques) et de traitement de l’incident (investigation, gestion de crise, sortie de remédiation et amélioration continue)
Un travail ambitieux	Chantier de plus de deux ans, depuis les premiers travaux de diagnostic et de RETEX opérationnel
Un regard tourné vers l’écosystème	Une volonté de ne pas être « hors sol » ni endogène : consultations/enquêtes prospectives de l’écosystème, échanges réguliers sur les pratiques et les offres existantes

Travaux de l'ANSSI

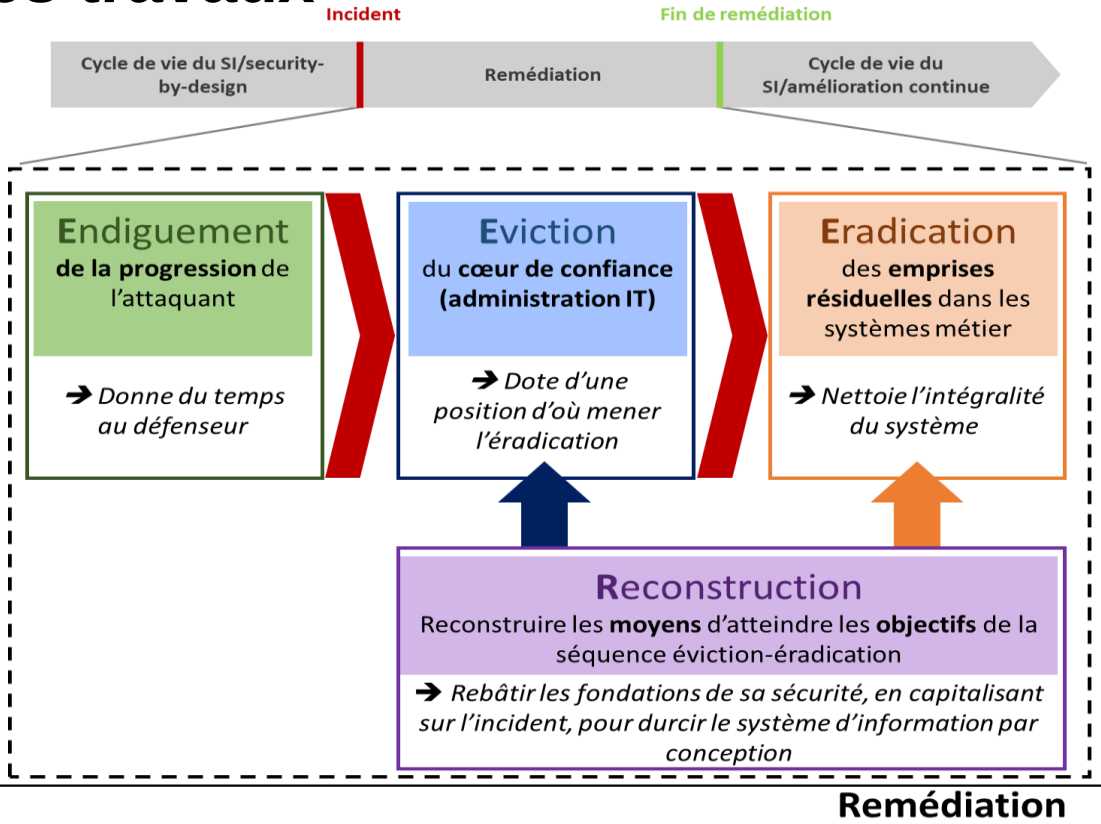
Conclusions

Les réflexions et les constats réalisés ont fait émerger une première étape : <u>partager la vision ANSSI sur les bases de la remédiation</u>

Objectifs :	Faire émerger un écosystème en remédiation	Rendre plus lisibles les offres	Construire les bases d'un langage commun	Rendre plus homogènes les pratiques et les interventions

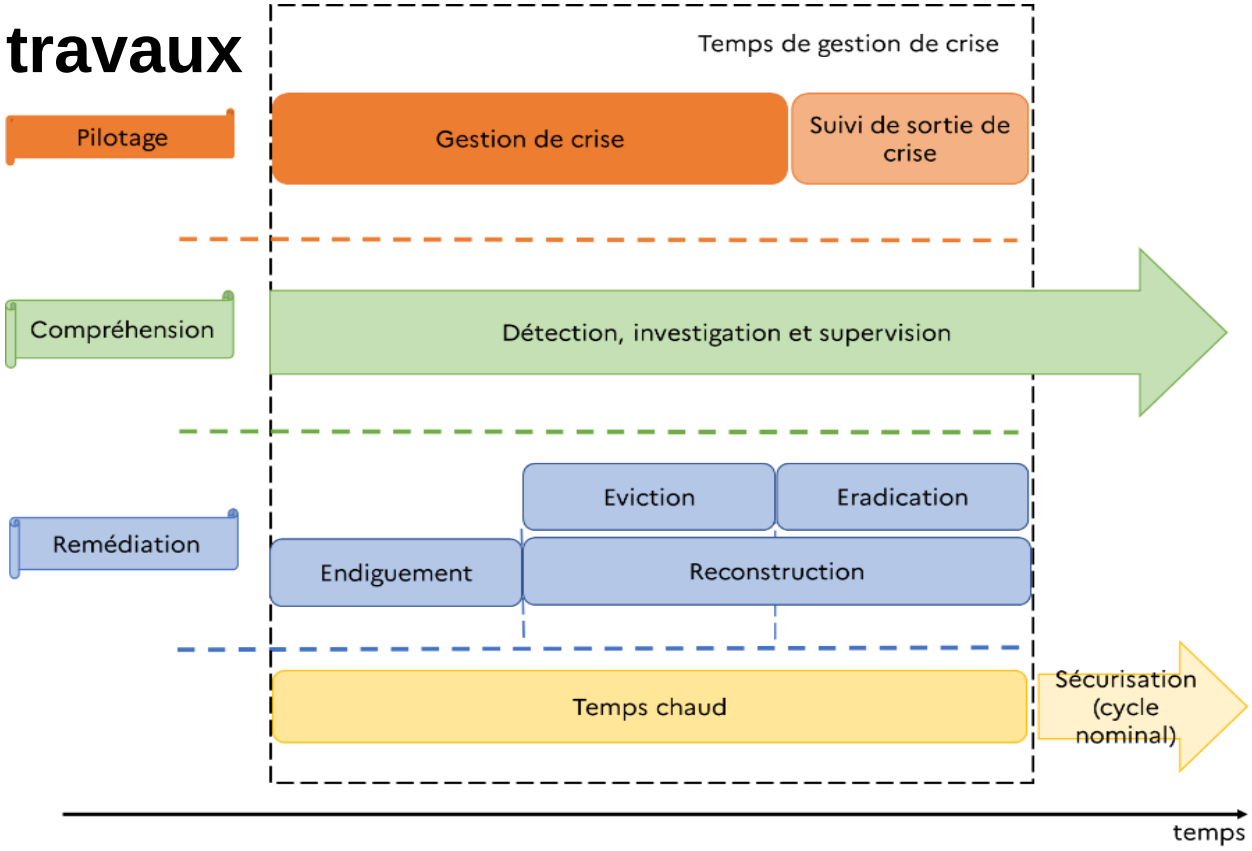
Conclusions des travaux

Le cycle E3R



Conclusion des travaux

Temps de la remédiation



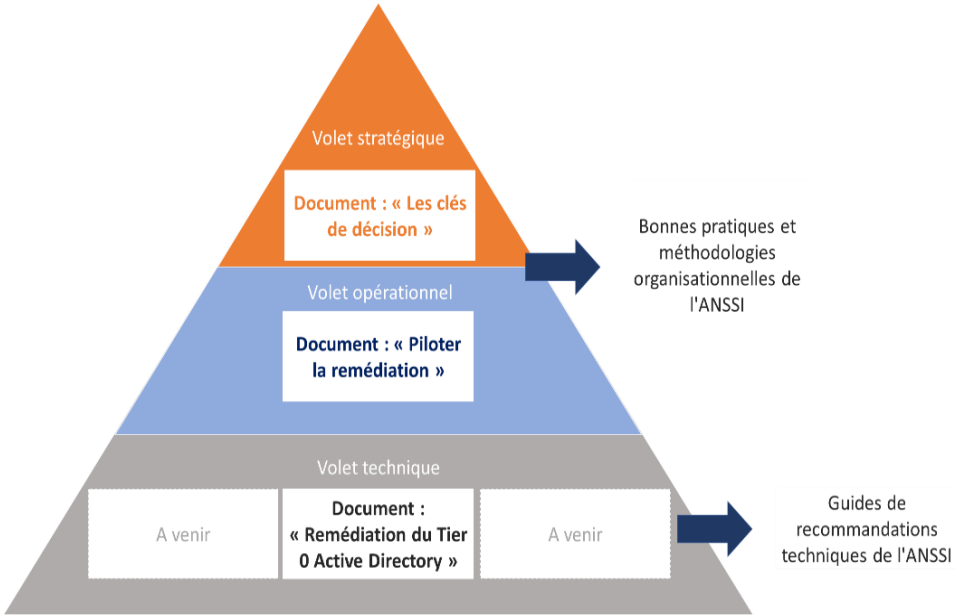
Corpus remédiation

Besoin d'initier un corpus

Sensibiliser les décideurs	La remédiation est une notion à fort enjeu, qui nécessite l'implication du décideur (arbitrages de haut niveau)
Poser le vocabulaire et les concepts clés	Fixer par écrit les bases doctrinales, pour orienter les acteurs de la remédiation, sans brider leur créativité
Donner un cadre aux opérations et actions techniques de remédiation	Doter les intervenants dans la remédiation d'un support concret d'où partir, avant et éventuellement pendant les opérations
Compléter et rendre plus cohérente l'architecture de publications ANSSI existantes	Une publication qui s'insère en cohérence par rapport aux autres publications liées à la réponse à incident : guides sur la gestion de crise, guides techniques de doctrine sécurisation

Corpus remédiation

3 familles de documents



- ***Cible*** : dirigeants et COMEX
- ***Objectif*** : définir et contextualiser la remédiation, expliciter les arbitrages à réaliser

- ***Cible*** : pilotes opérationnels dans la remédiation (prestataires, en interne…)
- ***Objectif*** *: tracer une méthode de gestion des actions, expliciter des scénarios-types rencontrés*

- ***Cible*** : exécutants techniques de la remédiation
- ***Objectif*** : cahier des charges synthétique des principales actions techniques à réaliser

Corpus remédiation

Le futur

Prolonger les travaux actuels :

Publier de nouveaux documents **techniques**

Compléter le volet **opérationnel** : fiches, livres blancs sur des cas d'applications/technologies spécifiques…

Intégrer de nouvelles publications au corpus, **sur la base des retours de l'écosystème**

Travaux de l’ANSSI

Les autres travaux

Actuellement en cours de réflexion :

Communiquer, expliquer, faire de la pédagogie sur les hypothèses et les conclusions des guides ANSSI

Initier une animation d’une communauté d’offreurs autour des thématiques de la remédiation

Valoriser les piliers doctrinaux des guides ANSSI à l’échelle nationale et internationale

LA SUITE

La suite

Accompagner le développement des compétences

Horizon à plus long terme : approfondir la montée en compétences

Projets d'accompagnement à la montée en maturité de l'écosystème

Réflexions sur les enjeux normatifs ou réglementaires

La suite

La suite dépend aussi de vous

L'écosystème doit se saisir de ces guides	Participer à la communauté de la remédiation	Faire émerger une offre de haut niveau en remédiation
• Un **échange** doit se créer sur ces guides : leur contenu n'est pas figé • L'objectif est de recevoir les **retours de l'écosystème**	• Participer aux **enceintes** qui pourront être créées pour échanger sur la structuration des prestations en remédiation • S'impliquer dans les réflexions sur les prochaines **productions** de l'ANSSI	• S'inspirer des **piliers et du langage** des guides ANSSI pour créer de nouvelles offres • Proposer des **prestations matures et plus globales** en remédiation

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

POUR EN SAVOIR PLUS :

- Sujets industriels (DIT) : industries@ssi.gouv.fr
- Sujets opérationnels : https://cert.ssi.gouv.fr

Nous recrutons pour avancer la remédiation !
https://talents.ssi.gouv.fr/offresdemploi/charge-de-mission-remediation-f-h