Does Cyber Crucible meet FFIEC and third-party risk management expectations?

Short answer: Cyber Crucible is built to be examinable against the security, operations, and business-continuity expectations that examiners apply to bank technology, and its prepared vendor package is organized to serve as the due-diligence evidence a financial institution needs under the 2023 interagency guidance on third-party relationships.

What a bank's program can rely on

- Control detail mapped to the domains found in standard questionnaires (SIG, CAIQ) and to the SOC 2 Trust-Service Criteria and NIST CSF.
- Independent driver validation (WHCP) as an external quality attestation.
- A documented, tested business-continuity posture, with the important property that endpoint protection continues even during a management-backend outage.
- Insurance evidence, financial information, and a sub-processor list available to reviewers on request.

Why the architecture lowers third-party risk

The single most useful fact for a bank's vendor-risk analyst is that Cyber Crucible never collects customer files, credentials, or keys. The data a reviewer worries about a vendor mishandling is not in Cyber Crucible's custody to mishandle. That is a structural reduction in risk, not a promise to manage it well.

Revision #2
Created 2026-07-23 15:18:07 UTC by Dennis Underwood
Updated 2026-07-23 18:19:39 UTC by Dennis Underwood