

FICHE RÉFLEXE

Fuite de données

Qualification



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 ?

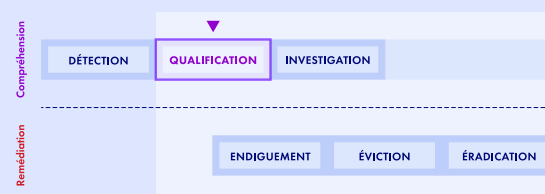
Deux parties principales composent cette fiche :

- 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) 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	3
Conclusions attendues de la qualification	4
Méthode d'évaluation pas à pas	6
Suite des actions	11
Annexes	12





PRÉREQUIS

Disposer des personnes nécessaires

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

- ▶ Les accès à l'administration et au monitoring du système d'information,
- ▶ Les accès aux équipements de sécurité du système d'information,
- ▶ La connaissance des priorités métier de l'organisation,
- ▶ L'annuaire de contacts d'urgence,
- ▶ 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 conclusions auxquelles doivent mener les évaluations, qui aboutiront à la qualification de l'incident. La partie suivante présentera des actions détaillées pour guider pas à pas ces évaluations.

Évaluer l'incident

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

- ☐ Le signalement reçu ou la revendication est-il crédible ?
- ☐ Un échantillon de la fuite de données est-il disponible ?
- ☐ Les données copiées sont-elles celles de mon organisation ou mon organisation est-elle simplement citée ?
- ☐ Les données fuitées sont-elles en réalité des données publiques ?
- ☐ S'il s'agit d'une suspicion d'exfiltration, y a-t-il des comportements anormaux sur mon système d'information ?

Mesure 2 - Identifier la source des données fuitées

- ☐ Les données fuitées sont-elles hébergées par mon organisation ou celle d'un tiers ?
- ☐ Si la fuite de données n'est pas confirmée, mais semble crédible, peut-on supposer l'origine de la fuite ?
- ☐ S'il y a une compromission ou suspicion de compromission en lien avec cette fuite de données, se référer aux fiches Compromission Système Qualification et Endiguement et aux fiches Compromission Messagerie Qualification et Endiguement

Mesure 3 - Évaluer le périmètre de la fuite de données

- ☐ De quelle nature sont les données ?
- ☐ Les données fuitées semblent-elles anciennes ou récentes ?
- ☐ Quelle est la quantité de données fuitées ?
- ☐ Est-ce qu'un volume plus important de données pourrait être publié par la suite ?
- ☐ Les autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque ?

Mesure 4 - Évaluer l'impact de la fuite de données

- ☐ Quel type de données a fuité ?
- ☐ Quelle est la gravité pour l'organisation (à court et long terme) ?
- ☐ Le système d'information affecté est-il soumis à une réglementation particulière (OSE, OIV, NIS2, DORA etc.) ?
- ☐ Peut-on savoir si le système d'information affecté stocke des données sensibles ?
- ☐ La fuite de données est-elle connue publiquement ? La presse, les clients et/ou les partenaires risquent-ils d'en être informés ?

Mesure 5 - Évaluer l'urgence à remédier la fuite de données

- ☐ L'exfiltration ou la fuite de données est-elle toujours en cours ?
- ☐ Suite à la fuite de données, un risque d'intrusion ou de compromission est-il à craindre ?
- ☐ Y a-t-il des délais pour déclarer l'incident (réglementation, assurance, etc.) ?
- ☐ Est-il urgent de communiquer sur la fuite de données ?

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 mon système d'information, ou est-elle étendue ?
- ☐ La fuite de données est-elle urgente à résoudre ?

Au final, quelle gravité représente cet incident de sécurité ?



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



MÉTHODE D'ÉVALUATION PAS À PAS

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

Évaluer l'incident

Mesure 1 - Confirmer la fuite de données

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

- ☐ S'il s'agit d'un signalement d'une fuite de données, est-ce : :
 - 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'il s'agit d'une suspicion d'exfiltration de données, y a-t-il :
 - Une alerte spécifique de mes équipements de sécurité (par exemple une règle DLP) ?
 - Une volumétrie réseau anormalement élevée ?

Action 1.b : Vérifier la crédibilité du signalement

- ☐ Confirmer si un échantillon de données fuitées est disponible et accessible.
- ☐ Vérifier si les données fuitées sont publiquement disponibles et s'assurer qu'il ne s'agit pas simplement de données publiques.
- ☐ Vérifier qu'il ne s'agit pas d'un regroupement de précédentes fuites publiées.
- ☐ 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.c : Déterminer si l'entité concernée est mon organisation ou un tiers

- ☐ Si les données fuitées sont publiées (tout ou en partie) :
 - Collecter l'ensemble des données mises à disposition et examiner les métadonnées pour identifier l'auteur et la date.
 - Vérifier si les données sont hébergées sur le système d'information de l'organisation.
 - ▷ Par exemple, via une recherche des noms des fichiers ou de leur contenu
 - ▷ 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 ?
 - Comparer les données collectées avec les données de référence de l'organisation pour vérifier les correspondances (l'échantillon de la fuite paraît-il correspondre à une base de données ou d'autres fichiers internes de l'organisation ?).
 - ▷ Ces données semblent-elles appartenir à l'organisation ?
 - ▷ L'organisation est-elle simplement citée ?
 - S'agit-il de données partagées avec un tiers (ex : contrat) ?
 - ▷ Si non, ces données semblent-elles appartenir à :
 - ☐ une organisation tierce identifiable (partenaire, client, fournisseur) ?
 - ☐ un tiers sans lien direct ?
- ☐ Si l'alerte est une suspicion d'exfiltration de données :



- Vérifier si des comportements inhabituels et anomalies de trafic ont été détectés via des outils de sécurité (par exemple : IDS, IPS, EDR, CASB, Proxy, Pare-feu, Anti-virus...).
- Y a-t-il des flux réseaux sortants importants et/ou anormaux ?
 - ▷ Si oui, est-ce un incident de production ou est-il nécessaire d'investiguer ?

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

- ☐ Le signalement reçu ou la revendication est-il crédible ?
- ☐ Un échantillon de la fuite de données est-il disponible ?
- ☐ Les données copiées sont-elles celles mon organisation ou mon organisation est-elle simplement citée ?
- ☐ Les données fuitées sont-elles en réalité des données publiques ?
- ☐ S'il s'agit d'une suspicion d'exfiltration, y a-t-il des comportements anormaux sur mon système d'information ?

Mesure 2 - Identifier la source des données fuitées

Action 2.a : Localiser l'origine des données

- ☐ 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,
 - ...
- ☐ Déterminer si les données proviennent d'un équipement interne ou d'un équipement externe par exemple :
 - un github ou gitlab public
 - un partage externalisé
 - un serveur web
 - un poste de travail professionnel ou personnel (BYOD)
 - le réseau interne
 - l'Active Directory
 - ...

Action 2.b : Identifier ce qui aurait permis la fuite de données

- ☐ Selon le temps disponible, examiner les journaux d'authentification, les accès suspects et les traces d'activité malveillante.
- ☐ Sur le(s) équipement(s) identifié(s) : analyser les journaux système, les configurations de sécurité et les règles d'accès.
- ☐ Déterminer si les données ont pu fuir via une mauvaise configuration d'un système ou d'une application (règles trop permissives, vulnérabilité connue, etc.).
- ☐ Déterminer s'il peut s'agir d'une compromission plus large qui aurait permis la fuite de données et corréliser avec les incidents en cours.

Action 2.c : Évaluer si la fuite de données est malveillante

- ☐ Évaluer si l'origine de la fuite est liée à une action humaine. Si oui, s'agit-il :
 - D'une fuite involontaire par un employé ou tiers autorisé (erreur humaine ou volonté de contourner le filtrage de l'organisation pour travailler) ?
 - D'une fuite intentionnelle par un employé ou tiers autorisé (acte de malveillance) ?
 - D'une fuite provoquée par un attaquant externe (exploitation de vulnérabilité, compromission de compte, etc.) ?

Action 2.d : (Conclure) Identifier la source des données fuitées

- ☐ Les données fuitées sont-elles hébergées par mon organisation ou celle d'un tiers ?
- ☐ Si la fuite de données n'est pas confirmée, mais semble crédible, peut-on supposer l'origine de la fuite ?
- ☐ S'il y a une compromission ou suspicion de compromission en lien avec cette fuite de données, se référer aux fiches Compromission Système Qualification et Endiguement



Mesure 3 - Évaluer le périmètre de la fuite de données

Action 3.a : Analyser la portée des données

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

- ☐ 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 ?
- ☐ Évaluer la quantité de données fuitées.

Action 3.b : Évaluer les risques d'une fuite de données plus étendue

- ☐ Vérifier si d'autres systèmes interconnectés à celui de l'organisation sont à risque.
- ☐ Évaluer la possibilité que la fuite de données soit plus étendue, en vérifiant par exemple :
 - Si d'autres données sont accessibles au même endroit.
 - Si l'accès au système où se trouvaient les données pourrait faciliter la connexion à des systèmes tiers.
- ☐ S'il s'agit d'une revendication, est-il mentionné que plus de données vont être publiées prochainement ?

Action 3.c : (Conclure) Évaluer le périmètre de la fuite de données

- ☐ De quelle nature sont les données ?
- ☐ Les données fuitées semblent-elles anciennes ou récentes ?
- ☐ Quelle est la quantité de données fuitées ?
- ☐ Est-ce qu'un volume plus important de données pourrait être publié par la suite ?
- ☐ Les autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque ?

Mesure 4 - Évaluer l'impact de la fuite de données

Action 4.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 (C3), diffusion restreinte (DR), secret (C4).
- ☐ Vérifier que l'attaque n'ait pas atteint les systèmes sensibles et/ou stratégiques.

Action 4.b : Évaluer les répercussions de la fuite

- ☐ Déterminer si la fuite ou les actions de réaction déjà entreprises impactent impacte les opérations de l'organisation (interruption de service, latence réseau, perte de données critiques).
- ☐ Déterminer les conséquences potentielles sur la confidentialité et l'intégrité en s'aidant de l'analyse de risque.
- ☐ Notoriété publique : 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.
- ☐ Risques médiatiques : 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.
- ☐ Impacts spécifiques selon le type de données :
 - ☐ Données métiers :
 - ▷ Répercussions économiques : pertes financières directes, perte d'avantage concurrentiel, interruption des activités (R&D). Quantifier les pertes, si possible.
 - ▷ Divulgaration 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 (divulgence 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, se référer aux fiches Compromission Système Qualification et Endiguement et aux fiches Compromission Messagerie Qualification et Endiguement.
- ▷ Risque d'utilisation des données techniques pour faciliter de futures cyberattaques (cartographie du système d'information, configurations, etc.).

Action 4.c : (Conclure) Évaluer l'impact de la fuite de données

- ☐ Quel type de données a fuité (métiers, personnelles ou contractuelles, authentification ou techniques) ?
- ☐ Quelle est la gravité pour l'organisation (à court et long terme) ?
- ☐ Le système d'information affecté est-il soumis à une réglementation particulière (OSE, OIV, NIS2, DORA etc.) ?
- ☐ Peut-on savoir si le système d'information affecté stocke des données sensibles ?
- ☐ La fuite de données est-elle connue publiquement ? La presse, les clients et/ou les partenaires risquent-ils d'en être informés ?

Mesure 5 - Évaluer l'urgence à remédier la fuite de données

Action 5.a : Évaluer le statut et l'évolution de la fuite

- ☐ Déterminer si la fuite de données est toujours active. Analyser les journaux système, les flux réseau et l'activité des utilisateurs identifiés précédemment.
- ☐ 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 Vulnerability Operations Center (VOC)).
- ☐ Si la fuite concerne des données d'authentification, évaluer le risque immédiat d'intrusion ou de compromission.
- ☐ S'il y a une compromission ou suspicion de compromission en lien avec cette fuite de données, se référer aux fiches Compromission Système Qualification et Endiguement

Action 5.b : Évaluer les risques futurs et la communication

- ☐ Compte tenu des éléments collectés ci-dessus, évaluer le risque de nouvelles fuites, d'intrusion ou de compromission.
- ☐ Constater si les clients, les partenaires et/ou la presse sont informés. Si la fuite est publique ou impacte les opérations extérieures, prioriser la communication.
- ☐ 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).

Action 5.c : (Conclure) Évaluer l'urgence à résoudre la fuite de données

- ☐ L'exfiltration ou la fuite de données est-elle toujours en cours ?
- ☐ Suite à la fuite de données, un risque d'intrusion ou de compromission est-il à craindre ? Si oui, se référer aux fiches Compromission Système, compromission messagerie et/ou compromission équipement bordure réseau¹.
- ☐ Y a-t-il des délais pour déclarer l'incident (réglementation, assurance, etc.) ?
- ☐ Est-il urgent de communiquer sur la fuite de données ?

1. voir les documents - <https://www.intercert-france.fr/publications/fichereflexe-compromissionsysteme-qualification> - <https://www.intercert-france.fr/publications/fichereflexe-compromissionsysteme-endiguement> - <https://www.intercert-france.fr/publications/fichereflexe-compromissionmessagerie-qualification> - <https://www.intercert-france.fr/publications/fichereflexe-compromissionmessagerie-endiguement> - <https://www.intercert-france.fr/publications/fichereflexe-compromissionequipementbordurereseau-qualification> - <https://www.intercert-france.fr/publications/fichereflexe-compromissionequipementbordurereseau-endiguement>



Qualifier l'incident

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

- ☐ La fuite de données de mon organisation est-elle *confirmée* ?
- ☐ La fuite de données est-elle circonscrite à mon système d'information, ou a-t-elle une portée plus large ?
- ☐ La fuite de données est-elle urgente à résoudre ?

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

- ☐ Anomalie courante
- ☐ Incident mineur
- ☐ Incident majeur
- ☐ 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 et demander de l'aide pour résoudre l'incident, en cohérence avec les impacts identifiés :
- ▶ Mettre en œuvre une gestion d'incident cyber pour piloter la résolution de l'incident.
 - Voir les annexes Contacts et Déclarations



ATTENTION

Une fuite de données peut être préliminaire à un chiffrement. Il est nécessaire d'arbitrer, s'agirait-il de : - une exfiltration pour revente ou espionnage - une exfiltration donnant suite à un chiffrement (rançongiciel), impactant plus lourdement mon organisation, auquel cas, se référer aux fiches Compromission Système Qualification et Endiguement - une malveillance interne ou erreur involontaire - une mauvaise configuration divulguant des données

Si une compromission sur le système d'information de son organisation ou sur le système d'information d'un tiers est suspectée, se référer aux fiches suivantes :

- ▶ 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



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 - Endiguement
- ▶ Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- ▶ Cyberattaques et remédiation

Définitions

Axes d'évaluation

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

Compromission d'un compte de messagerie

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

Compromission système

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

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

Degrés de gravité

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



Endiguer un incident

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

Fuite de données

Une *fuite de données*, également appelée *violation de données*, désigne un incident au cours duquel des informations confidentielles, sensibles ou protégées sont consultées, divulguées ou volées par une personne non autorisée. Cela peut concerner divers types de données, notamment des informations personnelles, financières, médicales, ou des secrets commerciaux.

Les fuites de données peuvent résulter de cyberattaques, comme le piratage ou le phishing, mais aussi d'erreurs humaines, telles que l'envoi d'informations à la mauvaise adresse e-mail ou la perte de dispositifs contenant des données sensibles. Les conséquences d'une fuite de données peuvent être graves, allant de pertes financières et d'atteintes à la réputation de l'entreprise à des problèmes juridiques et à la compromission de la vie privée des individus concernés.

Qualifier un incident

Qualifier un incident signifie :

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

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

Contacts

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

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les 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	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.