Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Déni de service réseau

Qualification

2026

InterCERT FRANCE

A qui s'adresse-t-elle ?

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

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.

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*.
- *Déterminer le périmètre informatique* du déni de service et notamment identifier l'élément défaillant de la chaîne.
- *Déterminer les caractéristiques* du déni de service.
- Évaluer la *gravité* de l'incident en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

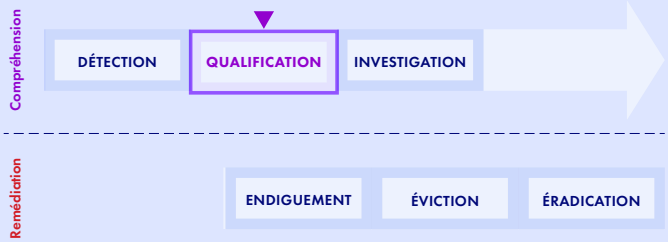
Comment l'utiliser ?

Deux parties principales composent cette fiche :

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

Cette fiche doit être exécutée en *temps court*. Pour cela, fixer un *temps contraint* selon l'urgence pressentie (ex : 30 minutes, 1 heure au maximum) et ne pas rechercher l'exhaustivité des réponses : des *réponses approximatives* et des réponses *"je ne sais pas répondre"* sont acceptables 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

Demander de l'aide

Ne jamais rester seul face à un incident. Solliciter l'aide d'un collègue afin de ne pas assumer seul la responsabilité de son traitement et de pouvoir répartir efficacement les tâches. Par exemple, une personne peut se concentrer sur l'approfondissement de la qualification de l'incident, tandis que d'autres peuvent contacter un responsable hiérarchique et le CSIRT/CERT, initier les premières mesures d'endiguement, voire paralléliser les actions prioritaires.

Disposer des personnes nécessaires

S'assurer que les personnes qui effectueront la qualification de l'incident aient :

- Les *accès à l'administration et aux outils de surveillance* du système d'information sur les différents périmètres (FAI, hébergeur infrastructure réseau & ressources, services tiers).
- Les *accès aux équipements de sécurité* du système d'information. et la capacité à faire des captures réseau.
- 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.

Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer tous 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, ayant en charge l'action en cours ou en suspens, ou ayant informé sur l'évènement.
3. La **description** de l'action ou de l'évènement, incluant les détails de son avancement ainsi que les comptes et machines concernés.

Ce document sera utile pour :

- 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 effets de bord.

Cette main courante doit être éditable et consultable par tous les intervenants. Il est déconseillé de la stocker dans le périmètre sous déni de service, mais peut l'être sur un partage de fichiers en ligne (cloud), 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 section présente les conclusions attendues des évaluations, qui permettront de qualifier l'incident. La section suivante détaillera les questions et actions à mener pour guider ces évaluations étape par étape.
La partie suivante présentera des actions détaillées pour guider 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 IP de broadcast FQDN Domaine

Type d'attaque	Couche OSI	Service	Protocol	Caractéristiques discriminantes (TCP Flag, User-agent, etc.)
- Attaque par réflexion ou rebond - Attaque par réflexion ou rebond de nos infrastructures - TCP SYN flood - UDP flood - Amplification DNS - Malformed SSL - HTTP(S) Flood - Attaque avec connaissance des faiblesses applicatives - HTTP/1.1 attack - Standard HTTP/2 attack - HTTP/2 Rapid Reset attack - Carpet bombing - Autres	Niveau3 Niveau4 Niveau6 Niveau7	DNS SNMP NTP HTTP HTTPS Autres	TCP UDP ICMP	

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 ?*
- ☐ *L'incident cause-t-il un impact chez un Tiers ? (en cas d'attaque par réflexion ou rebond de nos infrastructures)*

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 ?*

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-t-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ L'incident est-il *urgent* à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?
- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?

1. Anomalie courante
2. Incident mineur
3. Incident majeur
4. Crise cyber

MÉTHODE D'ÉVALUATION PAS À PAS

Le schéma d'architecture (Figure 1) illustré ci-après 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.
L'objectif du schéma est de faire comprendre que le trafic malveillant va traverser plusieurs périmètres :

- En amont, où l'administration est dans la plupart des cas déléguée (Fournisseur d'accès à internet - FAI, services dépendants)
- A l'hébergeur, où les moyens d'administration sont dans ce cas en général mieux maîtrisé

> **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

> **NOTE**
>
> Si la caractérisation d'un déni de service est sans équivoque, cette action peut être sautée. Dans le cas contraire, cette action peut être parallélisée avec l'action 1.b pour plus d'efficacité.

Avant de conclure que l'altération du service soit 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, pré-production, etc.) ;
- ☐ Expiration de licence, contrat, certificat, nom de domaine ;
- ☐ Problème technique interne ou externe (actifs au sein de l'hébergeur, les liens internet, les composants tiers, etc.) ;
- ☐ Compte de service supprimé, désactivé, bloqué ou dont le mot de passe a changé/expiré ;
- ☐ Faiblesse de conception de l'architecture : Pic d'activité plus élevé en fonction des activités métiers (ex : clôture comptable, résultat d'examen, etc.) ;
- ☐ Actions prévues en cours sur la production (Test de charge, scan de vulnérabilité, etc.).

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

- ☐ Supervision de sécurité
  - Détection du SOC ou du NOC
  - Alertes : pare-feux, pare-feux applicatifs, proxy inverse, commutateurs réseaux, NIPS/NIDS, etc.
- ☐ Supervision systèmes
  - 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 habituelle

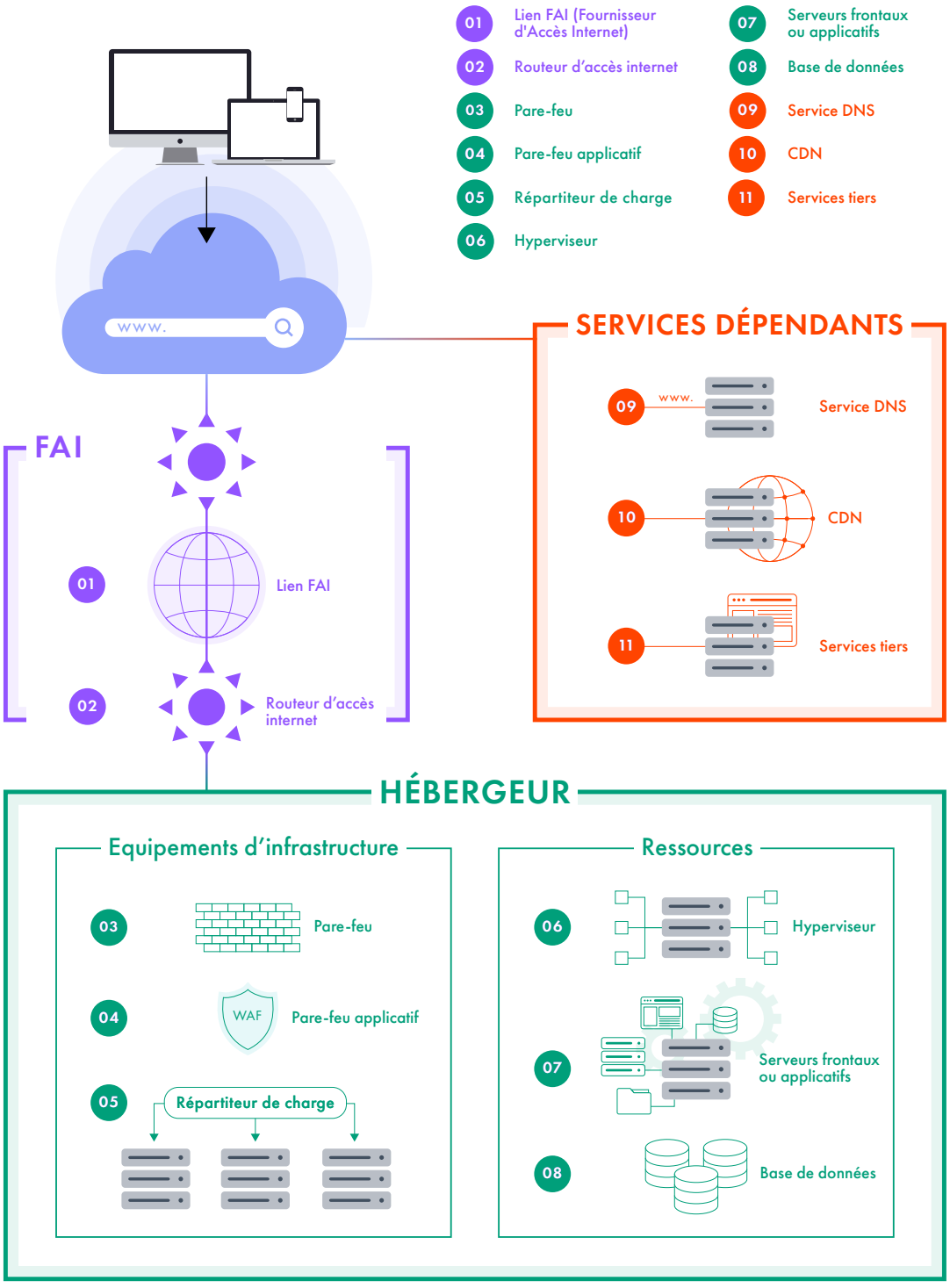


Figure 1 – Architecture d'hébergement

- ☐ Supervision réseaux : analyse de collecte du trafic réseau (fonction de capture réseau depuis les équipements de communication et sécurité ou depuis une machine sur le réseau) ou consultation du trafic réseau (journaux réseaux sur les équipements de communication et sécurité)
    - Volumétrie anormalement élevée observée dans le trafic réseau (nombre de requêtes plus élevé ou taille de requêtes élevée)
    - Récurrence et/ou motif réseaux caractéristique d'une attaque observée dans le trafic réseau
- ☐ Signalement
    - Utilisateurs ou partenaires n'accédant plus à un ou plusieurs services ou observant des ralentissements
    - Chercheur ou équipe Cyber threat Intelligence (CTI) qui aurait la connaissance de la configuration des botnets
    - Revendication d'un attaquant (Internet, Média sociaux, Courriel, autres)
        - ▷ Garder une trace de la revendication en réalisant une capture d'écran, par exemple

> **NOTE**
> Les attaques par déni de service peuvent perturber la chaîne de remonté des alertes. L'absence de remontée des journaux peut aussi être un indicateur.

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

Action 1.d : (Conclure) Confirmer l'incident de type déni de service réseau

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

- ☐ 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 du (3) pare-feu en bordure de l'entité ou à partir des équipements (1) et (2) 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 diagnostic 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

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 ou fournisseur d'accès à internet (FAI) `[Périmètre FAI]`

- (1) Lien FAI
  - ▷ Surcharge de la bande passante dans les outils de surveillance du FAI ou dans les outils de surveillance interne (sur le pare-feu en bordure par exemple)
- (2) Routeur d'accès internet
  - ▷ Indisponibilité de l'équipement dans les outils de surveillance du FAI ou les outils de surveillance interne (perte de ping sur l'équipement par exemple)

▶ Des équipements d'infrastructure réseau `[Périmètre Hébergeur]`

- (3) Pare-feu, (4) Pare-feu applicatif, (5) 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]`

- (6) Hyperviseur, (7) Serveurs frontaux ou applicatifs, (8) Serveurs de base de données
  - ▷ Saturation des ressources (calcul, mémoire ou disque)
  - ▷ Application, processus, service ou compte bloqué (surveillance dans l'interface d'administration ou dans les journaux applicatifs)
  - ▷ Indisponibilité réseau de l'équipement dans les outils de surveillance (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 atteint
    - □ 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]`

- (9) 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

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 vagues d'attaque observées et leur durée ?
- ☐ Quelles sont les métriques observables à partir des journaux ou des consoles des équipements (1) (2) (3) ?
  - 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

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

A partir des journaux du (3) pare-feu en bordure de l'entité ou à partir des équipements (1) et (2) avec l'assistance du FAI, déterminer les éléments suivants :

- ☐ Déterminer le type de déni de service en identifiant le nombre d'IP sources 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-reseaux 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 réflexion ou rebond]`)
  - D'adresses IP sources falsifiées dans les requêtes (UDP par ex.) :
    - ▷ IP source usurpée pour atteindre une autre cible (Type d'attaque : `[Attaque par réflexion ou rebond de nos infrastru` nos infrastructures participent à un déni de service)
    - ▷ IP source privée (RFC1918)
    - ▷ IP source null ou invalide
  - Difficile à différentier ou catégoriser ? (Source des requêtes : `[Hautement distribuée]`)
- ☐ Déterminer les *services visés* (IP de destination des requêtes) :
  - `IP`
  - `IP de broadcast`
  - `FQDN`
  - `Domaine`
- ☐ L'incident génère-t-il beaucoup de trafic sortant (réaction possible) ? (Type d'attaque : `[Attaque par réflexion ou rebond de nos infrastructures]` : nos infrastructures participent à un 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]`) :
  - *Diagnostic à partir des journaux des équipements (1), (2), (3), (4), (5), (7) ou par capture réseau*
  - Attaque sur les protocoles liée 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]`) :
  - *Diagnostic à partir des journaux des équipements (1) (2) (3) ou par capture réseau, et (9) pour les requêtes DNS*

- Attaque sur les protocoles liée 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])

☐ Déni de service sur protocole TLS (catégorie [Protocole], couche OSI [Niveau6]) :

- *Diagnostic à partir des journaux des équipements (1), (2), (3), (4), (5), (7) ou par capture réseau*
- 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])

☐ Déni de service applicatif (catégorie [Applicatif], couche OSI [Niveau7]) :

- *Diagnostic à partir des journaux des équipements (1), (2), (3), (4), (5), (7), (8) ou par capture réseau*
- 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 ou stockage)
    - □ Requêtes de très longue durée bloquant les sessions ouvertes (observation avec Netstat ou sur les pare-feux)
    - □ Requêtes forgées pour créer un bug dans l'application ou en base de données (Type d'attaque [Attaque avec connaissanc 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 pare-feux applicatifs)
- Attaque sur les services DNS
  - ▷ Inondation de requêtes DNS (Type d'attaque [DNS Flood] , [Amplification DNS])
- Attaque d'autres services
  - ▷ Inondation de requêtes SNMP, NTP, autres

☐ Autres éléments discriminants :

- *Diagnostic à partir des journaux des équipements (1), (2), (3), (4), (5), (7), (8) ou par capture réseau*
- 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

☐ Plusieurs catégories sont utilisées dans l'attaque : [Carpet bombing]

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

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

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 IP de broadcast FQDN Domaine

Type d'attaque	Couche OSI	Service	Protocol	Caractéristiques discriminantes (TCP Flag, User-agent, etc.)
- Attaque par réflexion ou rebond - Attaque par réflexion ou rebond de nos infrastructures - TCP SYN flood - UDP flood - Amplification DNS - Malformed SSL - HTTP(S) Flood - Attaque avec connaissance des faiblesses applicatives - HTTP/1.1 attack - Standard HTTP/2 attack - HTTP/2 Rapid Reset attack - Carpet bombing - Autres	Niveau3 Niveau4 Niveau6 Niveau7	DNS SNMP NTP HTTP HTTPS Autres	TCP UDP ICMP	

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 partie ?
- ☐ 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 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 en sens RGPD (santé, origine raciale, etc.)

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 payants ou de machines virtuelles, etc.) ?

Action 4.d : Cas de l'attaque par réflexion ou rebond de nos infrastructures

Nos infrastructures peuvent-être utilisées lors d'une attaque de déni de service pour atteindre une autre cible. Si du trafic sortant peut-être observé à destination d'IP identifiables :

- ☐ L'incident cause-t-il un impact chez un tiers ?

Action 4.e : 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 ?

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

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

- ☐ *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 ?*
- ☐ *L'incident cause-t-il un impact chez un tiers ? (en cas d'attaque par réflexion ou rebond de nos infrastructures)*

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-t-il une procédure de continuité d'activité en mode nominal ?
- ☐ Existe-t-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 mises 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 ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident :

- ☐ L'incident de sécurité 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-t-il un *impact fort* pour mon *activité métier* et le fonctionnement de mon *système d'information* ?
- ☐ L'incident est-il *urgent* à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?

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

1. Anomalie courante
2. Incident mineur
3. Incident majeur
4. Crise cyber

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

> **REMARQUE**
>
> Dans le cas de prestations externalisées, demander si des services peuvent être activés afin d'atténuer le déni de service (inclus et en supplément) et sous quel délai ils pourraient être mis en oeuvre 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*.

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

ANNEXES

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 - Déni de service réseau - Endiguement
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- Cyberattaques et remédiation

Contacts

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

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation	Se référer aux procédures internes.	Pour les organisation disposant d'une équipe de réponse à incident interne.
CERT/CSIRT externe en prestation de réponse à incident	`https://www.cybermalveillance.gouv.fr/diagnostic/accueil` `https://cyber.gouv.fr/prestataires-de-reponse-aux-incide`	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CSIRT régional	`https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux`	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations
CERT sectoriel	`https://www.cert-aviation.fr` `https://www.m-cert.fr` `https://esante.gouv.fr/produits-services/cert-sante`	Pour les organisations du secteur de l'aviation, maritime ou santé
CERT-FR	`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 effectuées :

Qui ?	Comment ?	Pourquoi ?
Assureurs		Notifier son assurance cyber permet de démarrer la prise en compte de la couverture et d'identifier des prestataires que l'assureur pourra recommander ou mandater.

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-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 préparée en amont, contextualisée et traduite en une *procédure interne et actionnable immédiatement* à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.
Il est également conseillé d'imprimer les fiches réflexes afin qu'elles restent disponibles en cas d'indisponibilité du système d'information. Il en va de même pour les autres documents utiles, comme la notice d'aide au dépôt de plainte ou votre annuaire de contacts.

Définitions

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.

Compromission d'un compte de messagerie

Une *compromission d'un compte de messagerie* désigne un accès non autorisé à un compte de messagerie, par un attaquant. Ce dernier peut alors lire et envoyer des courriels à l'insu de l'utilisateur légitime du compte, et accéder à ses données.

Compromission système

Une *compromission système* est l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information, résultant en sa prise de contrôle.
Faute de pouvoir qualifier précisément la prise de contrôle, dans de nombreux cas, toute activité adverse sur le système pouvant avoir donné lieu à une escalade de privilège est considérée comme une compromission. Une compromission entraîne généralement une forme de communication entre la machine compromise et un attaquant y exécutant des actions.

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*.

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.

Fuite de données

Une *fuite de données*, également appelée *violation de données*, désigne un incident au cours duquel des informations confidentielles, sensibles ou protégées sont consultées, divulguées ou volées par une personne non autorisée. Cela peut concerner divers types de données, notamment des informations personnelles, financières, médicales, ou des secrets commerciaux.
Les fuites de données peuvent résulter de cyberattaques, comme le piratage ou le phishing, mais aussi d'erreurs humaines, telles que l'envoi d'informations à la mauvaise adresse e-mail ou la perte de dispositifs contenant des données sensibles. Les conséquences d'une fuite de données peuvent être graves, allant de pertes financières et d'atteintes à la réputation de l'entreprise à des problèmes juridiques et à la compromission de la vie privée des individus concernés.

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.

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.

Vous pouvez trouver l'ensemble de ces fiches au lien suivant :
`https://www.intercert-france.fr/publications/fiches-reflexes/`

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