Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Fuite de données

Endiguement

2026

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 fuite ou exfiltration de données au sein de mon organisation est confirmée.

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.

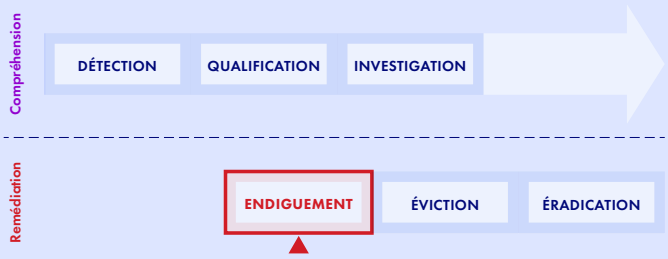
Comment l'utiliser ?

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 différents 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.

SOMMAIRE



PRÉREQUIS

Demander de l'aide

Ne jamais rester seul face à un incident. Solliciter l'aide d'un collègue afin de ne pas assumer seul la responsabilité de son traitement et de pouvoir répartir efficacement les tâches. Par exemple, une personne peut se concentrer sur l'approfondissement de la qualification de l'incident, tandis que d'autres peuvent contacter un responsable hiérarchique et le CSIRT/CERT, initier les premières mesures d'endiguement, voire paralléliser les actions prioritaires.

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 :

- Fuite de données en cours.
- Fuite de données causée par un compte interne (usurpation d'un compte ou malveillance).
- Fuite de données causée par une application compromise ou mal configurée exposée sur internet.
- Fuite prouvant une compromission d'un système interne.
- Fuite de données causée par une cause inconnue.

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.

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.
Selon les conclusions de la fiche qualification, les priorités ne seront pas les mêmes, il convient donc de se référer au tableau adéquat.

REMARQUE

- Si la fuite de données provient d'un tiers, se référer aux fiches compromission d'un tiers.
- Si la fuite de données révèle une compromission d'un système, se référer aux fiches réflexes Compromission d'un système après avoir endigué la fuite de données.
- Si la fuite de données implique des données personnelles, la partie communication aux régulateurs doit être intégrée au même moment que la communication en interne.

Cas 1 : Fuite de données en cours

Actions	Priorité
Bloquer les flux entrants et sortants *(Mesure 2 - Action 2.a)*	P0
Restreindre ou supprimer l'accès aux données *(Mesure 4 - Action 4.a)*	P0
Communiquer en interne et aux régulateurs sur la fuite de données *(Mesure 8)*	P1
Préserver les traces *(Mesure 5)*	P1
Mettre en place une surveillance des documents ou informations divulguées *(Mesure 4 - Action 4.b)*	P2
Si revendication ou publication des données, communiquer publiquement *(Mesure 9)*	P3

REMARQUE

- Après application des premières mesures d'endiguement, prendre le temps de faire une qualification plus approfondie pour identifier la cause. Une fois cela fait, se référer aux autres cas de cette fiche pour continuer l'endiguement.
- Si la fuite de données révèle une compromission d'un système, se référer aux fiches réflexes Compromission d'un système après avoir endigué la fuite de données.

Cas 2 : Fuite de données causée par un compte interne (usurpation d'un compte ou malveillance)

Actions	Priorité
Bloquer les accès suspects du collaborateur *(Mesure 1)*	P0
Notifier les équipes adéquates du blocage du compte *(Mesure 7)*	P0
Mettre en place une surveillance renforcée *(Mesure 2 - Action 2.b)*	P1
Sécuriser les comptes et systèmes compromis *(Mesure 3)*	P1
Préserver les traces *(Mesure 5)*	P2
Mettre en place une surveillance des documents ou informations divulguées *(Mesure 4 - Action 4.b)*	P3
Communiquer en interne et aux régulateurs sur la fuite de données *(Mesure 8)*	P4
Si revendication ou publication des données, communiquer publiquement *(Mesure 9)*	P4

Cas 3 : Fuite de données causée par une application compromise ou mal configurée exposée sur internet

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

Actions	Priorité
Si revendication ou publication des données, communiquer publiquement *(Mesure 9)*	P4

REMARQUE

- Il convient de ne pas exposer à nouveau le service sur internet avant d'avoir corrigé la cause de la fuite de données.
- Si la fuite de données révèle une compromission d'un système, se référer aux fiches réflexes Compromission d'un système après avoir endigué la fuite de données.

Cas 4 : Fuite prouvant une compromission d'un système interne

- Endiguer la fuite de données est se reportant aux cas 1, 2 ou 3 ci-dessus.
- Endiguer la compromission d'un système d'information en se référant aux fiches :
  - Fiche réflexe - Compromission système
  - Fiche réflexe - Chiffrement ou effacement en cours

Cas 5 : Fuite de données causée par une cause inconnue

- Endiguer la fuite de données est se reportant au cas 3 ci-dessus.

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 et renforcer leur surveillance
  - 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 - Notifier les équipes adéquates du blocage du compte
  - Mesure 8 - Communiquer en interne et aux régulateurs sur la fuite de données
  - Mesure 9 - 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.

Contenir techniquement la propagation de la fuite

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 : 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 récidive).
- ☐ 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.

IMPACT

Attention lors du verrouillage du compte à avertir la chaine de commandement pour ne pas impacter l'organisation (ex : compte administrateur sur des machines de production).

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.
- ☐ Si les points précédents sont insuffisants pour contrer une exfiltration en cours, isoler le serveur d'internet en prenant en compte les impacts, en dernier recours éteindre le serveur.

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.

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 de l'authentification multifacteur (MFA) si le compte n'en dispose pas.

Limiter l'exposition des données et renforcer leur surveillance

Mesure 4 - Limiter l'exposition des données et renforcer leur surveillance

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-divulgation (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 : isoler le serveur d'internet, ne plus exposer l'API). 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.

Préserver les traces

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.

Maintenir les activités

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.

Communiquer sur la fuite de données

Mesure 7 : Notifier les équipes adéquates du blocage du compte

Action 7 : Notifier les équipes RH ou commerciales et juridiques

- ☐ Suivre les procédures internes, par exemple :
  - ☐ 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. S'il s'agit d'un collaborateur externe, contacter l'équipe commercial à la place de l'équipe RH.
  - ☐ Si la fuite semble malveillante, contacter les équipes RH et juridiques pour exposer la situation.
- ☐ Prévenir le service IT ou la DSI de ne pas rouvrir le compte tant que l'investigation n'est pas terminée. Le service IT pourrait recevoir des demandes du collaborateur pour rouvrir ses accès.

> **REMARQUE**
>
> S'il s'agit d'un acte malveillant, il est possible que le collaborateur n'agisse pas seul et que d'autres personnes soient impliquées. Il faut donc choisir consciencieusement à qui on communique afin d'éviter des effacements de preuves par des complices.

Mesure 8 - Communiquer en interne et aux régulateurs sur la fuite de données

Action 8.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 8.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. Par ailleurs, une indisponibilité des données doit également être déclarée à la CNIL.
- ☐ Indiquer à la direction qu'il est envisageable de déposer plainte et que l'assurance cyber peut l'exiger.

Mesure 9 - Communiquer publiquement sur la fuite de données

Action 9.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 9.b : Communiquer auprès de la presse

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

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*.

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.

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

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-incide`	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	`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.

Qui ?	Comment ?	Pourquoi ?
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.

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.

FICHE RÉFLEXE

L'InterCERT France fédère aujourd'hui plus de 100 CERTs sur le territoire national, constituant ainsi la 1ère communauté de CERTs en France.

Cette fiche réflexe est issue de la coopération et du partage d'expérience de plusieurs de ces CERTs. Elle a pour objectif d'être un outil efficace lors des premières étapes de gestion de l'incident en cours, en proposant des actions concrètes pour débuter le processus de remédiation.

Vous pouvez trouver l'ensemble de ces fiches au lien suivant :
`https://www.intercert-france.fr/publications/fiches-reflexes/`

Votre expérience dans le traitement d'un incident et l'utilisation de cette fiche est précieuse. Dans le but d'améliorer sa qualité, nous vous invitons à partager vos commentaires et suggestions d'amélioration, en nous contactant à l'adresse suivante :
fichesreflexes-remediation@intercert-france.fr