

Comment Cyber Crucible réduit-il le risque tiers et fournisseurs pour les acheteurs soumis à réglementation ?

Réponse courte : en supprimant le risque plutôt qu'en se contentant de le gérer. Les trois faits qui répondent aux questions les plus difficiles en matière de risque fournisseur sont les suivants : Cyber Crucible ne collecte aucun contenu client, aucune information d'identification ni aucune clé ; la protection s'exécute localement et survit à toute panne du backend ; et son IA n'existe qu'en phase de développement, jamais sur votre terminal. Ensemble, ces éléments réduisent considérablement la surface qu'un examen de diligence raisonnable est conçu pour sonder.

Les trois facteurs structurels de réduction du risque

- **Aucun contenu collecté.** Aucun fichier client, aucune information d'identification, aucune clé ne sont jamais collectés. Ce seul fait répond aux questions relatives à la PCI-DSS, aux données confidentielles et au scénario « que se passe-t-il en cas de violation » — les données ne sont tout simplement pas là pour être perdues.
- **Protection indépendante du backend.** Detect-Decide-Respond s'exécute localement, avec un objectif de temps de récupération effectif de zéro sur le terminal. Une panne totale du backend ne réduit pas la protection.
- **IA déterministe.** L'IA n'est utilisée qu'en phase de développement ; des heuristiques déterministes s'exécutent en temps réel. Pas de modèle en direct, pas de dérive, des résultats testables.

Renforcement par des tiers indépendants

Lorsque l'attestation indépendante a du poids, Cyber Crucible met en avant ce qui est réel : la signature de pilotes Microsoft WHCP, et — pour le backend géré — les attestations tierces des fournisseurs d'infrastructure sur lesquels il s'appuie. Ne disposant pas de sa propre certification SOC 2, ces éléments assument honnêtement cette charge plutôt que d'être survendus.

Revision #1

Created 2026-07-24 07:13:51 UTC by Dennis Underwood

Updated 2026-07-24 07:13:52 UTC by Dennis Underwood