網路安全中的人工智慧 -- 既可用來為善，也可用以作惡？

2023 年 6 月 26 日發布 | 專家觀點

Rob Greer
副總裁兼總經理
賽門鐵克企業部門

從安全角度探討人工智慧生成技術

當我回顧自己職業生涯中最大的技術創新--網際網路、智慧型手機、社交媒體……時，一項新的突破值得在名單上佔據一席之地。生成式人工智慧（Generative AI）似乎已經席捲全球，影響著從軟體開發到市場行銷，再到餐桌上我們與孩子們的對話等方面。

在最近的六五高峰會 (Six Five Summit) 上，我有幸與派特・莫海德 (Pat Moorhead) 討論生成式人工智慧對企業網路安全的影響。與許多顛覆性創新一樣，生成式人工智慧雖然前途無量，有望為組織提供從根本上更好的成果，但同時也帶來一系列全新的網路安全風險和挑戰。

生成式人工智慧的主要風險

目前，生成式人工智慧為企業帶來三個主要風險：

敏感資料洩漏：企業用戶可能會在 ChatGPT 等人工智慧生成系統中輸入敏感資訊或其他公司機密資訊，有意或無意地暴露機密資訊並危及公司聲譽。

版權問題：企業員工使用生成式人工智慧來建立原始程式碼、圖像和文件等內容。但人們無法知道 ChatGPT 提供內容的來源，而該內容可能有侵犯他人版權疑慮，這給組織帶來風險。

攻擊者的濫用：也有人擔心攻擊者會利用 ChatGPT 等生成式人工智慧工具開發新的攻擊手段。雖然生成式人工智慧可以使攻擊者在某些任務上更有效率，但截至目前，它還不能建立全新的攻擊。生成式人工智慧系統是資訊內容開發工具，而不是機器人--你可以要求這樣的工具『告訴我所有感染機器的常見方法』，但你不能要求它『感染這家公司的這些機器』。

保護企業

那麼，安全專業人員該如何正確保護員工使用生成式人工智慧工具呢？

首先，每個組織都必須確定在自己環境中使用生成式人工智慧的政策，例如：在應用適當的安全控制同時，什麼是支援業務的最佳方法。鑒於我們仍處於生成式人工智慧的早期階段，各組織應定期審查並根據需要發展自己的政策。

賽門鐵克企業安全雲端使我們的客戶能夠執行其特定的生成式人工智慧政策。一些組織在解決這些問題時決定暫時禁止使用這些工具，並利用我們的安全網頁閘道 (SWG) 來實施此類控制。其他組織則允許謹慎使用生成式人工智慧，並導入賽門鐵克的 DLP 雲端服務，可對提交資料進行即時的精細檢查和矯正，以確保機密資訊不被洩露。我們的 DLP 雲端安全服務內建豐富

的經實務驗證過且立即可用的樣板，涵蓋最多關鍵監管類別的資料外洩預防策略，例如：HIPAA、PCI、PII……等。組織還可以為生成式人工智慧建立全新的 DLP 策略，或利用現有策略。更多詳情，請參閱賽門鐵克企業部落格和生成式人工智慧保護展示。

組織還應考慮提供明確、文字說明精準的要求，規定每位員工都有義務驗證生成式人工智慧工具的輸出的準確性、版權合規性以及是否符合公司的整體政策。

根據我們的預測，攻擊者最終會使用生成式人工智慧來更有效地建立和傳播新威脅。因此，組織必須高度警惕，確保其整體網路安全態勢（包括資訊、威脅、網路和電子郵件工具）能夠應對日益老練的攻擊者。迄今為止，生成式人工智慧無法創造出人類以前未曾創造過的全新攻擊技術。因此，我們的賽門鐵克解決方案經過精心調整，可以攔截這些攻擊，我們也使用生成式人工智慧作為為客戶建立防禦的一部分。

AI 對決 AI

鑑於攻擊者和防禦者 (網路安全公司) 都可以免費使用生成式人工智慧工具，因此對這種「軍備競賽」如何演變的擔憂是可以理解。

生成式人工智慧工具肯定會隨著時間繼續進化，並且在未來某個時候，此類工具可能可以針對特定目標組織生成並執行全新的攻擊。同時，安全公司將能夠利用此類工具來增強其防禦能力。在賽門鐵克，我們正在研究在每個解決方案中導入生成式人工智慧，以改進我們的防護並使安全專業人員的日常工作變得更加輕鬆。假以時日，我們可以利用解決方案中的生成式人工智慧來優化客戶特定的安全性政策、快速生成矯正指令、為資安監控中心 (SOC) 的分析師以技術觀點對安全資訊進行總結，並執行許多其他重要任務。

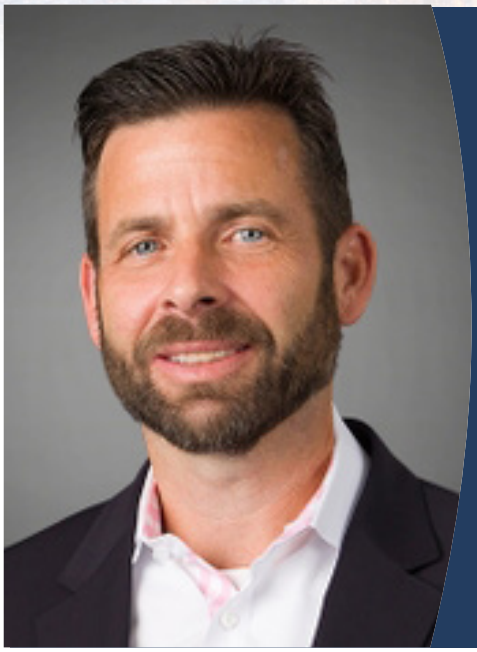
我們相信，誰擁有最強的運算能力，誰就最終佔優勢。OpenAI 開發 ChatGPT 所使用的龐大運算能力是該工具早期成功的關鍵因素。我們認為，安全公司將在運算能力和研究方面進行適當投資，以保持防禦者在這場競賽中的領先地位。

我們接下來應該怎麼做？

正如我們在其他顛覆性科技中看到的那樣，我們無法預測生成式人工智慧未來的發展。社群媒體最初是一種幫助人們透過桌上型電腦和筆記型電腦與朋友和家人保持聯繫的工具，後續的發展卻遠遠超乎所有人的想像。

同樣的，生成式人工智慧這股浪潮正在翻轉一切，包含改變我們的工作及生活。就像其他突破性科技，例如：網際網路、智慧型手機和社群媒體一樣，生成式人工智慧將帶來一系列前所未見的網路安全和隱私問題。使組織能夠從生成式人工智慧的強大力量中受益，同時保護他們免受相關風險的影響，必將推動新一波的網路安全創新浪潮。在賽門鐵克，我們正在全心全意投入其中，力求持續保持在網路安全的領先地位。

原廠網址：https://www.broadcom.com/blog/artificial-intelligence-in-cybersecurity-good-or-evil
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2023/6



關於作者

Rob Greer

副總裁兼總經理--賽門鐵克企業部門

Rob Greer 是博通公司 (Broadcom) 的賽門鐵克企業部 (SED: Symantec Enterprise Division at Broadcom) 副總裁兼總經理。在這個職位上，他負責賽門鐵克市場領先的網頁安全閘道 (SWG)、資料外洩防護 (DLP)、端點防護平臺 (EPP) 和電子郵件安全服務 (ESS) 解決方案營運核心的市場推廣、產品管理、產品開發和雲服務交付職能。

Greer 先生是在賽門鐵克企業安全業務收購加入公司，他最近的職務是資訊安全部副總裁。在此之前，他是 Forescout Technologies 公司的高級管理人員，在公司上市和任期內業務增長四倍的過程中發揮關鍵作用。在加入 Forescout 之前，他是惠普 TippingPoint 企業網路安全業務的副總裁兼總經理。在加入惠普之前，在賽門鐵克 (Symantec) 擔任四年的高層，期間領導了多項職能部門，包括企業行動業務以及核心安全、端點管理和資料外洩防護 (DLP) 業務。在此之前，他曾擔任 SonicWALL 全球系統工程副總裁，該公司被 Ignyte Technology 收購後加入 SonicWALL，並擔任該公司的創始人兼首席執行官。Greer 先生持有聖約瑟州立大學工商管理學士學位，主修管理資訊系統。

Symantec
A Division of Broadcom

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

保安資訊
KEEPSAFE
INFORMATION SECURITY

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。