

Fiche réflexe

# Compromission d'un compte de messagerie

## Qualification

2025

## Présentation de la fiche

### 1 A qui s'adresse-t-elle ?

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

### 2 Quand l'utiliser ?

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

### 3 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.

### 4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Conclusions attendues de la qualification** correspondant aux questions auxquelles la qualification devra répondre.
- La partie **Méthode d'évaluation pas à pas** correspondant 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 acceptées 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.

## Sommaire

Fiche réflexe  
- Compromission d'un compte de messagerie –  
Qualification

|                                             |    |
|---------------------------------------------|----|
| ○ Présentation de la fiche                  | 2  |
| ○ Sommaire                                  | 3  |
| ○ Prérequis                                 | 4  |
| ○ Conclusions attendues de la qualification | 5  |
| ○ Méthode d'évaluation pas à pas            | 7  |
| ◦ Évaluer l'incident                        | 7  |
| ◦ Déclarer l'incident                       | 14 |
| ◦ Qualifier l'incident                      | 15 |
| ○ Suite des actions                         | 16 |
| ○ Annexes                                   | 17 |

## Prérequis

01

### Avoir les 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.

02

### 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 ayant réalisé cette action ou ayant informé sur l'évènement ;
3. La description de l'action ou de l'évènement et les machines concernées.

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.

03

### 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. Commencer à reporter ces notes d'intervention dans la main courante.

\*Cette main courante doit être **éditable 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.

## 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 détaillera justement des actions détaillées qui aideront à conduire 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, etc.) ?
- L'accès initial peut-il être détecté (un mail de phishing, une attaque de type bruteforce, ou un maliciel 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 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 manière imminente ?

## Conclusions attendues de la qualification

### 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 **circonscriit** sur mon système d'information, ou est-il étendu ?
- L'incident présente-t-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 pu être maintenues ?

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

☐ ☐ Crise cyber

☐ ☐ Incident majeur

☐ ☐ Incident mineur

☐ ☐ Anomalie courante

## 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 appartient bien à l'organisation et correspond à un compte valide

##### Action 1.c : Identifier des délégations de droits

- ☐ Identifier des délégations de droits d'autres comptes sur cette boîte aux lettres
- ☐ Identifier des délégations de droits 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 certitude le(s) compte(s) suspecté(s) ?

## Méthode d'évaluation pas à pas

### Évaluer l'incident

#### 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 boîte 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 ?
- ☐ 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 peuvent-elles être observées ?
- ☐ De nouveaux comptes utilisateurs suspects ont-ils été créés ?

##### Action 2.c : Analyse des applications tierces

- ☐ Des **plugins** suspects ont-ils pu être frauduleusement installés ?
- ☐ Des accès d'application tierces ont-ils pu être détectés (**OAuth**, etc.) ?

## Méthode d'évaluation pas à pas

### Évaluer l'incident

#### Mesure 2 - Confirmer le signalement

##### 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'adresse IP inhabituelles ?
- ☐ Détection de connexions réussies à des horaires inhabituels ?
- ☐ Détection d'alertes d'échecs de connexion suivie 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 événements 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 ?*

## Méthode d'évaluation pas à pas

### Évaluer l'incident

#### Mesure 3 - Évaluer le périmètre de l'incident

##### Action 3.a : Identifier le type de compte affecté

- ☐ Type de compte :
  - ☐ Compte utilisateur standard ?
  - ☐ Compte 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, même 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 infostealer ?
  - Ce type d'alertes concerne-t-il d'autres postes ?

## Méthode d'évaluation pas à pas

### Évaluer l'incident

#### Mesure 3 - Évaluer le périmètre de l'incident

##### Action 3.e : Identifier un courriel suspect

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

##### Action 3.f : Identifier un vol de matériel

- ☐ Du matériel lié à l'utilisateur compromis aurait-il été volé (téléphone, ordinateur, clef USB, etc.) ?

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

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

- ☐ *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 phishing, une attaque de type bruteforce, ou un malware de type infostealer ciblant le poste de l'utilisateur) ?*

##### Important :

Un **phishing** ou autre vol de données n'a pu extraire qu'un seul couple login/mot de passe, mais qui peut potentiellement être réutilisable sur d'autres applications.

Un **infostealer** a pu extraire du navigateur de l'utilisateur compromis non seulement plusieurs couples login/mot de passe, mais également des **jetons (tokens) de sessions actives**.

## Méthode d'évaluation pas à pas

### Évaluer l'incident

#### Mesure 4 - Évaluer l'impact de l'incident

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

- ☐ Des données peuvent-elles avoir été exfiltrées ?
- ☐ Ces données sont-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 concernés 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 peuvent-elles avoir un impact sur le plan humain ?

##### 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

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

##### Action 4.e : (Conclure) Évaluer l'impact potentiel 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 ?

## Méthode d'évaluation pas à pas

### Évaluer l'incident

#### 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-il une procédure de continuité d'activité en mode nominal ?
- ☐ Existe-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 essentielles qui pourraient être perturbées suite à la compromission de la boîte 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 ?

## Méthode d'évaluation pas à pas

### Déclarer l'incident

#### Obligation de déclarer les incidents au CERT Santé

En vertu de l'article L1111-8-2 du Code de la santé publique, les établissements de santé, les laboratoires de biologie médicale, les centres de radiothérapie et les établissements et services médico-sociaux sont tenus de **signaler tout incident de sécurité des systèmes d'information aux autorités compétentes**.

#### Contacts du CERT Santé

- **Numéro d'urgence 24h/24 et 7j/7** : 09 72 43 91 25
- **Contact mail** : [cyberveille@esante.gouv.fr](mailto:cyberveille@esante.gouv.fr)
- **Portail de signalement** : <https://signalement.social-sante.gouv.fr/espace-declaration/profil>

#### Procédure pour déclarer un incident

- 1) Accéder au portail de signalement : <https://signalement.social-sante.gouv.fr/espace-declaration/profil>
- 2) Cliquer sur "**Je suis un professionnel de santé**"
- 3) Sélectionner "**Cybersécurité**" dans la liste
- 4) Cocher la case "**Incident de sécurité des systèmes d'information**"
- 5) Réaliser la procédure pour déclarer l'incident

## Méthode d'évaluation pas à pas

### 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** à un unique compte de messagerie, à un système d'information, ou est-il étendu ?
- L'incident présente-t-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 ?

☐

Crise cyber

☐

Incident majeur

☐

Incident mineur

☐

Anomalie courante

## Suite des actions

Si la compromission de compte de messagerie n'a pas pu être confirmée, il est tout de même **conseillé** de forcer un renouvellement du mot de passe et du MFA par sécurité pour le(s) compte(s) affecté(s) .

Si l'incident de compromission de compte de messagerie est confirmé, vous pouvez suivre 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*  
[<https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-dun-compte-de-messagerie-qualification-et-endiguement>]

Par ailleurs, si un incident de compromission système est suspecté, qualifier précisément cet incident :

*Fiche suivante conseillée : Fiche réflexe - Compromission système - Qualification*  
[<https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-systeme-qualification-et-endiguement>]

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.*

**Remarque** : 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 : Faire face à une menace  
(<https://cyberveille.esante.gouv.fr/dossier-thematique/faire-face-une-menace>)

## Annexes

### Définitions

#### 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.

#### 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.

#### 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.

#### Axes d'évaluation

- **Périmètre** : Le périmètre d'un incident désigne son étendue sur les composants du système d'information (comptes, applications, systèmes, etc..) et leur 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.

#### Degrés de gravité

- **Anomalie courante** (gravité **faible**) : Une anomalie courante est un incident de sécurité ne représentant 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*.

## Annexes

### 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                   |                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                 |
| CERT Santé                                             | <a href="https://esante.gouv.fr/produits-services/cert-sante">https://esante.gouv.fr/produits-services/cert-sante</a><br><a href="https://cyberveille.esante.gouv.fr/">https://cyberveille.esante.gouv.fr/</a>                                       | Pour les organisations du secteur de la santé et du médico-social                                                                                                                                                                                               |
| CERT/CSIRT externe en prestation de réponse à incident | <a href="https://www.cybermalveillance.gouv.fr/diagnostic/accueil">https://www.cybermalveillance.gouv.fr/diagnostic/accueil</a><br><a href="https://cyber.gouv.fr/produits-services-qualifies">https://cyber.gouv.fr/produits-services-qualifies</a> | Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance<br>Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS) |
| CERT-FR                                                | <a href="https://www.cert.ssi.gouv.fr/contact">https://www.cert.ssi.gouv.fr/contact</a>                                                                                                                                                              | Pour les administrations et les Opérateurs d'importance vitale et de services essentiels                                                                                                                                                                        |
| CSIRT régional                                         | <a href="https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux">https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux</a>                                                                                                                                  | Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations                                                                                                                                                          |

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

- Gérer la crise
- Gérer les communications 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.

## Annexes

### Déclarations complémentaires

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

| Qui ?            | Comment ?                                                                                                                                                                                                                                                                 | Pourquoi ?                                                                                                                                                                                                                                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANSSI            | <a href="https://www.cert.ssi.gouv.fr/contact/">https://www.cert.ssi.gouv.fr/contact/</a><br><a href="https://cyber.gouv.fr/notifications-reglementaires">https://cyber.gouv.fr/notifications-reglementaires</a>                                                          | 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 | <a href="https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de">https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de</a> | Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.                                                                                                                                                               |
| CNIL             | <a href="https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles">https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles</a>                                                                                                                 | <p>Les incidents affectant des données personnelles doivent faire l'objet de déclaration à la CNIL dans un délai de 72 heures.</p> <p>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.</p> |
| 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.                                                                                                                                |

## Annexes

### Préparation

En **prévention** d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être contextualisée et traduite en une **procédure interne et actionnable immédiatement** dans le cadre de 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.

### Préparation

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 (<https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-dun-compte-de-messagerie-qualification-et-endiguement>)
- Fiches techniques du CERT Santé pour améliorer la sécurité de son SI (<https://cyberveille.esante.gouv.fr/se-proteger-contre-les-menaces>)
- Fiches reflexes du CERT Santé pour réagir à un acte de cyber malveillance (<https://cyberveille.esante.gouv.fr/reagir-un-acte-de-cybermalveillance>)
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique (<https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique>)
- Cyberattaques et remédiation (<https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber>)

## Annexes

### Licence

Ce document est dérivé des travaux du GT Fiches Réflexes de remédiation de l'InterCERT France

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (<https://www.intercert-france.fr/>).

Le présent document est publié sous licence CC BY-NC-SA 4.0.