網路安全挑戰：GenAI 漸強 IoT 仍漏洞百出

■文：編輯部

技術的不斷進步，在為人們創造更多便利的同時，也讓助長了網路犯罪活動，網路安全威脅在不斷演變。本文將結合多篇近期的網路安全報告，從當前全球網路安全態勢，包括關鍵技術發展、威脅行為者活動、以及網路安全防禦策略，分析網路安全的現狀，探討未來可能面臨的挑戰。

在 CYBEREDGE 的 2024 年《網路威脅防禦報告》指出，在過去的一年中，有 82% 的機構或組織去年至少遭受了一次成功的網路攻擊，在支付贖金的勒索軟體受害者中，只有 57% 恢復了他們的資料，86% 的安全團隊面臨技能短缺，各公司或組織 2024 年的安全預算增長了 5.7%。

IDC 通過對全球 500 多位安全和 IT 運營領導者展開調研，瞭解到當前企業對現代安全威脅的看法和實現網路彈性的方法。其中 61% 的受訪者認為由於攻擊日益精進，在未來 12 個月內“可能”或“非常可能”發生資料丟失。受訪者認為本地工作負載比雲工作負載更易受到攻擊。

IBM 發佈的《2024 年資料洩露成本報告》指出：2023 年 3 月至 2024 年 2 月間全球 604 家機構的資料洩露事件，這些資料洩露事件的平均成本在 2024 年創下 488 萬美元的新高，同比增加 10%。這是自 2020 年以來資料洩露成本增幅最大的一年。70% 的受訪企業表示，資料洩露造成了重大或非常重大的損失。

CertiK 公佈的資料顯示，在 2024 年第二季度，共發生了 184 起鏈上安全事件，損失金額達到 6.88 億美元，與 2024 年第一季度相比，損失金額增加了 37%。其中，釣魚攻擊最為嚴重，造成了 4.33 億美元的損失；私密金鑰洩露事件緊隨其後，共造成 1.7 億美元的損失。乙太坊受到的打擊最為嚴重，83 起事件共造成了 1.7 億美元的損失。儘管發生了這些安全性漏洞，但最終有 9,900 余萬美元的資金被追回，使得該季度最終的實際損失為 5.89 億美元。

這表明網路安全造成的損失正在擴大。

一．當前網路安全威脅態勢

1.AI 技術的快速發展與安全挑戰

隨著人工智慧、區塊鏈和量子計算等新技術的快速發展，網路安全問題日益凸顯。這些技術在推動社會進步的同時，也為網路犯罪分子提供了新的攻擊手段。例如，生成式人工智慧 (GenAI) 技術被用於創建深度偽造內容，進行精准的網路釣魚攻擊。

網路犯罪組織利用 GenAI 實施誘騙使用者資訊：利用 AI 生成高度逼真、針對性強的釣魚郵件。這些郵件在內容上與正常的業務郵件或個人通信極為相似，無論是語言表達、格式還是語氣都很難讓收件人察

覺出異常。例如，AI 可以根據目標使用者的興趣愛好、工作領域等資訊，生成與之相關的郵件主題和內容，誘導使用者點擊郵件中的連結或下載附件，從而獲取使用者的敏感資訊，如帳號密碼、銀行卡號等。

借助 AI 生成圖片、視頻、音訊等多媒體內容來欺騙使用者，利用 AI 合成逼真的語音資訊，模仿主管、同事、客服等的聲音，通過電話或語音資訊進行詐騙。

此外，AI 技術還被訓練用來破解密碼與身份驗證，尋找系統漏洞與弱點以及實施深度偽造攻擊，利用 AI 技術生成虛假的身份資訊，包括頭像、個人資料、社交網路動態等，以此來偽裝成合法的用戶或機構。駭客可以利用這些偽造的身份在網路上進行社交工程攻擊，獲取他人的信任，進而竊取敏感資訊或進行其他惡意活動。

2. 勒索軟體與針對性攻擊的增加

勒索軟體攻擊者正在利用自動化、人工智慧 (AI) 和超大規模雲系統來擴大攻擊規模和提高盈利能力。在近一年的各種報告中，勒索軟體攻擊的頻率和規模都在上升，針對關鍵基礎設施的攻擊可能導致災難性後果。針對性攻擊，如高級持續性威脅 (APT) 攻擊，變得更加複雜且隱蔽，對特定行業或組織構成嚴重威脅。

微軟的《2023 年數字防禦報告》(Microsoft Digital Defense Report 2023) 指出：勒索軟體運營商越來越多地採用手動加密和資料洩露技術，以隱藏他們的蹤跡。80-90% 的成功勒索軟體入侵源自未管理的設備。針對中小企業的針對性勒索軟體攻擊增加了 200% 以上。

2023 年 IBM《資料洩露成本報告》(Cost of Data Breach Report) 報告發現，人工智慧及自動化讓資料洩露處理週期縮短了 108 天；未尋求法律說明的勒索軟體受害者平均遭受 47 萬美元的額外損失；只有三分之一的企業能夠依靠自身檢測到漏洞。2023 年全球資料洩露的平均成本達到 445 萬美元，創該報告有史以來以來最高記錄，也較過去 3 年均值增長了 15%。同一時期內，檢測安全性漏洞和漏洞惡化帶來的安全成本上升了 42%，占安全性漏洞總成本的比值也來到史上最高。

一些被研究組織在遭勒索軟體攻擊後仍不願與執法部門接觸，因為他們擔心這只會使情況變得複雜。今年，IBM《資料洩露成本報告》首次深入研究了這個情況，並證明，結論與擔憂的恰恰相反。無執法部門介入的情況下，被攻擊組織的資料洩露生命週期比有執法組織介入的情況平均長 33 天。而這種 " 沉默 " 意味著巨大的代價。研究表明，相比採取法律行動的勒索軟體受害者，未採取法律行動的受害者平均要承受高出 47 萬美元的資料洩露成本。

趨勢科技 (Trend) 在 2024 年上半年的報告指出，銀行、科技與政府機關是今年上半年

圖說：勒索軟體受害者在涉及執法時節省了時間和金錢

圖片來源：IBM

遭勒索病毒攻擊最多的前三大產業，而即便全球執法機關 2 月成功瓦解 LockBit 的攻擊行動，LockBit 仍是上半年檔案偵測數量最多的勒索病毒，偵測數量超過其他勒索病毒家族的一半以上。趨勢科技提醒，勒索病毒集團仍不斷地演變，試圖採用各種不同的攻擊手法、技巧與程式 (TTP) 來進行突破防線、長期潛伏受害者系統、存取登入憑證等動作以竊取資料、操作加密勒索任務。

3. 物聯網設備的安全風險

物聯網 (IoT) 設備的廣泛部署帶來了新的安全挑戰。這些設備往往安全防護不足甚至沒有防禦機制的狀態，很容易成為攻擊者的主要目標。從路由器、攝像頭到工業物聯網邊緣設備，IoT 設備的安全性問題日益突出。

很多物聯網設備由於尺寸功耗的限制，因此在軟硬體安全防護、通信方式、資料傳輸方面相對薄弱，甚至很多部署在邊遠地區的物聯網設備，面對物理攻擊也無法做出有效應對。

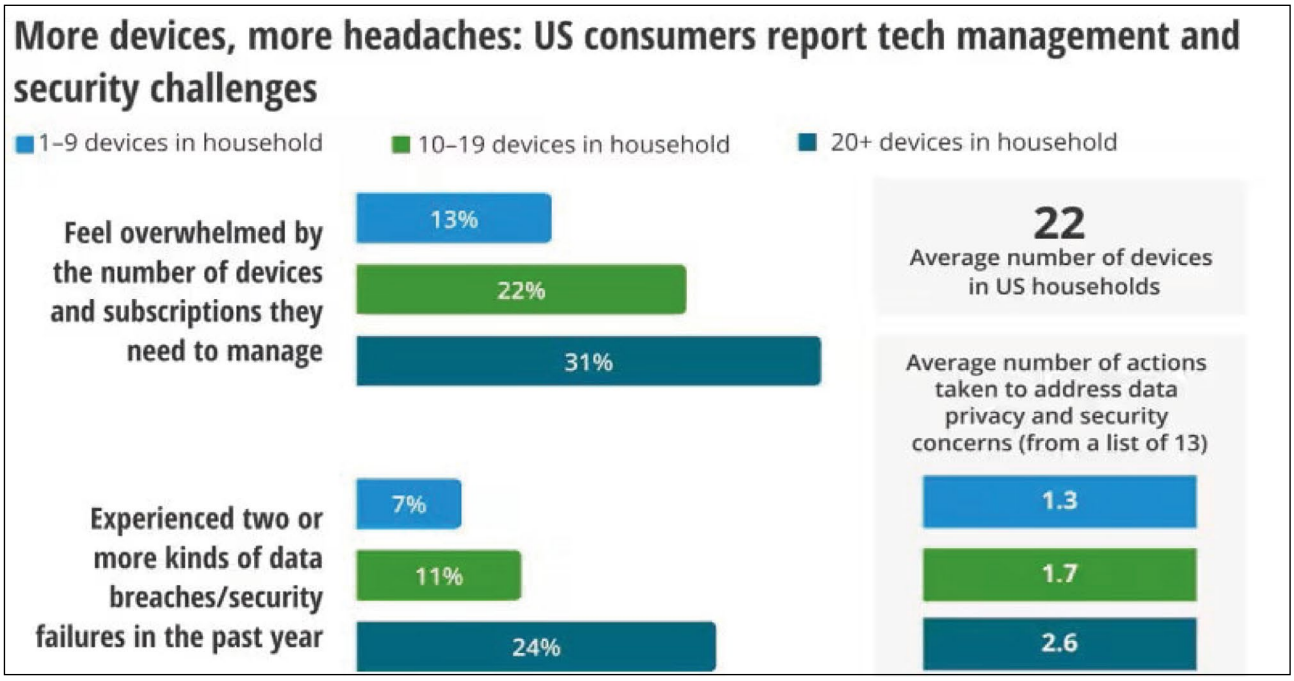
最近的研究估計，當今企業平均擁有 3,000 多台互聯的物聯網設備，而 2020 年只有不到 700 台。這種快速增長是由多種因素推動的，包括感測器成本的下降以及低功耗連接選項 (如低功耗藍牙和 LoRa) 的激增。最近的研究還預測，未來幾年互聯物聯網設備的數量將繼續增加，到 2025 年，平均每個企業將超過 9,000 台。

隨著 IT 與 OT 進一步融合，企業物聯網資產與漏洞管理、威脅檢測與事件回應難度不斷加大。供應鏈攻擊、地緣政治衝突、國家駭客與 APT 組織對工業物聯網和關鍵基礎設施的威脅不斷增長。

根據 Deloitte 的連接和移動趨勢 (CMT) 調查，隨著物聯網的不斷擴展，平均每個家庭擁有 22 台智慧設備，保護這些設備的挑戰變得越來越複雜。

2024 年，物聯網安全威脅焦點將向邊緣轉移，經常被忽視的邊緣設備 (包括防火牆、路由器、VPN、交換機、多工器和閘道等) 正在成為勒索軟體和 APT 組織的熱門目標。(物聯網) 邊緣設備面臨獨特的網路安全挑戰，因為駭客將更多

圖說：德勤研究報告指出 物聯網設備的迅速普及使得其安全問題變得複雜



圖片來源：deloitte.com

地利用零日漏洞來實現長期駐留和訪問，而且這些邊緣設備與傳統網路元件不同，難以通過部署 IDS/IPS 進行入侵偵測。

4. 網路安全防禦能力不足

儘管 2024 年企業和機構的平均 IT 安全預算增長了 5.7%，而且 6 成以上的公司配備了具有安全背景的董事會成員，但是這些投入仍顯不足。安全性漏洞未及發現，即便發現也需要花費較長事件來修復。

以雲端應用為例，40% 的安全應用程式和服務通過雲部署。企業的上雲速度正在加快。到 2025 年，企業和機構的雲端市場預計將從 2021 年的 3,700 億美元增長至 8,300 億美元。威脅者往往會利用雲中的常見問題發動入侵，例如配置錯誤、憑證弱、身份驗證不足、漏洞未修復、惡意 OSS 資源包等。

派拓網路副總裁兼亞太及日本地區首席安全官 Sean Duca 表示：“雲技術的發展日趨成熟。但隨著雲使用量不斷上漲，威脅者也變得更加狡猾和強大，他們會利用隱藏的薄弱環節和漏洞實施攻擊。雲物件存儲服務的大範圍採用加劇了企業的安全緊張態勢，使攻擊者能夠更快、更輕易地入侵共用軟體供應鏈，同時伏擊大量受害者。雲給威脅者提供了可乘之機——一旦管理不當，企業就會暴露於風險之中。因此，企業需要採取全面的平臺策略，在雲環境被入侵之前即時發現和消滅威脅。”

而 Palo Alto Networks (派拓網路) 的研究發現，受害者企業的安全團隊平均需要 145 個小時 (6 天) 解決一個警報，這給給潛在攻擊者留下了大量可乘之機。

此外，安全意識和培訓的缺乏也使得員工容易成為釣魚攻擊等社會工程學攻擊的目標。遠端工作的增加也帶來了新的安全風險，如對 VPN、RDP 等遠端存取技術的依賴。

根據 Gartner 的報告，2022 年 82% 的資料洩露是“員工不安全或疏忽行為造成的”，三分之一的成功網路攻擊來自影子 IT，給企業造成數百萬美元的損失。而影子 AI 正在加速放大這種“人為因素”產生的威脅。

根據 The Conference Board 的一項調查，56% 的北美企業員工在工作中使用生成式 AI，但只有 26% 的企業制定了明確的生成式 AI 使用政策。在沒有制訂 AI 政策的企業中，使用影子 AI 的員工中只有 40% 向主管如實彙報。

很多公司都在嘗試限制或規範員工在工作中使用生成式 AI 的行為。但是，在提高生產力的需求刺激下，多達 30% 的員工在沒有 IT 部門的許可，不計後果地使用生成式 AI，也就是所謂的影子 AI，這些 AI 工具在給使用者帶來便利的同時，也是攻擊者手中的利器。

二・未來網路安全挑戰

生成式 AI 應用如火如荼的大型語言模型，在激發生產力的同時也被網路犯罪分子濫用進行正在成為攻擊的武器。

GPT-4、Claude 和 PaLM2 等領先的大語言模型在生成連貫文本、回答複雜查詢、解決問題、編碼和許多其他自然語言任務方面取得了突破性的進展，讓威脅者發現了一種經濟高效的工具，使用這項工具，威脅者們無需大量專業知識、時間和資源就可發動大規模針對性攻擊。

2023 年，FraudGPT 和 WormGPT 等武器化的惡意大語言模型工具已經在網路犯罪網路中佔據主導地位，用於自動化創建網路釣魚電子郵件、假冒網頁以及能夠逃避檢測的惡意軟體，使得大規模網路釣魚活動變得更便宜且更容易實施。根據 CrowdStrike 的報導，惡意大語言模型已經成為暗網最暢銷的駭客工具，吸引了數以千計的不法分子。

惡意大語言模型應用極大

圖說：惡意軟體家族區域流行度排行榜　　圖片來源：fortinet.com

	非洲	亞洲	欧洲	拉丁美洲	中东	北美洲	大洋洲
JS/Agent	40.9%	34.2%	34.0%	37.4%	30.9%	30.0%	35.9%
JS/Phishing	17.6%	15.9%	19.2%	19.8%	12.7%	12.0%	18.5%
MSIL/Kryptik	17.4%	22.6%	19.8%	16.6%	16.9%	4.8%	7.5%
HTML/Phish	16.5%	19.9%	18.6%	15.2%	13.9%	7.9%	12.0%
JS/ScrInject	20.1%	13.1%	11.9%	18.6%	33.4%	10.3%	18.7%
JS/Cryxos	12.8%	28.6%	13.6%	14.7%	12.1%	13.3%	18.7%
MSIL/GenKryptik	14.6%	20.8%	17.9%	16.1%	15.4%	4.3%	7.2%
PDF/Phishing	14.1%	12.8%	14.9%	12.9%	11.2%	8.9%	14.1%
MSIL/GenericKDS	11.8%	19.1%	15.2%	13.6%	12.7%	3.7%	6.1%
HTML/Phishing	12.5%	13.1%	12.0%	9.6%	9.2%	5.6%	7.3%
MSIL/Agent	11.6%	16.1%	14.6%	11.4%	12.1%	3.5%	5.6%
MSOffice/CVE_2018_0798	9.8%	15.0%	15.1%	9.4%	10.2%	3.4%	4.7%
JS/Redirector	13.7%	7.7%	9.6%	8.0%	7.8%	7.5%	10.7%
MSIL/Stealer	9.5%	14.6%	11.8%	10.3%	10.3%	2.8%	4.5%
NSIS/Injector	8.5%	13.4%	13.1%	7.1%	10.1%	2.4%	5.3%
MSOffice/CVE_2017_11882	8.4%	12.1%	11.0%	17.6%	9.5%	2.5%	3.4%
HTML/infObfus	11.8%	5.9%	6.3%	4.2%	10.1%	10.5%	15.7%
BAT/Agent	5.5%	9.1%	6.3%	9.0%	6.7%	3.7%	4.3%
W32/Injector	8.6%	11/9%	8.9%	6.8%	9.0%	2.2%	3.0%
MSExcel/CVE_2017_11882	8.2%	12/3%	8.6%	5.0%	7.4%	2.3%	3.3%

地降低了網路犯罪的門檻並極大提高攻擊效率和成功率，預計 2024 年惡意大語言模型工具的開發和濫用將加速，惡意軟體的數量將以前所未有的速度增加。

Fortinet 發佈《2024 年網路威脅趨勢預測報告》預測高級持續性網路犯罪變得更加複雜且更具針對性、網路犯罪集團之間的“地盤爭奪戰”愈加激烈以及 AI 應用於攻擊戰術的巨大變革。

趨勢 1：Attack Playbook 再升級

隨著越來越多的網路犯罪分子發起勒索軟體攻擊，以期獲得豐厚回報，攻擊者也將更精密、更複雜的攻擊技術滲透網路，攻勢愈發猛烈。我們預測 2024 年網路犯罪分子將更加倡狂，且抱著“要麼出衆，要麼出局”的心態，爭相擴大目標清單和 Attack Playbook (攻擊預定步驟和策略)。而且，不法分子還將繼續追逐“高額獲利”，將攻擊目標轉向醫療保健、公用事業、製造業和金融業等關鍵基礎設施行業，試圖挖掘成功入侵後可對社會產生重大不利影響的目標。除了將目光投向更高價值目標外，攻擊者還將升級現有戰術，其 Attack Playbook 將變得更加激進和更具破壞性，攻擊手段將從資料加密轉為拒絕服務和敲詐勒索。

趨勢 2：零日威脅更易獲利

隨著組織不斷擴大其賴以支援日常業務運營的平臺、應用程式和技術的數量，犯罪分子在發現和利用軟體漏洞方面得以獲得無數可乘之機。對於攻擊者而言，發現新的零日威脅非常有利可圖。鑒於這類漏洞的高價值屬性，Fortinet 預測許多零日漏洞不會被公開披露。可以預見，未公開披露的零日漏洞對攻擊者而言更具價值，因為攻擊者可通過利用多數人未發現的零日漏洞勒索更多的不義之財，這意味著安全團隊需時刻保持高度警惕，沉著佈防洶湧而來的零日漏洞攻擊。與此同時，組織不應忽視“N-days”漏洞，應將其視

為仍具有攻擊性的零日漏洞。Fortinet 預測，CaaS 社區將出現“零日經紀人”，即一類在暗網上向多個買家兜售零日漏洞的網路犯罪集團。“零日經紀人”的興起將成為網路犯罪分子擴展攻勢的有效路徑，並通過更協同配合的攻擊活動挖掘更廣泛的攻擊面。

趨勢 3：內部威脅持續上升

為有效應對不斷演進的威脅態勢，許多組織正著手升級安全控制措施，並採用新技術和新流程強化防禦機制。這些效能增強的控制機制，使攻擊者從目標群組織內部招募人員協助其完成初始訪問。例如，網路犯罪分子可輕易使用生成式 AI，克隆高管或授信人員的聲音，繼而利用這些偽造錄音，迫使毫無戒心的目標執行命令、洩露密碼或資料甚至進行資金轉帳。我們預測，招募即服務模式將發展為下一個新趨勢，？明攻擊者獲得更多資訊以分析其潛在攻擊目標。

趨勢 4：事件驅動成為新一波攻擊浪潮

2024 年攻擊者將聚焦更具針對性和事件驅動性的攻擊機遇，例如 2024 年巴黎奧運會。過去，不少攻擊者曾試圖破壞重大事件或利用地緣事件發動攻擊，但如今，網路犯罪分子可使用全新工具，尤其是生成式 AI，助其達成不法目的。即將舉辦的巴黎奧運會的與會者和觀眾可能遭遇來自“鐵粉”的騙局轟炸。隨著各大賽事越來越依賴各項技術進行比賽計時、賽事管理和轉播，相關賽事系統可能淪為攻擊者的靶標。

趨勢 5：縮小 TTP 攻擊範圍

攻擊者將不可避免地繼續擴大其用以入侵目標的策略、技術和戰術 (TTP) 集。然而，通過縮小攻擊範圍並找到破壞這些活動的方法，防禦者可搶佔先機。

Crowdstrike 在《2024 年全球網路安全威脅報告》中指出，CrowdStrike CAO 觀察到 APT 攻擊者在有針對性的入侵、電子犯罪和駭客行動領域以前所未有的隱蔽方式開展行動。2023 年，在地緣政治衝突 (即俄羅斯－烏克蘭和以色列－哈馬斯衝突) 引發了大量有針對性的入侵和駭客網路活動，特別是對伊朗關係和俄羅斯關係的攻擊者。2024 年，這些衝突和其他備受矚目的衝突仍將是駭客活動的重要驅動因素。除了與以色列－哈馬斯衝突相關的網路活動外，伊朗的攻擊者一直在攻擊電信組織，這一趨勢在 2024 年可能會繼續。俄羅斯的攻擊者也繼續以烏克蘭、北約成員國和夥伴國為目標。可以肯定，他們將在 2024 年繼續在這些地區開展情報收集行動和資訊運營工作。

國家支持的 APT 集團一直在探索新的方法、潛入連網路由器甚至利用全球事件議題來變換其發展攻擊的工具和手法，擴大攻擊範圍。他們會使用更複雜的工具和技術，如定制植入物和零日漏洞的快速利用。這些行為者通常擁有更多的資源和更高級的技術，使得防禦更加困難。俄羅斯、伊朗和北韓等國家的行為者繼續提高他們的網路攻擊能力。網路雇傭兵市場擴張可能破壞更廣泛的線上環境。

APT 攻擊：高級持續性威脅 (Advanced Persistent Threat，APT)，又叫高級長期威脅，是一種複雜的、持續的網路攻擊，包含三個要素：高級、長期、威脅。高級是指執行 APT 攻擊需要比傳統攻擊更高的定制程度和複雜程度，需要花費大量時間和資源來研究確定系統內部的漏洞；長期是為了達到特定目的，過程中“放長線”，持續監控目標，對目標保有長期的訪問權；威脅強調的是人為參與策劃的攻擊，攻擊目標是高價值的組織，攻擊一旦得手，往往會給攻擊目標造成巨大的經濟損

失或政治影響，乃至於毀滅性打擊。比較知名的案例有：2010 年，Stuxnet 病毒成功攻擊了伊朗核設施的離心機，導致大量設備報廢；2014 年，索尼影業遭受來自朝鮮的 APT 攻擊，大量資料被刪除和洩露；2020 年，SolarWinds 供應鏈被植入惡意程式碼，導致多個美國政府部門和大型企業遭受攻擊，美國政府認為是俄羅斯情報機構所為。

三．小結

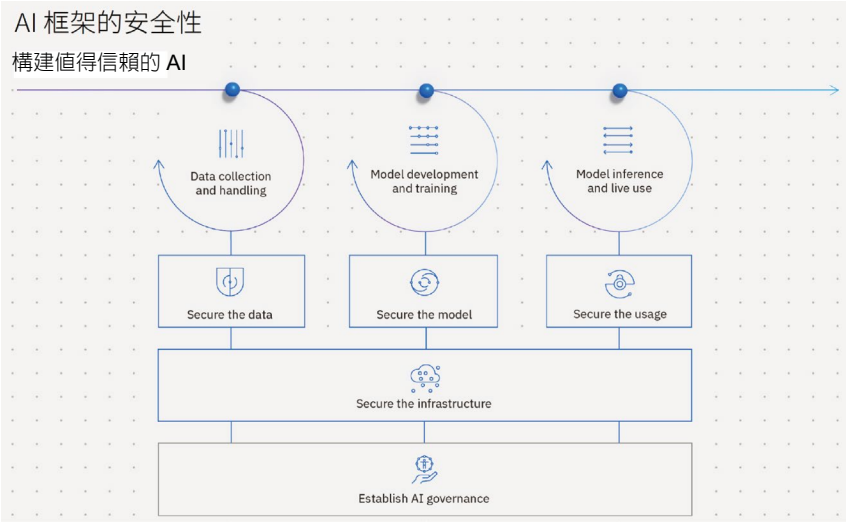
網路安全是一個不斷變化的領域，需要持續的創新和合作來應對日益複雜的威脅。必須投資于先進的技術，如 AI 和零信任架構，並加強跨部門合作，以確保數字環境的安全和韌性。同時，隨著網路犯罪的規模化和新興網路威脅的快速增長，防禦者將面臨前所未有的艱巨挑戰。根據 Cybersecurity Ventures 的預測，到 2024 年底，網路攻擊給全球經濟造成的損失預計將高達 10.5 萬億美元。這意味著，2024 年全球網路犯罪造成的損失有望首次突破 10 萬億美元大關，網路犯罪已經成為“GDP”增速驚人的全球另一大“經濟體”。面對複雜動態且不斷惡化的威脅態勢，如何進行威脅預測和優先順序排序成為從政府、企業到個人風險管理的頭號議題。我們需要更為先進的工具，並且不斷評估和更新其安全性原則，以應對這些不斷變化的威脅。

IBM 商業價值研究院最新報告顯示，全球僅 24% 的生成式 AI 計畫獲得了保護，隨著全球網路攻擊面不斷擴大，網路安全人員面臨巨大挑戰。世界經濟論壇預測，到 2030 年，全球網路安全人員的缺口可能達到 8500 萬人，這一短缺將進一步推高資料洩露成本。資源緊張的安全團隊將越來越多地轉向以 AI 為特色的安全技術，以加強網路防禦能力，最大限度地減少被成功攻擊的影響。

人工智慧驅動的預防工作正在取得成效。超過 6 成的企業和更多機構正在其安全運營中心 (SOC) 中部署安全人工智慧和自動化技術。當用戶在預防階段廣泛使用 AI 和自動化工具，其平均數據洩露成本與未使用這些技術的組織相比要少 220 萬美元，這表明 AI 和自動化技術有助於加速威脅緩解和補救，為防禦者爭取更多時間。

如 Gartner 所說：GenAI 引發短期疑慮，但同時也點燃了長期希望。

圖說：AI 框架的安全性



圖片來源：ibm.com

參考資料：

- Gartner：2024 年網路安全重要趨勢
- Crowdstrike：2024 年全球網路安全威脅報告
- 2023 Microsoft 數位防禦報告
- CyberEdge：2024 網路威脅防禦報告
- Fortinet：2023 年下半年全球威脅態勢研究報告
- IBM：生成式 AI 時代的網路安全 CTA