¿Cómo le ayuda Cyber Crucible con las expectativas de la FFIEC y de gestión de riesgos de terceros?

Respuesta breve: Cyber Crucible está diseñado para ser examinable frente a las expectativas de seguridad, operaciones y continuidad del negocio que los examinadores aplican a la tecnología bancaria, y su paquete de proveedor preparado está organizado para servir como la evidencia de diligencia debida que una institución financiera necesita conforme a la guía interagencial de 2023 sobre relaciones con terceros.

Más información: protección contra ransomware e infostealers para el sector financiero

En qué puede apoyarse el programa de un banco

- Detalle de controles mapeado a los dominios que se encuentran en los cuestionarios estándar (SIG, CAIQ) y a los Criterios de Servicios de Confianza de SOC 2 y al NIST CSF.
- Validación independiente de controladores (WHCP) como una atestación de calidad externa.
- Una postura de continuidad del negocio documentada y probada, con la propiedad importante de que la protección de endpoints continúa incluso durante una interrupción del backend de gestión.
- Evidencia de seguro, información financiera y una lista de subprocesadores disponibles para los revisores bajo solicitud.

Por qué la arquitectura reduce el riesgo de terceros

El dato más útil para un analista de riesgo de proveedores de un banco es que Cyber Crucible nunca recopila archivos, credenciales o claves de los clientes. Los datos que preocupan a un revisor de que un proveedor maneje mal no están bajo la custodia de Cyber Crucible para ser mal

manejados. Se trata de una reducción estructural del riesgo, no de una promesa de gestionarlo bien.

Revision #3
Created 2026-07-24 02:02:27 UTC by Dennis Underwood
Updated 2026-11-24 15:46:23 UTC by Dennis Underwood