

AUDIT • GOUVERNANCE • DÉTECTION

Sécuriser Microsoft Entra ID et Microsoft 365

Le guide du RSSI

Frédéric PEREZ

Méthode d'audit • Chantiers prioritaires • Feuille de route 12 mois

Sécuriser Microsoft Entra ID et Microsoft 365

Le guide du RSSI

Frédéric PEREZ

Sécuriser Microsoft Entra ID et Microsoft 365 — Le guide du RSSI

© 2026 Frédéric PEREZ

Tous droits réservés. Aucune partie de cet ouvrage ne peut être reproduite sans l'autorisation écrite de l'auteur.

Microsoft, Microsoft 365, Entra ID, Azure, Intune, Purview et Defender sont des marques du groupe Microsoft.
Cet ouvrage est indépendant et n'est ni approuvé ni sponsorisé par Microsoft.

Les informations relatives aux produits, licences et interfaces sont susceptibles d'évoluer après la parution.

Sommaire

Avant-propos.....	3
Plan de l'ouvrage.....	4
PARTIE I — LA SURFACE D'ATTAQUE IDENTITAIRE.....	6
Chapitre 1. Pourquoi l'identité est devenue le périmètre.....	7
Chapitre 2. Anatomie d'un tenant Entra ID et Microsoft 365.....	10
Chapitre 3. Les sept chemins d'attaque réellement observés.....	13
Chapitre 4. Responsabilité partagée : ce que Microsoft couvre, ce qui reste à votre charge	16
PARTIE II — ÉVALUER : LA MÉTHODE D'AUDIT.....	19
Chapitre 5. Cadrer un audit : périmètre, parties prenantes, durée, livrables.....	20
Chapitre 6. Choisir son référentiel : CIS, ANSSI, Zero Trust, MITRE ATT&CK.....	23
Chapitre 7. Collecter la preuve : sources de données, fiabilité, pièges.....	26
Chapitre 8. Les vingt contrôles qui révèlent quatre-vingts pour cent du risque.....	29
Chapitre 9. Noter et prioriser : criticité, effort, impact utilisateur.....	32
Chapitre 10. Rédiger un rapport que le comité de direction lit vraiment.....	35
PARTIE III — CORRIGER : LES CHANTIERS PRIORITAIRES.....	37
Chapitre 11. Comptes à privilèges : rôles, élévation temporaire, accès d'urgence.....	38
Chapitre 12. Authentification résistante à l'hameçonnage et fin des protocoles hérités.....	41
Chapitre 13. Accès conditionnel : un jeu de règles maintenable et testable.....	43
Chapitre 14. Applications et consentements : l'angle mort.....	45
Chapitre 15. Identités non humaines : principaux de service, secrets, certificats.....	47
Chapitre 16. Invités, B2B et partage externe.....	49
Chapitre 17. Données : classification, prévention de fuite, étiquettes — le minimum viable	51
Chapitre 18. Appareils : la conformité comme condition d'accès.....	53
Chapitre 19. Hybride : synchronisation, fédération, résidus.....	55
PARTIE IV — DÉTECTER ET RÉAGIR.....	57
Chapitre 20. Journalisation : quoi garder, combien de temps, à quel coût.....	58
Chapitre 21. Détections qui comptent, bruit à éliminer.....	61
Chapitre 22. Compromission d'un compte à privilèges : le déroulé heure par heure.....	63
Chapitre 23. Reconstruire : révocation, rotation, investigation d'identité.....	66
PARTIE V — GOUVERNER DANS LA DURÉE.....	68
Chapitre 24. Gouvernance des identités : cycle de vie, revues, séparation des tâches.....	69

Chapitre 25. Conformité : NIS2, DORA, ISO 27001, RGPD.....	71
Chapitre 26. Piloter : indicateurs et contrôle continu.....	74
Chapitre 27. Budget et feuille de route à douze mois.....	76
Chapitre 28. Les dix erreurs les plus fréquentes rencontrées en mission.....	78
ANNEXES — OUTILS DE MISE EN ŒUVRE.....	80
Annexe A. Checklist d'audit condensée.....	81
Annexe B. Matrice licences et contrôles.....	83
Annexe C. Modèle de rapport.....	85
Annexe D. Glossaire.....	86
Résumé.....	88

Avant-propos

Ce livre n'est pas un manuel d'administration Microsoft 365. Il ne vous apprendra pas à cocher une case dans un portail : la documentation officielle le fait mieux, et elle est à jour tous les mois.

Il répond à une autre question, celle que l'on me pose en comité de direction depuis dix ans de missions d'audit et d'architecture identitaire : *où en sommes-nous vraiment, qu'est-ce qui nous expose, et dans quel ordre faut-il corriger ?*

La différence est importante. Un tenant Microsoft 365 comporte plusieurs centaines de réglages de sécurité, répartis dans une demi-douzaine de consoles d'administration qui changent de nom tous les dix-huit mois. Aucun responsable de la sécurité n'a le temps de tous les connaître, et il n'en a pas besoin. En revanche, il doit savoir lesquels décident réellement du sort d'une compromission, lesquels ne sont que du confort, lesquels dépendent d'une licence qu'il ne possède peut-être pas, et comment prouver à un auditeur, à un assureur ou à un régulateur que les premiers sont en place.

L'ouvrage est donc construit comme une mission d'audit : comprendre la surface d'attaque, l'évaluer avec une méthode reproductible, corriger par ordre de rendement, détecter ce qui passe malgré tout, puis gouverner dans la durée. Chaque chapitre se termine par une section « Ce que vous devez décider » : ce ne sont pas des recommandations techniques, ce sont les arbitrages qui vous reviennent et que personne ne prendra à votre place.

Les commandes, requêtes et scripts d'extraction ne figurent pas dans le corps du texte. Ils vieillissent vite et alourdissent la lecture. Vous les trouverez en annexe sous forme de checklist condensée, dans un format que votre équipe technique pourra exécuter.

Un dernier avertissement, qui vaut pour tout écrit sur le cloud : les noms de produits, les seuils de licence et les écrans changent. Les mécanismes d'attaque et les principes de contrôle, eux, bougent beaucoup moins. C'est sur ces derniers que ce livre s'appuie, et c'est pourquoi il devrait rester utile plus longtemps qu'une capture d'écran.

Plan de l'ouvrage

Partie I — La surface d'attaque identitaire

- Pourquoi l'identité est devenue le périmètre
- Anatomie d'un tenant Entra ID et Microsoft 365 : le strict nécessaire pour un RSSI
- Les sept chemins d'attaque réellement observés
- Responsabilité partagée : ce que Microsoft couvre, ce qui reste à votre charge

Partie II — Évaluer : la méthode d'audit

- Cadrer un audit : périmètre, parties prenantes, durée, livrables
- Choisir son référentiel : CIS, ANSSI, Zero Trust, MITRE ATT&CK
- Collecter la preuve : sources de données, fiabilité, pièges
- Les vingt contrôles qui révèlent quatre-vingts pour cent du risque
- Noter et prioriser : matrice criticité, effort, impact utilisateur
- Rédiger un rapport que le comité de direction lit vraiment

Partie III — Corriger : les chantiers prioritaires

- Comptes à privilèges : rôles, élévation temporaire, accès d'urgence
- Authentification résistante à l'hameçonnage et fin des protocoles hérités
- Accès conditionnel : un jeu de règles maintenable et testable
- Applications et consentements : l'angle mort
- Identités non humaines : principaux de service, secrets, certificats
- Invités, B2B et partage externe
- Données : classification, prévention de fuite, étiquettes — le minimum viable
- Appareils : la conformité comme condition d'accès
- Hybride : synchronisation, fédération, résidus

Partie IV — Détecter et réagir

- Journalisation : quoi garder, combien de temps, à quel coût
- Détections qui comptent, bruit à éliminer
- Compromission d'un compte à privilèges : le déroulé heure par heure
- Reconstruire : révocation, rotation, investigation d'identité

Partie V — Gouverner dans la durée

- Gouvernance des identités : cycle de vie, revues, séparation des tâches
- Conformité : NIS2, DORA, ISO 27001, RGPD
- Piloter : indicateurs et contrôle continu
- Budget et feuille de route à douze mois

- Les dix erreurs les plus fréquentes rencontrées en mission

Annexes — A. Checklist d’audit condensée · B. Matrice licences et contrôles · C. Modèle de rapport · D. Glossaire

PARTIE I

La surface d'attaque identitaire

CHAPITRE 1

Pourquoi l'identité est devenue le périmètre

Pendant vingt ans, la sécurité d'entreprise s'est organisée autour d'une frontière physique. Il y avait un intérieur et un extérieur, un pare-feu entre les deux, et l'essentiel de l'effort consistait à contrôler ce qui traversait cette ligne. Ce modèle avait un mérite considérable : il était visible. On pouvait le dessiner sur un tableau blanc, l'auditer en suivant des câbles, le budgéter en équipements.

Ce modèle n'a pas disparu, mais il ne décide plus grand-chose. Quand la messagerie, les fichiers, la visioconférence, l'intranet et une part croissante des applications métier sont hébergés par un fournisseur tiers et accessibles depuis n'importe quel réseau, la question « d'où vient cette connexion ? » perd la primauté. La question qui décide devient : « qui est-ce, avec quel appareil, et jusqu'où cette personne peut-elle aller ? »

Le déplacement du point de contrôle

Dans une architecture Microsoft 365, le point de décision n'est plus le pare-feu mais le service d'émission de jetons d'Entra ID. C'est lui qui, à chaque tentative d'accès, évalue l'identité, applique les règles d'accès conditionnel, puis délivre — ou refuse — un jeton qui ouvre la porte d'Exchange Online, de SharePoint, de Teams ou de l'API Microsoft Graph.

Cette bascule a trois conséquences directes pour un responsable sécurité.

La première est que la configuration de ce point de décision devient, à elle seule, une part majeure de la posture de sécurité de l'entreprise. Une règle d'accès conditionnel mal écrite ne produit pas une alerte : elle produit un accès autorisé. C'est un mode de défaillance silencieux, et c'est ce qui le rend dangereux.

La deuxième est que le périmètre est désormais partagé avec des tiers que vous n'administrez pas. Les prestataires, les partenaires, les applications SaaS connectées à votre tenant et les identités applicatives disposent d'accès qui ne passent par aucun de vos équipements réseau.

La troisième, la plus dérangeante, est que la compétence qui protège l'entreprise n'est plus celle de l'équipe réseau. Elle est détenue par les administrateurs de l'annuaire, qui sont souvent restés rattachés à la production informatique, avec des habitudes d'exploitation et non des habitudes de sécurité.

Ce que l'attaquant vise réellement : une session, pas un mot de passe

L'erreur d'analyse la plus répandue consiste à raisonner en termes de mot de passe. On déploie l'authentification multifacteur, on considère le sujet clos, et on découvre en incident que l'attaquant n'a jamais eu besoin du mot de passe.

Ce qui a de la valeur dans une architecture moderne, c'est le jeton : l'artefact délivré après l'authentification, qui prouve à l'application que la vérification a déjà eu lieu. Un jeton d'accès volé donne à l'attaquant exactement ce qu'il vient chercher — l'accès aux données — sans lui demander de rejouer l'authentification. Un jeton de rafraîchissement volé lui

donne mieux encore : la capacité de renouveler cet accès pendant des jours, voire des semaines, sans qu'aucune alerte d'authentification suspecte ne se déclenche.

C'est la raison pour laquelle les campagnes d'hameçonnage actuelles ne cherchent plus à collecter des identifiants mais à intercepter une session complète, en relayant en temps réel la page d'authentification légitime. L'utilisateur voit la vraie page Microsoft, saisit son vrai mot de passe, valide sa vraie notification d'authentification forte — et l'attaquant repart avec le cookie de session.

Retenez la conséquence pratique : un contrôle qui ne protège que le moment de l'authentification est un contrôle partiel. La question à poser à vos équipes n'est pas « avons-nous le MFA ? » mais « que se passe-t-il si un jeton valide est utilisé depuis un appareil que nous ne connaissons pas ? ».

Ce que les incidents publics ont montré

Trois affaires largement documentées suffisent à cadrer le sujet, et elles ont l'avantage d'être vérifiables plutôt que théoriques.

En 2023, l'acteur identifié par Microsoft sous le nom de Storm-0558 a utilisé une clé de signature compromise pour forger des jetons d'authentification et accéder à des boîtes aux lettres d'organisations gouvernementales. Aucun mot de passe n'a été volé, aucune alerte d'authentification anormale n'a été produite chez les victimes : les jetons étaient, du point de vue de l'application, parfaitement valides. Cet incident a également révélé que la capacité à investiguer dépendait du niveau de licence de journalisation détenu — un point qui a suffisamment ému les régulateurs pour que Microsoft élargisse ensuite l'accès aux journaux d'audit.

En janvier 2024, Microsoft a rendu public le fait qu'un acteur étatique, désigné Midnight Blizzard, avait obtenu un accès initial par une attaque par pulvérisation de mots de passe sur un ancien compte de test non protégé par authentification multifacteur, dans un tenant hérité. L'accès a ensuite été étendu via une application OAuth disposant de permissions élevées sur Exchange Online. Deux enseignements : le compte oublié n'est pas un détail d'hygiène, et l'application applicative est un vecteur d'élévation au même titre qu'un compte humain.

Enfin, plusieurs groupes criminels ont démontré ces dernières années que le maillon le plus rentable restait le processus humain : appel au support informatique, demande de réinitialisation de la méthode d'authentification, contournement complet du dispositif technique. Aucun de vos budgets d'outillage ne couvre ce chemin. Seule une procédure de vérification d'identité au support le couvre.

Pourquoi ce sujet ne se délègue pas

Il existe une tentation légitime, pour un responsable sécurité, de considérer la configuration d'Entra ID comme un sujet d'exploitation à confier à l'équipe qui administre déjà la messagerie et les postes de travail. Cette délégation produit systématiquement le même résultat en audit.

L'équipe d'exploitation optimise la disponibilité et la fluidité du service. Elle est jugée sur le nombre de tickets et sur l'absence d'interruption. Face à un arbitrage entre un contrôle qui bloquera dix utilisateurs et un contrat de service à tenir, elle tranchera dans le sens de la continuité — non par négligence, mais parce que c'est exactement ce qu'on lui

demande. C'est ainsi que naissent les exclusions permanentes dans les règles d'accès conditionnel, les comptes de service dispensés d'authentification forte, les applications autorisées « en attendant » depuis trois ans.

Le rôle du responsable sécurité n'est pas d'administrer l'annuaire. Il est de fixer ce qui n'est pas négociable, d'exiger que toute exception soit datée et tracée, et de disposer d'une mesure indépendante de l'état réel du tenant. Les trois parties suivantes de ce livre servent précisément à cela.

Ce que vous devez décider

- **Qui est propriétaire de la configuration d'identité ?** Tant que la réponse est « la production », vous n'avez pas de contrôle, vous avez une espérance. Nommez un propriétaire et distinguez explicitement qui configure, qui valide et qui contrôle.
- **Quel est votre niveau d'ambition sur le vol de session ?** C'est l'arbitrage structurant de tout le programme : accepter le risque de rejeu de jeton coûte peu aujourd'hui et beaucoup le jour de l'incident. Le traiter suppose d'engager la conformité des appareils et l'authentification résistante à l'hameçonnage, avec un impact utilisateur réel.
- **Combien d'exceptions êtes-vous prêt à tolérer, et pour combien de temps ?** Fixez le principe maintenant, à froid : toute exception porte une date de fin et un nom de responsable. Cette règle, décidée en amont, vous évitera l'essentiel des dérives constatées en mission.
- **Le support informatique fait-il partie de votre périmètre de sécurité ?** Si la réinitialisation d'une méthode d'authentification peut être obtenue par téléphone sans preuve d'identité forte, votre investissement technique est plafonné par cette procédure.

CHAPITRE 2

Anatomie d'un tenant Entra ID et Microsoft 365

Ce chapitre est un raccourci délibéré. Il ne décrit pas l'ensemble de la plateforme, mais le sous-ensemble d'objets et de consoles qu'un responsable sécurité doit connaître pour poser les bonnes questions, comprendre une réponse technique et repérer une réponse évasive.

Le tenant : une frontière, pas un réseau

Le tenant est l'instance d'annuaire dédiée à votre organisation. C'est la véritable unité de sécurité de l'écosystème Microsoft : les identités, les groupes, les applications, les stratégies et les données de collaboration y résident, et toute action d'administration s'y rattache.

Deux conséquences méritent d'être comprises dès le départ.

D'abord, la frontière n'a rien de géographique ni de réseau. Un tenant est atteignable depuis internet par construction. Ce ne sont pas des équipements qui filtrent l'accès, mais des stratégies.

Ensuite, une organisation possède rarement un seul tenant. Les fusions, les filiales, les projets pilotes et les environnements de test en créent, et ces tenants secondaires — moins surveillés, moins licenciés, souvent oubliés — sont un point d'entrée récurrent. Le premier réflexe d'audit consiste à établir l'inventaire des tenants réellement rattachés à l'entreprise, y compris ceux créés par inscription libre d'un utilisateur avec une adresse professionnelle.

Les objets qui comptent

Les utilisateurs. Comptes membres synchronisés depuis un annuaire local ou créés dans le cloud, comptes invités issus d'autres organisations, comptes de service détenus par des équipes techniques. Ces trois populations n'ont ni le même cycle de vie, ni le même niveau de contrôle, et doivent être traitées séparément.

Les groupes. Ils portent les droits d'accès. Deux natures coexistent : les groupes de sécurité, contrôlés par l'informatique, et les groupes Microsoft 365, qui peuvent être créés par les utilisateurs eux-mêmes et sont adossés à une boîte aux lettres, un site SharePoint et une équipe Teams. Un groupe est aussi un objet à privilèges dès lors qu'il est utilisé pour attribuer un rôle : qui peut modifier son appartenance peut, indirectement, s'attribuer ce rôle.

Les rôles d'annuaire. Une centaine de rôles intégrés existent, mais une poignée seulement porte un risque majeur : administrateur général, administrateur de rôle privilégié, administrateur d'application, administrateur d'authentification, administrateur d'utilisateurs, administrateur Exchange. Le rôle d'administrateur général doit être considéré comme l'équivalent d'un compte d'administrateur de domaine dans un annuaire local : sa possession équivaut à la possession de l'organisation.

Les applications et les principaux de service. C'est l'objet le plus mal compris et, en pratique, le plus dangereux. Une inscription d'application définit une identité

applicative ; le principal de service en est l'instance active dans votre tenant, avec ses permissions et ses secrets. Ces identités s'authentifient sans intervention humaine, ne sont soumises à aucune authentification multifacteur, et peuvent détenir des permissions bien supérieures à celles d'un utilisateur, y compris la lecture de l'ensemble des boîtes aux lettres.

Les appareils. Un appareil peut être inscrit, joint à Entra ID ou joint en mode hybride. Cet état conditionne la possibilité même d'exiger un appareil conforme comme condition d'accès. Sans gestion des appareils, une partie importante de l'arsenal d'accès conditionnel reste hors de portée.

Les unités administratives. Elles permettent de restreindre la portée d'un administrateur à une population donnée. Utilisées correctement, elles sont l'un des rares outils de réduction structurelle des privilèges dans Entra ID.

Les plans de contrôle : qui administre quoi

Une source récurrente de confusion en réunion tient à la multiplicité des consoles. Retenez la répartition suivante.

Le centre d'administration Entra ID porte les identités, les rôles, les applications et l'accès conditionnel. Le centre d'administration Microsoft 365 porte les utilisateurs, les licences et les services de collaboration. Le portail Microsoft Purview porte la conformité, la classification des données, la prévention de fuite et une part de la journalisation d'audit. Microsoft Intune porte les appareils et leur conformité. Le portail Microsoft Defender porte la détection et la réponse. Le portail Azure, enfin, porte les abonnements et les ressources d'infrastructure, qui constituent un domaine de sécurité distinct mais dépendent du même annuaire.

La conséquence pratique est qu'il n'existe pas d'écran unique donnant l'état de sécurité du tenant. Toute affirmation du type « le tableau de bord est au vert » doit être précisée : quel tableau de bord, quel périmètre, quelle date. C'est aussi la raison d'être des démarches d'audit outillées : consolider une vue que la plateforme ne fournit pas nativement.

Les points d'entrée réels

Un tenant expose bien plus que ses portails d'administration. Les charges de travail — Exchange Online, SharePoint, OneDrive, Teams — sont accessibles par navigateur, par client lourd et par mobile. Surtout, l'API Microsoft Graph offre un accès programmatique à l'ensemble de l'annuaire et des données, et les modules PowerShell d'administration constituent un canal d'administration complet, indépendant des interfaces graphiques.

Il en découle une règle qui surprend souvent les directions : restreindre l'accès aux portails d'administration ne protège rien si les mêmes actions restent possibles via Graph ou PowerShell. Les contrôles doivent porter sur l'identité et la session, pas sur l'interface.

Vocabulaire minimum

Quelques termes reviendront constamment, et les employer correctement change la qualité des échanges avec vos équipes techniques.

L'**authentification** établit qui vous êtes ; l'**autorisation** détermine ce que vous pouvez faire. Le **jeton** matérialise le résultat des deux. Le **consentement** est l'acte par lequel un utilisateur ou un administrateur accorde des permissions à une application. Les

permissions déléguées s'exercent au nom d'un utilisateur connecté et restent bornées par ses droits ; les **permissions d'application** s'exercent sans utilisateur et ne connaissent pas cette borne. Cette dernière distinction est probablement la plus rentable de tout ce chapitre : c'est elle qui sépare une application inoffensive d'une application capable de lire l'intégralité de votre messagerie d'entreprise.

Ce que vous devez décider

- **Disposez-vous d'un inventaire des tenants ?** Tant qu'il n'existe pas, votre périmètre d'audit est déclaratif. Décidez qui l'établit et à quelle fréquence il est révisé.
- **Qui a le droit de créer des applications et de consentir en leur nom ?** C'est une décision de gouvernance, pas un réglage technique, et elle conditionne le chapitre 14.
- **Acceptez-vous que des administrateurs disposent d'une portée globale ?** Si non, les unités administratives et la délégation par périmètre doivent entrer dans la feuille de route dès la première année.
- **Quel niveau de connaissance exigez-vous de vos propres équipes sécurité ?** Un responsable sécurité qui ne distingue pas permission déléguée et permission d'application ne peut pas arbitrer les risques applicatifs. C'est un besoin de formation à budgéter, au même titre qu'un outil.

CHAPITRE 3

Les sept chemins d'attaque réellement observés

Les catalogues de menaces sont longs et peu actionnables. Ce chapitre prend le parti inverse : sept chemins, ceux que l'on retrouve dans la grande majorité des compromissions de tenants Microsoft 365 documentées publiquement ou traitées en mission. Pour chacun, trois éléments seulement : comment il fonctionne, à quoi on le repère, et quel contrôle le coupe.

1. L'hameçonnage avec relais et vol de session

L'attaquant héberge un site qui relaie en temps réel la page d'authentification Microsoft légitime. La victime s'authentifie normalement, valide sa notification d'authentification forte, et l'attaquant capture le cookie de session émis à l'issue du processus. Il rejoue ensuite ce cookie depuis sa propre machine et accède à la messagerie sans jamais s'authentifier.

Signal : une même session utilisée depuis deux adresses réseau ou deux empreintes de navigateur très différentes, l'apparition de règles de boîte aux lettres qui déplacent ou suppriment automatiquement des messages, une inscription de nouvelle méthode d'authentification juste après la connexion.

Contrôle qui coupe le chemin : l'authentification résistante à l'hameçonnage — clés FIDO2, Windows Hello Entreprise, authentification par certificat — car le relais ne peut pas rejouer une preuve liée à l'origine du site. À défaut, l'exigence d'appareil conforme ou joint au domaine réduit fortement l'exploitabilité du jeton volé.

2. Le consentement applicatif abusif

L'attaquant fait parvenir à la victime une invitation à autoriser une application d'apparence anodine. En un clic, l'application obtient des permissions durables sur la messagerie ou les fichiers. Aucun mot de passe n'est échangé, aucun jeton n'est volé, et le changement de mot de passe de la victime ne révoque rien.

Signal : consentement accordé à une application dont l'éditeur n'est pas vérifié, création récente d'un principal de service, activité de l'API Graph depuis une application inconnue.

Contrôle qui coupe le chemin : désactivation du consentement utilisateur libre, mise en place d'un flux de demande d'approbation, et revue périodique des applications consenties. C'est un contrôle peu coûteux et très rentable, presque toujours absent dans les tenants audités.

3. L'abus des flux d'authentification alternatifs

Certains flux d'authentification, notamment le flux par code d'appareil prévu pour les équipements sans clavier, permettent à un attaquant de faire valider par la victime une authentification qu'il a lui-même initiée. La victime croit approuver une action légitime.

Signal : connexions utilisant un flux d'authentification inhabituel pour votre parc, en particulier depuis des adresses ou des pays qui ne correspondent pas au profil de l'utilisateur.

Contrôle qui coupe le chemin : le blocage explicite des flux d'authentification non nécessaires par accès conditionnel. La plupart des organisations n'ont aucun besoin fonctionnel de ces flux et peuvent les interdire sans effet de bord.

4. La prise de contrôle d'un compte à privilèges

Trois variantes dominent : la pulvérisation de mots de passe sur des comptes anciens ou de test non protégés, la sollicitation répétée de notifications d'authentification jusqu'à validation par lassitude, et l'appel au support informatique pour obtenir la réinitialisation d'une méthode d'authentification.

Signal : échecs d'authentification massifs et distribués, notifications refusées en rafale suivies d'une acceptation, réinitialisation de méthode d'authentification hors procédure.

Contrôle qui coupe le chemin : aucun contrôle technique isolé n'y suffit. Il faut la conjonction d'une authentification forte résistante à l'hameçonnage pour les administrateurs, de la correspondance de numéro sur les notifications, de l'élévation temporaire des privilèges plutôt que de l'attribution permanente, et d'une procédure de vérification d'identité au support. Ce point sera repris en détail au chapitre 11.

5. Les identités non humaines

Les principaux de service, comptes de service et secrets applicatifs constituent le chemin le plus discret. Ils échappent à l'authentification multifacteur par nature, leurs secrets sont souvent stockés dans des dépôts de code ou des fichiers de configuration, et leurs permissions ont rarement été revues depuis leur création. Une identité applicative disposant d'un accès complet à Exchange Online équivaut à un accès à toute la messagerie de l'entreprise.

Signal : secrets à durée de validité longue ou expirée puis renouvelée sans revue, permissions d'application de portée globale, authentification d'un principal de service depuis une adresse inhabituelle.

Contrôle qui coupe le chemin : inventaire et propriétaire nommé pour chaque identité applicative, remplacement des secrets par des certificats ou des identités managées, restriction des permissions au strict nécessaire, et application de règles d'accès conditionnel aux identités de charge de travail lorsque la licence le permet.

6. Le chemin hybride, de l'annuaire local vers le cloud

Lorsqu'un Active Directory local est synchronisé avec Entra ID, la compromission du domaine local devient une compromission du tenant. Les composants de synchronisation détiennent des privilèges élevés, les serveurs de fédération résiduels permettent de forger des assertions d'authentification, et certains mécanismes d'authentification unique reposent sur des comptes d'annuaire dont le secret n'est jamais renouvelé.

Signal : authentifications fédérées incohérentes avec l'activité réelle, modifications de la configuration de fédération, comptes de synchronisation utilisés depuis un serveur inattendu.

Contrôle qui coupe le chemin : traiter les serveurs de synchronisation et de fédération comme des systèmes de niveau zéro, au même titre qu'un contrôleur de domaine ; supprimer la fédération résiduelle quand elle n'est plus nécessaire ; renouveler les secrets des comptes techniques hérités. Ce chantier fait l'objet du chapitre 19.

7. La collaboration externe et les invités

Le partage externe, les liens anonymes et les comptes invités créent des accès qui échappent aux revues classiques. Un invité oublié conserve son accès pendant des années ; un lien « toute personne disposant du lien » survit à la fin du projet ; un canal partagé ouvre un accès croisé entre organisations.

Signal : invités sans activité récente, liens anonymes sur des sites contenant des données sensibles, invitations émises par des utilisateurs non habilités.

Contrôle qui coupe le chemin : paramétrage des accès entre organisations, expiration automatique des liens, revues d'accès régulières sur la population des invités.

Ce qu'il faut retenir de ces sept chemins

Aucun ne repose sur une vulnérabilité logicielle à corriger par un correctif. Tous exploitent une configuration, une permission ou une procédure. C'est une bonne nouvelle budgétaire — la correction relève rarement de l'achat — et une mauvaise nouvelle organisationnelle : la correction relève d'arbitrages, de gouvernance et de discipline dans la durée.

Ce que vous devez décider

- **Traitez-vous ces sept chemins comme des scénarios de risque formalisés ?** S'ils ne figurent pas dans votre analyse de risque, votre plan d'action ne pourra pas être priorisé rationnellement.
- **Quel chemin acceptez-vous consciemment de ne pas couvrir cette année ?** Il est légitime de renoncer, à condition de le décider explicitement, de le documenter et de le porter au registre des risques — plutôt que de le découvrir en post-mortem.
- **Vos capacités de détection couvrent-elles les signaux listés ci-dessus ?** Le chapitre 21 y revient, mais la question se pose dès maintenant : sans journalisation adaptée, ces sept chemins sont invisibles.

CHAPITRE 4

Responsabilité partagée : ce que Microsoft couvre, ce qui reste à votre charge

Le modèle de responsabilité partagée est cité dans toutes les présentations et compris dans peu d'organisations. La formule usuelle — « le fournisseur est responsable de la sécurité *du* cloud, le client de la sécurité *dans* le cloud » — est exacte mais trop abstraite pour arbitrer un budget. Ce chapitre la traduit en termes opérationnels.

Ce que le fournisseur assure effectivement

Microsoft opère l'infrastructure physique, l'hyperviseur, le réseau du service, la disponibilité de la plateforme, l'application des correctifs sur ses propres composants et la résilience des données au niveau du service. Il fournit également l'outillage de sécurité que vous activez : accès conditionnel, protection contre les menaces, journalisation, classification.

Il faut lire attentivement le verbe : le fournisseur *fournit* ces capacités. Il ne les configure pas pour vous, ne décide pas de vos exceptions et ne porte pas la responsabilité d'un accès accordé par votre propre configuration. Un tenant compromis par un consentement applicatif abusif est un incident client, pas un incident fournisseur.

Ce qui reste intégralement à votre charge

Les identités et leur cycle de vie. Les privilèges et leur attribution. La configuration des stratégies d'accès. Les applications autorisées dans votre tenant et les permissions qui leur sont accordées. La classification et le partage de vos données. La conformité des appareils. La détection et la réponse sur votre périmètre. Et, point systématiquement sous-estimé, la conservation de vos données au-delà des durées natives du service.

Le malentendu le plus coûteux : sauvegarde et rétention

Deux confusions reviennent en audit et méritent d'être tranchées une fois pour toutes.

La première concerne la sauvegarde. La réplication assurée par le fournisseur protège contre la défaillance de son infrastructure. Elle ne protège pas contre une suppression massive par un attaquant disposant de privilèges, ni contre un chiffrement de contenus, ni contre une erreur d'exploitation détectée trois mois plus tard. Les mécanismes natifs de rétention et de conservation offrent des fenêtres de récupération limitées et pilotées par des paramètres que l'attaquant privilégié peut lui-même modifier. Si votre plan de continuité repose sur l'hypothèse d'une sauvegarde de la messagerie et des fichiers, cette hypothèse doit être vérifiée explicitement, et documentée.

La seconde concerne les journaux. La durée de conservation native des journaux d'authentification et d'audit dans l'annuaire se compte en jours ou en semaines selon le niveau de licence, et les journaux d'activité de collaboration en mois. Or la durée moyenne entre la compromission initiale et sa détection dépasse fréquemment ces fenêtres. Une organisation qui découvre un incident au bout de quatre mois sans avoir exporté ses journaux ne pourra pas établir le déroulé des faits : elle ne saura ni quand l'accès a

commencé, ni ce qui a été consulté. Cette incapacité a des conséquences réglementaires directes, notamment sur les obligations de notification. Le chapitre 20 traite du dimensionnement de cette conservation.

La licence comme facteur limitant

C'est la contrainte que les responsables sécurité découvrent le plus tard, et souvent au pire moment. Dans l'écosystème Microsoft, une part significative des contrôles de sécurité est conditionnée au niveau de licence détenu, et cette dépendance porte sur des fonctions structurantes.

Les règles d'accès conditionnel, socle de toute la politique d'accès, relèvent du premier niveau de licence premium de l'annuaire. L'élévation temporaire de privilèges, les revues d'accès et la protection basée sur le risque relèvent du second. La gouvernance des identités — gestion des droits d'utilisation, flux de cycle de vie — relève d'une offre dédiée. Le contrôle d'accès conditionnel appliqué aux identités applicatives relève d'un module additionnel. Côté données, la classification automatique et une partie de la prévention de fuite relèvent du niveau supérieur des suites Microsoft 365.

Deux erreurs symétriques en découlent. La première consiste à concevoir une architecture cible qui suppose des licences que l'entreprise n'a pas et n'achètera pas : le plan est irréalisable et perd sa crédibilité dès la première revue. La seconde consiste à ne pas chiffrer l'écart : la direction générale arbitre alors sans savoir que le renoncement à un niveau de licence signifie l'absence de revue d'accès ou l'impossibilité d'élever temporairement des privilèges.

La position professionnelle consiste à produire systématiquement deux versions de la feuille de route : celle réalisable avec le socle licencié actuel, et celle qui nécessite une évolution, avec le coût associé et les risques qu'elle couvre. C'est l'unique manière de transformer une contrainte commerciale en décision éclairée.

Compléter par un tiers, ou monter en gamme ?

L'arbitrage revient dans presque toutes les missions. Trois critères permettent de le trancher sans dogmatisme.

L'intégration d'abord : un contrôle natif s'applique au point de décision d'authentification, là où un outil tiers agit souvent en aval, en détection plutôt qu'en blocage. Le coût total ensuite : une solution tierce moins chère à l'achat mobilise du temps d'intégration, de maintenance et de compétence rare. La réversibilité enfin : l'adhérence au fournisseur unique est un risque réel de concentration, que certains régulateurs commencent explicitement à examiner.

En pratique, deux domaines justifient fréquemment un complément tiers, quel que soit le niveau de licence : la sauvegarde des données de collaboration, et la conservation longue durée des journaux à coût maîtrisé.

Ce que vous devez décider

- **Avez-vous une position écrite sur la sauvegarde de Microsoft 365 ?** Si la réponse est « on suppose que c'est couvert », vous avez un risque non traité qui se matérialisera au pire moment.

- **Quelle durée de conservation des journaux vous engagez-vous à tenir ?** Fixez-la à partir de vos obligations réglementaires et du délai de détection réaliste, pas à partir de la valeur par défaut du service.
- **Le coût des licences de sécurité est-il porté par le budget sécurité ou par le budget bureautique ?** Cette question paraît administrative ; elle détermine en réalité qui arbitre les renoncements de sécurité.
- **Votre feuille de route existe-t-elle en deux versions ?** Une version à licence constante, une version cible chiffrée. Sans cela, aucun arbitrage éclairé n'est possible au niveau de la direction générale.

PARTIE II

Évaluer : la méthode d'audit

CHAPITRE 5

Cadrer un audit : périmètre, parties prenantes, durée, livrables

La qualité d'un audit se joue avant la première extraction. Un cadrage flou produit un rapport que personne ne conteste et que personne n'applique : trop large pour être actionnable, trop technique pour être arbitré, trop vague pour être opposé à qui que ce soit. Ce chapitre décrit le cadrage minimal d'une mission d'évaluation de la sécurité d'un environnement Entra ID et Microsoft 365.

Ce que l'audit doit trancher

Commencez par écrire la question à laquelle le rapport devra répondre. Elle n'est jamais « sommes-nous sécurisés ». Elle prend l'une des trois formes suivantes, et elles ne conduisent pas au même travail.

Quel est notre niveau d'exposition ? C'est l'audit de posture. Il mesure l'écart entre la configuration réelle et un état de référence, priorise, et alimente une feuille de route.

Sommes-nous conformes à un référentiel donné ? C'est l'audit de conformité. Il produit une réponse contrôle par contrôle, avec preuve à l'appui, opposable à un auditeur externe, un assureur ou un régulateur.

Avons-nous été compromis ? C'est une investigation, pas un audit. Les méthodes, les compétences et l'urgence diffèrent radicalement. Si le doute existe, traitez-le d'abord, séparément.

La confusion la plus fréquente en entreprise consiste à commander le premier et à attendre le troisième. Écrivez la question dans la lettre de mission.

Les trois périmètres à distinguer

Le périmètre d'identité couvre le tenant, les identités humaines et applicatives, les rôles, les stratégies d'accès et les méthodes d'authentification. C'est le cœur.

Le périmètre de collaboration couvre Exchange Online, SharePoint, OneDrive et Teams : partage externe, liens anonymes, règles de transport, rétention.

Le périmètre d'infrastructure couvre les abonnements Azure et leurs ressources. Il dépend du même annuaire mais constitue un domaine technique distinct, avec ses propres référentiels. L'inclure double la charge. Le décider explicitement évite la dérive de périmètre en cours de mission.

À ces trois périmètres s'ajoute une question préalable qui n'est pas optionnelle : **combien de tenants ?** Tant que l'inventaire n'est pas établi, le périmètre annoncé est une hypothèse. Prévoyez systématiquement une phase de découverte en amont, y compris pour les tenants créés par inscription libre sur un domaine d'entreprise.

Les accès nécessaires, et ceux qu'il faut refuser

Un audit de posture se conduit intégralement en lecture seule. Les rôles de lecture globale et de lecture de sécurité, complétés selon les cas d'un accès en lecture aux journaux de conformité et à la gestion des appareils, suffisent à collecter l'ensemble des preuves.

Refusez un rôle d'administration, même proposé de bonne foi pour « aller plus vite ». Un auditeur disposant d'un rôle d'administrateur général contamine sa propre preuve : il devient impossible d'affirmer ensuite qu'une modification observée ne vient pas de lui. La séparation entre celui qui mesure et celui qui configure est la première règle du métier.

Point pratique souvent négligé : l'accès en lecture doit être demandé au moins une semaine avant le démarrage. Le délai d'obtention des habilitations est, dans la majorité des missions, le premier facteur de retard.

Parties prenantes

Quatre rôles doivent être nommés dans la lettre de mission, avec un nom de personne et non un nom d'équipe.

Le commanditaire, qui arbitrera les recommandations — en général le responsable de la sécurité ou le directeur des systèmes d'information. Le référent technique identité, qui répond aux questions de configuration et prépare les accès. Le référent conformité ou juridique, dès lors que l'audit touche à des données personnelles ou à une obligation réglementaire. Le représentant de l'exploitation, car c'est lui qui portera la charge des corrections et dont l'absence en phase de cadrage garantit un plan d'action irréaliste.

Durée réaliste

Pour un tenant unique, sans annuaire local, sans exigence de conformité formelle : cinq à huit jours ouvrés, dont deux de collecte, trois d'analyse et de rédaction.

Pour un environnement hybride avec synchronisation d'annuaire, plusieurs domaines et un périmètre de collaboration inclus : dix à quinze jours.

Pour un groupe multi-tenants, avec exigences réglementaires et restitution en comité : au-delà de vingt jours, et il devient préférable de découper en lots plutôt que de produire un rapport unique de trois cents pages que personne ne lira.

Ajoutez systématiquement un délai calendaire entre la collecte et la restitution : les questions de clarification aux équipes techniques prennent des jours, pas des heures.

Livrables

Trois livrables, pas plus, et ils s'adressent à trois publics différents.

Une synthèse de direction de deux à quatre pages : verdict d'exposition, trois scénarios de risque majeurs, décisions demandées, budget indicatif.

Un rapport détaillé : constat par domaine, preuve, criticité, recommandation, effort estimé.

Un plan d'action séquencé, exploitable tel quel comme feuille de route, avec pour chaque action un responsable pressenti et une vague temporelle.

Le chapitre 10 revient en détail sur la rédaction de ces documents. Retenez seulement ici qu'un livrable unique de cent pages n'est pas un livrable : c'est une archive.

Les pièges de cadrage

Le premier est l'audit fondé sur le déclaratif. Une réponse d'équipe technique n'est pas une preuve. Tout constat doit reposer sur une extraction datée.

Le deuxième est la dérive de périmètre. Une fois la mission engagée, chaque partie prenante souhaite y ajouter son sujet. Fixez la règle : toute extension fait l'objet d'un avenant écrit.

Le troisième est la confusion avec un test d'intrusion. L'audit de configuration mesure l'exposition ; le test d'intrusion démontre l'exploitabilité. Les deux sont complémentaires, aucun ne remplace l'autre, et les commander comme un seul lot produit généralement un résultat médiocre sur les deux plans.

Ce que vous devez décider

- **Quelle est la question à laquelle le rapport doit répondre ?** Écrivez-la en une phrase dans la lettre de mission. Sans elle, vous obtiendrez une liste d'écarts, pas une aide à la décision.
- **Le périmètre d'infrastructure Azure est-il inclus ?** La réponse change la charge, le profil de compétence requis et le référentiel utilisé.
- **Qui portera les corrections ?** Si cette personne n'est pas présente au cadrage, le plan d'action sera irréaliste et le rapport restera lettre morte.
- **Le rapport a-t-il vocation à être opposable ?** Si oui, la conservation des preuves, leur horodatage et leur intégrité doivent être organisés dès la collecte, pas reconstitués après coup.

CHAPITRE 6

Choisir son référentiel : CIS, ANSSI, Zero Trust, MITRE ATT&CK

Un audit sans référentiel n'est qu'une opinion. Le choix du référentiel détermine ce qui sera regardé, ce qui sera considéré comme un écart, et la légitimité du constat face à une équipe technique qui le contestera. Ce chapitre présente les quatre corpus utiles et, surtout, la manière de les combiner sans les empiler.

CIS Microsoft 365 Foundations Benchmark

C'est le référentiel de configuration le plus directement exploitable. Il énumère des contrôles précis, chacun assorti d'une justification, d'une procédure de vérification et d'une procédure de remédiation. Il se décline en deux niveaux : le niveau 1 rassemble les mesures applicables sans effet notable sur les utilisateurs, le niveau 2 les mesures de renforcement dont l'adoption suppose un arbitrage d'usage.

Ses forces : granularité, neutralité, mise à jour régulière, et surtout la possibilité de produire un constat non discutable — le contrôle est appliqué ou il ne l'est pas.

Ses limites : il ne hiérarchise pas les contrôles par risque réel. Deux cents écarts de niveau 1 traités sans priorisation donneront un plan d'action ingérable. Il suppose également un niveau de licence qui n'est pas toujours détenu. Enfin, il évalue une configuration, jamais un usage : un contrôle correctement configuré mais assorti de trente exclusions passe le test.

Le benchmark CIS est donc un excellent instrument de mesure et un mauvais instrument de priorisation. Utilisez-le pour la première fonction seulement.

Les publications de l'ANSSI

L'ANSSI n'édite pas de référentiel de configuration Microsoft 365 comparable au CIS, mais ses publications apportent trois éléments que le CIS ne fournit pas.

Le modèle de cloisonnement par niveaux d'administration, issu des guides de sécurisation de l'Active Directory, reste la meilleure grille d'analyse pour traiter le chemin hybride et les postes d'administration. Il transpose directement au cloud : les composants de synchronisation et les administrateurs de l'annuaire appartiennent au niveau le plus sensible et doivent être administrés depuis des postes dédiés.

La doctrine relative au recours aux services d'informatique en nuage donne le cadre d'analyse de la sensibilité des données confiées à un fournisseur — question que le CIS n'aborde pas et que votre direction générale posera.

Enfin, la qualification des prestataires et des services fournit un langage commun avec les autorités et les clients du secteur public. Dans un dossier de conformité français, une recommandation adossée à une publication de l'ANSSI porte davantage qu'une recommandation adossée à un référentiel étranger.

Zero Trust

Zero Trust n'est pas un référentiel d'audit : c'est un modèle d'architecture cible. Ses trois principes — vérifier explicitement, appliquer le moindre privilège, présumer la compromission — ne se cochent pas, ils orientent.

Son utilité est ailleurs : il donne au rapport sa colonne vertébrale narrative. Il permet d'expliquer à une direction générale pourquoi l'exigence d'appareil conforme et l'authentification résistante à l'hameçonnage ne sont pas deux mesures de plus dans une liste de deux cents, mais les deux piliers d'un modèle cohérent. Un audit qui ne s'appuie que sur une liste de contrôles produit une pile de correctifs ; un audit adossé à un modèle produit une direction.

Sa limite est symétrique : employé seul, il autorise tous les discours. « Nous sommes en démarche Zero Trust » ne signifie rien de mesurable. Ne l'acceptez jamais comme réponse à un constat.

MITRE ATT&CK

ATT&CK décrit les techniques employées par les attaquants, y compris pour les environnements d'identité et les services de type logiciel en tant que service. Ce n'est ni un référentiel de configuration ni un modèle d'architecture : c'est une grille de couverture pour la détection.

Son emploi en audit est précis et limité, ce qui fait sa valeur : confronter la liste des techniques applicables à votre environnement à la liste de vos règles de détection effectives, et produire une carte des zones aveugles. C'est le seul des quatre corpus qui répond à la question « que verrions-nous si cela se produisait ? ». Le chapitre 21 s'appuie directement dessus.

Le cas particulier du score natif

Le score de sécurité fourni par la plateforme est utile comme indicateur de tendance et inutile comme mesure d'exposition. Trois raisons.

Il attribue des points pour des mesures dont l'impact réel varie considérablement, sans pondération par le risque de votre organisation. Il inclut des recommandations liées à des produits que vous ne possédez pas, ce qui plafonne mécaniquement le score et rend la comparaison entre organisations dénuée de sens. Il valorise l'activation d'une capacité davantage que la qualité de son application.

Un score de soixante-quinze pour cent ne signifie donc pas que trois quarts du risque sont couverts. Il peut parfaitement coexister avec un chemin d'attaque complet et non traité. Utilisez-le pour suivre une évolution dans le temps ; ne l'utilisez jamais comme conclusion d'audit, et surtout pas devant un comité de direction, où il produira un faux sentiment de maîtrise très difficile à corriger ensuite.

Comment les combiner

La combinaison qui fonctionne en mission tient en quatre lignes.

Le CIS sert d'instrument de mesure : il fournit le constat contrôle par contrôle. Zero Trust sert de modèle cible : il donne la cohérence et la trajectoire. ATT&CK sert de grille de détection : il révèle les angles morts. Les publications de l'ANSSI et les textes

réglementaires servent de cadre d'opposabilité : ils justifient l'exigence auprès de la direction générale et des tiers.

Ce qu'il ne faut pas faire : additionner les quatre en un tableau unique de plusieurs centaines de lignes. Le lecteur abandonne, et l'audit perd sa fonction de hiérarchisation.

Ce que vous devez décider

- **Quel référentiel fait foi en cas de désaccord ?** Nommez-en un, une fois pour toutes. Sans arbitre désigné, chaque constat se rediscute avec l'équipe technique.
- **Visez-vous le niveau 1 ou le niveau 2 du benchmark ?** Le niveau 2 suppose d'accepter un impact utilisateur. C'est une décision de direction, pas un choix technique.
- **Le score natif est-il un indicateur de pilotage officiel dans votre organisation ?** Si oui, encadrez immédiatement son interprétation, avant qu'il ne serve de preuve de maîtrise en comité.
- **Votre couverture de détection est-elle évaluée, ou seulement votre configuration ?** La plupart des audits s'arrêtent à la seconde et laissent la première entièrement inconnue.

CHAPITRE 7

Collecter la preuve : sources de données, fiabilité, pièges

Un constat d'audit vaut ce que vaut sa preuve. Ce chapitre traite de la collecte : d'où viennent les données, ce qu'elles disent réellement, et les pièges qui produisent des conclusions fausses avec une apparence de rigueur.

Le principe : extraction datée, reproductible, indépendante

Une preuve d'audit doit satisfaire trois conditions. Elle est datée : la configuration d'un tenant change quotidiennement, un constat sans horodatage n'est pas opposable. Elle est reproductible : un tiers doit pouvoir rejouer l'extraction et obtenir le même résultat. Elle est indépendante du déclaratif : elle provient d'une lecture de l'état réel, non d'une réponse d'entretien.

Cette exigence paraît évidente. En pratique, une part importante des rapports d'audit que je relis en seconde lecture repose sur des captures d'écran non datées et sur des affirmations d'équipes, ce qui les rend inutilisables dès la première contestation.

Les sources

L'interface d'administration convient à la vérification ponctuelle et à l'illustration, jamais à la collecte de masse : elle est lente, non reproductible et ne restitue qu'une vue partielle des objets.

L'interface de programmation de l'annuaire — l'API Microsoft Graph — est la source de référence. Elle expose les objets tels qu'ils existent réellement, y compris des propriétés que les portails n'affichent pas. C'est la seule source qui permette une collecte exhaustive et rejouable.

Les modules d'administration en ligne de commande couvrent les charges de travail de collaboration, dont certaines configurations restent inaccessibles autrement, notamment côté messagerie.

Les journaux d'authentification, d'audit d'annuaire et d'activité de collaboration constituent la quatrième source. Ils ne servent pas à établir la configuration, mais à mesurer l'usage réel — distinction essentielle sur laquelle repose la section suivante.

Le piège numéro un : confondre capacité et application

C'est l'erreur qui invalide le plus grand nombre de rapports.

Une stratégie d'accès conditionnel peut exister, être correctement rédigée, et ne s'appliquer à personne : parce qu'elle cible un groupe vide, parce qu'elle est en mode rapport seul, parce que ses exclusions couvrent la population entière, ou parce qu'une seconde stratégie moins restrictive produit le même accès par un autre chemin.

De même, une méthode d'authentification forte peut être *enregistrée* par un utilisateur sans être *exigée* pour son accès. Un tenant où quatre-vingt-quinze pour cent des

utilisateurs ont enregistré une méthode forte, mais où aucune stratégie ne l'impose, est un tenant sans authentification forte.

La règle de collecte est donc : ne jamais conclure sur la seule lecture de la configuration. Confrontez systématiquement la configuration aux journaux d'authentification réels. La question à laquelle vous devez répondre n'est pas « la règle existe-t-elle ? » mais « combien d'accès ont-ils eu lieu sans elle sur les trente derniers jours ? ». Ce chiffre change la conversation avec l'équipe technique, parce qu'il n'est pas discutable.

Les autres pièges classiques

Les permissions insuffisantes produisent des faux négatifs silencieux. Une extraction menée avec un rôle de lecture incomplet renvoie une liste vide plutôt qu'une erreur. Vérifiez toujours qu'un jeu de contrôle connu remonte bien avant de conclure à l'absence d'un objet.

La pagination tronque. Les interfaces de programmation renvoient des résultats par lots. Une collecte qui ignore la pagination produit un inventaire partiel, et l'objet à risque se trouve statistiquement autant dans le second lot que dans le premier.

Certaines propriétés ne sont pas retournées par défaut. Les dates de dernière connexion, les propriétés d'extension et certains attributs de sécurité doivent être demandés explicitement. Leur absence dans une extraction ne signifie pas leur absence dans l'annuaire.

Les états de compte se ressemblent. Un compte désactivé, un compte sans licence, un compte bloqué à la connexion et un compte supprimé en corbeille ne présentent pas le même risque. Les confondre gonfle artificiellement les constats et décrédibilise le rapport dès la première relecture technique.

Les mécanismes hérités se superposent. Une authentification forte peut être imposée par une configuration ancienne par utilisateur, par les valeurs par défaut de sécurité, ou par une stratégie d'accès conditionnel. Ces mécanismes coexistent, s'excluent parfois, et leur cumul crée des angles morts. Établissez lequel est réellement en vigueur avant tout constat sur ce sujet.

Les objets synchronisés ne se corrigent pas là où on les observe. Un attribut incohérent constaté dans le cloud provient souvent de l'annuaire local. Le constat est valide, la recommandation doit viser la bonne source.

Données personnelles et conservation des preuves

Une collecte d'audit ramène des données personnelles : identités, adresses, journaux d'authentification, adresses réseau, parfois données de localisation. Trois règles suffisent.

Extraire le strict nécessaire : les identifiants et attributs utiles au constat, jamais le contenu des boîtes aux lettres ou des fichiers. Stocker les extractions dans un espace maîtrisé, chiffré, avec une durée de conservation définie à l'avance et alignée sur la durée de contestation possible du rapport. Documenter cette conservation dans la lettre de mission — c'est aussi ce que vous demanderez à vos propres prestataires.

Ce que vous devez décider

- **Vos constats reposent-ils sur des extractions ou sur des entretiens ?** Exigez la preuve datée pour chaque constat du rapport que l'on vous remet, y compris de la part d'un cabinet réputé.
- **Mesurez-vous l'usage ou seulement la configuration ?** Sans confrontation aux journaux, votre audit décrit une intention, pas une réalité.
- **Où sont stockées les extractions et pendant combien de temps ?** C'est une question de sécurité et de protection des données ; elle doit être tranchée avant la collecte, jamais après.
- **Vos audits sont-ils rejouables à l'identique ?** Un audit non reproductible ne permet pas de mesurer un progrès, et le chapitre 26 en dépend entièrement.

CHAPITRE 8

Les vingt contrôles qui révèlent quatre-vingts pour cent du risque

Un benchmark complet compte plusieurs centaines de points de contrôle. Cette liste en retient vingt. Ce ne sont pas les vingt plus importants dans l'absolu : ce sont ceux dont la vérification, en début de mission, discrimine le plus efficacement un tenant tenu d'un tenant exposé. En pratique, elle permet d'établir un premier diagnostic en une journée.

Chacun se formule comme une question à laquelle une extraction répond par un fait, jamais par une appréciation.

Privilèges

- 1. Combien de comptes détiennent le rôle d'administrateur général, et depuis quand ?** Au-delà de cinq dans une organisation de taille moyenne, la valeur informative du rôle disparaît. Vérifiez également les attributions permanentes par rapport aux attributions éligibles.
- 2. Ces comptes sont-ils dédiés à l'administration ?** Un compte à privilèges qui reçoit du courrier, navigue sur internet et ouvre des documents mutualise le risque de la bureautique et celui de l'administration.
- 3. Existe-t-il des comptes d'accès d'urgence, et ont-ils été testés ?** Deux comptes, exclusivement dans le cloud, avec une authentification forte, surveillés, et une procédure de test datée de moins d'un an.
- 4. L'élévation de privilèges est-elle temporaire ?** L'attribution permanente d'un rôle sensible transforme chaque compromission d'un poste d'administrateur en compromission du tenant.
- 5. Qui peut modifier l'appartenance des groupes utilisés pour attribuer des rôles ?** C'est le chemin d'élévation le plus souvent oublié dans les audits.

Authentification

- 6. Quelle proportion des authentifications réussies des trente derniers jours a mis en œuvre une méthode forte ?** La question porte sur les authentifications, pas sur les enregistrements de méthode.
- 7. Les administrateurs utilisent-ils une méthode résistante à l'hameçonnage ?** Une authentification forte par notification ou par code reste contournable par relais. Pour les rôles sensibles, elle ne constitue pas une réponse suffisante.
- 8. Les protocoles d'authentification hérités sont-ils encore utilisés, et par qui ?** Le constat ne se fait pas sur la configuration mais sur les journaux : le protocole peut être bloqué en théorie et rester actif pour une population dérogatoire.
- 9. Quelle est la procédure de réinitialisation d'une méthode d'authentification au support ?** Contrôle organisationnel, mais il plafonne l'efficacité des huit précédents.

Accès conditionnel

10. Combien de stratégies sont actives, et combien en mode rapport seul depuis plus de trois mois ? Une stratégie en mode rapport depuis un an est une intention, pas un contrôle.

11. Qui est exclu, de quelles stratégies, et depuis quand ? Consolidez toutes les exclusions en une seule liste : c'est le document le plus révélateur d'un audit, et il n'existe dans aucun portail.

12. Existe-t-il une stratégie de repli bloquant les accès non explicitement autorisés ? Sans elle, l'ensemble du dispositif fonctionne en liste d'exceptions plutôt qu'en liste d'autorisations.

Applications et identités non humaines

13. Les utilisateurs peuvent-ils consentir librement à des applications tierces ? Réglage unique, effet majeur, coût de correction quasi nul.

14. Quelles applications détiennent des permissions d'application de portée large sur la messagerie, les fichiers ou l'annuaire ? Cette liste est courte et doit être justifiable ligne par ligne.

15. Combien de secrets applicatifs expirent dans moins de quatre-vingt-dix jours, et combien ont une durée de validité supérieure à deux ans ? Les secrets longs signalent l'absence de gestion du cycle de vie applicatif.

Collaboration externe

16. Combien de comptes invités n'ont aucune authentification depuis quatre-vingt-dix jours ? Le rapport entre invités actifs et invités inactifs est un indicateur direct de la qualité de la gouvernance.

17. Le partage par lien anonyme est-il autorisé, et sur quels sites ? À croiser avec la classification des données lorsqu'elle existe.

Données, appareils, journalisation

18. Les accès aux ressources sensibles exigent-ils un appareil conforme ou joint ? C'est le contrôle qui limite l'exploitabilité d'un jeton volé, donc celui qui traite le chemin d'attaque le plus fréquent.

19. Quelle est la durée de conservation effective des journaux d'authentification et d'audit, et sont-ils exportés hors de la plateforme ? Comparez cette durée à votre délai de détection réaliste, pas à une valeur théorique.

20. Les composants de synchronisation avec l'annuaire local sont-ils administrés comme des systèmes de niveau zéro ? Un seul de ces serveurs mal cloisonné annule l'ensemble des dix-neuf contrôles précédents.

Comment s'en servir

Ces vingt questions ne remplacent pas un audit complet ; elles le préparent. Posez-les en début de mission, et la répartition des réponses vous indiquera où porter l'effort d'analyse détaillée. Elles constituent également une excellente grille d'entrée pour évaluer un

tenant que vous héritez — après une acquisition, un changement de prestataire ou une prise de poste.

Ce que vous devez décider

- **Ces vingt réponses existent-elles aujourd’hui dans votre organisation ?** Si obtenir la liste consolidée des exclusions demande trois semaines, c’est déjà un constat en soi.
- **À quelle fréquence les recalculez-vous ?** Une mesure annuelle ne dit rien de l’état du tenant le reste de l’année ; le chapitre 26 traite du contrôle continu.
- **Acceptez-vous de publier ces chiffres à votre direction ?** Les indicateurs qui ne remontent pas ne financent aucune correction.

CHAPITRE 9

Noter et prioriser : criticité, effort, impact utilisateur

Une liste d'écarts n'est pas un plan d'action. La priorisation est la partie du travail qui transforme un constat en décision, et c'est aussi celle que la plupart des rapports traitent le plus mal, en se contentant d'une note de gravité héritée du référentiel.

Pourquoi la note unique ne suffit pas

Une criticité seule ne permet pas d'arbitrer, car elle ignore ce qui bloque réellement les corrections. En mission, les mesures qui ne sont pas appliquées ne sont presque jamais celles que l'on ignore : ce sont celles dont l'organisation redoute l'effet. Une priorisation qui ne modélise pas ce frein produit un plan que l'exploitation refusera poliment et n'exécutera jamais.

Trois axes suffisent, et il faut les tenir séparés.

Axe 1 — La criticité

Elle se compose de deux facteurs : la probabilité d'exploitation et l'impact en cas d'exploitation. Une échelle à quatre niveaux suffit, à condition d'ancrer chaque niveau sur un fait observable et non sur une impression.

Le niveau le plus élevé se réserve à ce qui ouvre un chemin complet vers la compromission du tenant : un rôle d'administrateur général sans authentification résistante à l'hameçonnage, une identité applicative disposant d'un accès étendu à la messagerie, un serveur de synchronisation non cloisonné.

Le niveau immédiatement inférieur couvre ce qui facilite fortement une attaque sans la réaliser seul : protocoles hérités actifs, consentement applicatif libre, absence d'exigence d'appareil.

Ancrez la cotation sur les sept chemins du chapitre 3. Un écart qui n'appartient à aucun de ces chemins ne peut pas être coté au niveau maximal, quelle que soit la note que lui attribue le référentiel.

Axe 2 — L'effort

L'effort n'est pas seulement technique. Il additionne trois composantes : la charge de mise en œuvre, la charge de validation et de test, et la charge de coordination organisationnelle. Cette dernière est presque toujours la plus lourde et presque toujours absente des estimations.

Retirer le consentement applicatif libre demande une minute de configuration et trois semaines de préparation d'un circuit d'approbation avec le support. Coter cette mesure comme un effort faible garantit un plan d'action en retard dès le premier mois.

Axe 3 — L'impact utilisateur

C'est l'axe déterminant, et celui que les rapports omettent le plus souvent. Il mesure ce que la mesure change pour les personnes : une action supplémentaire à l'authentification, un

appareil personnel qui cesse de fonctionner, un partage externe qui doit passer par une demande.

Une mesure à impact utilisateur élevé n'est pas une mauvaise mesure. Mais elle exige un arbitrage explicite au niveau approprié, une communication préparée et souvent un déploiement progressif par population. La traiter comme une mesure technique parmi d'autres est la cause la plus fréquente d'échec de déploiement, et de retour arrière — le retour arrière étant plus coûteux que l'absence de déploiement, parce qu'il discrédite le programme entier.

La matrice de décision

Croisez criticité et effort, en utilisant l'impact utilisateur comme critère de séquençement plutôt que de sélection.

Criticité élevée et effort faible : traitement immédiat, sans passer par un comité. Ce sont les gains rapides, et ils financent la crédibilité du reste du plan.

Criticité élevée et effort important : ce sont les chantiers. Ils demandent un budget, un responsable et un jalon. Leur nombre doit rester limité — trois par an au maximum dans une organisation moyenne.

Criticité faible et effort faible : à traiter en lot, dans une campagne d'hygiène trimestrielle, sans en faire un sujet de comité.

Criticité faible et effort important : à documenter comme risque accepté, avec une date de réexamen. C'est une décision légitime, à condition d'être écrite.

Séquencer en vagues

Trois vagues fonctionnent mieux qu'un calendrier détaillé, qui se périmé en deux mois.

À trente jours, les mesures sans impact utilisateur et sans dépendance : elles démontrent l'exécution.

À quatre-vingt-dix jours, les mesures à impact limité et à préparation courte, notamment sur les populations à privilèges, qui sont peu nombreuses et donc rapides à traiter.

À cent quatre-vingts jours, les chantiers structurants : appareils, authentification résistante à l'hameçonnage sur l'ensemble de la population, gouvernance applicative.

Cette séquence a une propriété utile : elle place les mesures les plus sensibles après une période où l'équipe a déjà livré, ce qui rend l'arbitrage plus facile à obtenir.

Ce que vous devez décider

- **Votre échelle de criticité est-elle ancrée sur des chemins d'attaque ou sur une note héritée d'un référentiel ?** Sans ancrage, la priorisation est arbitraire et se rediscutera à chaque comité.
- **Qui arbitre les mesures à impact utilisateur élevé ?** Si la réponse est « l'équipe technique », l'arbitrage n'aura pas lieu et la mesure ne sera pas déployée.
- **Combien de chantiers structurants votre organisation peut-elle réellement absorber cette année ?** Répondre trois plutôt que dix est un acte de pilotage, pas un renoncement.

- **Les risques acceptés sont-ils écrits, datés et attribués ?** Un risque accepté sans nom ni date n'est pas un arbitrage, c'est un oubli.

CHAPITRE 10

Rédiger un rapport que le comité de direction lit vraiment

Un rapport d'audit a une seule fonction : provoquer des décisions. Un document exact, exhaustif et sans effet n'est pas un bon rapport ; c'est un travail perdu. Ce chapitre décrit la structure qui, en pratique, obtient l'arbitrage.

Ce que le lecteur cherche

Le décideur qui ouvre votre rapport se pose trois questions, dans cet ordre : sommes-nous en danger, à quel point, et que dois-je décider aujourd'hui. Il ne cherche pas la liste des écarts. S'il ne trouve pas ces réponses dans les deux premières pages, il déléguera la lecture, et l'arbitrage n'aura pas lieu.

Cela conduit à une règle simple : la synthèse n'est pas un résumé du rapport, c'est le rapport. Le reste est de la justification.

La structure en cinq blocs

Le verdict, une page. Une phrase de conclusion sur le niveau d'exposition, trois faits qui la soutiennent, une échéance. Le verdict s'exprime en exposition et non en conformité : « un compte d'administrateur compromis permettrait aujourd'hui d'accéder à l'ensemble des boîtes aux lettres sans détection » est un verdict. « Quarante-sept contrôles CIS sont en écart » n'en est pas un.

Les scénarios, deux pages. Trois scénarios au maximum, tirés des chemins du chapitre 3 et instanciés sur votre environnement, avec les faits d'audit qui les rendent plausibles. C'est la partie qui fait comprendre le risque, parce qu'elle raconte une séquence plutôt qu'un état.

Le plan par vagues, une à deux pages. Les trois vagues du chapitre 9, avec pour chaque action un responsable pressenti, un effort estimé et le risque couvert. Pas de dates au jour près.

Les décisions demandées, une page. C'est le bloc le plus souvent absent, et c'est celui qui transforme le rapport en réunion utile. Trois à cinq décisions, formulées de manière à pouvoir recevoir un oui ou un non : accepter tel impact utilisateur, financer telle évolution de licence, désigner tel propriétaire, accepter formellement tel risque résiduel.

L'annexe technique, sans limite de taille. Constats détaillés, preuves, extractions, références au référentiel. Elle sert à l'équipe technique et à l'opposabilité. Personne d'autre ne la lira, et ce n'est pas un problème.

Ce qu'il faut éviter

Le score unique en couverture. Il sera retenu, cité hors contexte, et deviendra l'objectif à la place du risque.

Les captures d'écran de portails. Elles vieillissent en quelques semaines, ne prouvent rien sans horodatage et gonflent le document.

Le jargon non traduit. Une direction générale n'a pas à connaître le vocabulaire technique du fournisseur. Écrire « une application autorisée par un utilisateur peut lire toutes les boîtes aux lettres » plutôt que la formulation technique équivalente n'est pas de la vulgarisation : c'est la condition pour que la décision soit prise.

Les recommandations non chiffrées. Une recommandation sans effort estimé ne peut pas être arbitrée et sera reportée.

Le catalogue exhaustif en corps de rapport. Deux cents lignes de constats produisent de la paralysie, jamais de l'action.

La restitution

Prévoyez deux réunions distinctes, jamais une seule.

La revue technique, avec les équipes concernées, avant la restitution de direction. Elle sert à corriger les erreurs factuelles — il y en a toujours — et à obtenir l'adhésion sur les efforts estimés. Un constat contesté en séance devant la direction générale détruit la crédibilité du rapport entier, même si vous avez raison.

La restitution de direction, courte, centrée sur le verdict, les scénarios et les décisions demandées. Une heure suffit si le document est bien construit. Terminez par les décisions, pas par les remerciements : la réunion doit produire des noms et des engagements, consignés par écrit dans les vingt-quatre heures.

La suite

Un rapport sans mécanisme de suivi retourne à l'état de document en six semaines. Fixez dès la restitution la date du point d'avancement, le format de suivi des trois vagues, et l'indicateur qui sera présenté au comité suivant. Le chapitre 26 traite du dispositif de pilotage durable ; il commence ici.

Ce que vous devez décider

- **Votre rapport contient-il une page de décisions ?** Sans elle, vous obtiendrez des remarques, pas des arbitrages.
- **Le verdict est-il exprimé en exposition ou en conformité ?** La seconde formulation obtient de la conformité ; la première obtient du budget.
- **Qui valide les faits avant la restitution de direction ?** Sauter cette étape est le meilleur moyen de perdre un audit techniquement irréprochable.
- **Quelle est la date du premier point d'avancement ?** Fixez-la dans la réunion de restitution, ou elle ne sera jamais fixée.

PARTIE III

Corriger : les chantiers prioritaires

CHAPITRE 11

Comptes à privilèges : rôles, élévation temporaire, accès d'urgence

Si votre programme ne devait comporter qu'un seul chantier, ce serait celui-ci. Les comptes à privilèges concentrent le rapport effort-bénéfice le plus favorable de tout l'écosystème : la population est petite, les mesures sont connues, et l'impact utilisateur reste circonscrit à des personnes qui comprennent pourquoi on le leur impose.

Réduire avant de protéger

Le réflexe habituel consiste à renforcer la protection des comptes existants. L'ordre correct est inverse : réduire d'abord, protéger ensuite. Protéger vingt comptes d'administrateur général coûte plus cher et fonctionne moins bien que d'en ramener le nombre à quatre.

La réduction se conduit en trois passes. La première élimine les attributions historiques, celles dont plus personne ne connaît la justification. La deuxième remplace le rôle le plus large par un rôle spécialisé : la majorité des tâches d'administration quotidiennes ne demandent pas le rôle d'administrateur général mais un rôle de portée limitée. La troisième restreint la portée elle-même, par unité administrative, pour les administrateurs dont le périmètre correspond à une entité, un pays ou une filiale.

L'objectif de sortie est un chiffre, et il doit figurer dans votre feuille de route : moins de cinq attributions permanentes du rôle le plus élevé, quelle que soit la taille de l'organisation.

Séparer l'identité d'administration de l'identité bureautique

Un compte à privilèges ne doit pas recevoir de courrier, ne doit pas naviguer, ne doit pas ouvrir de documents. La règle est ancienne, elle est valable dans l'annuaire local depuis vingt ans, et elle s'applique identiquement dans le cloud : elle interdit qu'un document piégé ou un lien d'hameçonnage ouvre directement une session à privilèges.

En pratique, cela signifie un compte distinct, sans licence de messagerie, avec un identifiant qui ne suit pas le format d'adresse de l'entreprise — car un format prévisible facilite l'énumération et la pulvérisation de mots de passe.

L'objection est toujours la même : le confort. Elle est recevable pour les administrateurs occasionnels, et c'est précisément à quoi sert l'élévation temporaire.

L'élévation temporaire

Une attribution permanente signifie que le privilège existe vingt-quatre heures sur vingt-quatre, y compris pendant que l'administrateur consulte ses courriels. Une attribution éligible, activée à la demande pour une durée limitée, avec justification et validation, réduit la fenêtre d'exploitation dans des proportions considérables.

Trois réglages font la différence entre un dispositif réel et un dispositif de façade : l'activation exige une authentification forte au moment de l'élévation, et non le simple

rejeu de la session ouverte le matin ; la durée d'activation est courte, deux à quatre heures ; les activations des rôles les plus sensibles déclenchent une notification et, pour certains, une approbation par un tiers.

Le piège classique : configurer l'élévation temporaire tout en conservant des attributions permanentes « pour les urgences ». Ces attributions résiduelles annulent le bénéfice, car un attaquant visera précisément celles-là. La bonne réponse aux urgences n'est pas une attribution permanente, ce sont les comptes d'accès d'urgence.

Les comptes d'accès d'urgence

Deux comptes, exclusivement dans le cloud, jamais synchronisés, avec un identifiant sur un domaine dédié, protégés par une authentification forte matérielle, exclus des stratégies susceptibles de les bloquer en cas de panne du dispositif d'authentification, et surveillés : toute authentification de ces comptes doit produire une alerte immédiate vers l'équipe sécurité.

Les deux erreurs à éviter : les exclure de tout contrôle sans les surveiller — ils deviennent alors la meilleure cible du tenant — et ne jamais les tester. Une procédure de test semestrielle, avec compte rendu daté, fait partie du contrôle. Un compte d'urgence non testé n'est pas un compte d'urgence.

Les postes d'administration

C'est la mesure la plus efficace et la moins appliquée. Tant que l'administration s'effectue depuis le poste bureautique ordinaire, la sécurité du tenant est plafonnée par celle de ce poste : un code malveillant qui y réside verra passer les sessions à privilèges.

Le principe de cloisonnement issu des guides de sécurisation d'annuaire s'applique sans transposition : les tâches d'administration du tenant s'exécutent depuis un poste dédié, durci, sans messagerie ni navigation générale, administré séparément. Ce poste appartient au niveau de sensibilité le plus élevé, au même titre que les serveurs de synchronisation.

C'est un chantier à impact organisationnel réel, à placer en troisième vague, mais il doit y figurer. Une organisation qui applique toutes les mesures des sections précédentes en administrant depuis un poste bureautique conserve un chemin de compromission complet.

Le support et la réinitialisation

Dernier maillon, souvent hors du périmètre technique et pourtant décisif. Si une méthode d'authentification peut être réinitialisée sur simple appel, l'ensemble du dispositif se contourne par téléphone. Trois mesures suffisent : une vérification d'identité qui ne repose pas sur des informations publiques ou devinables, une traçabilité de chaque réinitialisation, et une procédure distincte et renforcée pour les comptes à privilèges, avec validation par un second intervenant.

Ce que vous devez décider

- **Quel est votre objectif chiffré d'attributions permanentes du rôle le plus élevé ?** Sans cible écrite, la réduction ne se fera pas.

- **Acceptez-vous des comptes d'administration distincts pour vos équipes ?** C'est un arbitrage de confort contre risque, et il vous revient, pas à l'exploitation.
- **Les postes d'administration dédiés entrent-ils dans la feuille de route de l'année ?** Sinon, écrivez explicitement le risque résiduel : il annule une partie du bénéfice des autres mesures.
- **La procédure de réinitialisation au support est-elle renforcée pour les comptes à privilèges ?** C'est le contournement le plus employé et le moins coûteux pour un attaquant.

CHAPITRE 12

Authentification résistante à l'hameçonnage et fin des protocoles hérités

Ce chapitre traite de deux chantiers distincts que l'on mène en parallèle parce qu'ils se conditionnent : élever le niveau des méthodes d'authentification, et supprimer les chemins qui permettent de s'en dispenser.

La hiérarchie des méthodes

Toutes les méthodes d'authentification forte ne se valent pas, et l'écart entre elles est plus important que l'écart entre mot de passe seul et authentification forte.

Les codes envoyés par message texte constituent le niveau le plus faible : interception par détournement de numéro, transmission par un réseau qui n'est pas sous votre contrôle. Ils restent préférables à l'absence de méthode, et rien de plus.

Les notifications d'approbation et les codes générés par application représentent le niveau intermédiaire. Ils résistent au vol de mot de passe mais pas au relais en temps réel : la victime approuve, l'attaquant récupère la session. La correspondance de numéro et l'affichage du contexte réduisent l'approbation par lassitude, sans traiter le relais.

Les méthodes résistantes à l'hameçonnage — clés de sécurité, authentification par certificat, authentification liée à la plateforme du poste — constituent le seul niveau qui traite réellement le chemin d'attaque numéro un du chapitre 3, parce que la preuve produite est liée à l'origine du site et ne peut être rejouée ailleurs.

La séquence de déploiement

Le déploiement intégral et simultané échoue presque toujours. La séquence qui fonctionne procède par population, du plus sensible au plus large.

D'abord les rôles à privilèges : population réduite, motivation élevée, aucun argument de coût recevable. Elle doit être traitée en quatre-vingt-dix jours.

Ensuite les populations exposées : direction générale, finance, ressources humaines, assistantat de direction — les cibles réelles de la fraude au virement et de l'espionnage.

Enfin le reste de l'organisation, sur un calendrier annuel, avec une phase de coexistence pendant laquelle les anciennes méthodes restent acceptées pour les usages non sensibles.

Trois conditions déterminent le succès : disposer d'une méthode de secours pour les cas de perte ou d'oubli, avoir traité la procédure de réinitialisation au support avant le déploiement, et fournir un accompagnement pour les populations sans smartphone professionnel — c'est le point de blocage social le plus fréquent, et il se traite par la clé de sécurité matérielle.

La question du mot de passe

Une fois une méthode résistante à l'hameçonnage déployée, le mot de passe cesse d'être le facteur déterminant. Deux conséquences pratiques.

Les politiques de complexité et d'expiration périodique produisent aujourd'hui plus de réutilisation et de notes autocollantes que de sécurité. La position recommandée par les principaux organismes normatifs converge : allonger, interdire les mots de passe compromis connus, et cesser l'expiration systématique sans indice de compromission.

L'objectif de moyen terme est la suppression du mot de passe comme facteur d'authentification pour les populations équipées. Ce n'est plus une position d'avant-garde, c'est la trajectoire par défaut de la plateforme.

Les protocoles hérités

Un protocole d'authentification ancien ne sait pas présenter de second facteur. Tant qu'il reste accepté, il constitue un contournement complet de votre politique d'authentification, quel que soit le soin apporté aux stratégies d'accès.

Le blocage se heurte toujours aux mêmes usages : imprimantes multifonctions qui envoient des courriels, applications métier anciennes, scripts de supervision, quelques clients de messagerie non maintenus. La démarche efficace consiste à travailler à partir des journaux : identifier ce qui utilise réellement ces protocoles sur trente jours, traiter chaque cas nominativement, puis bloquer.

Une fois bloqué, le protocole doit rester bloqué. Chaque dérogation accordée « le temps de migrer l'application » doit porter une date de fin réelle, sans quoi elle deviendra permanente — c'est le mécanisme par lequel des organisations ayant officiellement supprimé l'authentification héritée la conservent pour une population de quelques dizaines de comptes, dont plusieurs à privilèges.

Ne pas oublier le second chemin

Bloquer les protocoles hérités et exiger une méthode forte ne suffit pas si un flux d'authentification alternatif reste ouvert, ou si une application ancienne dispose d'une exclusion. Le contrôle final consiste à vérifier, dans les journaux, qu'aucune authentification réussie des trente derniers jours n'a échappé au dispositif. Cette vérification est le seul constat qui vaille ; le reste est une intention de configuration.

Ce que vous devez décider

- **Quelle population passe à une méthode résistante à l'hameçonnage cette année ?** Les administrateurs au minimum, et la décision se prend maintenant, pas après l'incident.
- **Financez-vous des clés matérielles ?** C'est la réponse aux populations sans téléphone professionnel et le blocage social le plus courant du projet.
- **Maintenez-vous encore l'expiration périodique des mots de passe ?** Si oui, l'arbitrage vous appartient : cette pratique dégrade la sécurité et coûte du support.
- **Quelle est la date de fin réelle des dernières dérogations aux protocoles hérités ?** Sans date, elles sont permanentes.

CHAPITRE 13

Accès conditionnel : un jeu de règles maintenable et testable

L'accès conditionnel est le point de décision central de l'architecture. C'est aussi le composant qui se dégrade le plus vite : les stratégies s'accumulent, les exclusions se sédimentent, et personne n'ose plus modifier un ensemble que plus personne ne comprend. Ce chapitre vise moins la sophistication que la maintenabilité.

Le principe directeur

Un jeu de stratégies doit être lisible par une personne qui ne l'a pas écrit, en moins d'une heure. Cette contrainte, apparemment esthétique, est en réalité le premier contrôle de sécurité : un ensemble illisible n'est jamais audité, jamais testé, et finit par autoriser ce qu'il croit interdire.

Il en découle une structure recommandée : peu de stratégies, chacune avec un objectif unique, nommées selon une convention explicite qui indique la population ciblée, la condition et l'effet.

L'architecture minimale

Six stratégies couvrent l'essentiel des besoins d'une organisation moyenne.

Une stratégie de blocage des protocoles et flux d'authentification non nécessaires. Une stratégie imposant une méthode résistante à l'hameçonnage aux rôles à privilèges. Une stratégie imposant une authentification forte à l'ensemble des utilisateurs. Une stratégie exigeant un appareil conforme ou joint pour l'accès aux ressources sensibles. Une stratégie encadrant les accès des comptes invités. Une stratégie de blocage par défaut de ce qui n'est pas explicitement autorisé.

Cette dernière est la plus importante et la plus souvent absente. Sans elle, le dispositif fonctionne en liste d'interdictions : tout ce qui n'a pas été prévu est autorisé. Avec elle, il fonctionne en liste d'autorisations, ce qui est la seule posture défendable.

Les exclusions

Les exclusions sont le point de défaillance systématique. Elles s'ajoutent une par une, chacune justifiée sur le moment, et personne ne dispose jamais de la vue consolidée.

Trois règles suffisent à contenir la dérive. Toute exclusion porte un nom de responsable et une date de fin, sans exception, y compris pour les comptes d'accès d'urgence — dont la date de fin est simplement la prochaine revue. Toute exclusion est portée par un groupe dédié et nommé explicitement, jamais par un compte inscrit en dur dans la stratégie, afin que la liste consolidée puisse être extraite. Enfin, la liste consolidée des exclusions est revue trimestriellement, en réunion, par le responsable sécurité.

Ce dernier point paraît bureaucratique. Il est en pratique le contrôle qui fait la différence entre un dispositif tenu et un dispositif qui s'érode.

Tester avant d'appliquer

Toute modification passe par le mode rapport seul, sur une durée définie, avec analyse des accès qui auraient été bloqués. Ce mode est une étape, pas un état : une stratégie qui y demeure plus de quelques semaines doit être appliquée ou supprimée.

Les outils de simulation permettent de vérifier l'effet d'une stratégie sur un utilisateur et un contexte donnés avant application. Leur usage doit être systématique pour toute modification touchant une population large, et il doit être documenté dans le dossier de changement.

Ce qui casse la production

Trois erreurs provoquent l'essentiel des incidents d'accès en production.

Le verrouillage complet : une stratégie appliquée à tous les utilisateurs, y compris aux comptes d'urgence, avec une condition impossible à satisfaire. C'est précisément le scénario que les comptes d'accès d'urgence traitent, à condition qu'ils aient été exclus et testés.

L'oubli des identités non humaines : les comptes de service et principaux applicatifs ne peuvent pas satisfaire une exigence d'authentification forte. Les inclure dans une stratégie généraliste interrompt des chaînes techniques, souvent la nuit. Ils doivent être traités par des stratégies dédiées, comme indiqué au chapitre 15.

La superposition non maîtrisée : deux stratégies se recouvrent, la plus restrictive s'applique, et l'effet observé ne correspond à aucune des deux intentions. C'est l'argument principal en faveur d'un nombre réduit de stratégies bien nommées.

La documentation

Chaque stratégie doit être accompagnée de trois lignes : ce qu'elle protège, pourquoi elle existe, et qui l'a validée. Cette documentation tient dans un tableau et se maintient en quelques minutes par modification. Son absence est le meilleur prédicteur d'une dégradation à dix-huit mois, lorsque l'équipe aura changé.

Ce que vous devez décider

- **Existe-t-il une stratégie de blocage par défaut ?** Si non, votre politique d'accès fonctionne en liste d'exceptions, et l'exhaustivité y est impossible.
- **Qui revoit la liste consolidée des exclusions, et à quelle fréquence ?** Nommez la personne et la fréquence, ou la liste ne sera jamais revue.
- **Le mode rapport seul est-il une étape ou un refuge ?** Fixez une durée maximale et tenez-la.
- **Combien de stratégies votre organisation peut-elle réellement maintenir ?** Répondre six et s'y tenir vaut mieux que trente stratégies que personne ne relit.

CHAPITRE 14

Applications et consentements : l'angle mort

Il n'existe pas de sujet où l'écart entre le risque réel et l'attention portée soit aussi grand. Dans la majorité des tenants audités, personne ne sait combien d'applications tierces disposent d'un accès aux données de l'entreprise, ni qui le leur a accordé.

Le mécanisme

Une application tierce demande des permissions ; un utilisateur ou un administrateur les accorde ; l'application obtient un accès durable, exercé au moyen de ses propres jetons. Trois propriétés rendent ce mécanisme dangereux.

L'accès survit au changement de mot de passe et à la révocation des sessions de l'utilisateur : seule la révocation du consentement le supprime.

Il ne produit pas d'événement d'authentification identifiable comme suspect, puisque l'application s'authentifie légitimement.

Enfin, l'utilisateur qui accorde le consentement ne mesure pas la portée de ce qu'il accorde. Un écran demandant l'autorisation de « lire vos courriels » est accepté sans réflexion dans un contexte professionnel courant.

La distinction qui décide de tout

Les permissions déléguées s'exercent au nom d'un utilisateur connecté : l'application ne peut atteindre que ce que cet utilisateur peut atteindre. Les permissions d'application s'exercent sans utilisateur, avec la portée accordée, potentiellement l'ensemble du tenant.

Une application disposant d'une permission d'application de lecture sur la messagerie peut lire toutes les boîtes aux lettres de l'organisation, y compris celles de la direction générale. C'est le vecteur employé dans plusieurs compromissions majeures documentées. Cette liste, dans votre tenant, doit être courte, connue et justifiable ligne par ligne.

Les trois mesures qui traitent le sujet

Fermer le consentement libre. Le réglage par défaut historique autorisait les utilisateurs à consentir eux-mêmes. Le restreindre est une mesure sans coût technique et à effet immédiat. La restriction doit s'accompagner d'un circuit de demande, faute de quoi les utilisateurs contourneront par des comptes personnels — ce qui aggrave le problème au lieu de le résoudre.

Instruire les demandes. Un circuit d'approbation n'a de valeur que si l'approbateur dispose des éléments pour décider : éditeur vérifié ou non, permissions demandées, portée, alternative existante. Trois questions suffisent en pratique : qui édite l'application, quelles données elle atteint, et que se passe-t-il si son éditeur est compromis.

Revoir l'existant. L'inventaire initial est presque toujours instructif : applications de test consenties il y a des années, outils d'un projet terminé, connecteurs d'un prestataire dont le contrat s'est achevé. La revue porte en priorité sur les permissions d'application de

portée large, puis sur les applications dont l'éditeur n'est pas vérifié, puis sur celles sans activité récente.

Les applications internes

Les applications développées en interne relèvent du même régime, avec une difficulté supplémentaire : elles sont créées par des équipes de développement, souvent avec des permissions plus larges que nécessaire, et personne ne revient les réduire ensuite.

Deux exigences : un propriétaire nommé pour chaque inscription d'application, et une justification des permissions au moment de la création. Ce contrôle relève de la gouvernance applicative, pas de la sécurité opérationnelle, mais il doit être exigé par la sécurité.

La détection

Un consentement accordé est un événement journalisé. Trois alertes utiles : consentement accordé à une application non vérifiée, ajout d'une permission d'application de portée large, création d'un principal de service en dehors d'un circuit connu. Ces trois alertes sont peu bruyantes et couvrent le chemin d'attaque numéro deux du chapitre 3.

Ce que vous devez décider

- **Le consentement utilisateur libre est-il encore ouvert dans votre tenant ?** Si oui, c'est la mesure la plus rentable de tout ce livre, et elle se ferme en une journée.
- **Qui approuve les demandes d'application, et avec quel délai de réponse ?** Un circuit dont le délai dépasse quelques jours sera contourné.
- **Disposez-vous de la liste des applications à permissions étendues sur la messagerie ?** Si obtenir cette liste demande plus d'une heure, le sujet n'est pas gouverné.
- **Les applications internes ont-elles un propriétaire nommé ?** Sans propriétaire, aucune revue ultérieure ne sera possible.

CHAPITRE 15

Identités non humaines : principaux de service, secrets, certificats

Les identités non humaines dépassent souvent en nombre les identités humaines, et elles ne bénéficient d'aucun des contrôles conçus pour ces dernières : pas d'authentification forte, pas de départ de l'entreprise, pas de revue par le manager. C'est un angle mort structurel.

De quoi parle-t-on

Trois familles, à traiter différemment.

Les principaux de service correspondant à des applications tierces ou internes, qui s'authentifient avec un secret ou un certificat. Les identités managées, dont le secret est géré par la plateforme et jamais exposé. Les comptes utilisateurs détournés en comptes de service — un compte humain utilisé par un script ou une application, souvent avec un mot de passe partagé et une exemption d'authentification forte.

La troisième famille est la plus dangereuse et la plus répandue. Elle cumule les inconvénients : elle consomme une licence, elle est exclue des contrôles, elle appartient nominalement à quelqu'un qui a parfois quitté l'organisation, et son mot de passe circule dans des fichiers de configuration.

Le chantier, dans l'ordre

Inventorier et attribuer. Chaque identité non humaine doit avoir un propriétaire nommé, une justification et une date de revue. Cet inventaire n'existe dans aucun portail : il se construit et se maintient, et c'est le préalable à tout le reste.

Éliminer les comptes de service humains. Chaque cas se traite individuellement : remplacer par un principal de service ou une identité managée. C'est un travail long, à mener par vagues, en commençant par les comptes disposant de privilèges ou d'un accès aux données.

Remplacer les secrets par des certificats ou des identités managées. Un secret partagé finit toujours par se retrouver dans un dépôt de code, un ticket ou un fichier de configuration. Lorsque le remplacement n'est pas possible, imposer une durée de validité courte force la rotation et révèle les identités abandonnées.

Restreindre les permissions. Les permissions accordées à la création sont presque toujours excessives. La revue doit viser en priorité les permissions d'application de portée large, comme au chapitre précédent.

Appliquer un contrôle d'accès. Lorsque la licence le permet, les identités de charge de travail peuvent être soumises à des restrictions d'origine réseau : une identité applicative qui s'authentifie depuis une adresse inattendue est alors bloquée, et non simplement journalisée. C'est le seul contrôle qui traite réellement le vol de secret.

La rotation

La rotation des secrets est un sujet d'exploitation avant d'être un sujet de sécurité. Elle échoue pour une raison unique : personne ne sait ce qui casse quand un secret change.

La réponse tient dans l'inventaire et le propriétaire. Une rotation planifiée, annoncée au propriétaire, avec une fenêtre de recouvrement pendant laquelle l'ancien et le nouveau secret coexistent, se passe sans incident. Une rotation improvisée après un incident casse la production et alimente l'argument selon lequel « la sécurité empêche de travailler ».

La surveillance

Trois signaux méritent une alerte : l'authentification d'un principal de service depuis une origine inhabituelle, l'ajout d'un secret ou d'un certificat à une application existante — technique classique de persistance après compromission — et l'utilisation d'une identité applicative en dehors de sa plage d'activité habituelle.

Le deuxième signal est particulièrement important. Un attaquant ayant obtenu des privilèges ajoute fréquemment un secret à une application légitime existante : il obtient ainsi un accès durable qui survit à la réinitialisation des mots de passe et à la révocation des sessions.

Ce que vous devez décider

- **Existe-t-il un inventaire des identités non humaines avec un propriétaire ?** Sans lui, aucune des autres mesures n'est exécutable.
- **Acceptez-vous encore la création de comptes de service humains ?** Interdire la pratique pour l'avenir est plus simple que de traiter le stock, et c'est le point de départ.
- **Quelle durée maximale de validité imposez-vous aux secrets ?** Une valeur courte force la rotation et révèle les identités abandonnées.
- **Que se passe-t-il aujourd'hui si un secret applicatif fuit ?** Si la réponse est « nous ne le saurions pas », la surveillance de cette famille d'identités doit entrer dans la feuille de route.

CHAPITRE 16

Invités, B2B et partage externe

La collaboration externe est le domaine où la sécurité entre le plus directement en conflit avec l'usage. Les mesures y sont simples techniquement et difficiles politiquement, parce qu'elles touchent la manière dont les équipes travaillent avec leurs partenaires. Elles se traitent donc par la gouvernance plus que par le blocage.

Ce qui crée un accès externe

Quatre mécanismes, souvent confondus, avec des risques distincts.

L'invitation d'un compte invité, qui crée une identité dans votre annuaire et lui donne accès aux ressources qui lui sont partagées. Le partage par lien, qui peut être restreint à des personnes désignées, étendu à toute personne de l'organisation, ou anonyme. Les canaux partagés, qui ouvrent un accès entre deux organisations sans création de compte invité. Enfin l'accès des applications tierces, traité au chapitre 14.

Le partage anonyme est le plus problématique : le lien circule, survit au départ des personnes concernées, et n'apparaît dans aucune revue d'accès portant sur les identités.

Le paramétrage de base

Trois décisions structurent le domaine.

Qui peut inviter ? Autoriser l'ensemble des utilisateurs à inviter est un choix par défaut rarement conscient. Restreindre l'invitation à certains rôles, ou la soumettre à approbation, réduit fortement la population d'invités sans bloquer la collaboration.

Avec quelles organisations ? Le paramétrage des accès entre organisations permet de définir des règles différenciées : partenaires connus avec des conditions allégées, reste du monde avec des conditions strictes ou un blocage. C'est le mécanisme le plus utile du domaine, et le moins utilisé.

Quels liens de partage ? La désactivation du partage anonyme, ou à défaut la limitation de sa durée de vie et de ses droits en lecture seule, traite l'essentiel du risque de fuite documentaire.

La question de l'authentification des invités

Un point mal compris : les stratégies d'accès de votre organisation s'appliquent aux invités qui accèdent à vos ressources, mais l'authentification s'effectue dans leur organisation d'origine. Vous héritez donc de leur niveau de sécurité.

Deux conséquences. D'abord, exiger une authentification forte des invités est légitime et techniquement possible, y compris en acceptant la vérification effectuée par leur organisation lorsque celle-ci est de confiance. Ensuite, pour les partenaires critiques — prestataires d'infogérance, cabinets ayant accès à des données sensibles — le niveau de sécurité de leur propre tenant devient votre problème, et il relève du contrat.

Le cycle de vie

C'est le cœur du sujet. Un invité est créé pour un projet et n'est presque jamais supprimé à la fin de ce projet, car personne n'est chargé de la fin.

Trois mesures traitent la question. L'attribution d'un parrain interne à chaque invité, responsable de sa justification. L'expiration automatique de l'accès, avec renouvellement explicite plutôt que reconduction tacite. Et la revue d'accès périodique portant sur la population des invités, qui relève des capacités de gouvernance décrites au chapitre 24.

À défaut de ces mécanismes, une revue manuelle semestrielle sur la base d'une extraction — invités sans authentification depuis quatre-vingt-dix jours — donne déjà l'essentiel du bénéfice pour un coût faible.

Les canaux partagés et les tenants multiples

Les canaux partagés entre organisations et les configurations multi-tenants créent des accès qui n'apparaissent pas dans les revues classiques portant sur les comptes invités. Ils doivent être inventoriés séparément.

Le cas fréquent : une filiale disposant de son propre tenant, connectée au tenant du groupe par des accords d'accès. La posture de sécurité de la filiale devient alors une composante de celle du groupe, sans qu'aucune ligne de reporting ne le reflète nécessairement.

Ce que vous devez décider

- **Tous vos utilisateurs peuvent-ils inviter des externes ?** C'est un choix par défaut ; le confirmer ou le restreindre est une décision, pas un réglage.
- **Le partage par lien anonyme est-il acceptable dans votre organisation, et sur quels espaces ?** Répondez par écrit, sinon la réponse par défaut est « partout ».
- **Qui est le parrain d'un invité ?** Sans parrain nommé, aucune revue ne pourra conclure.
- **Le niveau de sécurité de vos partenaires critiques figure-t-il dans vos contrats ?** Vous héritez de leur authentification ; c'est un sujet d'achat autant que de sécurité.

CHAPITRE 17

Données : classification, prévention de fuite, étiquettes — le minimum viable

Les programmes de protection des données échouent plus souvent que les autres, pour une raison constante : ils commencent par une taxonomie ambitieuse et se terminent par un outil déployé que personne n'utilise. Ce chapitre propose l'inverse : le minimum qui produit un effet, et l'ordre dans lequel l'atteindre.

Pourquoi ces programmes échouent

Trois causes reviennent.

La classification est conçue par un groupe de travail qui produit six niveaux, avec des règles d'usage détaillées, avant toute confrontation au terrain. Les utilisateurs ne savent pas choisir entre « interne » et « restreint », donc ils choisissent au hasard ou pas du tout.

La prévention de fuite est activée en mode blocage sur un périmètre large. Les faux positifs interrompent des processus métier légitimes en quelques jours, la direction exige un retour arrière, et le sujet devient politiquement mort pour deux ans.

Enfin le programme est porté par la sécurité seule, sans propriétaire métier des données. Or la sensibilité d'une donnée est une question métier ; la sécurité peut l'outiller, pas la décider.

Le minimum viable

Trois niveaux, pas six. Public, interne, confidentiel. Un quatrième niveau, réservé à une catégorie précise et rare — dossiers de fusion-acquisition, données de santé, secrets industriels — peut être ajouté si un besoin réel l'exige. Au-delà, l'utilisateur ne choisit plus correctement, et une classification erronée est pire qu'une absence de classification.

Une étiquette par défaut. Le contenu non classé doit recevoir automatiquement le niveau interne. Cela supprime la population, souvent majoritaire, des documents sans étiquette, et rend les statistiques exploitables.

Le chiffrage sur un seul niveau. Réserver le chiffrage attaché au document au niveau le plus élevé. C'est la mesure la plus protectrice — elle survit à l'exfiltration du fichier — et la plus contraignante à l'usage, notamment pour le partage externe et les traitements automatisés.

La prévention de fuite en observation d'abord. Activer les règles en mode journalisation pendant deux à trois mois, mesurer les déclenchements, ajuster, et ne basculer en blocage que sur les règles dont le taux de faux positifs est maîtrisé. Cette séquence n'est pas une précaution excessive : c'est la différence entre un dispositif qui tient et un dispositif abandonné.

Par où commencer

Non par l'ensemble du patrimoine documentaire, mais par les flux à risque avéré : envois de données réglementées vers l'extérieur, partage anonyme de documents portant une

étiquette confidentielle, transferts automatiques de courrier vers des adresses personnelles.

Ce dernier cas mérite une mention particulière : la règle de transfert automatique créée dans une boîte compromise est à la fois un mécanisme d'exfiltration courant et un signal de compromission. Le traiter apporte un bénéfice immédiat en détection comme en protection.

La gouvernance des données

Deux éléments manquent presque toujours et coûtent peu à mettre en place.

Un propriétaire par grand domaine de données — finance, ressources humaines, juridique, recherche — qui décide de la sensibilité et arbitre les exceptions. La sécurité outille, le métier décide.

Une politique de rétention. Les données que l'on ne conserve pas ne peuvent pas fuir. La suppression programmée des contenus dont la durée d'utilité est dépassée réduit la surface d'exposition et la charge réglementaire, et c'est souvent le seul chantier de ce domaine dont le retour sur investissement soit incontestable.

Ce que vous devez décider

- **Combien de niveaux de classification ?** Trois est presque toujours la bonne réponse ; six est presque toujours l'erreur d'origine.
- **Qui décide de la sensibilité des données ?** Si la réponse est « la sécurité », le programme échouera faute de légitimité métier.
- **Acceptez-vous une phase d'observation avant blocage ?** Refuser cette phase, c'est accepter le retour arrière quelques semaines plus tard.
- **Existe-t-il une politique de rétention appliquée ?** C'est la mesure de réduction de surface la plus rentable et la plus souvent oubliée.

CHAPITRE 18

Appareils : la conformité comme condition d'accès

C'est le chantier qui traite réellement le vol de session, donc le chemin d'attaque le plus fréquent. C'est aussi le plus lourd, parce qu'il touche l'ensemble du parc et l'expérience quotidienne de tous les utilisateurs. Il ne se décide pas au niveau technique.

Le raisonnement

Un jeton volé par relais s'utilise depuis la machine de l'attaquant. Si l'accès aux ressources exige, en plus de l'identité, un appareil connu et conforme, le jeton devient inutilisable hors du parc. C'est la seule mesure qui coupe le chemin sans dépendre du comportement de l'utilisateur.

Elle apporte un second bénéfice, souvent décisif dans l'arbitrage budgétaire : elle rétablit la notion d'inventaire. Une organisation qui exige un appareil conforme sait quels appareils accèdent à ses données — information que l'on croit détenir et que l'on ne détient presque jamais.

Les prérequis

L'exigence d'appareil suppose un parc géré : appareils enregistrés ou joints à l'annuaire, inscrits dans la gestion de parc, avec des règles de conformité définies.

Les règles de conformité doivent rester frugales. Chiffrement du disque, système d'exploitation à jour, protection contre les codes malveillants active, écran verrouillé après inactivité : quatre critères couvrent l'essentiel. Une politique à trente critères produit une population d'appareils non conformes pour des motifs mineurs, et donc des exclusions, et donc l'échec de la mesure.

Les cas difficiles

Trois populations bloquent systématiquement le déploiement, et il faut les traiter avant, pas pendant.

Les appareils personnels. Deux options : les exclure des ressources sensibles en n'autorisant qu'un accès en navigateur sans téléchargement, ou les intégrer par un mécanisme de gestion applicative qui protège les données d'entreprise sans administrer l'appareil. Le choix relève de la culture de l'organisation et du droit du travail applicable, pas de la technique.

Les prestataires et intérimaires. Ils travaillent souvent sur du matériel qui ne vous appartient pas. La réponse contractuelle — fourniture d'un poste, ou exigence de conformité du poste du prestataire — doit être arbitrée en amont.

Les appareils partagés et les postes de production. Ateliers, points de vente, laboratoires : ils exigent des configurations spécifiques et souvent des exceptions permanentes, qui doivent alors être compensées par d'autres contrôles.

La séquence de déploiement

Par ressource plutôt que par population. Commencer par les applications d'administration et les données les plus sensibles, où la population concernée est réduite et motivée. Étendre ensuite aux applications métier, puis à la messagerie et aux fichiers.

Cette progression permet de démontrer la valeur avant d'affronter le volume, et de traiter les cas particuliers au fur et à mesure plutôt qu'en une seule vague d'exceptions.

Le lien avec la révocation

Un dernier point, souvent ignoré : l'exigence d'appareil conforme ne prend pleinement son sens que si la perte de conformité produit un effet rapide sur les sessions en cours. Les mécanismes d'évaluation continue permettent de réagir à un changement de contexte sans attendre l'expiration du jeton. Vérifiez qu'ils sont actifs ; sans eux, un appareil devenu non conforme conserve son accès pendant la durée de vie de la session.

Ce que vous devez décider

- **Les appareils personnels accèdent-ils aux données d'entreprise, et à quelles conditions ?** C'est une décision de direction, avec des implications sociales et juridiques.
- **Combien de critères de conformité ?** Quatre bien tenus valent mieux que trente qui produisent des exclusions.
- **Quelles ressources exigent un appareil conforme dès cette année ?** Commencer par l'administration et les données sensibles rend le chantier atteignable.
- **Que se passe-t-il lorsqu'un appareil devient non conforme ?** Si la réponse est « rien avant la fin de la session », le contrôle est partiel.

CHAPITRE 19

Hybride : synchronisation, fédération, résidus

Lorsqu'un annuaire local est synchronisé avec le tenant, les deux environnements ne forment plus qu'un seul périmètre de sécurité. La compromission du domaine local devient une compromission du tenant, et l'inverse est parfois vrai. Ce chapitre traite des composants qui font la jonction.

Les composants qui comptent

Le serveur de synchronisation détient un compte à privilèges dans les deux annuaires. Il écrit dans le tenant, lit l'ensemble de l'annuaire local, et selon la configuration détient les moyens de valider des authentifications. Sa compromission équivaut à la compromission des deux environnements.

Les agents d'authentification déployés pour la validation directe des mots de passe reçoivent, par construction, les identifiants présentés. Ils doivent être traités avec le même niveau de protection.

Les serveurs de fédération, lorsqu'ils subsistent, détiennent les clés permettant d'émettre des assertions d'authentification. Une clé volée permet de forger l'authentification de n'importe quel utilisateur, y compris un administrateur, sans qu'aucun mot de passe ne soit compromis et sans qu'aucune trace d'échec n'apparaisse. C'est la technique employée dans plusieurs compromissions majeures.

Enfin, certains mécanismes d'authentification unique reposent sur un compte d'annuaire dont le secret n'est jamais renouvelé depuis sa création. Ce compte est un objectif connu et documenté ; son secret doit être renouvelé régulièrement.

La règle unique

Ces composants appartiennent au niveau d'administration le plus sensible, exactement comme les contrôleurs de domaine. Cela signifie : administration depuis des postes dédiés, comptes d'administration distincts, aucune application tierce installée, journalisation exportée, mises à jour prioritaires, et restriction des connexions entrantes.

Cette règle est simple à énoncer et rarement appliquée, parce que ces serveurs ont souvent été installés par l'équipe de messagerie ou d'annuaire dans un contexte de projet, sans classification particulière. La première action du chantier consiste donc à les identifier — leur inventaire n'est pas toujours à jour — et à les reclasser.

Supprimer la fédération résiduelle

Beaucoup d'organisations ont migré vers une authentification directe dans le cloud tout en conservant l'infrastructure de fédération « au cas où ». Cette infrastructure reste un chemin d'attaque complet, sans apporter de service.

Lorsque la fédération n'est plus nécessaire, elle doit être supprimée, pas éteinte. Un serveur éteint mais toujours déclaré comme émetteur de confiance dans la configuration du tenant reste exploitable.

Lorsqu'elle demeure nécessaire — exigence d'authentification par carte, contrainte réglementaire, application ancienne — le renouvellement régulier des clés de signature et la surveillance de la configuration de fédération deviennent des contrôles obligatoires.

La direction du risque

Le chemin habituel va du local vers le cloud. L'inverse existe aussi : selon la configuration, un administrateur du tenant peut disposer de moyens d'action sur l'annuaire local, notamment par les mécanismes d'écriture différée ou par les agents installés. Cette possibilité doit être vérifiée explicitement, car elle contredit l'hypothèse fréquente selon laquelle le local serait protégé du cloud.

Ce qu'il faut vérifier en priorité

Quels comptes locaux sont synchronisés et bénéficient de rôles dans le tenant : un compte à privilèges dans le cloud dont l'identité est gérée localement dépend de la sécurité de l'annuaire local. Les comptes d'administration du tenant devraient être exclusivement dans le cloud.

Quels objets sont exclus de la synchronisation : les comptes à privilèges locaux et les comptes de service ne doivent pas être synchronisés sans raison.

Quel est l'état des secrets et clés des composants de jonction, et depuis quand ils n'ont pas été renouvelés.

Ce que vous devez décider

- **Les serveurs de synchronisation et de fédération sont-ils classés au niveau le plus sensible ?** Sinon, l'ensemble des chapitres précédents est plafonné par leur sécurité.
- **La fédération résiduelle peut-elle être supprimée cette année ?** Si oui, c'est un des meilleurs rapports risque-effort du programme.
- **Vos comptes à privilèges du tenant sont-ils exclusivement dans le cloud ?** Un administrateur général synchronisé depuis l'annuaire local hérite du risque local.
- **Depuis quand les secrets des composants de jonction n'ont-ils pas été renouvelés ?** Si la réponse est « depuis l'installation », l'action est immédiate et peu coûteuse.

PARTIE IV

Détecter et réagir

CHAPITRE 20

Journalisation : quoi garder, combien de temps, à quel coût

La journalisation est le seul chantier dont l'absence ne produit aucun symptôme jusqu'au jour où elle devient indispensable. C'est pourquoi elle est systématiquement sous-dimensionnée : elle coûte tous les mois et ne sert que quelques heures, une fois tous les trois ans — au moment précis où l'entreprise ne peut se permettre de ne pas savoir.

Les trois familles

Les journaux d'authentification enregistrent chaque tentative d'accès : identité, application visée, protocole, origine, appareil, résultat, et les stratégies évaluées. C'est la source la plus riche et la plus volumineuse.

Les journaux d'audit de l'annuaire enregistrent les modifications : création de comptes, attribution de rôles, ajout de secrets à une application, consentement accordé, modification d'une stratégie d'accès. C'est la source qui permet de reconstituer ce qu'un attaquant a fait après son entrée.

Les journaux d'activité des services de collaboration enregistrent l'usage : accès à une boîte aux lettres, téléchargement de fichiers, création de règles de messagerie, partage externe. C'est la source qui permet de répondre à la question qui décide de la notification réglementaire — quelles données ont été consultées.

Ces trois familles n'ont ni la même rétention native, ni le même volume, ni la même valeur d'investigation. Les traiter comme un ensemble unique conduit soit à payer trop, soit à perdre l'essentiel.

Le raisonnement de durée

La règle est simple à formuler : la durée de conservation doit être supérieure au délai réaliste entre une compromission et sa détection, augmenté du temps d'investigation.

Ce délai se compte en mois, pas en jours, y compris dans des organisations bien outillées, et particulièrement pour les compromissions discrètes — vol de jeton, consentement applicatif, accès applicatif à la messagerie. Les rétentions natives des plateformes se comptent, elles, en jours ou en semaines pour l'annuaire et en mois pour la collaboration.

L'écart entre les deux définit exactement ce que vous devez exporter et conserver ailleurs. Il n'y a pas d'autre raisonnement à tenir, et il conduit dans la quasi-totalité des cas à une cible de douze mois minimum, souvent dix-huit ou vingt-quatre selon le secteur et les obligations applicables.

Chaud et froid

L'erreur budgétaire classique consiste à conserver tout en ligne, immédiatement interrogeable, à un coût qui rend le projet insoutenable au bout de deux ans.

Le modèle qui fonctionne distingue deux niveaux. Un niveau chaud, de trente à quatre-vingt-dix jours, contenant ce qui alimente les détections et le travail quotidien de l'équipe

sécurité. Un niveau froid, jusqu'à la durée cible, en archive à faible coût, interrogeable en différé — quelques heures d'attente sont acceptables dans une investigation qui durera des semaines.

La discipline consiste à décider ce qui monte au chaud plutôt qu'à tout y envoyer par défaut. Les journaux d'audit d'annuaire et les authentifications à privilèges méritent le niveau chaud ; le détail de l'activité documentaire de l'ensemble des utilisateurs, rarement.

Ce qu'il faut conserver en priorité

Si le budget impose des choix, l'ordre de priorité est le suivant.

Les journaux d'audit de l'annuaire, en totalité : faible volume, valeur d'investigation maximale. Ils contiennent les traces de persistance de l'attaquant.

Les authentifications des comptes à privilèges et des identités applicatives, en totalité, sans échantillonnage.

Les authentifications de l'ensemble des utilisateurs, avec les propriétés d'origine et d'appareil, qui permettent de caractériser un vol de session.

L'activité de messagerie et de partage, indispensable pour établir le périmètre des données consultées — c'est la source qui décide d'une notification réglementaire, et son absence conduit à notifier au maximum par précaution.

L'intégrité

Un point que la plupart des organisations découvrent trop tard : un attaquant disposant de privilèges dans le tenant peut modifier la configuration de journalisation, désactiver des collectes, ou réduire des durées de rétention. Les journaux qui ne sortent pas de l'environnement compromis ne sont pas des preuves.

L'export vers un espace de stockage sous un contrôle distinct, avec des droits d'écriture séparés des droits d'administration du tenant, est donc une exigence, pas une commodité. Cette séparation est également ce que vous demandera un assureur ou un régulateur.

Le coût

Le coût se pilote sur trois leviers : le volume ingéré au niveau chaud, la durée de conservation par niveau, et le tri des catégories de journaux. Un dimensionnement correct commence toujours par une mesure sur trente jours du volume réel par catégorie — les estimations théoriques se trompent d'un facteur trois dans les deux sens.

Une remarque de gouvernance : ce budget appartient à la sécurité et non à la production. Confié à l'exploitation, il sera le premier arbitré à la baisse, car il n'a aucun effet visible sur le service rendu.

Ce que vous devez décider

- **Quelle durée de conservation vous engagez-vous à tenir, par famille de journaux ?** Écrivez-la ; c'est le seul moyen de la défendre en arbitrage budgétaire.
- **Les journaux sortent-ils du tenant, vers un espace au contrôle distinct ?** Si non, votre preuve dépend de l'environnement que vous auditez.

- **Pouvez-vous répondre aujourd'hui à « quelles données ont été consultées » sur un incident vieux de six mois ?** Si la réponse est non, la conséquence est réglementaire avant d'être technique.
- **Qui porte le budget de journalisation ?** S'il est porté par la production, il sera réduit au premier exercice contraint.

CHAPITRE 21

Détections qui comptent, bruit à éliminer

Une organisation qui reçoit deux cents alertes par jour n'en traite aucune. La qualité d'un dispositif de détection ne se mesure pas au nombre de règles activées mais au nombre d'alertes réellement instruites et au délai de traitement. Ce chapitre propose un socle court.

Partir des chemins, pas du catalogue

Les plateformes proposent des dizaines de détections prêtes à l'emploi. Les activer toutes produit un flux ingérable et une désensibilisation rapide de l'équipe.

La méthode consiste à repartir des sept chemins du chapitre 3 et à demander, pour chacun : que verrions-nous si cela se produisait ? La réponse donne une liste courte, hiérarchisée par risque, et elle est défendable devant une direction parce qu'elle se rattache à des scénarios et non à un catalogue de produit.

Le socle utile

Vol de session. Une même session ou un même jeton employé depuis deux origines incompatibles ; une authentification réussie suivie immédiatement d'une inscription de méthode d'authentification ; l'apparition d'une règle de boîte aux lettres qui déplace ou supprime des messages entrants. Cette dernière détection est parmi les plus rentables de toutes : elle est peu bruyante et signale presque toujours une compromission réelle.

Consentement applicatif. Consentement accordé à une application dont l'éditeur n'est pas vérifié ; ajout d'une permission d'application de portée large ; création d'un principal de service hors circuit connu.

Persistance après compromission. Ajout d'un secret ou d'un certificat à une application existante ; création d'un compte à privilèges ; ajout d'un membre à un groupe attribuant un rôle ; modification d'une stratégie d'accès conditionnel ou ajout d'une exclusion.

Comptes à privilèges. Toute authentification d'un compte d'accès d'urgence ; activation d'un rôle sensible hors des plages habituelles ; échec massif d'authentification suivi d'une réussite sur un même compte.

Identités applicatives. Authentification d'un principal de service depuis une origine inhabituelle ; usage en dehors de sa plage d'activité normale.

Chemin hybride. Modification de la configuration de fédération ; authentification du compte de synchronisation depuis un serveur inattendu.

Une quinzaine de détections, correctement calibrées, couvrent l'essentiel. C'est un objectif atteignable ; deux cents règles ne le sont pas.

Le bruit à éliminer

Trois catégories produisent l'essentiel des faux positifs.

Les détections de déplacement impossible mal calibrées, qui se déclenchent sur les réseaux privés virtuels d'entreprise, les proxys sortants et les personnels en déplacement. Elles nécessitent une phase d'apprentissage et une liste d'origines connues, sans quoi elles doivent être coupées.

Les comptes de service et identités applicatives, dont le comportement diffère structurellement de celui des humains. Ils doivent faire l'objet de règles séparées, avec leurs propres seuils, jamais des règles générales.

Les alertes de faible gravité issues du catalogue par défaut, qui informent sans nécessiter d'action. Elles ne devraient pas atteindre une file de traitement humaine ; leur place est dans un tableau de bord hebdomadaire.

Le triage

Une détection sans destinataire ni délai d'action n'est pas une détection. Pour chaque règle, trois éléments doivent être écrits avant activation : qui la reçoit, dans quel délai elle doit être instruite, et quelle est la première action attendue.

Ce dernier point est le plus négligé. Une alerte de compromission d'un compte à privilèges à trois heures du matin doit être assortie d'une consigne exécutable par la personne d'astreinte — révoquer les sessions, désactiver le compte, appeler tel numéro — et non d'une invitation à analyser.

Vérifier que cela fonctionne

Une règle activée n'est pas une règle opérationnelle. Trois vérifications, à mener au moins annuellement.

Générer volontairement les événements attendus dans un cadre maîtrisé et vérifier que l'alerte remonte, arrive au bon destinataire, et dans le délai prévu. La plupart des dispositifs échouent dès cette étape, généralement sur le chemin de notification.

Vérifier la couverture au moyen de la grille de techniques du chapitre 6, et documenter explicitement les zones aveugles assumées.

Mesurer le délai réel entre l'événement et son instruction, et non le délai théorique. C'est l'indicateur à présenter en comité, celui du chapitre 26.

Ce que vous devez décider

- **Combien d'alertes votre organisation peut-elle réellement instruire par jour ?** Dimensionnez le dispositif sur cette capacité, pas sur le catalogue disponible.
- **Chaque détection a-t-elle un destinataire et une première action écrite ?** Sans cela, elle produit du bruit et une fausse assurance.
- **Vos détections ont-elles été testées de bout en bout ?** Une règle jamais déclenchée en conditions réelles n'a jamais prouvé qu'elle fonctionne.
- **Quelles zones aveugles acceptez-vous ?** Les écrire vaut mieux que de croire à une couverture complète.

CHAPITRE 22

Compromission d'un compte à privilèges : le déroulé heure par heure

Ce chapitre décrit la conduite des premières soixante-douze heures. Il ne remplace pas un plan de réponse formalisé, mais il fournit la séquence et, surtout, l'ordre des actions — car l'erreur la plus fréquente n'est pas l'inaction, c'est l'action précipitée qui détruit la preuve ou alerte l'attaquant avant que le périmètre ne soit connu.

L'erreur d'ouverture

Le réflexe naturel, devant le signalement d'un compte compromis, consiste à réinitialiser le mot de passe et à considérer l'incident traité.

Dans un environnement d'identité moderne, cette action seule ne traite presque rien. Elle ne révoque pas les sessions en cours, ne supprime pas les méthodes d'authentification ajoutées par l'attaquant, ne révoque pas les consentements applicatifs accordés, ne supprime pas les secrets ajoutés à une application, ni les règles de messagerie créées. Elle prévient en revanche l'attaquant qu'il a été repéré.

Heure 0 à heure 1 — Confirmer et préserver

Confirmer le signal avant d'agir : identifier l'authentification suspecte, son origine, l'application visée, la méthode employée. Une alerte sur cinq est un faux positif, et une réponse déclenchée à tort a un coût réel.

Préserver immédiatement : exporter les journaux d'authentification et d'audit sur la période concernée, avant toute modification. C'est la seule action à mener avant tout le reste, car les fenêtres de rétention courent.

Constituer la cellule : un responsable de l'incident, un opérateur habilité à agir sur le tenant, un référent juridique ou conformité en veille. Ouvrir un journal d'incident horodaté, tenu en continu — il servira à la notification réglementaire et, éventuellement, à l'assurance.

Heure 1 à heure 4 — Contenir

L'ordre compte. Révoquer les sessions et jetons du compte concerné, puis désactiver le compte ou retirer ses rôles selon la stratégie retenue. La révocation des jetons de rafraîchissement est indispensable : sans elle, l'attaquant conserve son accès malgré la réinitialisation du mot de passe.

Puis rechercher les persistance, dans cet ordre de probabilité : méthodes d'authentification ajoutées ou modifiées sur le compte ; règles de boîte aux lettres créées ; délégations d'accès à la boîte ; consentements applicatifs récents ; secrets ou certificats ajoutés à des applications existantes ; comptes créés ou rôles attribués depuis la compromission présumée ; modifications des stratégies d'accès conditionnel et de leurs exclusions.

Cette liste doit être parcourue intégralement, même lorsque la première anomalie est trouvée. Un attaquant expérimenté pose plusieurs points de persistance, et la découverte du premier crée un faux sentiment de résolution.

Décider enfin d'une question stratégique : contenir immédiatement ou observer. L'observation permet de mesurer l'ampleur réelle mais laisse l'attaquant actif. Ce choix appartient au responsable de l'incident et doit être écrit, avec son heure et sa justification.

Heure 4 à heure 24 — Éradiquer

Supprimer toutes les persistances identifiées. Révoquer les consentements applicatifs suspects. Renouveler les secrets des applications concernées.

Élargir le périmètre : le compte compromis a-t-il servi à atteindre d'autres comptes ? Rechercher les authentifications provenant des mêmes origines, les autres comptes ayant présenté les mêmes anomalies, et les actions d'administration effectuées depuis la compromission.

Si un compte à privilèges élevés est concerné, considérer que l'ensemble du tenant est potentiellement affecté et engager la rotation décrite au chapitre suivant.

Heure 24 à heure 72 — Établir l'impact

C'est la phase qui détermine les obligations légales. La question n'est plus « comment est-il entré » mais « à quelles données a-t-il accédé ».

Elle se traite avec les journaux d'activité de collaboration : boîtes aux lettres consultées, fichiers téléchargés, partages créés, exports effectués. La qualité de la réponse dépend entièrement des décisions prises au chapitre 20. En l'absence de journaux, l'organisation se trouve contrainte de notifier au périmètre maximal, avec les conséquences que cela emporte.

Engager en parallèle l'analyse juridique des obligations de notification, dont les délais sont courts et courent à partir de la connaissance de l'incident, non de sa résolution.

Après

Deux livrables, à ne pas confondre. Le rapport d'incident, factuel et horodaté, destiné aux obligations réglementaires et contractuelles. Le retour d'expérience, destiné à la correction, qui doit identifier non seulement la faille exploitée mais aussi les contrôles qui auraient dû détecter ou bloquer et ne l'ont pas fait.

Le second doit produire des actions inscrites dans la feuille de route, avec un responsable. Un retour d'expérience sans action est un document de conformité, pas une amélioration.

Ce que vous devez décider

- **Qui est autorisé à révoquer et désactiver, à trois heures du matin, sans validation hiérarchique ?** Si personne, votre délai de réaction est celui d'une chaîne d'appels.
- **Contenir immédiatement ou observer : qui tranche ?** Ce choix doit être attribué avant l'incident, pas discuté pendant.

- **Vos journaux permettent-ils d'établir les données consultées ?** C'est ce qui décide de l'étendue de votre notification réglementaire.
- **Le retour d'expérience produit-il des actions suivies ?** Sinon, le même incident se reproduira avec un autre compte.

CHAPITRE 23

Reconstruire : révocation, rotation, investigation d'identité

Après une compromission touchant des privilèges, une question domine toutes les autres : à partir de quel moment peut-on de nouveau faire confiance au tenant ? Y répondre suppose un travail méthodique de révocation, de rotation et de vérification.

Révoquer réellement

La révocation d'un accès dans un environnement fondé sur les jetons n'est pas instantanée et ne se limite pas au mot de passe.

Trois actions distinctes doivent être menées : révoquer les jetons de rafraîchissement, qui permettent le renouvellement de l'accès ; forcer la réévaluation des sessions en cours, faute de quoi un jeton d'accès valide continue de fonctionner jusqu'à son expiration ; et supprimer ou réinitialiser les méthodes d'authentification enregistrées, car un attaquant ayant inscrit sa propre méthode conserve un moyen d'authentification légitime après la réinitialisation du mot de passe.

Les mécanismes d'évaluation continue réduisent fortement le délai de prise en compte. Leur activation, décidée à froid, est ce qui fait la différence entre une révocation effective en minutes et une révocation effective en heures.

Rotation : le périmètre réel

La rotation est presque toujours sous-dimensionnée. En cas de compromission d'un compte à privilèges élevés, le périmètre à traiter comprend, au minimum : les secrets et certificats des applications ayant reçu des modifications récentes ; les identifiants des comptes d'accès d'urgence ; les secrets des composants de synchronisation et de fédération ; les clés de signature de fédération si elle subsiste ; et les identifiants de tout compte de service ayant transité par un système potentiellement compromis.

Cette rotation doit être planifiée, avec les propriétaires identifiés au chapitre 15. C'est précisément dans cette situation que l'absence d'inventaire des identités non humaines devient coûteuse : l'organisation ignore ce qu'elle doit renouveler et ce qui cassera.

L'investigation d'identité

Elle répond à trois questions, dans l'ordre.

Quand l'accès a-t-il commencé ? La date de la première authentification anormale détermine la période à examiner. Elle est fréquemment antérieure de plusieurs semaines à la détection.

Qu'a fait l'attaquant ? Les journaux d'audit de l'annuaire fournissent la réponse : rôles attribués, applications modifiées, stratégies changées, comptes créés. C'est la source la plus dense et la plus rapide à exploiter.

À quoi a-t-il accédé ? Les journaux d'activité des services de collaboration, seule source permettant de délimiter l'exposition des données.

La limite de l'exercice est toujours la même : la rétention. Une investigation ne peut pas remonter au-delà des journaux disponibles, et l'organisation qui découvre cette contrainte pendant un incident ne peut plus rien y faire.

Les persistance que l'on oublie

Six mécanismes échappent régulièrement au nettoyage et méritent une vérification explicite : les délégations d'accès aux boîtes aux lettres ; les règles de transport au niveau de l'organisation ; les applications consenties et leurs secrets ; les attributions de rôles éligibles, qui n'apparaissent pas dans une revue des rôles actifs ; les unités administratives et les délégations de portée ; et les comptes invités créés pendant la période de compromission.

À cette liste s'ajoute, en environnement hybride, la vérification des objets synchronisés : une modification effectuée dans l'annuaire local se propage vers le tenant et survivra à un nettoyage effectué uniquement côté cloud.

Nettoyer ou reconstruire

La reconstruction complète d'un tenant est en pratique irréalisable pour une organisation en activité. La question se pose différemment : ce sont les composants de jonction et les postes d'administration qui doivent être reconstruits, pas l'annuaire.

Un serveur de synchronisation ou de fédération suspecté de compromission se réinstalle ; il ne se nettoie pas. Un poste d'administration également. Cette règle est coûteuse et elle est la seule qui permette d'affirmer, ensuite, que la confiance est rétablie.

Rétablir la confiance

Le retour à la normale doit être déclaré explicitement, sur la base de critères écrits : persistance vérifiées et supprimées, rotations effectuées, composants sensibles reconstruits, surveillance renforcée maintenue sur une période définie, et absence de nouvel indicateur pendant cette période.

Cette déclaration, datée et signée par le responsable de l'incident, ferme l'épisode. Sans elle, l'organisation reste dans un état intermédiaire où personne ne sait plus si le sujet est traité.

Ce que vous devez décider

- **L'évaluation continue des sessions est-elle active ?** Elle détermine si votre révocation prend effet en minutes ou en heures.
- **Savez-vous ce qu'il faudrait faire tourner en cas de compromission d'un administrateur ?** Si la liste n'existe pas, elle se construira dans l'urgence et sera incomplète.
- **Acceptez-vous de reconstruire les composants sensibles plutôt que de les nettoyer ?** C'est un arbitrage de coût contre certitude, et il se prépare avant l'incident.
- **Qui déclare le retour à la normale, et sur quels critères ?** Sans critères écrits, cette déclaration ne sera jamais prononcée.

PARTIE V

Gouverner dans la durée

CHAPITRE 24

Gouvernance des identités : cycle de vie, revues, séparation des tâches

Les quatre parties précédentes traitent d'un état : mesurer, corriger, détecter. Celle-ci traite d'un mouvement. Une organisation qui ne gouverne pas ses identités retrouve, dix-huit mois après un programme de remédiation réussi, un niveau d'exposition comparable à celui du départ. Les accès s'accumulent parce que rien n'organise leur retrait.

Le cycle de vie

Trois moments décident de tout, et deux d'entre eux sont mal traités partout.

L'arrivée est le moment le mieux couvert : il existe presque toujours un processus, parce que l'absence d'accès bloque le travail et se signale immédiatement.

Le changement de poste est le moment le plus destructeur. Les accès de l'ancien poste ne sont pas retirés, ceux du nouveau s'ajoutent, et une personne ayant fait trois mobilités cumule trois périmètres. C'est l'origine principale des accumulations de privilèges constatées en audit, et le contrôle correspondant — retrait des accès de l'ancien poste dans un délai défini — n'existe presque jamais.

Le départ est traité pour les salariés et oublié pour tous les autres : prestataires, stagiaires, comptes de partenaires, invités. Or ces populations n'ont pas de processus de sortie centralisé, puisque leur départ ne passe pas par les ressources humaines.

La mesure de contrôle est simple et rarement suivie : le délai entre la date de sortie effective et la désactivation du compte, mesuré et présenté chaque trimestre.

Les revues d'accès

Une revue d'accès a une seule fonction : retirer ce qui n'est plus justifié. Elle échoue lorsqu'elle devient une formalité de conformité.

Trois causes d'échec reviennent. La revue porte sur un volume trop important : un manager qui reçoit deux cents lignes valide tout en bloc. Elle est confiée à la mauvaise personne : la sécurité ne sait pas si un accès est justifié métier, seul le responsable hiérarchique ou le propriétaire de l'application le sait. Enfin, elle n'a pas de conséquence : les accès non validés ne sont pas retirés, et l'exercice suivant est traité avec le sérieux qu'il mérite.

Ce qui fonctionne : des revues ciblées et fréquentes plutôt qu'exhaustives et annuelles. En priorité, les rôles à privilèges, les invités, les applications à permissions étendues et les groupes attribuant des droits. Ces quatre populations sont petites, et leur revue trimestrielle produit plus d'effet qu'une revue générale annuelle de l'ensemble des accès.

Une règle non négociable : le retrait automatique en l'absence de réponse. Une revue dont l'absence de réponse vaut maintien de l'accès ne sert à rien.

La séparation des tâches

Le principe est ancien et se transpose directement : celui qui configure ne doit pas être celui qui contrôle, et celui qui accorde un accès ne doit pas être celui qui en bénéficie.

Trois applications concrètes dans un environnement Entra ID.

L'administrateur qui modifie les stratégies d'accès ne devrait pas être celui qui revoit la liste des exclusions. Le propriétaire d'une application ne devrait pas approuver seul les permissions qu'il demande. Et l'équipe qui administre le tenant ne devrait pas être seule destinataire des journaux qui tracent ses propres actions — d'où l'export vers un espace au contrôle distinct décrit au chapitre 20.

Ces séparations sont difficiles dans les petites structures, où une seule personne détient tout. La réponse n'est alors pas la séparation mais la traçabilité renforcée et une revue externe périodique.

L'accès par le besoin plutôt que par la demande

L'étape de maturité suivante consiste à attacher les accès à un rôle métier ou à un catalogue de demandes plutôt qu'à des attributions individuelles. L'accès devient alors une conséquence d'une situation — appartenance à une équipe, participation à un projet — et non le résultat d'une demande ponctuelle jamais annulée.

C'est un chantier long, qui suppose des données de référence fiables sur les personnes et l'organisation. Il ne se lance pas en première année. Mais son absence explique pourquoi les revues d'accès restent nécessaires : elles compensent l'absence de retrait automatique.

Ce que vous devez décider

- **Le changement de poste déclenche-t-il un retrait d'accès ?** Sinon, l'accumulation de privilèges est structurelle et aucune correction ponctuelle ne la traitera.
- **Qui sort les prestataires et les invités ?** Si la réponse est « les ressources humaines », elle est fausse : ces populations n'y figurent pas.
- **L'absence de réponse à une revue vaut-elle maintien ou retrait ?** C'est la décision qui détermine si vos revues servent à quelque chose.
- **Combien de revues ciblées par an, sur quelles populations ?** Quatre revues trimestrielles ciblées valent mieux qu'une revue générale annuelle.

CHAPITRE 25

Conformité : NIS2, DORA, ISO 27001, RGPD

La conformité n'améliore pas la sécurité, mais elle finance des mesures qui l'améliorent. C'est sa fonction réelle dans un programme, et c'est ainsi qu'il faut l'utiliser : comme un levier d'arbitrage, pas comme un objectif.

Ce chapitre décrit ce que chacun de ces textes exige concrètement d'un environnement Entra ID et Microsoft 365. Les régimes évoluent et leur transposition nationale varie ; vérifiez toujours l'état applicable à votre organisation avec votre direction juridique.

RGPD

Le règlement européen n'impose pas de mesures techniques nommées, mais l'obligation de sécurité appropriée au risque, l'obligation de notification d'une violation dans un délai court, et la minimisation des données.

Trois conséquences directes sur votre environnement. La capacité à établir quelles données personnelles ont été consultées lors d'un incident, faute de quoi la notification devra couvrir le périmètre maximal — c'est le raisonnement du chapitre 20. La maîtrise des transferts et des accès des tiers, qui relie ce texte au chapitre 14 sur les applications. Et la politique de rétention, qui relève à la fois de la minimisation et de la réduction de surface d'exposition.

NIS2

La directive européenne sur la sécurité des réseaux et des systèmes d'information élargit considérablement le champ des entités concernées et introduit deux nouveautés qui changent la conversation interne.

La première est la responsabilité explicite des organes de direction, qui doivent approuver les mesures de gestion du risque et peuvent être tenus responsables des manquements. C'est l'argument le plus efficace dont vous disposez pour obtenir un arbitrage sur les mesures à impact utilisateur : la décision de renoncer n'est plus une décision technique.

La seconde est le régime de notification en plusieurs temps — une alerte précoce dans les vingt-quatre heures, une notification circonstanciée sous soixante-douze heures, un rapport final ultérieur. Ce calendrier est incompatible avec une organisation qui ne sait pas, en trois jours, ce qui a été consulté. Il valide directement les chapitres 20 et 22.

La directive impose également des exigences sur la sécurité de la chaîne d'approvisionnement, ce qui inclut vos prestataires disposant d'accès à votre tenant, et sur l'authentification multifacteur.

DORA

Le règlement sur la résilience opérationnelle numérique du secteur financier est plus prescriptif et directement applicable aux entités concernées.

Quatre exigences touchent l'identité. La gestion du risque lié aux technologies, incluant explicitement la gestion des accès et des privilèges. Le registre des prestataires de services

technologiques, qui doit recenser vos fournisseurs critiques — votre fournisseur de messagerie et d'identité en fait partie. La notification des incidents majeurs selon un calendrier strict. Et les tests de résilience, qui portent sur des scénarios réalistes.

Pour un environnement Microsoft 365, cela se traduit par des questions concrètes : que se passe-t-il si le fournisseur d'identité est indisponible, avez-vous une stratégie de sortie, et vos accès d'urgence fonctionnent-ils. Le chapitre 11 y répond partiellement, mais la question de la dépendance à un fournisseur unique relève de la direction générale.

ISO 27001

La norme n'impose pas de configuration mais un système de gestion et un ensemble de mesures dont plusieurs portent directement sur l'identité : gestion des identités, information d'authentification, droits d'accès, gestion des accès à privilèges, authentification sécurisée, journalisation et surveillance.

Son intérêt pratique dans un programme est double. Elle fournit un cadre reconnu pour structurer la gouvernance décrite au chapitre 24. Et sa logique d'amélioration continue, avec revue de direction, offre le véhicule le plus simple pour institutionnaliser le pilotage du chapitre 26 sans créer une instance supplémentaire.

Les assureurs

Un cinquième référentiel s'est imposé sans être un texte : les questionnaires des assureurs cyber. Ils exigent aujourd'hui de manière quasi systématique l'authentification multifacteur sur les accès distants et les comptes à privilèges, la sauvegarde hors ligne, la gestion des accès à privilèges, et la journalisation.

Leur intérêt tient à leur effet immédiat : une déclaration inexacte peut fonder un refus de garantie. C'est souvent l'argument qui obtient un budget refusé pendant deux ans par la voie du risque.

Comment s'en servir

Le tableau de correspondance entre vos mesures et les exigences applicables doit être construit une fois, puis maintenu. Il sert trois fois : pour justifier un budget, pour répondre à un questionnaire client ou assureur sans remobiliser les équipes, et pour éviter de traiter deux fois la même exigence sous deux noms différents.

Ce qu'il ne faut pas faire : structurer le programme de sécurité selon les textes. Vous obtiendriez un programme conforme et incohérent. Structurez-le selon les chemins d'attaque, puis rattachez les mesures aux exigences.

Ce que vous devez décider

- **Quels régimes s'appliquent réellement à votre organisation ?** La réponse relève du juridique, et elle conditionne l'ensemble de la trajectoire.
- **Votre direction générale sait-elle qu'elle porte une responsabilité personnelle ?** C'est le levier d'arbitrage le plus puissant, et il est rarement énoncé.
- **La correspondance mesures-exigences est-elle maintenue ?** Sans elle, chaque questionnaire remobilise les équipes pendant une semaine.

- **Vos déclarations aux assureurs sont-elles exactes ?** Une inexactitude découverte au sinistre annule la couverture.

CHAPITRE 26

Piloter : indicateurs et contrôle continu

Un audit annuel décrit l'état du tenant un jour par an. Les trois cent soixante-quatre autres jours, la configuration dérive : exclusions ajoutées, applications consenties, comptes créés, stratégies modifiées. Le pilotage consiste à réduire cet angle mort.

Le principe

Le contrôle continu ne consiste pas à surveiller davantage, mais à recalculer périodiquement un petit nombre de mesures et à en suivre la tendance. La question pertinente n'est pas « sommes-nous conformes » mais « la dérive est-elle positive ou négative depuis le dernier point ».

Cela suppose une exigence méthodologique : les mesures doivent être calculées de la même manière à chaque fois. Un indicateur dont la méthode change n'est plus un indicateur. C'est la raison pour laquelle le chapitre 7 insiste sur la reproductibilité des extractions.

Les indicateurs qui méritent d'être suivis

Une dizaine suffit, et ils doivent tous être issus d'une extraction, jamais d'une déclaration.

Nombre d'attributions permanentes des rôles les plus sensibles. Proportion d'administrateurs disposant d'une méthode résistante à l'hameçonnage. Nombre d'exclusions actives dans les stratégies d'accès, et nombre d'exclusions dont la date de fin est dépassée. Proportion des authentifications réussies couvertes par une méthode forte. Nombre d'applications disposant de permissions étendues sur la messagerie. Nombre de secrets applicatifs expirant dans les quatre-vingt-dix jours. Nombre d'invités sans authentification depuis quatre-vingt-dix jours. Délai moyen entre la sortie effective d'une personne et la désactivation de son compte. Délai médian entre une alerte de sécurité et son instruction. Durée de conservation effective des journaux.

Ces dix mesures se calculent automatiquement et racontent, ensemble, l'état réel de la gouvernance.

Ce qu'il ne faut pas suivre

Le score natif de la plateforme comme indicateur principal, pour les raisons du chapitre 6. Le nombre d'alertes traitées, qui récompense le bruit. Le nombre de contrôles conformes sur un référentiel, qui incite à traiter les écarts faciles plutôt que les écarts importants. Et le nombre d'actions de la feuille de route réalisées, qui mesure l'activité et non le risque.

Un indicateur mal choisi ne se contente pas d'informer mal : il oriente le travail de l'équipe vers ce qu'il mesure. C'est la raison pour laquelle le choix des indicateurs est une décision de direction.

La fréquence et le destinataire

Mensuel pour l'équipe sécurité, sur l'ensemble des mesures, avec analyse des variations.

Trimestriel pour la direction, sur trois à cinq mesures seulement, accompagnées d'une lecture. Une direction générale n'a pas besoin de dix indicateurs ; elle a besoin de savoir si la trajectoire est tenue et ce qui la freine.

Annuel pour la revue complète, qui rejoue l'audit et vérifie que les mesures automatisées n'ont pas laissé de zone aveugle.

Le contrôle des dérives

Trois dérives sont si fréquentes qu'elles méritent une surveillance dédiée, indépendamment des indicateurs.

L'ajout d'une exclusion dans une stratégie d'accès. La création d'un compte à privilèges ou l'attribution d'un rôle sensible. Le consentement à une nouvelle application disposant de permissions étendues.

Ces trois événements devraient produire une notification vers le responsable sécurité, non comme alerte d'incident mais comme information de gouvernance. Elles sont peu nombreuses dans un tenant sain, et leur volume est lui-même un indicateur.

Ce que vous devez décider

- **Quels trois indicateurs présentez-vous à votre direction ?** Choisissez-les vous-même ; à défaut, ils seront choisis par l'outil.
- **Vos mesures sont-elles calculées automatiquement ?** Un indicateur qui coûte deux jours de travail par mois ne sera pas maintenu.
- **Qui est notifié de l'ajout d'une exclusion ou d'un rôle sensible ?** C'est le contrôle de dérive le plus rentable de ce chapitre.
- **Quelle est la fréquence de recalcul complète ?** Annuelle est le minimum ; trimestrielle est la cible.

CHAPITRE 27

Budget et feuille de route à douze mois

Ce chapitre propose une trajectoire d'une année, à partir d'un état initial typique : authentification forte déployée mais incomplète, accès conditionnel présent mais accumulé, applications non gouvernées, journalisation aux valeurs par défaut.

Ce que coûte réellement un programme

Quatre postes, dont un seul est visible.

Les licences, si l'écart de couverture le justifie. C'est le poste le plus discuté et rarement le plus déterminant : la majorité des mesures des chapitres 11 à 19 s'appliquent avec un socle de licence courant.

L'outillage : journalisation et conservation, éventuellement sauvegarde des données de collaboration, éventuellement outil d'audit et de contrôle continu. C'est un coût récurrent, à défendre comme tel.

La prestation externe, pour l'audit initial et pour les chantiers exigeant une compétence rare et ponctuelle.

Le temps interne, qui est le poste le plus lourd et celui qui n'apparaît dans aucun budget. Un chantier d'authentification résistante à l'hameçonnage sur plusieurs milliers de personnes mobilise le support, la communication interne, les relais métier. Le chiffrer explicitement évite l'échec par sous-estimation.

Les trois vagues

Jours 1 à 30 — sans impact utilisateur. Fermer le consentement applicatif libre et mettre en place le circuit de demande. Constituer et publier la liste consolidée des exclusions. Créer et tester les comptes d'accès d'urgence. Activer l'export des journaux d'audit vers un espace au contrôle distinct. Établir l'inventaire des identités non humaines et des applications à permissions étendues.

Ce sont des mesures peu coûteuses, à fort rendement, et elles établissent la crédibilité du programme auprès de la direction comme des équipes.

Jours 31 à 90 — populations restreintes. Réduire les attributions permanentes des rôles sensibles et mettre en place l'élévation temporaire. Déployer une méthode résistante à l'hameçonnage sur les administrateurs et les populations exposées. Renforcer la procédure de réinitialisation au support. Rationaliser le jeu de stratégies d'accès conditionnel et introduire la stratégie de blocage par défaut. Mettre en place les quinze détections du chapitre 21 avec leur circuit de traitement.

Jours 91 à 365 — chantiers structurants. Exigence d'appareil conforme, par ressource puis par population. Reclassement et durcissement des composants de jonction hybrides, suppression de la fédération résiduelle. Gouvernance des identités : cycle de vie, revues ciblées trimestrielles. Extension de l'authentification résistante à l'hameçonnage à l'ensemble de l'organisation. Postes d'administration dédiés.

Ce qui bloque, et comment le débloquent

Le blocage n'est presque jamais technique. Trois obstacles reviennent.

L'absence de propriétaire de la configuration d'identité. Il se traite par une décision de gouvernance, pas par un projet.

Le refus de l'impact utilisateur. Il se traite par un arbitrage explicite au bon niveau, appuyé sur les scénarios du chapitre 3 et, le cas échéant, sur la responsabilité de direction évoquée au chapitre 25.

La concurrence avec les projets métier. Elle se traite en séquençant : les mesures de la première vague ne consomment pas de capacité projet, et les livrer rapidement crédibilise la demande de capacité pour la suite.

Comment défendre le budget

Trois éléments, dans cet ordre. Un scénario chiffré : ce que coûterait la compromission d'un compte à privilèges, en indisponibilité, en notification, en assurance, en atteinte de réputation. Une comparaison des deux trajectoires — à licence constante et à licence cible. Et un engagement de mesure : les trois indicateurs que vous présenterez trimestriellement pour démontrer l'effet.

Un budget de sécurité obtenu sans engagement de mesure ne sera pas reconduit.

Ce que vous devez décider

- **Quelle est votre première vague, et sa date de fin ?** Trente jours est un engagement tenable et il change la perception du programme.
- **Le temps interne est-il chiffré dans votre budget ?** S'il ne l'est pas, la troisième vague ne sera pas exécutée.
- **Sur quels indicateurs vous engagez-vous ?** Le budget suivant en dépend davantage que du contenu du plan.
- **Que renoncez-vous à faire cette année ?** Un plan sans renoncement écrit est un plan qui dérivera.

CHAPITRE 28

Les dix erreurs les plus fréquentes rencontrées en mission

Ces dix constats reviennent d'une organisation à l'autre, indépendamment de la taille et du secteur. Ils constituent une grille de relecture rapide de votre propre programme.

- 1. Croire que l'authentification forte règle le sujet.** Elle traite le vol de mot de passe, pas le vol de session. Tant que la question « que se passe-t-il si un jeton valide est utilisé depuis un appareil inconnu » reste sans réponse, l'essentiel du risque demeure.
- 2. Laisser le consentement applicatif ouvert.** Mesure d'une journée, effet majeur, presque toujours absente. C'est le meilleur rapport effort-bénéfice de tout l'écosystème.
- 3. Confondre configuration et application.** Une stratégie en mode rapport depuis un an, un groupe cible vide, des exclusions couvrant la moitié de l'organisation : la règle existe et ne protège personne. Le contrôle se fait sur les journaux, jamais sur l'écran de configuration.
- 4. Ne pas tenir la liste des exclusions.** Elles s'ajoutent une par une, chacune justifiée, et personne n'a la vue d'ensemble. C'est le document le plus révélateur d'un audit, et il n'existe dans aucun portail.
- 5. Ignorer les identités non humaines.** Elles sont souvent plus nombreuses que les identités humaines, échappent à l'authentification forte, et leurs secrets circulent. Un inventaire avec un propriétaire nommé est le préalable, et il manque presque partout.
- 6. Administrer depuis le poste bureautique.** Toutes les mesures de protection des comptes à privilèges sont plafonnées par la sécurité du poste depuis lequel on administre.
- 7. Dimensionner la journalisation sur les valeurs par défaut.** La rétention native est inférieure au délai réel de détection. L'organisation découvre l'écart pendant l'incident, au moment précis où il n'est plus rattrapable.
- 8. Traiter le support informatique comme hors périmètre.** Une réinitialisation de méthode d'authentification obtenue par téléphone contourne l'ensemble du dispositif technique.
- 9. Oublier le chemin hybride.** Les serveurs de synchronisation et de fédération sont des systèmes de niveau zéro. Installés en mode projet, rarement reclassés, ils annulent le bénéfice de tout le reste.
- 10. Produire un rapport sans page de décisions.** Un audit exact qui ne demande rien n'obtient rien. La liste des écarts n'est pas un plan, et un plan sans arbitrage explicite n'est pas exécuté.

Le fil commun

Neuf de ces dix erreurs ne sont pas des erreurs techniques. Ce sont des défauts de gouvernance : absence de propriétaire, absence de date de fin, absence d'inventaire, absence de décision écrite. C'est cohérent avec le constat du chapitre 3 — aucun des chemins d'attaque observés ne repose sur une vulnérabilité logicielle.

La conséquence pour un responsable sécurité est encourageante : l'essentiel du chemin ne dépend pas d'un budget d'acquisition. Il dépend de décisions que vous êtes en position de prendre, et de la discipline à les tenir dans la durée.

ANNEXES

Outils de mise en œuvre

ANNEXE A

Checklist d'audit condensée

Chaque ligne se vérifie par une extraction datée. La colonne implicite à renseigner en face de chacune est la preuve : source, date, méthode.

Privilèges

- Nombre d'attributions permanentes et éligibles de chaque rôle sensible, avec ancienneté
- Comptes à privilèges disposant d'une boîte aux lettres ou d'une licence bureautique
- Existence, configuration et date du dernier test des comptes d'accès d'urgence
- Groupes pouvant attribuer des rôles, et personnes pouvant modifier leur appartenance
- Portée des administrateurs : globale ou restreinte par unité administrative
- Comptes à privilèges dont l'identité est gérée dans l'annuaire local

Authentification

- Répartition des méthodes d'authentification enregistrées, et des méthodes réellement employées sur trente jours
- Authentifications réussies sans méthode forte, par application et par population
- Méthodes résistantes à l'hameçonnage sur les rôles sensibles
- Usage résiduel des protocoles hérités, par compte et par application
- Mécanisme d'authentification forte réellement en vigueur : par utilisateur, valeurs par défaut, ou stratégie d'accès
- Procédure de réinitialisation au support et traçabilité des réinitialisations

Accès conditionnel

- Liste des stratégies, état, date de dernière modification, auteur
- Stratégies en mode rapport seul depuis plus de trois mois
- Liste consolidée des exclusions, par stratégie, avec responsable et date de fin
- Existence d'une stratégie de blocage par défaut
- Traitement spécifique des identités non humaines

Applications et identités non humaines

- Paramétrage du consentement utilisateur et existence d'un circuit de demande
- Applications détenant des permissions d'application de portée large, avec propriétaire et justification
- Applications sans éditeur vérifié, et applications sans activité récente

- Inventaire des principaux de service et des comptes de service humains
- Durées de validité des secrets et certificats, secrets expirés renouvelés sans revue

Collaboration externe

- Population d'invités, dont invités sans authentification depuis quatre-vingt-dix jours
- Paramétrage des invitations et des accès entre organisations
- Partage par lien anonyme : autorisation, durée, périmètre
- Canaux partagés et accords multi-tenants

Données et appareils

- Étiquettes de classification en usage et taux de contenus non classés
- Règles de prévention de fuite : mode, taux de déclenchement, taux de faux positifs
- Règles de transfert automatique de courrier vers l'extérieur
- Parc géré : appareils enregistrés, joints, conformes, et critères de conformité appliqués
- Ressources exigeant un appareil conforme

Journalisation et hybride

- Durée de conservation effective par famille de journaux, et destination d'export
- Contrôle d'accès distinct sur l'espace de conservation
- Inventaire et classification des composants de synchronisation et de fédération
- Fédération résiduelle déclarée dans la configuration du tenant
- Ancienneté des secrets et clés des composants de jonction

ANNEXE B

Matrice licences et contrôles

Cette annexe donne la structure du raisonnement, non l'état commercial du moment : les offres, les noms et les seuils évoluent. Vérifiez toujours l'état applicable à votre contrat avant d'engager une décision budgétaire.

Socle sans licence premium

Blocage des protocoles hérités par la configuration des services. Paramétrage du consentement applicatif. Gestion des invitations et du partage externe. Valeurs par défaut de sécurité pour les petites organisations. Journalisation à rétention native. Comptes d'accès d'urgence. Séparation des comptes d'administration. Postes d'administration dédiés.

Autrement dit : une part significative des chapitres 11, 12, 14 et 16 ne dépend d'aucune licence supplémentaire.

Premier niveau premium d'annuaire

Accès conditionnel, y compris exigence d'appareil conforme et exigence de méthode résistante à l'hameçonnage. Écriture différée de certaines opérations en environnement hybride. Rétention étendue des journaux d'annuaire.

C'est le seuil structurant : sans accès conditionnel, la politique d'accès du chapitre 13 n'existe pas.

Second niveau premium d'annuaire

Élévation temporaire de privilèges avec approbation et notification. Revues d'accès. Protection fondée sur le risque et stratégies associées.

Ce seuil conditionne les chapitres 11 et 24 dans leur forme automatisée. En son absence, les mêmes objectifs se traitent manuellement, avec un coût de fonctionnement supérieur et une couverture moindre.

Gouvernance des identités

Gestion des droits d'utilisation, flux de cycle de vie, revues avancées. Correspond au chapitre 24 dans sa forme industrialisée.

Identités de charge de travail

Application de conditions d'accès aux principaux de service. Correspond au dernier point du chapitre 15, et il n'existe pas d'équivalent manuel.

Niveau supérieur des suites de collaboration

Classification automatique, prévention de fuite étendue, capacités avancées de détection et d'investigation, rétention d'audit prolongée. Correspond aux chapitres 17, 20 et 21.

Comment présenter l'arbitrage

Pour chaque seuil, trois éléments : les mesures qu'il débloquent, le risque qu'elles couvrent, et l'alternative manuelle avec son coût de fonctionnement annuel. C'est la seule présentation qui permette à une direction générale de décider en connaissance de cause plutôt que de comparer deux prix.

ANNEXE C

Modèle de rapport

Structure à reprendre telle quelle. Les longueurs indiquées sont des maxima.

Page 1 — Verdict

Une phrase de conclusion sur le niveau d'exposition, formulée en termes de conséquence et non de conformité. Trois faits d'audit qui la soutiennent, datés. Une échéance : la date à laquelle la situation aura changé si les décisions demandées sont prises.

Pages 2 à 3 — Scénarios

Trois scénarios au maximum, chacun sur un tiers de page : la séquence d'attaque, les faits d'audit qui la rendent possible dans votre environnement, l'impact attendu, et le contrôle qui la couperait.

Pages 4 à 5 — Plan par vagues

Trente jours, quatre-vingt-dix jours, cent quatre-vingts jours et au-delà. Pour chaque action : intitulé en une ligne, responsable pressenti, effort estimé en jours-homme, risque couvert. Pas de dates au jour près, pas de dépendances détaillées.

Page 6 — Décisions demandées

Trois à cinq décisions formulées pour recevoir un oui ou un non, chacune avec l'option retenue par défaut en l'absence de décision. Exemples de formulation : accepter l'impact utilisateur de l'exigence d'appareil conforme sur telle population ; financer tel niveau de licence pour couvrir tel risque ; désigner tel propriétaire de la configuration d'identité ; accepter formellement le risque résiduel sur tel périmètre jusqu'à telle date.

Annexe technique

Constats détaillés par domaine, dans l'ordre de la checklist de l'annexe A. Pour chaque constat : énoncé, preuve avec source et date, criticité et son justificatif, recommandation, effort. Aucune limite de taille.

Ce qui ne figure pas dans le rapport

Le score de la plateforme en couverture. Les captures d'écran de portails. Les explications de fonctionnement des produits. La liste exhaustive des écarts en corps de rapport. Les recommandations non chiffrées.

ANNEXE D

Glossaire

Accès conditionnel. Mécanisme évaluant, à chaque tentative d'accès, un ensemble de conditions — identité, appareil, application, origine, risque — pour accorder, refuser ou renforcer l'accès.

Appareil conforme. Appareil géré satisfaisant les règles de conformité définies par l'organisation, et pouvant être exigé comme condition d'accès.

Comptes d'accès d'urgence. Comptes à privilèges réservés aux situations de blocage, exclus des stratégies susceptibles de les empêcher de fonctionner, et étroitement surveillés.

Consentement. Acte par lequel un utilisateur ou un administrateur accorde à une application des permissions sur des données ou des fonctions.

Élévation temporaire de privilèges. Attribution d'un rôle activée à la demande pour une durée limitée, plutôt que détenue en permanence.

Évaluation continue d'accès. Mécanisme réévaluant une session en cours lorsqu'un événement significatif survient, sans attendre l'expiration du jeton.

Fédération. Délégation de l'authentification à un fournisseur d'identité tiers, qui émet des assertions attestant de l'identité de l'utilisateur.

Hameçonnage avec relais. Technique interceptant une session complète en relayant en temps réel la page d'authentification légitime, permettant le vol du cookie de session malgré une authentification forte.

Identité managée. Identité applicative dont le secret est géré par la plateforme et jamais exposé.

Jeton d'accès. Artefact délivré après authentification, présenté à l'application pour obtenir l'accès.

Jeton de rafraîchissement. Artefact permettant d'obtenir de nouveaux jetons d'accès sans réauthentification ; sa révocation est nécessaire pour couper réellement un accès.

Méthode résistante à l'hameçonnage. Méthode d'authentification dont la preuve est liée à l'origine du site, ne pouvant donc être rejouée par un relais.

Permission déléguée. Permission exercée au nom d'un utilisateur connecté, bornée par les droits de cet utilisateur.

Permission d'application. Permission exercée sans utilisateur, à la portée accordée, potentiellement sur l'ensemble du tenant.

Principal de service. Instance d'une application dans un tenant, avec ses permissions et ses moyens d'authentification.

Tenant. Instance d'annuaire dédiée à une organisation, unité de sécurité de l'écosystème.

Unité administrative. Objet permettant de restreindre la portée d'un administrateur à une population donnée.

Zéro confiance. Modèle d'architecture reposant sur la vérification explicite, le moindre privilège et la présomption de compromission.

Résumé

Un tenant Microsoft 365 comporte plusieurs centaines de réglages de sécurité répartis dans une demi-douzaine de consoles. Aucun responsable de la sécurité ne peut tous les connaître — et il n'en a pas besoin.

Ce guide répond à la seule question qui compte en comité de direction : où en sommes-nous vraiment, qu'est-ce qui nous expose, et dans quel ordre faut-il corriger ?

Construit comme une mission d'audit, il conduit le lecteur de la compréhension de la surface d'attaque identitaire à la gouvernance dans la durée, en passant par une méthode d'évaluation reproductible, une hiérarchie de correction fondée sur le rendement réel des contrôles, et un dispositif de détection dimensionné pour l'investigation. Chaque chapitre se termine par les arbitrages qui reviennent au responsable sécurité et que personne ne prendra à sa place.

Frédéric PEREZ est architecte en gestion des identités et des accès, et consultant indépendant en sécurité des environnements Microsoft. Il conduit des missions d'audit et de gouvernance identitaire en France, en Belgique et au Luxembourg.