Comment Cyber Crucible protège-t-il les environnements de fabrication, OT et ICS ?

Réponse courte : La solution s'exécute entièrement sur le poste (endpoint), sans aucune dépendance au cloud, ce qui lui permet de protéger les technologies opérationnelles et les systèmes de contrôle industriel qui sont hors ligne, isolés (air-gapped) ou connectés de manière intermittente — et elle ne suspend que le processus malveillant, de sorte que la production continue.

Pourquoi les outils conventionnels peinent ici

Les environnements OT et ICS ne peuvent tolérer ni un aller-retour vers le cloud ni un verrouillage complet du réseau. Beaucoup sont volontairement déconnectés. Les modèles de sécurité qui supposent une connectivité constante et un SOC distant ne s'appliquent tout simplement pas.

Ce qui change

- **Fonctionnement 100 % hors ligne** — protection complète sans signal requis, prête pour les environnements isolés (air-gap).
- **Aucun verrouillage** — les processus malveillants sont suspendus en mémoire pendant que la production se poursuit.
- **Un seul agent pour l'ensemble de l'environnement** — le même agent léger protège les automates (PLC) sur le site de production, les véhicules d'un réseau logistique et les navires en mer, sans intervention d'analyste et sans hypothèse de connectivité.

Revision #1
Created 2026-07-24 07:01:19 UTC by Dennis Underwood
Updated 2026-07-24 07:01:19 UTC by Dennis Underwood