Comment Cyber Crucible aide-t-il à répondre aux attentes du FFIEC et de la gestion des risques liés aux tiers??

Réponse courte : Cyber Crucible est conçu pour être auditable au regard des attentes en matière de sécurité, d'exploitation et de continuité d'activité que les examinateurs appliquent à la technologie bancaire, et son dossier fournisseur préparé est organisé pour servir de preuve de diligence raisonnable dont un établissement financier a besoin en vertu des directives interagences de 2023 sur les relations avec les tiers.

En savoir plus : protection contre les rançongiciels et les infostealers pour les services financiers

Sur quoi le programme d'une banque peut s'appuyer

- Un niveau de détail des contrôles cartographié selon les domaines des questionnaires standards (SIG, CAIQ) ainsi que selon les critères des services de confiance SOC 2 et le NIST CSF.
- Une validation indépendante des pilotes (WHCP) en tant qu'attestation de qualité externe.
- Une posture de continuité d'activité documentée et testée, avec la propriété importante que la protection des terminaux se poursuit même en cas de panne du backend de gestion.
- Des preuves d'assurance, des informations financières et une liste des sous-traitants disponibles sur demande pour les évaluateurs.

Pourquoi l'architecture réduit le risque lié aux tiers

Le fait le plus utile pour un analyste des risques fournisseurs d'une banque est que Cyber Crucible ne collecte jamais les fichiers, identifiants ou clés des clients. Les données qu'un évaluateur craint de voir mal gérées par un fournisseur ne sont pas sous la garde de Cyber Crucible, et ne peuvent

donc pas être mal gérées de ce fait. Il s'agit d'une réduction structurelle du risque, et non d'une simple promesse de bien le gérer.

Revision #3
Created 2026-07-24 07:12:32 UTC by Dennis Underwood
Updated 2026-11-24 15:47:45 UTC by Dennis Underwood