Wie unterstützt Cyber Crucible bei den Erwartungen des FFIEC und an das Drittparteienrisikomanagement?

Kurze Antwort: Cyber Crucible ist so konzipiert, dass es im Hinblick auf die Sicherheits-, Betriebs- und Geschäftskontinuitätserwartungen, die Prüfer an Banktechnologie stellen, überprüfbar ist, und das vorbereitete Anbieterpaket ist so aufgebaut, dass es als Sorgfaltspflicht-Nachweis dient, den ein Finanzinstitut gemäß der 2023 veröffentlichten interagency guidance zu Drittanbieterbeziehungen benötigt.

Mehr erfahren: Ransomware- und Infostealer-Schutz für Finanzdienstleister

Worauf sich das Programm einer Bank verlassen kann

- Kontrolldetails, die den in Standardfragebögen (SIG, CAIQ) enthaltenen Domänen sowie den SOC 2 Trust-Service Criteria und dem NIST CSF zugeordnet sind.
- Unabhängige Treibervalidierung (WHCP) als externe Qualitätsbestätigung.
- Eine dokumentierte, getestete Geschäftskontinuitätshaltung, mit der wichtigen Eigenschaft, dass der Endpunktschutz auch bei einem Ausfall des Management-Backends weiterhin aktiv bleibt.
- Versicherungsnachweise, Finanzinformationen und eine Liste der Unterauftragsverarbeiter, die Prüfern auf Anfrage zur Verfügung stehen.

Warum die Architektur das Drittparteirisiko senkt

Die für den Vendor-Risk-Analysten einer Bank nützlichste Tatsache ist, dass Cyber Crucible niemals Kundendateien, Zugangsdaten oder Schlüssel erfasst. Die Daten, deren möglicher Missbrauch durch einen Anbieter einen Prüfer beunruhigt, befinden sich gar nicht erst im Besitz von Cyber Crucible, sodass ein Missbrauch ausgeschlossen ist. Dies stellt eine strukturelle Risikominderung

dar, kein bloßes Versprechen, das Risiko gut zu verwalten.

Revision #3
Created 2026-07-24 04:51:09 UTC by Dennis Underwood
Updated 2026-11-24 15:44:03 UTC by Dennis Underwood