Comment Cyber Crucible s'aligne-t-il avec la norme IEC 62443 pour les systèmes de contrôle industriel ?

Réponse brève : Cyber Crucible prend en charge le modèle de défense en profondeur de la norme IEC 62443 pour les systèmes d'automatisation et de contrôle industriels en ajoutant une protection autonome des terminaux au niveau du noyau qui ne perturbe pas la production. Il fonctionne localement, tolère un fonctionnement déconnecté et ne suspend que les processus malveillants, ce qui s'aligne avec l'accent mis par la norme à la fois sur la sécurité et sur la disponibilité opérationnelle.

Comment cela s'articule avec l'objectif de la norme

- **Protection des zones et des conduits.** La prévention résidant sur le terminal renforce la sécurité des appareils au sein d'une zone sans dépendre d'un aller-retour réseau.
- **La disponibilité avant tout.** La suspension sélective d'un processus malveillant évite les temps d'arrêt d'usine que provoque un confinement brutal.
- **Fonctionne dans des environnements à faible connectivité.** Adapté aux ateliers de fabrication, aux flottes logistiques et aux sites périphériques où la connectivité au cloud est peu fiable ou volontairement absente.

La limite en toute honnêteté

La certification IEC 62443 s'applique à des systèmes et des processus, et non à un seul outil de terminal ; Cyber Crucible est un composant qui appuie les objectifs de la norme. La cartographie des contrôles est disponible sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 07:15:07 UTC by Dennis Underwood
Updated 2026-07-24 07:15:07 UTC by Dennis Underwood