

Fiche réflexe

Compromission d'un tiers

Endiguement

2026

Présentation de la fiche

1 À qui s'adresse-t-elle ?

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

2 Quand l'utiliser ?

Utiliser cette fiche lorsqu'une entité tierce en relation avec votre organisation est victime d'une compromission et que la qualification a été réalisée (confirmation de la typologie d'incident).

3 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.

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 2 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 d'un tiers - Endiguement

○ Présentation de la fiche	2
○ Prérequis	5
○ Actions d'endiguement par priorités	7
○ I - Ni la compromission du Tiers, ni celle de l'entreprise ne sont en l'état confirmées	7
○ II - La compromission du Tiers est confirmée, mais pas celle de l'entreprise	8
○ III et IV Détection d'un incident au sein de l'entreprise liée à la compromission d'un Tiers	9
○ Déclarer l'incident	10
○ Actions d'endiguement par thèmes	11
○ Sommaire	11
○ Theme 1 - Continuité d'activité	12
– Mesure 1 - Sensibiliser les effectifs sur le risque actuel	12
– Mesure 2 - Maintenir la communication avec le Tiers pour suivre l'évolution de la situation	12
– Mesure 3 - Plan de Continuité et de Reprise d'Activité (PCA/PRA)	12
○ Theme 2 - Endiguement de l'incident	14
– Mesure 4 - Premières remédiations d'urgence	14
– Mesure 5 - Surveillance et Threat Hunting	14
– Mesure 6 - Traiter l'incident interne selon la fiche réflexe correspondant au type d'incident identifié	14
○ Suite des actions	16

○ **Annexes**

18

Prérequis

01 Avoir qualifié l'incident

Il faut avoir **qualifié** qu'il y a bien une compromission d'un Tiers, et en avoir évalué le type et la gravité :

- Fiche précédente conseillée : [Fiche réflexe - Compromission d'un tiers - 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.

02 Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement ont 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.

Il peut également être utile d'inclure assez tôt dans les échanges des personnes ayant la connaissance des relations avec le Tiers ou déjà en relation avec lui et autorisée à suivre l'incident.

03 Ouvrir une main courante

Dès le début de l'incident, ouvrir une **main courante** pour tracer tous les actions et évènements 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 selon le cas de figure identifié lors de la qualification, à savoir :

- * Cas I - Aucune compromission n'est confirmée : ni celle du Tiers, ni celle de l'entreprise ne sont avérées ;
- * Cas II - La compromission du Tiers est confirmée, mais aucun impact identifié au sein de l'entreprise ;
- * Cas III - Détection d'un comportement anormal de la part du Tiers : La compromission du Tiers n'est pas forcément confirmée (il peut s'agir d'un incident de production non lié à un incident de sécurité dans le système d'information du Tiers) mais un incident de sécurité est suspecté au sein de l'entreprise ;
- * Cas IV - Détection d'un comportement malveillant provenant du Tiers : La compromission du Tiers est confirmée ou fortement suspectée et un incident a également été détecté au sein de votre entreprise.

I - Ni la compromission du Tiers, ni celle de l'entreprise ne sont en l'état confirmées

Ce cas s'applique si la confirmation n'est confirmée ni sur l'organisation ni chez le tiers, ou si la compromission confirmée pour un tiers ayant très peu ou pas de liens avec l'entreprise.

Actions	Priorité
Sensibiliser les effectifs sur les potentiels risques actuels (Mesure 1)	P0
Maintenir un canal de communication avec le Tiers pour suivre l'évolution de la situation (Mesure 2)	P1

II - La compromission du Tiers est confirmée, mais pas celle de l'entreprise

Ce cas s'applique si la compromission du tiers est confirmée, mais que rien ne permet de considérer l'organisation défendue comme compromise. Le tiers a potentiellement de forts liens avec l'organisation.

Actions	Priorité
Premières remédiations d'urgence selon la pertinence (Mesure 4)	P0
Surveillance et Threat Hunting (Mesure 5)	P1
Maintenir la communication avec le Tiers pour suivre l'évolution de la situation (Mesure 2)	P1
Sensibiliser les effectifs sur le risque actuel (Mesure 1)	P2
Plan de Continuité et de Reprise d'Activité (PCA/PRA) (Mesure 3)	P3

III et IV Détection d'un incident au sein de l'entreprise liée à la compromission d'un Tiers

Actions	Priorité
Premières remédiations d'urgence selon la pertinence (Mesure 4)	P0
Traiter l'incident interne selon la fiche réflexe correspondant au type d'incident identifié (Mesure 6)	P0
Surveillance et Threat Hunting (Mesure 5)	P1
Maintenir la communication avec le Tiers pour suivre l'évolution de la situation (Mesure 2)	P1
Sensibiliser les effectifs sur le risque actuel (Mesure 1)	P2
Plan de Continuité et de Reprise d'Activité (PCA/PRA) (Mesure 3)	P3

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** : signalement.social-sante.gouv.fr/espace-declaration/profil

Procédure pour déclarer un incident

1. Accéder au portail de signalement : signalement.social-sante.gouv.fr
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

Sommaire

Cette partie détaille les différentes mesures d'endiguement possibles selon 2 axes thématiques. Chaque **mesure** est ensuite scindée en **actions unitaires** :

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités ! Pour comprendre quelles mesures et dans quel ordre effectuer ces actions, se référer à la précédente partie [Actions d'endiguement par priorités](#).

- Thème 1 : Continuité d'activité
 - Mesure 1 - Sensibiliser les équipes en interne
 - Mesure 2 - Maintenir la communication avec le Tiers pour suivre l'évolution de la situation
 - Mesure 6 - Mettre en place des mesures de continuité d'activité
- Thème 2 : Endiguement de l'incident
 - Mesure 3 - Limiter l'exposition au tiers compromis
 - Mesure 4 - Mettre en place une surveillance de circonstance (Surveillance et Threat Hunting)
 - Mesure 5 - Traiter l'incident en interne

Theme 1 - Continuité d'activité

Mesure 1 - Sensibiliser les effectifs sur le risque actuel

- Définir une posture de communication (prestataire, effectifs en lien avec le prestataire...) en fonction :
 - du niveau de risque et
 - du niveau de sensibilisation des collaborateurs
 - de la sensibilité de l'incident
- Informer les collaborateurs sensibilisés en relation avec le Tiers ou couper les liens + notification du Tiers
 - Communiquer plus largement sur les éléments à disposition concernant la compromission si décidé ainsi
 - Définir une conduite à tenir vis-à-vis du Tiers (nouveau processus de travail et/ou d'interactions...)
- Mettre en place un processus de signalement de comportements suspects
 - Liste de diffusion temporaire pour les employés
- Processus de traitement des signalements internes afin qu'ils puissent être pris en compte dans les actions d'endiguement et de qualification

Mesure 2 - Maintenir la communication avec le Tiers pour suivre l'évolution de la situation

- Prévoir, selon les disponibilités des parties prenantes et l'impact, un point plus ou moins régulier
- Suivre éventuellement les remédiations côté Tiers à l'aide des fiches endiguement correspondant à l'incident identifié chez le Tiers (voir Mesure 6)

Mesure 3 - Plan de Continuité et de Reprise d'Activité (PCA/PRA)

Action 3.a : Consulter les procédures de PCA existantes

- Vérifier la documentation et les protocoles en place
- Identifier les contacts clés et les ressources nécessaires

Action 3.b : Définir un plan de PCA avec le tiers

- Élaborer un plan d'action pour les actifs IT indisponibles en coopération avec les métiers
- Établir un niveau minimum de sécurité pour reprendre partiellement l'activité

Action 3.c : Définir un plan de reprise d'activité sur la base de pré-requis de sécurité avec le tiers

- Documenter les exigences et mesures de sécurité pour assurer la reprise d'activité
- Par exemple :
 - Partage d'un rapport d'investigation sur l'attaque incluant les actions de remédiation
 - Rotation des identifiants de connexion

Theme 2 - Endiguement de l'incident

Mesure 4 - Premières remédiations d'urgence

- Étudier au cas par cas les actions à entreprendre (par exemple en cas de compromission d'un compte de messagerie, il ne sera pas forcément utile de couper tous les accès VPN) sur la base des deux critères suivants :
 - Étendue de l'interconnexion (plus l'interconnexion est grande, plus la surface d'attaque l'est également, justifiant de vouloir couper les accès)
 - Gravité de l'incident (plus l'incident chez le Tiers est important, plus la coupure sera justifiée)
- Désactiver/couper les accès (IT) selon la typologie de l'incident identifiée chez le Tiers
 - Interconnexions de machines (firewall, proxy, VPN)
 - Accès à une ou plusieurs applications (ou désactivation de compte)
 - Blocage de mails (Antispam/Passerelle mail/Parefeu)
 - Mise en quarantaine de logiciel, d'applications ou de matériel fournis par le Tiers
- Notifier le Tiers des actions entreprises

Mesure 5 - Surveillance et Threat Hunting

Action 5.a : Surveillance

- Sensibilisation des équipes de surveillance et mise en place de monitoring pour une attention particulière sur les activités liées à ce tiers

Action 5.b : Investigations et Threat Hunting

- Recherche dans l'infrastructure de l'entreprise des IOCs semblables à ceux observés chez le tiers

Mesure 6 - Traiter l'incident interne selon la fiche réflexe correspondant au type d'incident identifié

Action 6.a : Dans le cadre d'une Compromission d'un Système

- Traiter l'incident comme une compromission système : '[Fiche réflexe - Compromission Système - Qualification et Endiguement](#)'

Action 6.b : Dans le cadre d'une Compromission de Messagerie

- Traiter l'incident comme une compromission de messagerie : '[Fiche réflexe - Compromission Messagerie - Qualification et Endiguement](#)'

Action 6.c : Dans le cadre du déploiement d'un logiciel de chiffrement ou d'effacement

- Traiter l'incident comme un déploiement de logiciel de chiffrement en cours ou imminent : '[Fiche réflexe - Chiffrement - Endiguement](#)'

Action 6.d : Dans le cadre d'une Compromission de Tenant Azure

- Traiter l'incident comme une compromission d'un tenant Azure : '[Fiche réflexe - Tenant Cloud - Qualification et Endiguement](#)'

Action 6.e : Dans le cadre d'une Défiguration Web

- Traiter l'incident comme une défiguration de site web : '[Fiche réflexe - Défiguration Web - Qualification et Endiguement](#)'

Action 6.f : Dans le cadre d'une Compromission d'un Equipement Réseau de Bordure

- Traiter l'incident comme une compromission d'un équipement réseau de bordure : '[Fiche réflexe - Équipement de bordure Réseau - Qualification et Endiguement](#)'

Action 6.g: Dans le cadre d'un Déni de Service

- Traiter l'incident comme un déni de service : '[Fiche réflexe - Déni de Service - Qualification et Endiguement](#)'

Action 6.h : Dans le cadre d'une Fuite de Données

- Traiter l'incident comme une fuite de données : '[Fiche réflexe - Fuite de données - Qualification et Endiguement](#)'

Suite des actions

Remarques générales

À 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 compromission de Tiers, il pourra s'avérer utile de calquer le suivi interne aux points organisés avec le Tiers pour s'assurer de la bonne circulation de l'information et que le tempo est adéquate pour des mises à jour régulières.

Retour d'expérience et capitalisation sur la gestion de l'incident

Une fois l'incident terminé, il pourra être utile de documenter et capitaliser la gestion de cet incident, en termes de processus et de standard :

- ▶ Enrichir l'analyse de la menace par la rédaction de rapport d'investigation en cas d'incident
 - ▶ Analyser la source de l'attaque et les TTP de l'attaquant ainsi que ses motivations
 - ▶ Mettre en place des actions de remédiation
- ▶ Évaluer le besoin d'appliquer de nouveaux standards de sécurité, ou de les adapter au contexte
 - ▶ Estimer la conformité aux normes de sécurité pertinentes
 - ▶ Intégrer ces standards dans le plan de PCA/PRA.

Annexes

Définitions

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.

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.

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**.

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.

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.

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

Déclarations complémentaires

Selon le type de votre organisation et la nature de l'incident, des déclarations complémentaires peuvent être requises :

Qui ?	Comment ?	Pourquoi ?
ANSSI	www.cert.ssi.gouv.fr/contact	Pour les Opérateurs d'importance vitale (OIV) et les Opérateurs de services essentiels (OSE), la déclaration d'incident à l'ANSSI est obligatoire
CNIL	www.cnil.fr/fr/notifier-une-vi...	En cas de violation de données à caractère personnel, la notification à la CNIL est obligatoire dans les 72 heures
Dépôt de plainte	www.masecurite.interieur.go...	Déposer une plainte en ligne
	www.cybermalveillance.gou...	Signaler sur Cybermalveillance

Préparation

Pour une meilleure préparation à la gestion d'un incident de sécurité, il est conseillé de :

- Tenir à jour un **annuaire de contacts d'urgence** accessible même en cas d'indisponibilité du SI ;
- Préparer un **kit de réponse à incident** comprenant les outils et procédures nécessaires ;
- Réaliser des **exercices de gestion de crise** réguliers ;
- S'assurer que les **sauvegardes** sont fonctionnelles et testées ;
- Maintenir une **cartographie du SI** à jour.

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 :

Document	Lien
Fiche réflexe - Compromission d'un tiers - Qualification	cyberveille.esante.gouv.fr/compromission-dun-tiers...
Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique	messervices.cyber.gouv.fr/guides/crise-cyber-les-cle...
Cyberattaques et remédiation	cyber.gouv.fr/piloter-la-remediation-dun...

Licence

Ce document est dérivé des travaux du GT Fiches Réflexes de remédiation de l'InterCERT France.

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (www.intercert-france.fr).

Le présent document est publié sous licence CC BY-NC-SA 4.0.