Por que as ferramentas de segurança baseadas em "coletores em nuvem" enfrentam dificuldades contra ataques modernos?

Resposta curta: Um coletor em nuvem é um agente leve para endpoint que realiza pouca análise local e, em vez disso, envia telemetria bruta para uma plataforma em nuvem para processamento. Essa ida e volta adiciona um atraso que um ataque automatizado não lhe concede, e o agente depende justamente dos componentes do sistema operacional que os invasores atualmente comprometem.

Por que o setor construiu dessa forma

A engenharia em nível de kernel é difícil e cara. Enviar a telemetria para a nuvem permitiu que os fornecedores criassem softwares de endpoint mais baratos, monetizassem o armazenamento em nuvem e divulgassem capacidades de "IA em nuvem". O modelo foi otimizado para facilitar o desenvolvimento, não para a defesa.

Os dois modos de falha

1. **Muito lento.** Ataques automatizados do tipo "smash-and-grab" se completam em milissegundos. As análises em nuvem não conseguem emitir uma resposta a tempo.
2. **Cego justamente quando mais importa.** Como esses agentes dependem de bibliotecas nativas do sistema operacional para funcionar e coletar dados, um invasor que comprometa essas bibliotecas pode silenciar o agente. Ele continua em execução, mas não reporta nada — um painel indicando que está tudo bem enquanto os dados são exfiltrados.

A Cyber Crucible processa localmente no kernel e toma suas próprias decisões, portanto não há ida e volta para a nuvem nem dependência de um sistema operacional potencialmente comprometido.

Revision #1
Created 2026-07-24 05:45:09 UTC by Dennis Underwood

Updated 2026-07-24 05:45:09 UTC by Dennis Underwood