

Comment Cyber Crucible s'intègre-t-il aux exigences NERC CIP et à la sécurité des infrastructures critiques ?

Réponse courte : Cyber Crucible convient aux environnements d'infrastructures critiques et de services publics car il protège les terminaux de manière autonome et peut fonctionner hors ligne ou en réseau isolé (air-gapped), sans aucune dépendance au cloud dans le chemin de protection. Cela correspond aux BES Cyber Systems et à d'autres environnements où la connectivité est restreinte et où la disponibilité est primordiale.

Pourquoi cela convient aux services publics et aux infrastructures critiques

- **Fonctionnement hors ligne / en réseau isolé.** Protection complète sans connexion Internet, adaptée aux réseaux OT isolés et aux postes de transformation.
- **Réponse préservant la disponibilité.** Seul le processus malveillant est suspendu, de sorte que les systèmes opérationnels continuent de fonctionner — aucun blocage complet du système pendant un incident.
- **Décisions locales et déterministes.** Detect-Decide-Respond s'exécute sur l'appareil sans aller-retour vers le cloud et sans modèle d'IA en direct.

Notes relatives à la sélection des fournisseurs

Les obligations NERC CIP incombent à l'entité enregistrée, et non à un fournisseur individuel ; Cyber Crucible est un contrôle qui appuie plusieurs objectifs CIP (prévention des logiciels malveillants, surveillance, gestion des incidents). Il ne s'agit pas d'une entité enregistrée et l'entreprise ne se présente pas comme certifiée CIP. La documentation à l'appui est disponible sous accord de confidentialité (NDA).

