

Si se previene un ataque, ¿aún tenemos que reportar una brecha?

Respuesta breve: Generalmente no. Cuando un ataque se detiene antes de su ejecución y no se accede, altera ni exfiltra ningún dato, típicamente no hay una brecha que divulgar. Las obligaciones de divulgación suelen activarse por el acceso no autorizado a datos protegidos, no por un intento que fracasó.

Un ejemplo real

En la implementación de servicios financieros donde Cyber Crucible interceptó casi 10,000 procesos maliciosos, el resultado para el CISO incluyó cero divulgación regulatoria. Debido a que los ataques se detuvieron antes de su ejecución y no se tocó ningún dato, no hubo notificaciones requeridas a clientes, proveedores o reguladores gubernamentales, ni titulares de noticias, lo que preservó la confianza del cliente.

Una advertencia importante

Los requisitos de divulgación varían según la jurisdicción, la industria y el contrato, y los hechos específicos de un incidente importan. Cyber Crucible no es un bufete de abogados y esto no constituye asesoramiento legal. El principio confiable es que la prevención reduce drásticamente su exposición a la divulgación en comparación con la detección posterior al hecho, pero su asesor legal y su equipo de cumplimiento deben tomar la determinación para cualquier evento en particular.

Revision #1

Created 2026-07-24 01:51:16 UTC by Dennis Underwood

Updated 2026-07-24 01:51:16 UTC by Dennis Underwood