



La minute de l'expert

Amine MIRHOM, Cloud Solution Architect

Les agents IA se généralisent... et avec eux, de nouveaux risques. Côté Microsoft, on voit une accélération très claire sur la sécurité "agentic" : visibilité, posture, et protection à l'exécution.

Threat protection pour les AI agents (Preview) – Defender for Cloud

Une nouvelle capacité "Threat protection for AI agents (Preview)" est dans Microsoft Defender for Cloud, disponible en public preview via le plan **Defender for AI Services**.

AI Security Posture Management : savoir "où sont vos IA"

Defender for Cloud renforce la découverte continue des workloads IA (inventaire / AI BOM) sur des services comme Azure OpenAI, Azure AI Foundry, Azure Machine Learning, Amazon Bedrock et Google Vertex AI.

Protection runtime des agents (Preview) – Defender for Cloud Apps

Avec **AI Agent Protection (Preview)**, Defender peut découvrir des agents (Copilot Studio / Azure AI Foundry), surveiller l'activité, et remonter les alertes dans l'expérience **XDR Incidents & Alerts** avec une entité **Agent** dédiée.

Pourquoi c'est important

On passe d'une IA "boîte noire" à une IA **traitée comme un actif** : on **recense**, on **mesure le risque**, et on **bloque** quand ça dévie — directement dans les workflows SecOps.