Como devemos conduzir uma prova de conceito para uma ferramenta de prevenção?

Resposta curta: Implemente-a em conjunto com sua pilha de ferramentas existente em um ambiente de produção real e compare o que cada ferramenta detecta. O resultado mais informativo não é um teste em laboratório — é a lacuna entre o que suas ferramentas atuais alertam e o que realmente é interceptado.

Por que implementar em conjunto funciona melhor

A empresa de serviços financeiros do nosso caso mais bem documentado fez exatamente isso. Eles não removeram nada. Adicionaram o Cyber Crucible especificamente para descobrir o que seu investimento existente estava deixando passar, e obtiveram uma resposta definitiva em até 60 dias.

O que medir

- **Interceptações sobre as quais sua pilha atual nunca alertou.** Este é o sinal principal.
- **Tempo até a decisão.** A prevenção precisa ser concluída antes do dano ocorrer, não antes do fechamento de um chamado.
- **Interrupção nos negócios.** Conte o tempo de inatividade, reinicializações e interrupções causadas por falsos positivos.
- **Horas de analistas consumidas.** A prevenção autônoma deve reduzir a carga de trabalho, não gerar uma fila adicional.

Um alerta sobre testes em laboratório

Testar amostras retiradas de bancos de dados de malware muitas vezes mede muito pouco, pois os invasores projetam o malware para permanecer inativo, a menos que receba um sinal de validação de um servidor de comando e controle ativo que eles ainda operam. Uma amostra que não faz nada em seu laboratório não prova nada sobre um ataque real.

Revision #1
Created 2026-07-24 05:52:32 UTC by Dennis Underwood
Updated 2026-07-24 05:52:32 UTC by Dennis Underwood