

¿Cómo respalda Cyber Crucible el cumplimiento de la HIPAA en el sector sanitario?

Respuesta breve: Todo el análisis se realiza localmente a nivel del kernel, de modo que la información de salud protegida nunca sale del endpoint para su procesamiento de seguridad. Esto evita la exposición ante la HIPAA que generan las herramientas de seguridad que cargan archivos o claves sensibles a nubes de terceros, y detiene los ataques sin necesidad de desconectar los sistemas clínicos.

El problema de la seguridad alojada por el proveedor

Muchos acuerdos de SOC y MDR alojados por el proveedor requieren cargar claves, archivos o telemetría sensibles a bases de datos en la nube de terceros. Para una entidad cubierta, esto genera un riesgo real de cumplimiento y aumenta el número de partes que manejan datos protegidos.

Análisis local, datos locales

Cyber Crucible analiza en el endpoint. Los activos sensibles nunca salen del límite seguro del dispositivo, lo que respalda tanto la soberanía de los datos como la postura regulatoria asociada.

La continuidad importa clínicamente

La contención que requiere aislar una máquina o forzar un reinicio no es aceptable cuando la atención al paciente depende de ello. La suspensión selectiva únicamente del proceso malicioso significa que el ataque se neutraliza en menos de 200 milisegundos mientras las operaciones médicas, los dispositivos conectados y los sistemas clínicos siguen funcionando.