Como o Cyber Crucible se enquadra na NERC CIP e na segurança de infraestruturas críticas?

Resposta curta: O Cyber Crucible é adequado para ambientes de infraestrutura crítica e concessionárias porque protege endpoints de forma autónoma e pode funcionar offline ou em air-gap, sem qualquer dependência da nuvem no percurso de proteção. Isto adequa-se a Sistemas Cibernéticos BES e a outros ambientes onde a conectividade é restrita e a disponibilidade é primordial.

Porque se adequa a concessionárias e infraestruturas críticas

- **Capacidade offline / air-gapped.** Proteção total sem qualquer ligação à internet, adequada a redes OT isoladas e subestações.
- **Resposta que preserva a disponibilidade.** Apenas o processo malicioso é suspenso, pelo que os sistemas operacionais continuam a funcionar — sem bloqueio total do sistema durante um incidente.
- **Decisões locais e determinísticas.** O Detect-Decide-Respond é executado no dispositivo, sem comunicação de ida e volta com a nuvem e sem modelo de IA em tempo real.

Notas sobre a seleção de fornecedores

As obrigações da NERC CIP recaem sobre a entidade registada, não sobre um fornecedor individual; o Cyber Crucible é um controlo que apoia diversos objetivos da CIP (prevenção de malware, monitorização, gestão de incidentes). Não é uma entidade registada e não se apresenta como certificado para a CIP. Documentação de suporte está disponível mediante acordo de confidencialidade (NDA).

Revision #1
Created 2026-07-24 06:03:25 UTC by Dennis Underwood
Updated 2026-07-24 06:03:25 UTC by Dennis Underwood