Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Fuite de données

Qualification

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 de données de l'entreprise est suspectée ou confirmée.

A quoi sert-elle ?

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

- *Confirmer* qu'une fuite de donnée est en cours ou a eu lieu.
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

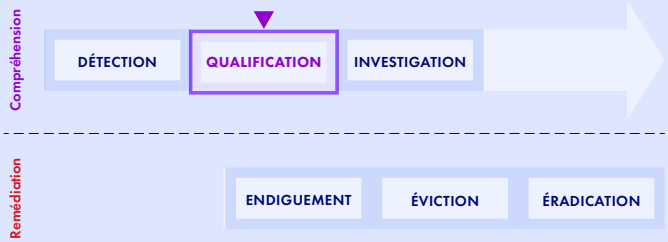
Comment l'utiliser ?

Deux parties principales composent cette fiche :

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

Cette fiche doit être exécutée en *temps court*. Pour cela, fixer un *temps contraint* selon l'urgence pressentie (ex : 30 minutes, 1 heure au maximum) et ne pas rechercher l'exhaustivité des réponses : des *réponses approximatives* et des réponses *"je ne sais pas répondre"* sont acceptables dans un premier temps. Par la suite, une qualification plus approfondie se fera sûrement, avec plus de recul ou l'appui d'une équipe spécialisée en réponse à incident.

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.

Disposer des personnes nécessaires

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

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

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

Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer tous 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 (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 les retours d'expérience.
- 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 EM l'organisation en possède un, voire être au format papier.

Avoir pris connaissance des actions déjà entreprises

Avoir pris note des personnes ayant déjà agi en réponse à l'incident en cours et des actions qu'elles ont déjà entreprises sur le système d'information. Commencer à reporter ces notes d'intervention dans la main courante.

CONCLUSIONS ATTENDUES DE LA QUALIFICATION

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

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type fuite de données

- ☐ *En cas de suspicion d'exfiltration, s'agit-il bien d'une exfiltration avérée et non d'un faux positif ?*
- ☐ *Sinon, le signalement reçu ou la revendication de la fuite de données a-t-il été confirmé ? À défaut, présente-t-il un niveau de crédibilité suffisant ?*
- ☐ *Les données prétendument copiées appartiennent-elles effectivement à l'organisation ou celle-ci est-elle uniquement mentionnée ?*
- ☐ *Les données fuitées étaient-elle bien hébergées sur le système d'information de l'organisation ? Arrive-t-on à les localiser précisément ?*

Mesure 2 - Évaluer le périmètre et la cause de la fuite de données

- ☐ *La cause de la fuite peut-elle être plausiblement établie (fuite volontaire ou involontaire par un utilisateur interne, usurpation d'un utilisateur, compromission d'une application exposée, compromission d'un serveur du système d'information ?)*
- ☐ *Le périmètre des données concernées par la fuite peut-il être identifié précisément ?*
- ☐ *Le périmètre des données fuitées est-il circonscrit ou peut-il être étendu ?*
- ☐ *Le périmètre de l'incident pourrait-il être plus étendu qu'initialement estimé, au-delà de la seule fuite de données ?*

Mesure 3 - Évaluer l'impact de la fuite de données

- ☐ *Quel type de données a fuité (métiers, personnelles ou contractuelles, authentification ou techniques) ?*
- ☐ *La fuite de données est-elle connue publiquement ? La presse, les clients et/ou les partenaires risquent-ils d'en être informés ?*
- ☐ *Quel est l'impact de cette fuite pour l'organisation (à court et long terme) ?*
- ☐ *Quel est l'impact sur l'organisation des mesures d'endiguement déjà prises ?*

Mesure 4 - Évaluer l'urgence à remédier la fuite de données

- ☐ *L'attaque peut-elle encore évoluer et est-il urgent de la contenir ?*
- ☐ *Est-il urgent de rétablir les activités impactées ?*
- ☐ *Est-il urgent de communiquer sur la fuite de données ?*
- ☐ *Y a-t-il des délais urgents pour déclarer l'incident (réglementation, assurance, etc.) ?*

Qualifier l'incident

Conclure quant à la gravité de la fuite de données

- ☐ La fuite de données de mon organisation est-elle *confirmée* ?
- ☐ La fuite de données est-elle *circonscrite* à un système, ou a-t-elle une portée plus large ?
- ☐ La fuite de donnée a-t-elle un *impact fort* sur l'activité ou pouvant le devenir ?
- ☐ Est-il *urgent* d'agir pour endiguer la fuite de données ou rétablir des activités ?
- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?

1. Anomalie courante
2. Incident mineur
3. Incident majeur
4. Crise cyber

MÉTHODE D'ÉVALUATION PAS À PAS

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

Évaluer l'incident

Mesure 1 - Confirmer la fuite de données et sa nature

Action 1.a : Identifier l'origine de l'alerte de la fuite de données

- ☐ S'agit-il d'un signalement d'une fuite de données passée ?
  - ☐ Un signalement fait en interne par un employé ou en externe par un partenaire ?
  - ☐ Une alerte extérieure ou revendication, comme sur un forum ou un réseau social ?
- ☐ S'agit-il d'une suspicion d'exfiltration de données en cours ?
  - ☐ Une alerte spécifique de mes équipements de sécurité (par exemple une règle DLP) ?
  - ☐ Une volumétrie réseau anormalement élevée ?

Action 1.b : Vérifier la crédibilité de l'exfiltration de données en cours

- ☐ Quel événement induit l'idée d'une exfiltration de données ?
  - ☐ Une alerte spécifique de mes équipements de sécurité (par exemple une règle DLP) ?
  - ☐ Une volumétrie réseau anormalement élevée ?
  - ☐ Un comportement anormal de trafic détectés via des outils de sécurité (par exemple : IDS, IPS, EDR, CASB, Proxy, Pare-feu, etc.) ?
  - ☐ Autre ?
- ☐ Les données censées avoir été exfiltrées sont-elles accessibles ?
- ☐ L'exfiltration de données est-elle confirmée ou crédible, ou cet incident peut-il être un incident de production ?
  - ☐ Est-il nécessaire d'investiguer d'avantage ?

> **REMARQUE**
>
> S'il s'agit d'une suspicion d'exfiltration de données en cours, il convient d'évaluer dès à présent l'opportunité de mettre en place des mesures d'endiguement afin de tenter d'enrayer la fuite. Voir : Fiche réflexe - Fuite de données - Endiguement.

Action 1.c : Vérifier la crédibilité du signalement et si l'organisation semble bien être victime d'une fuite de données

- ☐ Un échantillon de données fuitées est-il disponible et accessible ? Si oui :
  - ☐ Collecter l'ensemble des données mises à disposition sur une machine déconnectée du réseau de l'organisation.

Si les données sont accessibles, confirmer qu'il s'agit bien d'une fuite :

- ☐ Les données semblent-elles réellement provenir d'une fuite ?
  - Les données ne sont-elles pas en fait déjà publiquement disponibles ?
  - Les données ne sont-elles pas le regroupement de précédentes fuites déjà publiées ?
  - Les données ne sont-elles pas forgées ? (Comparer les données fuitées à celles connues pour s'en assurer).
- ☐ Les données fuitées semblent-elles appartenir à l'organisation ? Si non :
  - L'organisation est-elle seulement citée ?
  - Les données semblent-elles appartenir à un tiers avec lequel l'organisation est en lien (partenaire, client, fournisseur) ?*

REMARQUE

Si les données semblent appartenir à un tiers, il convient de qualifier l'incident. Voir notamment Fiche réflexe - Compromission d'un tiers - Qualification.

Si les données ne sont pas accessibles, confirmer que la fuite semble crédible :

- ☐ S'il s'agit d'un groupe d'attaquant, se renseigner sur la menace : l'acteur est-il connu pour bluffer ou au contraire a-t-il fait des dégâts à ses précédentes victimes revendiquées ?
- ☐ S'il s'agit d'un signalement fait par un employé ou par un partenaire :
  - L'alerte provient-elle d'une source de confiance (prestataire CTI, ANSSI, CERT sectoriels et régionaux, etc.) ?
  - Quelles informations et preuves peut fournir la personne ou le partenaire ?
  - Quelle confiance accorde-t-on à la personne ou au partenaire concernant ce signalement ?

Action 1.d : Tenter d'identifier l'origine des données et confirmer leur hébergement par l'organisation

Si les données sont accessibles et ont été collectées :

- ☐ Déterminer le type de données fuitées. Par exemple :
  - base de données,
  - application,
  - emails,
  - fichiers d'un poste utilisateur,
  - fichiers propres à un service particulier,
  - données clientes,
  - identifiants et mots de passe,
  - autre ?
- ☐ Tenter de trouver si les données proviennent d'une machine appartenant à l'organisation. Par exemple :
  - ☐ Une machine exposée publiquement ?
    - ▷ un github ou gitlab public,
    - ▷ un partage externalisé,
    - ▷ un serveur web,
    - ▷ autre ?
  - ☐ Une machine interne ?
    - ▷ un poste de travail professionnel ou personnel (BYOD),
    - ▷ un serveur sur le réseau interne,
    - ▷ l'Active Directory,
    - ▷ autre ?
- ☐ Si les données n'ont pas été trouvées sur le système d'information :
  - ☐ Identifier si une équipe ou filiale serait concernée par ces données pour leur demander l'emplacement des données.
  - ☐ Si non, serait-il probable que ces données soient hébergées ailleurs que sur le système d'information de l'organisation ?

Action 1.e : (Conclure) Confirmer la fuite de données

- ☐ *En cas de suspicion d'exfiltration, s'agit-il bien d'une exfiltration avérée et non d'un faux positif ?*
- ☐ *Sinon, le signalement reçu ou la revendication de la fuite de données a-t-il été confirmé ? À défaut, présente-t-il un niveau de crédibilité suffisant ?*
- ☐ *Les données prétendument copiées appartiennent-elles effectivement à l'organisation ou celle-ci est-elle uniquement mentionnée ?*
- ☐ *Les données fuitées étaient-elle bien hébergées sur le système d'information de l'organisation ? Arrive-t-on à les localiser précisément ?*

Mesure 2 - Identifier périmètre et la cause de la fuite de données

Action 2.a : Évaluer le périmètre de la fuite selon les données accessibles

Si un extrait des données fuitées est disponible :

- ☐ Identifier si les données concernent un seul projet/sujet ou si elles sont variées.

- ☐ Identifier si les données fuitées sont anciennes ou récentes.
  - ☐ Si elles sont anciennes, s'agit-il de données combinées issues d'anciennes fuites ?
- ☐ Estimer la quantité de données fuitées.
- ☐ S'il s'agit d'une revendication, est-il mentionné que plus de données vont être publiées prochainement ?
- ☐ **Au final, selon les données accessibles, est-il possible d'identifier précisément le périmètre des données concernées par la fuite, ou celui-ci demeure-t-il flou ?**

> **REMARQUE**
>
> Pour cette action, il peut être bénéfique de s'aider des équipes (métiers, bénéficiaires, clients) dont les données sont impactées.

Action 2.b : Évaluer le périmètre de la fuite selon l'origine des données

Si l'origine des données a été trouvée à l'étape précédente :

- ☐ Évaluer si d'autres données que celles déjà identifiées étaient hébergées sur le serveur concerné par les données fuitées et auraient également fuitées ?
- ☐ Dans quelle zone sont hébergées les données fuitées ?
  - ☐ Zone exposée sur Internet ?
    - ☐ DMZ
    - ☐ Hébergement externalisé
    - ☐ Application Cloud
    - ☐ Autre ?
  - ☐ Zone non exposée
    - ☐ Zone bureautique
    - ☐ Zone métier
    - ☐ Infrastructure Cloud
    - ☐ Autre ?
- ☐ D'autres systèmes situés dans la même zone que le système ont-ils potentiellement pu être accédés ?
  - ☐ Si oui, quelles types de données contenaient-ils ?
- ☐ Une intrusion vers d'autres zones du système d'information de l'organisation est-il probable ?
  - ☐ Si oui, une étendue large de fuite de données est-elle à craindre ?
- ☐ **Au final, le périmètre des données fuitées est-il circonscrit ou peut-il être étendu ?**

Action 2.c : Tenter d'identifier la cause de la fuite de données

Si l'origine des données a été trouvée à l'étape précédente, tenter d'identifier la cause de la fuite de données :

Si les données étaient hébergées dans une zone exposée sur Internet :

- ☐ Les données ont-elles pu être consultées via un accès légitime à partir d'un compte usurpé ? *(connexions suspectes dans les journaux d'authentification, etc.).*
- ☐ Les données ont-elles pu être consultées à la suite de l'exploitation d'une vulnérabilité de l'application ou une mauvaise configuration ? *(alertes WAF, URL suspectes, application non à jour et ayant des vulnérabilités, campagne en cours d'exploitation, règles d'accès trop permissives, etc.).*
  - ☐ Se renseigner sur l'analyse de la menace récente pour étudier si une nouvelle vulnérabilité aurait pu être utilisée pour effectuer la fuite de données (auprès de son équipe CTI interne ou Vulneravility Operations Center (VOC).
- ☐ Le serveur exposé présente-t-il des signes de compromission ? *(fichiers malveillants identifiés, alertes AV/EDR, altération des fichiers de configuration, etc.).*

Si les données se situent dans une zone non exposée sur Internet, pourrait-il s'agir de :

- ☐ D'un employé ou un tiers qui réalise une exfiltration involontaire et expose ainsi les données ? *(erreur humaine ou volonté de contourner le filtrage de l'organisation pour travailler)*

- ☐ D'un employé ou un tiers autorisé qui réalise une exfiltration intentionnelle *(acte de malveillance)* ?
- ☐ Une exfiltration suite à la compromission d'un serveur ? Possiblement dans une compromission plus large ?
    - Le cas échéant, cet incident pourrait-il être corrélé avec un incident en cours ou récent ?
- ☐ **Selon la cause probable, le périmètre de l'incident pourrait-il être plus étendu qu'initialement estimé, au-delà de la seule fuite de données ?**

> **REMARQUE**
>
> Si des données ont fuitées involontairement, elle peuvent probablement être la conséquence d'autres incidents qu'il convient de qualifier. Voir notamment Fiche réflexe - Compromission d'un compte de messagerie - Qualification ou Fiche réflexe - Compromission système - Qualification ou Fiche réflexe - Compromission d'un tiers - Qualification.

Action 2.d : (Conclure) Évaluer le périmètre et la cause de la fuite de données

- ☐ *La cause de la fuite peut-elle être plausiblement établie (fuite volontaire ou involontaire par un utilisateur interne, usurpation d'un utilisateur, compromission d'une application exposée, compromission d'un serveur du système d'information ?)*
- ☐ *Le périmètre des données concernées par la fuite peut-il être identifié précisément ?*
- ☐ *Le périmètre des données fuitées est-il circonscrit ou peut-il être étendu ?*
- ☐ *Le périmètre de l'incident pourrait-il être plus étendu qu'initialement estimé, au-delà de la seule fuite de données ?*

Mesure 3 - Évaluer l'impact de la fuite de données

Action 3.a : Analyser le type et la sensibilité des données

- ☐ Identifier précisément le type de données fuitées parmi les catégories suivantes :
    - **Données métiers** : informations confidentielles liées à l'activité de l'organisation (secrets industriels, stratégies commerciales, données financières, etc.).
    - **Données personnelles** ou contractuelles : informations relatives aux individus (employés, clients, partenaires) protégées par des réglementations (RGPD, etc.). Inclure les contrats et accords.
    - **Données d'authentification ou techniques** : informations permettant l'accès aux systèmes (mots de passe, clés API, certificats) ou des données techniques sensibles (architecture du système d'information, configurations).
    - **Données classifiées** : confidentiel, diffusion restreinte, secret...

Action 3.b : Évaluer les impacts de la fuite

- ☐ **Évaluer l'impact public et médiatique :**
    - ☐ Vérifier si la fuite de données est déjà connue du public (médias, réseaux sociaux, dark web). Si oui, évaluer l'étendue de la diffusion et les réactions.
    - ☐ Évaluer le risque que la fuite soit relayée par les médias et l'impact potentiel sur l'image de l'organisation, notamment vis-à-vis de ses clients et partenaires.
- ☐ **Évaluer les impacts contre l'organisation** de la fuite de ces données selon les critères de confidentialité et d'intégrité (en s'aidant par exemple d'une analyse de risque).
    - ☐ Données métiers :
        - ▷ Répercussions économiques : pertes financières directes, perte d'avantage concurrentiel, interruption des activités (R&D). Quantifier les pertes, si possible.
        - ▷ Divulgation de secrets industriels ou d'informations sensibles pouvant être exploitées par des concurrents ou à des fins d'espionnage.
        - ▷ Impact sur la poursuite des activités, notamment pour les données stratégiques (R&D, plans de développement).
        - ▷ Impact sur la sécurité physique (divulgation de plan d'accès, des bâtiments, etc.).
        - ▷ Impact sur le respect des réglementations : si des données classifiées (confidentielles, marquées DR, etc.) sont impactées, la réglementation ne sera plus respectée. Contacter l'équipe conformité pour identifier tous les impacts.
    - ☐ Données personnelles ou contractuelles :
        - ▷ Impacts juridiques : non-conformité avec le RGPD ou autres réglementations, amendes, actions en justice de la part des personnes concernées.
        - ▷ Atteinte à la réputation et à la confiance des clients et partenaires.

- ☐ Données d'authentification ou techniques :
  - ▷ Risque d'accès non autorisé au système d'information par des attaquants utilisant les identifiants compromis (accès aux boîtes de messagerie, accès distant au système d'information, accès distant à des applications exposées sur Internet, etc.).
  - ▷ Risque d'utilisation des données techniques pour faciliter de futures cyberattaques (cartographie du système d'information, configurations, etc.).

> **REMARQUE**
>
> Si des données d'authentification ont fuitées, elle seront probablement utilisées pour réaliser d'autres incidents, qu'il convient de qualifier. Voir notamment Fiche réflexe - Compromission d'un compte de messagerie - Qualification ou Fiche réflexe - Compromission système - Qualification.

Action 3.c : (Conclure) Évaluer l'impact de la fuite de données

- ☐ *Quel type de données a fuité (métiers, personnelles ou contractuelles, authentification ou techniques) ?*
- ☐ *La fuite de données est-elle connue publiquement ? La presse, les clients et/ou les partenaires risquent-ils d'en être informés ?*
- ☐ *Quel est l'impact de cette fuite pour l'organisation (à court et long terme) ?*
- ☐ *Quel est l'impact sur l'organisation des mesures d'endiguement déjà prises ?*

Mesure 4 - Évaluer l'urgence à remédier la fuite de données

Action 4.a : Évaluer l'urgence à endiguer l'incident

- ☐ La fuite semble-t-elle passée ou en cours ?
- ☐ Une nouvelle fuite est-elle probable en l'état actuel ?
- ☐ Au-delà de la fuite de données, une compromission du système d'information est-elle probable ?
- ☐ Si la fuite concerne des données d'authentification, le risque immédiat d'intrusion ou de compromission est-il possible ?
- ☐ Un acte de malveillance non encore traité a-t-il les moyens de recommencer ?
- ☐ **Au final, l'attaque peut-elle encore évoluer et est-il urgent de la contenir ?**

Action 4.b : Évaluer l'urgence à rétablir les activités

- ☐ Si des mesures d'endiguement ont impacté des activités essentielles de l'organisation :
  - ☐ Une continuité d'activité en **mode nominal** a-t-elle été mise en oeuvre ?
  - ☐ Un maintien d'activité en **mode dégradé** a-t-il été mis en oeuvre ?
  - ☐ Si oui, combien de temps pourraient-elles tenir ?
- ☐ Des actions de restauration ont-elles déjà été entreprises ?
- ☐ **Au final, est-il urgent de rétablir les activités impactées ?**

Action 4.c : Évaluer l'urgence à communiquer

- ☐ Le système d'information affecté est-il soumis à une réglementation particulière (OSE, OIV, NIS2, DORA etc.) ?
  - ☐ Y a-t-il des délais pour déclarer l'incident (réglementation, assurance, etc.).
  - ☐ Prendre en compte les délais pour déclarer l'incident à son assurance et aux autorités (ex : délai de 72h pour effectuer une pré-déclaration de violation de données personnelles à la CNIL).
- ☐ Constater si les clients, les partenaires et/ou la presse sont informés.
  - ☐ Si la fuite est publique ou impacte les opérations extérieures, est-il urgent de communiquer de manière proactive ?
  - ☐ Est-il utile de préparer une communication réactive pour ne pas être pris de court en cas de sollicitation (de la part de partenaires, medias, etc.) ?

Action 4.d : (Conclure) Évaluer l'urgence à résoudre l'incident

- ☐ *L'attaque peut-elle encore évoluer et est-il urgent de la contenir ?*
- ☐ *Est-il urgent de rétablir les activités impactées ?*
- ☐ *Est-il urgent de communiquer sur la fuite de données ?*
- ☐ *Y a-t-il des délais urgents pour déclarer l'incident (réglementation, assurance, etc.) ?*

Qualifier l'incident

Conclure quant à la gravité de la fuite de données

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 :

- ☐ La fuite de données de mon organisation est-elle *confirmée* ?
- ☐ La fuite de données est-elle *circonscrite* à un système, ou a-t-elle une portée plus large ?
- ☐ La fuite de donnée a-t-elle un *impact fort* sur l'activité ou pouvant le devenir ?
- ☐ Est-il *urgent* d'agir pour endiguer la fuite de données ou rétablir des activités ?
- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?

    1. Anomalie courante
    2. Incident mineur
    3. Incident majeur
    4. Crise cyber

SUITE DES ACTIONS

Si la fuite de données est confirmée alors :

- Mettre en œuvre des **mesures d'endiguement** pour contenir la fuite de données.
  - Fiche suivante conseillée : Fiche réflexe - Fuite de données - Endiguement

Parallèlement, piloter la suite du traitement de cet incident. Il peut être utile de solliciter 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*.

⚠ ATTENTION

La fuite de données pouvait être l'objectif de l'attaque en soi (pour revente, espionnage ou atteinte réputationnelle). Néanmoins, elle peut être le préliminaire à d'autres incidents plus graves :

- Une exfiltration peut précéder une destruction des données et des serveurs par chiffrement (rançongiciel).
- Une exfiltration de données d'authentification et techniques peut donner lieur à une future intrusion sur le système d'information.
- Si la cause de la fuite est non traitée, l'incident pourra perdurer et devenir plus grave.

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 :
Fiches réflexes :

- Fiche réflexe - Compromission système - Qualification
- Fiche réflexe - Compromission système - Endiguement
- Fiche réflexe - Compromission d'un compte de messagerie - Qualification
- Fiche réflexe - Compromission d'un compte de messagerie - Endiguement
- Fiche réflexe - Compromission d'un tiers - Qualification
- Fiche réflexe - Compromission d'un tiers - Endiguement
- Fiche réflexe - Compromission d'un équipement réseau - Qualification
- Fiche réflexe - Compromission d'un équipement réseau - Endiguement
- Fiche réflexe - Fuite de données - Endiguement

Autres documents :

- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- 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.
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