AYI NEDJIMI
Consultants

Audit cyber 2026 : pourquoi je commence par la supply chain

12 mai 2026 • Mis à jour le 17 mai 2026 • 8 min de lecture • 1297 mots • 46 vues •

Trois ans à auditer les pare-feux et l''AD en priorité. Mai 2026 a confirmé qu''il fallait commencer ailleurs : par la supply chain logicielle. Voici ma méthode et mes trois questions de départ.

Trois ans à signer des rapports d''audit qui commençaient par les pare-feux et finissaient par l''AD. Aujourd''hui je commence par les fichiers package-lock.json, les workflows GitHub Actions et la liste des paquets pip installés sur les builders. Ce n''est pas une lubie : c''est l''unique endroit où les attaquants gagnent vraiment du terrain en 2026.

Ce que la semaine du 5 au 12 mai 2026 a confirmé

Mini Shai-Hulud sur TanStack le 11 mai. Avant ça, PCPJack sur les clusters Kubernetes exposés. Avant ça, Trellix piraté avec exfiltration de code source. n8n CVSS 10.0, Spring AI trois HIGH, AzuraCast RCE 8.8, OpenCTI takeover non-auth, FastGPT 9.8. Et je ne parle même pas de l''affaire Instructure qui a balayé 275 millions de comptes étudiants. En une semaine.

Le point commun de toutes ces affaires n''est pas le périmètre technique attaqué. C''est le périmètre social. Des bibliothèques tierces, des plateformes d''orchestration auto-hébergées, des frameworks LLM, des outils de threat intelligence : autant de briques qu''aucune équipe sécurité ne maintient elle-même mais que toute organisation moderne consomme massivement. Le ROI de l''attaquant qui compromet une dépendance largement diffusée est d''un ou deux ordres de grandeur supérieur à celui de l''attaquant qui phishe un comptable.

Cette concentration n''est pas une surprise. Elle était annoncée depuis SolarWinds en 2020, depuis Log4Shell en 2021, depuis xz utils en 2024. Ce qui change en 2026, c''est l''industrialisation. TeamPCP a publié 84 versions npm en six minutes le 11 mai. Ce n''est pas un attaquant qui bricole un soir, c''est un harnais d''automatisation prêt à dégainer dès qu''une fenêtre s''ouvre.