VOICE OF SECOPS 4TH EDITION 2023

deep instinct

生成式AI與資訊安全: 是光明的未來還是商業戰場？

RESEARCH REPORT

Table of contents

03 介紹

04 主要調查

05 **第 1 部分：利用生成AI的潛力，應對其威脅**

06 生產力和協作方面的優勢

08 生成式AI正在增加組織的弱點

10 **第 2 部分：不斷變化的威脅形勢將平衡轉向預防**

11 勒索軟體應對措施現已納入公司政策

12 效果不佳，贖金仍在增加

14 趨勢正在轉向預防

16 **第 3 部分：新舊威脅對網路防禦者心理健康的損害**

17 誤報使工作量增加，帶來壓力

20 生成式AI的不確定性加劇了不安全感

21 壓力持續導致專業人士離開這個行業

22 結論和建議

導論

如果在過去的一年中有一個迅速攀升至全球董事會議程頂部的話題，那就是生成式人工智慧：它如何運作，它在哪些領域能夠增加價值，以及採用這項新興技術所帶來的風險。他提供的競爭優勢潛力已經導致了69%的組織正式採用生成式人工智慧工具。然而，在資訊安全社群中，人們的興奮情緒卻被謹慎地抑制住了，因為 46% 的人認為生成式人工智能將使組織更容易受到攻擊。

威脅形勢正在以迅猛的速度演變，惡意行為者正在採用並武裝生成式人工智慧。事實上，這項技術已駭客重新應用，如新的生成式人工智慧工具**WormGPT**，已在地下論壇上作為駭客發動精密釣魚和商業電子郵件侵犯攻擊的一種方式進行宣傳。在過去十二個月中，那些見證了網路攻擊增加的安全操作專業人員中，有**85%**認為最近的攻擊很可能是由生成式人工智慧提供支援的。

隨著駭客利用這些新工具，我們已經清楚地了解，**對抗人工智慧的唯一方式是使用更先進的人工智慧形式**，或者更精確地說，是使用**深度學習**。受到大腦學習能力的啟發，**深度學習利用神經網路來自主預測威脅**，以阻止未知的惡意軟體和零日攻擊，從而防止它們進入您的環境。

由於攻擊面的擴大和新興技術（如生成式人工智慧）的日益採用，**資訊安全社群正在從傳統的被動式資料安全方法轉變為更加關注預防的方法**。根據調查，有95%的人轉為更傾向於在攻擊發生之前防止攻擊的方法，從去年的37%到今年提升為72%。

在應對新威脅時，除了維持堅固的安全姿態的挑戰進一步加劇，同時還需要應對長期存在的問題，包括勒索軟體（根據我們的調查，這是對組織安全性的最大威脅）以及應對大量誤報報帶來的疲勞。

這些複雜而具有挑戰性的需求對資訊安全專業人士的心理健康造成了影響。超過一半的受訪者表示，過去十二個月內他們的壓力水平有所增加，其中主要原因是「人員和資源的限制」。

《安全運營之聲》報告的第四版深入探討了這些標題，以研究安全運營專業人員如何應對當今的威脅，以及未來將採用哪些策略。

主要調查

生成式AI:
商業夥伴還是敵人？

- 69%的受訪者已在其組織內採用了生成式AI工具。
- 將近四分之三（70%）的安全專業人員表示，生成式AI對員工的生產力和協作產生了正面影響，其中63%的人表示該技術還提高了員工的士氣。
- 然而，高級安全專業人員將生成式人工智慧視為一個具有破壞性的威脅，近一半（46%）的受訪者認為生成式人工智慧會增加他們組織受到攻擊的風險。
- 75% 的安全專業人員目睹了過去 12 個月中攻擊的增加，其中85%的人將這種增加歸因於使用生成式 AI 的駭客。
- 對生成式AI三個最大的威脅擔憂包括不斷增加的隱私擔憂（39%）；無法檢測的釣魚攻擊（37%）；攻擊的數量和速度增加（33%）。

勒索軟體：隨著新漏洞的出現，
舊的威脅仍然是挑戰

- 近一半（46%）的受訪者認為勒索軟體是對其組織數據安全的最大威脅。
- 62% 的人承認勒索軟體是高階管理層最關心的問題，比2022年的44%還要高。
- 為應對持續的勒索軟體威脅，組織正在調整其資訊安全方法，近一半（47%）的受訪者現在已經制定了支付贖金的政策，而2022年為34%。
- 這導致42%的受訪者在過去一年中支付贖金來取回其機密數據，較去年的32%有所增加。

安全團隊壓力日益增大：
呼籲改變現狀

- 超過一半 (55%) 的安全專業人員表示，他們的壓力有所增加，首要原因(42%)是人員配置和資源限制。
- 51%的人可能會在未來 12 個月內因壓力而離職。
- **過時的資訊安全工具產生的誤報**對安全運營團隊的時間造成了巨大的壓力，每週損失超過兩個工作日的生產力。
- 三分之二(65%) 的受訪者表示，他們應該從端點檢測和響應(EDR) 和次世代防毒(NGAV) 解決方案中獲得更好的體驗，這一數字比2022 年增加了51%。
- 近四分之三的受訪者 (72%) 認為，**在攻擊發生之前預防攻擊是當務之急**，這表明行業需要做出改變。

“在這個生成式人工智慧的新時代，應對新興的人工智慧威脅的唯一方式是使用先進的人工智慧——一個能夠預防和預測未知威脅的方法。依賴像EDR這樣的舊工具，就好比用花園塑膠水管對抗五級火警。假設入侵一直是一種被接受的立場，但相信EDR能夠預先應對威脅是不正確的。轉向對資料安全進行預測性預防，是為了保持在漏洞前面、減少誤報和減輕安全團隊的壓力所必需的。”

01

第一部份:

利用生成AI的潛力，應對其威脅

生成式AI為企業帶來了許多好處，尤其是在提升生產力和加速創新方面。新的、易於使用的界面使其使用不再僅限於技術人員，這使得生成式人工智慧進一步普及，成為大眾意識和商業領域的一部分，隨著ChatGPT、Bard和Midjourney等工具的普及。據Gartner的說法，生成式人工智慧提供了"增加收入、降低成本、提升生產力和更好管理風險的新型機會和破壞性機會。在不久的將來，它將成為競爭優勢和區別因素。"[1]

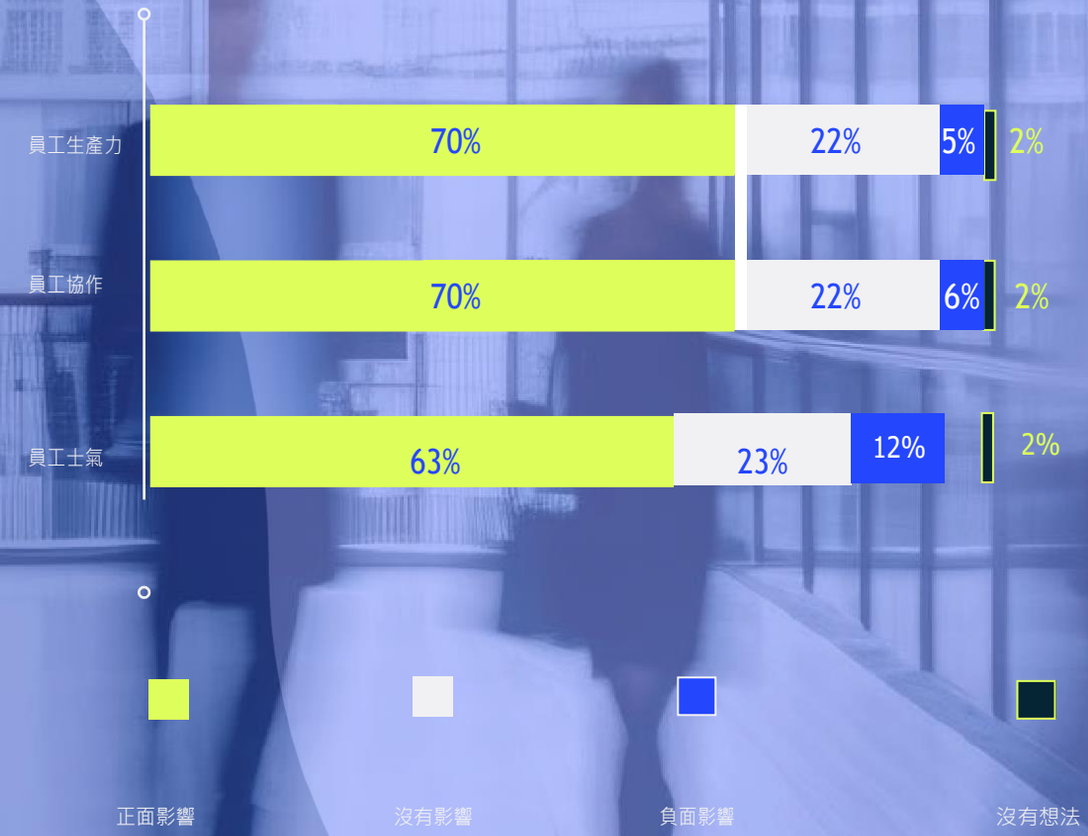
但我們是否正在進入一個虛擬的荒野，在這裡任何人都可以採用這項技術，而監管機構則在竭力追趕。當涉及資訊安全時，生成式AI是一個有價值的工具，還是一個存在的威脅呢？

1 https://www.gartner.com/en/topics/generative-ai

效益體現在生產力和協作方面

組織正在抓住現有的機會：69%的組織已正式採用生成式人工智慧工具用於工作場所。超過三分之二（64%）的人表示，他們期待藉助這項技術變得更具生產力和效率。

事實上，生成式人工智慧的影響已經開始顯現。70%的受訪者報告說明，生成式人工智慧對員工的生產力和協作都產生了積極影響。至於員工士氣，經驗則更加多樣化。雖然有63%的人表示生成式人工智慧對員工士氣有正面影響，但認為其對協作產生負面影響的人數是其士氣有害影響的人數的兩倍以上。



圖：受訪者被問及到目前為止，生成式人工智慧對以下方面在他們的工作場所是否產生了影響。

在技術成熟程度較高的行業，如科技行業本身，對生成式AI對其角色影響感到樂觀的受訪者比例較高，達到70%。而與之相比，傳統上在新技術採用方面落後的行業，如醫療保健行業，則表現出較少的樂觀情緒，只有51%的人表示感到興奮。

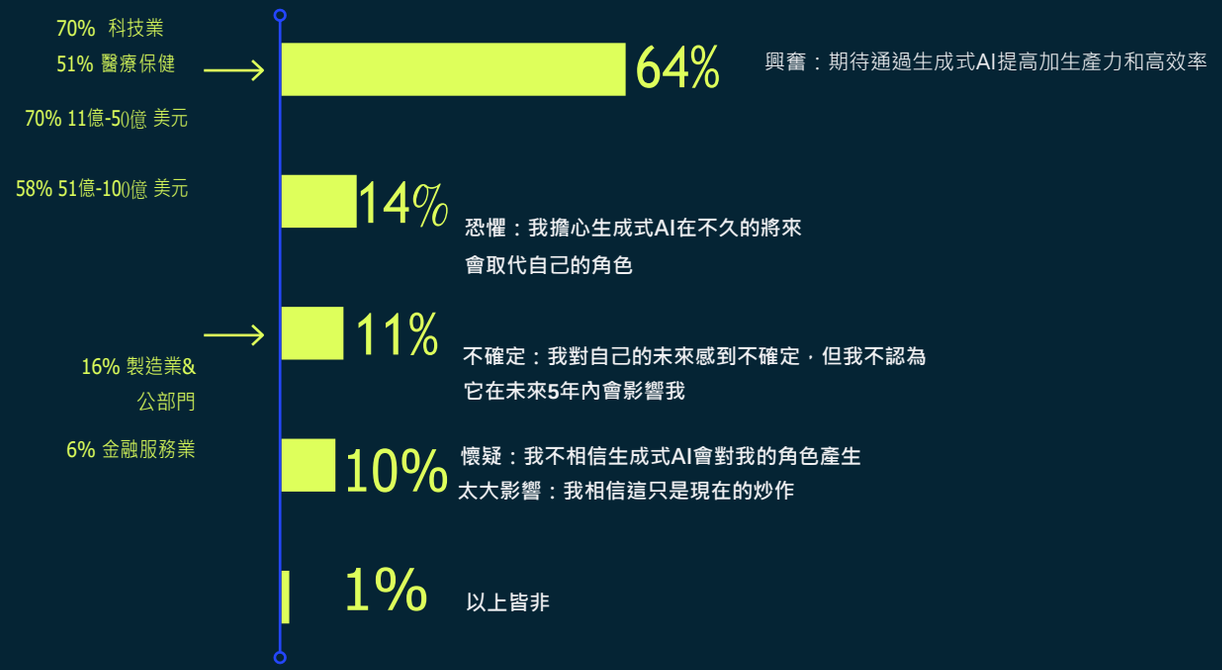


FIGURE 2: 受訪者被問及哪種情緒最能描述他們對於因生成式AI對其工作角色前景的看法。

生成式AI正在增加組織的弱點

除了樂觀情緒外，我們也看到人們對生成式人工智慧對組織安全態勢影響的真實擔憂。根據麥肯錫的說法，生成式AI"通過開放更多攻擊區域和新形式的攻擊，增加了安全漏洞的風險。"[2]

根據我們的調查，有46%的資訊安全專業人員認為生成式AI工具將使他們的組織更容易受到網路攻擊。在技術成熟且潛在危害更加清楚的行業中，這個比例上升到一半以上：科技業達到52%，金融服務業達到51%。

最明顯的威脅是隱私問題的增加。 圍繞生成式AI的興奮可能會導致公司在不了解其後果的情況下嘗試該技術。 最近備受矚目的公司機密資料被上傳到 ChatGPT 的案例凸顯了這種危險。

受訪者認為生成式AI將使他們的組織更容易受到攻擊的第二大原因是駭客能夠進行更多無法偵測的釣魚攻擊。事實上，對攻擊可能變得更加普遍的感覺體現在第三個最常見的擔憂原因中：攻擊的數量和速度增加。由於駭客現在幾乎根本不需要技術就能利用生成式AI的潛力，危險性因此增加。

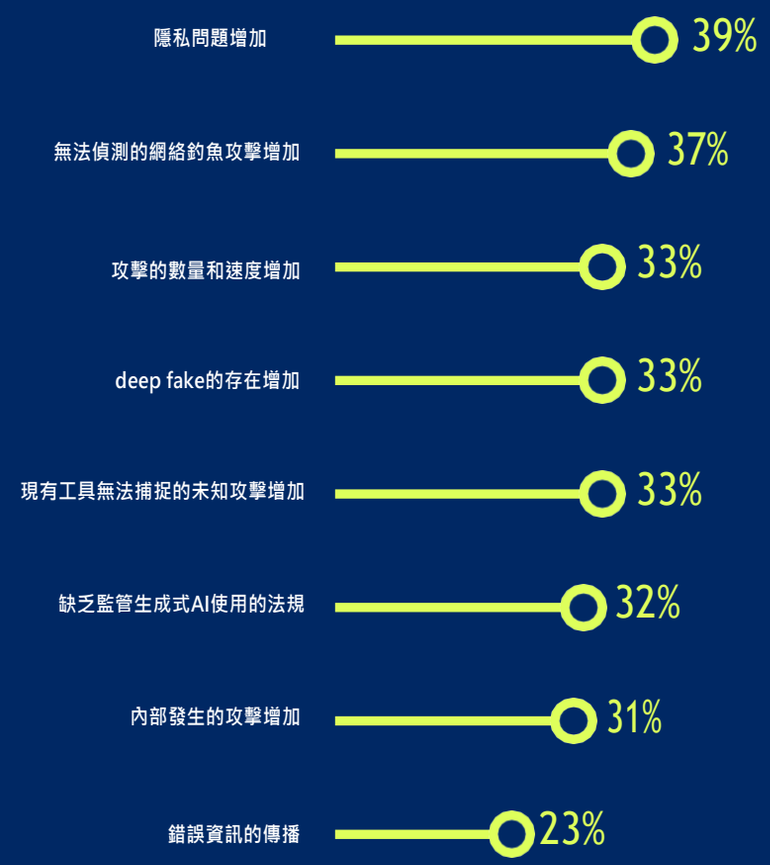


FIGURE 3: 請受訪者選擇最多三個生成式AI最有可能使他們的組織更容易受到攻擊的原因。

2 https://www.mckinsey.com/capabilities/quantumblack/our-insights/four-essential-questions-for- boards-to-ask-about-generative-ai

那些在安全運營第一線工作的人正在親眼目睹生成式AI開始廣泛使用所帶來的最終結果。在過去 12 個月中經歷過攻擊增加的網路安全專業人士中，86% 的人認為這可能是由於駭客使用生成式AI造成的。

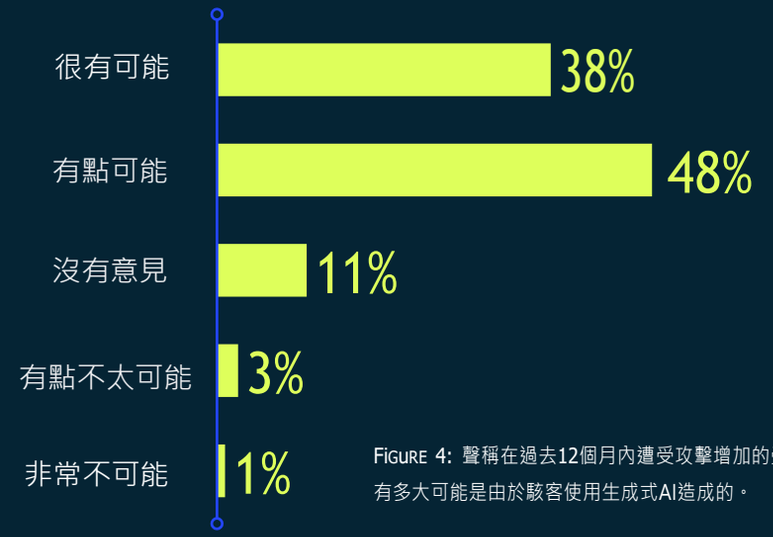


FIGURE 4: 聲稱在過去12個月內遭受攻擊增加的受訪者被問及最近的攻擊有多大可能是由於駭客使用生成式AI造成的。

02

第2部分：

不斷變化的威脅形勢將平衡轉向預防

勒索軟體應對措施現已納入公司政策

除了對由生成式AI驅動的未知攻擊的擔憂外，勒索軟體也持續困擾著組織，有62%的受訪者同意勒索軟體是其高階管理層的頭號關切，而去年這一比例僅為44%。

儘管勒索軟體並不是一個新問題，但為打擊和控制勒索軟體而製定的措施仍然不足。 各組織正在調整其內部政策以應對威脅。人們對攻擊的可能性以及付出代價的必要性有一種不可避免的感覺；

今年，有 超過38% 的受訪者表示，他們支付贖金的理由是因為公司有這樣做的政策。相反，他們對保險的依賴較少，選擇支付贖金的人因擁有勒索軟體保險而下降，從2022年的62%降至2023年的43%。

由於勒索軟體攻擊的激增，2022年第一季度，網路保險價格上漲了110%，這有助於解釋這種行為變化。

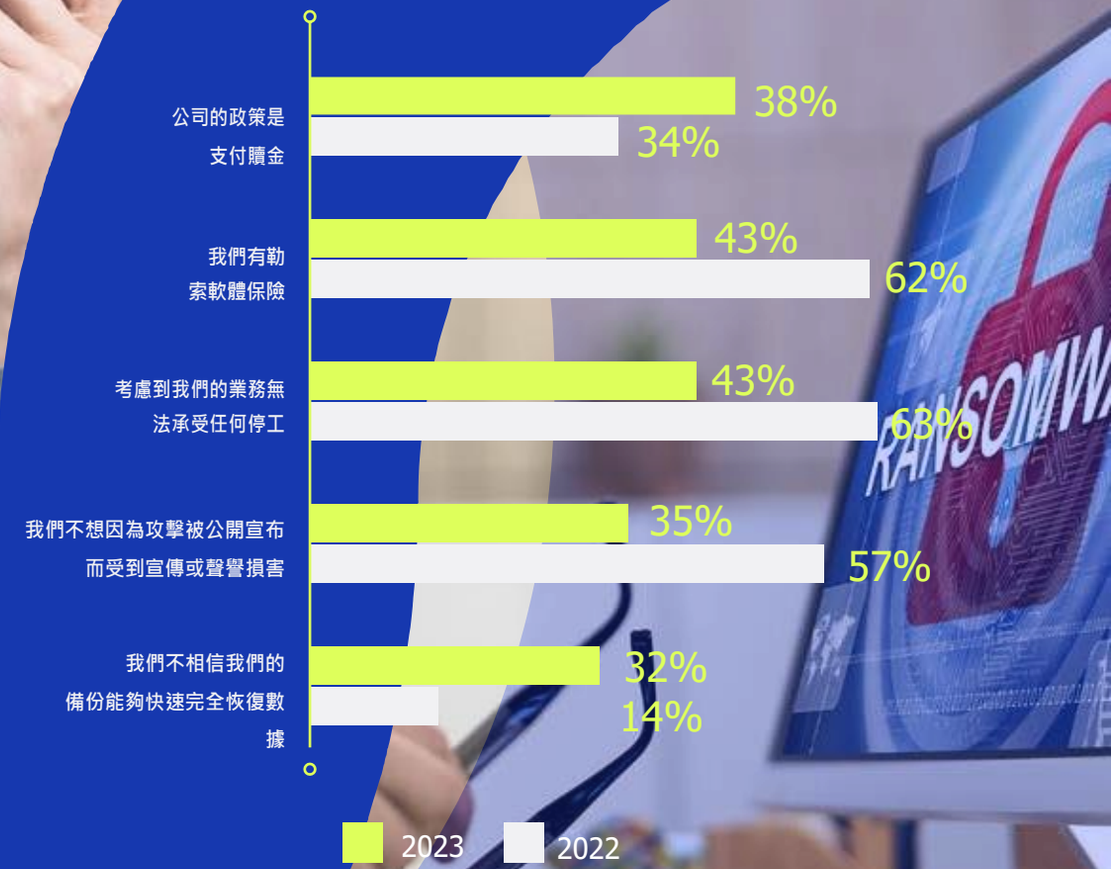
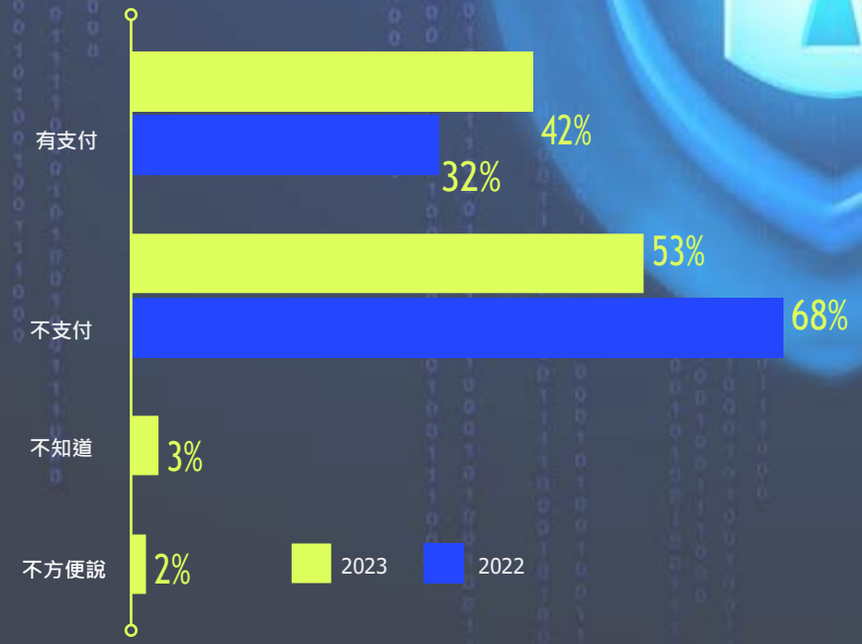


FIGURE 5: 受訪者被問及上述哪些（如果有）可能是他們支付贖金的理由。

3 https://www.bloomberg.com/news/articles/2023-02-24/cyber-insurance-back-from-the-brink-after-ransomware-onslaught

效果不佳，贖金仍在增加

42%的受訪者支付贖金來取回他們的數據，較去年的調查（32%）增加了10個百分點。在支付贖金之後，有45%的人仍然被駭客曝露了記錄或是敏感數據（相比2022年的42%更高）。



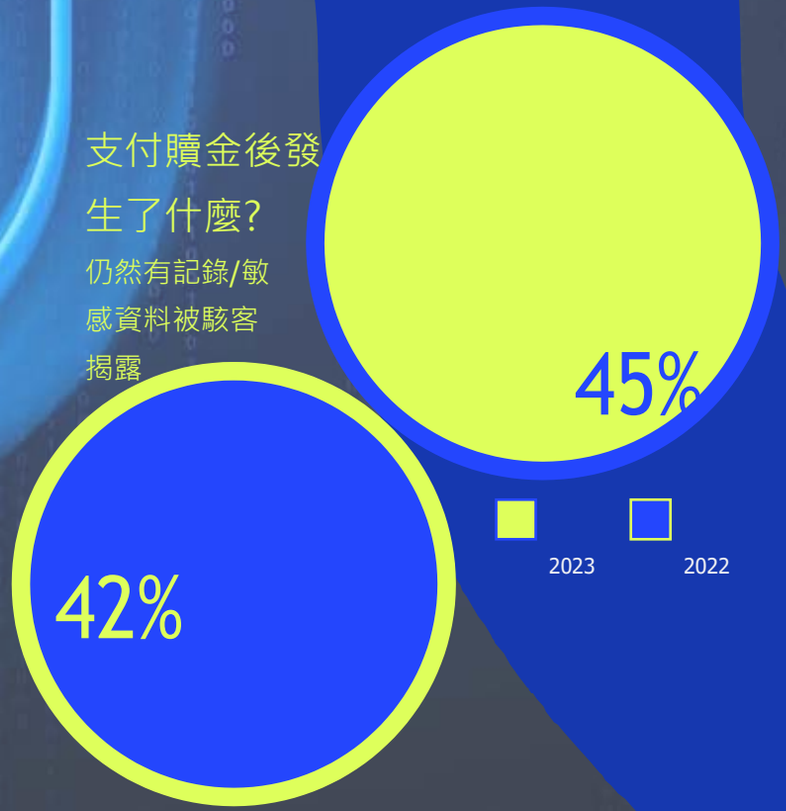


FIGURE 6:受訪者被問及是否曾經支付過贖金，如果支付的話，之後發生了什麼。

FIGURE 7: 受訪者被問到：將來，您是否會支付贖金來歸還資料或取得解密密鑰？

儘管數據被洩露，48%的人在將來仍然會支付贖金以取回數據或解密密鑰，而在2022年的調查中，只有24%的受訪者會這麼做。高階管理層更有可能表示他們會支付贖金（53%），而他們的下屬則較少這麼表示（39%）。

考慮到儘管支付贖金，數據仍然會被洩露，以及考慮到勒索軟體攻擊造成的聲譽和運營損害，將支付作為威脅緩解措施的依賴是不可持續的。此外，根據Gartner的預測，"到2025年，30%的國家將通過立法來規範勒索軟體的付款、罰款和談判，這一比例從在2021年還不到1%。"[4]

安全運營團隊承受著尋找更好解決方案的壓力，不僅限於勒索軟體，還包括更廣泛的威脅。73%的人表示，他們的董事會一直在詢問他們如何提高對威脅的預防能力。

4 https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio

趨勢正在轉向預防

四分之三的受訪者表示，在過去的十二個月裡，他們所在的組織遭受了網路攻擊的有所增加。在這些人當中，有41%表示攻擊量的增加是由於「未知」攻擊，例如零日漏洞或現有惡意軟體的新變種，受影響最大的行業是公共部門（85%）和金融服務業（83%）。

組織正在投資於解決方案，以減輕未知威脅的增加。最受歡迎的措施是端點檢測和回應（EDR）。在受訪者中，受管理的檢測和回應（MDR）服務以及能夠提供更大防護的解決方案同列第二。

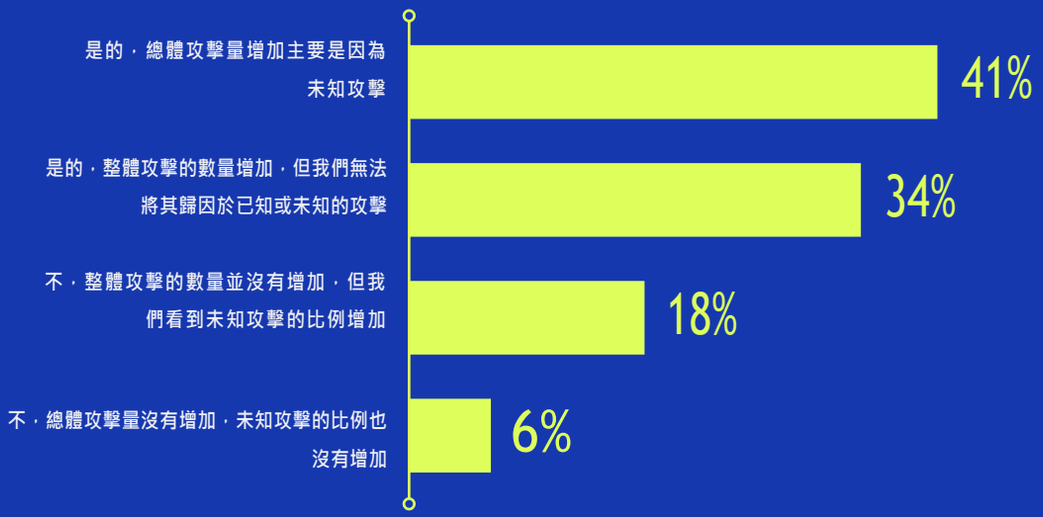
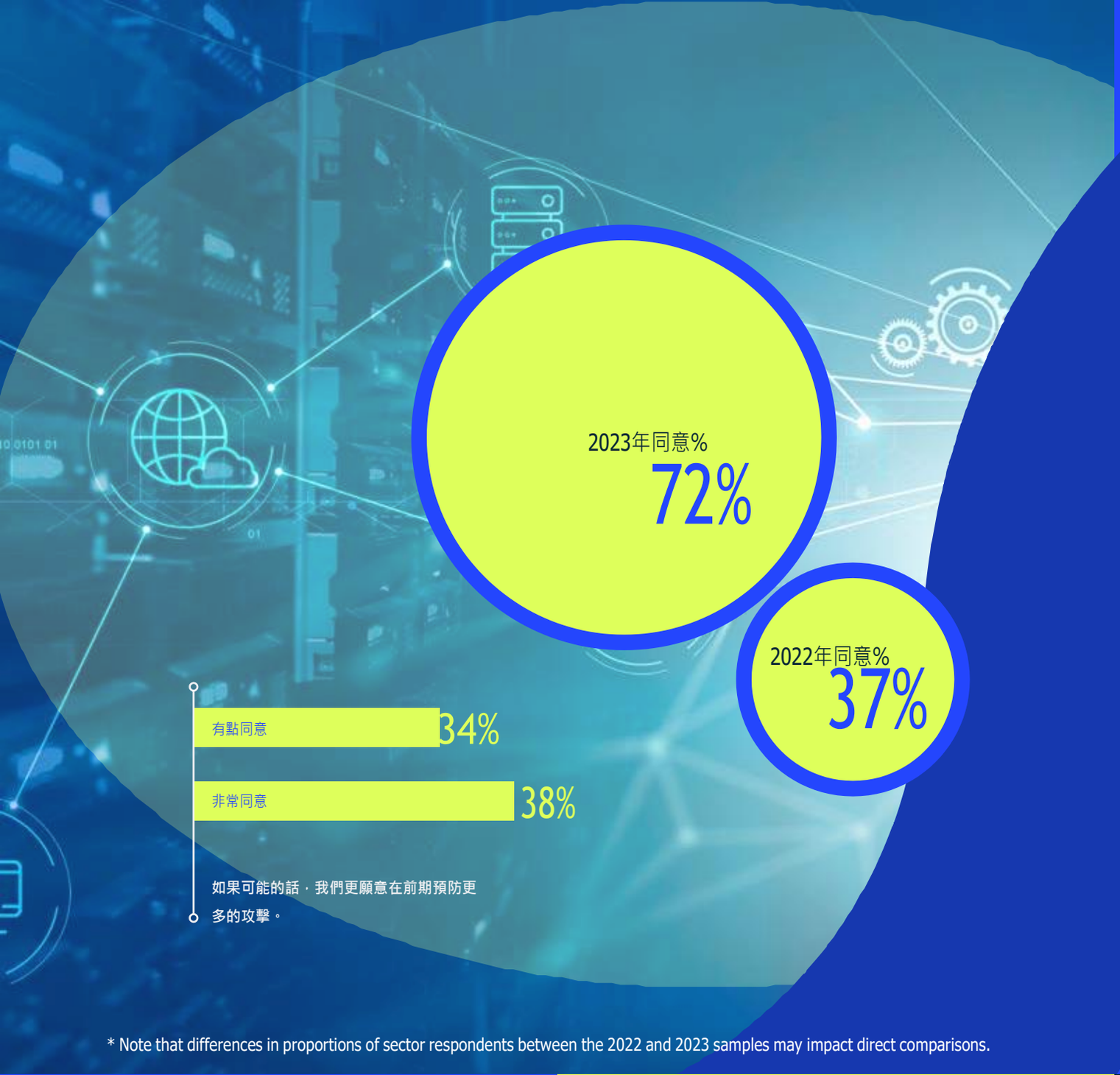


FIGURE 8: 受訪者被問及在過去 12 個月中，他們組織中的網路攻擊總量是否有所增加



* Note that differences in proportions of sector respondents between the 2022 and 2023 samples may impact direct comparisons.

根據IDC的說法，"該市場已進入了端點檢測和回應（EDR）的後蜜月期。在這個期間，組織正在評估他們在減少網路風險和應對網路事件方面取得的成果，相對於他們在將EDR和/或管理型EDR服務添加到他們的網路安全工具組中所增加的額外支出。"[5]

在已知和新興威脅方面，EDR和MDR解決方案的限制正在推動人們對網絡安全週期早期的預防平台的需求。**我們從去年的調查（37%）到今年的調查（72%）中看到了對於在攻擊發生之前進行預防的偏好增加了95%。**

5 https://www.idc.com/getdoc.jsp?containerId=US49349323

03

第 3 部分:

新舊威脅對網路防禦者心理健康的損害

對於安全運營領域的人來說，壓力是日常，這已經不是新聞。在我們的行業中留住人才是一項艱鉅的任務，由於多種與工作相關的壓力因素，有四分之一的資訊安全領導者計劃在2025年前轉到完全不同的角色。[6]

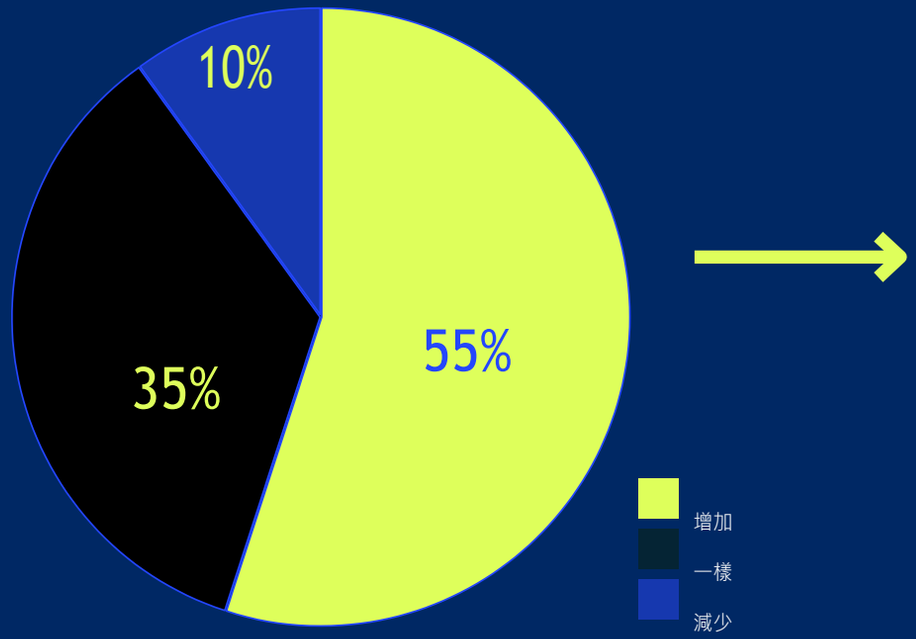
高人才流動率增加了保持強大的安全態勢的困難。團隊不僅面臨應對現有威脅的壓力，還需要預防和保護免受新威脅的影響；同時，**寶貴的時間和資源被用來處理非惡意警告或誤報產生的雜訊。**

6 Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025

誤報使工作量增加，帶來壓力

過去的十二個月對於資訊安全專業人員來說是艱苦的，超過一半（55%）的調查受訪者表示他們的壓力水平增加了。在當今的環境中，為了確保組織的安全所需的工作量對團隊造成了巨大的壓力，壓力增加的首要原因是人員和資源的限制（42%）。

過去 12 個月中壓力有何變化？



壓力變大的原因？

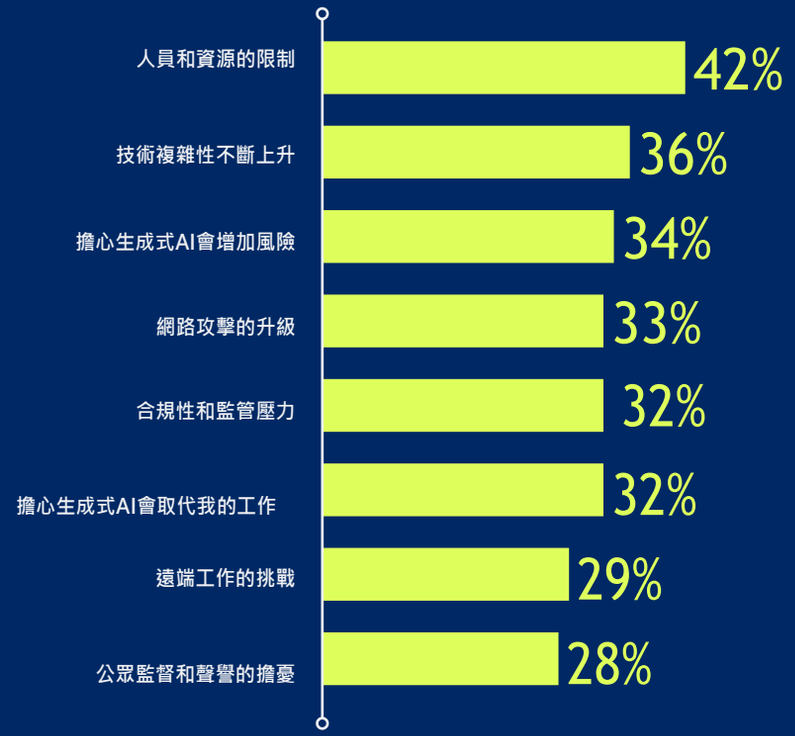


FIGURE 9: Respondents were asked how their stress levels at work have changed over the past twelve months and why.

雖然新的解決方案和技術應該可以緩解壓力，但實際上工具的激增正在加劇壓力。 我們的調查顯示，技術複雜性的增加在造成壓力的因素列表中排名第二。

團隊正在嘗試平衡管理事件（包括由於不足的預防措施或高誤報率引起的事件）與採用額外技術帶來的工作負荷增加。在2022年，受訪者表示減少事件的最大影響將會對業務風險產生影響，而今年的受訪者則指出最大影響變成他們花在了理解威脅來源上的時間（72%，相比之下，2022年這個領域的比例為58%）。

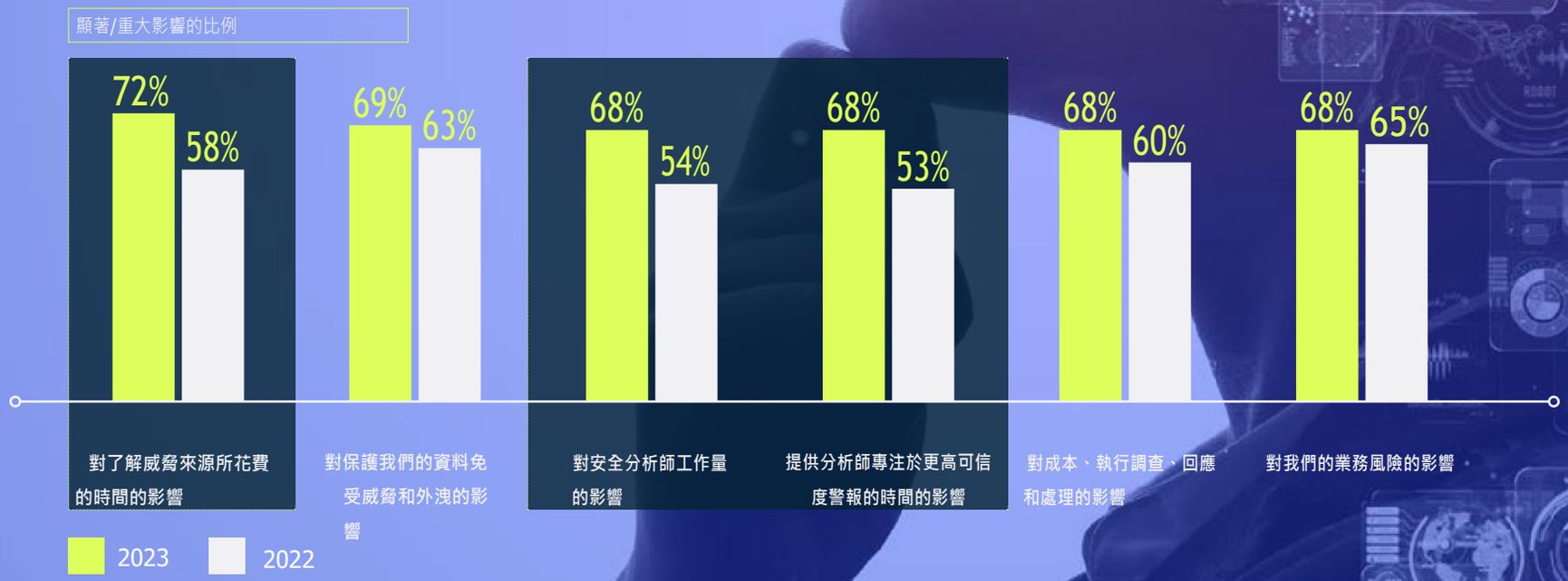


FIGURE 10: 受訪者被問及，如果您或您的團隊今天可以通過改進預防措施和/或減少誤報來減少50%或更多的事件，請指出對您的安全運營中心會有哪些影響（如果有的話）。

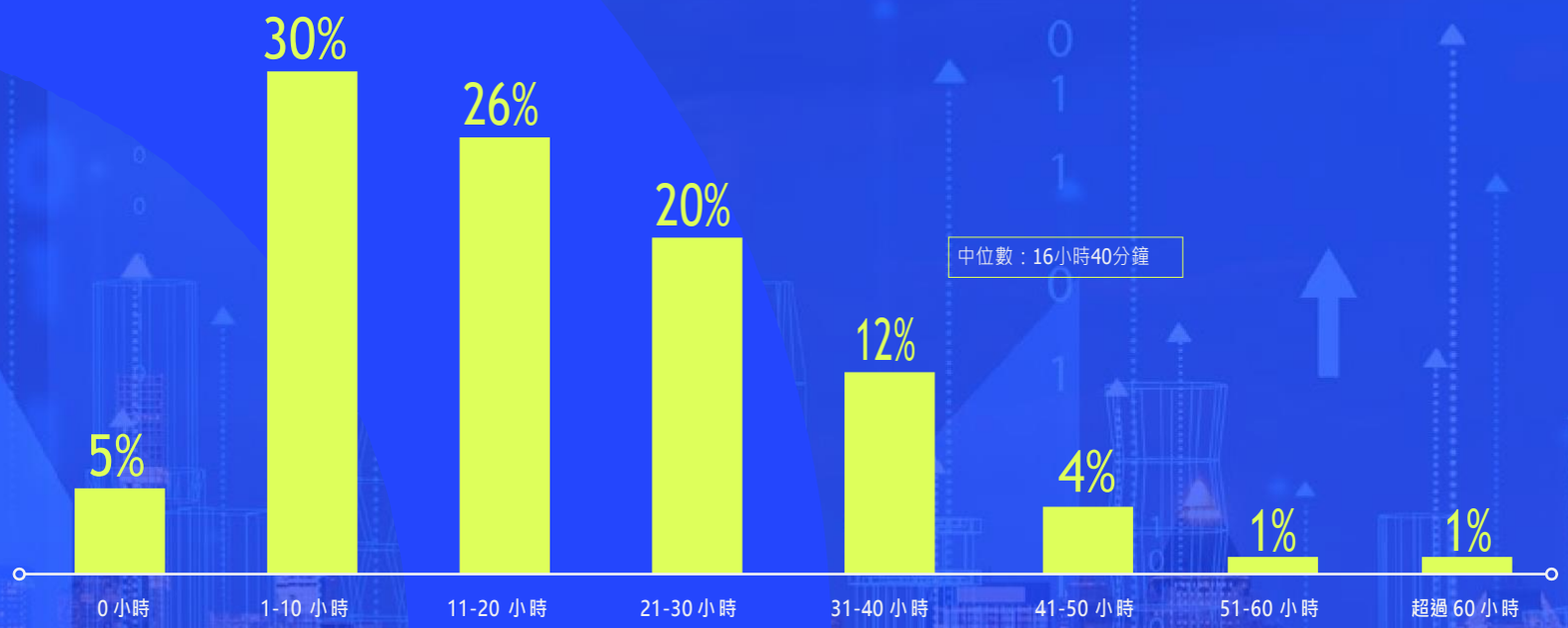
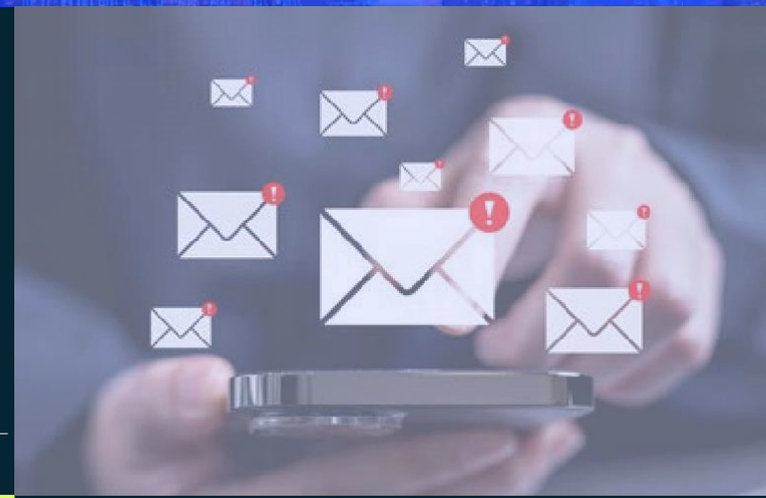


FIGURE 11: 受訪者被問及他們的團隊每周有多少小時是被誤報引起的警報佔用。

鑑於這些擔憂，我們的調查受訪者中，近三分之一對其現有的人員水準沒有自信。考慮到這些員工所面臨的壓力，這個問題變得更加嚴重。**處理誤報對安全運營團隊的時間造成了巨大的耗損，通常每週佔據了超過兩個工作日的時間**。

顯然，組織正在意識到對他們的團隊施加的不可持續承受的壓力，並正在尋找減少誤報的方法，從而為其他任務釋放更多時間。根據IDC的說法，「客戶更換端點防護供應商的首要原因是需要提高安全效能（即，**以更低的誤報率封鎖更多的攻擊**）。僅有少數調查受訪者表示是出於價格較低的原因而更換供應商。」[7]



生成式AI的不確定性加劇了不安全感

認為需要通過AI實現更高程度的自動化來改善安全運營的人數已從2022年的51% 躍升至今年的71%。 與此同時，同意"我們寧願依靠人類而不是AI來追蹤威脅"這一說法的人從去年的18%上升到今年的52%。

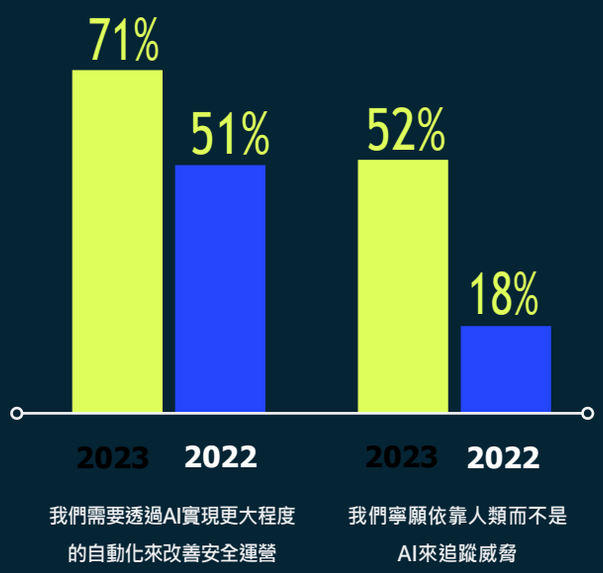


FIGURE 12: 稍微或強烈同意所給出的有關AI的陳述的受訪者

這種保留可能歸因於對於隨著AI的使用增加，工作可能會受到威脅的擔憂。有14%的受訪者擔心生成式AI會在不久的將來使他們的角色變得無關緊要，還有11%的人對於未來五年感到不確定。

在金融服務等領域，我們的受訪者中有80%已經正式採用了生成式AI，這種不確定性最低（6%）。希望抓住AI在威脅防禦和偵測方面提供的機會的企業，需要管理員工對於工作安全性的擔憂，才能看到進展。

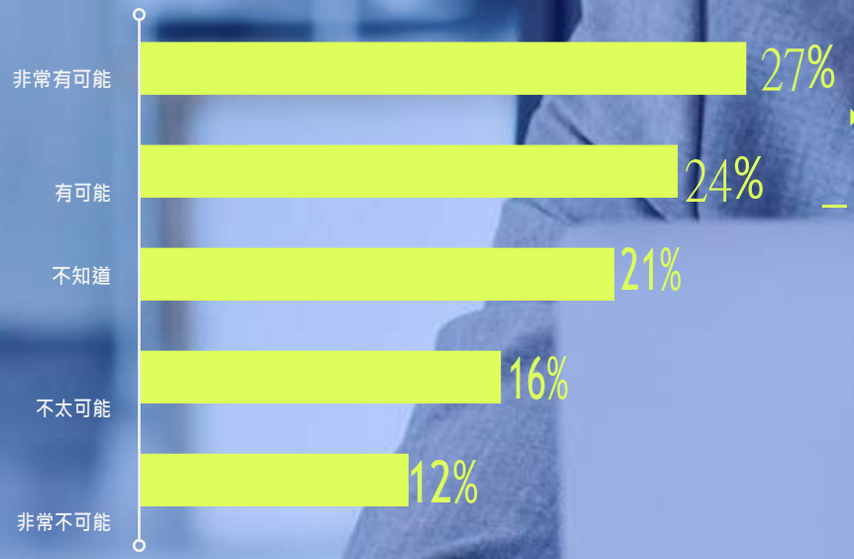
我們發現，對生成AI的擔憂與網路安全領域的壓力之間存在明顯的相關性。在過去 12 個月中感到工作壓力更大的受訪者中，有 58%也認為生成式AI可能會引發更多網路攻擊。

壓力持續導致專業人士離開這個行業

在未來的幾個月中，減少誤報的數量、解決團隊在採用複雜技術時所面臨的困難，以及解決關於生成式AI對工作和數據安全影響的不確定性，對於組織至關重要。否則，51%的受訪者可能會因為壓力而在未來十二個月內離職。在高度監管的金融服務領域，這一數字上升至66%。

考慮跳槽的員工在很多情況下之所以這麼做，是因為他們感覺壓力變得更加嚴重。

在那些表示可能離職的人中，有63%在過去十二個月中工作中的壓力水平增加，相比之下，只有33%的人壓力水平沒有變化。



51% likely

66% 金融服務業
42%製造業

62% 51億 - 100億美元
49% 11億 - 50億美元

63% 工作壓力變大
33% 工作壓力不變

FIGURE 13: 受訪者被問及他們在未來 12 個月內因壓力而離職的可能性有多大

結論和建議

生成式AI在安全運營社群內引發了不確定性和興奮。在我們評估其限制、潛力、威脅和機會時，保護組織資料安全的基本工作仍在繼續進行。

網路安全專業人員壓力增加和工作量增大的情況意味著單純做更多已不再是可行的選擇。65%的受訪者表示，網路安全專業人員應該得到更好的次世代防毒和EDR解決方案支援，較去年增加了43%。

隨著壓力的增加，網路安全防禦者將被迫證明其平台和技術投資的價值。雖然網路硬體和終端設備被認為是攻擊者最容易進入的入口點，但超過三分之二 (69%) 的受訪者在惡意文件滲透其網路時擔心檔案被上傳。在今天的威脅環境中，調整投資和資源以更好地平衡預防與偵測將是確保強大的數據安全態勢所必不可少的。

利用人工智能來對抗人工智能確實是明智之舉，但許多機器學習或生成式AI驅動的解決方案完全是被動式的。缺少的是一個位於端點保護前方的資料安全層。像Deep Instinct這樣的深度學習平台，完全是為了防止未知威脅而進行專門的訓練和架構。

通過將重點轉移到更早地應對攻擊，利用從頭開始為網路安全建立的深度學習平台，安全運營團隊可以更好地利用當今的技術來應對當前的威脅，減少誤報，減少技術複雜性，為團隊釋放更多增值工作的時間，從而減輕壓力。

方法

Sapio Research對美國1000名以上員工的公司進行了調查，共有652名高級網路安全專家參與。調查於2023年6月在線進行，使用電子郵件邀請和網上問卷進行訪問。

受訪者任職於金融服務、科技、製造、零售、醫療保健、公共部門或關鍵基礎設施（例如電信、能源、公用事業和交通運輸）等行業的組織。

高階管主被定義為擔任首席、全球、部門主管或總監角色的人員，而下屬則被定義為擔任經理、管理員、分析師、團隊領導或官員角色的人員。

關於 Deep Instinct

Deep Instinct採用預防為主的方法來阻止勒索軟體和其他惡意軟體，使用全球首個也是唯一專為深度學習而建立的資安架構。我們可以在不到20毫秒內預測並阻止已知、未知和零日威脅，速度比最快的勒索軟體加密快了750倍。Deep Instinct具有超過99%的零日準確率，並承諾低於0.1%的誤報率。Deep Instinct預測式預防平台是每個安全堆疊中必不可少的部分，可在混合環境中提供完整的多層次威脅保護。

For more, visit www.deepinstinct.com.

關於 Sapio Research

Sapio Research 是一家提供全方位服務的 B2B 和技術市場研究機構，通過高品質、高效和誠實的研究解決方案幫助企業發展。 我們是一支充滿熱情、目標驅動的專家市場研究團隊，我們熱衷於在定量和定性研究的所有領域為品牌以及公關和傳播機構提供支持。

我們為客戶提供有價值的證據，以幫助他們了解自己的受眾，創建非凡的內容和標題，並做出與他們市場相關的重要業務決策。

我們的總部位於英國，覆蓋 130 個國家/地區的超過 1.49 億人，合作客戶包括頂級科技公司、全球諮詢公司、公關與傳播機構以及家喻戶曉的品牌。

通過 Sapio Research 找到您的聲音、吸引您的市場並推動您的發展。

Andrew White
CEO and Founder
Sapio Research

Jessica Bunce
COO and Founder
Sapio Research

Sapio Research
2nd, Pentagon House
52 - 54 Southwark St
London SE1 1UN
United Kingdom

+44 20 7236 1604