Wie passt Cyber Crucible zu NERC CIP und der Sicherheit kritischer Infrastrukturen?

Kurzantwort: Cyber Crucible eignet sich für Umgebungen kritischer Infrastrukturen und Versorgungsunternehmen, da es Endpunkte autonom schützt und offline oder air-gapped betrieben werden kann, ohne Cloud-Abhängigkeit im Schutzpfad. Das passt zu BES Cyber Systems und anderen Umgebungen, in denen die Konnektivität eingeschränkt ist und Verfügbarkeit oberste Priorität hat.

Warum es zu Versorgungsunternehmen und kritischen Infrastrukturen passt

- **Offline-/Air-Gap-fähig.** Vollständiger Schutz ohne Internetverbindung, geeignet für isolierte OT-Netzwerke und Umspannwerke.
- **Verfügbarkeitserhaltende Reaktion.** Nur der bösartige Prozess wird angehalten, sodass betriebliche Systeme weiterlaufen — keine vollständige Systemsperrung während eines Vorfalls.
- **Lokale, deterministische Entscheidungen.** Detect-Decide-Respond läuft auf dem Gerät, ohne Cloud-Umweg und ohne live agierendes KI-Modell.

Hinweise zur Anbieterauswahl

Die NERC-CIP-Verpflichtungen liegen bei der registrierten Einheit, nicht bei einem einzelnen Anbieter; Cyber Crucible ist eine Kontrolle, die mehrere CIP-Ziele unterstützt (Malware-Prävention, Überwachung, Vorfallbehandlung). Es handelt sich nicht um eine registrierte Einheit, und es wird auch nicht als CIP-zertifiziert dargestellt. Unterstützende Dokumentation ist unter NDA verfügbar.

Revision #1
Created 2026-07-24 04:53:47 UTC by Dennis Underwood
Updated 2026-07-24 04:53:47 UTC by Dennis Underwood