Em que é que a Cyber Crucible é diferente de EDR, XDR e MDR?

Resposta breve: EDR, XDR e MDR são ferramentas de deteção e resposta: observam um ataque, geram um alerta e dependem de um ser humano ou de um serviço na cloud para decidir o que fazer. A Cyber Crucible é uma ferramenta de prevenção: decide de forma autónoma no endpoint e interrompe o processo malicioso em menos de 200 milissegundos, antes de ocorrerem danos.

As diferenças práticas

	EDR / XDR / MDR	Cyber Crucible
Tempo de resposta	Minutos a horas	Menos de 200 milissegundos
Método de deteção	Assinaturas e dados históricos	Intenção comportamental, sem assinaturas
Cobertura de dia zero	Parcial	Concebida para ameaças desconhecidas
Dependência humana	Elevada — analistas e SOCs	Nenhuma — totalmente autónoma
Onde as decisões ocorrem	Análise na cloud	Localmente, no kernel

Porque é que esta diferença importa

As ferramentas de deteção foram concebidas para uma era em que os ataques se desenrolavam ao longo de horas ou dias. Os ataques automatizados concluem-se agora em segundos. Uma ferramenta que produz um alerta preciso depois de os dados terem sido exfiltrados documentou a perda, não a preveniu.

Isto não significa que a deteção não tenha valor — a análise forense e a investigação são importantes. Significa que a deteção por si só não consegue impedir um ataque à velocidade de uma máquina.

Revision #1
Created 2026-07-24 05:44:25 UTC by Dennis Underwood
Updated 2026-07-24 05:44:25 UTC by Dennis Underwood