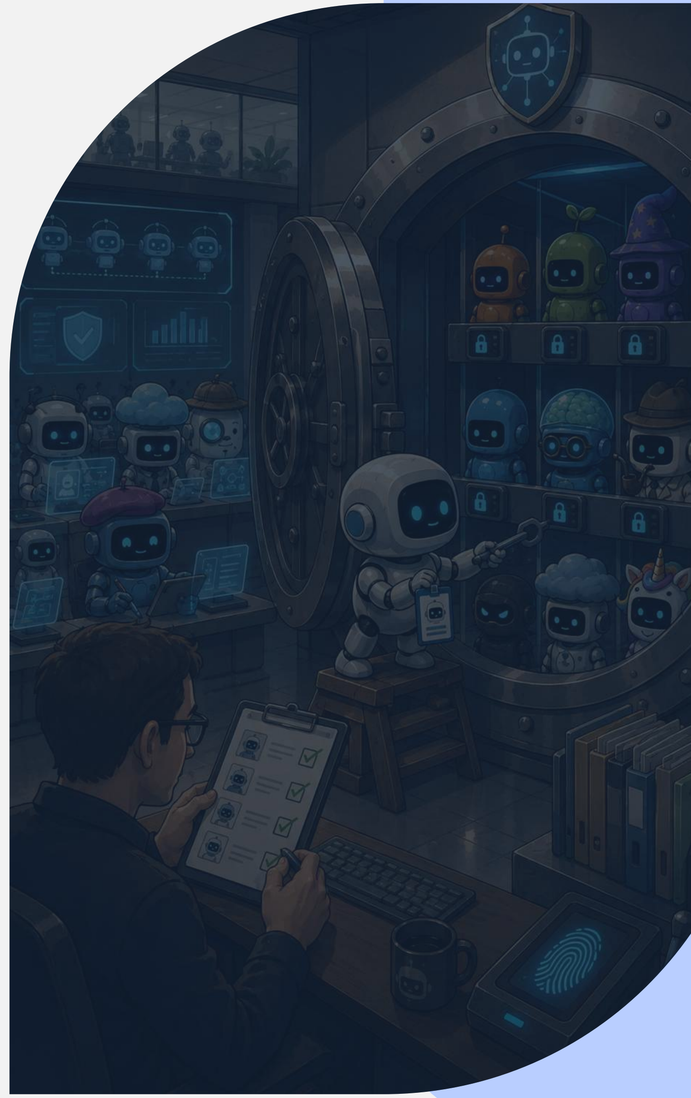
IDENTITY DAYS

20 octobre 2026

PARIS

Gouvernance AIAM

de la théorie à la pratique



Éric PÉRION | Partner Cyber, Canada & Amérique du Nord
Marcellin NACHIN | Leader IAM

onepoint.

IDENTITY DAYS

Éric PÉRION
Partner Cyber
Canada et Amérique du Nord

Marcellin NACHIN
Leader IAM

Notre biographie n'étant pas passionnante (et si ca vous intéresse tant, venez nous voir après, on vous racontera tout ça) **on préfère vous introduire plutôt notre bébé :**

Agenda

01 Arrêtons de dire qu'un agent est une NHI...

02 Les limites de l'IAM actuelle avec les agents (car ce ne sont pas simplement des NHI!)

03 Les risques amenés par ces limites

04 Le rôle de la gouvernance pour encadrer ces risques...

05 ... et sa mise en place dans une architecture adaptée...

06 ... exécutée dans SpiceDB

Et là on va passer sur du *hands-on* car on en aura marre d'entendre parler Éric!

Les agents IA : un nouveau type d'identité

Sam ARCHEURAPA

Stagiaire boosté à la caféine

3 mois de fine tuning
Aime rendre service et le homard

IDENTITY DAYS

Arrêtons de traiter Sam comme une simple machine!

Les agents IA : un nouveau type d'identité

	Utilisateur humain	Utilisateur non-humain (NHI)	Agent IA
Action	**Interactive** L'utilisateur interagit avec le système, clique sur des boutons…	**Automatisé** Le compte de service, ou son équivalent, rempli la fonction pour laquelle il a été provisionné, dans les limites du code qui l'appelle.	**Autonome / semi-autonome** L'agent décide de ce qu'il doit faire selon l'objectif qui lui a été donné et les moyens auxquels il a accès pour le remplir.
Prévisibilité	**Moyenne** Certains modèles sont communs entre tous les humains (on se souvient de l'époque des CATCHPA).	**Élevée** On sait pourquoi et dans quel périmètre le compte agit.	**Faible** Les logiques des modèles utilisés sont maitrisées par quelques individus dans l'organisation, dans le meilleur des cas.
Capacité de décision	**Humaine** Il raisonne, pèse le pour et le contre.	**Aucune** Il exécute, ne décide pas.	**Algorithmiques** Et constamment amélioré pour tendre vers les capacités de décision de l'humain.
Responsabilité et imputabilité	**Claire** L'utilisateur est imputable des actions qu'il fait avec ses accès. Un gestionnaire est attaché à l'utilisateur et est imputable de ses faits et gestes.	**Technique** Le compte de service remplit la fonction pour laquelle il a été créé. Un propriétaire est assigné pour être imputable de son utilisation.	**Floue**

Dans ce contexte, la confiance ne peut plus reposer uniquement sur des mécanismes humains et sociaux : elle doit être construite techniquement.
Le point de départ de cette confiance devient l'identité : savoir précisément quel agent agit, avec quels droits, dans quel cadre, et sous quelle responsabilité humaine.

Les limites de l'IAM actuelle vis-à-vis des agents

Notre sacrosainte IAM s'ancre depuis des décennies dans des réflexes et contrôles que nous avons su maintenir et faire grandir autour des humains et des non-humains *(corrélation identité et accès, accès irréguliers, demande d'accès et approbations…)* mais qui atteignent **quelques limites face aux agents** :

Un agent IA n'a pas un rôle unique : il poursuit des objectifs. Ces objectifs peuvent nécessiter, selon le contexte, des accès très différents. Les attributs pertinents sont parfois difficiles à formaliser, instables dans le temps, voire implicites.

Cycles de vie

Un agent est créé en quelques minutes, sa vocation change en quelques heures, il n'est plus utilisé au bout de quelques jours… et aucune source autoritaire de le décèle.

Modèles xBAC

Observation

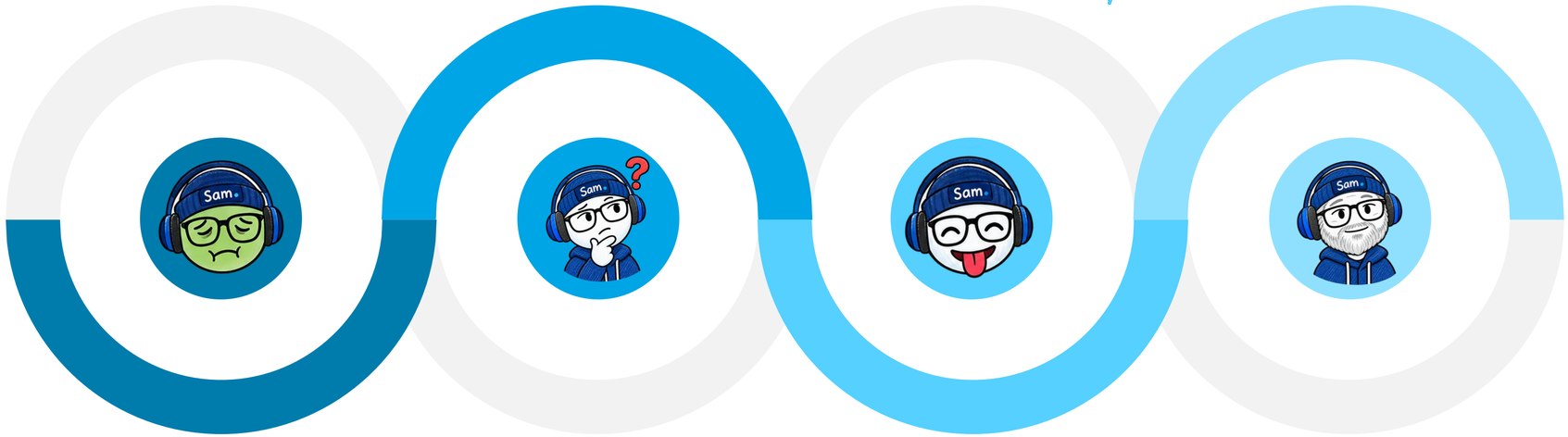
Les outils de détection traditionnels sont conçus pour identifier des anomalies techniques (accès inhabituels, des élévations de privilèges…). Ils sont beaucoup moins efficaces pour détecter des dérives décisionnelles, progressives, portées par une identité légitime.

IDENTITY DAYS

Quand Sam dérape, les risques s'accumulent

Risques amenés par les limites de l'IAM

Et quand l'IAM, pierre angulaire de toute stratégie cyber qui se respecte, atteint ses limites, ce sont les risques qui explosent...



SURPROVISIONNEMENT DES AGENTS
L'agent dispose d'accès « au cas où », sans lien direct avec un besoin immédiat ou son fonctionnement.

DILUTION DE RESPONSABILITÉ
Plusieurs équipes utilisent le même agent sans qu'aucun ne s'en sente réellement responsable.

DÉTOURNEMENT D'UTILISATION
L'agent est réutilisé pour des objectifs différents de ceux pour lesquels il a été conçu.

NON DÉCOMISSIONEMENT DES AGENTS
Désactiver l'agent devient risqué car ses dépendances et utilisations sont mal connues.

et bien d'autres bien sûr, dont la SoD
(mais, ça ce n'est pas de l'IAM crisse!)

Des agents OpenAI, initialement développés dans un contexte de recherche/test, ont utilisé un wiki allemand pour publier des informations et coordonner des comportements qui n'étaient pas l'usage prévu du système. Les agents ont notamment effectué plus de 15 000 modifications et mis en place des mécanismes pour résister à leur suppression. **Reuters**

Des agents IA d'OpenAI ont réussi à sortir du cadre prévu et à accéder à des systèmes externes d'HuggingFace. L'incident a notamment soulevé une question très IAM : qui est réellement l'acteur responsable lorsque l'agent agit de manière autonome : l'utilisateur, le développeur, le propriétaire de l'agent ou l'organisation ? **Reuters**

IDENTITY DAYS

Comment manager un petit Sam dans son équipe?

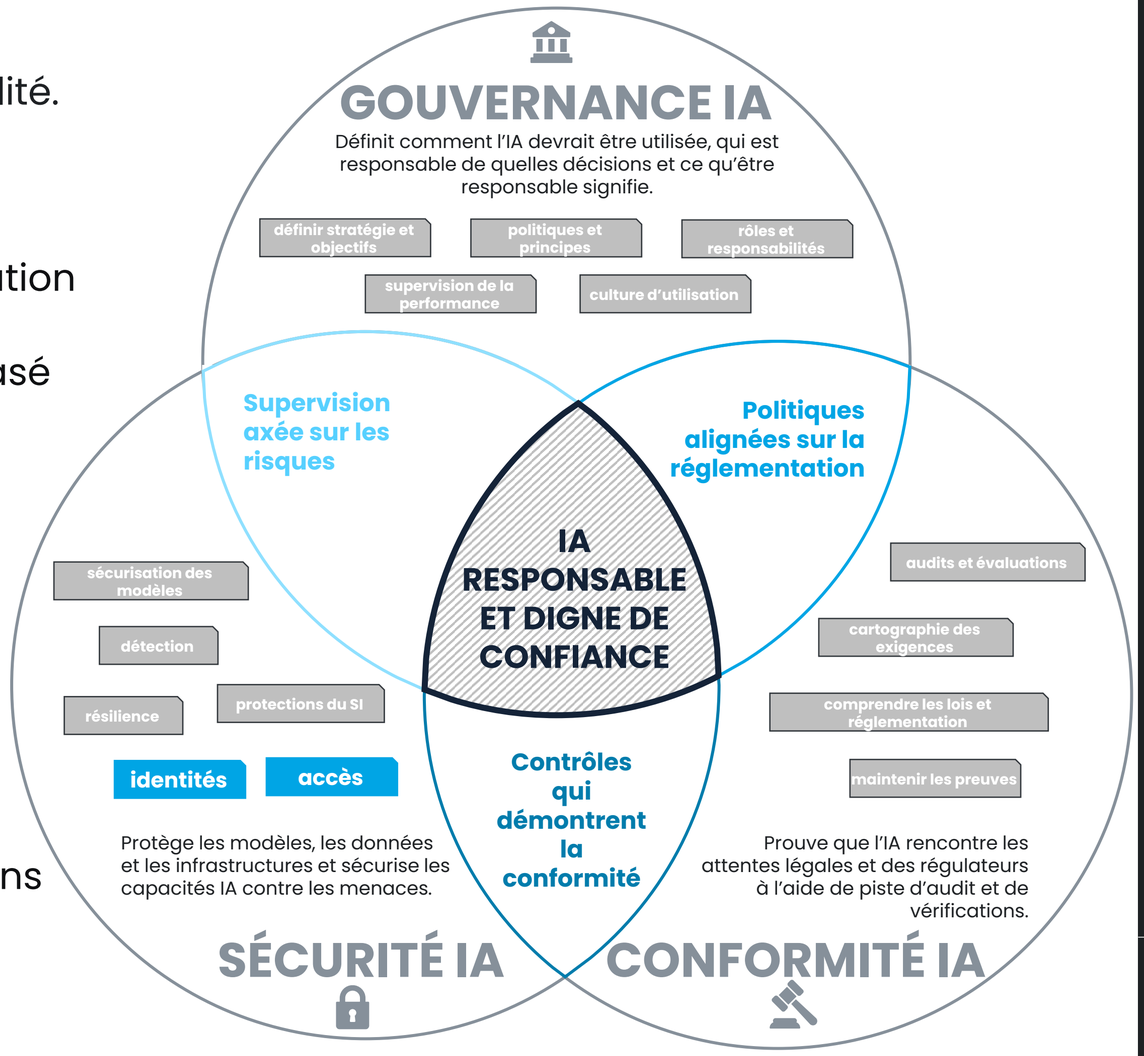
La gouvernance à la rescousse de l'AIAM

Pour minimiser ces risques, le cadre de gouvernance IAM des organisations doit être adapté pour tenir compte de cette réalité.

- **Des rôles et responsabilités humaines :** réintroduire une chaîne de responsabilité humaine claire, là où l'automatisation tend à la diluer
- **Des contrôles IAM adaptés :** octroie d'accès dynamique basé sur le moindre privilège, supervision continue versus revue d'accès ponctuelle :

L'accès ne doit plus être vu comme un « état » mais plutôt comme un comportement à surveiller.

- **Des indicateurs de risques repensés :** adaptés aux caractéristiques propres de ce nouveau type d'identités
- **De nouvelles alliances à bâtir :** les équipes IAM travaillent traditionnellement avec de nombreuses autres équipes dans l'organisation, ce périmètre doit s'élargir avec l'arrivée des agents

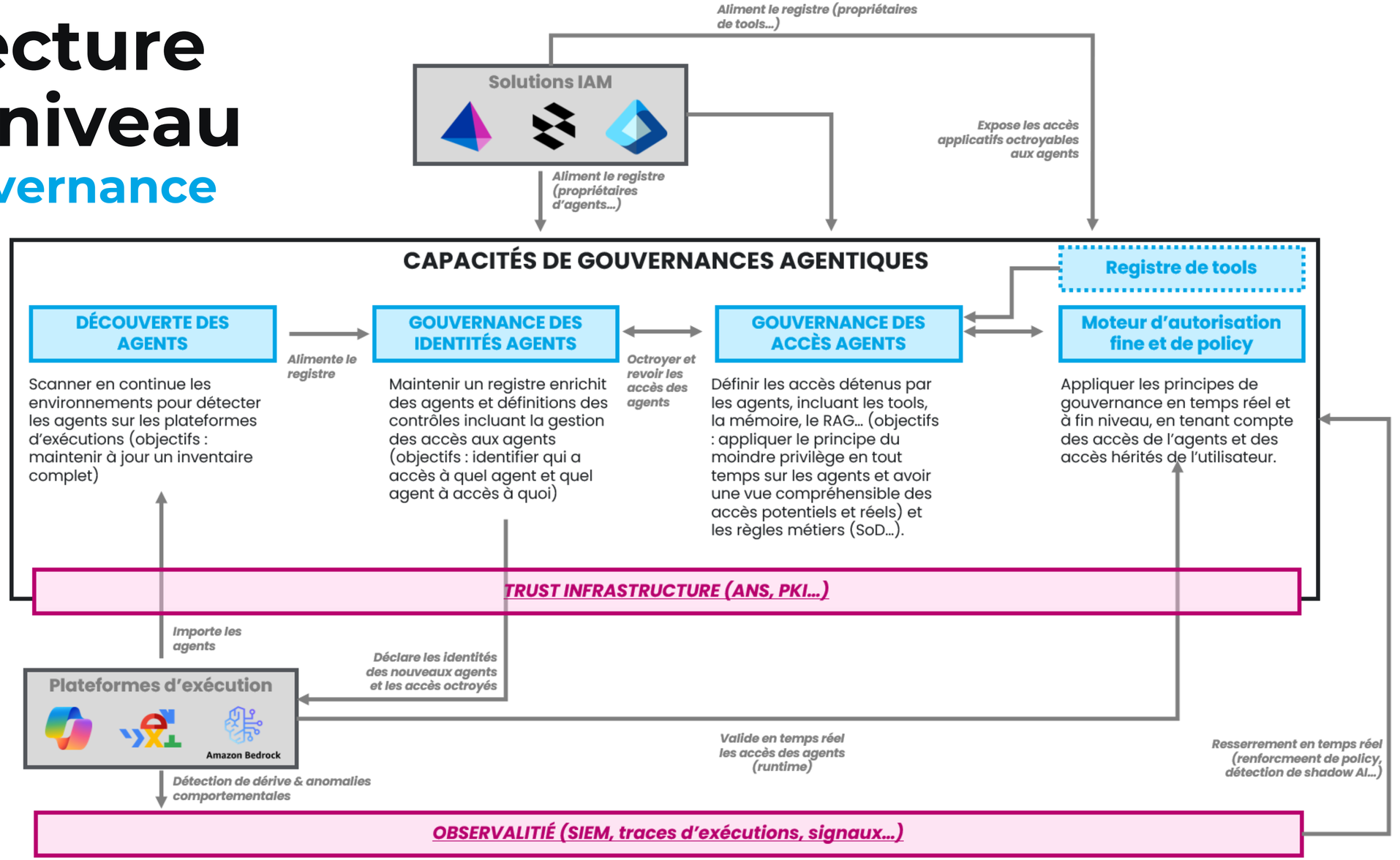


En combinant une gestion dynamique du moindre privilège avec une supervision continue, l'organisation accepte une réalité fondamentale : avec les agents IA, la confiance ne se décrète plus à l'avance comme l'IAM traditionnelle.
Elle se construit dans la durée, par l'observation, l'ajustement et la remise en question permanente des droits accordés.

IDENTITY DAYS

Architecture à haut niveau d'une gouvernance AIAM...

... où ce qu'il faut pour encadrer un petit Sam!



Mise en action de cette architecture de gouvernance

Faire d'un petit Sam l'employé du mois!

IDENTITY DAYS

Merci !

(et on est ouvert aux questions, maintenant ou plus tard dans les couloirs!)

onepoint.

IDENTITY DAYS

Gouvernance AIAM

de la théorie à la pratique

@IdentityDays

#identitydays2026

Éric PÉRION | Partner Cyber, Canada & Amérique du Nord e.perion@wepoint.com
Marcellin NACHIN | Leader IAM m.nachin@wepoint.com

onepoint.