Como a Cyber Crucible apoia a conformidade com a HIPAA no setor de saúde?

Resposta curta: Toda a análise ocorre localmente, no nível do kernel, portanto as informações de saúde protegidas nunca saem do endpoint para o processamento de segurança. Isso evita a exposição relacionada à HIPAA criada por ferramentas de segurança que enviam arquivos ou chaves sensíveis para nuvens de terceiros, e interrompe os ataques sem tirar os sistemas clínicos do ar.

O problema da segurança hospedada por fornecedores

Muitos acordos de SOC e MDR hospedados por fornecedores exigem o envio de chaves, arquivos ou telemetria sensíveis para bancos de dados em nuvem de terceiros. Para uma entidade coberta, isso cria um risco real de conformidade e amplia o número de partes que lidam com dados protegidos.

Análise local, dados locais

A Cyber Crucible realiza a análise no endpoint. Os ativos sensíveis nunca saem do perímetro seguro do dispositivo — o que apoia tanto a soberania dos dados quanto a postura regulatória associada a ela.

A continuidade importa clinicamente

A contenção que exige isolar uma máquina ou forçar uma reinicialização não é aceitável quando o atendimento ao paciente depende dela. A suspensão seletiva apenas do processo malicioso significa que o ataque é neutralizado em menos de 200 milissegundos, enquanto as operações médicas, os dispositivos conectados e os sistemas clínicos continuam em funcionamento.

Revision #1
Created 2026-07-24 05:49:47 UTC by Dennis Underwood
Updated 2026-07-24 05:49:47 UTC by Dennis Underwood