Por que os MSPs e revendedores fazem parceria com a Cyber Crucible?

Resposta curta: Porque a prevenção autônoma permite que um parceiro fique com a margem, o relacionamento com o cliente e o SLA — em vez de revender um SOC hospedado por um fornecedor e assumir a culpa quando esse SOC não detecta um ataque em velocidade de máquina.

A armadilha de revender detecção

O setor empurrou os parceiros para revender serviços de MDR e SOC hospedados por fornecedores. Quando o monitoramento conduzido por humanos inevitavelmente deixa passar um ataque automatizado, o fornecedor perde a violação — e o cliente não demite o fornecedor. Ele demite o parceiro.

O que muda operacionalmente

- As ameaças são neutralizadas instantaneamente, antes que os analistas recebam um alerta.
- O volume de alertas cai drasticamente em relação aos mais de 100 por endpoint por dia que causam a fadiga de alertas.
- Não há ajuste de regras YARA nem caça manual a ameaças.
- Os parceiros capturam o fluxo de receita em vez de se contentarem com comissões do fornecedor.

E do lado do risco

Um parceiro cuja oferta de segurança previne ataques em vez de apenas documentá-los tem uma conversa fundamentalmente diferente com os clientes sobre resultados e responsabilização.

Revision #1
Created 2026-07-24 05:51:11 UTC by Dennis Underwood
Updated 2026-07-24 05:51:11 UTC by Dennis Underwood