AI in Prozessen von IT-Sicherheitsteams: Effizienz und Genauigkeit steigern

Die zunehmende Verfügbarkeit und Leistungsfähigkeit von AI-Tools machen sie zu unverzichtbaren Hilfsmitteln für IT-Sicherheitsteams. AI-Algorithmen unterstützen Experten dabei, große Datenmengen zu analysieren, potenzielle Angriffe zu erkennen und Risiken durch Drittanbieter zu identifizieren. Sie ermöglichen das Scannen von Netzwerken nach Schwachstellen, die Automatisierung von Reaktionen auf Vorfälle und die Erkennung bedrohlicher Anomalien, was Sicherheitsteams einen Wettbewerbsvorteil verschafft.

Auswahl relevanter Prompts für die Optimierung von Sicherheitsprozessen mit AI

Der Schlüssel zur Nutzung eines AI-Modells für die Sicherheit des Unternehmens liegt im sogenannten „Prompting", bei dem dem Modell klare Anweisungen für seine Aufgabe gegeben werden. Mit folgendem Vorgehen können die effektivsten Ergebnisse erzielt werden:

- Sicherheitsziele festlegen: Die Prompts sind so zu formulieren, dass relevante Bedrohungen erkannt und identifiziert werden können. Vage oder mehrdeutige Prompts führen zu ungenauen Ergebnissen.
- Umfang der Sicherheitsaufgabe definieren: Beispielsweise kann ein Netzwerk-IP-Bereich angegeben oder festgelegt werden, auf welche Geräte zugegriffen werden soll.
- Kontext bieten: Das Modell braucht ein Verständnis über die Umgebung und die Sicherheitsherausforderungen, mit denen es konfrontiert wird.
- Analysen und Empfehlungen anfragen: Vom Modell sollten nicht nur Rohdaten erbeten werden, sondern auch eine Analyse der Daten und Empfehlungen, um spezifische Bedrohungen zu identifizieren und Abhilfestrategien vorzuschlagen.
- Ergebnisse überprüfen und validieren: AI-Modelle können Fehler machen. Sie sollten in Verbindung mit einer menschlichen Überprüfung und Entscheidungsfindung verwendet werden.

Abschaffung manueller Prozesse durch Mustererkennung

Die vermehrte Verwendung von AI-Tools anstelle manueller Analysen resultiert aus der Fähigkeit von Algorithmen des maschinellen Lernens (ML). Sie können große Datenmengen effizient analysieren und Muster erkennen. Diese Algorithmen können dabei helfen, subtile oder weitläufige Datenabweichungen sowie Angriffsmuster zu identifizieren, die für Menschen nur schwer erkennbar sind.

Um die manuelle, auf menschlicher Arbeit basierende Analyse zu stärken und zu ergänzen, können IT-Sicherheitsteams ML-Algorithmen wie folgt nutzen:

- Erkennung verdächtiger Aktivitäten im Netzwerkverkehr (z.B. Spitzen im Datenverkehr, Änderungen im Zugriff oder Zugriffsanfragen, die nicht mit den üblichen Aufgaben in Zusammenhang stehen)
- Analyse von Sicherheitsprotokollen (z.B. unbefugter Zugriff auf sensible Daten)
- Aufdeckung von Insider-Bedrohungen (z.B. sensible Unternehmensdaten offenlegen).

Dennoch sollten jegliche Ergebnisse stets von menschlichen Sicherheitsanalysten überprüft werden, um eine angemessene Interpretation und Einordnung in den realen Kontext sicherzustellen. Darüber hinaus ist es entscheidend, dass IT-Sicherheitsteams ML-Algorithmen kontinuierlich trainieren und die Qualität der Ergebnisse durch sorgfältige Datenauswahl sicherstellen, indem sie die Daten sorgfältig kuratieren, bereinigen und vorbereiten, idealerweise unter Verwendung von tatsächlichen Protokollen und forensischen Analysen historischer Ereignisse.

Verbesserte Sicherheitserkennung dank AI

AI-Tools tragen wesentlich zur Erhöhung der Sicherheit bei, indem sie Cyber-Bedrohungen in Echtzeit identifizieren, die Reaktion auf Vorfälle automatisieren und potenzielle Schwachstellen erkennen. Dies verkürzt die Zeit, die für die Erkennung, Eindämmung und Behebung von Cyberangriffen benötigt wird und gibt Angreifern weniger potenzielle Angriffsfläche.

Durch ihre Fähigkeit, große Datenmengen zu analysieren, Muster zu erkennen und aus Erfahrungen zu lernen, bieten AI-Tools eine wertvolle Ergänzung für das Sicherheitsportfolio jedes Unternehmens.

Von Tim Mullen, Chief Information Security Officer & Julian Head, Director of Information Security Architecture

Weiteres praktisches Wissen, wie AI effektiv in die täglichen Abläufe von IT-Sicherheitsteams integriert werden kann, bietet das AI Playbook von OneTrust. Es behandelt eingehend die verschiedenen Aspekte der AI-Nutzung, einschließlich potenzieller Risiken und bewährter Methoden, um sicherzustellen, dass AI-Anwendungen den aktuellen Compliance-Anforderungen entsprechen. Laden Sie das AI-Playbook herunter, um einen Leitfaden für den bestmöglichen Datenschutz zu erhalten und die unternehmensweite Nutzung von AI zu optimieren.