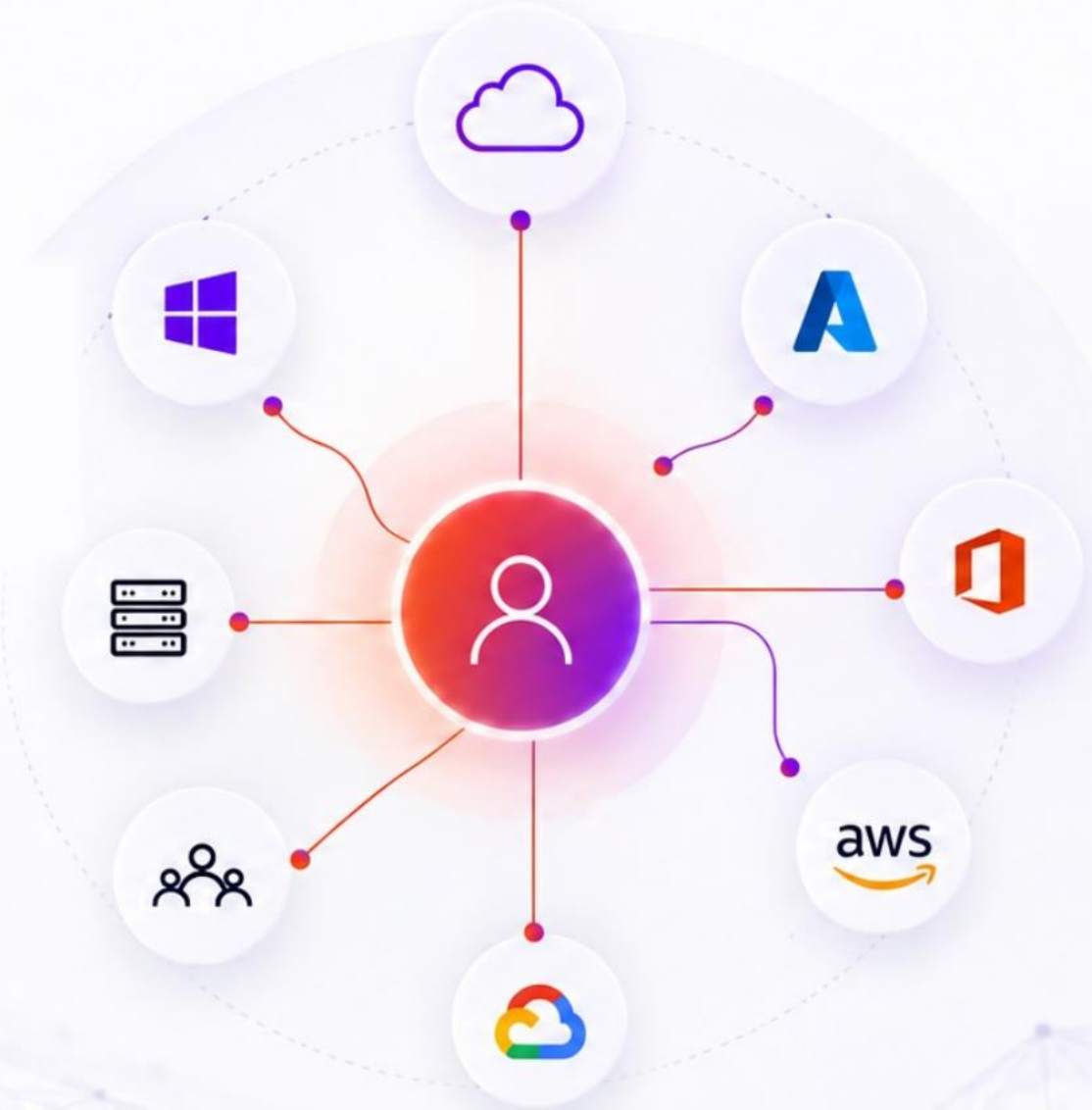
SAPORO
ORDER IN CHAOS

IDENTITY DAYS 2026

Sécuriser Active Directory et Microsoft Entra ID en 2026

Cartographie des chemins d'attaque et validation continue du tiering

Mardi 20 octobre 2026 · 12h00 · Salle NEO-GEO · Niveau 200



Votre intervenant aujourd'hui



Nicolas Lagrange

Head of Solution Engineering

- 8 ans auprès des équipes sécurité et IT, consultant puis Saporo
- De la cartographie à la remédiation, aux côtés des équipes AD et cloud
- Comprendre comment l'attaquant progresse pour couper ses chemins

SAPORO
ORDER IN CHAOS

- Scale-up suisse basée à Lausanne
- Des clients allant des grands groupes aux ETI
- Cartographie des chemins d'attaque liés aux identités
- AD, Entra ID, Azure, AWS, Okta, M365, ADCS
- Sans agent, accès en lecture seule

SAPORO
ORDER IN CHAOS

De la réaction à la protection préventive des identités



SAPORO
ORDER IN CHAOS

Au programme

01

Anatomie des chemins

Quatre chemins réels entre AD et Entra ID

02

Points de convergence

Corriger peu pour supprimer beaucoup

03

Tiering

Une règle pour garder le contrôle dans la durée

04

Référentiels et exploitabilité

ANSSI et CIS face au graphe

05

À retenir et questions

Cinq actions, puis vos questions

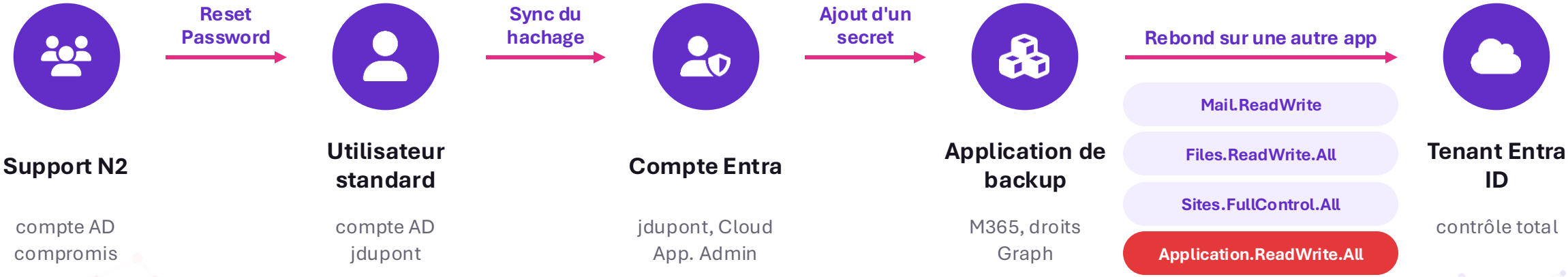
Fil conducteur : voir les chemins, savoir où couper, tenir dans la durée

SAPORO
ORDER IN CHAOS

01 · ANATOMIE DES CHEMINS

Chemin 1 : un utilisateur standard, admin dans Entra ID

Un compte AD standard, synchronisé, a reçu un rôle d'administration Entra : un chemin hybride s'ouvre.



Support N2

compte AD compromis

Utilisateur standard

compte AD jdupont

Compte Entra

jdupont, Cloud App. Admin

Application de backup

M365, droits Graph

Tenant Entra ID

contrôle total

SAPORO
ORDER IN CHAOS

01 · ANATOMIE DES CHEMINS

Chemin 2 : une GPO d'imprimantes jusqu'au domaine

Pour gérer les imprimantes, une GPO accorde aux utilisateurs le droit de charger des pilotes sur les postes.



Utilisateur standard

session sur un poste partagé

Poste partagé

SYSTEM via un pilote

Technicien support

session ouverte sur le poste

Admins serveurs

serveurs et DC confondus

Contrôleur de domaine

administré par le même groupe

SAPORO
ORDER IN CHAOS

01 · ANATOMIE DES CHEMINS

Chemin 3a : un certificat au nom d'un Domain Admin

ADCS déployé, une autorité de certification qui accepte un SAN libre dans les requêtes.



Condition : DC sans strong mapping des certificats (KB5014754), ou extension SID désactivée (ESC16)

SAPORO
ORDER IN CHAOS

Chemin 3b : un modèle de certificat modifiable

Plus discret : aucun modèle n'est vulnérable, mais une erreur de droits permet à tout utilisateur d'en modifier un.



Utilisateurs du domaine

droit accordé par erreur

Modèle de certificat

configuration conforme

Modèle modifié

SAN fourni par le demandeur

Autorité de certification

émet sans contrôle

Certificat admin

au nom d'un Domain Admin

Domaine AD

authentification sur un DC

Invisible pour un audit de configuration : le modèle reste conforme jusqu'à ce que quelqu'un le modifie

SAPORO
ORDER IN CHAOS

01 · ANATOMIE DES CHEMINS

Chemin 4 : un provisioning RH mal cloisonné

Des délégations faites pour automatiser les arrivées, jamais revues.



jmartin	Groupe RH	OU SIRH	Connecteur SIRH	sys_admin_ad	Admins du domaine
gestionnaire RH	GG_RH	délégation RH	svc_sirh	admins AD délégués	contrôle total

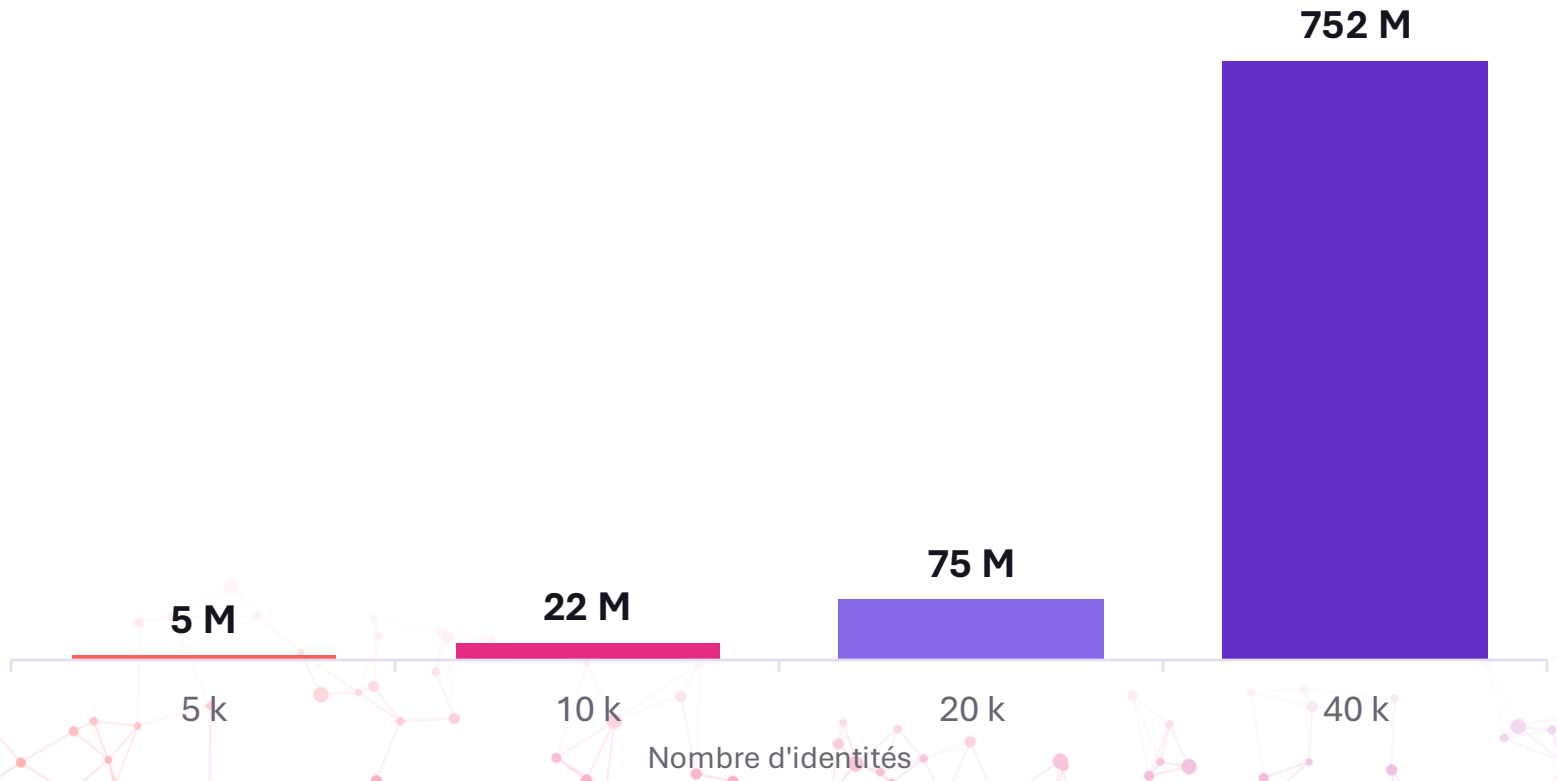
5 relations toutes justifiées par un besoin métier, aucune alarmante

400 909 chemins issus d'objets mal configurés, chez un client de 11 000 objets

? lequel corriger en premier, sans casser la production ?

SAPORO
ORDER IN CHAOS

Traiter les chemins d'attaque à grande échelle est essentiel



Plus de chemins vers
les actifs critiques

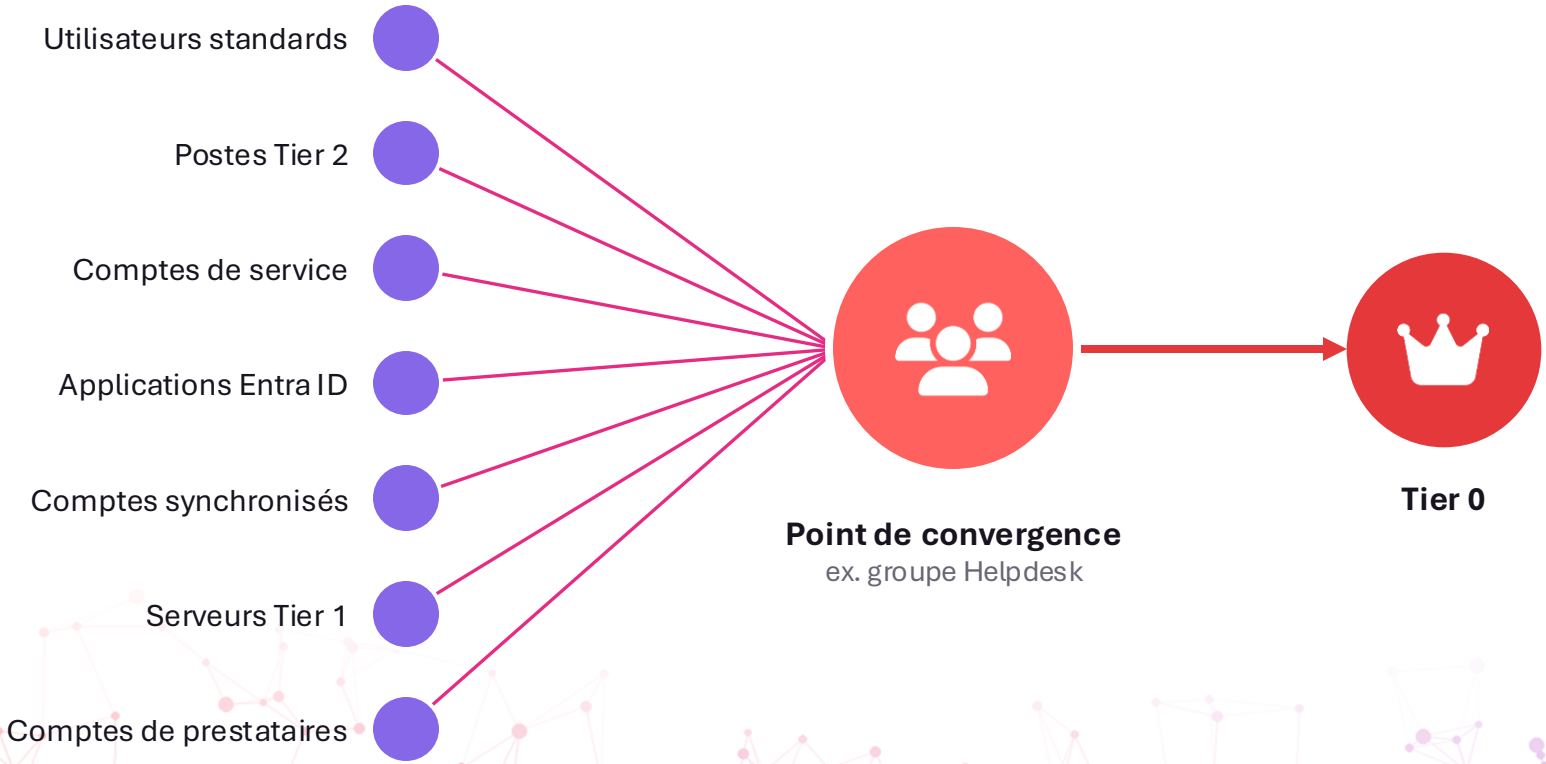
Plus difficile de voir
ce qui compte

La priorisation
est essentielle

02 · POINTS DE CONVERGENCE

Corriger le point de convergence, pas chaque chemin

Des milliers de chemins transitent souvent par quelques objets. C'est là qu'une correction a le plus d'effet.



1 correction

supprime tous les chemins qui transitent par ce point, quelle que soit leur origine.

SAPORO
ORDER IN CHAOS

03 · TIERING

Le tiering : rendre le problème gérable dans la durée

CLASSER CHAQUE OBJET

Tier 0
DC, Entra Connect, ADCS, rôles Entra privilégiés

Tier 1
Serveurs et applications métier

Tier 2
Postes et utilisateurs

contrôle descendant

CE QUE ÇA CHANGE DANS LA DURÉE

1 **Deux règles simples**
Pas de contrôle vers le haut, pas de connexion d'admin vers le bas. Chaque violation devient lisible.

2 **Des coupes évidentes**
On coupe là où un chemin change de niveau, pas à chacun de ses sauts.

3 **Une règle qui tient**
Chaque nouveau droit, compte ou session se vérifie contre le modèle, à chaque évaluation.

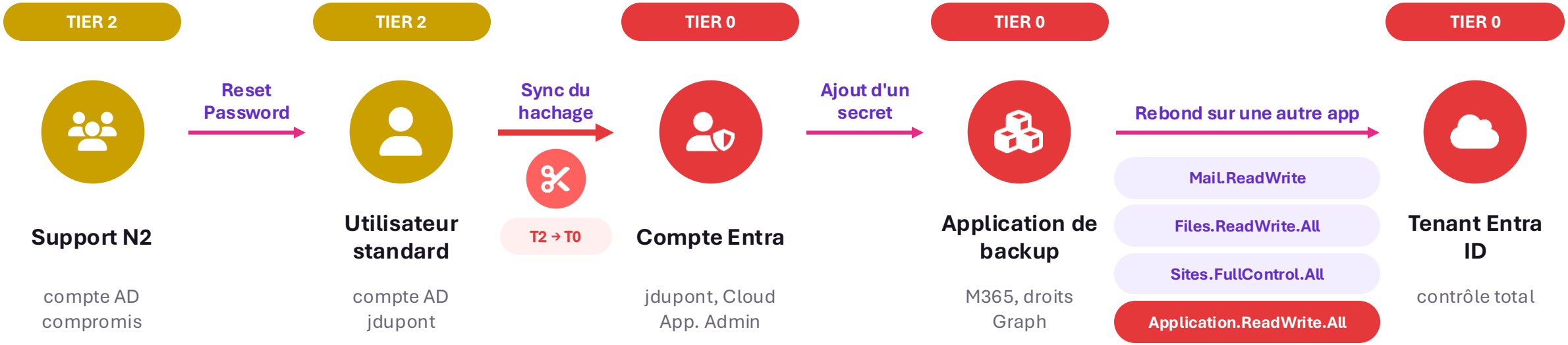
Aucun chemin vers un niveau supérieur, aucune session d'admin sur un niveau inférieur

SAPORO
ORDER IN CHAOS

03 · TIERING

Chemin 1, vu par le tiering : où couper

jdupont est un utilisateur standard (Tier 2), son identité Entra porte un rôle Tier 0 : la synchronisation crée la violation.



Coupe prioritaire : aucun rôle Entra privilégié sur un compte synchronisé depuis l'AD

SAPORO
ORDER IN CHAOS

03 · TIERING

Chemin 2, vu par le tiering : où couper

Sans tiering, admins serveurs et admins du domaine ne faisaient qu'un : le même groupe administrait serveurs et DC.



Coupes : SeLoadDriverPrivilege, GenericAll du support, un groupe dédié seul admin des DC

SAPORO
ORDER IN CHAOS

03 · TIERING

Chemin 3a, vu par le tiering : où couper

S'inscrire est normal. La faille : l'autorité accepte un SAN libre, donc un certificat au nom de n'importe qui.



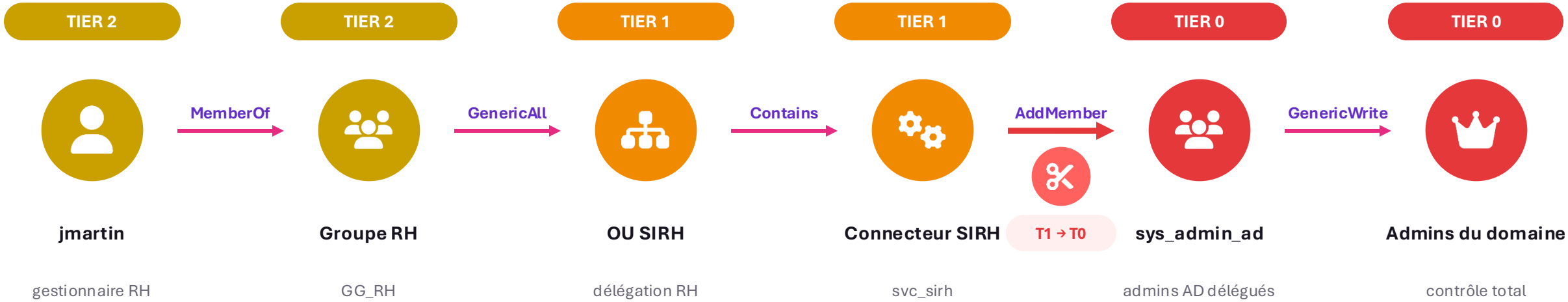
Coupe prioritaire : retirer le flag EDITF_ATTRIBUTESUBJECTALTNAME2 de l'autorité de certification

SAPORO
ORDER IN CHAOS

03 · TIERING

Chemin 4, vu par le tiering : où couper

Le connecteur SIRH (Tier 1) peut modifier sys_admin_ad (Tier 0) : un compte applicatif devient Tier 0 de fait.



Coupe prioritaire : retirer au connecteur SIRH le droit de gérer sys_admin_ad

SAPORO
ORDER IN CHAOS

03 · TIERING

Une dérive visible le lendemain, pas à l'audit suivant

Le tiering est conforme le jour de la revue. Il peut ne plus l'être après le premier changement non maîtrisé.

J0

Revue de tiering

Aucun chemin Tier 1 ou Tier 2 vers le Tier 0.

J+30

Changement projet

Le groupe SRV-Admins (Tier 1) reçoit le droit de modifier une GPO liée à l'OU des contrôleurs de domaine.

J+31

Évaluation planifiée

Nouveau chemin Tier 1 vers Tier 0 détecté. Le responsable du tiering est alerté.

J+32

Correction validée

Délégation retirée après vérification du Business Impact. L'évaluation suivante confirme zéro chemin.

Sans revalidation planifiée, cette dérive reste ouverte jusqu'au prochain audit, souvent un an plus tard

SAPORO
ORDER IN CHAOS

Conformité et exploitabilité se complètent

CONFIGURATION ATTENDUE

ANSSI · CIS Benchmarks

Ce qui doit être vrai : administration cloisonnée, paramètres durcis, comptes dédiés.

La règle est-elle respectée ?

EXPOSITION RÉELLE

Chemins d'attaque

Ce qui est atteignable aujourd'hui depuis une identité compromise, jusqu'au Tier 0.

La cible est-elle atteignable ?

Les contrôles indiquent ce qui doit être corrigé. Les chemins montrent ce qui peut réellement être atteint.

SAPORO
ORDER IN CHAOS

04 · RÉFÉRENTIELS ET EXPLOITABILITÉ

Tout est conforme, et le Tier 0 reste atteignable

CONTRÔLES DE CONFIGURATION

4 / 4 conformes

- Admins du domaine : 3 comptes nominatifs
- Comptes privilégiés dans Protected Users
- LAPS déployé sur tous les postes
- MFA sur les rôles Entra privilégiés

CHEMIN D'ATTAQUE

Toujours ouvert

svc-backup
aucun groupe sensible, ignoré par les contrôles

GenericWrite

GPO Default Domain Controllers Policy
appliquée à tous les contrôleurs de domaine

Appliquée aux DC

Contrôleurs de domaine
exécution de code en SYSTEM

SAPORO
ORDER IN CHAOS

05 · À RETENIR

Cinq actions à lancer dès lundi

Chacune coupe une famille de chemins, pas un chemin isolé.

1 CHEMIN 1

Comptes admin cloud-only

Aucun rôle Entra privilégié sur un compte synchronisé depuis l'AD.

2 CHEMIN 2

Auditer les droits des GPO

Chercher SeLoadDriverPrivilege et les autres droits locaux sensibles accordés aux utilisateurs.

3 CHEMIN 3

Verrouiller ADCS

Retirer le flag SAN de l'autorité, auditer qui peut modifier les modèles de certificat.

4 CHEMIN 4

Comptes de service

Revue en profondeur des processus internes (SIRH, provisioning) et des droits de leurs comptes de service.

5 TIERING

Classer, puis revalider

Classer chaque objet dans un tier et revérifier les chemins à chaque changement.

SAPORO

ORDER IN CHAOS

SAPORO

Audit gratuit de vos identités

Gratuit

Évaluation des risques sur votre environnement AD et Entra ID

1 heure

de déploiement : une VM Linux chez vous

0 agent

Comptes en lecture seule, rien à installer sur vos serveurs

Vous repartez avec vos chemins d'attaque les plus critiques, vos points de convergence et vos écarts de tiering. Et nous vous aidons à les corriger.

Venez me voir après la session, ou écrivez-moi à nicolas@saporo.io

SAPORO
ORDER IN CHAOS

Merci

Des questions ?



Démo à 14h, salle SEGA

Nicolas Lagrange
Head of Solution Engineering, Saporo

nicolas@saporo.io

saporo.io