Fiche réflexe

Déni de service

Endiguement

2025

CC BY-NC-SA 4.0

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 ?

Utiliser cette fiche lorsqu'un incident de type **déni de service réseau est détecté ou suspecté** contre un ou plusieurs services de votre organisation exposés sur Internet.

3 A quoi sert-elle ?

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

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Actions d'endiguement par priorités** pointe l'ordre prioritaire des actions détaillées dans la partie suivante.
- La partie **Actions d'endiguement par périmètre et type de déni de service** détaille les différentes actions d'endiguement possibles selon 4 axes thématiques.

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

CC BY-NC-SA 4.0

Sommaire

Fiche réflexe
- Compromission système -
Endiguement

- Présentation de la fiche 2
- Sommaire 3
- Prérequis 4
- Actions d'endiguement par priorités 5
- Actions d'endiguement par périmètre et type de déni de service 6
  - Déclarer l'incident 6
  - Sélectionner les actions appropriées 9
  - Limiter les impacts 11
  - Préserver les traces 18
- Suite des actions 19
- Annexes 20

CC BY-NC-SA 4.0

Prérequis

01

Avoir qualifié l'incident

Avoir **qualifié** que l'incident de type déni de service réseau ne soit pas un incident de production, mais soit bien la conséquence d'un acte malveillant, et avoir évalué sa gravité. Avoir établi les caractéristiques de l'attaque et l'élément défaillant de la chaîne :

Fiche précédente conseillée : Fiche réflexe – Déni de service réseau - Qualification

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

02

Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement aient les **droits d'administration** du système d'information (réseau, système, sécurité opérationnelle) et que les acteurs externes **en capacité de faire les actions soient identifiés et puissent être sollicités**.

03

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.

CC BY-NC-SA 4.0

Actions d'endiguement par priorités

Cette partie pointe l'ordre prioritaire des actions détaillées dans la partie suivante :

Actions	Priorité
Déclarer l'incident	P0
Ordonner vos actions dans le périmètre défini et sélectionner les mesures en fonction des caractéristiques du déni de service (Mesure 1)	P0
Limiter le trafic en amont de l'entité (avec le FAI) (Mesure 2)	P1
Activer le service anti-DDoS externe, si possible (Mesure 4 - Action 4.d)	P1
En cas d'attaque sur les services DNS : agir sur les configurations (Mesure 4 - Action 4.a)	P1
En cas d'attaque sur les applications : activer le CDN (Content Delivery Network) si possible (Mesure 4 - Action 4.b)	P1
Agir dans le périmètre de l'hébergeur (Mesure 3)	P2
Agir sur les composants tiers (Mesure 4 Action 4.c)	P3
Préserver les traces des journaux d'équipements (Mesure 5)	P4

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

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

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Cette partie détaille les différentes mesures d'endiguement possibles selon 3 axes thématiques. Chaque **mesure** est ensuite scindée en **actions unitaires** :

❑ Sélectionner les actions appropriées
- Mesure 1 - Ordonner vos actions dans le périmètre défini et sélectionner les mesures en fonction des caractéristiques du déni de service

❑ Limiter les impacts
- Mesure 2 - Limiter le trafic en amont de l'entité (avec le FAI)
- Mesure 3 - Agir dans le périmètre de l'hébergeur
- Mesure 4 - Agir dans le périmètre des services dépendants

❑ Préserver les traces
- Mesure 5 - Préserver les traces

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités ! Pour cela, se référer à la précédente partie **Actions d'endiguement par priorités**.

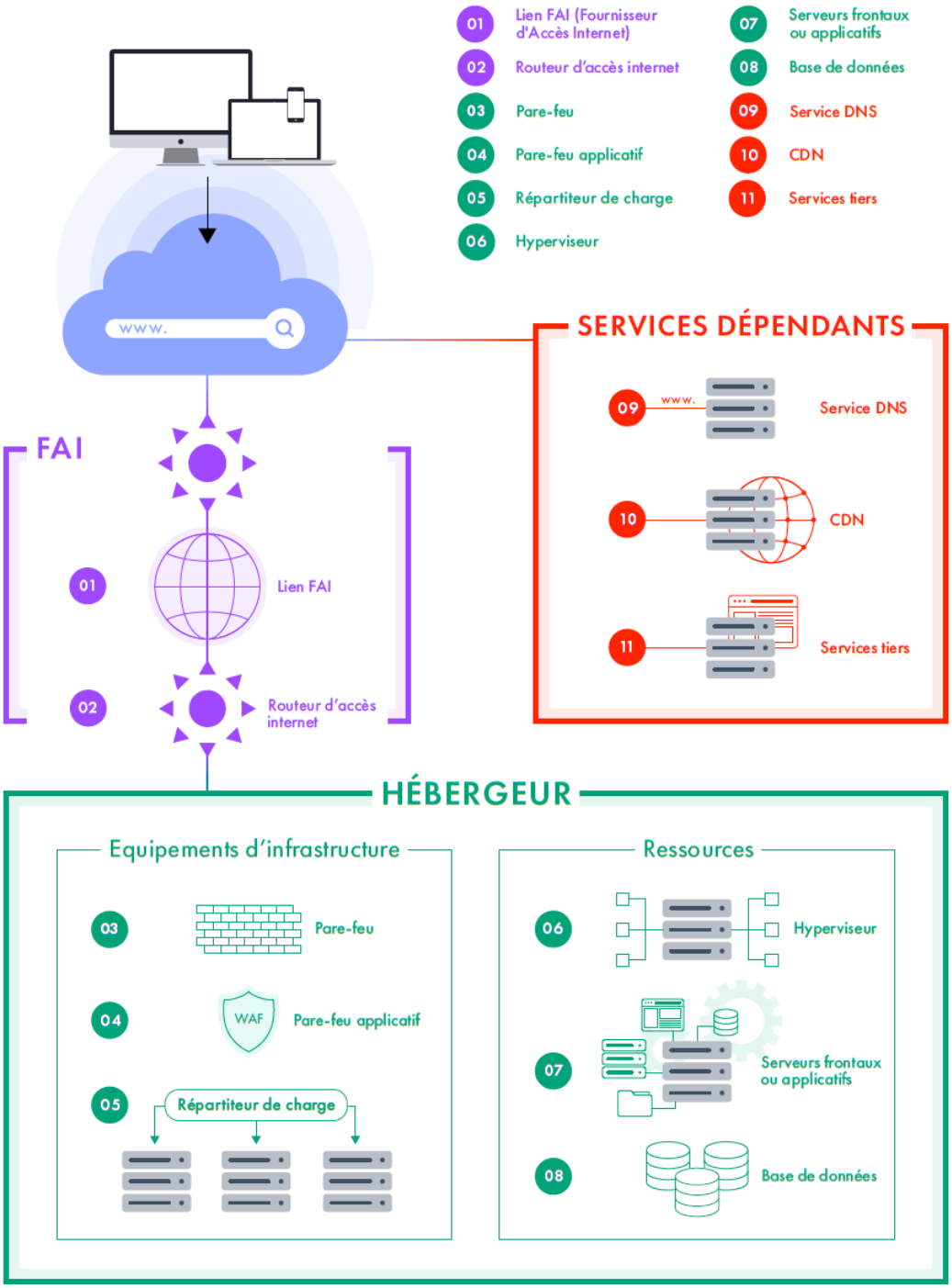
Le schéma d'architecture ci-après va servir de base pour illustrer la démarche d'endiguement.
Il représente une architecture classique de service exposé sur internet qui devra être ajusté en fonction des conditions spécifiques dans lesquelles l'organisation opère : les variations des équipements d'infrastructure, le choix entre un hébergement sur site ou dans le cloud, etc....

Remarque :
Les services dans le périmètre [Services dépendants] peuvent également faire partie du périmètre Hébergeur [Périmètre Hébergeur].

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Architecture classique de services exposés sur Internet



CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Sélectionner les actions appropriées

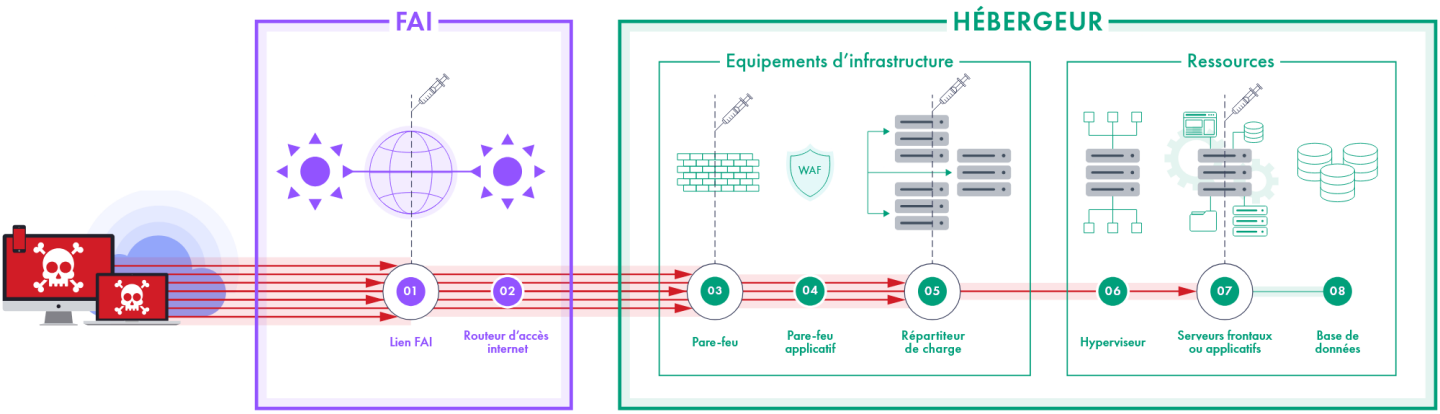
Mesure 1 - Ordonner vos actions dans le périmètre défini et sélectionner les mesures en fonction des caractéristiques du déni de service

Action 1.a : Déterminer le périmètre et l'ordre des actions d'endiguement

Le traitement de l'endiguement doit :

- ❑ Commencer par le ou les **éléments en amont du composant défaillant** afin de réduire le trafic à destination du composant défaillant
- ❑ **Se terminer par** le ou **les composants défaillants** afin de réduire la surcharge subie
- ❑ Appliquer les actions d'endiguement de façon **unitaire** afin de juger de leur **efficacité** et de mesurer les éventuels **effets de bord**

Point de saturation d'une infrastructure



CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Sélectionner les actions appropriées

Mesure 1 - Ordonner vos actions dans le périmètre défini et sélectionner les mesures en fonction des caractéristiques du déni de service

Action 1.b : Sélectionner les actions d'endiguement

Les actions sélectionnées sont à mettre en œuvre en fonction :

- ❑ Des caractéristiques du déni de service établies à travers la fiche réflexe : Fiche réflexe - Déni de service réseau - Qualification (https://cyberveille.esante.gouv.fr/deni-de-service-reseau-qualification-et-endiguement) (généralités, [**Déni de service volumétrique**], [**Déni de service sur les protocoles**], [**Déni de service sur les applications**], [**Déni de service sur les services DNS**], etc.)
- ❑ Du contexte d'infrastructure de l'organisation

Remarque :
- ❑ Les **actions d'endiguement** sont proposées de façon **générique** et ne constituent **pas une liste exhaustive** de mesures possibles d'atténuation.
- ❑ Avant l'exécution des actions d'endiguement, leurs **impacts** doivent être **évalués** au regard des résultats attendus et des conséquences métiers potentielles.
- ❑ Les actions **d'activation de service** comme un CDN ou un service de filtrage spécifique aux attaques de déni de service (anti-DDoS) supposent que la **contractualisation et l'intégration aient déjà été faites** ou que la prise en compte du **coût**, du **délai** de mise en œuvre et de **l'adaptation de l'implémentation** avec le système d'information ait été évaluées.
- ❑ Les choix d'actions d'endiguement peuvent avoir des effets sur la **facturation**, en particulier dans les environnements Cloud.

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 2 - Limiter le trafic en amont de l'entité (avec le FAI)

Ces actions tentent de filtrer le trafic dans le périmètre du fournisseur d'accès internet (FAI) et limitent les requêtes vers l'infrastructure de l'entité.
Ce type d'endiguement s'adresse plus particulièrement lorsqu'un **discriminant** fort (exemples : IP source, protocole, etc.) a pu être trouvé dans la phase de qualification.

Attention : Il convient de contacter le fournisseur de service, idéalement en amont, afin de connaitre les niveaux de services proposés, leurs coûts, le délai de mise en œuvre effectif et l'éventuelle adaptation de l'implémentation avec le système d'information de l'entité.

Action 2.a : Identifier un contact technique de votre FAI

❑ **Contacter** le support technique de votre FAI qui peut être en mesure de vous donner de la **visibilité** et peut vous **orienter** dans le traitement de votre incident.

Action 2.b : Limiter le trafic en amont de l'entité (avec le FAI)

❑ **01** Infrastructure FAI
- **Bloquer les requêtes** à partir des éléments discriminants (ex : IP source, protocole, géolocalisation, etc) issus de la qualification
- Si les services ciblés ne sont pas essentiels, **supprimer temporairement les requêtes (Blackhole)** à destination des IP cibles causant **un déni de service effectif sur le service visé** par l'attaque
  - › Parallèlement, **rétablir les services** indirectement impactés s'ils sont importants
- En cas d'attaque sur le FQDN, un changement d'entrée DNS du service visé peut également rétablir les services indirectement impactés

❑ **02** Routeur d'accès internet
- **Redémarrer** l'équipement (en cas de processus bloqué)

Attention : Un redémarrage de routeur, selon le modèle, peut prendre plusieurs minutes. Les impacts de cette action sont donc à mesurer.

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 2 - Limiter le trafic en amont de l'entité (avec le FAI)

Action 2.c : Activer le Service anti-DDoS du FAI

- ❑ Si disponible, **activer ce service**
- ❑ **Mettre à jour les règles** (blocage de requêtes) **et les seuils** (contrôle de débit - rate-limiting) avec les éléments discriminants de la qualification
- ❑ Si disponible, activer des fonctionnalités qui permettront de :
  - **Bloquer les requêtes** qui ont une destination erronée (ex: requête visant un service en spécifiant un port qui n'est pas exposé)
  - **Bloquer les requêtes** par IP source réputée malveillante issue des bases de la Cyber Threat Intelligence (CTI)
  - Mettre en place des règles de blocage à partir de critères discriminants basés sur les empreintes JA3/S et JA4 (profilage à partir d'informations collectées lors des échanges SSL/TLS)
  - Mettre en place d'autres fonctionnalités du service anti-DDoS

Mesure 3 - Agir dans le périmètre de l'hébergeur

Action 3.a : Activer le service anti-DDoS de l'hébergeur (en amont du pare-feu et du routeur)

- ❑ Si disponible, **activer ce service**
- ❑ **Mettre à jour les règles** (blocage de requêtes) **et les seuils** (contrôle de débit - rate-limiting) avec les éléments discriminants de la qualification
- ❑ Si disponible, activer des fonctionnalités qui permettront de :
  - **Bloquer les requêtes** qui ont une destination erronée (ex: requête visant un service en spécifiant un port qui n'est pas exposé)
  - **Bloquer les requêtes** par IP source réputée malveillante issue des bases de la Cyber Threat Intelligence (CTI)
  - **Bloquer les requêtes** par reconnaissance de robot (Challenge captcha dynamique ou challenge Javascript - JS)
  - Mettre en place de blocage à partir de critères discriminants basés sur les empreintes JA3/S et JA4 (profilage à partir d'information collectée lors des échanges SSL/TLS)
  - Mettre en place d'autres fonctionnalités du service anti-DDoS

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 3 - Agir dans le périmètre de l'hébergeur

Action 3.b : Limiter les requêtes sur les équipements d'infrastructure réseau

❑ Généralité
- Réseau d'administration
  - Si possible, **marquer le trafic d'administration prioritaire** au moyen de la mise en place d'une QoS (Quality of Service) en cas d'indisponibilité du réseau d'administration

❑ 03 Pare-feu
- Généralités
  - **Mettre à jour** l'équipement en cas de déni de service lié à des vulnérabilités de la version du firmware
  - Ajuster les règles de pare-feu afin de **limiter les services et protocoles exposés** et rejeter les autres requêtes
  - Si possible, mettre en place une **politique de blocage des paquets mal formés** ou une **politique de protection DoS**
  - **Bloquer les requêtes** à partir des éléments discriminants (ex : IP source, protocole, géolocalisation, etc.) issus de la qualification
  - **Bloquer les requêtes** par IP source réputée malveillante issue des bases de la Cyber threat Intelligence (CTI)
  - **Filtrer sur les IP/bloc/AS (Autonomous System)/géolocalisation autorisées** à se connecter aux services
  - Si les services ciblés ne sont pas essentiels, **supprimer temporairement les requêtes (Blackhole)** à destination des IP cibles causant **un déni de service effectif sur le service visé** par l'attaque
    - › Parallèlement, **rétablir les services** indirectement impactés en fonction de leur importance

- Cas des [**Déni de service volumétrique**]
  - Appliquer un **contrôle de débit** (rate limiting). Par exemple, définir des **seuils de blocage de requête par IP source** en fonction de paramètres comme la bande passante, le nombre de paquets par seconde, le nombre de requêtes applicatives avec des signatures malveillantes
    - › Assurer une supervision afin d'observer d'éventuels effets de bord
  - Appliquer une **régulation de flux** (traffic shaping) afin de prioriser certains flux

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 3 - Agir dans le périmètre de l'hébergeur

Action 3.b : Limiter les requêtes sur les équipements d'infrastructure réseau

- Cas des [**Déni de service sur les protocoles**]
  - Réduire les **durées de vie de suivi de connexions**
  - Limiter le nombre de **paquets SYN par seconde par IP source**
  - Limiter le nombre de **paquets SYN par seconde par IP de destination**
  - S'assurer que la fonctionnalité **SYN cookie** est activée
  - Mettre un **seuil sur le nombre de requêtes ICMP par IP source**
  - Mettre un **seuil sur le nombre de requêtes UDP par IP source**

❑ **04** Pare-feu applicatif
- Généralités
  - › **Mettre à jour les signatures d'attaques**
  - › **Simplifier la configuration** pour décharger les processeurs
- Cas des [**Déni de service volumétrique**]
  - › Appliquer un **contrôle de débit** (rate limiting) ou une **régulation de flux** (traffic shaping)
- Cas des [**Déni de service sur les applications**]
  - **Appliquer le blocage** des requêtes malveillantes avec des signatures
  - Définir des règles précises pour **bloquer sur les discriminants de niveau 7** (applicatif) observés lors de la qualification (**Attention : ne pas mettre en œuvre cette mesure sur des attaques volumétriques d'ampleur, au risque de surcharger le processeur et causer un nouveau déni de service**)
  - Appliquer une **limite de session** au niveau des services web
    - › Utiliser les fonctionnalités de **cache**
    - › Bloquer les requêtes par **reconnaissance de robot** (Challenge captcha dynamique ou challenge Javascript - JS)
    - › Réduire les **durées de vie de suivi de connexions**

❑ **05** Répartiteur de charge
- Appliquer un **contrôle de débit** (rate limiting)
- Réduire les **durées de vie de suivi de connexions**

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 3 - Agir dans le périmètre de l'hébergeur

Action 3.c : Limiter les requêtes sur les ressources

❑ 06 Hyperviseur
- **Optimiser les ressources** en cas de saturation
  - Répartir la charge (avec la création d'instances par exemple)
  - Répartir et/ou allouer les ressources
  - Séparer les instances sur des zones géographiques distinctes (sharding)
  - Mettre à jour l'hyperviseur
  - Migrer les autres machines pour avoir plus de ressources
  - Migrer la machine impactée pour relancer les autres services

❑ 07 Serveurs frontaux ou applicatifs
- Cas du système qui sature
  - › Si l'accès au serveur n'est plus possible pour cause de saturation :
    - Couper l'accès réseau de production
    - Redémarrer le serveur
    - Appliquer les optimisations système
    - Ré-ouvrir les flux de production
  - **Allouer d'avantage de ressources** à la machine
  - **Ajuster les seuils système** limitants (exemples : Ulimit et systemd sur les environnements Linux)
  - **Optimiser sur le bas niveau des systèmes d'exploitation** (exemples : sysctl sur les environnements Linux, system ressource manager sur les environnements Windows)

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 3 - Agir dans le périmètre de l'hébergeur

Action 3.c : Limiter les requêtes sur les ressources

- Cas des [**Déni de service sur les applications**]
  - **Désactiver les fonctionnalités non-importantes** posant problème, mais ne pas les supprimer (exemples : moteur de recherche, formulaire)
  - **Appliquer une limite** de sessions au niveau des services web
  - Utiliser la fonctionnalité de mise en **cache**
  - Bloquer les requêtes par **reconnaissance de robot** (Challenge captcha dynamique ou challenge Javascript - JS)
  - Réduire les **durées de vie de suivi de connexions**
  - **Optimiser la configuration** des services web et de leurs composants (serveur web : Apache, Nginx, IIS; runtime : .Net JRE; Applicatif : tomcat, jboss, nodeJS)
  - **Statifier** les contenus changeant peu, et dédier des serveurs à cet effet
  - **Redémarrer les services** en cas de processus applicatif bloqué (mesurer les impacts au préalable)

❑ 08 Serveurs de base de données
- Cas des [**Déni de service sur les applications**]
  - **Optimiser les ressources (calcul, mémoire, disque)** et la **configuration** en cas de saturation
    - › Ajouter des instances en cas de cluster

Mesure 4 - Agir dans le périmètre des services dépendants

En cas de déni de service sur les services DNS :

Action 4.a : Agir sur les configurations du service DNS

❑ 09 Service DNS
- Filtrer les **requêtes DNS malformées ou invalides**
- Filtrer sur les **enregistrements DNS qui n'existent pas**
- S'assurer que les **fonctions inutiles sont désactivées** (par exemple : transfert de zone, rôle récursif exposé sur internet)

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Limiter les impacts

Mesure 4 - Agir dans le périmètre des services dépendants

En cas d'attaque sur les applications :

Action 4.b : Activer le CDN sur les attaques visant du contenu statique, si possible

❑ 10 CDN
- Répartir la charge sur le contenu :
  - Publier le contenu statique
  - Mettre en cache le contenu dynamique (Attention aux effets de bord)
  - Bloquer les requêtes par reconnaissance de robot (Challenge captcha dynamique ou challenge Javascript - JS)
- Activer le service anti-DDoS du CDN :
  - Définir une blacklist dans la configuration à partir d'éléments issus de la qualification (source, user-agent, entête spécifique, etc.)

Attention : Le recours à un CDN doit prendre en compte les problématiques autour du RGPD et de la confidentialité des données (possible déchiffrement du flux).

Action 4.c : Agir sur les composants tiers

❑ 11 Composants tiers
- Désactiver les composants tiers optionnels et non essentiels

Action 4.d : Activer un service anti-DDoS externe, si possible

❑ Service de filtrage anti-DDoS externalisé dans le cloud
- Activer le service externalisé par :
  - Déroutement du trafic par des annonces BGP et mise en place d'un tunnel GRE
  - Redirection du trafic via le protocole DNS

Attention : Pour la redirection du trafic via le protocole DNS :
- Prendre en compte le délai de propagation DNS et le certificat TLS à mettre sur le service externalisé
- Le recours à ce service doit prendre en compte les problématiques autour du RGPD et de la confidentialité des données (possible déchiffrement du flux)
- Cette méthode protège uniquement les attaques sur le nom de domaine et non sur les adresses IP

CC BY-NC-SA 4.0

Actions d'endiguement par périmètre et type de déni de service

Préserver les traces

Mesure 5 - Préserver les traces

Action 5 : Préserver les traces des journaux d'équipements

❑ Exporter les logs des éléments cartographiés ou des captures manuelles du réseau

Pour soutenir la réponse à incident dans son objectif d'investigation, il faut préserver l'intégrité des journaux avec une durée de rétention minimum de 6 mois.

Si les logs sont déjà exportés dans un SIEM ou un centralisateur de logs, il est alors inutile de les exporter et d'augmenter leur rétention sur les machines sources.

Attention : Une attaque par déni de service va augmenter la volumétrie de journaux. Une augmentation de la verbosité doit se faire au strict besoin de l'investigation tout en considérant le risque de saturation du stockage pouvant déclencher un nouveau déni de service.

CC BY-NC-SA 4.0

Suite des actions

A la fin de ces actions d'endiguement, l'incident peut être potentiellement contenu. Cependant, une **vigilance** à travers la supervision doit être mise en œuvre, afin de **détecter le retour** d'un attaquant qui pourrait s'être adapté aux mesures de défense mises en œuvre.

Si l'incident n'est toujours pas contenu, la **remédiation** doit passer pour une **révision de l'architecture**, de la **contractualisation de service spécifique** et de la **formation** des personnels.

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés : **investigation forensique et remédiation par une équipe spécialisée**, **maintien d'activité**, **communication interne aux partenaires**, **dépôt de plainte et déclarations**, etc.

Pour ce faire, il est conseillé de piloter la suite de la résolution de l'incident en cohérence avec les impacts identifiés et demander de l'aide :

- Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident.
  Voir les annexes Contacts et Déclarations.

Remarque :
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)

CC BY-NC-SA 4.0

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*.

CC BY-NC-SA 4.0

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.

CC BY-NC-SA 4.0

Annexes

Déclarations

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.
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.

CC BY-NC-SA 4.0

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 - Déni de service réseau - Qualification (https://cyberveille.esante.gouv.fr/deni-de-service-reseau-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)

CC BY-NC-SA 4.0

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.