Fiches Réflexes de remédiation

InterCERT FRANCE

FICHE RÉFLEXE

Compromission système

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'une compromission est suspectée ou confirmée sur une machine Windows ou Linux du système d'information.

A quoi sert-elle ?

L'objectif de cette fiche est de proposer une *aide à la qualification* d'un signalement de compromission système. Les différentes actions proposées aideront à :

- *Confirmer* qu'un incident de sécurité est bien en cours, et qu'*un ou plusieurs systèmes sont compromis*.
- 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.

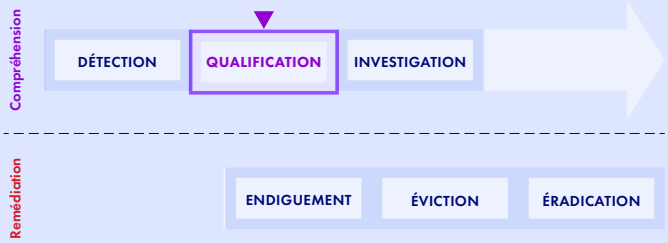
Comment l'utiliser ?

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 nécessaires au système d'information :

- Les *accès à l'administration et au monitoring* du système d'information.
- Les *accès aux équipements de sécurité* du système d'information.
- La connaissance des *priorités métier* de l'organisation.
- L'annuaire de contacts d'urgence.

Ces personnes peuvent être internes ou externes à l'organisation. Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.
Notifier les bonnes personnes dès le début de la qualification :

- ☐ Notifier le RSSI.
- ☐ Notifier le DSI / responsable IT.
- ☐ Si l'organisation est accompagnée par un prestataire (SOC, CSIRT, infogérant), le notifier.

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 les retours d'expérience
- 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.

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.

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 ou un logiciel de gestion à distance n'ouvrant pas de système (type RMM).
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.

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 - Identifier le système concerné

- ☐ *La nature des informations transmises permet-elle d'identifier avec sureté le système compromis ?*

Mesure 2 - Confirmer l'incident de type compromission système

- ☐ *L'incident de type compromission système est-il confirmé, est-il un faux positif ou nécessite-t-il des investigations complémentaires ?*

Mesure 3 - Évaluer le périmètre de l'incident

- ☐ *L'incident est-il circonscrit à une partie du système d'information identifiable ?*
- ☐ *Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ?*
- ☐ *Les autres systèmes d'information interconnectés avec celui de l'entreprise sont-ils en risque ?*

Mesure 4 - Évaluer l'impact de l'incident

- ☐ *Quelles activités métiers essentielles sont-elles ou peuvent-elles être perturbées ?*
- ☐ *Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?*

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

- ☐ *Quelles sont les activités essentielles potentiellement perturbées, pour lesquelles des mesures préventives de maintien d'activité doivent être envisagées ?*
- ☐ *L'activité détectée est elle récente et donc sujette à évolution ou ancienne et stable ?*
- ☐ *L'incident est-il à risque de généralisation imminente (forte connectivité, atteinte à une fonction de sécurité) ?*

Qualifier l'incident

Conclure quant à la gravité de l'incident

- ☐ La compromission d'une machine appartenant au système d'information est-elle *confirmée* ?
  - ☐ Si elle ne l'est pas, y a-t-il un risque de machine réellement compromise mais non identifiée ?
- ☐ 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

Cette partie détaillera des actions qui aideront à conduire les évaluations et à aboutir à la qualification de l'incident.
Vous avez reçu une notification vous signifiant que vous étiez compromis.
Que celle-ci soit une détection interne, ou un signalement de tiers, il va falloir en évaluer la pertinence et la gravité.
Les informations signalant une compromission système sont généralement de 3 natures différentes :

1. Adresse réseau : adresse IP, nom d'hôte qualifié (FQDN), l'adresse peut être celle d'un équipement relai plutôt que directement la machine compromise (pare-feu, proxy, serveur DNS).
2. Nom de machine : nom Windows ou Unix d'une machine sans le domaine DNS ou *Active Directory*
3. Alerte de sécurité : alerte remontée par un capteur système comme un EDR, ou un évènement système supervisé dans un SIEM

Évaluer l'incident

Mesure 1 - Qualifier le système concerné

Les informations suivantes doivent être recueillies avec les outils disponibles au moment du traitement. Plusieurs points de contrôle reposent sur un outil spécifique (EDR, CMDB, orchestrateur). Si ce type d'outillage n'est pas disponible sur le système d'information concerné par le signalement, ignorez le point.

Action 1.a : Identifier le système concerné

- ▶ **Si l'alerte vient d'un outil détection ou SOC interne avec une identification de machine**
  - ☐ Quel est l'indicateur qui a déclenché l'alerte ?
  - ☐ Les informations fournies par l'outil de détection permettent-elles d'identifier la machine compromise de façon sure ?
- ▶ **Si le signalement provient d'un SOC ou MSSP externe**
  - ☐ Demander immédiatement au prestataire :
    - ☐ le contexte de détection (règle déclenchée, comportement observé),
    - ☐ les IoC associés (IP, domaine, hash, nom de fichier...),
    - ☐ le niveau de confiance de la détection,
    - ☐ les actions déjà engagées par le prestataire (isolation déclenchée ? blocage côté EDR ? compte désactivé ?).
- ▶ **A partir d'une adresse réseau**
  - ☐ L'adresse IP est-elle connue comme attribuée (DHCP, reverse-DNS, annuaire, CMDB, inventaire...) ?
  - ☐ Le sous-réseau IP concerné fait-il partie des adresses (internes ou externes) utilisées sur le SI ?
  - ☐ Si l'adresse IP fait partie d'un pool DHCP, peut-on retrouver la machine portant l'adresse au moment de l'activité signalée ?
  - ☐ Si l'adresse est publique sur Internet, la machine peut-elle être associée à l'organisation (bannières, certificats TLS, services hébergés, etc.)
  - ☐ Le signalement pointe-t-il vers un équipement réseau susceptible de masquer plusieurs systèmes (Routeur, Proxy, Serveur DNS, Pare-feu, NAT) ?
    - ☐ Les informations du signalement permettent-elles d'identifier la machine derrière ce relais (horodatage précis, ports sources/destinatio
    - ☐ Les journaux de l'équipement réseau permettent-ils d'identifier les systèmes masqués ?
  - ☐ Si un EDR ou XDR est présent sur SI, la machine peut elle y être retrouvée par son adresse réseau au moment de l'activité signalée ?
- ▶ **Sur la base d'un nom de machine**
  - ☐ La machine existe-t-elle dans un annuaire centralisé (*Active Directory*, orchestrateur, supervision de sécurité) ?
  - ☐ La machine pourrait-elle être hors gestion centralisée (Workgroup, poste associé à une application métier, machine virtuelle hors domaine, instances de développement, etc.) ? Si oui existe-t-il un inventaire de ces machines.

Action 1.b : Recueillir les informations élémentaires de contexte technique

- ☐ Le système visé par le signalement peut-il être identifié ? Si oui :
  - ☐ Quel est le système d'exploitation opérant le système signalé ?
  - ☐ Quel est le niveau de version et d'installation de correctif déployé sur ce système ?
  - ☐ Est-ce que le système est relié à un système de synchronisation horaire (NTP) ?
  - ☐ Quelles applications métiers sont installées sur ce système ?

  - ☐ Si je dispose d'un système de suivi des vulnérabilités consultable au moment de la qualification :
    - ☐ Le système hébergeait-il un logiciel vulnérable au moment de l'activité signalée ?
    - ☐ Des traces d'exécution de logiciel vulnérable sont-elles visibles au moment de l'activité signalée (SIEM, sur l'EDR, dans des journaux système, outils de gestion d'activité utilisateur...) ?
    - ☐ Le système héberge-t-il encore un logiciel dans une version vulnérable à une faille activement exploitée ?
    - ▷ Bases de vulnérabilités notables en cours d'exploitation :
      - □ CISA KEV catalogue de vulnérabilités exploitées
      - □ EUVID de l'ENISA

Action 1.c : Confirmer la validité du signalement

Les erreurs de signalement étant fréquentes et source de perte de temps considérables, il est nécessaire de le confirmer :

- ☐ L'architecture et la configuration du système concerné permettent-elles de valider l'évènement à la date signalée ? (date trop ancienne ou changement du système d'information entre temps) ?
- ☐ L'horodatage est-il cohérent avec le reste du signalement ?
- ☐ Le fuseau horaire de l'horodatage du signalement est-il connu ?
- ☐ Le système était-il en production aux dates et heures d'activité signalées ?
- ☐ Les informations techniques signalées correspondent elles au système (versions de système d'exploitation, ou type de compromission pouvant être incohérents) ?
- ☐ Le système est-il concerné par un changement récent de solution ou d'architecture de supervision qui puisse avoir généré un faux positif ou détecté une compromission plus ancienne ?
  - changements de version de solutions de sécurité,
  - changements de configuration,
  - changement de version système ou applicative,
  - déplacement d'un système / changement d'architecture.
- ☐ Si une supervision de sécurité existe, la machine a-t-elle remonté d'autres alertes autour de la période de l'événement signalé ?
  - Ces alertes permettent-elles de préciser le signalement ?
  - D'autres machines montrent-elles des alertes similaires ?
- ☐ Est-ce que le signalement est un doublon d'un incident déjà traité ?

Action 1.d : (Conclure) Confirmer l'identification du système

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

- ☐ *La nature des informations transmises permet-elle d'identifier avec sûreté le système supposé compromis ?*

Mesure 2 - Confirmer l'incident de type compromission système

> **REMARQUE**
>
> Il crucial de ne pas rester bloquer sur un point de vérification spécifique. Une qualification qui prend trop de temps est inutile. Si un point ne peut être tranché, passez au suivants. De même, dès qu'assez d'éléments ont été recueilli pour confirmer la compromission, il est conseillé de passer directement à l'évaluation du périmètre (mesure 3).

Confronter les informations du signalement aux informations observables du système d'information doit permettre de confirmer l'incident de type compromission système :

Actions 2.a : Informations sur l'environnement machine

- ☐ Des opérations légitimes(maintenance, changements sur la solution de sécurité, changements de configuration) en cours concernent-elles la ou les systèmes signalés ?
  - ☐ Si oui, pourraient-ils être source d'une détection erronée ?
- ☐ La machine a-t-elle fait l'objet d'une réaffectation (rôle ou personne) avant les événements signalés ?
  - ☐ Si oui, ce changement pourrait-il avoir provoqué une détection de compromission erronée ?
- ☐ Un vol ou une perte de la machine a-t-il été signalé ?
- ▶ Si une information de géolocalisation est disponible :
  - ☐ La géolocalisation de la machine est-elle anormale ?

Action 2.b : Si le signalement est une détection de code ou comportement illégitime

- ☐ La supervision de sécurité (EDR/XDR) permet-elle de vérifier la présence du code sur la machine au moment du signalement ?
  - Le code est-il toujours présent sur la machine ?
- ☐ Une alerte antivirale est-elle visible (console, journaux et événements système) ?
- ☐ Exécution de commandes inhabituelle est elle visible dans la supervision de sécurité ou dans les journaux systèmes (LOLBin, Powershell...) ?

Action 2.c : Recueillir le contexte utilisateur

Si la machine signalée est utilisée par un ou plusieurs utilisateurs identifiés, et dans la mesure où la confidentialité de la qualification le permet, envisager de les questionner :

- ☐ L'utilisateur a-t-il observé un comportement anormal récent (lenteur, fenêtres pop-up, redémarrages, message d'erreur, antivirus déclenché) ?
- ☐ L'utilisateur a-t-il cliqué sur un lien suspect, ouvert une pièce jointe inhabituelle, exécuté un fichier ?
- ☐ L'utilisateur a-t-il reçu des appels suspects (vishing, faux support technique) ou des sollicitations type "MFA fatigue" ?
- ☐ L'utilisateur a-t-il connecté un support amovible (USB) ?
- ☐ L'utilisateur a-t-il partagé ses identifiants avec qui que ce soit récemment ?

Action 2.d : Si la supervision de sécurité est externalisée, croiser les informations avec le prestataire

- ☐ Demander au SOC/MSSP les éléments bruts ayant déclenché l'alerte (logs, captures, hash, télémétrie).
- ☐ Vérifier si d'autres alertes corrélées ont été observées sur le périmètre supervisé.
- ☐ Demander si l'alerte a été qualifiée en "vrai positif" / "faux positif" / "à investiguer" côté prestataire.
- ☐ S'assurer que les actions du prestataire (blocage automatique, mise en quarantaine) sont tracées dans la main courante.

Action 2.e : Croiser avec le contexte de menace

- ☐ Les IoC du signalement (IP, domaine, hash, nom de fichier) sont-ils référencés dans des bases publiques ?
- ☐ L'organisation dispose-t-elle d'un service de CTI (Threat Intelligence) ? Si oui, l'IoC y est-il référencé ?
- ☐ Le secteur d'activité de l'organisation est-il actuellement ciblé par une campagne connue (alertes CERT-FR, ANSSI, ENISA) ?

Action 2.f : Si le signalement est un flux réseau

- ☐ Le flux est-il visible dans des journaux d'infrastructure réseau :
  - journaux des pare-feux,
  - journaux de serveurs mandataires (proxy),
  - traces de flux (NetFlow/IPFIX),
  - console de CDN (type Cloudflare, Akamai...) ?
- ☐ Le flux est-il détecté par une sonde réseau (IDS) ?
- ☐ La supervision réseau de production montre-t-elle une volumétrie inhabituelle ?

Action 2.g : Modification d'un service exposé par le système

Tous les changements sur les services exposés d'un système ne sont pas facilement visibles (par exemple les ports non TCP). Par ailleurs, beaucoup d'exposition de service indésirable sont issues de fausses manipulations ou d'incident de manipulation de configuration plutot que d'une compromission. Néanmoins, il est fréquent que des changements soient publiquement visibles sur un système compromis et ils doivent faire l'objet d'une vérification.

- ☐ Défiguration d'application ou site web.
- ☐ Changement ou ajout de services exposés au réseau (ouverture de ports TCP, applications inhabituelles en écoute).
    - L'information peut venir de l'EASM, de la supervision de sécurité, ou d'une base de scan public sur Internet.

Action 2.h : Utilisation illégitime de compte utilisateur

Rechercher les traces d'un usage illégitime d'un compte utilisateur qui pourrait avoir été compromis. Ces traces peuvent être retrouvées dans les journaux système localement ou dans un puit de logs.

- ☐ Connexion d'un compte utilisateur inhabituel sur le système compromis.
- ☐ Connexion d'un compte révoqué sur le système compromis.
- ☐ Usage anormal d'un compte sur ou depuis le système compromis (ex : compte de service ou compte machine ouvrant des connexions interactives).

Action 2.i : Des flux inhabituels sont-ils visibles depuis et vers cette machine ?

REMARQUE

Ces informations peuvent être rendues plus pertinentes en l'appuyant sur une connaissance des flux réseaux légitimes (DAT, matrice de flux). Ici encore, il est plus important de chercher des points de contrôle disponible que de passer un temps précieux à réunir une information indisponible au moment du traitement. Par ailleurs, le caractère les flux réseau sont souvent plus changeant que les documentations. La détection d'un flux non documenté n'est pas forcément à considérer comme malveillante. Sa présence est juste une indication à prendre en compte dans l'analyse.

- ☐ Connexion de nature ou de destination Internet inhabituelle sur les serveurs mandataires :
    - vers des sous-réseaux IP dédiés à l'hébergement de VPS,
    - flux vers des infrastructures TOR,
    - utilisation de services ou ports réseau inhabituels.
- ☐ Connexion avec des destinations internes inhabituelles (filiale, sous-réseau, géolocalisation, type de système).
- ☐ Initiation de connexions, réussies ou non, avec des services inhabituels ou rares :
    - dans les journaux de connexion des machines distantes,
    - dans les journaux de pare-feu systèmes,
    - comportements à rechercher :
        - ▷ tentatives de montage réseau,
        - ▷ balayage réseau (scan) caractérisé par de multiples tentatives de connexions vers un nombre important de destination en peu de temps,
        - ▷ tentative de connexions interactives (RDP, SSH, WMIC...) depuis des machines, comme des serveurs, qui ne devraient pas en être la source,
        - ▷ tentatives de connexions vers des systèmes de niveau de protection supérieur (par exemple vers un silo tiers 0).
- ☐ Des alertes de blocages de flux sont-elles associées à la machine (pare-feu, IPS) ?
    - tentative de connexion,
    - et tentatives d'établissement de tunnels VPN,
    - résolution DNS vers des domaines suspects ou caractéristiques de tunnels (entrées DNS au nom long et complexe).

Action 2.j : Supervision d'infrastructure nuagique (cloud)

Quand la machine compromise est hébergée sur un *cloud*, différents types de journaux permettent d'identifier d'éventuelles activités suspectes autour du système.

- ☐ Changements d'attributs des objets associés au système compromis.
- ☐ Changement de groupes ou d'utilisateurs disposant de droits sur le système compromis.

- ☐ Des volumétries réseaux anormales autour de cette machine sont elles visibles ?
- ☐ Si un CSPM est disponible, des changements sur la machine y sont-ils visibles ?
- ☐ Pourcentage élevé d'échec de connexion à d'autres services *cloud*.

Action 2.k : (Conclure) Confirmer l'incident de type compromission système

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

- ☐ *L'incident de type compromission système est-il confirmé, est-il un faux positif ou nécessite-t-il des investigations complémentaires ?*

Mesure 3 - Évaluer le périmètre de l'incident

Action 3.a : Identifier la fonction de la ou des machines suspectées

- ☐ Smartphone ou tablette ?
- ☐ Postes de travail ?
  - Mobile ou pas
- ☐ Serveurs applicatif ?
- ☐ Serveurs de stockage ?
- ☐ Hyperviseurs ?
- ☐ Machines virtuelles ?
  - ☐ Sur quel hyperviseur ?
- ☐ Machines physiques ?
- ☐ La machine porte-t-elle la gestion d'autres machines (Annuaire AD ou LDAP, gestion de flotte ou orchestrateur) ?
- ☐ Appliance en boite noire (équipements réseau et de stockage, systèmes industriels sans console système interactive) ?
- ☐ La machine est-elle exempte de certaines mesures de sécurité (Machine de développement, partie d'un systeme industriel, système ancien non maintenu/*legacy*) ?
- ☐ L'équipement est-il un objet connecté (IOT) ?

Action 3.b : Identifier la connectivité de la ou des machines

- ☐ Internet :
  - ☐ La machine expose-t-elle des services sur Internet ?
  - ☐ La machine peut-elle initier des connexions vers Internet ?
- ☐ Interconnexions :
  - ☐ La machine peut-elle monter des connexions vers des systèmes de partenaires ou clients ?
  - ☐ La machine reçoit-elle des connexions de partenaires, clients ou utilisateurs distants ?
  - ☐ La machine peut-elle servir de pont entre le réseau local et des réseaux plus sensibles ?
  - ☐ La machine dispose-t-elle de connexions sans fil (Wifi, Bluetooth, Zigbee, cellulaire, satellitaire) ?
  - ☐ La machine a-t-elle des accès sur d'autres systèmes d'information de l'organisation : autres tenants cloud, autres sites, filiales...
  - ☐ La machine permet-t-elle d'accéder aux consoles locales de serveurs (carte mère IPMI, concentrateur de consoles séries) ?

Action 3.c : Identifier le nombre de machine potentiellement compromises

- ☐ Le signalement pointe-t-il vers plusieurs machines ?
  - Le signalement permet-il de supposer que les machines listées dans le signalement ne sont qu'un sous ensemble des machines compromises ?
- ☐ Si le système compromis était derrière un relais (routeur, proxy, pare-feu...) :
  - ☐ Les anomalies détectées sur la machine compromise existent-elles sur d'autres machines ?
- ☐ Si l'objet du signalement est hébergé dans un *cloud* un accroissement de facturation inhabituelle est-elle visible (data-transfert out, compute...) ?
  - Si c'est le cas, peut-il concerner plusieurs machines ?

Action 3.d : (Conclure) Évaluer le périmètre de l'incident

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

- ☐ *L'incident est-il circonscrit à une partie du système d'information identifiable ?*
- ☐ *Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ?*
- ☐ *Les autres systèmes d'information interconnectés avec celui de l'entreprise sont-ils en risque ?*
- ☐ *Si la machine porte une fonction de gestion d'autres équipements,* le traitement doit escalader :
  - Il faut considérer que la portion du système d'information gérée par la machine concernée est compromise.
- ☐ Si la machine est isolée, d'autres éléments permettent-ils d'identifier la source de sa compromission (autres systèmes compromis , supports USB contaminés) ?
- ☐ Si le système concerné est un équipement réseau, considérer de basculer vers le traitement de la fiche : Fiche réflexe - Compromission d'un équipement de bordure - Qualification.
- ☐ Si les événements Windows montre une saisie de clé de secours Bitlocker, considérer que la chaîne de démarrage est potentiellement piégée. Les supports de stockage du poste devraient être analysés hors ligne.
- ☐ Si la machine est une *smartphone* ou une tablette escalader vers la fiche Compromission de Smartphone.

Mesure 4 - Évaluer l'impact de l'incident

Action 4.a : Évaluer niveau de compromission pouvant résulter de la prise de contrôle de la machine

- ☐ Des comptes d'administration globaux (administrateur du domaine ou administrateur équivalent à pouvoir agir sur la totalité du SI) se sont-ils récemment connectés sur la machine et surtout depuis le dernier reboot ?
- ☐ La machine porte-t-elle une fonction de sécurité ?
  - ☐ Gestion des identités et accès (Contrôleur de domaine, annuaire, IDP...).
  - ☐ Gestion des mises à jour.
  - ☐ Gestion de configuration et déploiement (SCCM, Orchestrateur...).
  - ☐ Console de contrôle d'une fonction vitale (EDR/XDR, sauvegarde...).
  - ☐ Gestion de secrets : IGC (Autorités de Certification), coffre-fort de mots passe, serveur de déchiffrement de disque automatisé.
  - ☐ Hyperviseur.
  - ☐ La machine donne-t-elle accès à des services critiques ?
    - ☐ Poste d'administration.
    - ☐ Serveur de rebond d'administration (bastion).
    - ☐ Postes (PC, tablettes, IHM intégrées) de maintenance et d'ingénierie d'OT.

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

- ☐ Quelles *activités métiers* sont concernées par la machine suspectée, à usage interne ou externe ?
- ☐ Quelles activités potentiellement perturbées sont *vitales* pour l'organisation ?
  - ☐ Si votre organisation possède un BIA (Business Impact Analysis), ces activités y ont-elles été analysées ?
- ☐ Parmi les activités potentiellement perturbées, certaines provoquent-elles un risque identifié pour l'organisation ?
  - ☐ Importante perte financière ?
  - ☐ Risque image ?
  - ☐ Risque de perte de clientèle et d'opportunité ?
  - ☐ Risque sur les personnes ?
  - ☐ Fuite ou perte d'information métier critiques (base client, conceptions, prospect, ...) ?
- ☐ La machine ou les services qu'elle supporte est-elle soumise à un engagement de disponibilité (SLA) ?

Action 4.c : Évaluer les impacts réglementaires

- ☐ Le système d'information affecté est-il soumis à une réglementation particulière (OSE, OIV, NIS2, etc.) ?
- ☐ Peut-on savoir si le système d'information affecté stocke des données sensibles ?
  - ☐ données classifiées,
  - ☐ données personnelles ou RH,
  - ☐ données à statut protégé : de santé, financières,
  - ☐ données soumises à engagement contractuel ou réglementaire autre.

Action 4.d : (Conclure) Évaluer l'impact potentiel de l'incident

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

- ☐ *Quelles activités métiers essentielles sont-elles ou peuvent-elles être perturbées ?*
- ☐ *Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?*

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

Action 5.a : Évaluer l'urgence métier 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 (PCA/PRA) ?
- ☐ Existe-t-il une échéance importante qui pourrait être affectée par l'incident est-elle imminente ?
    - Événements proches, contrats, livraison, date de déclenchement d'action financière...
- ☐ La nature des données accédées nécessite-t-elle un traitement urgent ?
    - impact potentiel sur l'organisation,
    - données sensibles internes,
    - engagement de réaction vis-à-vis de tiers...

Action 5.b : Évaluer à quel point l'information est récente

- ☐ Le signalement est-il à propos d'une détection récente ?
- ☐ Si oui, l'activité détectée est-elle récente ou peut-elle être détectée dans le passé ?

Action 5.c : (Conclure) Évaluer l'urgence à résoudre l'incident

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

- ☐ *Quelles sont les activités essentielles potentiellement perturbées pour lesquelles des mesures préventives doivent être envisagées ?*
- ☐ *L'activité détectée est-elle récente et donc sujette à évolution, ou ancienne et stable ?*
- ☐ *L'incident est-il à risque de généralisation imminente (forte connectivité, atteinte à une fonction de sécurité) ?*
- ☐ *Est-ce qu'il existe un engagement ou une contrainte à traiter dans l'urgence ?*

Qualifier l'incident

Conclure quant à la *gravité* que représente l'incident de sécurité pour mon organisation, en prenant en compte le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre :

- ☐ La compromission d'une machine appartenant au système d'information est-elle *confirmée* ?
    - ☐ Si elle ne l'est pas, y a-t-il un risque de machine réellement compromise mais non identifiée ?
- ☐ L'incident est-il *circonscrit* sur mon système d'information, ou est-il étendu ?
- ☐ L'incident est-il susceptible de créer 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 compromission système est confirmé 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 - Compromission système - Endiguement

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

Si durant cette qualification vous suspectez une incident en cours de type rançongiciel, se référer aux fiches dédiées : Fiches réflexes - Chiffrement ou effacement en cours

ANNEXES

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.

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 - Compromission système - 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.
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