IDENTITY DAYS

20 octobre 2026

PARIS

Des rôles à l’intention : repenser l’autorisation pour les agents IA avec l’IBAC

Youssef AGHZERE
Youssef.aghzere@magellangroup.eu

Youssef – AGHZERE

Consultant en cybersécurité spécialisé en gouvernance des identités (IGA).

Après une formation en ingénierie cybersécurité et management, il se spécialise dans les enjeux IAM mêlant aspects techniques et organisationnels.

MAGELLAN

Agenda de la conférence

I

Agents IA et limites de l'IAM

Agents IA, Intent-Based Access Control (IBAC), autonomie, actions autorisées vs actions justifiées

II

Principes et mécanismes de l'IBAC

Interprétation de l'intention, réduction de l'autorité (narrowing), mapping technique, contrôle à l'exécution (runtime)

III

Perspectives et démonstration

Défis ouverts, fiabilité, démonstrateur PoC, passage de l'identité à l'intention

MÉCANIQUE D'UN AGENT

Un nouvel acteur dans le monde de l'IAM

HUMAIN MACHINE AGENT IA

01 · DÉCLENCHEUR

L'intention

Un objectif exprimé en langage naturel.

« Préviens mon manager que la réunion de demain est reportée à vendredi »

01 · COMPRENDRE
la demande et le contexte

02 · RAISONNER
planifie, choisit l'action

03 · AGIR
utilise les outils

04 · OBSERVER
vérifie, ajuste, recommence

AGENT
BRAIN
Cœur décisionnel : LLM

L'ENVIRONNEMENT

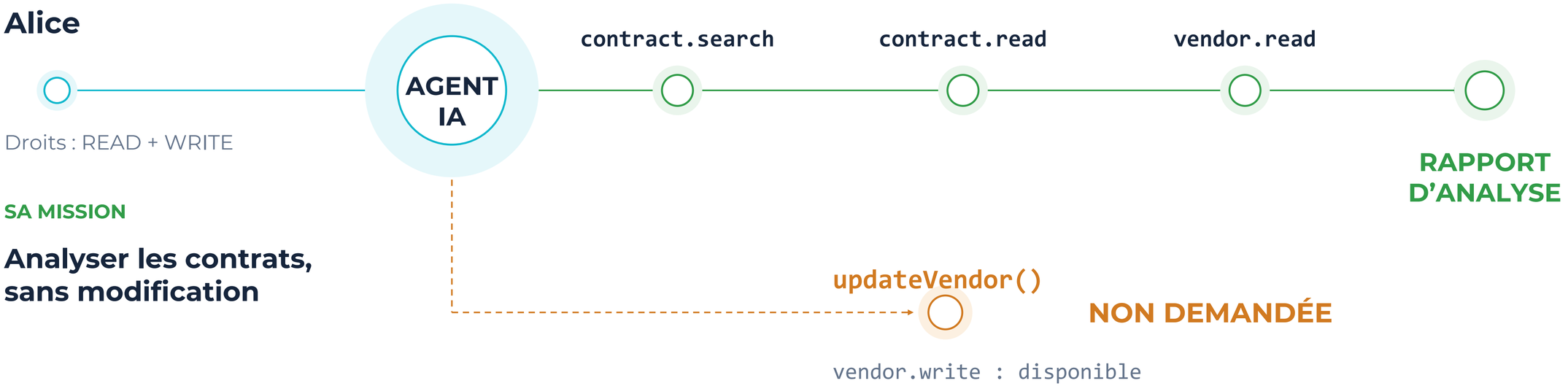
Les bras de l'agent

Les outils = le corps de l'agent.

- Recherche web
- Envoi d'un email
- Base de données
- ...

AUTORISATION ET MISSION

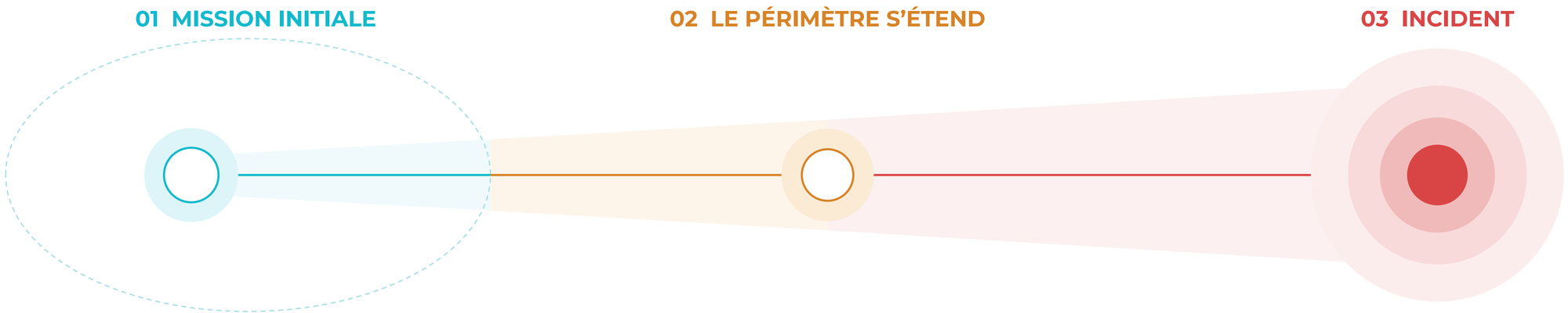
Problème : Permissions légitime, actions non-souhaitées



Ce n'est pas parce que l'agent **PEUT** modifier une donnée qu'il **DOIT** le faire pour accomplir sa mission.

POCKETOS × CURSOR / CLAUDE

PocketOS : quand les permissions dépassent la mission



Agent de codage

Tâche technique limitée

Token API trop permissif

Accès au-delà des besoins de la tâche

PRODUCTION AFFECTÉE

Base de données et sauvegardes supprimées

Le danger apparaît quand **l'autorité disponible** dépasse les besoins de la mission.

PARTIE 02

Principes et mécanismes de l'IBAC

Interprétation de l'intention, réduction de l'autorité (narrowing), mapping technique, contrôle à l'exécution (runtime)

POURQUOI L'IBAC ?

IBAC : du WHY déclaré au WHY appliqué

WHO · WHAT · WHEN / CONTEXT + WHY ?

L'intention enrichit la décision d'autorisation existante.

WHY déclaré

Justification :

« Pour analyser les contrats fournisseurs. »

↓

Motif enregistré

Pas de restriction supplémentaire liée à ce texte seul.

WHY appliqué

1. Mission autorisée

Analyser les contrats, sans modification.

↓

2. Intention structurée et validée

Lecture uniquement

↓

3. Contrainte d'autorisation

Autorisations limitées à la mission.

La différence n'est pas de connaître le **WHY**.
C'est de pouvoir **l'appliquer**.

L'INTENTION CHANGE LE PÉRIMÈTRE

Même agent, deux missions, deux périmètres

ALICE → **AGENT IA**

Droits existants : lecture + écriture

MISSION A : LECTURE SEULE

ANALYSER

Analyser les contrats, sans modification.

CAPACITÉS REQUISES

- `contract.search`
- `contract.read`
- `vendor.read`
- `analytics.query`

HORS MISSION

- `vendor.write`

MISSION B : ECRITURE NECESSAIRE

METTRE À JOUR

Modifier le statut des fournisseurs.

CAPACITÉS REQUISES

- `contract.search`
- `contract.read`
- `vendor.read`

NÉCESSAIRE

- ✓ `vendor.write`

L'intention définit les accès **nécessaires**, pas les accès automatiquement **autorisés**.

PRINCIPE CENTRAL

De l’autorité disponible à l’autorité effective

Autorité effective = Autorité disponible ∩ Autorité nécessaire à la mission ∩ Autorité permise par les politiques

Autorité disponible : Ce qu'Alice est autorisée à déléguer

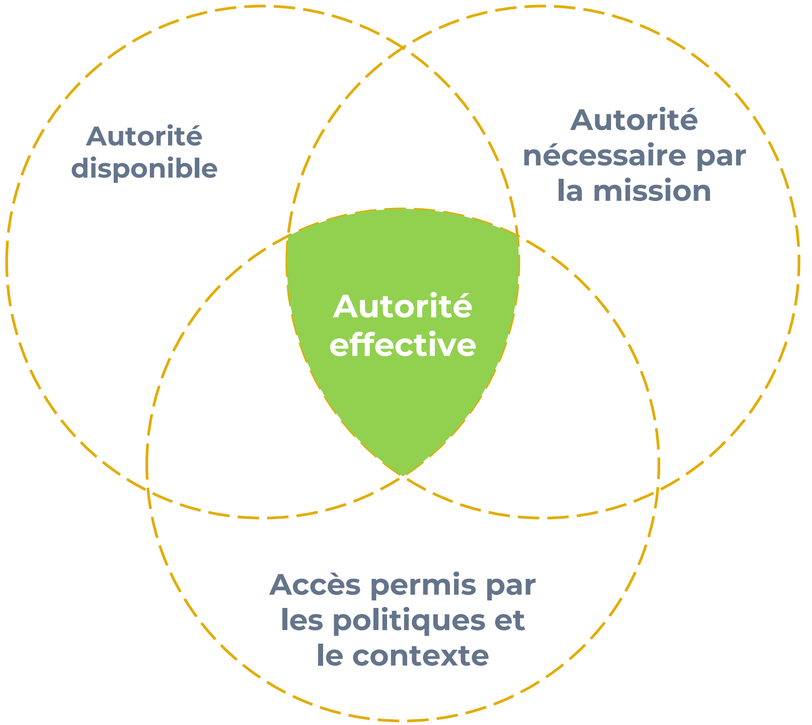
Autorité nécessaire à la mission : Ce que la mission nécessite

Autorité effective : Ce qui est disponible, nécessaire et permis

MISSION D'ANALYSE D'ALICE

✓ `vendor.read` → dans l'autorité effective

✗ `vendor.write` → hors mission



Périmètre de la mission en cours

On part des **droits existants**, puis **on réduit**. Jamais l'inverse

DE LA MISSION AUX CAPACITÉS

Comment traduire une mission en besoins d'accès ?

MISSION EN LANGAGE NATUREL

« Analyse les contrats fournisseurs, **sans modifier** les données sources. »

INTENTION STRUCTURÉE

INTERPRÉTATION IA

Goal :
Analyze supplier contracts and prepare a report

Requierments : contract.search, contract.read, vendor.read

Contraints :
source_data_modification: forbidden

VERIFIER LA COHERENCE AVEC LA MISSION

✓

Vérification des contraintes de la mission

Contrôles fiables
Intervention humaine si nécessaire

Incohérence → rejet / clarification

CAPACITES NECESSAIRES IDENTIFIEES

```
contract.search
contract.read
vendor.read
```

Catalogue contrôlé

Le LLM propose **une interprétation** de la mission, **pas une autorisation** : traduire fiablement le langage naturel en capacités techniques reste **un problème ouvert**.

LIMITE STRUCTURELLE

Un droit IAM peut être plus large que le besoin réel

Besoin métier ≠ **Granularité des droits IAM**

CAPACITÉ NÉCESSAIRE

vendor.read

Le besoin métier est fin : une seule opération, sur une seule ressource.

réalité IAM

ENTITLEMENT DISPONIBLE

GG_VENDOR_MASTER_RW

Permissions associées

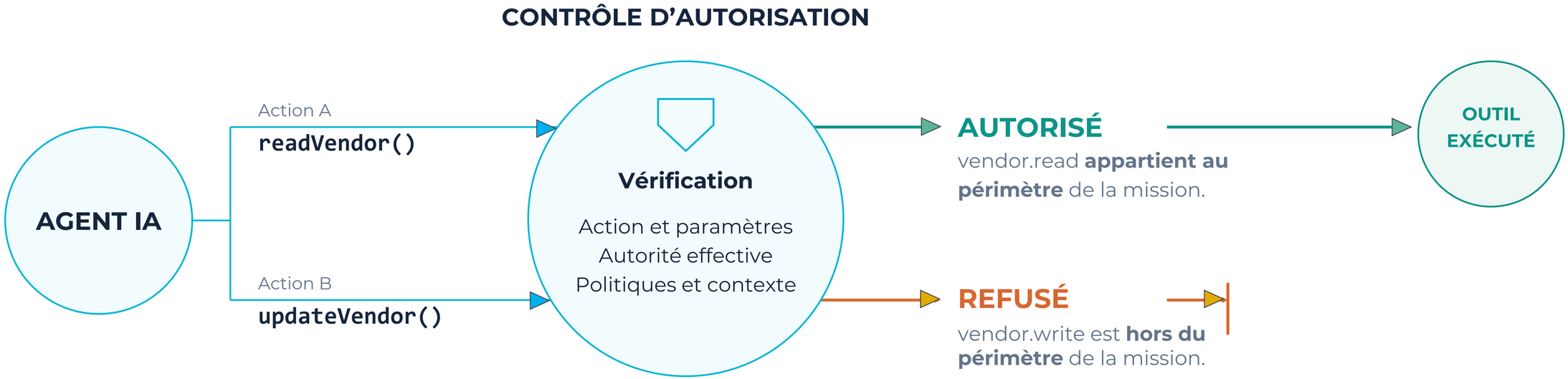
- ✔ vendor.read
- ✔ vendor.search
- ⚠ **vendor.write** — non nécessaire à la mission

Identifier le bon besoin ne **garantit pas** de pouvoir **l'appliquer techniquement**

CONTRÔLE À L'EXÉCUTION

L'autorisation ne s'arrête pas au début de la mission

Mission d'Alice : « Analyser les contrats fournisseurs, sans modifier les données. »



L'agent **propose**. Le système d'autorisation **décide**.

PARTIE 03

Perspectives et démonstration

Défis ouverts, fiabilité, démonstrateur PoC, passage de l'identité à l'intention

ÉTAT DE L'ART & PERSPECTIVES

IBAC : des travaux complémentaires, cinq défis à relever

NIST NCCoE

Identité et autorisation des agents

OpenFGA

Moteur d'autorisation fine

IBAC.dev

Intention et contrôle des outils

IGAC

Réduction d'autorité et cohérence

Des contributions complémentaires, pas un standard IBAC commun.

Les défis avant l'industrialisation

01 **Fiabilité de l'intention**

02 **Connaissance des accès IAM**

03 **Granularité et contrôle effectif**

04 **Performance et intégration**

05 **Gouvernance et audit**

Des pistes existent. Le défi, c'est de les rendre **fiables à l'échelle de l'entreprise.**

DE L'IDENTITÉ À L'INTENTION

Trois idées à retenir

PEUT ≠ DOIT

Une permission disponible n'est pas toujours justifiée par la mission.

L'INTENTION RÉDUIT

Elle limite l'autorité aux accès nécessaires et permis.

LE CONTRÔLE PROTÈGE

Les restrictions doivent être appliquées avant l'exécution des actions.

Gouverner les agents IA, c'est aussi gouverner **leur autonomie**.

IDENTITY DAYS
@IdentityDays
#identitydays2025