

FICHE RÉFLEXE

Chiffrement ou effacement en cours

Endiguement



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 logiciel malveillant de chiffrement ou d'effacement, par exemple de type rançongiciel, est en train de s'exécuter sur le système d'information.

À 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.

Comment l'utiliser ?

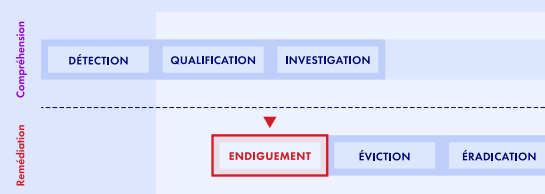
Deux parties principales composent cette fiche :

- La partie Actions d'endiguement par priorités pointe l'ordre chronologique et prioritaire des actions détaillées dans la partie suivante.
- La partie Actions d'endiguement par thèmes 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.

SOMMAIRE

Prérequis	3
Actions d'endiguement par priorités	4
Actions d'endiguement par thèmes	5
Suite des actions	13
Annexes	14





PRÉREQUIS

Avoir qualifié l'incident

Avoir *qualifié* que l'incident en cours sur le système d'information soit bien une *exécution d'un logiciel malveillant de chiffrement ou d'effacement*, par exemple de type rançongiciel, et en avoir évalué la gravité :

Fiche précédente conseillée : Fiche réflexe - Chiffrement ou effacement en cours - 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 et l'*urgence* à résoudre la situation.

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.

Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.

Ouvrir une main courante

Dès le début de l'incident, ouvrir une *main courante* pour tracer 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** en charge de cette action ou ayant informé sur l'évènement (ou le nom du service de sécurité ayant détecté 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 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.



ACTIONS D'ENDIGUEMENT PAR PRIORITÉS

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

Actions	Priorité
Isoler temporairement d'Internet (<i>Mesure 1 - Action 1.a</i>)	P0
Préserver les sauvegardes (<i>Mesure 4</i>)	P0
Préserver les serveurs de fichiers non sauvegardés (<i>Mesure 5</i>)	P0
Isoler les machines infectées (<i>Mesure 2</i>)	P0
Préserver un contrôleur de domaine (Windows) (<i>Mesure 6</i>)	P1
Entraver la propagation du chiffrement (<i>Mesure 3</i>)	P2
Préserver les traces (<i>Mesure 7</i>)	P2
Rétablir progressivement les accès Internet essentiels (<i>Mesure 1 - Action 1.b</i>)	P3



ACTIONS D'ENDIGUEMENT PAR THÈMES

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

- ▶ Contenir la propagation de l'attaque
 - Mesure 1 - Isoler temporairement d'Internet
 - Mesure 2 - Isoler les machines infectées
 - Mesure 3 - Entraver la propagation du chiffrement
- ▶ Préserver les biens essentiels de l'organisation
 - Mesure 4 - Préserver les sauvegardes
 - ▷ Mesure 4.1 - Préserver les serveurs de gestion des sauvegardes
 - ▷ Mesure 4.2 - Préserver les supports de stockage des sauvegardes
 - ▷ Mesure 4.3 - Préserver les serveurs de sauvegarde sur hyperviseur
 - ▷ Mesure 4.4 - Préserver les serveurs de sauvegarde dans le cloud
 - Mesure 5 - Préserver les serveurs de fichiers non sauvegardés
 - Mesure 6 - Préserver un seul contrôleur de domaine (Windows)
- ▶ Préserver les traces
 - Mesure 7 - 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.

Contenir la propagation de l'attaque

Mesure 1 - Isoler temporairement d'Internet

Avant d'essayer d'isoler une par une les machines chiffrées par le rançongiciel, il est possible dans un premier temps de couper temporairement les communications avec Internet :

Action 1.a : Couper les communications Internet sur les pare-feux périphériques

- ☐ Désactiver tous les *flux entrants* Internet vers toutes les zones internes
 - ☐ Ne pas oublier de désactiver notamment les accès VPN depuis Internet
- ☐ Désactiver tous les *flux sortants* Internet depuis toutes les zones internes
- ☐ Pour les *flux WAN* entre différents sites de l'organisation, arbitrer entre :
 - ☐ Maintenir les accès WAN essentiels pour préserver les flux métiers internes
 - ☐ Couper les accès WAN pour isoler le périmètre compromis du reste du système d'information
- ☐ Vérifier par des tests l'isolation d'Internet en entrée et en sortie (test de navigation Internet, test de *ping*, supervision du monitoring réseau, ou autres tests simples)

Cette mesure d'isolation a pour objectif de priver le rançongiciel de son serveur de contrôle, et ainsi :

- ▶ Empêcher le rançongiciel de recevoir de nouveaux ordres de chiffrement et de latéralisation, d'exfiltration de données sensibles, d'installation de nouvelles portes dérobées et persistances.
- ▶ Empêcher l'attaquant d'observer les actions des défenseurs et d'entraver la remédiation en cours.
- ▶ Donner du temps aux défenseurs pour analyser la situation et se concentrer sur la suite de l'endiguement de la propagation et des investigations.

Globalement, tant que l'investigation n'est pas terminée et que les moyens de communication de l'adversaire ne sont pas identifiés, il est déconseillé de permettre des communications non contrôlées par une *liste blanche* et non essentielles (ceci est valable pendant la remédiation ou une reconstruction trop hâtive).



IMPACT

L'action d'isolation d'Internet va temporairement saturer le service d'assistance HelpDesk, bloquer les télémaintenances, perturber les services essentiels, bloquer les mises à jour (y compris des antivirus et autres solutions de sécurité), bloquer les liens avec les applications cloud (y compris de sécurité), bloquer l'accès à des services tiers, etc.*



REMARQUE

Priver l'entreprise d'Internet peut engendrer un coût, mais celui-ci est à comparer au coût de la propagation du chiffrement et de la perte des données métiers, et au coût de la remédiation et de la reconstruction qui s'ensuivra (prestation de réponse à incident, prestation de reconstruction, service détérioré, coût RH - business - juridique, etc.).

Action 1.b : Rétablir progressivement les accès Internet nécessaires au traitement de l'incident ou à la survie de fonctions essentielles

- ☐ **Flux entrant** : Un flux entrant essentiel peut être rétabli à condition d'ajouter un second facteur d'authentification en plus du simple mot de passe (adresse IP source en *liste blanche*, MFA, etc.) aux acteurs suivants :
 - ☐ Acteurs de services de réponse à incident
 - ☐ Acteurs essentiels au maintien d'activité et à l'infogérance (avec prudence car ils sont potentiellement vecteurs de la compromission)
- ☐ **Flux sortant** : Un flux sortant essentiel peut être rétabli à condition de restreindre l'adresse IP ou le domaine de destination avec une *liste blanche* (en utilisant un équipement de type proxy ou pare-feu) aux services suivants :
 - ☐ Services de sécurité : SOC, mises à jour et accès à la console de l'antivirus/EDR, supervision
 - ☐ Services essentiels au maintien d'activité

Attention : Avant de rétablir les flux réseau, s'assurer que la passerelle d'accès Internet et le VPN n'aient pas été compromis. Pour cela, vérifier si l'équipement est à jour, que sa version n'est pas vulnérable à une CVE en cours, et qu'aucun compte illégitime n'ait été rajouté dans les groupes d'administration de l'équipement.

Mesure 2 - Isoler les machines infectées

Préserver une machine infectée par un rançongiciel permettra d'éviter sa propagation depuis cette machine vers le reste du système d'information :

Action 2.a : Préserver les machines infectées du reste du système d'information

- ☐ Si ce sont des *machines virtuelles*, mettre ces serveurs en pause
- ☐ Si ce sont des *machines physiques Windows*, les mettre en *veille prolongée*
- ☐ Sinon, si possible, *isoler* la machine du réseau, par exemple en débranchant le câble réseau et en désactivant le Wifi (cela évitera de purger la mémoire mais n'arrêtera pas le chiffrement s'il était encore en cours).
 - Si vous avez utilisé une fonction d'isolation de votre EDR, mentionnez-le explicitement dans la main courante.
- ☐ Sinon, en dernier recours, *éteindre* la machine si elle n'est pas complètement chiffrée (cela arrêtera le chiffrement mais purgera la mémoire).



REMARQUE

Autant que possible, *éviter d'éteindre électriquement* une machine chiffrée car cela purgerait la mémoire RAM. Or, préserver la mémoire pourrait permettre de trouver des *artefacts d'investigation*, retrouver des fichiers supprimés, concourir à retrouver des *clés de déchiffrement* nécessaire au recouvrement des données par des entreprises spécialisées, etc.

Si les zones infectées sont identifiées et peuvent être concrètement isolées au niveau réseau, isoler ces zones peut éviter à l'incident de s'étendre davantage :

Action 2.b : Isoler les zones infectées du reste du système d'information

- ☐ *Isoler* au niveau du réseau les zones infectées (réseau physique ou virtualisé)

**IMPACT**

Une telle action peut avoir de grands impacts sur les applications métiers dont les interdépendances pourraient ne plus être accessibles. Si jamais cette action est réalisée, il faudra être vigilant aux remontées de dysfonctionnements de la part des équipes internes et avoir la capacité d'effectuer un retour arrière ou de filtrer finement les flux réseau strictement nécessaires.

Mesure 3 - Entraver la propagation du chiffrement

Si vous observez que la propagation du chiffrement semble continuer malgré les mesures précédentes, il est alors probable qu'un système central d'administration ait été compromis (exemple : GPO) ou que le rançongiciel chiffre les partages réseau qui lui sont accessibles depuis une machine quelconque mais avec un compte privilégié. Dans de tels cas, seules des équipes spécialisées pourront investiguer et donner des contre-mesures ciblées et efficaces. En attendant l'intervention de ces équipes, quelques actions complémentaires et génériques peuvent être tentées...

Lorsqu'on est probablement en présence d'un chiffrement des partages réseau avec des comptes privilégiés :

Action 3.a : Neutraliser les comptes à privilèges suspectés compromis

Si, pendant la phase de qualification, des comptes ont été identifiés suspects ou compromis, certaines actions peuvent être tentées, tout en prenant garde aux effets de bord qu'elles pourraient entraîner :

- ☐ Réinitialiser ces comptes (efficace uniquement si la latéralisation s'effectue par une authentification par mot de passe)
- ☐ Désactiver ces comptes (efficace immédiatement si authentification par mot de passe et avec un peu de latence pour une authentification Kerberos)
- ☐ Si, pendant la phase de qualification, le groupe ESXi Admins a été identifié comme ayant été créé de manière illégitime, il doit être renommé.

Action 3.b : Réinitialiser tous les comptes à privilèges

Si on ne sait pas quel compte à privilèges est utilisé pour le chiffrement des partages réseau, on peut vouloir neutraliser tous les comptes à privilèges avec les mêmes leviers précédents :

- ☐ Créer un nouveau compte *Administrateur de domaine* dit *bris de glace*
- ☐ Réinitialiser tous les comptes à privilèges sans oublier les comptes *administrateurs du domaine* (en utilisant le compte *bris de glace* précédent)
 - Important : ne pas oublier de noter les nouveaux mots de passe !

**IMPACT**

Agir sur les comptes à privilèges peut avoir de gros impacts en production et cela doit être fait avec précaution. Généralement, on peut rarement arrêter une propagation d'un maliciel sans causer des dommages sur la production, et le pilotage par une équipe spécialisée devient nécessaire.

**REMARQUE**

- ▶ Sur un parc Active Directory, une modification sur un compte utilisateur effectuée sur un contrôleur de domaine peut prendre du temps à être synchronisée avec les autres contrôleurs de domaine.
- ▶ Un simple compte utilisateur, même sans privilège, peut chiffrer tout un serveur de fichiers si les droits d'accès aux fichiers sont trop larges.
- ▶ La latéralisation par rebond est également possible (exemple : ver informatique), mais pour un rançongiciel, cette méthode de propagation est moins probable. Dans ce cas, les actions d'endiguement précédentes restent valables.

Lorsqu'un système central d'administration a probablement été compromis :

Action 3.c : Analyser avec un antivirus le dossier SYSVOL du domaine Active Directory

- ☐ Analyser le dossier SYSVOL du domaine Active Directory avec un antivirus à jour, depuis un ordinateur sain



Action 3.d : Inspecter certains moyens de propagation usuels

- ☐ Inspecter si des scripts ou exécutables inconnus sont présents dans le dossier SYSVOL du domaine Active Directory (exemple : \SYSVOL\<domain>)
 - Aide : Chercher les derniers fichiers créés dans le SYSVOL
- ☐ Inspecter si une GPO a été illégitimement modifiée ou créée pour exécuter du code inconnu (exécution de tâche planifiée, lancement de script au démarrage, déploiement d'un logiciel, etc.)
 - Aide : Chercher les dernières GPO modifiées
- ☐ Inspecter si une tâche planifiée inconnue a été créée sur les machines compromises et a exécuté du code inconnu

REMARQUE

Des mesures de *durcissement* permettent également d'entraver une latéralisation d'attaque, mais il est difficile de les mettre en œuvre dans le *temps chaud* d'un incident. Leur mise en œuvre sera généralement plus tard dans la remédiation, lorsque les défenseurs auront repris le contrôle de leur système d'information et pourront s'atteler à son durcissement. On peut citer comme telles mesures :
- Retirer les droits d'administration locale de tous les utilisateurs (pour entraver une élévation de privilèges locale des machines infectées). - Activer LAPS (pour entraver la latéralisation avec un compte administrateur local compromis). - etc.

Préserver les biens essentiels de l'organisation

Les sauvegardes ne doivent pas être chiffrées car elles seront primordiales pour rétablir les services du système d'information après l'incident : il faut donc les préserver au plus tôt.

Mesure 4 - Préserver les serveurs de gestion des sauvegardes

Action 4.a : Identifier les différents types de sauvegarde du système d'information

- ☐ Identifier la solution de sauvegarde des machines virtuelles
- ☐ Identifier la solution de sauvegarde des fichiers

Action 4.b : Identifier les serveurs de gestion des sauvegardes

- ☐ Identifier les serveurs physiques
- ☐ Identifier les serveurs virtuels (et l'hyperviseur qui les héberge)

Action 4.c : Préserver les serveurs de gestion des sauvegardes

- ☐ Si ce sont des *machines virtuelles*, mettre ces serveurs en pause
- ☐ Si ce sont des *machines physiques Windows*, les mettre en veille prolongée
- ☐ Dans le cas contraire, *éteindre* ces serveurs

D'autres actions sont possibles pour préserver un serveur, mais contrairement aux actions ci-dessus, elles ne permettent pas d'arrêter le chiffrement du serveur s'il était déjà en cours, ou seraient plus compliquées à réaliser sans réelle plus-value de sécurité dans le cas présent :

- ☐ *Isoler du réseau*, tout en gardant un accès d'administration physique, virtuel ou hors-bande
- ☐ *Confiner* dans un VLAN ayant des flux extrêmement limités
- ☐ *Sortir le compte d'administration du domaine Active Directory compromis*

REMARQUE

- ▶ Les sauvegardes ne doivent pas être restaurées tant que l'analyse de l'équipe de réponse à incident n'a pas conclu une *date de restauration sûre*.
- ▶ Arrêter les processus de sauvegarde des clients (*agent*) depuis la console de gestion protégera les sauvegardes des clients mais pas le serveur de sauvegarde lui-même. Cette action est donc également faisable mais a été jugée moins efficace.



IMPACT

Impossibilité de réaliser de nouvelles sauvegardes jusqu'à leur remise en service.

Mesure 5 - Préserver les supports de stockage des sauvegardes

Action 5.a : Identifier les supports de stockage des sauvegardes, accessibles depuis le réseau

- ☐ NAS
- ☐ SAN
- ☐ Robots de sauvegardes
- ☐ Lecteurs de bandes, etc.

Action 5.b : Préserver les supports de stockage des sauvegardes, accessibles depuis le réseau

- ☐ Éteindre ces supports ou les isoler du réseau, au plus efficace

D'autres actions sont possibles pour préserver un serveur, mais contrairement aux actions ci-dessus, elles ne permettent pas d'arrêter le chiffrement du serveur s'il était déjà en cours, ou seraient plus compliquées à réaliser sans réelle plus-value de sécurité dans le cas présent :

- ☐ Isoler du réseau, tout en gardant un accès d'administration physique, virtuel ou hors-bande
- ☐ Confiner dans un VLAN ayant des flux extrêmement limités
- ☐ Sortir le compte d'administration du domaine Active Directory compromis



REMARQUE

Les serveurs de gestion des sauvegardes ayant déjà été préservés par la mesure précédente : - Les supports de stockage des sauvegardes sont donc normalement sans activité et peuvent être simplement éteints. - Les supports de stockage des sauvegardes hors-ligne ou uniquement accessibles en back-end des serveurs de gestion ne sont pas accessibles par le réseau et sont considérés comme déjà préservés : disques locaux, DAS, SAN, etc. Ils n'ont donc pas besoin d'être éteints.



IMPACT

Aucun impact ne résulterait de cette mesure si ces supports ne stockent que des sauvegardes. Mais s'ils stockent des fichiers d'applications métiers, des effets de bord d'indisponibilité seront à gérer.

Action 5.c - Préserver les serveurs de sauvegarde sur hyperviseur

Si le serveur de gestion des sauvegardes est une machine virtuelle éteinte précédemment, il faut alors le préserver en l'exportant de l'hyperviseur qui l'héberge :

- ☐ Prendre un instantané de la machine virtuelle (déjà mise en pause) puis l'exporter sur un disque dédié hors ligne



REMARQUE

- ▶ Cette mesure peut ne pas être prioritaire si les serveurs hyperviseurs semblent non ciblés par le chiffrement.
- ▶ En parallèle de cette mesure de préservation, des mesures pour restreindre l'accès aux hyperviseurs peuvent être étudiées, comme les sortir du domaine Active Directory (s'ils y étaient) et n'utiliser que des comptes d'administration locaux.

Mesure 6 - Préserver les serveurs de sauvegarde dans le cloud

Des serveurs de gestion ou de stockage des sauvegardes peuvent être hébergés dans le cloud. Pour de tels serveurs, effectuer les mêmes actions que précédemment en considérant que ce sont des machines virtuelles :



Action 6.a : Préserver les serveurs de sauvegarde dans le cloud

- ☐ Identifier les serveurs de sauvegarde dans le cloud
- ☐ Mettre en pause, sinon éteindre ces serveurs
- ☐ Réinitialiser les accès des comptes privilégiés à l'environnement cloud (mot de passe, MFA, session)



IMPACT

Impossibilité de réaliser de nouvelles sauvegardes jusqu'à leur remise en service.

Mesure 7 - Préserver les serveurs de fichiers non sauvegardés

Si des serveurs de fichiers ne sont pas sauvegardés, alors ils doivent être préservés au même titre que les sauvegardes, car ils sont susceptibles de contenir des données nécessaires à la reprise d'activité de l'organisation :

Action 7.a : Identifier les serveurs de fichiers non sauvegardés

- ☐ Lister les serveurs non couverts par les moyens de sauvegarde

Action 7.b : Préserver les serveurs de fichiers non sauvegardés

- ☐ Si possible, éteindre ces serveurs immédiatement et attendre l'éradication de l'adversaire avant de les rallumer
- ☐ Sinon, pour le maintien des activités vitales, il est envisageable de les confiner dans une nouvelle bulle réseau avec les applications critiques qui en dépendent



REMARQUE

Dans le doute que les serveurs de fichiers soient sauvegardés ou pas, envisager tout de même de les éteindre selon l'impact de leur chiffrement potentiel.



IMPACT

Malheureusement, préserver un serveur de fichiers aura plus d'impacts que de préserver un serveur de stockage de sauvegardes car ils sont accessibles directement par les utilisateurs et les applications. Cette mesure engendrera sûrement une indisponibilité de service.

Mesure 8 - Préserver un contrôleur de domaine (Windows)

Si le système d'information utilise un domaine Active Directory et si on craint la compromission de compte à privilège, on peut dès à présent préserver un contrôleur de domaine en prévision de la restauration du système d'information :

Action 8.a : Préserver un seul contrôleur de domaine

- ☐ De préférence choisir un contrôleur de domaine physique et l'éteindre
- ☐ Sinon, préserver un contrôleur de domaine virtuel en l'exportant de l'hyperviseur sur un disque hors ligne (mais il peut rester allumé)



REMARQUE

Si l'entreprise possède plusieurs domaines Active Directory avec des contrôleurs de domaine distincts, il est recommandé de conserver un contrôleur de domaine par domaine. En revanche, si les différents domaines font partie d'une seule forêt, un seul contrôleur de domaine suffit.



IMPACT

Normalement, les services rendus par les contrôleurs de domaine sont redondants par clusterisation, et l'un d'eux peut donc être mis à l'écart sans coupure de service. Des effets de bord peuvent toutefois survenir si le contrôleur de domaine est le premier contacté dans la liste des DNS reçus par les clients (dont les résolutions DNS peuvent résulter en timeout) ou si le FQDN ou l'IP du contrôleur de domaine a été renseigné en dur dans un service.

Préserver les traces

Mesure 9 - Préserver les traces

Pour soutenir la réponse à incident dans son objectif d'investigation, il faut prioritairement préserver les logs les plus anciens possibles, augmenter leur rétention et leur verbosité. Plus les équipes d'investigation auront les traces d'activité de l'adversaire, plus efficace sera son éradication :

Action 9.a : Préserver les traces dans les journaux d'équipements

- ☐ Identifier les équipements de sécurité du système d'information :
 - ☐ pare-feux
 - ☐ passerelles VPN
 - ☐ proxy
 - ☐ console antivirus et EDR, etc.
- ☐ Exporter les logs sur un disque hors ligne (s'ils ne sont pas déjà dans un puits de logs)
- ☐ Augmenter la rétention des logs
- ☐ (Si possible, configurez les logs de manière à ce qu'ils soient les plus détaillés possibles)



REMARQUE

Les journaux des machines compromises sont normalement déjà préservés puisqu'elles sont soit en veille soit éteintes.

Action 9.b : Préserver les traces dans les journaux d'authentification

- ☐ Identifier la solution de stockage des journaux d'identification sur le réseau interne, comme le domaine Active Directory
- ☐ Exporter ces logs (s'ils ne sont pas déjà dans un puits de logs)
- ☐ Augmenter la rétention de ces logs

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, mais il faut néanmoins augmenter leur verbosité lorsque cela est possible. Aussi, s'il y a un doute que le puits de logs puisse être compromis, un arbitrage s'impose :

Action 9.c : Arbitrer la préservation du puits de logs

Si l'infrastructure du puits de logs (serveur de stockage, serveur de collecte, hyperviseur, etc.) doit être compromise, il convient de faire un choix entre les options suivantes :

- ☐ Préserver le puits de logs en le déconnectant du réseau (ce qui permettra de conserver les traces de l'attaque jusqu'à présent, mais sans possibilité de suivre les actions futures de l'attaquant)
- ☐ Maintenir le puits de logs accessible sur le réseau.

Action 9.d : Récupérer des fichiers liés au chiffrement

- ☐ Récupérer des fichiers chiffrés (un petit fichier et un gros de plusieurs Mo)
- ☐ Récupérer une note de rançon (ou plusieurs, s'il en existe de plusieurs types)



REMARQUE

En plus d'être indispensable à la compréhension de l'incident, sauvegarder les éléments de preuve pourra être nécessaire pour répondre aux forces de l'ordre lors d'éventuelles poursuites judiciaires.



SUITE DES ACTIONS

A la fin de ces actions d'endiguement, la compromission devrait être contenue. Pour autant, l'incident a très probablement impacté l'organisation au-delà de son système d'information et il reste encore beaucoup à faire.

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*.

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



REMARQUE

Dans le cas d'une attaque par rançongiciel, des aides spécifiques au dépôt de plainte sont mises à disposition par le CERT Santé, en collaboration avec le CSIRT-PJ : <https://cyberveille-sante.gouv.fr/dossier-thematique/aide-au-depot-de-plainte-en-cas-dattaque-par-rancongiel> Lors du dépôt de plainte, le Rapport Initial d'Incident (R2IP) est à annexer systématiquement à la plainte. Le CSIRT-PJ peut vous accompagner dans cette démarche.



ANNEXES

Liens utiles

Lors d'une lecture préparatoire de cette fiche ou pour aller plus loin dans la compréhension et la mise en œuvre des notions évoquées, certains documents annexes peuvent être utiles :

- ▶ Fiche réflexe - Chiffrement ou effacement en cours - Qualification
- ▶ Comment réagir en cas d'incident rançongiciel
- ▶ Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique
- ▶ Cyberattaques et remédiation

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.

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 organisations 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-incidents-de-securite-pris	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.
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.