The Pivotal Role of Artificial Intelligence in Cybersecurity

人工智能在網絡安全中的關鍵角色

Fortinet International Inc.

The Hong Kong government's recently proposed legislation on critical infrastructure operators (CIOs) highlights the growing regulatory focus on cybersecurity. The draft framework covers organizational, preventative, and reporting/response obligations for CIOs across sectors like communications and broadcasting.

One of the cybersecurity challenges is emerging threats like deepfake technology. Over the past year, Hong Kong authorities have reported several incidents where malicious actors leveraged deepfakes to scam companies, including one case where a multinational firm lost HK$200 million after employees were fooled by a digitally recreated video of the CFO ordering fraudulent fund transfers.

Amidst this shifting landscape, artificial intelligence (AI) is emerging as a powerful tool for bolstering cybersecurity defenses. AI-powered systems can automate and enhance a range of critical security functions, from threat detection to malware analysis and incident response.

香港政府最近提出針對關鍵基礎設施營運者（CIO）的立法建議，此舉突顯了正加強對網路安全的監管。該草案框架涵蓋了CIO在通信到廣播等多個行業中的架構、預防以及事故通報及應對的責任。

新興威脅如深度偽造技術正為網路安全帶來全新挑戰。過去一年，香港監管機構公布多宗惡意行為者利用深度偽造技術進行欺詐的騙案，其中一個個案中，騙徒利用相關技術製作影片並模仿成為一家跨國企業的首席財務總監，藉此欺騙員工進行資金轉移並造成2億港元的損失。

面對不斷變化的形勢，人工智能（AI）正成為提升網絡安全防禦不可或缺的工具。不論是威脅偵測、惡意軟件分析以至事故應對等一系列的網絡安全功能，都可以透過AI驅動的系統進行自動化及增強。

Applications of AI in Cybersecurity

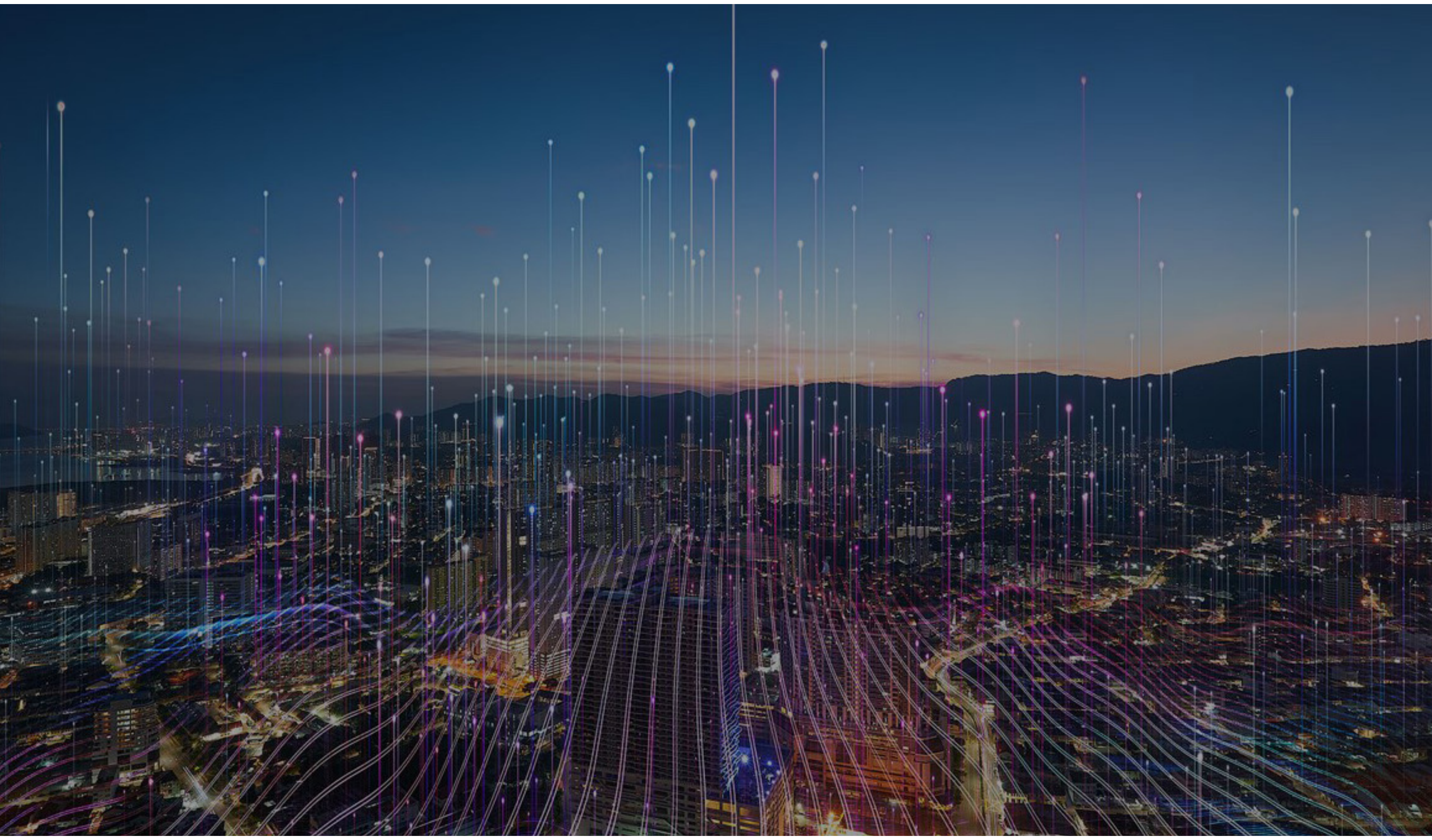
AI in cybersecurity has various applications, including:

1. Password protection and authentication: AI tools, such as CAPTCHA, facial recognition, and fingerprint scanners, enable organizations to automatically detect whether an attempt to log in to a service is genuine, better protecting passwords and securing user accounts.
2. Phishing detection and prevention: Phishing remains one of the biggest cybersecurity threats facing businesses. AI-powered email security solutions can leverage machine learning algorithms to discover anomalies and indicators of malicious messages, helping organizations prevent these attacks.
3. Vulnerability management: As cyber criminals deploy more sophisticated methods, thousands of new vulnerabilities are discovered and reported every year. AI-powered security solutions, such as user and entity behavior analytics (UEBA), enable businesses to analyze the activity of devices, servers, and users, helping them identify anomalous or unusual behavior that could indicate a zero-day attack.
4. Network security: Creating and maintaining security policies across multiple networks requires significant time and manual effort. AI can learn an organization's network traffic patterns over time, allowing it to recommend the right policies and workloads, thereby enhancing network security.
5. Behavioral analytics: Traditional security defenses rely on attack signatures and indicators of compromise (IOCs) to discover threats. Organizations can implement behavioral analytics, using AI models to develop profiles of the applications deployed on their networks and process vast volumes of device and user data, to enhance their threat-hunting processes.

AI 在網絡安全中的應用

AI 在網絡安全有多種應用，包括：

1. 密碼保護與認證：AI 工具如 CAPTCHA、面部識別和指紋掃描器，能讓企業自動識別用家登錄的真偽，從而更好地保障密碼和用戶帳戶安全。
2. 識別和防禦釣魚攻擊：釣魚攻擊仍是企業面臨的最大網絡安全威脅之一。AI 驅動的電郵安全方案可以利用機器學習演算法來識別異常情況和惡意訊息的特徵，協助企業防止有關攻擊。
3. 漏洞管理：隨著網絡犯罪分子運用更複雜的方法，每年都有數千個新漏洞被發現。AI 驅動的網絡安全方案，如用戶和實體行為分析（UEBA），使企業能分析設備、伺服器和用戶的活動，幫助它們識別異常行為和潛在的零日攻擊。
4. 網絡安全：建立和維護跨網絡的安全策略需要甚多的時間和人力。AI 可以透過持續學習企業的網絡流量模式，推薦合適的策略和工作負載，從而增強網絡安全。
5. 行為分析：傳統安全防禦依賴入侵攻擊的特徵和入侵指標（IOC）來偵測威脅。企業可以進行行為分析，利用 AI 模型建立用於網絡應用程序的配置檔案，及處理大量的設備和用戶數據，從而增強其識別潛在威脅的能力。



The Future of AI in Cybersecurity

As cyber threats continue to evolve, AI in cybersecurity is playing an increasingly pivotal role in the fight against more advanced attacks. New technologies built on AI processes and techniques are crucial for identifying the latest threats and preventing hackers from exploiting new vulnerabilities in the quickest time possible.

The benefits of integrating AI in cybersecurity are manifold, including:

- Ongoing learning: AI's capabilities constantly improve as it learns from new data, enabling techniques like deep learning and machine learning to recognize patterns, establish baselines of regular activity, and discover any unusual or suspicious behavior.
- Discovering unknown threats: As cyber criminals devise more sophisticated attack vectors, AI provides a solution for mapping and preventing unknown threats, including vulnerabilities that have yet to be identified or patched.
- Handling vast data volumes: AI systems can process and understand vast amounts of data that security professionals cannot, allowing organizations to automatically discover new threats among extensive network traffic and data that might go undetected by traditional systems.
- Improved vulnerability management: AI enables organizations to assess their systems more effectively, improve problem-solving, and make better decisions. It can also identify weak points in networks and systems, ensuring organizations focus on the most critical security tasks.
- Enhanced overall security posture: Manually managing the risk of a range of threats can be challenging and time-consuming. With AI, organizations can detect various types of attacks in real-time and efficiently prioritize and prevent risks, resulting in a stronger security posture.
- Better detection and response: Threat detection is a vital element of data and network protection. AI-enabled cybersecurity can lead to rapid detection of untrusted data and more systematic and immediate response to new threats.

The role of AI in cybersecurity is increasingly critical for protecting against evolving cyber threats. By leveraging AI's benefits, organizations can enhance security, improve vulnerability management, and better detect and respond to a wide range of attacks, strengthening their defenses against the growing threat landscape.

AI 在網絡安全中的未來

隨著網絡威脅不斷演變，AI 在網絡安全中的角色越見關鍵，以對抗更先進的攻擊。建基於 AI 程序和技術工具的新科技對於識別最新威脅和防止黑客在最短時間內利用新漏洞至關重要。

將 AI 融入網絡安全的好處多不勝數，包括：

- 持續學習：AI 的能力隨著它從新數據中學習而不斷提高，如透過深度學習和機器學習技術以辨認模式、建立常規活動的基線，並識別任何不尋常或可疑的行為。
- 發現未知威脅：隨著網絡犯罪分子設計出更複雜的攻擊手段，AI 能提供應對和防止未知威脅的方案，包括尚未被識別或修補的漏洞。
- 處理龐大數據：AI 系統可以處理和理解安全專家無法處理的大量數據。即使是因為龐大網絡流量和數據而被傳統系統忽視的新威脅，企業亦能靠此自動發現。
- 改善漏洞管理：AI 使企業能夠更有效地評估其系統，提升解難能力，並做出更明智的決策。AI 還可以識別網絡和系統中的弱點，以確保企業專注於最關鍵的安全工作。
- 增強整體安全防禦：以人手管理各種威脅的風險既具挑戰性又耗時。借助 AI，企業可以實時偵測各種攻擊，有效地優先處理和防範風險，從而強化其安全防禦。
- 更好的偵測和應對：威脅偵測是數據和網絡保護的關鍵元素。AI 驅動的網絡安全可以對不可信的數據進行快速偵測，並對新威脅進行更系統化和即時的應對。

為應對不斷演變的網絡威脅，AI 在網絡安全的角色變得更為關鍵。善用 AI 的優勢，企業可以增強安全性、改善漏洞管理並更有效地偵測和應對各種攻擊，強化其防禦，以應對日益增長的威脅。