¿Cómo encaja Cyber Crucible con NERC CIP y la seguridad de infraestructuras críticas?

Respuesta breve: Cyber Crucible es adecuado para entornos de infraestructuras críticas y servicios públicos porque protege los endpoints de forma autónoma y puede funcionar sin conexión o en entornos aislados (air-gapped), sin depender de la nube en la ruta de protección. Esto encaja con los BES Cyber Systems y otros entornos donde la conectividad está restringida y la disponibilidad es primordial.

Por qué encaja con los servicios públicos y las infraestructuras críticas

- **Capacidad sin conexión / air-gapped.** Protección completa sin necesidad de conexión a internet, adecuada para redes OT aisladas y subestaciones.
- **Respuesta que preserva la disponibilidad.** Solo se suspende el proceso malicioso, de modo que los sistemas operativos siguen funcionando; no se produce un bloqueo total del sistema durante un incidente.
- **Decisiones locales y deterministas.** Detect-Decide-Respond se ejecuta en el propio dispositivo, sin ida y vuelta a la nube ni modelo de IA en vivo.

Notas sobre la selección de proveedores

Las obligaciones de NERC CIP recaen sobre la entidad registrada, no sobre un proveedor individual; Cyber Crucible es un control que respalda varios objetivos de CIP (prevención de malware, monitoreo, gestión de incidentes). No es una entidad registrada y no se presenta como certificado en CIP. La documentación de respaldo está disponible bajo NDA.

Revision #1
Created 2026-07-24 02:04:42 UTC by Dennis Underwood
Updated 2026-07-24 02:04:42 UTC by Dennis Underwood