Fiche réflexe

Compromission d'un tenant Azure

Qualification

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, et plus particulièrement les administrateurs Microsoft 365 ainsi que Microsoft Entra ID

2 Quand l'utiliser ?

Utiliser cette fiche en cas de suspicion de compromission d'un tenant Azure, qui englobera le service EntraID, les services Microsoft 365 et le service Azure.

Cette fiche n'a pas vocation à couvrir l'ensemble des scénarios d'attaque pouvant affecter les services Microsoft 365 et Entra ID, mais se concentre sur les cas les plus couramment rencontrés dans le cadre des activités de réponse à incident :

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

3 À quoi sert-elle ?

Cette fiche sert à confirmer et à évaluer la gravité d'un incident de sécurité portant sur un tenant Azure.

(La compromission d'un tenant Microsoft Azure peut recouvrir plusieurs types d'incidents cyber, résultant eux-mêmes de différents modes opératoires d'attaque. Cette fiche se concentre sur les scénarios de compromission les plus fréquemment rencontrés dans les environnements Microsoft 365 et Entra ID. La liste détaillée des attaques prises en compte dans ce document est présentée dans l'annexe Attaques considérées).

4 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 acceptées 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

Fiche réflexe – Compromission d'un tenant Azure – Qualification

Prérequis

01 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.

02 Disposer des personnes et des ressources nécessaires

S'assurer que les personnes qui effectueront la qualification de l'incident aient :

- 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 Entra ID[1] ;
- PowerShell 5 (ou idéalement PowerShell 7) sur le poste utilisé pour 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.

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 et les comptes (voir machines) concernés.

La main courante a pour objectifs de :

- 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 menées 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.

04 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.

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 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 Microsoft Entra ID ;
  - relais de contenu malveillant ;
  - fuite d'information (via partage, ou attaque dite BEC (Business Email Compromise)) ;
  - compromission d'une application d'entreprise Microsoft Entra ID ;

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 ?
- Des changements de configuration suspects sont-ils visibles dans Microsoft Entra ID ?
  - Exemple : des règles de transfert ou de redirection de messages ont-elles été ajoutées sur des comptes compromis, exposant potentiellement d'autres correspondances ou utilisateurs ?
- L'incident est-il circonscrit à une partie du système d'information identifiable ?
  - 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) ?
- Des comptes de service ou d'applications ont-ils été compromis ou créés récemment ?

- D'autres systèmes d'information interconnectés avec celui de l'organisation sont-ils en risque, notamment en cas de fédération Microsoft Entra ?

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 ?
- Y a-t-il une suspicion de compromission d'intégrité de l'environnement Microsoft (ajout de scripts suspects, comptes illégitimes, etc.) ?
- Des données de production ont-elles été supprimées ou chiffrées indiquant une potentielle attaque par extorsion (rançongiciel) ?
- Des données ont-elles été exfiltrées ou partagées publiquement ou vers des domaines externes non autorisés (OneDrive, SharePoint, 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 pour les données des comptes utilisateurs considérés comme potentiellement compromis ?

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

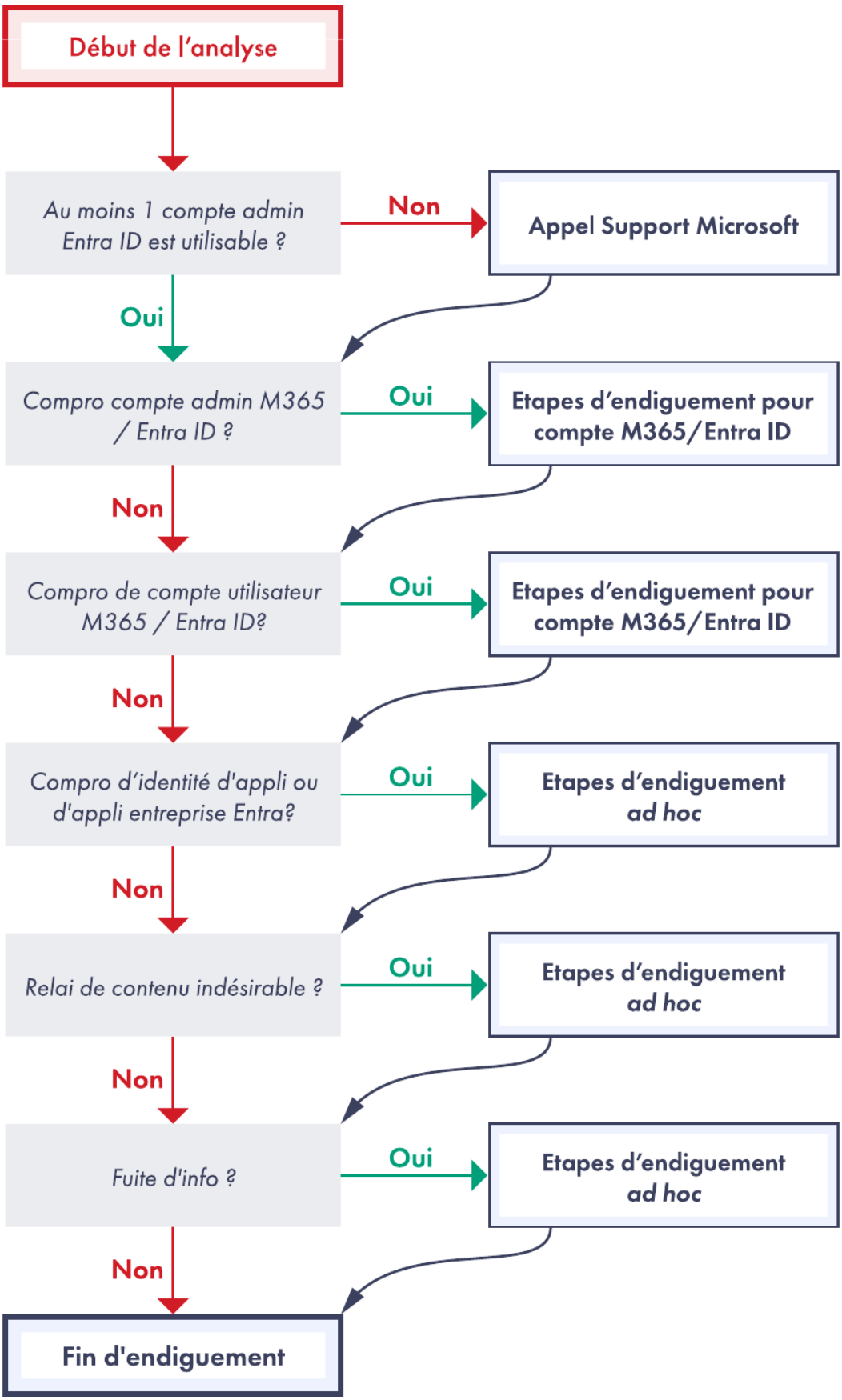
- Quelles sont les activités vitales à l'arrêt, pour lesquelles un rétablissement d'urgence doit être opéré ?
- Quelles sont les activités vitales maintenues en mode dégradé, pour lesquelles il faut préparer dès maintenant un rétablissement ?

Qualifier l'incident

Conclure quant à la gravité de l'incident

- L'incident de type compromission de **tenant** Azure 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 ?


Début de l'analyse
Au moins 1 compte admin Entra ID est utilisable ?
Non
Appel Support Microsoft
Oui
Compro compte admin M365 / Entra ID ?
Oui
Etapes d'endiguement pour compte M365/Entra ID
Non
Compro de compte utilisateur M365 / Entra ID?
Oui
Etapes d'endiguement pour compte M365/Entra ID
Non
Compro d'identité d'appli ou d'appli entreprise Entra?
Oui
Etapes d'endiguement ad hoc
Non
Relai de contenu indésirable ?
Oui
Etapes d'endiguement ad hoc
Non
Fuite d'info ?
Oui
Etapes d'endiguement ad hoc
Non
Fin d'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

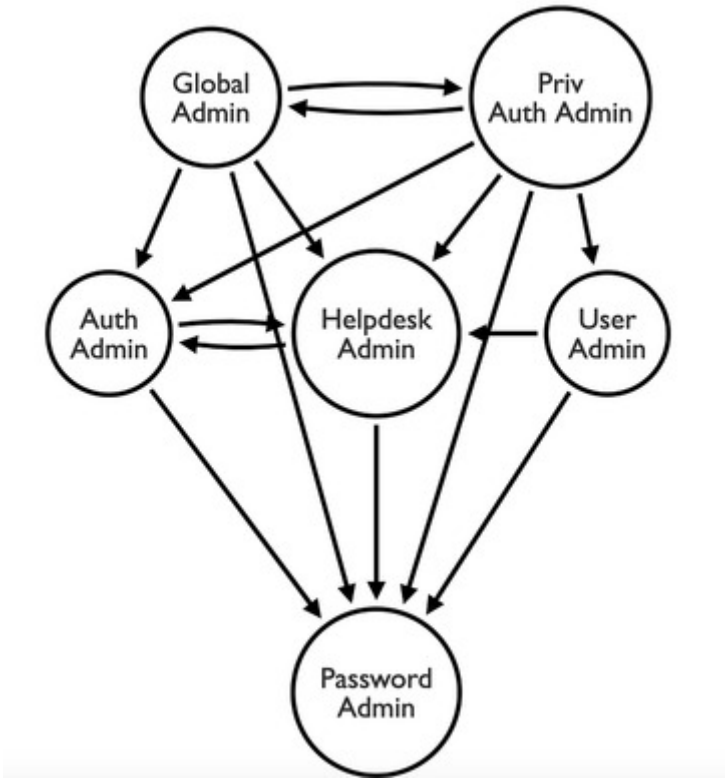
Note : En cas de compromission suspectée ou avérée d'une ressource telle qu'une machine virtuelle hébergée sur Azure : se référer à la fiche réflexe compromission système[2], et si un compte Entra ID est ou a été utilisé sur cette machine, se référer au cas d'usage de la présente fiche : **Compromission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

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 dispose d'un accès à privilèges ("administrateur") sur l'environnement Microsoft 365 et Entra ID de la victime. Si tel est le cas, vérifier 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).

Le schéma suivant montre les chemins d'attaque possibles entre comptes à privilèges[3] :



☐ 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 multifacteur (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**[4] en plus des consoles Microsoft comme celle de gestion du MFA[5] .

☐ 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).

- ☐ 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" [6]. Il est recommandé de faire un export sous Microsoft 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 multifacteur (MFA), à l'aide de la console Microsoft Azure de gestion du MFA [7] ;
- ☐ 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[8] 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 multifacteur ;
- ☐ 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 se faire de manière automatisée à l'aide de ce script : https://github.com/AzureAD/IdentityProtectionTools

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

- ☐ Traiter les alertes relatives aux authentifications considérées à risque, qui sont signalées dans la console MS Entra ID, pour les comptes à privilèges ;
- ☐ Si suspicion de compromission, noter les identifiants utilisateurs des comptes compromis pour lancer la réinitialisation de leurs mots de passe Entra ID, ainsi que forcer l'authentification multifacteur ;

- ☐ 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 automatisée à l'aide de ce 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 [9], puis :
  - ☐ Traiter les alertes relatives aux authentifications considérées à risque, qui sont signalées dans la console MS Entra ID[10] ;
  - ☐ Traiter les alertes relatives aux risques signalés par la console MS Entra ID[11] ;
  - ☐ Traiter les alertes relatives aux adresses IP dites risquées dans la console MS Entra Health Connect[12][13]
- ☐ 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" ;
- ☐ Si des connexions ont été effectuées avec des comptes invités, confirmer auprès des utilisateurs qui ont invité ces "guest" la légitimité de ces invitations, afin de vérifer la légitimité des connexions ;
- ☐ 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 paramétrages 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 ?
  - ☐ Si besoin, se référer à la fiche réflexe CERT Santé Compromission de messagerie.

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

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

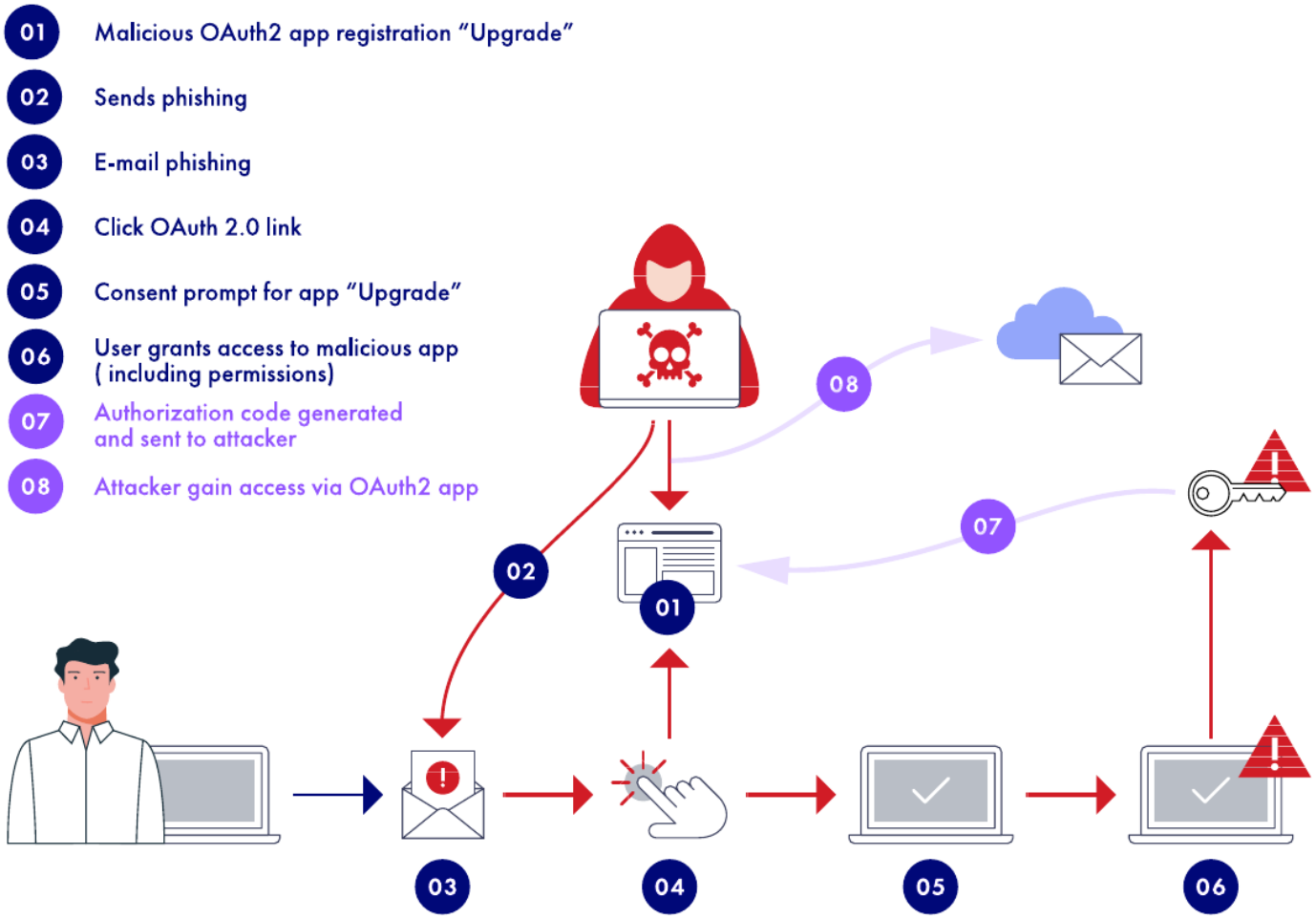
☐ Vérifier la configuration anti-spam

- ☐ 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 Entra ID

Le diagramme suivant représente un type d'attaque possible à partir d'une application malveillante que l'utilisateur 365 va valider[14]:



- [ ] **Traiter les anomalies de 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 Entra ID 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.

☐ Traiter les anomalies de sécurité associées aux services

- ☐ 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" (principaux) de services (source d'événements : "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'événements : "Service Principal Sign-In logs") ;
- ☐ Finalement, l'incident de type compromission d'application d'entreprise Microsoft Entra ID 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 utilisateur[15], en suivant les recommandations Microsoft. Un article décrivant les étapes de cette vérification est disponible dans la documentation Microsoft[16].

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 Entra ID 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"[17];
    - ☐ 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[18];
  - ☐ 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[19].

- ☐ **Vérifier que toute BAL partagée a l'authentification désactivée**
  - ☐ Désactiver l'authentification des boites 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[20].
- ☐ Vérifier qu'il n'y a pas de caractère joker dans les paramétrages "RemoteDomain", notamment les valeurs des paramètres suivants :
  - ☐ "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[21] :

  `powershell 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 :

```
```powershell
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 CERT Santé relative à la compromission d'une BAL / d'un compte de messagerie.

> **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

- [ ] Le compte Microsoft 365 ou Entra ID considéré compromis permet-il au cyber-attaquant de se connecter au SI local aussi, en VPN par exemple ?
- [ ] Un compte à privilèges Microsoft 365 ou Entra ID est-il confirmé comme compromis ?
  - [ ] le cas échéant, le compte Entra ID compromis a-t-il un accès à des machines dans le SI local (compte administrateur InTune, ou compte de réponse à incidents, par exemple) ?

- ☐ Un compte utilisateur Microsoft 365 considéré VIP/VOP est-il confirmé comme compromis ?
- ☐ Les données utilisateur (BAL, OneDrive, espaces Teams) sont-elles altérées voire détruites ?
- ☐ Le vecteur initial pourrait-il provenir d'une entité faisant partie d'une fédération Entra ID avec celle qui déroule la présente fiche ?
- ☐ Des règles de configuration de sécurité ("Conditional Access", MFA) ont-elles été altérées voir supprimées ?

> **Note :** Si compromission d'un compte à privilège ou d'une application privilégiée, le **tenant** doit être considéré comme compromis et la confiance que l'on peut avoir dans son administration doit être réduite. Pour tous les autres cas cités, l'approche recommandée est de remédier avec la confiance que l'administration n'est à priori pas compromise.

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 ?
- ☐ Idem pour des équipements connectés (pare-feu, MDM, etc.) ou éléments d'infrastructure (hyperviseurs...) ?

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 ?
- ☐ Des intervenants externes (prestataires, CERT) sont-ils nécessaires pour la remédiation ?

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.

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 ? (ex : données à caractère personnelles protégées par le RGPD, documents protégés par des règlementations métier)
- ☐ est-ce que des activités métiers dépendent fortement de briques qui seraient dans ce tenant ? (exemple : une structure dont l'application principale niveau S.I. serait un ensemble de machines virtuelles Azure)

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 ?
- ☐ Quelles sont les données sensibles (voire confidentielles) qui sont impactées (volées, altérées, détruites), pour lesquelles il faut lancer dès maintenant un plan d'action ? (exemples : mots de passe, données à caractère personnel, données financières, données de paiement, données contractuelles, données relatives à des brevets ou savoirs-faire industriels, ...)

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 ?

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

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

Suite des actions

Si l'incident est confirmé et qu'il est de type compromission de **tenant** Azure 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 / OneDrive / SharePoint online...	T1114 , T1213
Utilisation illégitime d'un compte utilisateur (à privilèges ou non) Microsoft Entra ID	T1078.004 , T1021.007
Rebond, avec diffusion de contenus malveillants depuis le **tenant** Microsoft 365, ex. : courriels indésirables tels que du **spam** et hameçonnage	T1496.004
Exploitation d'une application d'entreprise légitime enregistrée dans Entra ID (vulnérabilité ou usage détourné)	T1190 et/ou T1528
Installation d'une application d'entreprise malveillante 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.

Définitions

Qualifier un incident

Qualifier un incident signifie :

- **Confirmer** qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa **nature**.
- **Évaluer la gravité/priorité de l'incident** en évaluant le **périmètre** affecté, l'**impact** potentiel sur le fonctionnement de l'organisation et l'**urgence** à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

Axes d'évaluation

- **Périmètre** : Le périmètre d'un incident désigne son étendue sur les composants du système d'information (comptes, applications, systèmes, etc.) et leur administration.
- **Impact** : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- **Urgence** : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Degrés de gravité

- **Anomalie courante** (gravité **faible**) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- **Incident mineur** (gravité **modérée**) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.
- **Incident majeur** (gravité **élevée**) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- **Crise cyber** (gravité **critique**) : Une crise cyber représente un incident de sécurité ayant un **périmètre étendu** sur le système d'information, un **impact fort** sur l'activité métier et nécessitant une **résolution urgente**.

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-servi... cyberveille.esante.gouv.fr	Pour les organisations du secteur de la santé
CERT/CSIRT externe en prestation de réponse à incident	www.cybermalveillance.gou... cyber.gouv.fr/offre-de-servic...	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
Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique	cyber.gouv.fr/piloter-la-remediation-dun...
Fiche réflexe - Compromission de tenant Azure - Endiguement	cyberveille.esante.gouv.fr/dossier-thematique/com...
Qu'est-ce que les services Microsoft 365 ?	learn.microsoft.com/fr-fr/office365/servicedes...
Qu'est-ce que Microsoft Entra et les identifiants Entra ID ?	learn.microsoft.com/fr-fr/entra/fundamentals/w...
Applications Microsoft Entra	learn.microsoft.com/fr-fr/entra/identity/enter...
Rôles Microsoft Entra	learn.microsoft.com/fr-fr/entra/identity/role-...
Rôles Microsoft 365	learn.microsoft.com/fr-fr/microsoft-365/admin/...
Règles de transport Exchange Online	learn.microsoft.com/fr-fr/exchange/security-an...
"RemoteDomain" dans Exchange Online	learn.microsoft.com/en-us/exchange/mail-flow-b...
Présentation rapide de Microsoft Graph	learn.microsoft.com/fr-fr/graph/overview
10 principales façons de sécuriser Microsoft 365 et Entra ID, selon le niveau de licence	learn.microsoft.com/en-us/microsoft-365/admin/...
Recommandation de sécurisation des BAL partagées, niveau authentification	www.tenable.com/audits/CIS_Microsoft_365_F...
Recommandations Microsoft pour la remédiation d'attaques utilisant les règles Outlook	learn.microsoft.com/en-us/defender-office-365/...
Recommandations Microsoft pour la détection et le traitement de l'attaque "Illicit consent Grant"	learn.microsoft.com/en-us/defender-office-365/...
Empêcher un ancien employé de se connecter et bloquer l'accès aux services Microsoft 365	learn.microsoft.com/fr-fr/microsoft-365/admin/...
Recommandations Microsoft pour l'attaque de pulvérisation de mots de passe	learn.microsoft.com/fr-fr/security/operations/...
Attaque dite "Business Email Compromise"	www.microsoft.com/fr-fr/security/business/se...

Document	Lien
Common attacks targeting Microsoft 365 and Azure AD	blog.microwavewitness.eu/work/microsoft/m365_at...
Abusing Azure application credentials to attack supply chains	www.secureworks.com/research/abusing-azure-app...
Matrice ATT&CK pour les services Office de type Microsoft 365	attack.mitre.org/matrices/enterprise/cloud/...
Matrice ATT&CK pour les services de fournisseurs d'identité type Microsoft Entra ID	attack.mitre.org/matrices/enterprise/cloud/...
Module PowerShell Azure AD incident Response	github.com/AzureAD/Azure-AD-Incident-...
Flux de travaux recommandé par Microsoft pour cas d'usage de compromission d'application Azure	learn.microsoft.com/en-us/security/operations/...
Outil d'analyse 365Inspect	github.com/soteria-security/365Inspect

Licence

1. voir en section liens utiles pour plus d'information sur les services "cloud" Microsoft, Microsoft 365 ou sur les rôles Entra ID. ↩
2. Voir https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-systeme-qualification-et-endiguement ↩
3. source https://blog.microwavewitness.eu/work/microsoft/m365_attacks/#action ↩
4. pour plus de détail sur 365Inspect voir l'annexe liens utiles ↩
5. voir https://portal.azure.com/#view/Microsoft_AAD_IAM/MultifactorAuthenticationConfig.ReactView/tabId/users ↩
6. https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/SignIns ↩
7. https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskyUsersBlade ↩
8. https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskySignInsBlade ↩
9. voir https://haveibeenpwned.com ↩
10. voir https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskySignInsBlade ↩
11. voir https://portal.azure.com/#view/Microsoft_AAD_IAM/RiskDetectionsBlade ↩
12. voir https://entra.microsoft.com/#view/Microsoft_AAD_DXP/ScenarioHealthSummary.ReactView ↩
13. 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. ↩

14. voir https://blog.microwavewitness.eu/work/microsoft/m365_attacks/ ↩
15. 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. ↩
16. voir https://learn.microsoft.com/en-us/defender-office-365/detect-and-remediate-illicit-consent-grants?view=o365-worldwide#steps-in-powershell ↩
17. console d'administration MS Exchange Online https://admin.exchange.microsoft.com/#/reports/autoforwardedmessages ↩
18. voir https://learn.microsoft.com/en-us/powershell/module/exchange/export-transportrulecollection?view=exchange-ps ↩
19. Se référer à la section liens utiles pour plus d'information sur les règles de transport. ↩
20. Se référer à la section liens utiles pour plus d'informations sur la sécurisation des boites partagées. ↩
21. Voir en section liens utiles pour plus d'information sur les paramètres "RemoteDomain". ↩