Comment Cyber Crucible sécurise-t-il et contrôle-t-il les terminaux ?

Réponse courte : De deux manières. Le produit lui-même constitue une solution de prévention autonome des terminaux fonctionnant au niveau du noyau, et Cyber Crucible contrôle ses propres terminaux d'entreprise et d'ingénierie dans le cadre d'un programme formel. Les deux reposent sur le développement en interne du code le plus privilégié.

Protection des terminaux du produit

Le produit assure une prévention autonome contre les rançongiciels, les attaques en mémoire (sans fichier) et l'injection de processus, appliquée au niveau du noyau. Il est délibérément découplé des bibliothèques du système d'exploitation, de sorte que lorsque des attaquants compromettent ou détournent ces bibliothèques en mémoire, le produit continue de fonctionner, d'appliquer les protections et de générer des rapports. Étant donné que la détection et la réponse s'exécutent localement, la protection se poursuit lors d'une interruption du backend de gestion ou dans un déploiement délibérément isolé du réseau (air-gapped).

Intégrité de la chaîne d'approvisionnement et validation indépendante

Les algorithmes de détection, les heuristiques du noyau, les capteurs et les pilotes sont conçus et maintenus en interne ; aucune bibliothèque tierce non vérifiée ni aucun mécanisme de télémétrie caché n'est intégré au logiciel. Étant donné que le composant disposant des privilèges les plus élevés est propriétaire, toute une catégorie d'exposition liée à la chaîne d'approvisionnement des tiers est éliminée plutôt que simplement gérée. Tous les pilotes de noyau Windows sont validés et signés dans le cadre du Windows Hardware Compatibility Program (WHCP) de Microsoft.

Contrôles des terminaux d'entreprise

Les terminaux gérés suivent des configurations de référence sécurisées approuvées, exécutent une protection et une analyse des terminaux, et appliquent les mêmes contrôles aux supports amovibles et portables qu'aux supports fixes, l'utilisation non autorisée de supports étant restreinte. L'installation de logiciels est régie par une politique, les données au repos sur les terminaux sont chiffrées, et les terminaux sont maintenus à jour dans le cadre du programme de gestion des correctifs.

Alignement avec les référentiels et limites assumées

Les contrôles des terminaux s'alignent sur les CIS Critical Security Controls (v8) et le NIST SP 800-53 (SI-3, CM-2, MP-7). Aucune certification n'est revendiquée. Des normes de configuration détaillées et des preuves sont fournies aux évaluateurs sous accord de confidentialité (NDA).

Revision #1
Created 2026-07-24 23:44:09 UTC by Dennis Underwood
Updated 2026-07-24 23:44:09 UTC by Dennis Underwood