Daniel Miessler sobre o equilíbrio entre ataque e defesa da IA – Schneier s

Data: 2025-10-02 21:12:12

Autor: Inteligência Against Invaders

Dele conclusão:

> O contexto vence
>
> Basicamente, quem puder ver mais sobre o alvo e conseguir manter essa imagem em sua mente melhor, será o melhor em encontrar as vulnerabilidades mais rapidamente e aproveitá-las. Ou, como defensor, aplicando patches ou mitigações mais rapidamente.
>
> E se você está por dentro, sabe o que os aplicativos fazem. Você sabe o que é importante e o que não é. E você pode usar todo esse conhecimento interno para consertar as coisas – esperançosamente antes que os bandidos tirem vantagem.
>
> Resumo e previsão
>
> 1. Os atacantes terão a vantagem por 3-5 anos. Para equipes de defesa menos avançadas, isso levará muito mais tempo.
> 2. Após esse ponto, AI/SPQA terá o contexto interno adicional para dar vantagem aos Defensores.
>
> A tecnologia LLM está longe de estar pronta para lidar com o contexto de uma empresa inteira agora. É por isso que isso levará de 3 a 5 anos para que o verdadeiro Blue habilitado para IA se torne uma coisa.
>
> E, enquanto isso, o Red poderá usar o contexto publicamente disponível do OSINT, Recon, etc. para potencializar seus ataques.

Eu concordar.

A propósito este é a arquitetura SPQA.

Tags: IA, Ataque cibernético, defesa

Postado em 2 de outubro de 2025 às 12:19 •
1 Comentários

Foto da barra lateral de Bruce Schneier por Joe MacInnis.