Por que a Cyber Crucible utiliza IA em vez de uma equipe humana de SOC para conter ransomware?

Resposta curta: A Cyber Crucible foi construída como um sistema totalmente automatizado desde o primeiro dia, porque os ataques de ransomware se desenrolam muito mais rápido do que qualquer equipe de segurança humana consegue reagir, e a inteligência artificial é a única forma prática de modelar e agir sobre o comportamento de ataque em tempo real.

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

O Problema de Depender dos Tempos de Resposta Humanos

Quando a Cyber Crucible foi desenvolvida pela primeira vez, por volta de 2019, o ransomware já estava superando a capacidade de resposta das equipes de operações de segurança. Mesmo as primeiras variantes de ransomware conseguiam bloquear todos os sistemas de uma organização em poucos minutos. Isso não deixava nenhuma janela realista para que uma pessoa percebesse os sinais de alerta, avaliasse o que estava acontecendo e intervisse antes que ocorressem danos sérios. Desde então, os ataques só se tornaram mais rápidos—alguns relatórios sugerem que a rede de uma empresa de médio porte pode ser totalmente comprometida em apenas 90 segundos. Nessa velocidade, esperar que um analista humano detecte e interrompa um ataque em andamento simplesmente não é viável, independentemente de quão habilidosa ou bem equipada seja a equipe.

Por Que a Modelagem Comportamental Requer IA

Interromper um ataque tão rápido exige mais do que alertas velozes—exige um software capaz de reconhecer padrões de comportamento malicioso e tomar uma decisão de contenção instantaneamente, sem esperar que uma pessoa interprete os dados. Construir manualmente esse tipo de modelagem comportamental detalhada, cobrindo as diversas formas pelas quais um ataque pode se desenrolar, levaria muito mais tempo do que qualquer defensor tem disponível. A inteligência artificial se tornou a ferramenta necessária para construir esses modelos comportamentais com eficiência suficiente para serem incorporados diretamente ao software de segurança, permitindo que as decisões ocorram no exato momento em que um ataque começa, em vez de depois do fato consumado.

IA Como Necessidade Prática, Não Como Tendência

A adoção de uma defesa orientada por IA não teve relação com o acompanhamento de uma tendência do setor—foi uma resposta prática a um problema de tempo que o monitoramento baseado em humanos não conseguia resolver. A abordagem da Cyber Crucible reflete a ideia de combinar a ferramenta certa com a tarefa certa: quando os ataques se comprimem em segundos, a defesa precisa operar na mesma escala de tempo, o que significa tomada de decisão automatizada e baseada em IA, em vez de revisão manual.

https://player.vimeo.com/video/1046871333?texttrack=pt

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

Revision #3
Created 2026-07-24 06:14:35 UTC by Dennis Underwood
Updated 2026-11-24 15:50:03 UTC by Dennis Underwood