Fiche réflexe

Compromission système

Endiguement

2025

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'une **compromission est fortement suspectée** (levée de doute en cours) **ou confirmée sur une machine Windows ou Linux du système d'information.**

3 A quoi sert-elle ?

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

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Actions d'endiguement par priorités** pointe l'ordre 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

Fiche réflexe
- Compromission système -
Endiguement

Prérequis

01

Avoir qualifié l'incident

Avoir qualifié que l'incident en cours sur mon système d'information soit bien lié à **l'activité d'un code ou d'un acteur malveillant sur une ou plusieurs machine(s) du système d'information** :
Fiche précédente conseillée : Fiche réflexe - Compromission système - Qualification

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

Si la qualification permet de suspecter un début d'incident rançongiciel, il convient de dérouler la séquence :
• Fiche réflexe - Chiffrement ou effacement en cours – Qualification/Endiguement (https://cyberveille.esante.gouv.fr/dossier-thematique/chiffrement-en-cours-qualification-et-endiguement)

02

Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement aient les **droits d'administration** du système d'information : réseau, système, sécurité opérationnelle.

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

03

Ouvrir une main courante*

Dès le début de l'incident, ouvrir une **main courante** pour **tracer toutes les actions et événements** survenus sur le système d'information dans un **ordre chronologique**. Chaque ligne de ce document doit représenter une action avec au minimum trois informations :

1. La date et l'heure de l'action ou de l'évènement (si estimé nécessaire, ajouter le fuseau horaire UTC)
2. Le nom de la personne ayant réalisé cette action ou ayant informé sur l'évènement
3. La description de l'action ou de l'évènement et les machines concernées

Ce document sera utile pour :
- Réaliser un historique du traitement de l'incident et partager la connaissance
- Piloter la coordination des actions et suivre leur état d'avancement
- Évaluer l'efficacité des actions et leurs potentiels impacts non prévus

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

Prérequis

04

Prendre en considération la présence active d'un attaquant

Important : Dans les actions d'endiguement, il est important d'éviter d'ouvrir une session interactive avec la machine suspectée compromise : connexion locale, RDP et SSH sont à minimiser, à fortiori avec un compte privilégié.

Si les actions à distance sont impossibles, autant que faire se peut :

1. Préférer les actions au travers d'un EDR.
2. Sinon, préférer une connexion locale - console physique, hors bande (Out-of-Band) ou d'hyperviseur – avec un compte administrateur uniquement local au système concerné.
3. En dernier recours, utiliser une connexion par le réseau qui ne met pas en danger le mot de passe des administrateurs : **Powershell Remoting** ou **Windows Remote Shell (WinRS)** qui permettent d'ouvrir l'équivalent d'un terminal, ou **RDP** en mode **Restricted Admin** qui n'autorise que Kerberos et n'autorise pas la mise en cache du **TGT**.

Tracer impérativement ces actions de connexion sur une machine compromise dans la main courante

Actions d'endiguement par priorité

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

Actions	Priorité
Déclarer l'incident	P0
Figer la situation (Mesure 1)	P0
Sécuriser des sauvegardes à jour (Mesure 3)	P1
Préserver les traces sur les machines infectées (Mesure 4)	P1
Réinitialiser les identifiants probablement compromis (Mesure 2)	P2
Préserver les traces des journaux d'équipements (Mesure 5)	P2

Important : La préservation des traces doit être une préoccupation pour tous les choix d'actions. Il conviendra de préférer les actions les altérant le moins possible, y compris dans la partie "figer la situation".

Actions d'endiguement par thèmes

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

Actions d'endiguement par thèmes

Une compromission système n'est qu'une étape dans la tentative de compromission du système d'information. Un adversaire s'y est introduit et y a certainement eu une activité.

Le traitement d'un tel incident ne doit pas être limité à la suppression de codes malveillants mais doit faire l'objet de mesures complémentaires.

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

- Limiter l'extension de la compromission
  - Mesure 1 - Figer la situation
  - Mesure 2 - Réinitialiser les identifiants suspectés compromis
  - Mesure 3 - Réinitialiser les secrets liés à la machine infectée
- Préserver les biens essentiels de l'organisation
  - Mesure 4 - Sécuriser des sauvegardes à jour
- Préserver les traces
  - Mesure 5 - Préserver les traces sur les machines infectées
  - Mesure 6 - Préserver les journaux

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**.

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Lors d'une compromission système, il est a priori rare de savoir à quel stade de l'attaque la détection est survenue: intrusion initiale, latéralisation ou réalisation de l'effet recherché par l'attaquant.
Il convient donc de limiter les capacités de l'attaquant à contrôler la machine compromise et éventuellement à réagir aux mesures d'endiguement.

Mesure 1 - Figer la situation

Action 1.a : Interrompre l'activité de la machine infectée

- Si la machine infectée ne porte pas un système à forte exigence de disponibilité :
  - ❑ Si le système compromis est une machine virtuelle, mettre cette machine en pause
    - ➢ si possible renommer la machine avec une mention "ne pas rallumer" pour éviter un redémarrage accidentel
  - ❑ Si c'est une machine physique qui supporte la mise en veille, la mettre en veille prolongée
  - ❑ Sinon déconnecter la machine du réseau :
    - ❑ Préférer par isolation utilisant un EDR
    - ❑ Sinon par configuration
      - ➢ En utilisant au choix : pare-feu d'infrastructure ou commutateur réseau.
    - ❑ Enfin, par déconnexion physique
    - ➢ Attention: penser aux réseaux sans fil vers lequels l'équipement pourrait basculer
  - ❑ En dernier recours, si la déconnexion du réseau est impossible, éteindre la machine
    - ➢ Si les outils sont disponibles, effectuer une collecte forensique avant extinction (y compris copie mémoire)
- Si la machine ne peut être rendue indisponible :
  - ❑ Procéder aux isolations réseau de l'Action 1.b est particulièrement important
  - ❑ Si un EDR est disponible et que la machine ne peut être arrêtée, il est possible de neutraliser un processus attaquant identifié.
    - Cette mesure ne résout pourtant pas l'incident : l'outil hostile a été installé sur le poste et potentiellement déjà utilisé pour se latéraliser vers d'autres machines.
    - Veiller à préserver les informations relatives à l'outil : condensat, voire copie du fichier.

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Mesure 1 - Figer la situation

Action 1.b : Isoler au niveau réseau les zones infectées du reste du système d'information

- Si possible, isoler par le réseau les zones contenant la machine infectée (réseau physique ou virtuel) en pensant à couper les flux dans les deux sens :
  - ❑ Couper les flux par *configuration*, si possible
    - ➢ Sur des pare-feu d'infrastructure, règles de filtrage dans les serveurs mandataires (proxy) ou d'ACL sur les équipements de niveau 2
  - ❑ Sinon, procéder à une *déconnexion physique*
- Si la machine infectée accédait à une zone particulièrement sensible (réseau industriel, SIIV...)
  - ❑ Considérer un passage temporaire de ce dernier en mode isolé ("mode ilot" pour le monde industriel) déconnecté du SI bureautique, le temps de lever l'alerte.
- Si les zones infectées sont identifiées et peuvent être concrètement isolées par le réseau d'autres zones interconnectées (systèmes industriels, filiales, partenaires, etc.)
  - ❑ Isoler ces zones par le réseau peut éviter à l'incident de s'étendre davantage.
- Dans le cas d'infrastructures cloud (IaaS)
  - ❑ Fermer les réseaux exposés à Internet et vérifier qu'aucune interface réseau ne soit exposée sur Internet ou aux réseaux inter-clients

L'isolation pourra être levée dès qu'il sera possible de vérifier l'innocuité des autres machines de la zone.

Impacts : Une telle action peut avoir de grands impacts sur les applications métiers dont les dépendances pourraient ne plus être accessibles. Si jamais cette action est réalisée, il faudra être vigilant aux signalements de dysfonctionnements de la part des équipes métiers des applications critiques et avoir la capacité d'effectuer un retour arrière ou de filtrer finement les flux réseaux.

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Mesure 2 - Réinitialiser les identifiants suspectés compromis

Les comptes utilisés sur un système compromis doivent être également considérés comme compromis. Leurs identifiants doivent être réinitialisés et leur activité doit faire l'objet d'une revue.

Une machine Linux peut être inscrite dans un annuaire, y compris Windows Active Directory, et dans ce cas, les mêmes précautions que sous Windows s'imposent.

Action 2.a : Désactiver tous les comptes utilisateurs suspectés compromis

Si des comptes ont récemment été utilisés pour se connecter sur la machine compromise (depuis le dernier redémarrage) :

- ❑ Désactiver ces comptes dans l'Active Directory (quels que soient leurs privilèges et sensibilité)
- ❑ Prévoir une rotation d'identifiants par la suite

Action 2.b : Désactiver tous les comptes administrateurs du domaine suspecté compromis

- ❑ Si ce sont des comptes individuels, les désactiver dans l'Active Directory
- ❑ Si c'est le compte administrateur du domaine par défaut (RID 500), **effectuer une rotation de mot de passe du compte**

Il faut considérer la compromission du domaine Windows dans son ensemble car l'attaquant a pu en altérer l'intégrité ou s'émettre des tickets privilégiés.

Action 2.c : Réinitialiser les comptes homonymes sur les autres machines

Si des comptes locaux homonymes aux utilisateurs interactifs de la machine compromise existent sur d'autres machines :

- ❑ Effectuer une rotation du mot de passe de ces comptes.

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Mesure 2 - Réinitialiser les identifiants suspectés compromis

Action 2.d : Réinitialiser ou bloquer les comptes utilisés sur la machine infectée

Si la machine infectée contenait des identifiants de comptes permettant de s'authentifier sur d'autres machines ou applications du système d'information, comme ceux-ci :

- comptes de service
- comptes applicatifs utilisateurs internes et externes
- comptes privilégiés vers d'autres machines
- secrets applicatifs sur les postes développeurs

❑ Désactiver ces comptes
❑ Sinon, réinitialiser leurs identifiants et les secrets applicatifs

Action 2.e : Révoquer les sessions des comptes utilisés sur la machine infectée

Si des comptes, tels que mentionnés à l'action précédente ont ouvert des sessions sur des applications web de l'organisation :
❑ Déconnecter les sessions système en cours
❑ Révoquer les sessions applicatives
❑ Révoquer ou invalider les jetons en cours sur les applications Web et Cloud: OAuth, SAML...

Action 2.f : Supprimez les clefs SSH des autres serveurs

Si la machine infectée contenait des clefs privées SSH :
❑ Supprimer les clés publiques associées aux fichiers **authorized_keys** sur les autres serveurs (`$HOME/.ssh/authorized_keys` et `/etc/ssh/keys`)

- Considérez de chercher ces clés sur tous les composants du système d'information exposant un serveur SSH en interne ou externe à l'organisation.

Action 2.g : Réinitialiser les comptes cloud

Si la machine était utilisée pour accéder à des services cloud :
❑ Effectuer une rotation du mot de passe de ces comptes
❑ Révoquer sa session/token
❑ Fiche conseillée : Fiche réflexe - Qualifier la compromission d'un compte de messagerie (https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-dun-compte-de-messagerie-qualification-et-endiguement)

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Mesure 3 - Réinitialiser les secrets liés à la machine infectée

Action 3.a : Révoquer les certificats de la machine infectée

Si la machine infectée contenait des certificats (802.1X, VPN, etc.) :
- ❑ Révoquer ces certificats
- ❑ S'assurer de la publication de la révocation (rafraichissement de CRL, publication sur le serveur OCSP)

Action 3.b : Réinitialiser les jetons ou clés d'API présents sur les comptes des machines compromises

Si la machine infectée contenait des identifiants applicatifs (token d'API)
- ❑ Révoquer les jetons, et, si nécessaire, en déployer de nouveaux sur d'autres instances partageant la même clé

Action 3.c : Si la machine compromise est inscrite dans un *Active Directory*
- ❑ Désactiver le compte machine dans l'Active Directory

Impacts : Les changements de comptes de service impactent les fonctionnements applicatifs. Il convient de vérifier la disponibilité et la bonne exécution des processus métier après tout changement.

Actions d'endiguement par thèmes

Préserver les biens essentiels de l'organisation

Mesure 4 - Sécuriser des sauvegardes à jour

Les **sauvegardes** sont primordiales pour rétablir les services du système d'information en cas d'incident destructif : il faut donc les préserver en cas de suspicion d'incident majeur.

Ces sauvegardes pourront aussi servir de source de données pour l'investigation sur l'incident.

Action 4.a : Sécuriser des sauvegardes à jour

S'assurer de l'existence d'une sauvegarde récente des données accessibles depuis la machine compromise :
❑ Serveurs de fichiers
❑ Serveurs accessibles interactivement aux utilisateurs de la machine
❑ En cas de doute sur le périmètre de compromission, limiter l'accès

Action 4.b : Valider l'accès fonctionnel aux sauvegardes

❑ Serveur de restauration accessible uniquement aux utilisateurs de la machine

Actions d'endiguement par thèmes

Préserver les traces

Mesure 5 - Préserver les traces sur les machines infectées

Action 5.a : Préserver les traces sur les machines infectées

Si la machine infectée est une machine virtuelle :
❑ Prendre un instantané de la machine virtuelle (déjà mise en pause) puis l'exporter sur un disque dédié hors ligne

Sinon la machine infectée est une machine physique :
❑ Effectuer un prélèvement forensique
- ➢ en utilisant l'EDR
- ➢ par un agent forensique
- ➢ par service d'administration
- ➢ ou exécutant manuellement un outil de prélèvement

Mesure 6 - Préserver les journaux (Logs)

Action 6.a : Préserver les traces dans les journaux d'équipements

❑ Identifier les équipements de sécurité du système d'information :
- pare-feu
- passerelles VPN
- proxy
- console antivirus et EDR, etc.

❑ Exporter les journaux historiques
❑ Augmenter la rétention des évènements dans les journaux ou suspendre leur rotation
❑ Activer les journaux les plus complets possibles et supportables (espace disque, impact performance)

Action 6.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 journaux (depuis consoles; contrôleurs de domaine, IDP, ou cloud)
❑ Augmenter la rétention de ces journaux ou suspendre temporairement leur rotation

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 en cas d'éventuelles poursuites judiciaires.

Suite des actions

A la fin de ces actions d'endiguement, la compromission devrait être contenue.

La neutralisation supposée des actions de l'attaquant ne permet pas de savoir comment la machine a été compromise, à quelle étape de l'attaque la détection a eu lieu ou l'ampleur d'autres compromissions. Seule une analyse approfondie des événements permettra de comprendre ces éléments.

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

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

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

Remarque :
De plus, si l'incident a un **périmètre étendu** sur le système d'information, qu'il a un **impact fort** et qu'il nécessite une **résolution urgente** :

- Activer le **dispositif de gestion de crise cyber** de l'organisation pour piloter la résolution de l'incident et la continuité d'activité.
  Guide conseillé : Crise cyber, les clés d'une gestion opérationnelle et stratégique (https://cyber.gouv.fr/publications/crise-cyber-les-cles-dune-gestion-operationnelle-et-strategique)

Annexes

Définitions

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.

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 - Compromission système - Qualification (https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-systeme-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