

Fiche réflexe

Compromission Équipement Bordure Réseau

Qualification

2026

Présentation de la fiche

1 A qui s'adresse-t-elle ?

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

2 Quand l'utiliser ?

Cette fiche peut être employée dans deux cas de figure :

- **en cas de suspicion ou détection de compromission** d'équipement de bordure réseau;
- si un de vos équipements de bordure réseau **est affecté par une vulnérabilité**.

Est désigné comme équipement de bordure réseau dans une organisation un équipement, physique ou virtuel, pouvant recevoir du trafic depuis internet et dont le rôle est d'acheminer du trafic entre le SI de l'organisation et internet. Ce type d'équipement inclut donc :

- **les pare-feu** en périmètre d'organisation ;
- **les passerelles VPN** ;
- **les routeurs d'entreprises ou box internet** pour de petites organisations.

3 A quoi sert-elle ?

L'objectif de cette fiche est de proposer une aide à la qualification d'une attaque de ce type. Les différentes actions proposées aideront à :

- **Confirmer** qu'un incident de sécurité est en cours, et qu'il s'agit bien de la compromission d'un équipement de bordure réseau,
- 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.

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Conclusions attendues de la qualification** qui 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 acceptées 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

Fiche réflexe – Compromission d'un équipement de bordure réseau – Qualification

○ Présentation de la fiche	2
○ Sommaire	3
○ Prérequis	4
○ Conclusions attendues de la qualification	5
○ Méthode d'évaluation pas à pas	7
◦ Evaluer l'incident	7
◦ Déclarer l'incident	13
◦ Qualifier l'incident	14
○ Suite des actions	15
○ Annexes	16

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 bordure** 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

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 **toutes 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 (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

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.

*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.

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 qui aideront à conduire pas à pas ces évaluations.

Évaluer l'incident

Mesure 1 - Confirmer la compromission de l'équipement réseau

- L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ?
- L'attaquant dispose-t-il d'un accès à l'OS de l'équipement ?

Mesure 2 - Évaluer le périmètre de l'incident

- L'incident est-il circonscrit à une partie du système d'information identifiable ?
- Les ressources d'administration ont-elles été compromises ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?
- D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils à risque ?

Mesure 3 - Évaluer l'impact de l'incident

- Des activités vitales sont-elles perturbées ?
- Y a-t-il des chaînes d'activité impactées dont la défaillance peut causer des perturbations graves ?
- La DSI a-t-elle les compétences en interne pour réinstaller l'équipement ou installer ses correctifs ?
- La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?

Mesure 4 - Évaluer l'urgence à résoudre l'incident

- Quelles sont les activités vitales dégradées ou menacées par cette compromission ?
L'attaquant est-il en position de les dégrader facilement ?
- L'attaquant dispose-t-il de droits étendus sur le SI ?
- L'attaquant peut-il être facilement évincé de l'équipement ?

Conclusions attendues de la qualification

Qualifier l'incident

Conclure quant à la gravité de l'incident

- L'incident est-il **confirmé** ?
- L'incident est-il **circonscrit** sur mon système d'information, ou est-il étendu ?
- L'incident présente-t-il un **impact** fort pour mon **activité métier** et le fonctionnement de mon **système d'information** ?
- L'incident est-il **urgent** à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

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

☐ **Crise cyber**

☐ **Incident majeur**

☐ **Incident mineur**

☐ **Anomalie courante**

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 l'incident

Évaluer les détections et les dysfonctionnements sur son système d'information permet d'acquérir de la connaissance sur le type de malveillance qui le menace et, dans le cas présent, de confirmer ou infirmer une compromission :

Action 1.a : Identifier l'équipement suspect

- ☐ Si le signalement provient d'une alerte interne (SIEM, EDR, Antivirus,...), disposez-vous de suffisamment d'informations complémentaires dans le signalement pour identifier l'équipement ?
- ☐ Si le signalement provient d'une alerte externe, et identifie l'équipement de bordure réseau par une adresse IP publique ou un nom de domaine
 - ☐ L'adresse IP appartient-elle bien à votre SI ?
 - ☐ L'adresse IP publique ou le nom de domaine signalé correspond-il directement à l'équipement réseau suspect ou à un relais ?
 - ☐ Disposez-vous de suffisamment d'informations complémentaires dans le signalement pour identifier l'équipement ?
 - ☐ Y a-t-il des journaux accessibles qui vous permettent d'identifier l'équipement compromis (journaux de répartiteur de charge,...) ?

Action 1.b : Trouver des traces de compromission

- ☐ En cas de vulnérabilité annoncée sur la marque de l'équipement, la version logicielle de l'équipement est-elle affectée ?
- ☐ Si le signalement indique des connexions réseau malveillantes vers l'équipement
 - ☐ Retrouvez-vous dans vos journaux réseau des traces de ces connexions ?
 - ☐ Retrouvez-vous dans les journaux système de l'équipement des actions malveillantes (connexions illégitimes à un compte, modifications malveillantes de configuration,...)
- ☐ Si le signalement mentionne l'exploitation d'une vulnérabilité spécifique
 - ☐ Retrouvez-vous des traces spécifiques à cette exploitation mentionnées dans les différents bulletins de sécurité à votre disposition ? Dans ceux du CERT-FR (cf la section Liens utiles) ? Dans vos abonnements sur la cyber-menace ?
- ☐ Trouvez-vous dans vos différents journaux des traces de connexions illégitimes initiées par l'équipement suspect à la période indiquée par le signalement ? Entre cette période et maintenant ?

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 1 – Confirmer l'incident

Remarque : Si la conclusion est que l'équipement n'est pas compromis mais est affecté par une vulnérabilité non corrigée, il est recommandé de continuer à répondre aux questions de cette fiche et d'appliquer les mesures correspondantes de la fiche d'endiguement (cf la section Liens utiles).

Action 1.c : (Conclure) Confirmer la compromission de l'équipement réseau

- ☐ L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ?
- ☐ L'attaquant dispose-t-il d'un accès à l'OS de l'équipement ?



Architecture d'équipement réseau

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 2 – Évaluer le périmètre de l'incident

Remarque : Deux niveaux de compromission de l'équipement sont possibles. Le premier niveau est un accès utilisateur i.e. l'attaquant peut accéder à des fonctionnalités de l'équipement normalement mises à disposition du client. Cela peut avoir lieu si l'attaquant dispose d'identifiants de comptes locaux à l'équipement par exemple, ou peut contourner les mécanismes d'authentification de l'équipement. Le deuxième est un accès interne à l'équipement, où l'attaquant est capable d'exécuter du code arbitraire sur l'équipement. Un accès interne est généralement plus grave qu'un accès légitime car il donne à l'attaquant une grande liberté d'action sur l'équipement et rend difficile son expulsion.

Action 2.a : Déterminer le niveau de compromission de l'équipement

- ☐ L'attaquant a-t-il un accès utilisateur ?
 - ☐ L'attaquant dispose-t-il de secrets d'authentification valides pour utiliser des fonctions de l'équipement ?
 - ☐ L'attaquant a-t-il accès à des fonctionnalités de l'équipement qui devraient être protégées par authentification ?
- ☐ Y a-t-il des soupçons d'un accès interne i.e. l'attaquant peut-il exécuter du code arbitraire sur l'équipement ?
 - ☐ Les actions malveillantes observées sont-elles réalisables via les fonctions d'administration de l'équipement accessibles à un utilisateur légitime ?
 - ☐ Si vous retrouvez des traces d'exploitation de vulnérabilité sur votre équipement, la vulnérabilité en question était-elle de type "exécution de code à distance" (RCE) ?
 - ☐ Y a-t-il eu récemment des bulletins d'alerte sur l'équipement à propos de vulnérabilités de type RCE ? Y a-t-il eu un bulletin d'alerte CERT-FR sur le sujet (cf la section Liens utiles) ?

Remarque : En cas de doute sur cette question, considérer que le niveau de compromission le plus grave i.e. accès interne est atteint.

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 2 – Évaluer le périmètre de l'incident

Action 2.b : Déterminer les accès réseau de l'attaquant

- ☐ A quels LAN internes l'équipement potentiellement compromis a-t-il accès ?
- ☐ Y a-t-il un filtrage mis en place pour limiter les flux réseau transitant par l'équipement ?
 - ☐ Si l'équipement a une fonction de passerelle VPN, un filtrage s'applique-t-il aux adresses IP assignées lors de connexions VPN ?
- ☐ Y a-t-il un filtrage mis en place pour limiter les flux réseau initiés par l'équipement ?
- ☐ S'il y a du filtrage en place, est-il effectué par l'équipement potentiellement compromis ?
 - ☐ Si oui, l'attaquant est-il en mesure de le désactiver/modifier ?
- ☐ L'attaquant dispose-t-il d'un accès à des SI appartenant à des tiers via son accès ?

Action 2.c : Déterminer les secrets hébergés par l'équipement réseau permettant un accès direct au SI

- ☐ Cela inclut mais ne se limite pas à
 - ☐ Des mots de passe de comptes locaux à l'équipement, notamment ayant des droits d'administrateur
 - ☐ Des secrets LDAP ou de comptes Active Directory, notamment privilégiés (administrateur de domaine,...)
 - ☐ Des mots de passe, certificats et clés de tunnels VPN
 - ☐ Des secrets d'infrastructure de gestion de clés (clés privées de certificats, d'autorité de certification,...)
 - ☐ Des communautés et clés SNMP

Action 2.d : Déterminer si d'autres équipements sont à risque

- ☐ L'organisation a-t-elle d'autres équipements de bordure réseau ?
- ☐ Sont-ils du même fabricant et sont-ils à jour ?
- ☐ Les secrets de l'équipement potentiellement compromis sont-ils partagés sur ces autres équipements ?

Action 2.e : (Conclure) Évaluer le périmètre de l'incident

- ☐ L'incident est-il circonscrit à une partie du système d'information identifiable ?
- ☐ Les ressources d'administration ont-elles été compromises ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?
- ☐ D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils à risque ?

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 3 – Évaluer l'impact de l'incident

Action 3.a : Évaluer les impacts sur le SI

- ☐ Les secrets de l'équipement considérés comme compromis donnent-ils des accès privilégiés au SI ?
- ☐ Quels seraient les impacts de la réutilisation de ces secrets ?
- ☐ Ces secrets compromis peuvent-ils être rapidement renouvelés ?

Action 3.b : Évaluer les impacts sur les activités métier

- ☐ Des données sensibles transitent-elles par cet équipement ?
- ☐ Y a-t-il des applications ou serveurs portant des activités métier essentielles pour votre entité accessibles par cet équipement ?
 - ☐ L'attaquant a-t-il accès à des données sensibles ?
 - ☐ L'attaquant a-t-il accès à des interfaces d'administration d'équipements critiques ?
- ☐ Vos activités essentielles peuvent-elles fonctionner en cas d'indisponibilité de l'équipement réseau ?
 - ☐ Fonctionneront-elles en mode dégradé ?
 - ☐ Ces activités sont-elles prises en compte dans un Plan de Continuité d'Activité ou un Plan de Reprise d'Activité ?

Action 3.c : (Conclure) Évaluer l'impact de l'incident

- ☐ Des activités vitales sont-elles perturbées ?
- ☐ Y a-t-il des chaînes d'activité impactées dont la défaillance peut causer des perturbations graves ?
- ☐ La DSI a-t-elle les compétences en interne pour réinstaller l'équipement ou installer ses correctifs ?
- ☐ La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 4 – Évaluer l'urgence à résoudre l'incident

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

- ☐ Quelles sont les activités vitales dégradées ou menacées par cette compromission ?
L'attaquant est-il en position de les dégrader facilement ?
- ☐ L'attaquant dispose-t-il de droits étendus sur le SI ?
- ☐ L'attaquant peut-il être facilement évincé de l'équipement ?

Méthode d'évaluation pas à pas

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** : <https://signalement.social-sante.gouv.fr/espace-declaration/profil>

Procédure pour déclarer un incident

- 1) Accéder au portail de signalement : <https://signalement.social-sante.gouv.fr/espace-declaration/profil>
- 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

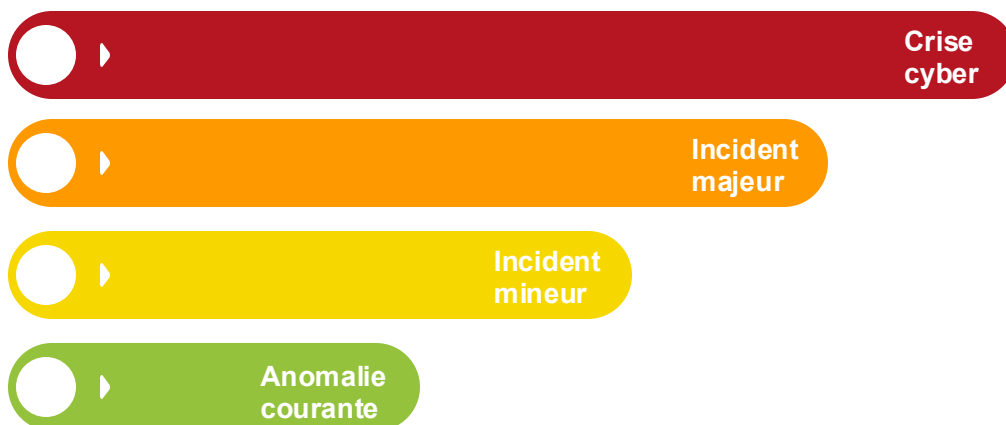
Méthode d'évaluation pas à pas

Qualifier 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 **compromission de l'équipement de bordure réseau** est-elle confirmée ?
- L'incident est-il **circonscrit** sur mon système d'information, ou est-il étendu ?
- L'incident présente-t-il un **impact fort pour mon activité métier** et le fonctionnement de mon **système d'information** ?
- L'incident est-il urgent à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

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



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

Suite des actions

Si l'incident est confirmé et qu'il s'agit bien d'une compromission d'équipement réseau, alors, en cohérence avec le **périmètre de compromission** évalué :

- Mettre en œuvre des mesures d'endiguement pour contenir l'attaque.
Fiche suivante conseillée : Fiche réflexe - *Compromission d'un équipement de bordure réseau - Endiguement*
[<https://cyberveille.esante.gouv.fr/compromission-equipement-de-bordure-qualification-et-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*.

De plus, si l'incident a un *périmètre étendu* sur le système d'information, qu'il a un *impact fort* et qu'il nécessite une résolution urgente :

- Activer le dispositif de **gestion de crise cyber** de l'organisation pour piloter la résolution de l'incident et la continuité d'activité.
Guide conseillé : *Crise cyber, les clés d'une gestion opérationnelle et stratégique* (cf la section Liens utiles)

Annexes

Définitions

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.

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.

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*.

Annexes

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		
CERT Santé	https://esante.gouv.fr/produits-services/cert-sante https://cyberveille.esante.gouv.fr/	Pour les organisations du secteur de la santé
CERT/CSIRT externe en prestation de réponse à incident	https://www.cybermalveillance.gouv.fr/diagnostic/accueil https://cyber.gouv.fr/produits-services-qualifies	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)
CERT-FR	https://www.cert.ssi.gouv.fr/contact	Pour les administrations et les Opérateurs d'importance vitale et de services essentiels
CSIRT régional	https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations

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.

Annexes

Déclarations complémentaires

Conjointement à la résolution de l'incident, des déclarations doivent être effectuées :

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.
	https://cyberveille.esante.gouv.fr/dossier-thematique/aide-au-depot-de-plainte-en-cas-dattaque-par-ranconciel	En cas d'attaque par rançongiciel
CNIL	https://www.cnil.fr/fr/notifier-une-violation-dedonnees-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.

Annexes

Préparation

En **prévention** d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être 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.

Préparation

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 – Compromission d'un équipement de bordure réseau – Endiguement (<https://cyberveille.esante.gouv.fr/compromission-equipement-de-bordure-qualification-et-endiguement>)
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique (<https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique>)
- Cyberattaques et remédiation (<https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber>)

Annexes

Licence

Ce document est dérivé des travaux du GT Fiches Réflexes de remédiation de l'InterCERT France.

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (<https://www.intercert-france.fr/>).

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