

Cyber Crucible peut-il protéger les navires et les opérations à distance ou déconnectées ?

Réponse courte : Oui, et cela a déjà été démontré. Lors d'un déploiement maritime, Cyber Crucible a fonctionné de manière autonome pendant des traversées de plusieurs jours sans aucun personnel informatique à bord, s'adaptant à des liaisons satellite à faible bande passante et à de longues périodes de déconnexion, tout en protégeant aussi bien les terminaux passagers que les systèmes de contrôle maritime critiques.

Ce que le déploiement a démontré

- **Réponse autonome** sans équipe informatique présente pendant plusieurs jours d'affilée.
- **Fonctionnement adapté au satellite** sur des liaisons instables, à faible bande passante et sujettes aux interruptions météorologiques.
- **Conservation des données à des fins d'analyse judiciaire** — des journaux détaillés préservés malgré la déconnexion, pour une analyse post-traversée.
- **Résilience face aux attaques** — le système a tenu bon lorsque des adversaires ont tenté de le désactiver ou de dégrader ses performances.

L'élément inhabituel

Les journaux ont révélé une activité compatible avec l'implication d'un État-nation, et le ciblage était sélectif : seuls les navires opérant en eaux internationales étaient touchés, tandis que les navires d'excursion nationaux restaient épargnés.

Lorsque les tentatives d'intrusion classiques ont échoué, les adversaires sont montés en puissance — détournant les identifiants de connexion Windows, puis accédant aux paramètres au niveau du BIOS pour verrouiller les systèmes avant le démarrage. Même avec des systèmes bloqués avant que le système d'exploitation ne puisse se charger, le déploiement a continué de tenir la ligne là où les piles de sécurité traditionnelles avaient déjà échoué.