Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Compromission d'un compte de messagerie

Qualification

InterCERT FRANCE

A qui s'adresse-t-elle ?

- Responsables de la sécurité des systèmes d'information (RSSI)
- Administrateurs du système d'information

Quand l'utiliser ?

Utiliser cette fiche lorsqu'une compromission de compte de messagerie est suspectée.

A quoi sert-elle ?

L'objectif de cette fiche est de proposer une *aide à la qualification* d'un signalement de compromission de compte de messagerie. Les différentes actions proposées aideront à :

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'un ou plusieurs comptes de messagerie sont compromis,
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

Comment l'utiliser ?

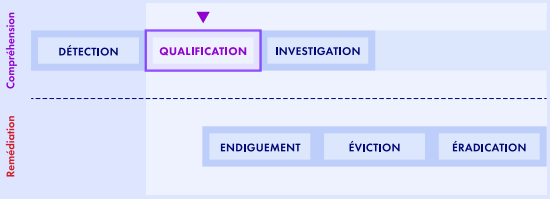
Deux parties principales composent cette fiche :

- La partie Conclusions attendues de la qualification correspond aux questions auxquelles la qualification devra répondre.
- La partie Méthode d'évaluation pas à pas correspond à la méthodologie pour aider à y répondre.

Cette fiche doit être exécutée en *temps court*. Pour cela, fixer un *temps contraint* (selon l'urgence pressentie) et ne pas rechercher l'exhaustivité des réponses : des *réponses approximatives* et des réponses *"je ne sais pas répondre"* sont acceptables dans un premier temps. Par la suite, une qualification plus approfondie se fera sûrement, avec plus de recul ou l'appui d'une équipe spécialisée en réponse à incident.

Retour au début

SOMMAIRE



PRÉREQUIS

Disposer des personnes nécessaires

S'assurer que les personnes qui effectueront la qualification de l'incident aient les accès nécessaires au système d'information :

- Les *accès à l'administration et au monitoring* du système d'information
- Les *accès aux équipements de sécurité* du système d'information
- La connaissance des *priorités métier* de l'organisation
- L'annuaire de contacts d'urgence

Ces personnes peuvent être internes ou externes à l'organisation. Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.

Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer toutes les actions et événements survenus sur le système d'information dans un *ordre chronologique*.
Chaque ligne de ce document doit représenter une action avec au minimum trois informations :

1. La **date et l'heure** de l'action ou de l'évènement (si estimé nécessaire, ajouter le fuseau horaire UTC).
2. Le **nom de la personne** en charge de cette action ou ayant informé sur l'évènement (ou le nom du service de sécurité ayant détecté l'évènement).
3. La **description** de l'action ou de l'évènement, incluant les détails de son avancement ainsi que les comptes et machines concernés.

Important : Lorsque l'incident couvre plusieurs fuseaux horaires, il est conseillé de choisir un fuseau pour le traitement de l'incident.
Ce document sera utile pour :

- Réaliser un historique du traitement de l'incident et partager la connaissance
- Piloter la coordination des actions et suivre leur état d'avancement
- Évaluer l'efficacité des actions et leurs potentiels impacts non prévus

Cette main courante doit être modifiable et consultable par tous les intervenants. Il est déconseillé de la stocker sur le système d'information compromis, où elle serait accessible par l'attaquant. En revanche, cette main courante peut être accessible sur un partage de fichiers en ligne (cloud) ou intégrée dans le logiciel de gestion d'incident, ou le SIEM si l'organisation en possède un, voire être au format papier.

Avoir pris connaissance des actions déjà entreprises

Avoir pris note des personnes ayant déjà agi en réponse à l'incident en cours et des actions qu'elles ont déjà entreprises sur le système d'information.
Important : Vous pouvez intégrer ces notes d'intervention dans la main courante, avec une ligne pour chaque action réalisée.

CONCLUSIONS ATTENDUES DE LA QUALIFICATION

Cette partie résume les conclusions auxquelles doivent mener les évaluations, qui aboutiront à la qualification de l'incident.
La partie suivante présentera des actions détaillées pour guider pas à pas ces évaluations.

Évaluer l'incident

Mesure 1 - Identifier le compte suspecté

- ☐ *La nature des informations transmises permet-elle d'identifier de manière fiable le(s) compte(s) suspecté(s) ?*

Mesure 2 - Confirmer le signalement

- ☐ *L'incident de compromission de compte de messagerie est-il confirmé, est-il un faux positif ou nécessite-t-il des investigations complémentaires ?*

Mesure 3 - Évaluer le périmètre de l'incident

- ☐ *L'incident est-il circonscrit à la messagerie ou d'autres accès à l'organisation pourraient-ils être potentiellement compromis ?*
- ☐ *L'utilisateur du compte compromis est-il particulier (utilisateur sensible, compte d'administration, VIP, etc.) ?*
- ☐ *L'accès initial peut-il être détecté (un message d'hameçonnage, une attaque de type force brute, ou un code malveillant de type infostealer ciblant le poste de l'utilisateur) ?*

Mesure 4 - Évaluer l'impact de l'incident

- ☐ *Des activités métiers essentielles sont-elles ou peuvent-elles être perturbées ?*
- ☐ *Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?*

Mesure 5 - Évaluer l'urgence à résoudre l'incident

- ☐ *Si les perturbations potentielles de certaines activités essentielles sont inacceptables, pour quelles activités des mesures préventives de maintien d'activité doivent être envisagées ?*
- ☐ *L'activité malveillante détectée est-elle récente et donc sujette à évolution, ou ancienne et stable ?*
- ☐ *Existe-t-il un risque que l'incident se généralise dans le SI de l'entreprise de manière imminente ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident

- ☐ L'incident de type *compromission d'un compte de messagerie* est-il *confirmé* ?
- ☐ L'incident est-il *circonscrit* sur mon système d'information, ou est-il étendu ?
- ☐ L'incident présente-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ Est-il *urgent* de résoudre l'incident, ou les activités vitales ont-elles pu être maintenues ?
- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?
  - ☐ Anomalie courante
  - ☐ Incident mineur
  - ☐ Incident majeur
  - ☐ Crise cyber

MÉTHODE D'ÉVALUATION PAS À PAS

Cette partie détaillera des actions qui aideront à conduire les évaluations et à aboutir à la qualification de l'incident.

Évaluer l'incident

Mesure 1 - Identifier le compte suspecté

Action 1.a : Évaluer l'origine du signalement de l'incident

- ☐ Signalement :
  - ☐ Réception de mails suspects sur un compte de messagerie de l'organisation
  - ☐ Envoi de mails suspects en provenance d'un compte de l'organisation
  - ☐ Suspicion de l'utilisateur que son compte soit compromis
  - ☐ Notification de la fuite de ses authentifiants (mail/mot de passe et/ou donnée d'authentification à multiples facteurs)
  - ☐ Suspicion de la présence de règles sur la messagerie non créées par l'utilisateur ou par les administrateurs
  - ☐ Changement de mot de passe illégitime
- ☐ Détection :
  - ☐ Détection d'attaques par force brute sur des comptes, suivi d'une authentification réussie
  - ☐ Activité inhabituelle détectée sur des comptes de messagerie
  - ☐ Notification de tentatives de connexion illégitimes

Action 1.b : Identifier le compte concerné

- ☐ Identifier précisément le compte concerné par le signalement
- ☐ S'assurer que l'adresse mail du compte appartienne bien à l'organisation et corresponde à un compte valide

Action 1.c : Identifier des délégations de droit

- ☐ Identifier des délégations de droit d'autres comptes sur cette boîte aux lettres
- ☐ Identifier des délégations de droit de ce compte sur d'autres boîtes aux lettres

> **ATTENTION**
>
> En cas de délégation de droits par un compte compromis, les autres comptes doivent également être considérés compromis.

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

Action 1.d : (Conclure) Confirmer l'identification du compte suspecté

- ☐ La nature des informations transmises permet-elle d'identifier avec sûreté le(s) compte(s) suspecté(s) ?

Mesure 2 - Confirmer le signalement

Cette mesure peut être menée par un entretien avec l'utilisateur affecté, qui pourra être en mesure de valider les événements inhabituels soupçonnés :

Action 2.a : Vérification des courriels du compte

- ☐ Des courriels ont-ils été identifiés dans la boite d'envoi, sans avoir été envoyés par la victime ?
- ☐ Des courriels de réponse ont-ils été reçus, non sollicités par la victime ?
- ☐ Un collaborateur aurait-il reçu un mail de spam de la victime, contenant un historique de conversation légitime ?
- ☐ Des courriels inconnus de la victime sont-ils dans la corbeille de sa boîte de messagerie ?
- ☐ Des courriels indiquant des réinitialisations de mot de passe ou d'appareils de confiance, non sollicités par la victime peuvent-ils être détectés ?
- ☐ Des courriels ont-ils disparu du compte de messagerie, sans action de la victime ?
- ☐ La victime peut-elle encore recevoir des mails ?

Action 2.b : Vérification de la gestion du compte

- ☐ Des règles de gestion illégitimes sont-elles configurées sur la boîte de messagerie du compte :
  - ☐ Règle de *délégations* illégitimes ?
  - ☐ Règle de *transfert automatique* à un compte tiers ?
  - ☐ Règle de suppression et lecture automatique de messages reçus (utilisée pour cacher les retours de mail de personnes contactées durant l'usurpation) ?
  - ☐ Autres règles ?
- ☐ Des actions ont-elles été effectuées à des horaires inhabituels ?
- ☐ Des modifications suspectes de permissions ont-elles êté observées ?
- ☐ De nouveaux comptes utilisateurs suspects ont-ils été créés ?

Action 2.c : Vérification des applications tierces

- ☐ Des *plugins* suspects ont-ils été frauduleusement installés ?
- ☐ Des accès d'applications tierces ont-ils pu être détectés (par exemple *OAuth*) ?

Action 2.d : Vérification de connexions inhabituelles

- ☐ Détection de connexions réussies provenant de localisations, de systèmes inhabituels ?
- ☐ Détection de connexions réussies provenant d'équipements de connexion inhabituels ?
- ☐ Détection de connexions réussies d'adresses IP inhabituelles ?
- ☐ Détection de connexions réussies à des horaires inhabituels ?
- ☐ Détection d'alertes d'échecs de connexion suivies d'une connexion réussie suspecte ?
- ☐ Détection d'erreurs *MFA* ?
- ☐ Détection de l'incohérence de la dernière date de connexion ?

Important : Dès lors **qu'un** ou **plusieurs** de ces évènements sont détectés, vous pouvez légitimement confirmer le signalement et avancer sur la suite des mesures.
L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

Action 2.e : (Conclure) Confirmer la compromission du compte de messagerie

- ☐ *L'incident de compromission de compte de messagerie est-il confirmé, est-il un faux positif ou nécessite-t-il des investigations complémentaires ?*

Mesure 3 - Évaluer le périmètre de l'incident

Action 3.a : Identifier le type de compte affecté

- ☐ Type de compte :
  - ☐ Compte d'utilisateur standard ?
  - ☐ Compte d'utilisateur sensible ?
  - ☐ Compte d'administration ?
  - ☐ Compte fonctionnel ?

Action 3.b : Identifier des accès potentiels du compte compromis en dehors de la messagerie

- ☐ Le compte compromis peut-il se connecter sur d'autres applications de l'organisation, notamment exposées sur Internet ?

- ☐ VPN
- ☐ Partage de fichiers
- ☐ Accès distants
- ☐ Service Cloud
- ☐ Extranet
- ☐ Applications diverses

Important : Vous pouvez constituer une liste des accès tiers potentiellement compromis afin de prioriser la suite de vos investigations.

Action 3.c : Identifier une compromission similaire sur d'autres comptes de messagerie

- ☐ Identification d'indicateurs de compromission identiques sur d'autres comptes de messagerie (même IP de connexion suspecte, mêmes horaires inhabituels, même user-agent, etc.) ?

Action 3.d : Identifier des détections antivirales

- ☐ Détection d'alertes antivirales sur le poste de l'utilisateur victime, notamment de type *info stealer* ?
  - ☐ Ce type d'alerte concerne-t-il d'autres postes ?

Action 3.e : Identifier un courriel suspect

- ☐ Présence de pièces jointes malveillantes dans la boîte de messagerie compromise ?
- ☐ Présence de mails suspects potentiellement liés à l'incident dans la boîte de messagerie compromise ?
  - ☐ Ce type d'alerte concerne-t-il d'autres postes ?

Actions 3.f : Identifier un vol de matériel

- ☐ Du matériel de l'utilisateur dont le compte de messagerie a été compromis aurait-il été volé (téléphone, ordinateur, clé USB, etc.) ?

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

Action 3.h : (Conclure) Évaluer le périmètre de l'incident

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- ☐ *L'incident est-il circonscrit à la messagerie ou d'autres accès à l'organisation sont-ils potentiellement compromis ?*
- ☐ *L'utilisateur du compte compromis est-il particulier (utilisateur sensible, compte d'administration, etc.) ?*
- ☐ *L'accès initial peut-il être détecté (un mail de hameçonnage, une attaque de type force brute, ou un code malveillant de type infostealer ciblant le poste de l'utilisateur) ?*

Important :

- ► Un *hameçonnage* ou autre vol de données n'a pu extraire qu'un seul couple identifiant/mot de passe, mais qui peuvent potentiellement être réutilisables sur d'autres applications ou services en ligne.
- ► Un *infostealer* a pu extraire du navigateur de l'utilisateur compromis non seulement plusieurs couples identifiant/mot de passe, mais également des *jetons de sessions actives.*

Mesure 4 - Évaluer l'impact de l'incident

Action 4.a : Évaluer les impacts d'une exfiltration de données

- ☐ Des données pourraient-elles avoir été exfiltrées ?
- ☐ Ces données seraient-elles relatives à des aspects critiques pour l'entreprise ?

Action 4.b : Évaluer les impacts d'une compromission plus étendue

- ☐ La compromission pourrait-elle avoir donné lieu à un accès à un autre compte ?
- ☐ La compromission pourrait-elle avoir donné lieu à un accès à un autre système ?
- ☐ La compromission pourrait-elle avoir donné lieu à un accès à une autre application ?

Action 4.c : Évaluer les impacts potentiels sur l'activité métier

- ☐ Quelles processus métiers sont concernées par le compte affecté, à usage interne ou externe ?
- ☐ Quelles activités potentiellement perturbées sont vitales pour l'organisation ?
- ☐ Si votre organisation possède un BIA (Business Impact Analysis), ces activités y ont-elles été analysées ?
- ☐ Parmi les activités potentiellement perturbées, certaines provoquent-elles une importante perte financière ?

Important : Cela vous permettra notamment d'identifier en amont les conséquences si ce compte venait à être isolé ou désactivé dans la suite des investigations.

Action 4.d : Évaluer les impacts réglementaires

- ☐ Peut-on savoir si le compte affecté stocke des données sensibles ?
  - ☐ Données classifiées ou sensibles
  - ☐ Données personnelles
  - ☐ Données de santé
  - ☐ Données financières
  - ☐ Données soumises à engagement contractuel ou réglementaire

Action 4.e : (Conclure) Évaluer l'impact potentiel de l'incident

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

- ☐ *Des activités métiers essentielles sont-elles ou peuvent-elles être perturbées ?*
- ☐ *Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?*

Mesure 5 - Évaluer l'urgence à résoudre l'incident

Action 5.a : Évaluer l'urgence métier à résoudre l'incident

Pour chacune des activités vitales impactées identifiées précédemment :

- ☐ Existe-t-il une procédure de continuité d'activité en mode nominal ?
- ☐ Existe-t-il une procédure de maintien d'activité en mode dégradé ?

Action 5.b : Évaluer la récence de l'information signalée

- ☐ Le signalement est-il en lien avec une détection récente ?
- ☐ L'activité détectée est-elle récente, récurrente et/ou ponctuellement détectée dans le passé ?

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

Action 5.c : (Conclure) Évaluer l'urgence à résoudre l'incident

- ☐ *Quelles sont les activités qui pourraient être perturbées suite à la compromission de la boite mail ?*
- ☐ *L'activité détectée est-elle récente et donc sujette à évolution, ou ancienne et stable ?*
- ☐ *L'incident est-il à risque de généralisation imminente ?*

Qualifier l'incident

Conclure quant à la *gravité* que représente l'incident de sécurité pour mon organisation, en prenant en compte le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre :

- ☐ L'incident de type *compromission d'un compte de messagerie* est-il *confirmé* ?
- ☐ L'incident est-il *circonscrit* sur un unique compte de messagerie ou système d'information, ou est-il étendu ?
- ☐ L'incident présente-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ L'incident est-il *urgent* à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

☐ Au final, quelle *gravité* représente cet incident de sécurité ?

- ☐ Anomalie courante
- ☐ Incident mineur
- ☐ Incident majeur
- ☐ Crise cyber

SUITE DES ACTIONS

Si la compromission de compte de messagerie n'a pas pu être confirmée, il reste *conseillé* de forcer un renouvellement du mot de passe et du MFA pour le(s) compte(s) affecté(s) par sécurité.
Si l'incident de compromission de compte de messagerie est confirmé, vous pouvez mettre en place les actions suivantes en cohérence avec le *périmètre de compromission* évalué :

- Mettre en œuvre des **mesures d'endiguement** pour contenir l'attaque.
  - Fiche suivante conseillée : Fiche réflexe - Compromission d'un compte de messagerie - Endiguement

Si un incident de compromission système est suspecté, qualifier précisément cet incident :

- Fiche suivante conseillée : Fiche réflexe - Compromission système - Qualification

Parallèlement, piloter la suite du traitement de cet incident et demander de l'aide pour résoudre l'incident, en cohérence avec les *impacts* identifiés :

- Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident.
  - Voir les annexes *Contacts* et *Déclarations*.

De plus, si l'incident a un *périmètre étendu* sur le système d'information, qu'il a un *impact fort* et qu'il nécessite une *résolution urgente* :

- Activer le dispositif de **gestion de crise cyber** de l'organisation pour piloter la résolution de l'incident et la continuité d'activité.
  - Guide conseillé : Crise cyber, les clés d'une gestion opérationnelle et stratégique

ANNEXES

Liens utiles

Lors d'une lecture préparatoire de cette fiche ou pour aller plus loin dans la compréhension et la mise en œuvre des notions évoquées, certains documents annexes peuvent être utiles :

- Fiche réflexe - Compromission d'un compte de messagerie - Endiguement
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation

Définitions

Axes d'évaluation

- *Périmètre* : Le périmètre d'un incident désigne son étendue sur le système d'information et dans son administration.
- *Impact* : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- *Urgence* : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Compromission d'un compte de messagerie

Une *compromission d'un compte de messagerie* désigne un accès non autorisé à un compte de messagerie, par un attaquant. Ce dernier peut alors lire et envoyer des courriels à l'insu de l'utilisateur légitime du compte, et accéder à ses données.

Compromission système

Une *compromission système* est l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information, résultant en sa prise de contrôle.

Faute de pouvoir qualifier précisément la prise de contrôle, dans de nombreux cas, toute activité adverse sur le système pouvant avoir donné lieu à une escalade de privilège est considérée comme une compromission. Une compromission entraîne généralement une forme de communication entre la machine compromise et un attaquant y exécutant des actions.

Degrés de gravité

- *Anomalie courante* (gravité faible) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- *Incident mineur* (gravité modérée) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.
- *Incident majeur* (gravité élevée) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- *Crise cyber* (gravité critique) : Une crise cyber représente un incident de sécurité ayant un *périmètre étendu* sur le système d'information, un *impact fort* sur l'activité métier et nécessitant une *résolution urgente*.

Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

Fuite de données

Une *fuite de données*, également appelée *violation de données*, désigne un incident au cours duquel des informations confidentielles, sensibles ou protégées sont consultées, divulguées ou volées par une personne non autorisée. Cela peut concerner divers types de données, notamment des informations personnelles, financières, médicales, ou des secrets commerciaux.
Les fuites de données peuvent résulter de cyberattaques, comme le piratage ou le phishing, mais aussi d'erreurs humaines, telles que l'envoi d'informations à la mauvaise adresse e-mail ou la perte de dispositifs contenant des données sensibles. Les conséquences d'une fuite de données peuvent être graves, allant de pertes financières et d'atteintes à la réputation de l'entreprise à des problèmes juridiques et à la compromission de la vie privée des individus concernés.

Qualifier un incident

Qualifier un incident signifie :

- *Confirmer* qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.
- *Évaluer la gravité/priorité de l'incident* en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les organisation disposant d'une équipe de réponse à incident interne.
CERT/CSIRT externe en prestation de réponse à incident	`https://www.cybermalveillance.gouv.fr/diagnostic/accueil` `https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris`	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CSIRT régional	`https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux`	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations
CERT sectoriel	`https://www.cert-aviation.frhttps://www.m-cert.frhttps://esante.gouv.fr/produits-services/cert-sante`	Pour les organisations du secteur de l'aviation, maritime ou santé
CERT-FR	`https://www.cert.ssi.gouv.fr/contact`	Pour les administrations et les opérateurs d'importance vitale et de services essentiels

De plus, pour les incidents complexes, une aide externe est également recommandée pour :

- Gérer la crise
- Gérer la communication interne et externe
- Augmenter les ressources humaines et capacitaires de reconstruction de votre direction informatique

Pour faciliter la mobilisation de tous ces acteurs, il est conseillé de s'appuyer sur des annuaires tenus à jour en amont et accessibles même en cas d'indisponibilité du système d'information.

Déclarations

Conjointement à la résolution de l'incident, des déclarations doivent être effectuées :

Qui ?	Comment ?	Pourquoi ?
Assureurs		Notifier son assurance cyber permet de démarrer la prise en compte de la couverture et d'identifier des prestataires que l'assureur pourra recommander ou mandater.
ANSSI	https://www.cert.ssi.gouv.fr/contact/ https://cyber.gouv.fr/notifications-reglementaires	L'administration, les opérateurs d'importance vitale et de services essentiels, et toute organisation impliquant des informations classifiées, doivent déclarer leurs incidents à l'ANSSI.
Dépôt de plainte	https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de	Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.
CNIL	https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles	Les incidents affectant des données personnelles doivent faire l'objet de déclaration à la CNIL dans un délai de 72 heures. En cas de doute, il faut faire une pré-déclaration précisant avoir subi une potentielle compromission même si aucune exfiltration de données n'a été confirmée.
Autres autorités		Une organisation d'un domaine réglementé (finance, santé, etc.) est astreinte à des obligations de déclaration spécifiques. Dans le doute, consulter le service juridique.

Préparation

En *prévention* d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être préparée en amont, contextualisée et traduite en une *procédure interne et actionnable immédiatement* à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.
Il est également conseillé d'imprimer les fiches réflexes afin qu'elles restent disponibles en cas d'indisponibilité du système d'information. Il en va de même pour les autres documents utiles, comme la notice d'aide au dépôt de plainte ou votre annuaire de contacts.