

Comment Cyber Crucible prend-il en charge les environnements gouvernementaux et à haute sécurité ?

Réponse courte : Grâce à une souveraineté totale des données — installation entièrement sur site dans des racks physiquement sécurisés, fonctionnement en air gap et architecture multi-tenant — sans cloud public, sans SOC tiers et sans partage de données.

Souveraineté par architecture

Pour les organisations exigeant un contrôle absolu, aucune donnée n'a besoin de quitter l'environnement. Il n'y a aucune plateforme tierce dans le circuit, aucun accès externe, et aucune analyse de vos données hébergée par le fournisseur.

Cela compte, car de nombreux fournisseurs téléchargent des données d'identité sensibles — clés privées, jetons de session — vers leurs équipes SOC hébergées. Ce stockage centralisé constitue un point de défaillance unique et une cible de grande valeur pour les attaquants soutenus par des États, et il peut être atteint par contrainte légale à votre insu.

Discret par défaut

Les menaces sont neutralisées silencieusement au niveau du noyau. Vous seul savez qu'une attaque a été tentée, et si aucune donnée n'a été touchée, il n'y a généralement aucune alerte externe ni aucune divulgation requise.

Multi-tenant

L'architecture prend en charge les déploiements multi-tenant, ce qui convient à la gestion de plusieurs départements ou agences depuis une seule instance sécurisée sur site.