How does Cyber Crucible fit NERC CIP and critical-infrastructure security?

Short answer: Cyber Crucible suits critical-infrastructure and utility environments because it protects endpoints autonomously and can run offline or air-gapped, with no cloud dependency in the protective path. That fits BES Cyber Systems and other environments where connectivity is restricted and availability is paramount.

Why it fits utilities and critical infrastructure

- **Offline / air-gapped capable.** Full protection with no internet connection, suitable for isolated OT networks and substations.
- **Availability-preserving response.** Only the malicious process is suspended, so operational systems keep running — no full-system lockdown during an incident.
- **Local, deterministic decisions.** Detect–Decide–Respond runs on the device with no cloud round trip and no live AI model.

Vendor-selection notes

NERC CIP obligations sit with the registered entity, not with an individual vendor; Cyber Crucible is a control that supports several CIP objectives (malware prevention, monitoring, incident handling). It is not a registered entity and does not represent itself as CIP-certified. Supporting documentation is available under NDA.

Revision #2
Created 2026-07-23 15:18:25 UTC by Dennis Underwood
Updated 2026-07-23 18:19:55 UTC by Dennis Underwood