¿Cómo se alinea Cyber Crucible con la norma IEC 62443 para sistemas de control industrial?

Respuesta breve: Cyber Crucible respalda el modelo de defensa en profundidad de IEC 62443 para sistemas de automatización y control industrial mediante la incorporación de protección autónoma de endpoints a nivel de kernel que no interrumpe la producción. Funciona de forma local, tolera la operación sin conexión y suspende únicamente los procesos maliciosos, lo cual se alinea con el énfasis de la norma tanto en la seguridad como en la disponibilidad operativa.

Cómo se corresponde con el propósito de la norma

- **Protección de zonas y conductos.** La prevención residente en el endpoint refuerza los dispositivos dentro de una zona sin depender de una comunicación de ida y vuelta con la red.
- **La disponibilidad ante todo.** La suspensión selectiva de un proceso malicioso evita el tiempo de inactividad de la planta que provoca la contención indiscriminada.
- **Funciona en entornos de baja conectividad.** Es adecuado para plantas de fabricación, flotas logísticas y sitios periféricos donde la conectividad en la nube es poco confiable o deliberadamente inexistente.

El límite honesto

La certificación IEC 62443 se aplica a sistemas y procesos, no a una única herramienta de endpoint; Cyber Crucible es un componente que respalda los objetivos de la norma. La correspondencia de controles está disponible bajo acuerdo de confidencialidad (NDA).

Revision #1
Created 2026-07-24 02:04:49 UTC by Dennis Underwood
Updated 2026-07-24 02:04:49 UTC by Dennis Underwood