Fiche réflexe

Fuite de données

Endiguement

2026

Présentation de la fiche

1 À qui s'adresse-t-elle ?

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

2 Quand l'utiliser ?

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

3 À quoi sert-elle ?

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

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

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

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

Sommaire

Fiche réflexe – Fuite de données – Endiguement

Prérequis

01 Avoir qualifié l'incident

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

Fiche précédente conseillée : Fiche réflexe - Fuite de données - Qualification

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

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

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

02 Ouvrir une main courante

Dès le début de l'incident, ouvrir une **main courante** pour tracer toutes les actions et évènements 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.

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

Attaque par un acteur malveillant externe

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

Acte malveillant interne

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

Erreur humaine involontaire

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

Déclarer l'incident

Obligation de déclarer les incidents au CERT Santé

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

Contacts du CERT Santé

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

Procédure pour déclarer un incident

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

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** :

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 : Notifier les équipes RH et juridiques

- ☐ Envoyer un mail au manager/RH du collaborateur pour les informer que des investigations sont en cours suite à un comportement suspect identifié sur la machine ou le compte du collaborateur.

- ☐ Si la fuite semble malveillante, contacter les équipes RH et juridiques pour exposer la situation.

Action 1.b : Bloquer les accès du collaborateur

- ☐ Bloquer les accès physiques et logiques (compte LDAP, accès aux applications, etc.), notamment les accès aux canaux utilisés pour l'exfiltration (remarque : il est possible de mettre le compte sous surveillance active pour avoir une preuve en cas de 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.

Mesure 2 - Bloquer et superviser les flux d'exfiltration

Action 2.a : Bloquer les flux entrants et sortants

- ☐ Identifier les flux suspect puis 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, évaluer l'impact d'un blocage des flux avant de le réaliser, pour éviter de bloquer des flux métier légitimes et 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 puis restreindre les communications entre les différentes zones du réseau.
- ☐ S'il s'agit d'une compromission d'un tiers, veiller à couper les flux entre l'entreprise compromise et l'organisation.

Action 2.b : Mettre en place une surveillance renforcée

- ☐ Si les adresses IP d'exfiltration sont connues, les mettre en surveillance dans le SIEM pour générer une alerte.
- ☐ Générer des alertes ou rapports dans le SIEM sur les processus ou protocoles d'exfiltration (rClone.exe, rsync, flux FTP, ...).

- ☐ En se basant sur les équipements qui ont remonté l'alerte, renforcer la surveillance pour détecter et réagir rapidement à toute nouvelle tentative de fuite de données.
- ☐ Renforcer la politique de sécurité sur la partie exfiltration (par exemple : mise en place d'une GPO, modification du seuil d'alerte sur la volumétrie réseau, etc.).
- ☐ Créer des alertes DLP en se basant sur le cas d'usage.

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

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

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

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

- ☐ Vérifier l'implémentation de mesures de sécurité avancées sur les comptes à privilèges, comme l'authentification multifacteur (MFA), l'authentification biométrique ou l'utilisation de jetons de sécurité. S'ils n'en disposent pas,

implémenter cette mesure pour tous les comptes avec privilèges identifiés comme compromis.

- ☐ Mettre en place des contrôles d'accès renforcés pour les systèmes critiques comportant des données sensibles, y compris la revue des permissions et l'application des principes de moindre privilège.

Limiter l'exposition des données

Mesure 4 - Limiter l'exposition des données

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

- ☐ Si les données sont exposées en dehors de l'organisation :
  - ☐ Si les données sont disponibles sur un site public (GitHub, GitLab, commentaire sur un forum, etc.), demander au propriétaire (ou au webmaster) de supprimer ou restreindre l'accès aux données divulguées et garder la trace de la demande (en veillant à partager des preuves de ce qui est avancé). Remarque : Veiller à bien adapter la demande aux destinataires (le webmaster hacktiviste ne se comportera pas comme un webmaster journaliste).
  - ☐ Faire signer une décharge auprès du collaborateur ou tiers (sous-traitant, prestataire, partenaire) stipulant qu'il atteste avoir supprimé l'ensemble des données exfiltrées sur ses équipements personnels ainsi qu'un accord de non-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, route d'une API ou page d'un serveur web). Attention, il convient de couper l'accès au service et pas d'éteindre la machine (en effet, il est nécessaire de conserver la machine allumée pour les investigations).

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

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

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'attaquant, 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 - Communiquer en interne sur la fuite de données

Action 7.a : Communiquer en interne

- ☐ Fournir sous forme de synthèse exécutive une analyse de risques et les actions en cours liées à la fuite de données à sa hiérarchie, à 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 à l'externe de l'organisation, demander à la direction d'indiquer aux collaborateurs les éléments de langage et d'en informer la cellule qui s'occupe de la communication extérieure.
- ☐ Si des données classifiées (confidentielles, marquage DR ou autre) sont impactées, informer l'équipe dédiée qui gère ce type de données.

Action 7.b : Communiquer aux régulateurs

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

Mesure 8 - Communiquer publiquement sur la fuite de données

Action 8.a : Communiquer aux clients et partenaires

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

Action 8.b : Communiquer auprès de la presse

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

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

Définitions

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.

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.

Axes d'évaluation

- **Périmètre** : Le périmètre d'un incident désigne son étendue sur les composants du système d'information (comptes, applications, systèmes, etc.) et leur administration.
- **Impact** : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- **Urgence** : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Degrés de gravité

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

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.

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.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation		
CERT Santé	esante.gouv.fr/produits-servi... cyberveille.esante.gouv.fr	Pour les organisations du secteur de la santé
CERT/CSIRT externe en prestation de réponse à incident	www.cybermalveillance.gou... cyber.gouv.fr/offre-de-servic...	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance. Pour les organisations opérant un SI complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CERT-FR	www.cert.ssi.gouv.fr/contact	Pour les administrations et les Opérateurs d'importance vitale et de services essentiels
CSIRT régional	www.cert.ssi.gouv.fr/csirt/csi...	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations

Déclarations complémentaires

Selon le type de votre organisation et la nature de l'incident, des déclarations complémentaires peuvent être requises :

Qui ?	Comment ?	Pourquoi ?
ANSSI	www.cert.ssi.gouv.fr/contact	Pour les Opérateurs d'importance vitale (OIV) et les Opérateurs de services essentiels (OSE), la déclaration d'incident à l'ANSSI est obligatoire
CNIL	www.cnil.fr/fr/notifier-une-vi…	En cas de violation de données à caractère personnel, la notification à la CNIL est obligatoire dans les 72 heures
Dépôt de plainte	www.masecurite.interieur.go…	Déposer une plainte en ligne
	www.cybermalveillance.gou…	Signaler sur Cybermalveillance

Préparation

Pour une meilleure préparation à la gestion d'un incident de sécurité, il est conseillé de :

- Tenir à jour un **annuaire de contacts d'urgence** accessible même en cas d'indisponibilité du SI
- Préparer un **kit de réponse à incident** comprenant les outils et procédures nécessaires
- Réaliser des **exercices de gestion de crise** réguliers
- S'assurer que les **sauvegardes** sont fonctionnelles et testées
- Maintenir une **cartographie du SI** à jour

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 :

Document	Lien
Fiche réflexe - Fuite de données - Qualification	cyberveille.esante.gouv.fr/fuite-de-donnees-qualific...
Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique	messervices.cyber.gouv.fr/guides/crise-cyber-les-cle...
Guide ANSSI Cyberattaques et remédiation	cyber.gouv.fr/piloter-la-remediation-dun...

Licence