Por que as equipas de segurança recebem milhares de alertas por dia e como podem lidar com isso?

Resposta breve: A sobrecarga de alertas não surgiu da noite para o dia — acumulou-se gradualmente à medida que os atacantes se tornaram mais automatizados e evasivos, transformando sinais de alerta antes claros em indícios ténues e ambíguos que exigem um profundo conhecimento especializado para serem interpretados. O Cyber Crucible foi criado para romper este ciclo, tratando a deteção e a resposta de forma automática, em vez de exigir que equipas humanas filtrem intermináveis sinais de baixa confiança.

Como a Fadiga de Alertas Se Tornou a Norma

A deteção de segurança não se degradou porque os fornecedores decidiram transferir o fardo para os clientes. Aconteceu lentamente, à medida que os atacantes refinaram as suas técnicas para mutarem e se automatizarem mais rapidamente do que as ferramentas defensivas conseguiam classificar de forma definitiva um evento como malicioso. O que antes era um indicador claro de comprometimento tornou-se um indício ténue perdido entre inúmeros outros indícios igualmente ténues. Analisá-los devidamente exige tempo considerável de analistas seniores, e muitas vezes aquilo que parece suspeito não é mais do que um controlador de impressora com mau funcionamento. Entretanto, um único alerta de baixa confiança que passe despercebido pode ser o único vestígio visível de uma intrusão grave e ativa.

Por Que Mais Alertas Não Significaram Melhor Segurança

À medida que as ferramentas de deteção tentavam acompanhar a evolução das ameaças, compensaram sinalizando qualquer coisa ligeiramente fora do comum. Isto criou uma torrente de alertas que, tecnicamente, cumpria o requisito de avisar os clientes, mas deixava as equipas de

segurança incapazes de investigar cada um de forma realista. O resultado natural é um de dois cenários: as equipas começam a ignorar alertas de baixa confiança — exatamente onde os atacantes mais sofisticados tendem a esconder-se — ou ficam sobrecarregadas, e o trabalho crítico simplesmente não é feito, independentemente do esforço ou da intenção.

Um Ponto de Partida Diferente

Reconhecendo que soluções incrementais não resolveriam um problema enraizado em anos de complexidade acumulada, a Cyber Crucible abordou a questão a partir de um ângulo totalmente diferente. Em vez de gerar mais alertas para os humanos analisarem, a nossa tecnologia FortressAI foi concebida para detetar e responder de forma autónoma, em tempo real, a ameaças de ransomware, roubo de dados e roubo de identidade. Utilizando abordagens modernas como a IA generativa, a Cyber Crucible visa reduzir a dependência da revisão manual de alertas e resolver o desequilíbrio subjacente entre a automatização dos atacantes e a capacidade dos defensores.

https://player.vimeo.com/video/1186492629

Ver no Vimeo · Legendas: English, Français, Español, العربية

Revision #1
Created 2026-07-24 06:14:55 UTC by Dennis Underwood
Updated 2026-07-24 06:14:55 UTC by Dennis Underwood