

IA 2026 : agents, outils utilisés et cybersécurité

Problématique : comment les agents IA transforment-ils le support, l'administration système/réseau et la cybersécurité, tout en gardant une logique de contrôle humain et de protection des données ?

Étudiant

Théo André

Formation

BTS SIO option SISR

TABLE DES MATIÈRES

1. Méthode de veille	p. 1	2. Synthèse de l'actualité	p. 1
3. Impact pour le SISR	p. 2	4. Captures des sources	p. 2
5. Sources utilisées	p. 3	6. Conclusion orale	p. 3

1. Méthode de veille

Outils utilisés

- Navigateur web et recherches ciblées sur des sources officielles.
- ChatGPT / Codex pour organiser les notes, comparer les informations et rédiger la synthèse.
- Captures d'écran des pages consultées pour garder une trace visuelle.
- Export PDF local pour obtenir un document propre à présenter.

Critères de sélection

- Actualité récente ou document de référence encore pertinent.
- Lien avec SISR : support, réseau, systèmes, automatisation, sécurité.
- Source identifiable : éditeur, organisme public ou documentation officielle.

2. Synthèse de l'actualité

OpenAI présente Codex comme un agent de développement capable d'aider à construire, corriger, documenter et travailler sur plusieurs tâches en parallèle. Anthropic décrit Claude Code comme un système agentique capable de lire un codebase, modifier des fichiers et lancer des tests.

Codex

Claude Code

Automatisation

En entreprise, la priorité devient la gouvernance des agents

Microsoft met en avant Copilot et Agent 365 pour travailler dans Microsoft 365 avec supervision, sécurité, identité et conformité. Google positionne Gemini Enterprise comme une plateforme d'agents reliée aux workflows et aux systèmes de l'entreprise.

Copilot

Agent 365

Gemini Enterprise

Pour un profil SISR, l'IA est utile mais doit être encadrée

L'ANSSI rappelle que l'IA crée trois sujets cyber : sécuriser les systèmes d'IA, utiliser l'IA pour la cybersécurité, et se défendre face à des attaquants qui exploitent aussi l'IA. La bonne approche reste basée sur les risques, les droits, les journaux et la validation humaine.

ANSSI

Risques

Traçabilité

3. Impact concret pour le SISR

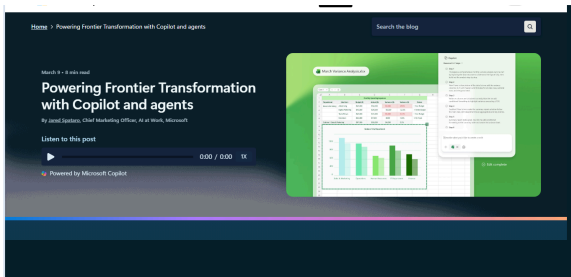
Support et administration

- Aide à rédiger des procédures utilisateurs et techniques.
- Diagnostic plus rapide à partir de messages d'erreur ou de journaux.
- Génération de scripts, à relire et tester avant usage.

Cybersécurité

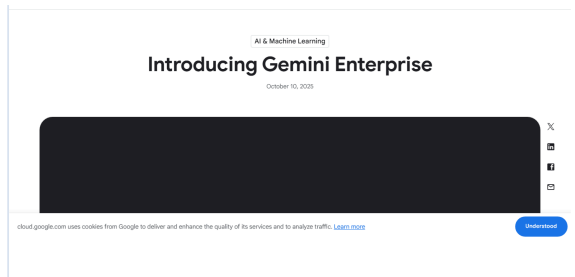
- Tri d'alertes, résumé d'incidents, aide à la documentation.
- Risque de fuite d'informations si des données sensibles sont envoyées sans contrôle.
- Besoin de MFA, permissions minimales, segmentation et journalisation.

4. Captures des sources



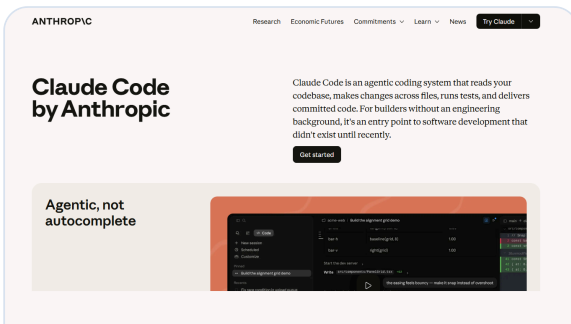
Microsoft

Article sur Copilot, agents et transformation en entreprise.



Google Cloud

Présentation de Gemini Enterprise et des agents IA.



Anthropic

Claude Code présenté comme système agentique de développement.



ANSSI

Posture cyber et approche par les risques autour de l'IA.

5. Sources utilisées

OpenAI	https://openai.com/codex/
Microsoft	https://www.microsoft.com/en-us/microsoft-365/blog/2026/03/09/powering-frontier-transformation-with-copilot-and-agents/
Google Cloud	https://cloud.google.com/blog/products/ai-machine-learning/introducing-gemini-enterprise
Anthropic	https://www.anthropic.com/product/claude-code
ANSSI	https://cyber.gouv.fr/enjeux-technologiques/intelligence-artificielle/

6. Conclusion orale

Les agents IA deviennent des assistants capables d'agir sur des fichiers, des applications et des workflows. Pour un technicien SISR, c'est une opportunité pour gagner du temps sur la documentation, le diagnostic et l'automatisation. Leur intégration doit rester maîtrisée : vérifier les résultats, limiter les droits, protéger les données et conserver des traces.