Fiche réflexe

Déni de service

Qualification

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 une. **aide à la qualification** d'un incident de type déni de service réseau, nécessaire pour la prise de décision des actions d'endiguement.
Les différentes actions proposées aideront à :

- **Confirmer** qu'un incident de sécurité est bien en cours, et qu'il est de type **déni de service réseau**,
- Évaluer la **gravité** de l'incident en évaluant le **périmètre** affecté, **l'impact** potentiel sur le fonctionnement de l'organisation et **l'urgence** à le résoudre.

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Conclusions attendues** de la qualification correspond aux questions auxquelles la qualification devra répondre.
- La partie **Méthode d'évaluation** pas à pas correspond à la méthodologie pour aider à y répondre.

Cette fiche doit être exécutée en **temps court**. Pour cela, fixer un *temps contraint* (selon l'urgence pressentie) et ne pas rechercher l'exhaustivité des réponses : **des réponses approximatives et des réponses *"je ne sais pas répondre"* sont acceptées dans un premier temps**. Par la suite, une qualification plus approfondie se fera sûrement, avec plus de recul ou l'appui d'une équipe spécialisée en réponse à incident.

Sommaire

Fiche réflexe
- Déni de service – Qualification

Prérequis

01

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
- Les connaissances des **schémas d'architecture** et de la **cartographie des flux d'application**
- Les connaissances techniques des applications impactées par le déni de service
- La connaissance des **priorités métier** de l'organisation
- L'annuaire de contacts d'urgence

02

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

03

Avoir pris connaissance des actions déjà entreprises

Avoir pris note des personnes ayant déjà agi en réponse à l'incident en cours et des actions qu'elles ont déjà entreprises sur le système d'information. Commencer à reporter ces notes d'intervention dans la main courante.

*Cette main courante doit être **éditable et consultable** par tous les intervenants. Il est déconseillé de la stocker sur le système d'information compromis, où elle serait accessible par l'attaquant. En revanche, cette main courante peut être accessible sur un partage de fichiers en ligne (cloud) ou intégrée dans le logiciel de gestion d'incident ou le SIEM si l'organisation en possède un, voire être au format papier.

Conclusions attendues de la qualification

Cette partie résume les conclusions auxquelles doivent mener les évaluations, qui aboutiront à la qualification de l'incident.
La partie suivante détaillera justement des actions détaillées qui aideront à conduire pas à pas ces évaluations.

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type déni de service réseau

- L'incident de type déni de service réseau est-il confirmé ?
- L'indisponibilité ou le ralentissement d'un ou plusieurs services ont-ils déjà été constatés ?

Mesure 2 - Évaluer le périmètre informatique de l'incident

- La cartographie du périmètre concerné, c'est à dire des équipements de la chaîne de flux du déni de service, est-elle établie ?
- Les personnes pouvant administrer ce périmètre sont-elles identifiées ?
- Le ou les éléments défaillants du périmètre sont-ils identifiés ?

Mesure 3 - Évaluer les caractéristiques du déni de service

Type de déni	Catégorie	Vague d'attaque	Durée	Métrique	Source des requêtes	Services visés
• Déni de service (Dos) • Déni de service distribué (DDoS) • Déni de service distribué hautement distribué (DDoS)	• Volumétrique • Protocole • Applicatif	• Nombre	• Minutes • Heures	• volume • paquet • connexion	• IP Unique • Range IP • AS • Zone géographique • Réseau d'anonymisation • Réseau de botnet • Réseau malveillant • Infrastructure légitime • Hautement distribué	• IP • FQDN • Domaine

Type d'attaque	Couche OSI	Service	Protocole	Caractéristiques discriminantes (TCP Flag, User-agent, etc.)
• Attaque par rebond • Attaque par rebond de nos infrastructures • TCP SYN flood • UDP flood • Amplification DNS • Malformed SSL • HTTP(S) Flood • Attaque avec connaissance des faiblesse applicatives • HTTP/1.1 attack • Standard HTTP/2 attack • HTTP/2 Rapid Reset attack • Autres	• Niveau 3 • Niveau 4 • Niveau 6 • Niveau 7	DNS • SNMP • NTP • HTTP • HTTPS • Autres	• TCP • UDP • ICMP	

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 4 - Évaluer l'impact de l'incident

- Quelles chaînes d'activité métier sont impactées ?
- L'incident cause-t-il un impact sur la réglementation ?
- L'incident cause-t-il un impact financier direct ?

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

- Quelles sont les activités essentielles perturbées sans maintien d'activité pour lesquelles un rétablissement d'urgence doit être opéré ?
- Quelles sont les activités en mode dégradé pour lesquelles il faut préparer dès maintenant un rétablissement ?

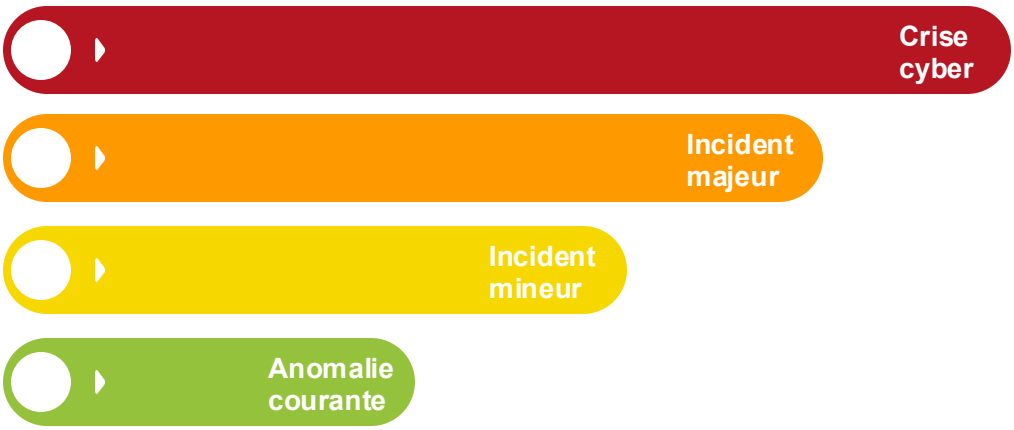
Conclusions attendues de la qualification

Qualifier l'incident

Conclure quant à la gravité de l'incident

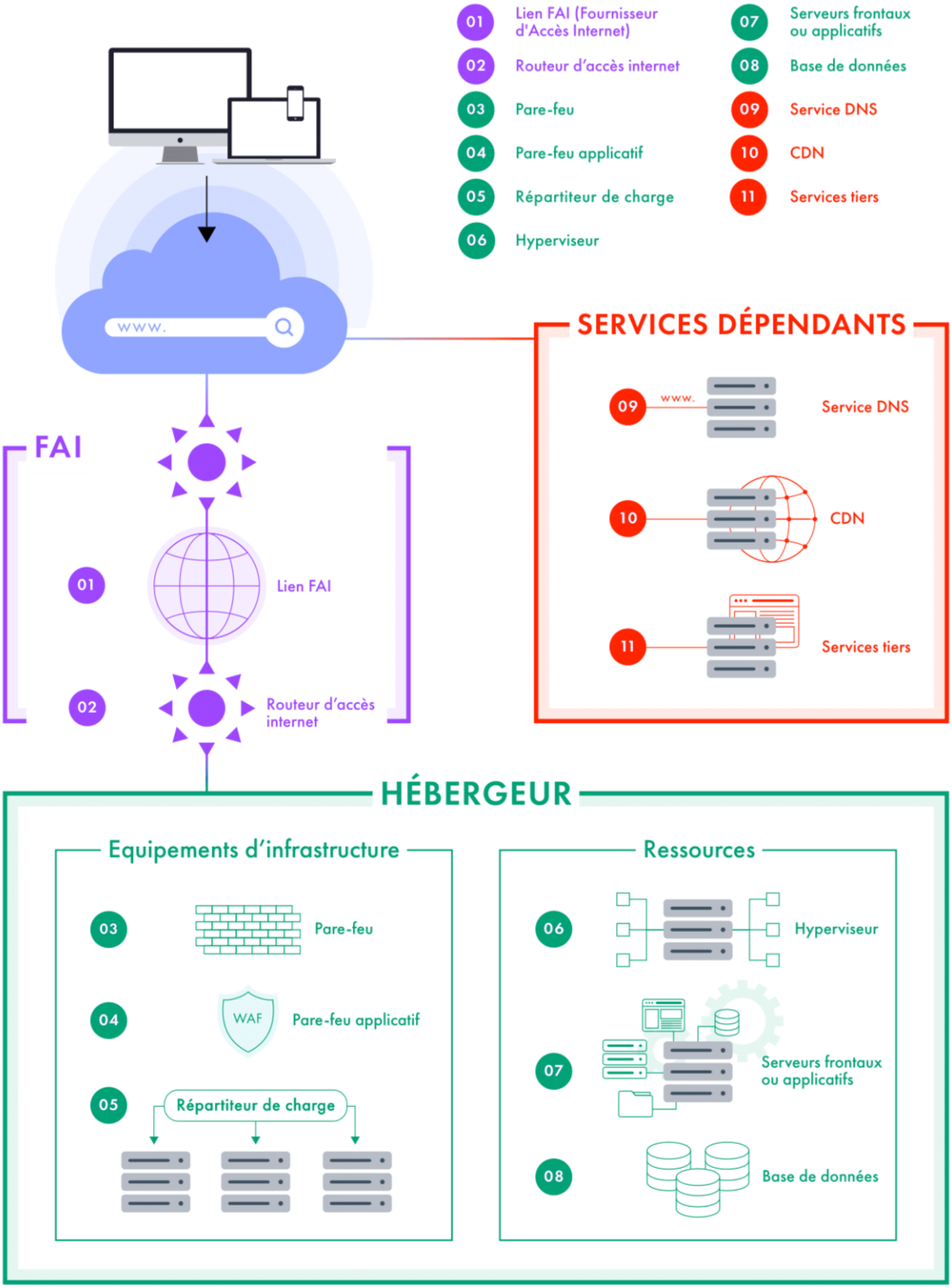
- L'incident de type **déni de service** réseau est-il **confirmé** ?
- L'incident est-il **circonscrit** sur mon système d'information, ou est-il étendu ?
- L'incident présente-il un **impact fort** pour mon **activité métier** et le fonctionnement de mon **système d'information** ?
- L'incident est-il **urgent** à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

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



Méthode d'évaluation pas à pas

Architecture classique de services exposés sur Internet



Méthode d'évaluation pas à pas

Le schéma d'architecture illustré sur la page précédente va servir de base pour les éléments de qualification. Il représente une architecture classique de service exposé sur internet qui devra être ajustée 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].

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type déni de service réseau

Action 1.a : Écarter la piste d'un incident de production

Avant de conclure que l'altération du service est causée par un incident de sécurité, l'incident de production doit être écarté en se basant sur les éléments suivants :

- ❑ Récente mise à jour opérationnelle ou de sécurité (MCO/MCS)
- ❑ Récent changement de configuration (ex: infrastructure, règle de pare-feu, système d'exploitation, modification applicative, bibliothèque, etc.)
- ❑ Problème constaté dans un environnement similaire (développement, recette, préproduction, etc.)
- ❑ Expiration de licence, contrat, certificat, nom de domaine
- ❑ Problème technique externe : les liens internet, les composants tiers, etc.
- ❑ Compte de service supprimé, désactivé, bloqué ou dont le mot de passe a changé/expiré
- ❑ Faiblesses intrinsèques de l'architecture : Pic d'activité plus élevé en fonction des activités métiers (ex: clôture comptable, résultat d'examen, etc.)

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 1 - Confirmer l'incident de type déni de service réseau

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

❑ Supervision de sécurité :
- Détection du SOC ou du NOC avec le SIEM
- Alertes : pare-feux, pare-feux applicatifs, proxy inverse, commutateurs réseaux, NIPS/NIDS, etc.

❑ Supervision de production :
- Services indisponibles ou lents (ex: erreur HTTP 503)
- Ressources saturées (processeur, mémoire, disque, table d'état, réseau) dans les consoles de serveurs
- Processus applicatifs ou requêtes en base de données bloqués ou anormalement nombreux
- Écart de volumétrie réseau constaté par rapport à la moyenne habituellement constatée

❑ Signalement :
- Utilisateurs ou partenaires n'accédant plus à un ou plusieurs services ou observant des ralentissements
- Revendication d'un attaquant (Internet, Média sociaux, Courriel, autres)
  - › Garder une trace de la revendication en réalisant une capture d'écran, par exemple

Action 1.c : Confirmer la nature réseau de l'incident

La nature réseau de l'incident peut être déterminée par :
❑ **Saturation des liens** FAI
❑ **Nombre des requêtes anormalement important dans les journaux réseaux** (pare-feu, répartiteur de charge, pare-feu applicatif, commutateur réseau, capture manuelle) ou **dans les journaux applicatifs**
❑ **Récurrences de requêtes réseaux**

Méthode d'évaluation pas à pas

Évaluer l'incident

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 déni de service réseau

- ❑ *L'incident de type déni de service réseau est-il confirmé ?*
- ❑ *L'indisponibilité ou le ralentissement d'un ou plusieurs services ont-ils déjà été constatés ?*

Mesure 2 - Évaluer le périmètre informatique de l'incident

Action 2.a : Cartographier la chaîne de flux du déni de service

A partir des journaux 03 du pare-feu en bordure de l'entité ou à partir des équipements 01 et 02 avec l'assistance du FAI :

- ❑ **Cartographier** les équipements et les machines qui sont concernés par la chaîne de flux **depuis l'origine des requêtes** (IP sources), **jusqu'à la destination** (IP de destination)
- ❑ **Identifier le ou les services visés** avec les adresses IP de destination de l'attaque
- ❑ **Cartographier toutes les dépendances informatiques** (équipements et machines) des services visés

Remarque : L'identification de chaque brique informatique traversée par la chaîne de flux du déni de service permettra de connaitre les journaux à disposition qui seront utiles au diagnostique et à l'évaluation des caractéristiques de l'attaque.

Action 2.b : Identifier les moyens et les personnes en charge de l'administration

- ❑ Identifier les moyens d'administration de ces équipements et machines
- ❑ Identifier qui a la responsabilité de l'administration de ces équipements et machines

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 2 - Évaluer le périmètre informatique de l'incident

Action 2.c : Identifier les éléments défaillants de la chaîne (impact informatique)

Le déni de service a-t-il un impact sur :

❑ Des ressources opérateurs [Périmètre FAI]

- 01 Lien FAI
  - › Surcharge de la bande passante dans le monitoring du FAI ou le monitoring interne (sur le pare-feu en bordure par exemple)
- 02 Routeur d'accès internet
  - › Indisponibilité de l'équipement dans le monitoring du FAI ou le monitoring interne (perte de ping sur l'équipement par exemple)

❑ Des équipements d'infrastructure réseau [Périmètre Hébergeur]

- 03 Pare-feu, 04 Pare-feu applicatif, 05 Répartiteur de charge
  - › Saturation des ressources (calcul, mémoire, disque)
  - › Indisponibilité réseau : perte de ping, saturation des tables d'état ou de sessions
  - › Autres alertes dans l'interface d'administration

❑ Des ressources [Périmètre Hébergeur]

- 06 Hyperviseur, 07 Serveurs frontaux ou applicatifs, 08 Serveurs de base de données
  - › Saturation des ressources (calcul, mémoire, disque)
  - › Application, processus ou service bloqué (monitoring dans l'interface d'administration ou dans les journaux applicatifs)
  - › Indisponibilité réseau de l'équipement dans le monitoring (perte de ping sur l'équipement par exemple)
  - › Spécifique aux bases de données :
    - Observation de blocage de processus
    - Requêtes en attente
    - Nombre maximum de connexions atteintes
    - Saturation des opérations d'entrée-sortie par seconde (I/O)
    - Autres erreurs observées dans l'interface d'administration ou dans les journaux de base de données

❑ Des ressources tiers [Périmètre Services dépendants]

- 09 Service DNS
  - › Indisponibilité du service (DNS lookup sans réponse)
- 10 CDN
  - › Indisponibilité du service
- 11 Composants tiers (exemple: outils de statistique, identité, etc.)
  - › Indisponibilité du service

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 2 - Évaluer le périmètre informatique de l'incident

Remarque : L'identification du ou des éléments défaillants est essentielle car, couplée avec la cartographie générale du ou des systèmes d'information, elle permettra de déterminer quels sont les impacts sur l'activité métier (Action 3.a)

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

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

- ❑ *La cartographie du périmètre concerné, c'est à dire des équipements de la chaîne de flux du déni de service, est-elle établie ?*
- ❑ *Les personnes pouvant administrer ce périmètre sont-elles identifiées ?*
- ❑ *Le ou les éléments défaillants du périmètre sont-ils identifiés ?*

Mesure 3 - Évaluer les caractéristiques du déni de service

Action 3.a : Évaluation générale

- ❑ Quel est le nombre de vague d'attaque observée et leur durée ?
- ❑ Quelles sont les métriques observables à partir des journaux ou des consoles des équipements 01 02 03 ?
  - Volumétrie (Mb/s)
    - › Si les volumes observés dépassent la capacité de la bande passante : Catégorie [**Volumétrique**]
  - Nombre de paquets par seconde (pps)
  - Nombre de connexions par seconde

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 3 - Évaluer les caractéristiques du déni de service

Action 3.b : Évaluation à partir de la chaîne de flux (origine et destination des requêtes)

A partir des journaux du 03 **pare-feu** en bordure de l'entité ou à partir des équipements 01 et 02 avec l'assistance du FAI, déterminer les éléments suivants :

❑ Déterminer le **type de déni** en identifiant les nombres d'IP source des requêtes :
- Unique ? (Type de déni : [**Déni de service (DoS)**])
- Multiple ? (Type de déni : [**Déni de service distribué (DDoS)**])
- Massivement Multiple ? (Type de déni : [**Déni de service hautement distribué (DDoS)**])

❑ La **source des requêtes** semble-t-elle venir de :
- IP Unique ? (Source des requêtes : [**IP Unique**])
- Ranges IP particuliers ? (Source des requêtes : [**Range IP**])
- AS spécifiques ? (Source des requêtes : [**AS**])
- Zones géographiques spécifiques ? (Source des requêtes : [**Zone géographique**])
- Infrastructure d'anonymisation (Tor, vpn) ? (Source des requêtes : [**Réseau d'anonymisation**])
- Une infrastructure réputée malveillante ? (Source des requêtes : [**Réseau de botnet**])
- Sous-réseaux IP des VPS ou IAAS ? (Source des requêtes : [**Réseau malveillant**])
- Une infrastructure légitime, proxy ou API exposée ? (Source des requêtes : [**Infrastructure légitime**], Type d'attaque : [**Attaque par rebond**])
- Difficile à différentier ou à catégoriser ? (Source des requêtes : [**Hautement distribuée**])

❑ Déterminer les **services visés** (IP de destination des requêtes) :
- **IP**
- **Domaine**
- **FQDN**

❑ L'incident génère-t-il beaucoup de trafic sortant (réaction possible) ? (Type d'attaque : [**Attaque par rebond de nos infrastructures**] : nos infrastructures participent à un déni de service)

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 3 - Évaluer les caractéristiques du déni de service

Action 3.c : Évaluer le caractère discriminant

Identifier le ou les **discriminants** du déni de service (trouver un ou des motifs communs ou réguliers)

- **Déni de service sur les protocoles niveau 3** (catégorie [**Protocole**], couche OSI [**Niveau3**]):
  - Diagnostique à partir des journaux des équipements 01 02 03 04 05 07
  - Attaque sur les protocoles liés à tout élément informatique sur le réseau (mais plus particulièrement ceux exposés sur internet dans le cadre d'une attaque depuis l'extérieur)
    - Inondation de requêtes ICMP ([**Ping flood, Attaque Smurf, Ping de la mort**])
- **Déni de service sur les protocoles niveau 4** (catégorie [**Protocole**], couche OSI [**Niveau4**]):
  - Diagnostique à partir des journaux des équipements 01 02 03, et 09 pour les requêtes DNS
  - Attaque sur les protocoles liés à tout élément informatique sur le réseau (mais plus particulièrement ceux exposés sur internet dans le cadre d'une attaque depuis l'extérieur)
    - Inondation de requêtes TCP (Type d'attaque [**TCP SYN Flood**])
    - Inondation de requêtes UDP (Type d'attaque [**UDP Flood**])
    - Inondation de requêtes DNS (Type d'attaque [**DNS Flood**] , [**Amplification DNS**])
    - Inondation de requêtes SNMP, NTP, autres
- **Déni de service sur protocole TLS** (catégorie [**Protocole**], couche OSI [**Niveau 6**]) :
  - **Diagnostique à partir des journaux des équipements** 01 02 03 04 05 07
  - Attaque sur le protocole TLS liée aux équipements et/ou serveurs portant la terminaison TLS
    - Inondation de requêtes SSL malformées causant une surcharge des processeurs des serveurs HTTPS (Type d'attaque [**Malformed SSL**])

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 3 - Évaluer les caractéristiques du déni de service

Action 3.c : Évaluer le caractère discriminant

- **Déni de service applicatif** (catégorie [**Applicatif**], couche OSI [**Niveau7**]) :
  - **Diagnostique à partir des journaux des équipements** 01 02 03 04 05 06 07 08
  - Attaque sur les services web HTTP, HTTPS (Type d'attaque [**HTTP(S) Flood**])
    - Entête HTTP
  - Inondation de requêtes GET
  - Inondation de requêtes POST
  - User-Agent récurrent
  - Autres entêtes HTTP récurrentes
    - Requêtes anormales (Catégorie [**Protocole**] ou [**Applicatif**])
  - Requêtes ou téléversements en nombre conduisant à un dépassement de la capacité (CPU, mémoire, stockage)
  - Requêtes de très longue durée bloquant les sessions ouvertes (observation avec Netstat ou sur les pares-feux)
  - Requêtes forgées pour créer un bug dans l'application (Type d'attaque [**Attaque avec connaissance des faiblesses applicatives**])
  - Bug protocolaire (Catégorie [**Protocole**], Type d'attaque [**HTTP/1.1 attack, Standard HTTP/2 attack, HTTP/2 Rapid Reset attack**])
  - Requêtes exploitant de mauvaises configurations d'infrastructure (Exemple : fonctionnalité gourmande en ressource)
  - Requêtes en nombre saturant les ressources des équipements de filtrage (règles gourmandes dans les pares-feux applicatifs)
- •Autres éléments discriminants :
  - Diagnostique à partir des journaux des équipements
  - Quels autres éléments semblent discriminant dans la caractérisation de l'incident ?
    - Protocole ([**UDP**], [**TCP**], [**ICMP**])
    - Service ([**DNS**], [**SNMP**], [**NTP**], [**HTTP**], [**HTTPS**], [**Autres**])
    - TCP flags
    - Port de destination
    - Autres caractéristiques discriminantes

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 3 - Évaluer les caractéristiques du déni de service

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

Action 3.d : (Conclure) Évaluer les caractéristiques du déni de service

Type de déni	Catégorie	Vague d'attaque	Durée	Métrique	Source des requêtes	Services visés
• Déni de service (Dos) • Déni de service distribué (DDoS) • Déni de service distribué hautement distribué (DDoS)	• Volumétrique • Protocole • Applicatif	• Nombre	• Minutes • Heures	• volume • paquet • connexion	• IP Unique • Range IP • AS • Zone géographique • Réseau d'anonymisation • Réseau de botnet • Réseau malveillant • Infrastructure légitime • Hautement distribué	• IP • FQDN • Domaine

Type d'attaque	Couche OSI	Service	Protocole	Caractéristiques discriminantes (TCP Flag, User-agent, etc.)
• Attaque par rebond • Attaque par rebond de nos infrastructures • TCP SYN flood • UDP flood • Amplification DNS • Malformed SSL • HTTP(S) Flood • Attaque avec connaissance des faiblesse applicatives • HTTP/1.1 attack • Standard HTTP/2 attack • HTTP/2 Rapid Reset attack • Autres	• Niveau 3 • Niveau 4 • Niveau 6 • Niveau 7	DNS • SNMP • NTP • HTTP • HTTPS • Autres	• TCP • UDP • ICMP	

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 4 - Évaluer l'impact de l'incident

*En s'appuyant sur la **cartographie générale du système d'information**, sur la cartographie précédemment établie en Action 2.a : Cartographier la chaîne de flux du déni de service et sur l'identification du ou des éléments défaillants en Action 2.c : Identifier les éléments défaillants de la chaîne (impact informatique) :*

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

- ❑ Quelles sont toutes les **activités métiers** impactées par le déni de service, à usage interne ou externe (client, partenaire, etc.) ?
- ❑ Le service impacté par le déni de service fournit-il un service à d'autres applications externes (dépendance d'application) ?
  - Contacter les services de communication pour informer les parties intéressées
- ❑ 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 atteinte à l'image de l'entité ?
  - Une importante perte financière ?
  - Un danger sur les personnes (par exemple : données de santé) ?

Remarque : Le service visé par l'attaque va conduire à une **défaillance** d'un ou plusieurs éléments de la chaîne de flux pouvant causer **indirectement un déni de service sur d'autres services**. En général, plus l'élément défaillant est haut dans la chaîne, plus le nombre de services impactés indirectement augmente.

Action 4.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 traite-t-il des données à caractère personnel ?
  - Données personnelles d'usagers internes à l'organisation
  - Données personnelles d'usagers externes
  - Données sensibles au sens RGPD (santé, origine raciale, etc.)

Méthode d'évaluation pas à pas

Évaluer l'incident

Mesure 4 - Évaluer l'impact de l'incident

Remarque : Une indisponibilité de l'accès à la donnée est une violation au sens RGPD, une notification au Délégué à la protection des données (DPD ou DPO) est à prévoir en cas d'impact significatif sur les personnes pour la tenue de registre des incidents et éventuellement une déclaration à la CNIL.

Action 4.c : Évaluer les éventuels impacts financiers de l'attaque

❑ L'attaque a-t-elle des conséquences financières directes avec un abus d'utilisation de fonctionnalités facturées (génération de SMS, appel à un outil tiers, démarrage automatique de services payant ou de machines virtuelles, etc.) ?

Action 4.d : Évaluer les impacts des actions d'endiguement entreprises

❑ Des actions d'endiguement ont-elles déjà été entreprises ? Si oui :
- Des flux ont-ils été filtrés ou coupés ?
  - › Si oui, sur quels équipements ?
- Y a-t-il un impact sur les activités métier ?

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

Action 4.e : (Conclure) Évaluer l'impact sur les métiers de l'incident

❑ *Quelles chaînes d'activité métier sont impactées ?*
❑ *L'incident cause-t-il un impact sur la réglementation ?*
❑ *L'incident cause-t-il un impact financier direct ?*

Méthode d'évaluation pas à pas

Évaluer l'incident

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 ?
- ❑ Sous combien de temps ces procédures peuvent-elles être mise en œuvre opérationnellement ?

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 essentielles perturbées sans maintien d'activité pour lesquelles un rétablissement d'urgence doit être opéré ?*
- ❑ *Quelles sont les activités en mode dégradé pour lesquelles il faut préparer dès maintenant un rétablissement ?*

Méthode d'évaluation pas à pas

Déclarer l'incident

Obligation de déclarer les incidents au CERT Santé

En vertu de l'article L1111-8-2 du Code de la santé publique, les établissements de santé, les laboratoires de biologie médicale, les centres de radiothérapie et les établissements et services médico-sociaux sont tenus de **signaler tout incident de sécurité des systèmes d'information aux autorités compétentes**.

Contacts du CERT Santé

- **Numéro d'urgence 24h/24 et 7j/7** : 09 72 43 91 25
- **Contact mail** : cyberveille@esante.gouv.fr
- **Portail de signalement** : https://signalement.social-sante.gouv.fr/espace-declaration/profil

Procédure pour déclarer un incident

1) Accéder au portail de signalement : https://signalement.social-sante.gouv.fr/espace-declaration/profil
2) Cliquer sur "**Je suis un professionnel de santé**"
3) Sélectionner "**Cybersécurité**" dans la liste
4) Cocher la case "**Incident de sécurité des systèmes d'information**"
5) Réaliser la procédure pour déclarer l'incident

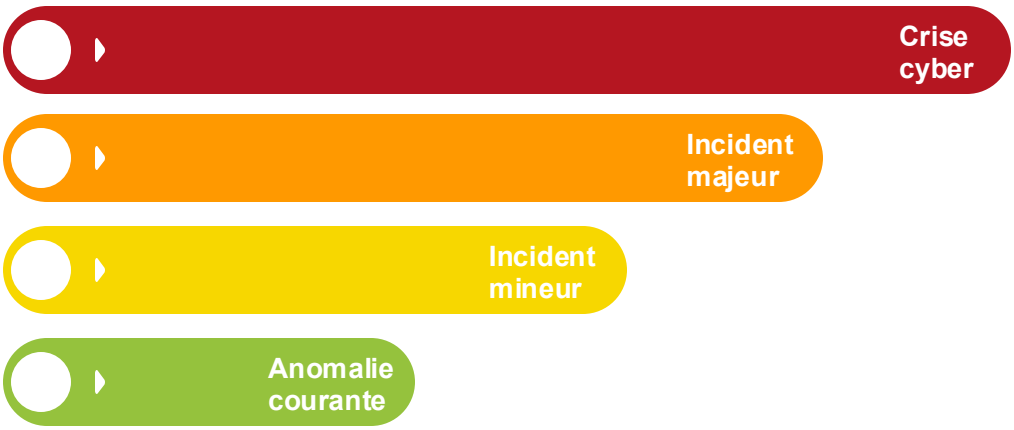
Méthode d'évaluation pas à pas

Qualifier l'incident

Conclure quant à la gravité de l'incident

- L'incident de type **déni de service** réseau 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 ?



Suite des actions

Si l'incident de sécurité est confirmé et qu'il est de type déni de service 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 - Déni de service réseau - Endiguement
  [https://cyberveille.esante.gouv.fr/deni-de-service-reseau-qualification-et-endiguement]

Remarque :
Dans le cas de prestations externalisées, demander si elles peuvent être activées afin d'atténuer le déni de service (incluses et en supplément) et sous quel délai elles pourraient être mises en œuvre de façon effective.

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.

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)

Annexes

Définitions

Qualifier un incident

Qualifier un incident signifie :

- **Confirmer** qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.
- **Évaluer la gravité/priorité de l'incident** en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

Axes d'évaluation

- **Périmètre** : Le périmètre d'un incident désigne son étendue sur les composants du système d'information (comptes, applications, systèmes, etc..) et leur administration.
- **Impact** : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- **Urgence** : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Degrés de gravité

- **Anomalie courante** (gravité **faible**) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- **Incident mineur** (gravité **modérée**) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.
- **Incident majeur** (gravité **élevée**) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- **Crise cyber** (gravité **critique**) : Une crise cyber représente un incident de sécurité ayant un *périmètre étendu* sur le système d'information, un *impact fort* sur l'activité métier et nécessitant une *résolution urgente*.

Annexes

Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation		
CERT Santé	https://esante.gouv.fr/produits-services/cert-sante https://cyberveille.esante.gouv.fr/	Pour les organisations du secteur de la santé
CERT/CSIRT externe en prestation de réponse à incident	https://www.cybermalveillance.gouv.fr/diagnostic/accueil https://cyber.gouv.fr/produits-services-qualifies	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CERT-FR	https://www.cert.ssi.gouv.fr/contact	Pour les administrations et les Opérateurs d'importance vitale et de services essentiels
CSIRT régional	https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations

De plus, pour les incidents complexes, une aide externe est également recommandée pour :

- Gérer la crise
- Gérer la communication interne et externe
- Augmenter les ressources humaines et capacitaires de reconstruction de votre direction informatique

Pour faciliter la mobilisation de tous ces acteurs, il est conseillé de s'appuyer sur des annuaires tenus à jour en amont et accessibles même en cas d'indisponibilité du système d'information.

Annexes

Déclarations

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.

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 - Endiguement (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)

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/).