

FICHE RÉFLEXE

# Compromission d'un tenant Azure

## Qualification

InterCERT FRANCE



CC BY-NC-SA 4.0





## A qui s'adresse-t-elle ?

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

## Quand l'utiliser ?

Une compromission de *tenant*<sup>a</sup> Microsoft Azure peut en fait correspondre à différents types d'incidents cyber, eux-mêmes les conséquences de différents modes opératoires d'attaque. Cette fiche a vocation à se focaliser sur les cas les plus communs de compromission d'environnements Microsoft 365 et Entra ID. Utiliser cette fiche en cas de suspicion de compromission d'un *tenant* Azure, pouvant résulter de l'une des causes mentionnées ci-dessous :

- compromission de compte à privilèges Microsoft 365 ou Microsoft Azure Entra, notamment suite vol de son mot de passe ;
- compromission d'application, ou caractère malveillant d'application d'entreprise intégrée à Microsoft Azure Entra ;
- altération malveillante de la configuration sécurité du *tenant* Microsoft 365 ou du *tenant* Microsoft Entra ID ;
- compromission de compte utilisateur Microsoft 365 / Entra ID.

## A quoi sert-elle ?

L'objectif de cette fiche n'est pas de proposer une *aide à la qualification* de tout type d'attaque possible sur Microsoft 365 et Entra ID, mais plutôt de se focaliser sur ceux couramment observés en réponse à incident. Le détail des attaques considérées par la présente fiche peut être trouvé dans l'annexe Attaques considérées.

## Comment l'utiliser ?

Deux parties principales composent cette fiche :

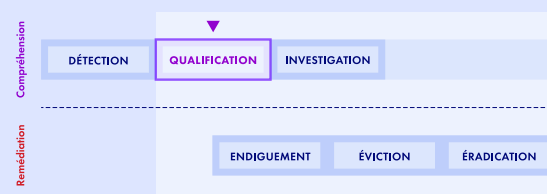
- La partie Conclusions attendues de la qualification correspond aux questions auxquelles la qualification devra répondre.
- La partie Méthode d'évaluation pas à pas correspond à la méthodologie pour aider à y répondre.

Cette fiche doit être exécutée en *temps court*. Pour cela, fixer un *temps contraint* (selon l'urgence pressentie) 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.

<sup>a</sup>. Le terme locataire (ou *tenant*) Azure désigne en fait souvent le même environnement locataire au niveau des services Microsoft 365, et/ou Entra ID (anciennement Azure AD).

# SOMMAIRE

Prérequis	3
Conclusions attendues de la qualification	4
Méthode d'évaluation pas à pas	7
Suite des actions	14
Annexes	15







# PRÉREQUIS

## Disposer des personnes et ressources 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 à la supervision du système d'information :
  - pour le cas présent, les identifiants d'un compte valide ayant le rôle "administrateur global" Microsoft Azure Entra ID <sup>1</sup> ;
- ▶ Powershell 5, voire 7 si possible, sur le poste d'où seront menées les investigations ;
- ▶ 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.

## 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 et les comptes (voir 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.

## 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.

1. voir en section liens utiles pour plus d'information sur les services "cloud" Microsoft, Microsoft 365 ou sur les rôles Entra 11





# CONCLUSIONS ATTENDUES DE LA QUALIFICATION

Cette partie résume les conclusions auxquelles doivent mener les évaluations, qui aboutiront à la qualification de l'incident. La partie suivante détaillera justement des actions qui aideront à conduire pas à pas ces évaluations.

## Évaluer l'incident

### Mesure 1 - Confirmer le type d'incident

- ☐ L'incident est-il confirmé ou nécessite-t-il des investigations complémentaires ? Est-il de type ?
  - ☐ compromission de compte utilisateur Microsoft 365 ;
  - ☐ compromission de compte à privilèges Microsoft 365 ;
  - ☐ compromission de compte à privilèges Azure Entra ID ;
  - ☐ relai de contenu malveillant ;
  - ☐ fuite d'information (via partage, ou attaque dite BEC) ;
  - ☐ compromission d'une application d'entreprise Microsoft Azure Entra ;
  - ☐ compromission d'une ressource telle qu'une machine virtuelle hébergée sur Azure.

### Mesure 2 - Évaluer le périmètre de l'incident

- ☐ Les ressources d'administration ont-elles été compromises (comptes, postes, serveurs) ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?
- ☐ L'incident est-il circonscrit à une partie du système d'information identifiable ?
- ☐ D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque, notamment en cas de fédération Microsoft Entra ?
- ☐ Est-ce que la compromission ne concerne que des comptes utilisateurs, et/ou administrateurs ?
- ☐ Est-ce que la compromission concerne également des périphériques (PC, tablettes, ordiphones) ?

### Mesure 3 - Évaluer l'impact de l'incident

- ☐ Quelles activités vitales sont perturbées, le cas échéant ?
- ☐ Quelles chaînes d'activité (services métier) sont impactées et dont la défaillance peut causer des perturbations graves ?
- ☐ La DSI a-t-elle les compétences en interne pour reconstruire les systèmes d'information impactés ?
- ☐ La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?
- ☐ Les données utilisateur (BAL, OneDrive, espaces Teams) sont-elles altérées voire détruites ?
- ☐ Existe-t-il une sauvegarde spécifique des données Entra ID et de la configuration Microsoft 365, récente et dont la restauration est considérée faisable ?
- ☐ Existe-t-il une sauvegarde pour les données des comptes utilisateurs considérés comme potentiellement compromis ?

### Mesure 4 - Évaluer l'urgence à résoudre l'incident

- ☐ Quelles sont les activités vitales à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?
- ☐ Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?

## Qualifier l'incident

### Conclure quant à la gravité de l'incident

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





- ☐ Anomalie courante
- ☐ Incident mineur
- ☐ Incident majeur
- ☐ Crise cyber



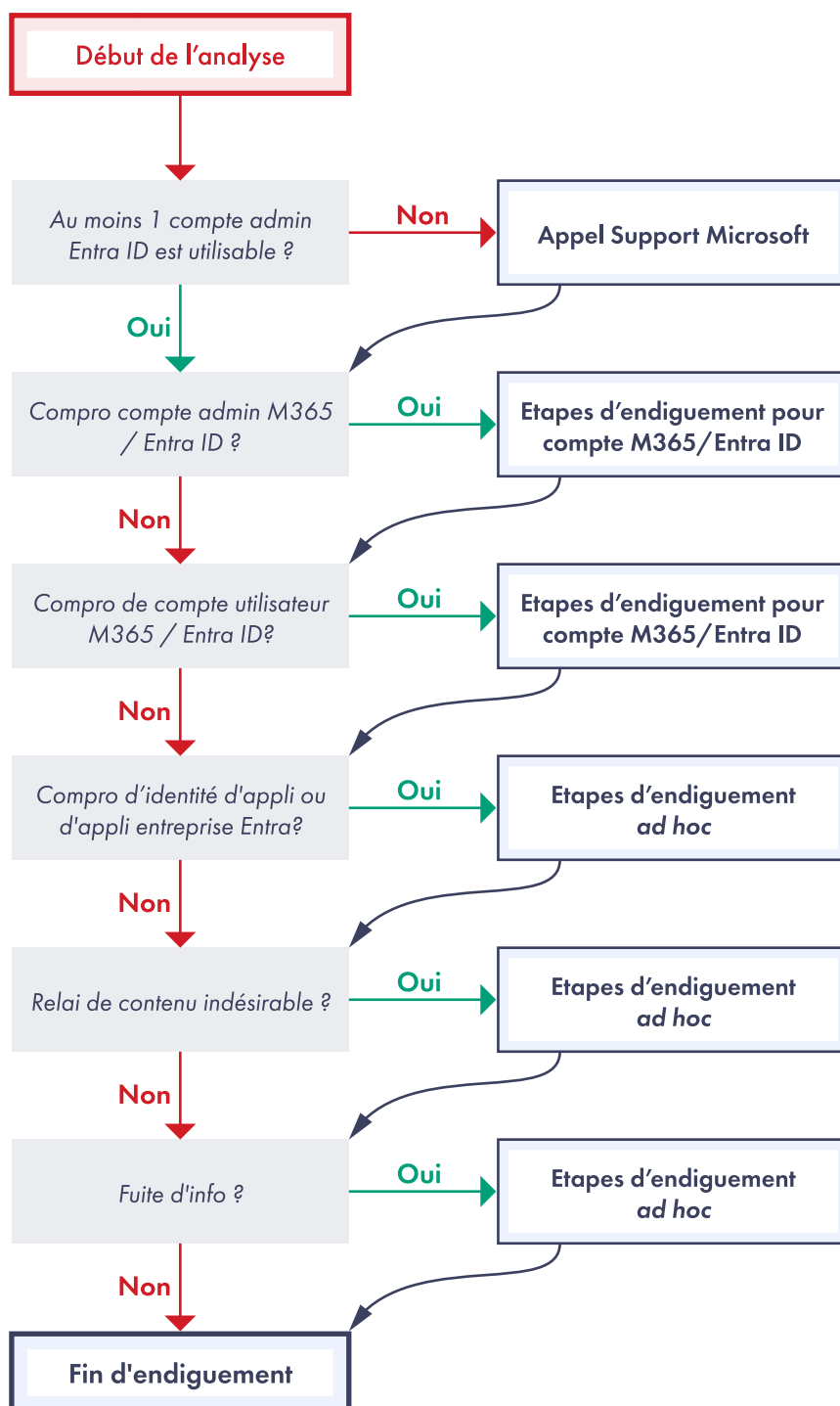


Figure 1 – Etapes de l'endiguement





# 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.

## Caractériser l'incident

**Note de préambule :** en cas de compromission suspectée ou avérée d'une ressource telle qu'une machine virtuelle hébergée sur Azure : se référer à la fiche réflexe compromission système<sup>2</sup>, et si un compte Entra ID est ou a été utilisé sur cette machine, se référer au cas d'usage "compromission de compte utilisateur Microsoft 365 / Entra ID" de la présente fiche.

### Mesure 1 - Confirmer le type de l'incident

#### Action 1.a Etablir si l'incident est une compromission de compte à privilèges Microsoft 365 ou Entra ID

##### NOTE

Il est impératif de vérifier si le cyber-attaquant a déjà un accès à privilèges ("administrateur") à l'environnement Microsoft 365 et Entra ID de la victime, ou non ; et si la victime est toujours administratrice de son propre environnement Microsoft 365 et Entra ID (cas d'usage de la rançon après que le cyber-attaquant ait récupéré de manière exclusive les privilèges administrateur).

Pour information, le schéma suivant montre les chemins d'attaque possibles entre comptes à privilèges<sup>3</sup> :

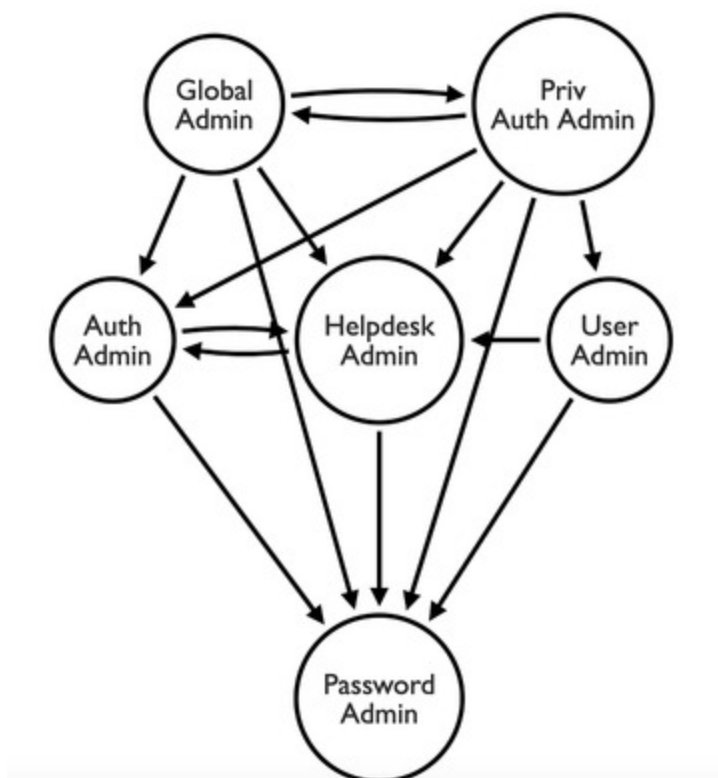


Figure 2 – image

2. Voir <https://www.intercert-france.fr/publications/fichereflexe-compromissionsysteme-qualification>

3. source [https://blog.microwavewitness.eu/work/microsoft/m365\\_attacks/#action](https://blog.microwavewitness.eu/work/microsoft/m365_attacks/#action)





### ☐ Vérifier les utilisateurs selon leurs rôles à privilèges Entra ID

- S'assurer qu'il y a au moins 2 utilisateurs ayant le rôle Administrateur global ("global administrator"), pour des raisons de résilience mais aussi de récupération (en cas de besoin);
- S'assurer que ces comptes sont bien tous considérés légitimes (comptes et personnes bien connus, qui sont bien censés avoir besoin de privilèges élevés au quotidien) et actifs;
  - ☐ pour le cas d'usage de comptes attribués à un prestataire, il est recommandé de vérifier leur légitimité à partir d'un annuaire;
- Vérifier qu'ils ont tous l'authentification forte (MFA) activée;
- Finalement, l'incident de type compromission de compte à privilèges Microsoft 365 ou Entra ID est-il confirmé ou non ?

#### NOTE

Pour réaliser ces actions, il peut être utile de lancer un scan avec un outil tel que 365Inspect<sup>a</sup> en plus des consoles Microsoft comme celle de gestion du MFA<sup>b</sup>.

a. pour plus de détail sur 365Inspect voir l'annexe liens utiles

b. voir [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/MultifactorAuthenticationConfig.ReactView/tabId/users](https://portal.azure.com/#view/Microsoft_AAD_IAM/MultifactorAuthenticationConfig.ReactView/tabId/users)

### ☐ Vérifier les sessions à privilèges

- Vérifier les adresses IP depuis lesquelles les utilisateurs ayant des rôles Entra ID à privilège, s'authentifient (sur les dernières semaines, si possible 6 mois). Si une trace d'authentification suspecte est détectée :
  - ▷ procéder à la réinitialisation du mot de passe pour le compte associé à ces traces (activer également l'authentification forte pour ce compte, et la forcer, si elle ne l'était pas déjà);
  - ▷ et veiller à terminer toutes ses sessions déjà actives (forcer la réauthentification); => pour cela, extraire les traces d'authentification pour ces comptes dans la console Microsoft Entra, en allant dans la page "sign-in logs"<sup>4</sup>). Il est recommandé de faire un export sous MS Excel, et de trier par la colonne "Location", puis aussi par "Status" (valeur : "Failure"), voire également par date/heure;
- Finalement, l'incident de type compromission de compte à privilèges Microsoft 365 ou Entra ID est-il confirmé ou non ?

### ☐ Vérifier les comptes à privilèges synchronisés entre Active Directory et Entra ID

- S'assurer qu'il n'y a pas de comptes AD sur site ("on-premises") qui soient synchronisés avec des rôles à privilèges Microsoft Entra ID :
  - ▷ si oui, vérifier leurs journaux d'authentification du *tenant* (quelques semaines, si possible 6 mois) pour ces comptes synchronisés; pour cela, extraire les traces d'authentification pour ces comptes dans la console Microsoft Entra, en allant dans la page "sign-in logs"<sup>5</sup>. Il est recommandé de faire un export sous MS Excel, et de trier par la colonne "Location", puis aussi par "Status" (valeur : "Failure"), voire également par date/heure.
    - ☐ si possible, les désactiver, ou au minimum, réinitialiser leur mot de passe et forcer l'activation de l'authentification forte (MFA), à l'aide de la console Microsoft Azure de gestion du MFA<sup>6</sup>;
- Finalement, l'incident de type compromission de compte à privilèges Microsoft 365 ou Entra ID est-il confirmé ou non ?

### ☐ Traiter les alertes utilisateurs à risque ("risky users") dans la console Microsoft

- ☐ Traiter les alertes relatives aux risques signalés par la console MS Entra ID<sup>7</sup> qui concerneraient des comptes à privilèges
  - ▷ En cas de doute, considérer le compte comme compromis, noter les identifiants utilisateurs des comptes compromis pour lancer la réinitialisation de leurs mots de passe Entra ID, ainsi que forcer l'authentification forte;
- ☐ Finalement, l'incident de type compromission de compte à privilèges Microsoft 365 ou Entra ID est-il confirmé ou non ?

#### NOTE

Cette action d'extraction peut également se faire de manière scriptée, avec le script

<https://github.com/AzureAD/IdentityProtectionTools>)

### ☐ Traiter les alertes authentifications à risque ("risky sign-ins")

4. [https://portal.azure.com/#view/Microsoft\\_AAD\\_UsersAndTenants/UserManagementMenuBlade/~/\\_/SignIns](https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/_/SignIns)

5. [https://portal.azure.com/#view/Microsoft\\_AAD\\_UsersAndTenants/UserManagementMenuBlade/~/\\_/SignIns](https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/_/SignIns)

6. [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/RiskyUsersBlade](https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskyUsersBlade)

7. [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/RiskySignInsBlade](https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskySignInsBlade)





- Traiter les alertes relatives aux authentifications considérées à risque, qui sont signalées dans la console MS Entra ID [^45], pour les comptes à privilèges;
- Si suspicion de compromission avérée, noter les identifiants utilisateurs des comptes compromis pour lancer la réinitialisation de leurs mots de passe Entra ID, ainsi que forcer l'authentification forte;
- Finalement, l'incident de type compromission de compte à privilèges Microsoft 365 ou Entra ID est-il confirmé ou non?



#### NOTE

Cette action d'extraction peut également se faire de manière scriptée, avec le script <https://github.com/AzureAD/IdentityProtectionTools>.

### Action 1.b - Confirmer si l'incident est une compromission de compte utilisateur Microsoft 365

#### ☐ Traitement des comptes éventuellement déjà suspectés au préalable

- Si des utilisateurs sont déjà identifiés comme ayant potentiellement une compromission de leur compte Entra ID, vérifier que leur compte n'est pas listé comme ayant été compromis, dans des bases de connaissance spécialisées telles que HaveIBeenPwned<sup>8</sup>, puis :
  - ▷ Traiter les alertes relatives aux authentifications considérées à risque, qui sont signalées dans la console MS Entra ID<sup>9</sup>;
  - ▷ Traiter les alertes relatives aux risques signalés par la console MS Entra ID<sup>10</sup>;
  - ▷ Traiter les alertes relatives aux IP dites risquées dans la console MS Entra Health Connect<sup>11 12</sup>
- Noter les identifiants utilisateurs des comptes compromis pour lancer la réinitialisation de leurs mots de passe Entra ID. Activer le MFA pour ces comptes;
- Finalement, l'incident de type compromission de compte utilisateur Microsoft 365 est-il confirmé ou non?

#### ☐ Vérification des invités

- Vérifier que la politique suivante est bien mise en place : "Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)";
- Vérifier que les invitations d'invités sont paramétrées sur : "Only users assigned to specific admin roles can invite guest users";
- Vérifier si des comptes invités ne se sont jamais authentifiés pour le moment : sont-ils légitimes?
- Finalement, l'incident de type compromission de compte utilisateur Microsoft 365 est-il confirmé ou non?

#### ☐ Vérifier les boîtes aux lettres (BAL) Exchange Online

- Vérifier les paramètres de délégations pour toutes les BAL associées aux comptes suspects ou potentiellement compromis;
  - ▷ ces délégations sont-elles légitimes?
- Vérifier les éventuelles BAL qui seraient cachées de l'annuaire global (GAL : "Global Addresses List");
- Vérifier les BAL avec des règles de transfert externe activées;
  - ▷ ces règles de transfert sont-elles légitimes?
- Vérifier les BAL ayant la délégation d'envoi en tant que ("SendAs delegates");
  - ▷ ces délégations sont-elles légitimes?
- Vérifier les BAL ayant la délégation envoyer de la part de ("SendOnBehalfOf delegates") activée;
  - ▷ ces délégations sont-elles légitimes?
- Finalement, l'incident de type compromission de compte utilisateur Microsoft 365 est-il confirmé ou non?



#### NOTE

Ces informations peuvent être extraites à l'aide d'un scan (si pas déjà fait) avec un outil tel que 365Inspect.

8. voir <https://haveibeenpwned.com>

9. voir [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/RiskySignInsBlade](https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskySignInsBlade)

10. voir [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/RiskDetectionsBlade](https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskDetectionsBlade)

11. voir [https://entra.microsoft.com/#view/Microsoft\\_AAD\\_DXP/ScenarioHealthSummary.ReactView](https://entra.microsoft.com/#view/Microsoft_AAD_DXP/ScenarioHealthSummary.ReactView)

12. Cf. section liens utiles pour plus d'infos sur l'investigation recommandée par Microsoft pour le cas d'usage de la pulvérisation de mots de passe.





Si besoin, se référer à la fiche réflexe InterCERT Compromission de messagerie.

### Action 1.c - Confirmer si l'incident est un relai de contenu indésirable

#### ☐ Vérifier la configuration anti-spam

- Vérifier la politique antispam du *tenant*, plus particulièrement les emails et les domaines qui sont paramétrés en blocage ou autorisation ("Blocked Senders" et "Allowed Senders") : est-ce qu'ils sont valides et légitimes ?
- Vérifier dans la politique anti-usurpation les entités autorisées à faire de l'usurpation de domaine : sont-elles valides et légitimes ?
- Finalement, l'incident de type relai de contenu indésirable est-il confirmé ou non ?

#### NOTE

Pour réaliser ces actions, il peut être utile d'exécuter le script *ScubaGear* (voir <https://github.com/cisagov/ScubaGear>).

### Action 1.d - Confirmer si l'incident est une compromission d'application d'entreprise Microsoft Azure Entra

Pour information, le diagramme suivant représente un type d'attaque possible à partir d'une application malveillante que l'utilisateur 365 va valider<sup>13</sup> :

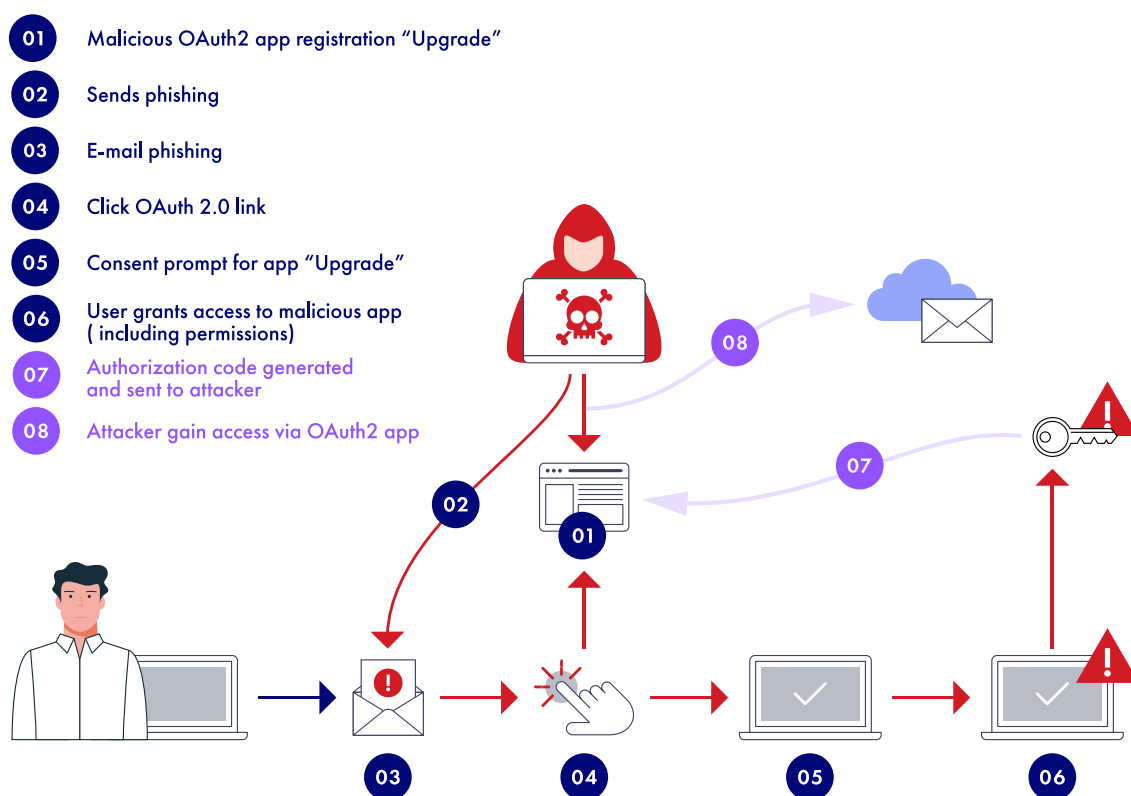


Figure 3 – Etapes de phishing

#### ☐ Traiter les anomalies sécurité associées aux applications

- Vérifier les applications enregistrées sur le *tenant* avec un secret de certificat ("Certificate Credentials"), ou avec un secret client ("Client Secret (password) Credentials") ;
- Vérifier les applications ayant les permissions d'accéder aux boîtes aux lettres (source d'événements : "unified audit logs") ;
- Vérifier les changements de propriétaire d'application (source d'événements : "unified audit logs") ;
- Finalement, l'incident de type compromission d'application d'entreprise Microsoft Azure Entra est-il confirmé ou non ?

13. voir [https://blog.microwavewitness.eu/work/microsoft/m365\\_attacks/](https://blog.microwavewitness.eu/work/microsoft/m365_attacks/)



 **NOTE**

Ces informations peuvent être extraites à l'aide d'un scan avec un outil tel que 365Inspect, en plus de la console et des journaux.

\* [ ] **Traiter toutes les anomalies sécurité associées aux services, notamment** - Les "Principals" de service ont-ils été trouvés sur le locataire avec un secret de certificat ("Certificate Credentials"), ou avec un secret client ("Client Secret (password) Credentials"); - Vérifier les nouvelles permissions accordées au "principals" de services (source d'évènements : "unified audit logs"); - Vérifier qu'il n'y a pas eu d'authentification avec un "principal" de service (voir <https://learn.microsoft.com/fr-fr/entra/identity-platform/app-objects-and-service-principals?tabs=browser>) depuis un emplacement à risque (source d'évènements : "Service Principal Sign-In logs"); - Finalement, l'incident de type compromission d'application d'entreprise Microsoft Azure Entra est-il confirmé ou non ?

**NOTE**

Ces informations peuvent être extraites à l'aide d'un scan avec un outil tel que 365Inspect, en plus de la console et des journaux.

☐ **Vérifier si l'incident est une attaque spécifique de type "Illicit Consent grant"**

Vérifier les transferts d'autorisation illégitimes par un usager <sup>14</sup>, en suivant les recommandations Microsoft avec les étapes décrites dans l'article Microsoft

<https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-illicit-consent-grants?view=o365-worldwide#steps-in-powershell>.

Puis, à partir du fichier CSV obtenu :

- ▶ Dans la colonne "ConsentType" (colonne G), chercher la valeur "AllPrinciples." La permission AllPrincipals permet à l'application cliente d'accéder à tout contenu de tout utilisateur dans le *tenant*. les applications natives Microsoft 365 ont besoin de cette permission pour fonctionner correctement. Cependant, toute application non-Microsoft avec cette permission devrait être vérifiée avec soin.
- ▶ Dans la colonne "Permission" (colonne F), vérifier les permissions que chaque application déléguée a sur le contenu. Chercher les permissions "Read" et "Write" ou "All", et traiter ces permissions rigoureusement, parce qu'elles pourraient ne pas être légitimes ;
- ▶ Vérifier les utilisateurs spécifiques qui ont un consentement validé ("consents granted"). Si ces utilisateurs sont de type VIP/VOP, avec des consentements inappropriés validés, ceci devrait être investigué rigoureusement ;
- ▶ Dans la colonne "ClientDisplayName" (colonne C), chercher des applications qui auraient l'air suspectes. Ex. : applications avec une faute dans leur nom, des blancs dans les noms, des applications portant le nom d'outils offensifs (ou "hacking"), cela nécessiterait une revue rigoureuse ;
- ▶ Finalement, l'incident de type compromission d'application d'entreprise Microsoft Azure Entra est-il confirmé ou non ?

**Action 1.e : Confirmer si l'incident est une Fuite d'informations (incluant BEC)**☐ **Vérifier les transferts automatiques**

- ☐ vérifier le contenu du rapport "Auto forwarded message report" <sup>15</sup> ;

- ▷ traiter tout compte utilisateur, via sa BAL, qui y serait mentionné. Si le transfert n'est pas légitimé, le compte doit être considéré comme potentiellement compromis. Si l'utilisateur concerné ne présente vraiment aucun signe de compromission, il faudra alors suspecter qu'un compte à privilèges Exchange Online soit compromis ;

☐ **Vérifier les règles de transport Exchange Online**

- ☐ Exporter les règles vers un fichier XML, par ex. à l'aide de la commande PowerShell pour MS Exchange Online <sup>16</sup> ;
- ☐ Vérifier toutes les conditions de règles de transport et les destinataires, en termes de légitimité.

Les règles de transport Exchange Online permettent d'opérer des traitements sur les flux de messagerie au niveau serveur, sans interaction (voire sans visibilité) de l'utilisateur final. Cela permet que des redirections, des suppressions, des copies, des modifications d'entêtes, etc. que les attaquants utilisent ces fonctions pour des accès illégitimes <sup>17</sup>.

☐ **Vérifier que toute BAL partagée a l'authentification désactivée**

Désactiver l'authentification des boîtes partagées est une bonne pratique de sécurité, sinon un attaquant pourrait s'y connecter directement et l'utiliser sans que ce soit associé à une identité unique <sup>18</sup>.

- ☐ Vérifier qu'il n'y a pas de caractère joker dans les paramètres "RemoteDomain"

14. Note : il peut être nécessaire d'installer Microsoft.Graph.Authentication 2.15.0 (<https://www.powershellgallery.com/packages/Microsoft.Graph.Authentication/2.15.0>) sur la machine d'analyse.

15. console d'administration MS Exchange Online <https://admin.exchange.microsoft.com/#/reports/autoforwardedmessages>

16. voir <https://learn.microsoft.com/en-us/powershell/module/exchange/export-transportrulecollection?view=exchange-ps>

17. Se référer à la section liens utiles pour plus d'information sur les règles de transport.

18. Se référer à la section liens utiles pour plus d'informations sur la sécurisation des boîtes partagées.





- ☐ Vérifier notamment les valeurs des paramètres "Delivery reports" (dont la valeur recommandée est "autorisé"), "Non-delivery report" (dont la valeur recommandée est "autorisé"), "Meeting forward notifications" (dont la valeur recommandée est "bloqué") La présence d'un caractère joker dans les paramétrages "RemoteDomain" peut traduire une altération malveillante de la configuration Exchange Online, ce qui réduit son niveau de sécurité et peut faciliter certaines actions de l'attaquant. Cette présence peut être vérifiée par la commande PowerShell suivante<sup>19</sup> :

```
get-remotedomain *
```

- ☐ Vérifier qu'il n'y a pas de fournisseur externe de stockage qui soit autorisé Vérifier les éventuels fournisseurs de stockage externe avec la commande PowerShell suivante

```
Get-OwaMailboxPolicy -Identity <affected policy>
```

- ☐ Vérifier la politique d'espace de stockage tierce partie dans Microsoft Teams
  - Vérifier que la politique d'espace de stockage tierce partie de Microsoft Team n'exporte pas les données du tenant vers un stockage illégitime.

- ☐ Vérifier la politique d'autorisation des utilisateurs anonymes

- Vérifier si la politique d'autorisation des utilisateurs anonymes permet des accès illégitimes.

- ☐ Conclure

- Finalement, l'incident de type Fuite d'informations (incluant BEC) est-il confirmé ou non ?

Si besoin, se référer à la fiche réflexe InterCERT relative à la Fuite d'information.



#### NOTE

Ces informations peuvent être extraites à l'aide d'un scan avec un outil tel que 365Inspect, en plus de la console et des journaux.

## Mesure 2 - Évaluer le périmètre de l'incident

### Action 2.a : Évaluer l'étendue de la compromission de l'environnement Azure

- ☐ Un compte à privilèges Microsoft 365 ou Entra ID est-il confirmé compromis ?
- ☐ Un compte utilisateur Microsoft 365 considéré VIP/VOP est-il confirmé compromis ?
- ☐ Est-ce que le vecteur d'infection semble être une autre entité qui fait partie d'une fédération Entra ID avec celle qui déroule la présente fiche ?
- ☐ Les données utilisateur (BAL, OneDrive, espaces Teams) sont-elles altérées voire détruites ?

### Action 2.b : Évaluer l'étendue de la compromission hors environnement Azure

- ☐ Y a-t-il des signalements liés à l'incident de sécurité, qui proviennent de l'extérieur de l'organisation (ex : clients finaux, partenaires commerciaux, fournisseurs...), qui auraient été signalés après le début de l'investigation, ou à d'autres personnes de l'organisation que les administrateurs M365 / Entra ID ?
- ☐ Le cas échéant, est-ce que l'Active Directory (sur site) est considéré compromis ?
- ☐ Est-ce que des périphériques utilisateur (PC, ordiphone, tablette) sont considérés comme potentiellement compromis ?

### Action 2.c : (Conclure) 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) ? Un compte à haut niveau de privilège semble-t-il avoir été compromis ?
- ☐ D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque ?

## Mesure 3 - Évaluer l'impact de l'incident

Les réponses aux questions ci-après doivent provenir majoritairement des résultats des actions réalisées durant le traitement de la mesure 1.

<sup>19</sup>. Voir en section liens utiles pour plus d'information sur les paramètres "RemoteDomain".





### Action 3.a : Évaluer les impacts sur l'activité métier

- ☐ Est-ce que le service Microsoft Entra ID est toujours opérationnel (ie. les utilisateurs peuvent toujours ouvrir une session sur un périphérique avec un compte Microsoft Entra ID, et l'accès aux portails Microsoft 365 est toujours possible avec les comptes Entra ID) ?
- ☐ Est-ce que le service Microsoft 365 Exchange Online est toujours opérationnel ?
- ☐ Est-ce que le service Microsoft 365 Teams est toujours opérationnel ?
- ☐ Est-ce que des informations sensibles et/ou des documents sensibles ont été suspectés voire confirmés comment ayant fuité ?

### Action 3.b : Évaluer les impacts sur la reprise d'activité

- ☐ Est-ce que l'organisation dispose toujours d'un compte valide (et considéré non compromis) "administrateur global" Microsoft Entra ID ?
- ☐ En cas d'altération voire destruction de données utilisateur (BAL, espaces OneDrive et Teams) :
  - ☐ Existe-t-il une sauvegarde spécifique des données Entra ID et de la configuration Microsoft 365, récente et dont la restauration est considérée faisable ?
  - ☐ Existe-t-il une sauvegarde (récente et valide) pour les données des comptes utilisateurs considérés comme potentiellement compromis ?

### Action 3.c : (Conclure) Évaluer l'impact de l'incident

- ☐ Quelles activités vitales sont perturbées ?
- ☐ Quelles chaînes d'activité sont impactées et dont la défaillance peut causer des perturbations graves ?
- ☐ La DSI a-t-elle les compétences en interne pour reconstruire les systèmes d'information impactés ?
- ☐ La DSI a-t-elle les compétences en interne pour maintenir les activités vitales ?

## Mesure 4 - Évaluer l'urgence à résoudre l'incident

### Action 4.a : un compte à privilèges Microsoft 365 ou Entra ID est-il confirmé compromis ?

Si un compte à privilège Microsoft 365 ou Entra ID est confirmé compromis, il est recommandé de considérer que le *tenant* est compromis.

### Action 4.b : (Conclure) Évaluer l'urgence à résoudre l'incident

- ☐ Quelles sont les activités vitales à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?
- ☐ Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?

## 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 :

- ☐ Le type d'incident suspecté est-il *confirmé* ?
- ☐ L'incident est-il *circonscrit* sur mon système d'information, ou est-il étendu ?
- ☐ L'incident présente-t-il un *impact fort* pour mon activité métier et le fonctionnement de mon système d'information ?
- ☐ L'incident est-il *urgent* à résoudre, ou les activités vitales ont-elles réussi à être maintenues ?
- ☐ Au final, quelle *gravité* représente cet incident de sécurité ?
  - ☐ Anomalie courante
  - ☐ Incident mineur
  - ☐ Incident majeur
  - ☐ Crise cyber





## SUITE DES ACTIONS

Si l'incident est confirmé et qu'il est de type ... 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 d'un tenant Azure - 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





# ANNEXES

## Attaques considérées

Type d'attaque	Référence MITRE ATT&CK
Business Email Compromise (BEC) et Email Account Compromise (EAC),	BEC : T1586.002, EAC : T1078.004
Fuite d'information : exfiltration d'emails , partage de fichiers, accès illégitime à des espaces Teams...	T1114 , T1213
Utilisation illégitime d'un compte utilisateur (à privilèges ou non) Microsoft 365	T1078.004 , T1021.007
Rebond, avec diffusion de contenus malveillants depuis le <i>tenant</i> Microsoft 365, ex. : courriels indésirables tels que du spam et hameçonnage	T1496.004
Application d'entreprise Microsoft Entra légitime vulnérable exploitée	T1190 et/ou T1528
Application d'entreprise Microsoft Entra malveillante installée par un utilisateur	T1496.004 notamment

### NOTE

Par extension, il est également possible de qualifier certains cas d'attaque de type diffusion de fichier malveillant hébergé sur un lien OneDrive/SharePoint/Teams du *tenant* investigué.

Les différentes actions proposées aideront à :

- Confirmer qu'un incident de sécurité est bien en cours, et qu'il peut être considéré comme une compromission, totale ou partielle, du *tenant* Microsoft 365 ou Entra ID ;
- 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.

Pour de plus amples détails sur les types d'attaques pouvant cibler Microsoft 365 et Entra ID (anciennement Azure AD), il est conseillé de se référer à la section liens utiles en fin de cette fiche.

## 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 :

- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique  
<https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber>
- Qu'est-ce que les services Microsoft 365 ?  
<https://learn.microsoft.com/fr-fr/office365/servicedescriptions/office-365-service-descriptions-technet-library>
- Qu'est-ce que Microsoft Entra et les identifiants Entra ID ?  
<https://learn.microsoft.com/fr-fr/entra/fundamentals/whatis>
- Applications Microsoft Entra  
<https://learn.microsoft.com/fr-fr/entra/identity/enterprise-apps/what-is-application-management>
- Rôles Microsoft Entra  
<https://learn.microsoft.com/fr-fr/entra/identity/role-based-access-control/permissions-reference>
- Rôles Microsoft 365  
<https://learn.microsoft.com/fr-fr/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>
- Règles de transport Exchange Online  
<https://learn.microsoft.com/fr-fr/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules>
- "RemoteDomain" dans Exchange Online  
<https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/remote-domains/remote-domains>
- Fédération Microsoft Entra ID entre organisations : <https://learn.microsoft.com/fr-fr/entra/identity/hybrid/connect/whatis-fed>





► Présentation rapide de Microsoft Graph

<https://learn.microsoft.com/fr-fr/graph/overview>



► 10 principales façons de sécuriser Microsoft 365 et Entra ID, selon le niveau de licence

<https://learn.microsoft.com/fr-fr/microsoft-365/business-premium/secure-your-business-data?view=o365-worldwide>

► Recommandation de sécurisation des BAL partagées, niveau authentification - lien

[https://www.tenable.com/audits/items/CIS\\_Microsoft\\_365\\_v3.1.0\\_E3\\_Level\\_1.audit:cfdc96ef3d222577b0aef7c8d2fc4ad3](https://www.tenable.com/audits/items/CIS_Microsoft_365_v3.1.0_E3_Level_1.audit:cfdc96ef3d222577b0aef7c8d2fc4ad3)

► Recommandations Microsoft pour la remédiation d'attaques utilisant les règles Outlook

<https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide>

► Recommandations Microsoft pour la détection et le traitement de l'attaque "Illicit consent Grant"

<https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-illicit-consent-grants?view=o365-worldwide#what-is-the-illicit-consent>

► Empêcher un ancien employé de se connecter et bloquer l'accès aux services Microsoft 365

<https://learn.microsoft.com/fr-fr/microsoft-365/admin/add-users/remove-former-employee-step-1?view=o365-worldwide#block-a-former-employees-access>

► Recommandations Microsoft pour l'attaque de pulvérisation de mots de passe

<https://learn.microsoft.com/fr-fr/security/operations/incident-response-playbook-password-spray>

► Attaque dite "Business Email Compromise"

<https://www.microsoft.com/fr-fr/security/business/security-101/what-is-business-email-compromise-bec>

► Common attacks targeting Microsoft 365 and Azure AD

[https://blog.microwavewitness.eu/work/microsoft/m365\\_attacks/](https://blog.microwavewitness.eu/work/microsoft/m365_attacks/)

► Abusing Azure application credentials to attack supply chains

<https://www.secureworks.com/research/abusing-azure-application-credentials-to-attack-supply-chains>

► Matrice ATT&CK pour les services Office de type Microsoft 365

<https://attack.mitre.org/matrices/enterprise/cloud/officesuite/>

► Matrice ATT&CK pour les services de fournisseurs d'identité type Microsoft Entra ID

<https://attack.mitre.org/matrices/enterprise/cloud/identityprovider/>



► Module PowerShell Azure AD incident Response

<https://github.com/AzureAD/Azure-AD-Incident-Response-PowerShell-Module>



► Dlux de travaux recommandé par Microsoft pour cas d'usage de compromission d'application Azure

<https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-compromised-malicious-app>

► Outil d'analyse 365Inspect

<https://github.com/soteria-security/365Inspect>

## 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	<a href="https://www.cybermalveillance.gouv.fr/diagnostic/accueil">https://www.cybermalveillance.gouv.fr/diagnostic/accueil</a> <a href="https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris">https://cyber.gouv.fr/prestataires-de-reponse-aux-incidents-de-securite-pris</a>	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	<a href="https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux">https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux</a>	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations
CERT sectoriel	<a href="https://www.cert-aviation.fr">https://www.cert-aviation.fr</a> <a href="https://www.m-cert.fr">https://www.m-cert.fr</a> <a href="https://esante.gouv.fr/produits-services/cert-sante">https://esante.gouv.fr/produits-services/cert-sante</a>	Pour les organisations du secteur de l'aviation, maritime ou santé
CERT-FR	<a href="https://www.cert.ssi.gouv.fr/contact">https://www.cert.ssi.gouv.fr/contact</a>	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	<a href="https://www.cert.ssi.gouv.fr/contact/">https://www.cert.ssi.gouv.fr/contact/</a> <a href="https://cyber.gouv.fr/notifications-reglementaires">https://cyber.gouv.fr/notifications-reglementaires</a>	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	<a href="https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de">https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de</a>	Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.
CNIL	<a href="https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles">https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles</a>	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.