

Können KI-Tools wie ChatGPT ein menschliches Cybersicherheitsteam ersetzen?

Kurze Antwort: Nein. Universelle KI-Tools können Sicherheitsarbeit unterstützen, indem sie Informationen zusammenfassen oder grundlegende Fragen beantworten, aber sie sind nicht zuverlässig genug, um ein geschultes Sicherheitsteam zu ersetzen, wenn es um echte Risikoentscheidungen geht.

Warum die Sicherheit von KI-Antworten irreführend sein kann

Tools wie ChatGPT präsentieren Antworten oft mit einem Ton der Gewissheit, selbst wenn die zugrunde liegenden Informationen unvollständig oder falsch sind. Dies kann ein falsches Gefühl von Autorität erzeugen, ähnlich wie bei einer überzeugenden Person, die etwas so selbstbewusst äußert, dass andere es als Tatsache akzeptieren, ohne es weiter zu überprüfen. Im alltäglichen Gespräch ist diese Art von fehlgeleitetem Selbstvertrauen ein kleineres Problem. In der Cybersicherheit, wo Entscheidungen darüber getroffen werden, wie eine Organisation Bedrohungen erkennt und darauf reagiert, kann die unkritische Übernahme ungenauer Ergebnisse zu echtem Schaden führen. Sicherheitsanalyse hängt von Kontext, Verifizierung und Urteilsvermögen ab, die aktuelle allgemeine KI-Modelle nicht vollständig nachbilden können.

Wo KI dennoch helfen kann

Trotz dieser Einschränkungen sind KI-Tools im Sicherheitskontext nicht ohne Wert. Sie können als Ausgangspunkt für Recherchen dienen, dabei helfen, Konzepte zu erklären, oder beim Verfassen und Organisieren von Informationen unterstützen. So eingesetzt, fungiert KI als Unterstützungswerkzeug und nicht als Entscheidungsträger. Entscheidend ist, den Unterschied zwischen KI, die einen sachkundigen Analysten unterstützt, und KI, die versucht, Risiken eigenständig zu bewerten und zu mindern, zu erkennen – Letzteres erfordert tiefere Fachkenntnisse, als diese Tools derzeit bieten können.

Das Argument für ehrliche Erwartungen

KI-Anbieter und Praktiker, die realistische Erwartungen setzen, anstatt zu übertreiben, was diese Tools leisten können, bauen mit größerer Wahrscheinlichkeit dauerhaftes Vertrauen auf. Die Fähigkeiten von KI im Sicherheitsbereich zu überverkaufen, birgt das Risiko, Vertrauen zu untergraben, sobald die Grenzen sichtbar werden. Klare, maßvolle Kommunikation darüber, was KI kann und was nicht, hilft Organisationen, fundierte Entscheidungen darüber zu treffen, wie sie diese verantwortungsvoll einsetzen können. Der Ansatz von Cyber Crucible spiegelt genau dieses Prinzip wider: Anstatt KI als Ersatz für qualifizierte Verteidiger darzustellen, sind autonome Schutztechnologien wie FortressAI so konzipiert, dass sie mit menschlichem Fachwissen zusammenarbeiten und die Fähigkeit einer Organisation stärken, Ransomware, Datendiebstahl und Identitätsdiebstahl zu verhindern, ohne vorzugeben, die Notwendigkeit einer informierten Aufsicht zu beseitigen.

<https://player.vimeo.com/video/1134578207>

[Auf Vimeo ansehen](#) · Untertitel: Englisch, Français, Español, العربية

Revision #1

Created 2026-07-24 05:01:31 UTC by Dennis Underwood

Updated 2026-07-24 05:01:31 UTC by Dennis Underwood