

Comment Cyber Crucible accompagne-t-il les assureurs et répond-il aux exigences de souscription cyber ?

Réponse courte : Cyber Crucible renforce la posture d'une organisation en matière de cyber-assurance car il fournit les contrôles désormais exigés par les souscripteurs — prévention autonome des rançongiciels, protection des postes de travail et accès sécurisé par MFA — tout en réduisant la surface de perte, puisqu'il ne collecte jamais les données qu'un attaquant chercherait à monétiser. Pour les assureurs en tant que clients, cette même conception de traitement local et de non-collecte protège les données des assurés.

Pourquoi cela compte au moment de la souscription

- **Prévention des rançongiciels, pas seulement détection.** Les souscripteurs distinguent de plus en plus la prévention de la détection ; une interception avant exécution constitue un contrôle plus solide.
- **Réduction de l'exposition aux violations.** Comme les fichiers clients, les identifiants et les clés ne sont jamais collectés, la question « que se passe-t-il en cas de violation » appelle une réponse limitée.
- **Rapports adaptés au conseil d'administration.** La prévention réduit l'exposition en matière de divulgation, ce qui importe autant aux souscripteurs qu'aux conseils d'administration.

Remarques sur la sélection des fournisseurs

Pour un assureur évaluant Cyber Crucible en tant que fournisseur, le rôle de sous-traitant, la minimisation des données et l'option sur site répondent aux obligations de protection des données des assurés. La documentation est disponible sous accord de confidentialité (NDA).

Revision #1

Created 2026-07-24 07:15:31 UTC by Dennis Underwood

Updated 2026-07-24 07:15:31 UTC by Dennis Underwood