Por que os modelos tradicionais de SOC têm dificuldade contra ciberataques em velocidade de máquina?

Resposta curta: Os centros de operações de segurança tradicionais foram projetados para uma era de hacking mais lenta e previsível, dependendo de assinaturas e de análise humana para detectar ameaças após o fato. Os atacantes de hoje utilizam ferramentas automatizadas que sofrem mutação constantemente, portanto as defesas precisam migrar para abordagens preventivas e sem assinaturas, que operem mais rápido do que o próprio ataque.

Saiba mais: prevenção de ransomware e de roubo de credenciais ao nível do kernel (Cyber Crucible Core)

Como o cenário de ameaças mudou

Anos atrás, as ferramentas maliciosas se comportavam de maneiras bastante consistentes e identificáveis. As equipes de segurança conseguiam criar métodos de detecção com base em padrões conhecidos, pois os atacantes ainda não dependiam fortemente da automação para alterar constantemente suas técnicas. Essa abordagem funcionava bem o suficiente para capturar algumas das ameaças mais sofisticadas daquela época, incluindo ataques altamente direcionados descobertos há mais de uma década.

Esse cenário não existe mais. Os atacantes modernos utilizam automação para gerar variações rápidas de suas ferramentas, dificultando que a detecção baseada em assinaturas consiga acompanhar o ritmo. Quando uma nova assinatura é identificada, catalogada e implantada em toda a pilha de segurança, o atacante muitas vezes já avançou para uma nova variante.

Por que os modelos legados de SOC ficam para trás

Os fluxos de trabalho tradicionais de SOC dependem da identificação de indicadores conhecidos, seguida de investigação e resposta por meio de processos majoritariamente manuais ou semiautomatizados. Esse modelo pressupõe que os atacantes se movem em um ritmo que dá tempo aos defensores para analisar e reagir. Quando os ataques são automatizados e podem sofrer mutação em tempo real, essa premissa deixa de se sustentar, deixando uma lacuna persistente entre o surgimento de uma ameaça e o momento em que ela é tratada.

O que as defesas modernas precisam fazer em vez disso

As ferramentas de segurança agora precisam operar sem depender exclusivamente de assinaturas previamente conhecidas. Em vez disso, precisam detectar e prevenir comportamentos maliciosos diretamente, agindo em velocidade de máquina em vez de esperar por ciclos de análise conduzidos por humanos. A tecnologia FortressAI da Cyber Crucible foi construída com base nesse princípio, com foco em interromper tentativas de ransomware, roubo de dados e roubo de identidade por meio de ação preventiva e automatizada, em vez de correspondência de assinaturas após o fato.

https://player.vimeo.com/video/1182235055?texttrack=pt

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

Revision #3
Created 2026-07-24 06:09:40 UTC by Dennis Underwood
Updated 2026-11-24 15:50:09 UTC by Dennis Underwood