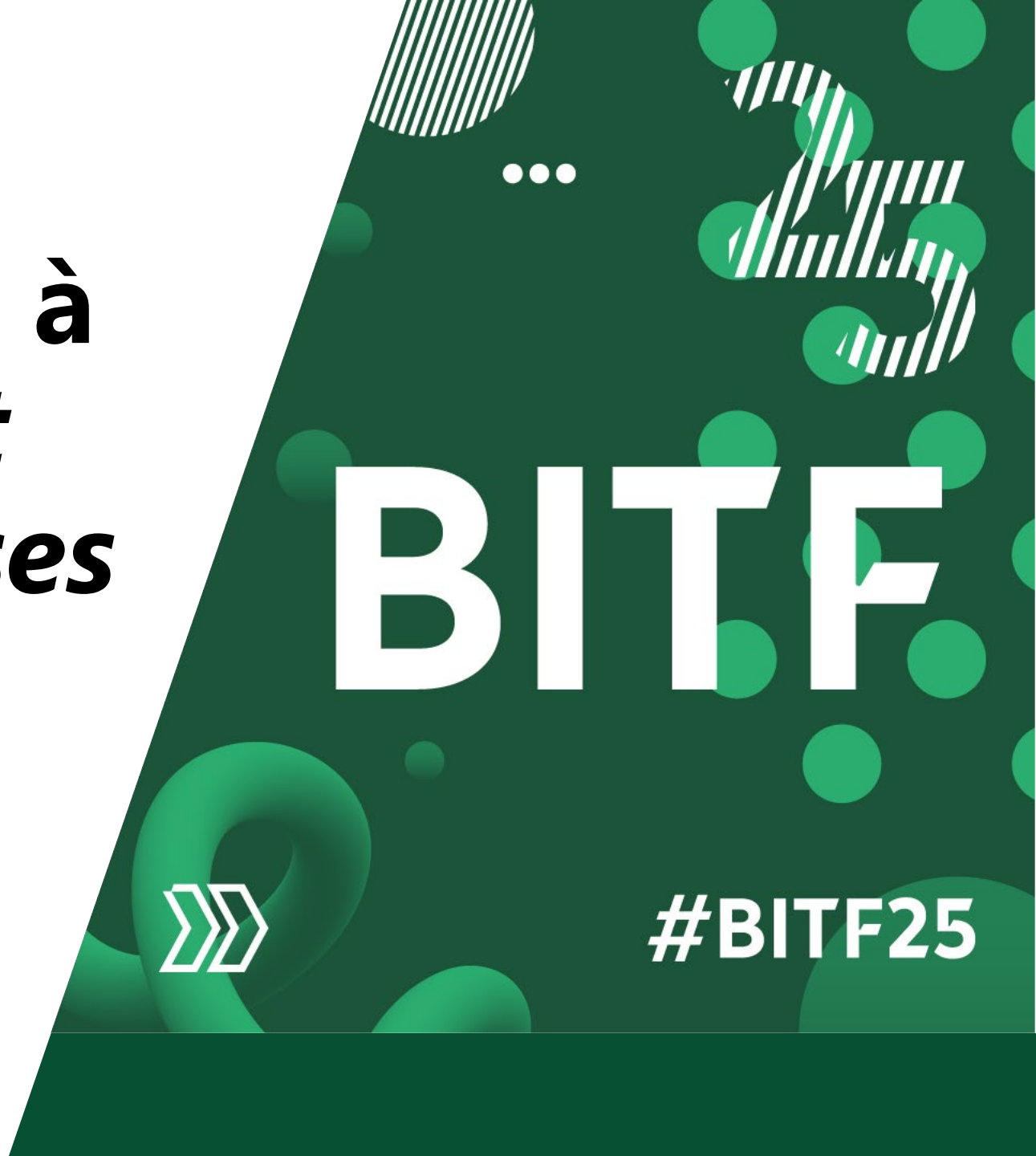
Vos identités sont à risques: *Comment construire des bases solides?*

Rita Dib – *Security Consultant, Bechtle Suisse*

Nicolas Lagrange – *Director Solution Engineer, Saporo*

Bechtle IT Forum, Lausanne.

24.06.2025



Agenda

Sujet:

Vos identités sont à risque, comment les sécuriser?

Ce que l’on couvrira aujourd’hui:

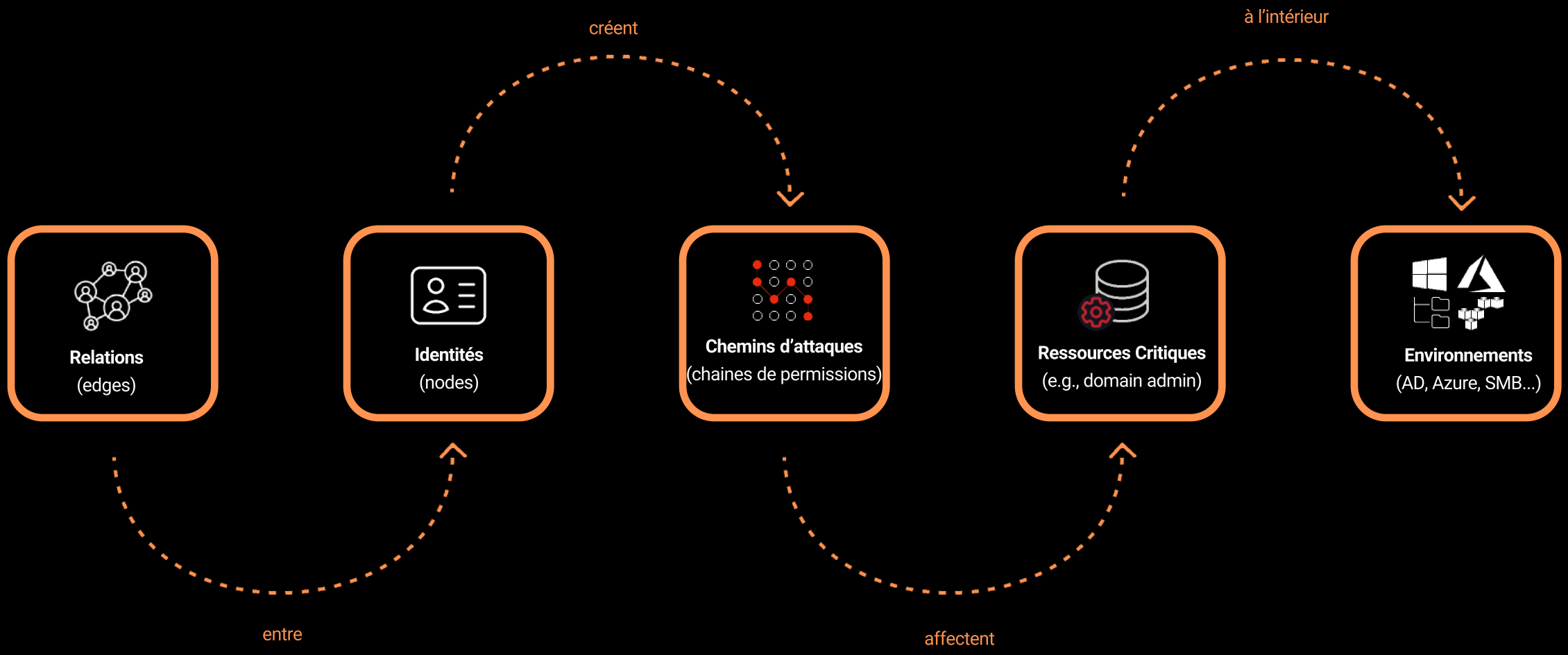
- Pourquoi est-il urgent de sécuriser vos environnements Active Directory et Azure?
- Principaux challenge
- Comment sécuriser les identités
- Comment Saporo & Bechtle vous aident à adresser ces challenges
- Live-Demo: Découvrez les risques cachés avec Saporo
- Q&A

Pourquoi est-il urgent de sécuriser vos environnements Active Directory et Azure?

L'identité est la première surface d'attaque.
Saporo renforce proactivement la posture de sécurité des identités critiques sur les environnements clés de votre infrastructure IT contre les cyberattaques.

Microsoft Active Directory · ADCS · SMB Shares · Azure · M365 · amazon web services · okta

Pourquoi est-il urgent de sécuriser vos environnements Active Directory et Azure?

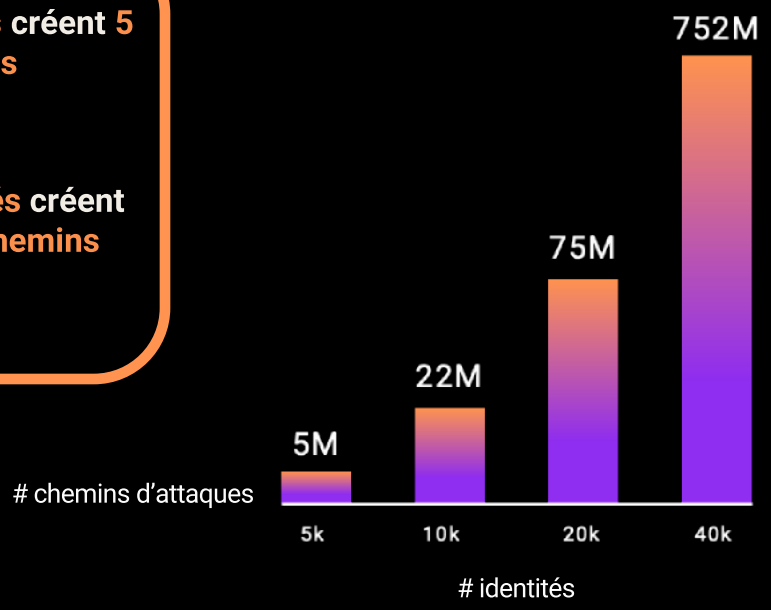


Pourquoi est-il urgent de sécuriser vos environnements Active Directory et Azure?

Le risque est massif et exponentiel

5’000 identités créent 5 million chemins d’attaques

40’000 identités créent 752 millions chemins d’attaques



SOURCE: FORESTALL; XM CYBER; AWS MARKETPLACE

Contextualiser et prioriser est essentiel

- Les chemins d'attaque permettent aux défenseurs de voir leur environnement comme des attaquants. Les attaquants n'ont besoin de trouver qu'un seul chemin vers les actifs critiques. Les défenseurs doivent tous les suivre pour mieux anticiper et se préparer.
- Les chemins d'attaque peuvent aider à prioriser tous types de découvertes, comme les mauvaises configurations, les vulnérabilités, les détections et les IoC. Cela permet aux défenseurs de connaître l'impact d'une découverte.
- Les attaquants rentrent dans 95% du temps. C'est pourquoi il est essentiel de séparer les actifs critiques de la plupart des objets (par exemple: les utilisateurs) afin d'atténuer les brèches.

Comment sécuriser les identités ?

Organisation et gouvernance	Gestion du **cycle de vie** des identités, en définissant rôles, responsabilités et processus de validation. Garantir un suivi régulier des droits et une prise de décision partagée entre IT, métiers et sécurité.
Renforcement de la sécurité	Appliquer des mesures de **durcissement** sur l'Active Directory et Entra ID. Renforcer et contrôler régulièrement les **configurations** et réduire la surface d'attaque.
Administration sécurisée	Séparer les environnements d'administration et limiter les droits selon le modèle en tiers (**Tier Model**). Assurer la traçabilité et le contrôle des actions d'administration pour réduire les erreurs ou les compromissions.
Continuité	Garantir la **disponibilité** et la **résilience** des services d'identité avec des plans de reprise et des sauvegardes sécurisées et isolées. Prévoir des procédures de restauration claires et testées.
Conformité	S'assurer que les processus et les pratiques respectant les **exigences réglementaires** (LPD, ISO 27001, etc.) et les standards de sécurité.

Cycle de vie des identités

Création > **Mobilité** > **Départ**

Attribution des droits selon le rôle en respectant le principe du moindre privilège

Revoir et modifier les droits

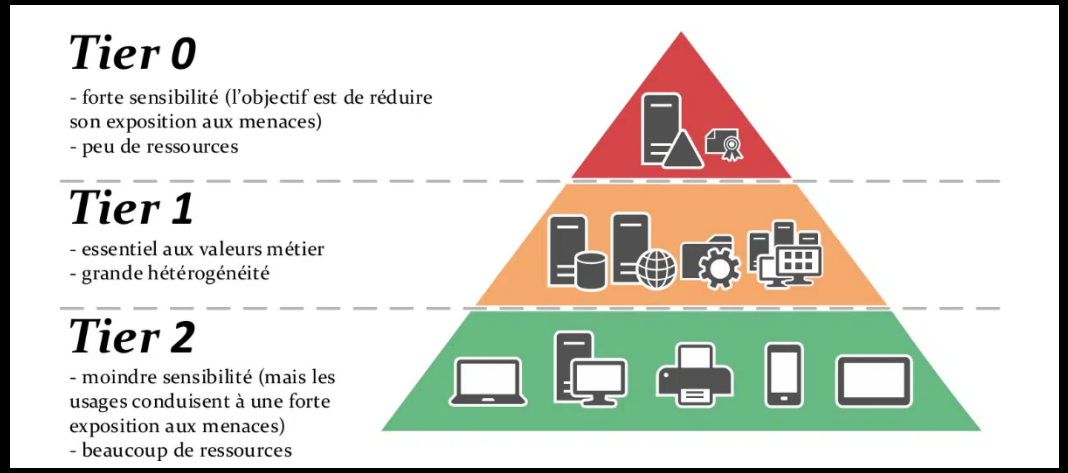
Désactiver le compte et retirer ses droits

Revue régulière

Administration de l'Active Directory et Entra ID

Architecture en Tiering Model

Le principe du modèle en tier d'administration est de cloisonner au maximum son infrastructure Active Directory pour se prémunir en cas d'attaque informatique.



Administration dédiée

Les comptes d'administration doivent être dédiés à chaque Tiers de l'AD pour limiter le nombre des comptes exposés, limiter les privilèges au strict nécessaire et garantir que les comptes d'administrateurs soient utilisés uniquement pour des tâches de gestion spécifiques.
Des restrictions d'ouverture de session doivent être appliquées pour garantir que les comptes à privilèges élevés n'aient pas accès aux ressources moins sécurisées et que les comptes d'administration des Tiers 1 et 2 n'aient pas accès aux ressources les plus sensibles.

Équipements dédiés

Une station d'administration dédiée à chaque Tiers et à chaque administrateur. Les postes d'administration à privilèges élevés bénéficient d'une sécurisation renforcée.

Supervision et alerte continue

Sécuriser les identités, c’est un chantier **permanent** : d’abord on construit, ensuite on **pilote** et on **améliore**.

Réaliser des audits réguliers et des tests d'intrusion sur l’annuaire Active Directory et Entra ID. Définir après chaque audit un plan d'actions et appliquer les mesures de sécurité correspondantes.

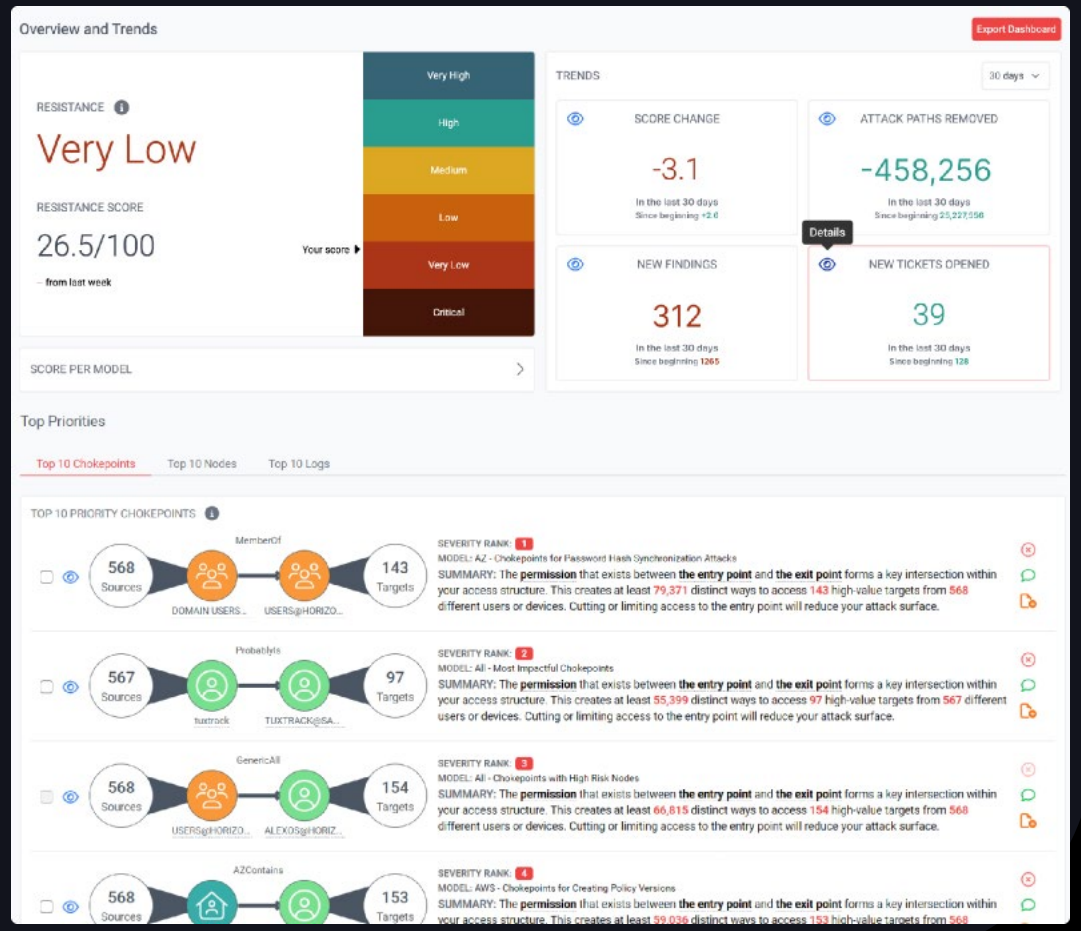
Définir des indicateurs clés à suivre (Nombre de comptes à privilèges, nombre de comptes dormants, taux de conformité aux revues de droits…) et ajuster le processus pour respecter les seuils de sécurité.

Activer la journalisation des évènements sensibles (ajout/suppression dans des groupes, modifications de droits, connexions admin) et configurer des alertes en temps réel sur les actions à risque.

Comment Saporo vous aide à adresser ces challenges

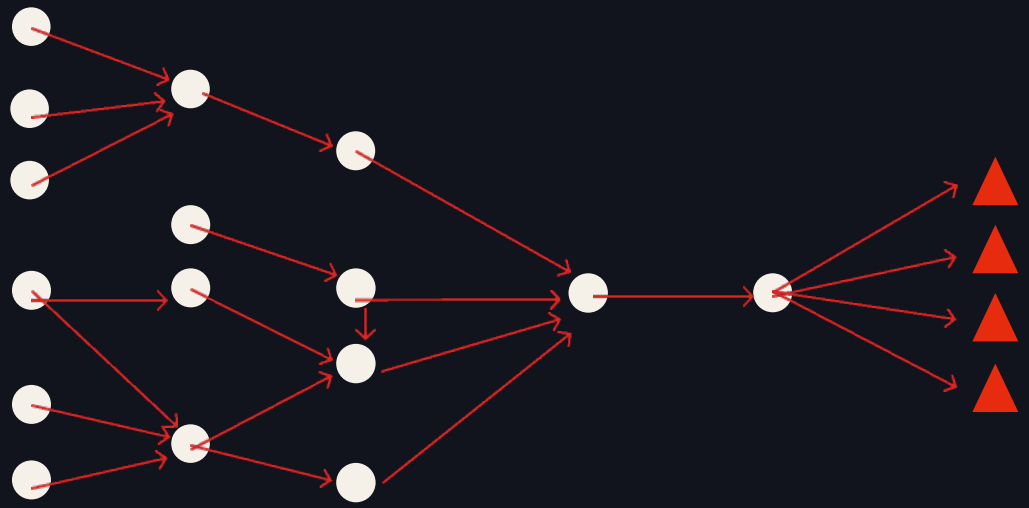
Visibilité complète et diagnostique

- **Segmentation des identités** vers les objets critiques pour **fermer les brèches**
- **Découverte automatique des chemins d'attaque** à grande échelle pour **prioriser les risques**
- **Trouver les mauvaises configurations** pour **réduire les opportunités des attaquants**
- **Montrer les changements** en continu pour **empêcher** toute hausse future du **risque**
- **Corriger** les résultats plus simplement grâce à de l'**IA embarquée**

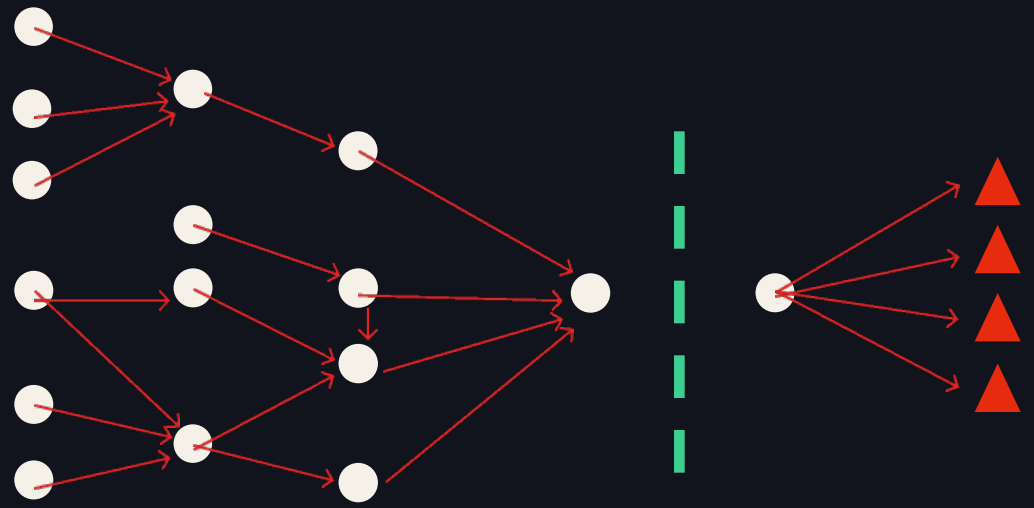


Comment Saporo vous aide à addresser ces challenges

De millions de chemin d'attaque...



...à aucun - en un seul changement.

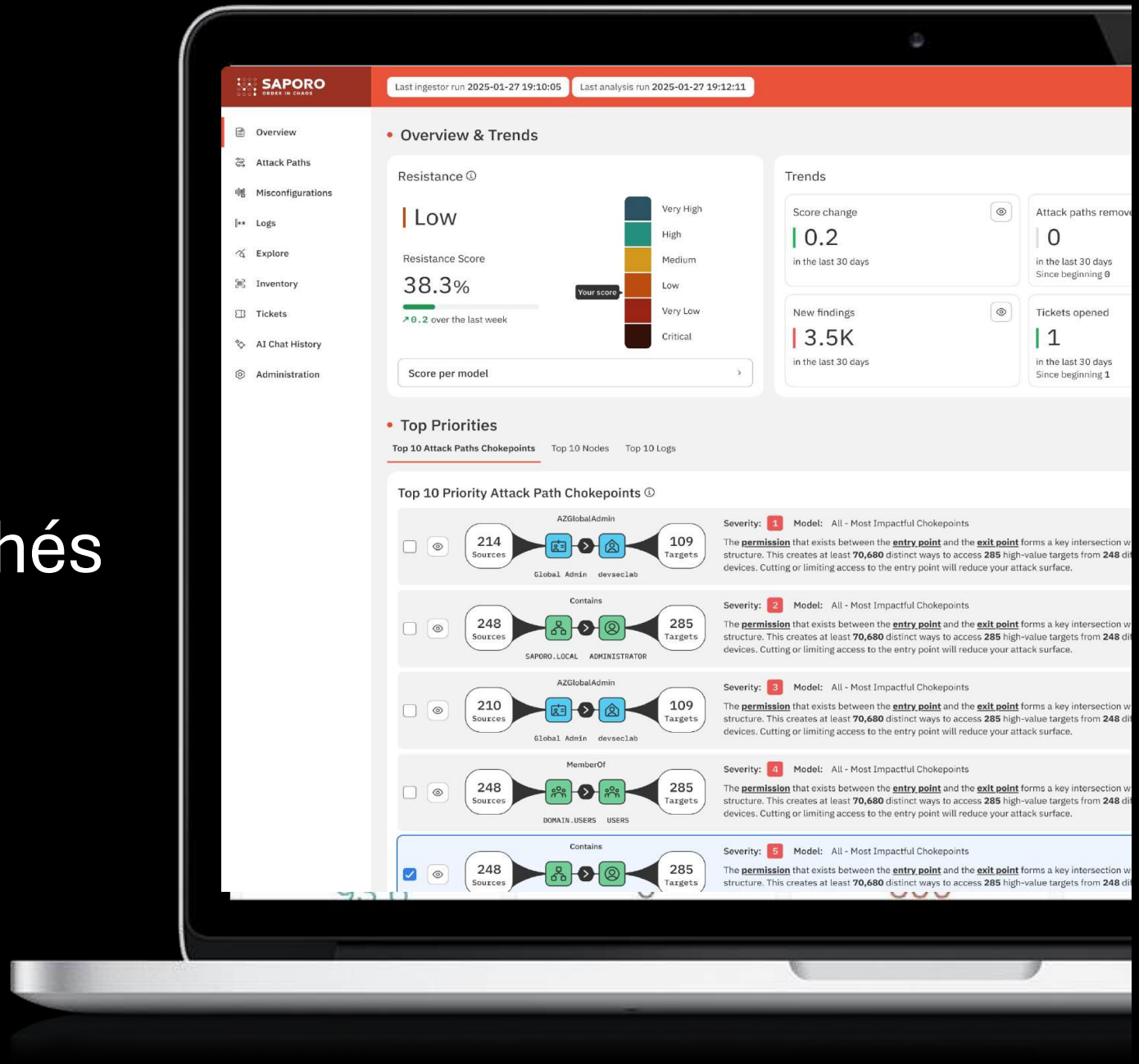


Objet standard

Asset critique

Live-Demo

Découvrez vos risques cachés avec Saporo



Active Directory Remediation.

bechtle

Notre offre basée sur une approche structurée, orientée vers la réduction du niveau de risque, l'amélioration de la posture de sécurité et le renforcement des contrôles critiques, vise à corriger les vulnérabilités identifiées dans l'environnement Active Directory.

- L'intervention inclut :
  - La priorisation des actions correctives, en fonction de leur impact et de leur faisabilité
  - L'accompagnement technique à la remédiation, en lien avec les équipes internes
  - La mise en œuvre de bonnes pratiques de sécurité AD (délégation, gestion des comptes, durcissement)
  - Le suivi des actions dans une logique de plan de remédiation piloté
  - Des recommandations techniques et organisationnelles pour limiter les régressions
  - La montée en compétence des administrateurs AD du client

SAPORO
ORDER IN CHAOS

Active Directory Tiering Model.

bechtle

L'offre Tiering Model AD a pour objectif de mettre en œuvre un modèle de segmentation logique des accès et des privilèges dans Active Directory, afin de réduire les risques de compromission latérale et de renforcer les barrières de sécurité internes.

- L'approche s'appuie sur les préconisations de Microsoft (Tier 0, 1, 2) et comprend :
  - La cartographie des comptes, groupes, machines et accès par niveau de sensibilité
  - La définition et mise en œuvre du modèle de Tiering (architecture, segmentation, séparation des rôles…)
  - Identification et mise en place des Privilege Access Workstation (PAW)
  - Accompagnement au changement et à l'adoption du fonctionnement du Tiering model

× SAPORO ORDER IN CHAOS

bechtle

Des **questions?**

Venez nous rendre visite sur notre stand.


bechtle