

Cyber Crucible fonctionne-t-il hors ligne ou dans des environnements isolés (air-gapped) ?

Réponse courte : Oui. Toute l'analyse et l'application se font localement sur le poste, si bien que Cyber Crucible assure une protection complète sans connexion internet, sans service cloud et sans aucun signal. Il convient aux réseaux isolés (air-gapped), aux environnements OT et ICS, ainsi qu'aux opérations de terrain déconnectées.

Pourquoi cela fonctionne sans connectivité

Comme la boucle Detect-Decide-Respond s'exécute entièrement dans le noyau sur l'appareil, la connectivité n'est jamais nécessaire pour prendre une décision de protection. La télémétrie se synchronise de manière opportuniste pour la collecte de preuves et le reporting lorsqu'une connexion est disponible, mais la protection n'en dépend pas.

Éprouvé en mer

Dans un déploiement maritime, Cyber Crucible a fonctionné de manière autonome durant des traversées de plusieurs jours sans personnel informatique à bord, s'est adapté à des liaisons satellite à faible bande passante et intermittentes, avec des interruptions dues aux conditions météorologiques, et a conservé des journaux d'investigation numérique riches pendant de longues périodes de déconnexion, en vue d'une analyse post-traversée. Les systèmes protégés allaient des terminaux de loisirs destinés aux passagers aux systèmes de contrôle maritime critiques pour la mission.

C'est également pour cette raison que le même agent convient aux ateliers de production, aux flottes logistiques et à d'autres environnements en périphérie où la connectivité cloud est peu fiable ou délibérément absente.