



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

*Agence nationale de la sécurité des
systèmes d'information*

**Secrétariat général de la défense
et de la sécurité nationale**

Paris, le 28/07/2025
N° CERTFR-2025-RFX-008

Fuite de données - Endiguement

Fiche Réflexe

ANSSI/SDO
28/07/2025



Version : 1
Nombre de pages : 18

Table des matières

1	Présentation de la fiche	3
1.1	À qui s'adresse-t-elle ?	3
1.2	Quand l'utiliser ?	3
1.3	À quoi sert-elle ?	3
1.4	Comment l'utiliser ?	3
2	Prérequis	3
2.1	Avoir qualifié l'incident	3
2.2	Ouvrir une main courante	4
3	Actions d'endiguement par priorités	4
4	Actions d'endiguement par thèmes	5
4.1	Contenir techniquement la propagation de la fuite	6
4.2	Limiter l'exposition des données	8
4.3	Préserver les traces	9
4.4	Maintenir les activités	10
4.5	Communiquer sur la fuite de données	10
5	Suite des actions	11
6	Annexes	12
6.1	Liens utiles	12
6.2	Définitions	13
6.3	Contacts	14
6.4	Déclarations	15
6.5	Préparation	15
6.6	Contacteur le CERT-FR	16
6.7	Licence	17

1 Présentation de la fiche

1.1 À qui s'adresse-t-elle ?

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

1.2 Quand l'utiliser ?

Utiliser cette fiche lorsqu'une fuite ou exfiltration de données au sein de mon organisation est confirmée.

1.3 À quoi sert-elle ?

L'objectif de cette fiche est de proposer les premières actions d'*endiguement* ayant pour objectif de circonscrire l'attaque. Elles tenteront de *limiter son extension et son impact* et de donner du temps aux défenseurs pour s'organiser et reprendre l'initiative.

1.4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Actions d'endiguement par priorités** pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante.
- La partie **Actions d'endiguement par thèmes** détaille les différentes actions d'endiguement possibles selon 4 axes thématiques.

Si l'organisation estime avoir besoin d'aide pour réaliser ces actions d'endiguement, elle peut contacter des équipes spécialisées en réponse à incident, qu'elles soient internes ou externes : voir la partie **Contacts**.

2 Prérequis

2.1 Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur le système d'information soit bien une fuite de données et en avoir évalué la gravité :

Fiche précédente conseillée : [Fiche réflexe - Fuite de données - Qualification](#)

Les mesures d'endiguement proposées dans cette fiche devront être appliquées en cohérence avec les conclusions de la *qualification* : le *périmètre* affecté par l'incident, son *impact* potentiel sur l'organisation, l'*urgence* à résoudre la situation, etc.

Les mesures à appliquer dépendront de la cause identifiée de la fuite de données, déterminée lors de la phase de qualification :

- Attaque par un acteur malveillant externe à l'organisation, il est nécessaire de se référer à la [fiche Fiche réflexe - Compromission Système - Endiguement](#),
- Erreur humaine involontaire,
- Acte malveillant interne (exfiltration via clé USB, mail, etc.).

2.2 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*.

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.

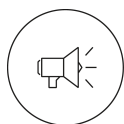
Ce document sera utile pour :

- 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 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.

3 Actions d'endiguement par priorités

Cette partie pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante pour chacun des cas d'usage mentionnés ci-dessus. Les mesures et actions sont détaillées par la suite.



Remarque

Si l'incident implique des DPO, la partie communication aux régulateurs doit être intégrée au même moment que la communication en interne.

Attaque par un acteur malveillant externe

Actions	Priorité
Bloquer et superviser les flux d'exfiltration (<i>Mesure 2</i>)	P0
Sécuriser les comptes et systèmes compromis (<i>Mesure 3</i>)	P0
Restreindre ou supprimer l'accès aux données (<i>Mesure 4 - Action 4.a</i>)	P0
Préserver les traces (<i>Mesure 5</i>)	P1
Mettre en place une surveillance des documents ou informations divulguées (<i>Mesure 4 - Action 4.b</i>)	P1
Maintenir la continuité des opérations (<i>Mesure 6</i>)	P2
Communiquer en interne sur la fuite de données (<i>Mesure 7</i>)	P3
Communiquer publiquement sur la fuite de données (<i>Mesure 8</i>)	P3

Acte malveillant interne

Actions	Priorité
Bloquer les accès suspects du collaborateur (<i>Mesure 1</i>)	P0
Sécuriser les comptes et systèmes compromis (<i>Mesure 3</i>)	P1
Bloquer et superviser les flux d'exfiltration (<i>Mesure 2</i>)	P1
Préserver les traces (<i>Mesure 5</i>)	P2
Communiquer en interne sur la fuite de données (<i>Mesure 7</i>)	P3

Erreur humaine involontaire

Actions	Priorité
Préserver les traces (<i>Mesure 5</i>)	P0
Mettre en place une surveillance renforcée (<i>Mesure 2 - Action 2.b</i>)	P1
Notifier les équipes RH et juridiques (<i>Mesure 1 - Action 1.a</i>)	P2
Communiquer sur l'incident en interne (<i>Mesure 7</i>)	P2

4 Actions d'endiguement par thèmes

Cette partie détaille les différentes mesures d'endiguement possibles selon 4 axes thématiques. Chaque *mesure* est ensuite scindée en *actions unitaires* :

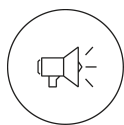
- Contenir techniquement la propagation de l'attaque
 - Mesure 1 - Bloquer les accès suspects du collaborateur
 - Mesure 2 - Bloquer et superviser les flux d'exfiltration
 - Mesure 3 - Sécuriser les comptes et systèmes compromis
- Limiter l'exposition des données
 - Mesure 4 - Limiter l'exposition des données
- Préserver les traces

- Mesure 5 - Préserver les traces
- Maintenir la continuité des opérations
 - Mesure 6 - Maintenir la continuité des opérations
- Communiquer sur l'incident
 - Mesure 7 - Communiquer en interne sur la fuite de données
 - Mesure 8 - Communiquer publiquement sur la fuite de données

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités !
Pour cela, se référer à la précédente partie Actions d'endiguement par priorités.

4.1 Contenir techniquement la propagation de la fuite

4.1.1 Mesure 1 - Bloquer les accès suspects du collaborateur



Remarque

Cette mesure est applicable s'il s'agit d'un collaborateur interne ou externe à l'entreprise et qui a provoqué la fuite de données.

Action 1.a : Notifier les équipes RH et juridiques

- ☐ Envoyer un mail au manager/RH du collaborateur pour les informer que des investigations sont en cours suite à un comportement suspect identifié sur la machine ou le compte du collaborateur.
- ☐ Si la fuite semble malveillante, contacter les équipes RH et juridiques pour exposer la situation.

Action 1.b : Bloquer les accès du collaborateur

- ☐ Bloquer les accès physiques et logiques (compte LDAP, accès aux applications, etc.), notamment les accès aux canaux utilisés pour l'exfiltration (remarque : il est possible de mettre le compte sous surveillance active pour avoir une preuve en cas de récurrence).
- ☐ Bloquer les flux du collaborateur aux applications et données sensibles.
- ☐ Désactiver l'ensemble des comptes associés au collaborateur (accès distant, accès interne, applications, partages collaboratifs, etc.) et renouveler les comptes auxquels il a pu avoir accès.
- ☐ Récupérer si possible, le matériel du collaborateur.

4.1.2 Mesure 2 - Bloquer et superviser les flux d'exfiltration

Action 2.a : Bloquer les flux entrants et sortants

- ☐ Identifier les flux suspects. Analyser les logs des pare-feux, IDS, IPS, proxy sortant, CASB, solution DLP, antivirus et EDR pour repérer des activités anormales.
- ☐ Si les flux malveillants sont identifiés, appliquer une règle au niveau des mécanismes de blocage réseau (pare-feu). Bloquer les adresses IP, ports ou protocoles associés aux tentatives identifiées. Evaluer l'impact d'un blocage des flux avant de le réaliser, pour éviter de bloquer des flux métier légitimes. Ne garder que les flux de données essentiels et nécessaires aux activités de l'organisation.
- ☐ Sinon, isoler les équipements ou segments de réseau suspects pour contenir la fuite de données. Restreindre les communications entre les différentes zones du réseau.
- ☐ S'il s'agit d'une compromission d'un tiers, veiller à couper les flux entre l'entreprise compromise et l'organisation.

Action 2.b : Mettre en place une surveillance renforcée

- ☐ Si les adresses IP d'exfiltration sont connues, les mettre en surveillance dans le SIEM pour générer une alerte.
- ☐ Générer des alertes ou rapports dans le SIEM sur les processus ou protocoles d'exfiltration (rClone.exe, rsync, flux FTP, ...).
- ☐ En se basant sur les équipements qui ont remonté l'alerte, renforcer la surveillance pour détecter et réagir rapidement à toute nouvelle tentative de fuite de données.
- ☐ Renforcer la politique de sécurité sur la partie exfiltration (par exemple : mise en place d'une GPO, modification du seuil d'alerte sur la volumétrie réseau, etc.).
- ☐ Créer des alertes DLP en se basant sur le cas d'usage.

Action 2.c : S'assurer que les données sensibles sont protégées

- ☐ Vérifier que les données sensibles de l'organisation sont bien chiffrées.

4.1.3 Mesure 3 - Sécuriser les comptes et systèmes compromis

Action 3.a : Identifier les comptes et systèmes compromis

- ☐ Si des données sont exposées en clair dans la fuite de données, identifier les comptes qui en ont l'accès, y compris ceux des clients, utilisateurs externes.
- ☐ Lister les comptes utilisateur et système ayant eu récemment accès aux données fuitées pour détecter toute compromission potentielle.
- ☐ Lister les systèmes qui pourraient ou auraient pu contenir les données fuitées.

Action 3.b : Renouveler les mots de passe des comptes et systèmes compromis

- ☐ Imposer la réinitialisation immédiate des mots de passe et jetons d'authentification pour tous les comptes identifiés comme compromis. S'aider si besoin de la fiche réflexe "Compromission de compte de messagerie".
- ☐ Révoquer toutes les sessions associées aux comptes identifiés comme compromis.
- ☐ Vérifier les appareils enrôlés des comptes compromis et désactiver l'enrôlement d'appareils suspects externes à l'organisation.
- ☐ S'assurer que les nouveaux mots de passe respectent les politiques de sécurité de l'organisation (taille, complexité).
- ☐ Analyser les accès sur les systèmes compromis. Adapter les droits d'accès, lecture, écriture en conséquence.
- ☐ Si les systèmes compromis comportent des accès SSH, renouveler les certificats SSH associés.

Action 3.c : Renforcer la sécurité des comptes et systèmes

- ☐ Vérifier l'implémentation de mesures de sécurité avancées sur les comptes à privilèges, comme l'authentification multifacteur (MFA), l'authentification biométrique ou l'utilisation de jetons de sécurité. S'ils n'en disposent pas, implémenter cette mesure pour tous les comptes avec privilèges identifiés comme compromis.
- ☐ Mettre en place des contrôles d'accès renforcés pour les systèmes critiques comportant des données sensibles, y compris la revue des permissions et l'application des principes de moindre privilège.

4.2 Limiter l'exposition des données

4.2.1 Mesure 4 - Limiter l'exposition des données

Action 4.a : Restreindre ou supprimer l'accès aux données

- ☐ Si les données sont exposées en dehors de l'organisation :
 - ☐ Si les données sont disponibles sur un site public (GitHub, GitLab, commentaire sur un forum, etc.), demander au propriétaire (ou au webmaster) de supprimer ou restreindre l'accès aux données divulguées et garder la trace de la demande (en veillant à partager des preuves de ce qui est avancé). Remarque : Veiller à bien adapter la demande aux destinataires (le webmaster hacktiviste ne se comportera pas comme un webmaster journaliste).
 - ☐ Faire signer une décharge auprès du collaborateur ou tiers (sous-traitant, prestataire, partenaire) stipulant qu'il atteste avoir supprimé l'ensemble des données exfiltrées sur ses équipements personnels ainsi qu'un accord de non-divulgaration (NDA). La suppression peut être réalisée en présence d'un huissier de justice.
- ☐ Si les données sont exposées dans une zone interne à l'organisation :

- ☐ Couper l'accès aux données (par exemple, route d'une API ou page d'un serveur web). Attention, il convient de couper l'accès au service et pas d'éteindre la machine (en effet, il est nécessaire de conserver la machine allumée pour les investigations).

Action 4.b : Mettre en place une surveillance des documents ou informations divulguées.

- ☐ Surveiller les documents et informations divulgués via des outils internes, la gestion des surfaces d'attaque externes (exemple : shodan, onyphe) et la veille sur l'entreprise.

4.3 Préserver les traces

4.3.1 Mesure 5 - Préserver les traces

Pour soutenir la réponse à incident dans son objectif d'investigation, il faut prioritairement préserver les logs les plus anciens possibles, augmenter leur rétention et leur verbosité. Plus les équipes d'investigation auront les traces d'activité de l'adversaire, plus efficace sera son éradication.

Action 5.a : Préserver les traces dans les journaux d'équipements

- ☐ Identifier les équipements de sécurité du système d'information :
 - ☐ pare-feux
 - ☐ passerelles VPN
 - ☐ proxy
 - ☐ consoles antivirus et EDR
 - ☐ CASB
 - ☐ solution DLP
 - ☐ ...
- ☐ Exporter les logs sur un disque hors ligne (s'ils ne sont pas déjà dans un puits de logs).
- ☐ Augmenter la rétention et la verbosité des logs. Si possible, configurez les logs de manière à ce qu'ils soient les plus détaillés possibles.

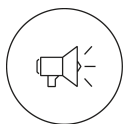
Action 5.b : Préserver les traces dans les journaux d'authentification

- ☐ Identifier la solution de stockage des journaux d'identification sur le réseau interne, comme le domaine Active Directory et exporter ces logs (s'ils ne sont pas déjà dans un puits de logs).
- ☐ Augmenter la rétention de ces logs.

Si les logs sont déjà exportés dans un SIEM ou un centralisateur de logs, il est alors inutile de les exporter et d'augmenter leur rétention sur les machines sources, mais il faut néanmoins augmenter leur verbosité lorsque cela est possible.

Action 5.c : Récupérer des fichiers liés à la fuite de données

- ☐ Récupérer les logs prouvant la fuite de données (accès aux fichiers via le compte compromis, exfiltration réseau, etc.).
- ☐ S'il y a une revendication, prendre une capture d'écran de la page, avec la date, l'heure et l'URL incluses (qui pourra servir de preuve en cas de dépôt de plainte).



Remarque

En plus d'être indispensable à la compréhension de l'incident, sauvegarder les éléments de preuve pourra être nécessaire pour répondre aux forces de l'ordre lors d'éventuelles poursuites judiciaires.

4.4 Maintenir les activités

4.4.1 Mesure 6 - Maintenir la continuité des opérations

Action 6.a : Stabiliser les opérations critiques

- ☐ Mettre en place des mesures temporaires pour sécuriser les systèmes critiques, assurant ainsi le maintien des opérations essentielles en incluant les équipes métier concernées.
- ☐ Évaluer et sécuriser rapidement les données et systèmes vulnérables identifiés lors des analyses précédentes.

Action 6.b : Assurer la continuité des services

- ☐ Si nécessaire, mettre en place des mesures pour garantir que les services clés restent opérationnels, s'aider du PCA si l'organisation en dispose.
- ☐ Se coordonner avec les équipes pour réorganiser les ressources et prioriser les tâches essentielles pendant la période d'investigation.

4.5 Communiquer sur la fuite de données

4.5.1 Mesure 7 - Communiquer en interne sur la fuite de données

Action 7.a : Communiquer en interne

- ☐ Fournir sous forme de synthèse exécutive une analyse de risques et les actions en cours liées à la fuite de données à sa hiérarchie, l'équipe des relations publiques, au DPO et à la direction. Attention à ne pas être trop technique dans cette analyse.

- ☐ Si la fuite est connue en interne ou externe à l'organisation, demander à la direction d'indiquer aux collaborateurs les éléments de langage et la cellule qui s'occupe de la communication extérieure.
- ☐ Si des données classifiées (confidentielles, marquage DR ou autre) sont impactées, informer l'équipe dédiée qui gère ce type de données.

Action 7.b : Communiquer aux régulateurs

- ☐ L'administration, les entités essentielles (EE), les entités importantes (EI) et toute organisation impliquant des informations classifiées, doivent déclarer leurs incidents à l'ANSSI, conformément à la législation en vigueur.
- ☐ Si des données personnelles figurent dans l'exfiltration ou que le DPO de l'organisation estime qu'une déclaration à la CNIL doit être réalisée, déclarer l'incident à la CNIL dans les 72 heures. En cas de doute, il faut faire une pré-déclaration précisant avoir subi une potentielle compromission, même si aucune fuite de données n'a été confirmée.
- ☐ Indiquer à la direction qu'il est envisageable de déposer plainte.

4.5.2 Mesure 8 - Communiquer publiquement sur la fuite de données

Action 8.a : Communiquer aux clients et partenaires

- ☐ Si les données personnelles de clients font partie de la fuite, prévoir une communication auprès des clients concernés.
- ☐ Si les services pour les clients sont impactés, prévoir une communication auprès des clients concernés.
- ☐ Si la fuite concerne également des partenaires, prévoir une communication auprès des partenaires.

Action 8.b : Communiquer auprès de la presse

- ☐ Informer la direction qu'elle peut, si elle l'estime nécessaire, engager une communication avec la presse.

5 Suite des actions

À la fin de ces actions d'endiguement, la fuite de données devrait être maîtrisée. Toutefois, il convient de rester vigilant et continuer de réaliser une veille sur sa surface d'exposition, sa marque, les médias et divers canaux de communication. Par ailleurs, seule une analyse approfondie permettra d'appréhender les indicateurs décelés durant cette première phase de remédiation.

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés : *investigation forensique et remédiation par une équipe spécialisée, maintien d'activité, communication interne aux partenaires, dépôt de plainte et déclarations, etc.*

Pour ce faire, il est conseillé de piloter la suite de la résolution de l'incident en cohérence avec les *impacts* identifiés et demander de l'aide :

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

5.0.1 Sensibiliser les collaborateurs

Dans le cas d'exfiltration de données par un acteur interne (erreur humaine involontaire ou acte interne malveillant), il est utile de sensibiliser les collaborateurs et administrateurs.

☐ Sensibiliser les utilisateurs dans un cas involontaire

- ☐ Sensibiliser le collaborateur à ne pas utiliser son PC professionnel pour un usage personnel (et inversement).
- ☐ Sensibiliser l'utilisateur sur les responsabilités et les risques d'une fuite de données pour l'organisation.
- ☐ Rappeler de partager les données sensibles uniquement via des canaux sécurisés validés en interne.
- ☐ Expliquer les risques de phishing et comment les identifier. Encourager l'utilisateur à signaler les communications suspectes.

☐ Sensibiliser les administrateurs

- ☐ Informer l'administrateur sur l'importance de maintenir des pratiques de sécurité strictes lors de la gestion des systèmes et des données.
- ☐ Expliquer les conséquences potentielles d'une mauvaise configuration des systèmes ou des réseaux qui pourrait conduire à une fuite de données.
- ☐ Encourager l'administrateur à effectuer des revues régulières de la sécurité des systèmes et des permissions utilisateur.
- ☐ Rappeler la nécessité de signaler immédiatement tout incident suspect ou toute anomalie observée dans les systèmes.
- ☐ Sensibiliser sur les risques liés à l'utilisation d'un seul compte pour plusieurs utilisateurs, et l'importance de mots de passe forts et uniques pour chaque compte.

6 Annexes

6.1 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 - Fuite de données - Qualification
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Guide ANSSI Cyberattaques et remédiation

6.2 Définitions

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 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*.

6.2.5 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.

6.2.6 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.

6.2.7 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.

6.3 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 organisations 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.fr https://www.m-cert.fr https://esante.gouv.fr/produits-services/cert-sante	Pour les organisations du secteur de l'aviation, maritime ou santé
CERT-FR	Consulter la section Contacter le CERT-FR	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.

6.4 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.

6.5 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.

6.6 Contacter le CERT-FR



Attention

Quand vous effectuez un signalement auprès du CERT-FR, un numéro de référence vous est attribué. Pensez à rappeler ce numéro quand vous nous recontactez, ou dans l'entête de vos messages afin de simplifier le suivi du cas.

6.6.1 Par Téléphone

Le CERT-FR est joignable 7J/7, 24H/24 :

- depuis la France métropolitaine au **3218** (service gratuit + prix d'un appel) ou 09 70 83 32 18
- depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au +33 9 70 83 32 18

6.6.2 Par Internet

- mël : `cert-fr@ssi.gouv.fr`
- site : `https://cert.ssi.gouv.fr/contact/`

6.6.3 Clé PGP du CERT-FR

Pour vérifier l'intégrité des informations fournies ci-dessous, veuillez contacter le CERT-FR.

Identifiant de la clé : 0x1B45CF2A

Empreinte de la clé : 7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A

Télécharger la clé publique : `https://cert.ssi.gouv.fr/uploads/public\_key\_2024.asc`

6.7 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/publications/fiches-reflexes/>).

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

ANSSI/SDO
Version 1- UNDEF

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr

