Wie richtet sich Cyber Crucible an IEC 62443 für industrielle Steuerungssysteme aus?

Kurze Antwort: Cyber Crucible unterstützt das Defense-in-Depth-Modell von IEC 62443 für industrielle Automatisierungs- und Steuerungssysteme, indem es einen autonomen, kernelbasierten Endpunktschutz hinzufügt, der die Produktion nicht unterbricht. Er läuft lokal, toleriert den Betrieb ohne Verbindung und setzt ausschließlich bösartige Prozesse aus, was der Betonung des Standards auf sowohl Sicherheit als auch betriebliche Verfügbarkeit entspricht.

Wie es sich mit der Zielsetzung des Standards deckt

- **Zonen- und Verbindungsschutz.** Auf dem Endpunkt ansässige Prävention härtet die Geräte innerhalb einer Zone, ohne von einer Netzwerk-Rückmeldung abhängig zu sein.
- **Verfügbarkeit an erster Stelle.** Das selektive Aussetzen eines bösartigen Prozesses vermeidet die Anlagenausfallzeiten, die durch pauschale Eindämmung entstehen.
- **Funktioniert in Umgebungen mit geringer Konnektivität.** Geeignet für Produktionshallen, Logistikflotten und Edge-Standorte, an denen die Cloud-Konnektivität unzuverlässig oder bewusst nicht vorhanden ist.

Die ehrliche Grenze

Die IEC 62443-Zertifizierung gilt für Systeme und Prozesse, nicht für ein einzelnes Endpunkt-Tool; Cyber Crucible ist eine Komponente, die die Ziele des Standards unterstützt. Die Zuordnung der Kontrollen ist unter NDA verfügbar.

Revision #1
Created 2026-07-24 04:53:57 UTC by Dennis Underwood
Updated 2026-07-24 04:53:57 UTC by Dennis Underwood