Como o Cyber Crucible toma uma decisão em menos de 200 milissegundos?

Resposta curta: Ele executa um ciclo de três etapas — Detect-Decide-Respond — inteiramente no endpoint, ao nível do kernel, utilizando um mecanismo de análise de computação de borda (edge computing) patenteado. Como nada precisa viajar até um serviço na nuvem e voltar, e nenhum ser humano está envolvido no processo, todo o ciclo é concluído em menos de 200 milissegundos.

O ciclo

1. **Detect** — sensores inovadores ao nível do kernel identificam padrões de comportamento malicioso na memória, na atividade de processos e no acesso a arquivos.
2. **Decide** — o modelo comportamental aprimorado por IA avalia instantaneamente a intenção do acesso a dados do programa.
3. **Respond** — se a intenção for maliciosa, o programa é interceptado e suspenso.

Por que o processamento local é inegociável

Enviar telemetria para um servidor na nuvem, aguardar a análise e receber a resposta de volta adiciona milissegundos que o atacante utilizará com prazer. Para se ter uma ideia da escala envolvida: essa decisão ocorre mais rápido do que um impulso nervoso viaja do olho ao cérebro. Qualquer arquitetura que dependa de uma comunicação de ida e volta pela rede no caminho crítico já perdeu essa corrida.

A telemetria bruta ainda é copiada para servidores posteriormente, para fins de evidência e enriquecimento — mas a decisão de proteção nunca espera por isso.

Revision #1
Created 2026-07-24 05:47:01 UTC by Dennis Underwood
Updated 2026-07-24 05:47:01 UTC by Dennis Underwood