

Como a IA é governada no ciclo de vida de desenvolvimento da Cyber Crucible?

Resposta rápida: Como a Genetic AI da Cyber Crucible é usada apenas em tempo de design, ela é governada sob o ciclo de vida de desenvolvimento seguro (SDLC) e não como um sistema de produção ativo. O trabalho de descoberta ocorre em um ambiente interno controlado, seu resultado é validado e traduzido em heurísticas determinísticas do kernel, e os drivers resultantes são assinados de forma independente sob o Microsoft WHCP antes do lançamento.

O ciclo de vida governado

Fase	Governança
Design	Requisitos de segurança definidos; a descoberta por IA faz parte da fase de design, sob o SDLC
Descoberta	A Genetic AI identifica variáveis determinísticas indicadoras de ataque usando apenas conjuntos de dados de pesquisa internos
Derivação	As descobertas se tornam heurísticas de kernel fixas e determinísticas — nenhum modelo ativo é implantado
Validação	Os resultados determinísticos são repetíveis e testáveis; modelos e drivers validados por meio de QA
Lançamento	Drivers do Windows assinados pelo WHCP; alterações seguem a gestão formal de mudanças

Dados e integridade

Nenhum conteúdo, credencial ou chave de cliente é usado para treinar, alimentar ou ajustar um modelo. Os modelos são proprietários e desenvolvidos internamente, sem dependência de modelos de terceiros. A integridade do modelo é mantida por meio de controle de versão, validação SDLC/QA e assinatura WHCP; a confidencialidade, por meio de um ambiente de desenvolvimento controlado.