Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Chiffrement ou Effacement en cours

Qualification

InterCERT FRANCE

A qui s'adresse-t-elle ?

Public visé :

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

Quand l'utiliser ?

Utiliser cette fiche lorsqu'un logiciel malveillant de chiffrement ou d'effacement, par exemple de type rançongiciel, est détecté ou suspecté sur le système d'information.

A quoi sert-elle ?

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

- **Confirmer** qu'un incident de sécurité est bien en cours, et qu'il est de type **rançongiciel**,
- 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 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

PRÉREQUIS

☐ Avoir les 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

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 ayant réalisé cette action ou ayant informé sur l'évènement
3. La description de l'action ou de l'évènement et les machines concernées

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.

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

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type rançongiciel

- L'incident est-il confirmé ou nécessite-il des investigations complémentaires ? Est-il de type rançongiciel ?
- Le chiffrement a-t-il déjà été constaté ? Sinon, la menace demeure-elle suffisamment crédible ?

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 (comptes, postes, serveurs) ? 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 en risque ?

Mesure 3 - Évaluer l'impact de l'incident

- Quelles activités vitales sont perturbées ?
- Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?
- La DSI a-t-elle les compétences en interne pour reconstruire les systèmes d'information impactés ?
- 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 à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?
- Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?

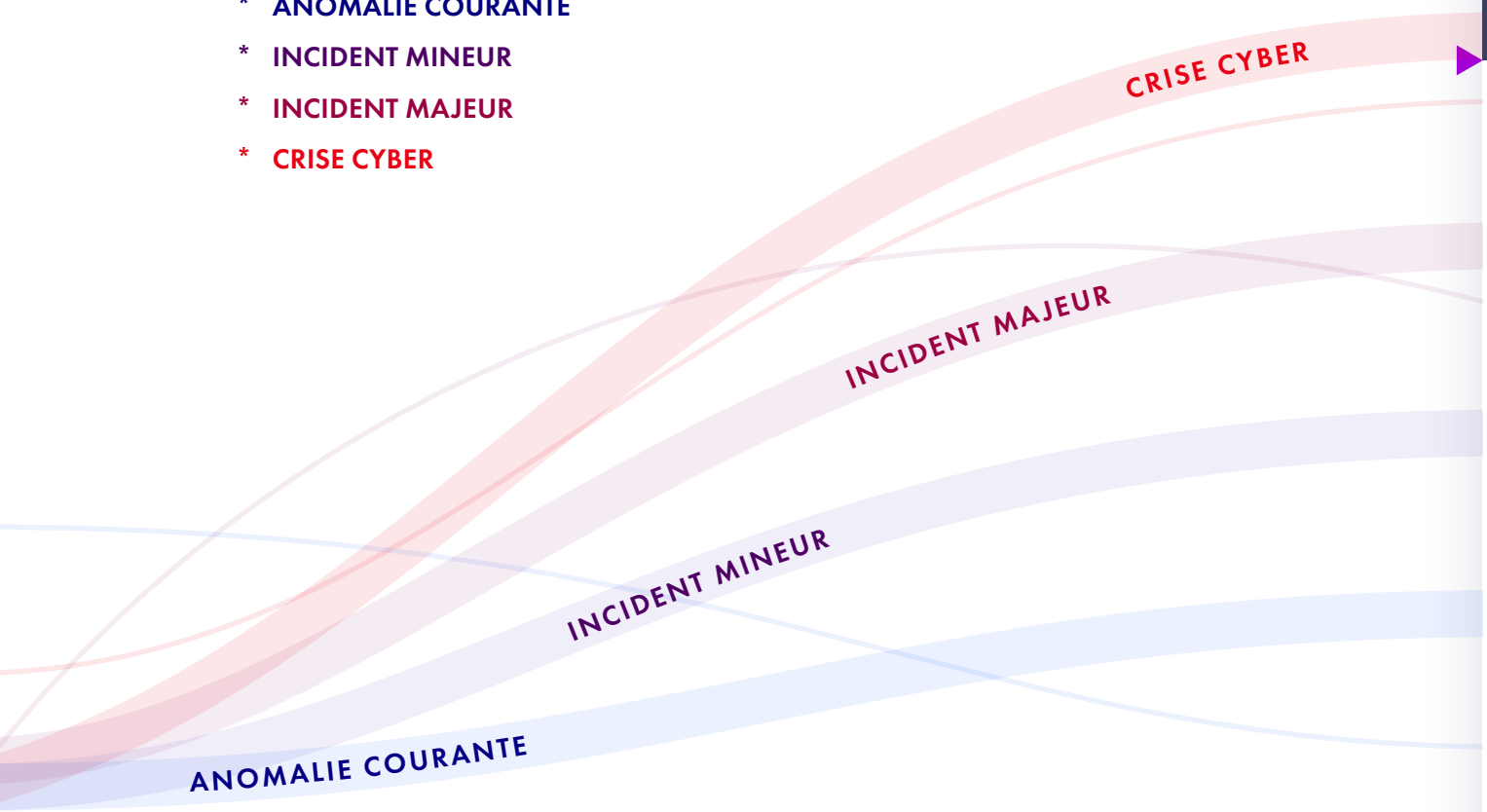
Qualifier l'incident

Conclure quant à la gravité de l'incident

- L'incident de type rançongiciel est-il **confirmé** ?
- L'incident est-il **circonscrit** sur mon système d'information, ou est-il étendu ?
- L'incident présente-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**



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 de type rançongiciel

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 une attaque de type rançongiciel** ou non :

Action 1.a : Évaluer la visibilité

Quels sont les moyens d'observations sur l'incident ?

- ☐ **Moyens de supervision** :
  - puits de logs ou SIEM
  - console antivirus ou EDR
  - console d'alertes des sondes réseaux ou des proxy web
- ☐ **Moyens de monitoring** : console de monitoring des serveurs et du trafic réseau
- ☐ **Vérification manuelle** : accès aux serveurs de fichiers et aux serveurs de sauvegardes
- ☐ **Signalements du SOC ou d'utilisateurs** en heures ouvrées

Action 1.b : Évaluer les signaux forts sur son système d'information

- ☐ Détection
  - Détection des outils de sécurité (antivirus et EDR)
  - Détection du SOC
  - Détection proactive via un scan de marqueurs positif
- ☐ Signalement d'utilisateurs
  - Signalement d'apparition d'une fenêtre, une pop-up ou un fichier demandant de payer une rançon (souvent nommé **README.txt**)
  - Signalement d'apparition de fichiers illisibles et avec des extensions anormales (**.encrypt**, **.abc**, **.aaa**, **.p5tkjw**, etc.)
  - Signalement de création d'archives en masse

Si aucun des signaux forts mentionnés ci-dessus n'est apparu, mais que vous avez des soupçons concernant un éventuel chiffrement en cours, analysez les dysfonctionnements typiques d'une attaque par rançongiciel :

Action 1.c : Évaluer les signaux faibles sur son système d'information

- ☐ Impossibilité d'accéder à des serveurs
- ☐ Indisponibilité de plusieurs services
- ☐ Impossibilité de lire des fichiers
- ☐ Désactivation de l'antivirus ou de l'EDR sur une portion significative du parc
- ☐ Extinctions de machines virtuelles en masse

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

Action 1.d : (Conclure) Confirmer l'incident de type rançongiciel

- ► **L'incident est-il confirmé ou nécessite-il des investigations complémentaires ? Est-il de type rançongiciel ?**
- ► **Le chiffrement a-t-il déjà été constaté ? Sinon, la menace demeure-elle suffisamment crédible ?**

IMPORTANT :

Si un chiffrement en cours est déjà constaté, envisager de réaliser les premières mesures d'endiguement selon la menace pressentie, en parallèle de la poursuite de la qualification.

Voir la partie Suite des actions

Mesure 2 - Évaluer le périmètre de l'incident

Action 2.a : Identifier le type de machines chiffrées

- ☐ Postes de travail ?
  - bureautique
  - métier ou opérationnel
- ☐ Serveurs ?
  - Windows
  - Linux
- ☐ Serveurs de stockage ?
  - Serveurs de fichiers (interne ou cloud)
  - Serveurs de sauvegardes
- ☐ Hyperviseurs ?
- ☐ Machines virtuelles ?
  - Fichiers chiffrés sur le système invité
  - Enveloppe de la machine virtuelle chiffrée sur l'hyperviseur
- ☐ Equipements embarqués ?

Action 2.b : Identifier le niveau de compromission

- ☐ Des comptes d'administration se sont-ils authentifiés sur le système d'information pendant les heures non ouvrées peu avant le chiffrement ?
- ☐ Des postes ou des serveurs d'administration ont-ils été chiffrés ?
- ☐ Des comptes illégitimes ont-ils été ajoutés au groupe **Administrateurs de domaine** ?

Action 2.c : Évaluer l'étendue de la compromission

- ☐ Quelles zones du système d'information contiennent des machines ayant des fichiers chiffrés ?
    - DMZ
    - Systèmes bureautiques
    - Systèmes métiers ou opérationnels
    - Systèmes d'administration
    - Systèmes de sauvegarde
    - Autres ?
- ☐ Les machines Windows chiffrées appartiennent-elles à plusieurs domaines Active Directory ou un seul ?
- ☐ Des mesures d'endiguement ont-elles déjà été entreprises ?
- ☐ Si oui, ont-elles permis d'arrêter la propagation ou l'incident semble-t-il se propager encore ?
- ☐ A quand remonte la 1ère anomalie constatée ?
    - Depuis quand l'incident semble-t-il avoir commencé ?

Action 2.d : Identifier les interconnexions

- ☐ Le système d'information est-il interconnecté avec d'autres systèmes d'information ?
- ☐ Quelles sont toutes les plateformes d'accès vers mon système d'information depuis l'extérieur ?

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

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 (comptes, postes, serveurs) ? 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 en risque ?**

Mesure 3 - Évaluer l'impact de l'incident

Action 3.a : Évaluer les impacts sur l'activité métier

- ☐ Quelles **activités métier** sont perturbées, à usage interne ou externe ?
    - Quelles activités perturbées sont **vitales** pour l'organisation ?
        - › Si votre organisation possède un BIA (Business Impact Analysis), ces activités perturbées en font-elles parties ?
    - Parmi les activités perturbées, certaines provoquent-elles une importante **perte financière** ?

Action 3.b : Évaluer les impacts réglementaires

- ☐ Le système d'information affecté est-il soumis à une réglementation particulière (OSE, OIV, etc.) ?
- ☐ Le système d'information affecté stocke-t-il des données sensibles ?
    - données classifiées
    - données personnelles
    - données à statut protégé : de santé, financières
    - données soumises à engagement contractuel ou réglementaire autre.

Action 3.c : Évaluer les impacts pour la reprise d'activité

- ☐ Quelles ressources informatiques support aux **activités vitales** identifiées ci-dessus ont été chiffrées ?
    - Les données ?
    - Les serveurs ?
- ☐ Quels **serveurs d'infrastructure critiques** pour le fonctionnement du système d'information ont été chiffrés ?
    - Contrôleur de domaine
    - DNS
    - Hyperviseur
    - Autres ?
- ☐ Y a-t-il encore des **postes d'administration** fonctionnels ?
- ☐ Les **serveurs de fichiers** ont-ils été chiffrés ?
    - Si oui, étaient-ils sauvegardés ?
- ☐ Concernant les **sauvegardes**...
    - Les sauvegardes ont-elles été chiffrées ?
    - Existe-il des sauvegardes hors ligne ?
    - Les sauvegardes saines sont-elles sur un site distant ou seraient-elles très longues à restaurer ?
    - L'infrastructure de restauration est-elle disponible et opérationnelle ?

Action 3.d : Évaluer les impacts des actions d'endiguement entreprises

- ☐ Des actions d'isolation ont-elles déjà été entreprises ? Si oui :
    - Des flux ont-ils été coupés ? Si oui :
        - › Sur quels équipements ?
    - Quelles sont les activités métiers qui en ont été impactées ?

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

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

- ► **Quelles activités vitales sont perturbées ?**
- ► **Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?**

- **La DSI a-t-elle les compétences en interne pour reconstruire les systèmes d'information impactés ?**
- **La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?**

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

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

Pour chacune des **activités vitales** impactées identifiées précédemment :

- ☐ Existe-il une procédure de continuité d'activité en mode nominal ?
- ☐ Existe-il une procédure de maintien d'activité en mode dégradé ?
- ☐ Si oui :
  - Ces procédures sont-elles déjà en cours de mise en œuvre ?
  - Combien de temps pourraient-elles tenir ?
- ☐ Des actions de restauration ont-elles déjà été entreprises ?

L'objectif des actions précédentes est finalement de vous aider à répondre au besoin d'évaluation suivant :

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

- **Quelles sont les activités vitales à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?**
- **Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?**

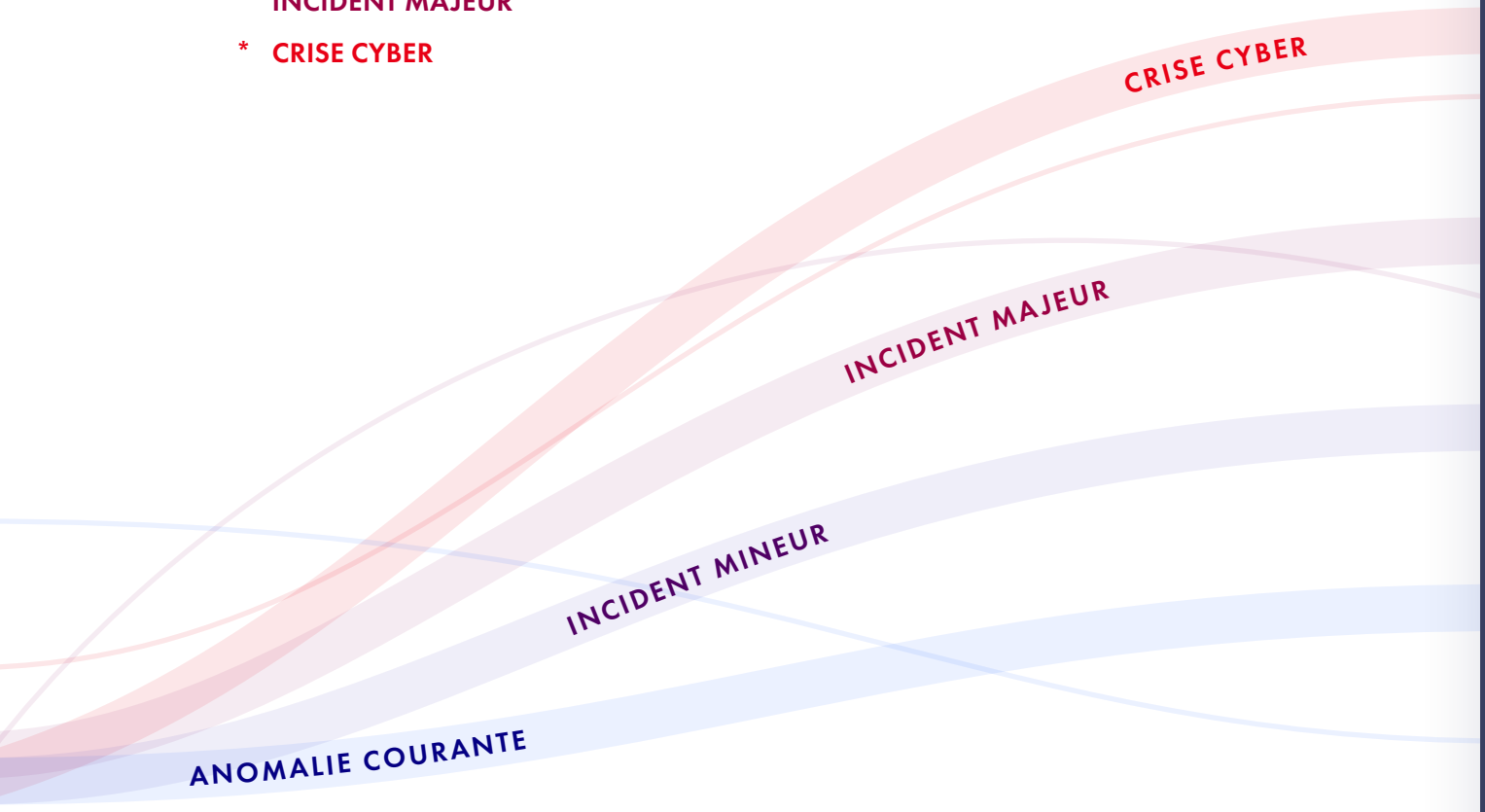
Qualifier l'incident

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 :

- L'incident de type rançongiciel est-il **confirmé** ?
- L'incident est-il **circonscrit** sur mon système d'information, ou est-il étendu ?
- L'incident présente-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**



SUITE DES ACTIONS

Si l'incident est confirmé et qu'il est de type rançongiciel 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 - Chiffrement ou effacement en cours - Endiguement *(https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-Chiffrement-Endiguement.pdf)*

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 *(https://cyber.gouv.fr/publications/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique)*

REMARQUE :

Dans le cas d'une attaque par rançongiciel, des aides spécifiques au dépôt de plainte sont mises à disposition par le CERT Santé, en collaboration avec le CSIRT-PJ : https://cyberveille-sante.gouv.fr/dossier-thematique/aide-au-depot-de-plainte-en-cas-dattaque-par-rancongiciel.

Lors du dépôt de plainte, le **Rapport Initial d'Incident** (**R2IP**) est à annexer systématiquement à la plainte. Le CSIRT-PJ peut vous accompagner dans cette démarche.

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 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.

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.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation		
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 *(https://www.cybermalveillance.gouv.fr/diagnostic/accueil)* Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS *(https://cyber.gouv.fr/produits-services-qualifies)*)
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 procédées :

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 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.

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 - Chiffrement ou effacement en cours - Endiguement (https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-Chiffrement-Endiguement.pdf)
- Comment réagir en cas d'incident rançongiciel (https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes)
- 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)

FICHE RÉFLEXE

L'InterCERT France fédère aujourd'hui plus de 100 CERTs sur le territoire national, constituant ainsi la 1ère communauté de CERTs en France.

Cette fiche réflexe est issue de la coopération et du partage d'expérience de plusieurs de ces CERTs. Elle a pour objectif d'être un outil efficace lors des premières étapes de gestion de l'incident en cours, en proposant des actions concrètes pour débuter le processus de remédiation.

Dans la même série, vous pouvez trouver :

Chiffrement ou effacement en cours	Qualification | Endiguement
Compromission d'un compte de messagerie	Qualification | Endiguement
Compromission système	Qualification | Endiguement
Défacement de site web	Qualification | Endiguement
Déni de service réseau	Qualification | Endiguement

Votre expérience dans le traitement d'un incident et l'utilisation de cette fiche est précieuse. Dans le but d'améliorer sa qualité, nous vous invitons à partager vos commentaires et suggestions d'amélioration, en nous contactant à l'adresse suivante :

fichesreflexes-remediation@intercert-france.fr