PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 29/08/2025
N° CERTFR-2025-RFX-001

Compromission d'un équipement de bordure réseau - Qualification

Fiche Réflexe

ANSSI/SDO
29/08/2025

Version : 1
Nombre de pages : 17

Table des matières

1 Présentation de la fiche **3**
- 1.1 À qui s'adresse-t-elle ? . . . 3
- 1.2 Quand l'utiliser ? . . . 3
- 1.3 À quoi sert-elle ? . . . 3
- 1.4 Comment l'utiliser ? . . . 3

2 Prérequis **4**
- 2.1 Disposer des personnes nécessaires . . . 4
- 2.2 Ouvrir une main courante . . . 4
- 2.3 Avoir pris connaissance des actions déjà entreprises . . . 5

3 Conclusions attendues de la qualification **5**
- 3.1 Évaluer l'incident . . . 5
- 3.2 Qualifier l'incident . . . 6

4 Méthode d'évaluation pas à pas **6**
- 4.1 Évaluer l'incident . . . 6
- 4.2 Qualifier l'incident . . . 11

5 Suite des actions **11**

6 Annexes **12**
- 6.1 Liens utiles . . . 12
- 6.2 Définitions . . . 12
- 6.3 Contacts . . . 14
- 6.4 Déclarations . . . 15
- 6.5 Préparation . . . 15
- 6.6 Contacter le CERT-FR . . . 16
- 6.7 Licence . . . 16

1 Présentation de la fiche

1.1 À qui s'adresse-t-elle ?

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

1.2 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

1.3 À 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 bien 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.

1.4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie Conclusions attendues de la qualification correspond aux questions auxquelles la qualification devra répondre.

CC BY-NC-SA 4.0

- 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.

2 Prérequis

2.1 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.

2.2 Ouvrir une main courante

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

CC BY-NC-SA 4.0

- 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.

2.3 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.

3 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 détaillera justement des actions détaillées qui aideront à conduire pas à pas ces évaluations.

3.1 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

CC BY-NC-SA 4.0

☐ *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 ?*

3.2 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 ?

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

4 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.

4.1 Évaluer l'incident

4.1.1 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* :

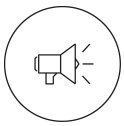
CC BY-NC-SA 4.0

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 ?*



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 ?*

CC BY-NC-SA 4.0

4.1.2 Mesure 2 - Évaluer le périmètre de l'incident

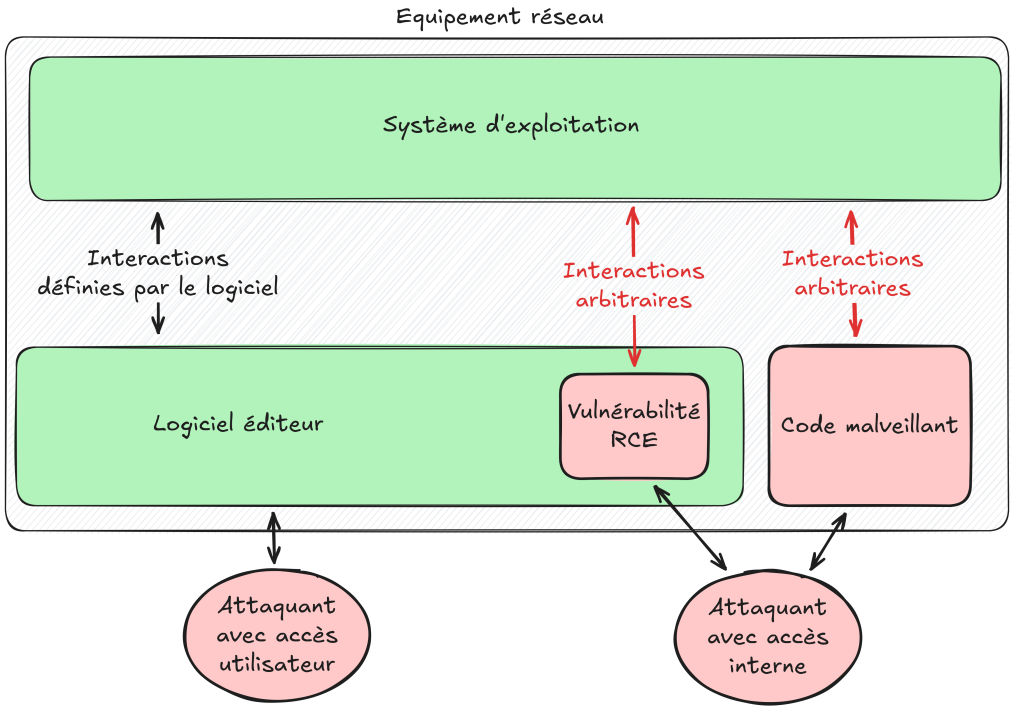
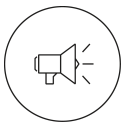


FIGURE 1 – Les différents niveaux de compromission



Remarque

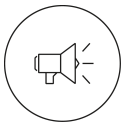
Deux niveaux de compromission de l'équipement, illustrés ci-dessus, sont possibles. Le premier niveau est un accès utilisateur i.e. l'attaquant peut accéder à des fonctionnalités de l'équipement normalement mises à disposition du client. Cela peut avoir lieu si l'attaquant dispose d'identifiants de comptes 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 ?*

CC BY-NC-SA 4.0

- ☐ *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.

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

- ☐ *A quels LAN internes l'équipement 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 soupçonné 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 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 soupçonné compromis sont-ils partagés sur ces autres équipements ?

CC BY-NC-SA 4.0

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 ?*

4.1.3 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 joignables 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.e : (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 ?*

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

CC BY-NC-SA 4.0

Action 4.a : (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 ?*

4.2 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 ?

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

5 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* (cf la section Liens utiles)

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*.

CC BY-NC-SA 4.0

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)

6 Annexes

6.1 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 - Compromission d'un équipement de bordure réseau - Endiguement	https ://cert.ssi.gouv.fr/fiche/CERTFR-2025-RFX-002
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
Guides ANSSI cyberattaques et remédiation	https ://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber
Bulletins d'alerte du CERT-FR	https ://www.cert.ssi.gouv.fr/alerte/

6.2 Définitions

6.2.1 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.

CC BY-NC-SA 4.0

6.2.2 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.

6.2.3 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.

6.2.4 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*.

6.2.5 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.

6.2.6 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

CC BY-NC-SA 4.0

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.

6.2.7 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.

6.3 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-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	Consulter la section Contacter le CERT-FR	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

CC BY-NC-SA 4.0

- 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.

6.4 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.

6.5 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.

CC BY-NC-SA 4.0

6.6 Contacter le CERT-FR



Attention

Quand vous effectuez un signalement auprès du CERT-FR, un numéro de référence vous est attribué. Pensez à rappeler ce numéro quand vous nous recontactez, ou dans l'entête de vos messages afin de simplifier le suivi du cas.

6.6.1 Par Téléphone

Le CERT-FR est joignable 7J/7, 24H/24 :

- depuis la France métropolitaine au **3218** (service gratuit + prix d'un appel) ou 09 70 83 32 18
- depuis certaines collectivités territoriales situées en Outre-mer ou depuis l'étranger au +33 9 70 83 32 18

6.6.2 Par Internet

- mèl : `cert-fr@ssi.gouv.fr`
- site : `https://cert.ssi.gouv.fr/contact/`

6.6.3 Clé PGP du CERT-FR

Pour vérifier l'intégrité des informations fournies ci-dessous, veuillez contacter le CERT-FR.

Identifiant de la clé : `0x1B45CF2A`

Empreinte de la clé : `7F4C 8FA6 A356 D1CC 2E5C AB09 5416 33B8 1B45 CF2A`

Télécharger la clé publique : `https://cert.ssi.gouv.fr/uploads/public_key_2024.asc`

6.7 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/publications/fiches-reflexes/`).

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

ANSSI/SDO
Version 1- UNDEF

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

cyber.gouv.fr