Comment Cyber Crucible favorise-t-il la conformité HIPAA dans le secteur de la santé ?

Réponse courte : L'ensemble de l'analyse s'effectue localement au niveau du noyau, de sorte que les informations de santé protégées ne quittent jamais le terminal à des fins de traitement de sécurité. Cela évite les risques d'exposition liés à HIPAA que créent les outils de sécurité qui transfèrent des fichiers ou des clés sensibles vers des clouds tiers, et permet de stopper les attaques sans mettre hors ligne les systèmes cliniques.

Le problème posé par la sécurité hébergée chez un fournisseur

De nombreux dispositifs de SOC et de MDR hébergés par des fournisseurs exigent le transfert de clés, de fichiers ou de télémétrie sensibles vers des bases de données cloud tierces. Pour une entité couverte, cela crée un risque de conformité réel et augmente le nombre de parties ayant accès aux données protégées.

Analyse locale, données locales

Cyber Crucible effectue son analyse directement sur le terminal. Les actifs sensibles ne quittent jamais le périmètre sécurisé de l'appareil — ce qui garantit à la fois la souveraineté des données et la position réglementaire qui en découle.

La continuité des soins est essentielle

Une mesure de confinement qui nécessite d'isoler une machine ou de forcer un redémarrage n'est pas acceptable lorsque la prise en charge des patients en dépend. La suspension sélective du seul processus malveillant permet de neutraliser l'attaque en moins de 200 millisecondes, tandis que les opérations médicales, les dispositifs connectés et les systèmes cliniques continuent de fonctionner.

Revision #1
Created 2026-07-24 07:00:29 UTC by Dennis Underwood
Updated 2026-07-24 07:00:29 UTC by Dennis Underwood