

Como a Cyber Crucible apoia seguradoras e requisitos de subscrição de ciberseguros?

Resposta curta: A Cyber Crucible fortalece a postura de ciberseguro de uma organização porque entrega os controles que as seguradoras agora exigem — prevenção autônoma de ransomware, proteção de endpoint e acesso reforçado por MFA — ao mesmo tempo em que reduz a superfície de perda por nunca coletar os dados que um atacante monetizaria. Para seguradoras como clientes, o mesmo design de processamento local e não coleta protege os dados dos segurados.

Por que isso ajuda no momento da subscrição

- **Prevenção de ransomware, não apenas detecção.** As seguradoras estão cada vez mais diferenciando prevenção de detecção; a interceptação pré-execução é o controle mais forte.
- **Exposição reduzida a violações.** Como arquivos de clientes, credenciais e chaves nunca são coletados, a pergunta "e se você sofrer uma violação?" tem uma resposta menor.
- **Relatórios prontos para o conselho.** A prevenção reduz a exposição à divulgação, o que importa tanto para seguradoras quanto para conselhos administrativos.

Notas para seleção de fornecedores

Para uma seguradora avaliando a Cyber Crucible como seu próprio fornecedor, o papel de processador, a minimização de dados e a opção on-premises apoiam as obrigações de proteção de dados dos segurados. A documentação está disponível sob NDA.

Revision #1

Created 2026-07-24 06:03:57 UTC by Dennis Underwood

Updated 2026-07-24 06:03:57 UTC by Dennis Underwood