Cyber Crucible fonctionne-t-il aux côtés d'autres outils de cybersécurité et d'EDR ?

Réponse courte : Oui. Cyber Crucible est construit sur ses propres capteurs propriétaires et sa propre technologie de surveillance comportementale, ce qui lui permet de fonctionner aux côtés de pratiquement n'importe quel autre produit de sécurité sans interférer avec les outils existants.

Pourquoi la compatibilité ne pose pas de problème

Cyber Crucible ne s'appuie pas sur des points d'ancrage EDR partagés ni sur des intégrations au niveau système dont dépendent également d'autres éditeurs de sécurité. Comme son approche de détection et de surveillance, y compris les méthodes de collecte comportementale qui sous-tendent FortressAI, est conçue sur mesure depuis la base, elle n'entre pas en concurrence pour les mêmes ressources système et n'interfère pas avec les points d'ancrage utilisés par d'autres outils de protection des points d'accès. Cette conception permet à Cyber Crucible de fonctionner comme une couche de protection supplémentaire plutôt que comme un remplacement ou une superposition conflictuelle. Il a été déployé aux côtés de produits d'un large éventail d'éditeurs de sécurité reconnus, et dans la pratique, la plupart des environnements ne présentent aucun problème de compatibilité.

Quand des ajustements sont nécessaires

La situation rare qui nécessite une configuration supplémentaire concerne les logiciels internes personnalisés qu'une entreprise a développés en interne. Il arrive occasionnellement que ces outils maison présentent des schémas de comportement qui ressemblent au type d'activité que Cyber Crucible est conçu pour détecter, comme des modifications rapides de fichiers ou des interactions système inhabituelles. Lorsque cela se produit, la solution est simple : une règle d'exclusion peut être ajoutée pour que Cyber Crucible reconnaisse l'outil interne comme légitime. Cette exclusion reste fiable tant que le logiciel interne demeure correctement signé et non modifié, c'est-à-dire qu'il continue de correspondre à son état attendu et vérifié. Si ces conditions sont respectées,

l'outil fonctionne normalement aux côtés de Cyber Crucible sans friction continue.

Ce que cela signifie pour les équipes de sécurité

Les organisations n'ont pas besoin de supprimer ou de reconfigurer leur dispositif de sécurité actuel pour adopter Cyber Crucible. Il est conçu pour compléter les défenses existantes, en ajoutant une couche dédiée axée sur la prévention des rançongiciels, du vol de données et de l'usurpation d'identité, sans perturber les outils qui protègent déjà l'environnement.

https://player.vimeo.com/video/1043463490

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Revision #1
Created 2026-07-24 07:23:41 UTC by Dennis Underwood
Updated 2026-07-24 07:23:41 UTC by Dennis Underwood