Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Défacement de site web

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 défacement est détecté sur un site web de l'organisation.

A quoi sert-elle ?

L'objectif de cette fiche est de proposer une aide à la qualification d'un défacement de site web. Les différentes actions proposées aideront à :

- **Confirmer** qu'un incident de sécurité est bien en cours, et qu'il est de type défacement de site web,
- Évaluer la **gravité** de l'incident en évaluant le périmètre affecté, l'impact potentiel sur 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 à l'administration** des serveurs web et des serveurs DNS
- Les **accès aux équipements de sécurité** en amont du site web

Si le système d'information est **infogéré**, ou si le site web est **hébergé** chez un tiers, s'assurer de la capacité à mobiliser leur support technique dans l'urgence. Il aura non seulement les capacités opérationnelles pour agir, et pourra sans doute faire bénéficier de son expérience sur ce type d'incident.

☐ 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 présentera des actions détaillées pour guider pas à pas ces évaluations.

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type défacement de site web

- L'incident de type défacement de site web est-il confirmé, ou nécessite-il des investigations complémentaires ?

Mesure 2 - Identifier les systèmes compromis

- Les serveurs hébergeant le site web défacé peuvent-ils être précisément identifiés ? Sont-ils internes ou externes à l'organisation ?
- Les serveurs hébergeant le site web défacé ont-ils été eux-mêmes compromis ? Si non, quel système tiers semble avoir été compromis (enregistrement DNS, fournisseur de contenu tiers, équipement en amont) ?
- Les systèmes compromis ont-ils pu être identifiés ou des investigations complémentaires sont-elles encore nécessaires ?

Mesure 3 - Évaluer le périmètre de l'incident

- Un compte d'administration a-t-il été usurpé ? Si oui, peut-il accéder à des serveurs plus sensibles que les serveurs web ?
- Le site web compromis est-il hébergé en interne ? Si oui, la compromission est-elle identifiable sur d'autres sites ?
- Les autres systèmes d'information interconnectés avec le serveur hôte sont-ils en risque ?

Mesure 4 - Évaluer l'impact de l'incident

- Quelles activités sont impactées par le défacement ? Sont-elles vitales ?
- Quelles activités seraient impactées par la mise hors-ligne du site web ou du serveur hôte ?
- Quelles contraintes réglementaires sont impactées ?

Mesure 5 - Évaluer l'urgence à résoudre l'incident

- Quelles sont les activités vitales perturbées, pour lesquelles des mesures préventives de maintien d'activité doivent être envisagées ?
- L'incident est-il à risque de généralisation imminente ?

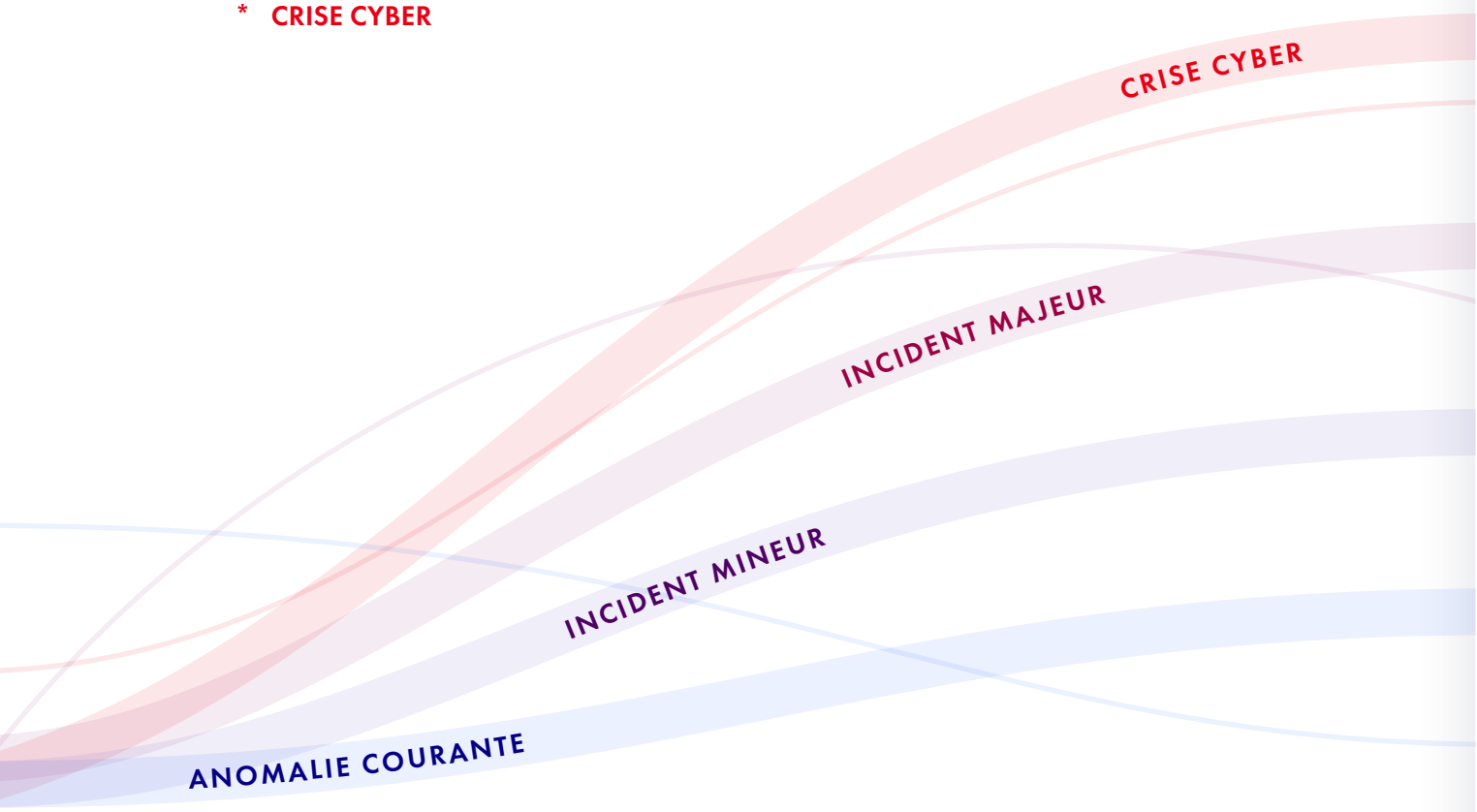
Qualifier l'incident

Conclure quant à la gravité de l'incident

- Le défacement du site web est-il causé par une compromission du site web lui-même ?
- 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

Un **défacement de site web** a principalement 7 causes :

Compromission du site web :

1. Usurpation d'un compte de gestion du site web ou d'un compte d'administration de son serveur hôte
2. Sabotage délibéré d'un employé interne
3. Exploitation d'une vulnérabilité (XSS, injection SQL, etc.), affectant le site web lui-même, un de ces composants (plugin, bibliothèque tierce), ou son moteur de gestion

Compromission d'un système tiers :

4. Compromission d'un site tiers, dont la page web importe du contenu (javascript, etc.)
5. Compromission des enregistrements DNS qui redirigent le trafic vers un serveur contrôlé par l'attaquant
6. Compromission d'un équipement en amont du serveur web
7. Compromission globale du système d'information ou de l'hébergeur

Cette fiche doit permettre de qualifier l'incident malgré la diversité des causes possibles.

Mesure 1 - Confirmer l'incident de type défacement de site web

Confirmer que l'incident est de type **défacement de site web** en évaluant différents signaux :

Action 1.a : Évaluer les signaux forts

- ☐ Changement illégitime de la page d'accueil
- ☐ Changements illégitimes dans le contenu du site (images ou messages inappropriés, informations falsifiées, liens malveillants, etc.)
- ☐ Affichage de contenus externes inappropriés (bannière de publicité, etc.)
- ☐ Apparition du site web sur une liste noire (**Google Safe Browsing**, **Microsoft Defender SmartScreen**, etc.)
- ☐ Revendication de l'attaque au nom d'un activisme politique ou religieux
    - Depuis quand ces premiers signaux forts sont-ils apparus ?

Action 1.b : Évaluer les signaux faibles

- ☐ Notifications des utilisateurs (sur le site web ou les réseaux sociaux)
- ☐ Augmentation soudaine de commentaires négatifs sur le site web
- ☐ Alertes antivirales sur le serveur hôte
- ☐ Baisse soudaine du trafic sur le site web (potentiellement due à son apparition dans une liste noire)

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

Action 1.c : (Conclure) Confirmer l'incident de type défacement de site web

► **L'incident de type défacement de site web est-il confirmé, ou nécessite-il des investigations complémentaires ?**

Mesure 2 - Identifier les systèmes compromis

Examiner si les serveurs hôtes ont eux-mêmes été compromis, ou au contraire semblent être restés intègres :

Action 2.a : Identifier le site web défacé

- ☐ Quel est le nom qualifié (**FQDN**) du site web victime du défacement ?
- ☐ Quelle page du site web est impactée ?
    - Y a-t-il d'autres pages également impactées ?
- ☐ Le défacement est-il visible sur d'autres sites web de l'organisation ?

Action 2.b : Identifier les serveurs hébergeant le site défacé

- ☐ Les serveurs hébergeant le site web défacé sont-ils hébergés :
    - chez un hébergeur externe (**cloud**, etc.) ?
    - sur le système d'information de l'organisation ? Si oui :
        - › dans une DMZ dédiée du système d'information de l'organisation ?
- ☐ Combien de serveurs hébergent le site web (**cluster**, etc.) ?

Action 2.c : Confirmer ou non la compromission des serveurs hôtes

- ☐ La page défacée du site web est-elle bien présente sur les disques du ou des serveurs hôtes ?
    - Si oui, combien de serveurs sont affectés ? (un seul ? tout le cluster ?)
    - Si non, peut-on confirmer que le site web est bien intègre et que les serveurs web ne sont pas compromis ?

Si les serveurs web semblent être intègres et non compromis, il se peut que la compromission ait ciblé un système tiers...

Examiner si les enregistrements DNS pointent vers un site illégitime :

Action 2.d : Examiner l'enregistrement DNS du site web

- ☐ En effectuant une résolution DNS du FQDN du site web défacé, l'enregistrement obtenu pointe-t-il vers une adresse IP appartenant à l'organisation ? Si non :
    - Les enregistrements DNS de l'organisation ont-ils été modifiés peu avant le défacement, et pointent-ils vers des adresses IP illégitimes ?
    - Les serveurs DNS sont-ils internes ou externes à l'organisation ?
        - › S'ils sont internes, identifier précisément ces serveurs

Si les enregistrements DNS semblent intègres, investiguer si un lien contenu dans la page pointe vers du contenu externe et semble contenir le contenu illégitime (au besoin, utiliser les outils développeur intégrés dans le navigateur web) :

Action 2.e : Investiguer si le contenu illégitime provient d'un fournisseur tiers

☐ Le contenu illégitime provient-il d'un contenu tiers pointé par un lien légitime de la page défacée ?

- javascript
- image
- etc.

Enfin, si aucun système n'a encore été identifié compromis, remonter la chaîne des équipements qui transportent le flux web afin de trouver celui qui cause le défacement :

Action 2.f : Trouver l'équipement à l'origine du défacement en amont des serveurs web

Procéder à des tests unitaires pour afficher la page défacée en remontant le flux web, puis identifier l'équipement responsable du défacement :

☐ Répartiteur de charge
☐ Reverse-proxy
☐ Pare-feu
☐ Autre ?

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

Action 2.g : (Conclure) Identifier les systèmes compromis

- **Les serveurs hébergeant le site web défacé peuvent-ils être précisément identifiés ? Sont-ils internes ou externes à l'organisation ?**
- **Les serveurs hébergeant le site web défacé ont-ils été eux-mêmes compromis ? Si non, quel système tiers semble avoir été compromis (enregistrement DNS, fournisseur de contenu tiers, équipement en amont) ?**
- **Les systèmes compromis ont-ils pu être identifiés ou des investigations complémentaires sont-elles encore nécessaires ?**

Si ce sont les **serveurs hébergeant le site web** qui ont été identifiés compromis, continuer cette fiche avec la partie suivante.

Sinon, si un **système tiers** semble être la cause du défacement (enregistrement DNS, fournisseur de contenu tiers, équipement en amont), voir directement la partie Suite des actions.

Mesure 3 - Évaluer le périmètre de l'incident

Action 3.a : Investiguer une usurpation d'accès d'administratif

☐ Une authentification avec un compte d'administration a-t-elle été réalisée illégitimement sur l'interface de gestion peu avant le défacement (interface du CMS / service d'hébergement / SFTP / base de données exposées) ? Si oui :

- Les logs permettent-ils de confirmer la modification illicite effectuée par ce compte, causant le défacement ?

Action 3.b : Évaluer la potentielle compromission du serveur web

☐ Détection :

- Des alertes antivirales sur les serveurs hôtes ont-elles détecté du dépôt de code malveillant ?
- Des alertes sur les équipements de sécurité en amont du site web (WAF, IPS, etc.) ont-elles détecté des tentatives d'exploitation de vulnérabilité, peu avant le défacement ?

☐ Investigation :

- A partir de l'identification des versions des composants (site web, plugins, bibliothèques, système d'exploitation), existe-t-il des vulnérabilités connues (CVE) qui permettraient ce défacement ?

Action 3.c : Évaluer la potentielle propagation de la compromission

☐ Le site web est-il hébergé par l'organisation ? Si oui :

- Plusieurs sites web hébergés par les mêmes serveurs hôtes sont-ils défacés également ?
- Des alertes d'exécution de commande ou de codes malveillants sont-elles remontées par l'antivirus ou l'EDR les serveurs hôtes ?
- Les serveurs hôtes sont-ils cloisonnés ou peuvent-ils joindre d'autres serveurs de l'organisation ?
- Le site web contient-il des mots de passe réutilisables sur d'autres systèmes du système d'information ?

☐ Si un compte administratif a été identifié usurpé :

- Des connexions illégitimes avec le même compte ont-elles réussies sur d'autres interfaces ?
- Combien de sites web peuvent être gérés par ce compte ?
- Combien de serveurs du système d'information sont administrables par ce compte ?

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

Action 3.d : (Conclure) Évaluer le périmètre de l'incident

- **Un compte d'administration a-t-il été usurpé ? Si oui, peut-il accéder à d'autres serveurs, plus sensibles que les serveurs web ?**
- **Le site web compromis est-il hébergé en interne ? Si oui, la compromission est-elle identifiable sur d'autres sites ?**
- **Les autres systèmes d'information interconnectés avec le serveur hôte sont-ils en risque ?**

Mesure 4 - Évaluer l'impact de l'incident

Action 4.a : Évaluer les impacts sur l'activité

- ☐ Le défacement a-t-il un impact sur l'activité de l'organisation en ce qui concerne :
  - une interruption de l'activité métier ?
  - l'atteinte à l'image de marque ?
  - une perte financière ?
- ☐ Y aurait-il un fort impact sur une des activités ci-dessus :
  - si le site web devait être mis hors-ligne ?
  - si le serveur hôte hébergeant le site web devait être isolé d'Internet ou éteint ?
    - › D'autres sites web ou d'autres services seraient-ils alors impactés ?
- ☐ Une **activité vitale** pour l'organisation est-elle liée au site web ou au serveur hôte ?
  - Si votre organisation possède un BIA (Business Impact Analysis), cette activité perturbée en fait-elle partie ?

Action 4.b : Évaluer les impacts réglementaires

- ☐ Les serveurs compromis sont-ils reliés à un système d'information soumis à une **réglementation particulière** (OSE, OIV, NIS2, etc.) ?
- ☐ Peut-on savoir si le serveur compromis stocke des données sensibles ?
  - données classifiées
  - données personnelles
  - données à statut protégé (santé, financières, etc.)
  - données soumises à engagement contractuel ou réglementaire autre

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

Action 4.c : (Conclure) Évaluer l'impact de l'incident

- ► **Quelles activités sont impactées par le défacement ? Sont-elles vitales ?**
- ► **Quelles activités seraient impactées par la mise hors-ligne du site web ou du serveur hôte ?**
- ► **Quelles contraintes réglementaires sont impactées ?**

Mesure 5 - Évaluer l'urgence à résoudre l'incident

Action 5.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 5.b : (Conclure) Évaluer l'urgence à résoudre l'incident

- ► **Quelles sont les activités vitales perturbées, pour lesquelles des mesures préventives de maintien d'activité doivent être envisagées ?**
- ► **L'incident est-il à risque de généralisation imminente ?**

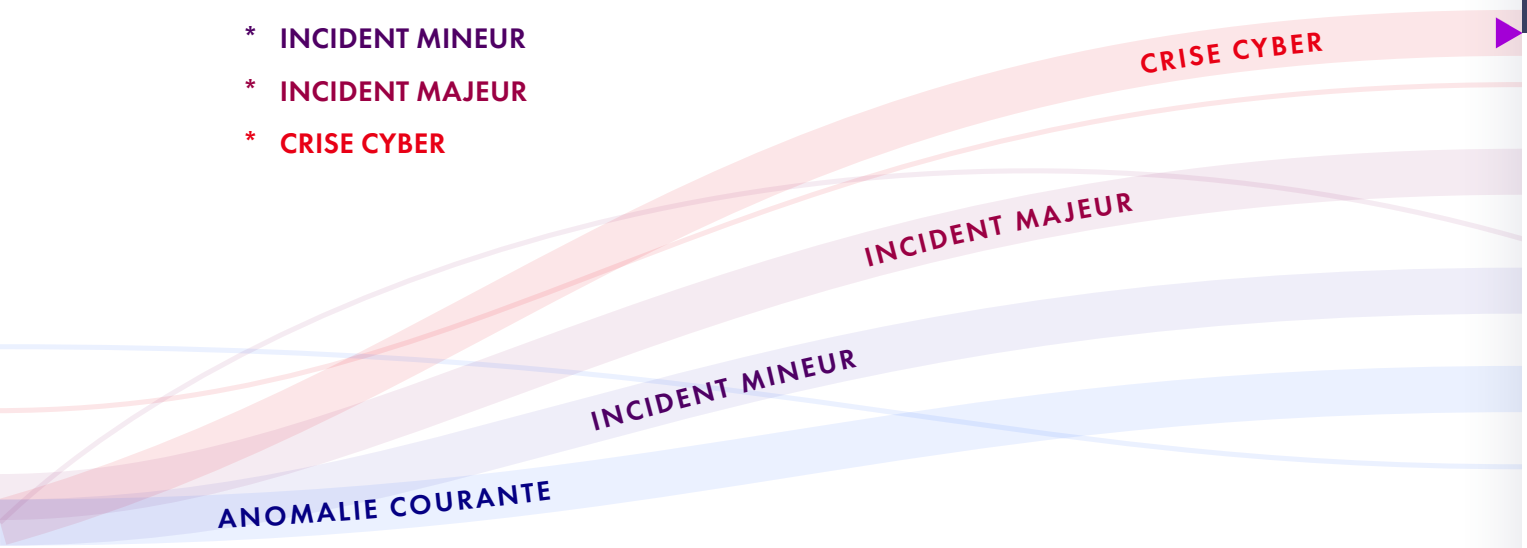
Qualifier l'incident

Conclure quant à la gravité de l'incident

- ► Le défacement du site web est-il causé par une compromission du site web lui-même ?
- ► L'incident est-il **circonscrit** sur mon système d'information, ou est-il étendu ?
- ► L'incident est 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 le défacement du site web est causé par une compromission du site web lui-même :

- Mettre en œuvre des **mesures d'endiguement** pour contenir l'attaque.
  - Fiche suivante conseillée : Fiche réflexe - Défacement de site web - Endiguement *(https:/www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-DefacementWeb-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.

Dans toutes les autres situations, des exemples de mesures d'endiguement sont suggérés ci-dessous :

Si les **enregistrements DNS** ont été compromis :

- Si le service DNS est externalisé, réinitialiser tous les accès d'administration et reconfigurer les enregistrements DNS légitimes.
- Si le serveur DNS est interne à l'organisation, utiliser en plus la fiche suivante : Fiche réflexe - Compromission système - Qualification *(https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-CompromissionMessagerie-Qualification.pdf)*

Si le contenu illégitime provient d'un **fournisseur tiers** identifié :

- Rendre inopérant tous les liens vers ce fournisseur dans les pages du site (supprimer, commenter ou renommer) et prévenir que le site fonctionne en mode dégradé. Entre-temps, une page de maintenance peut être affichée.
- Prendre en compte que cette mesure ne sera pas efficace tout de suite à cause de la mise en **cache** des pages web.

Si un **système en amont** des serveurs web est suspecté compromis :

- Mettre en ligne une page de maintenance sur un autre serveur et y rediriger les résolutions DNS.
- Utiliser en plus la fiche suivante sur le système suspecté compromis : Fiche réflexe - Compromission système - Qualification *(https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-CompromissionMessagerie-Qualification.pdf)*

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 - Défacement de site web - Endiguement *(https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-DefacementWeb-Endiguement.pdf)*
- 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