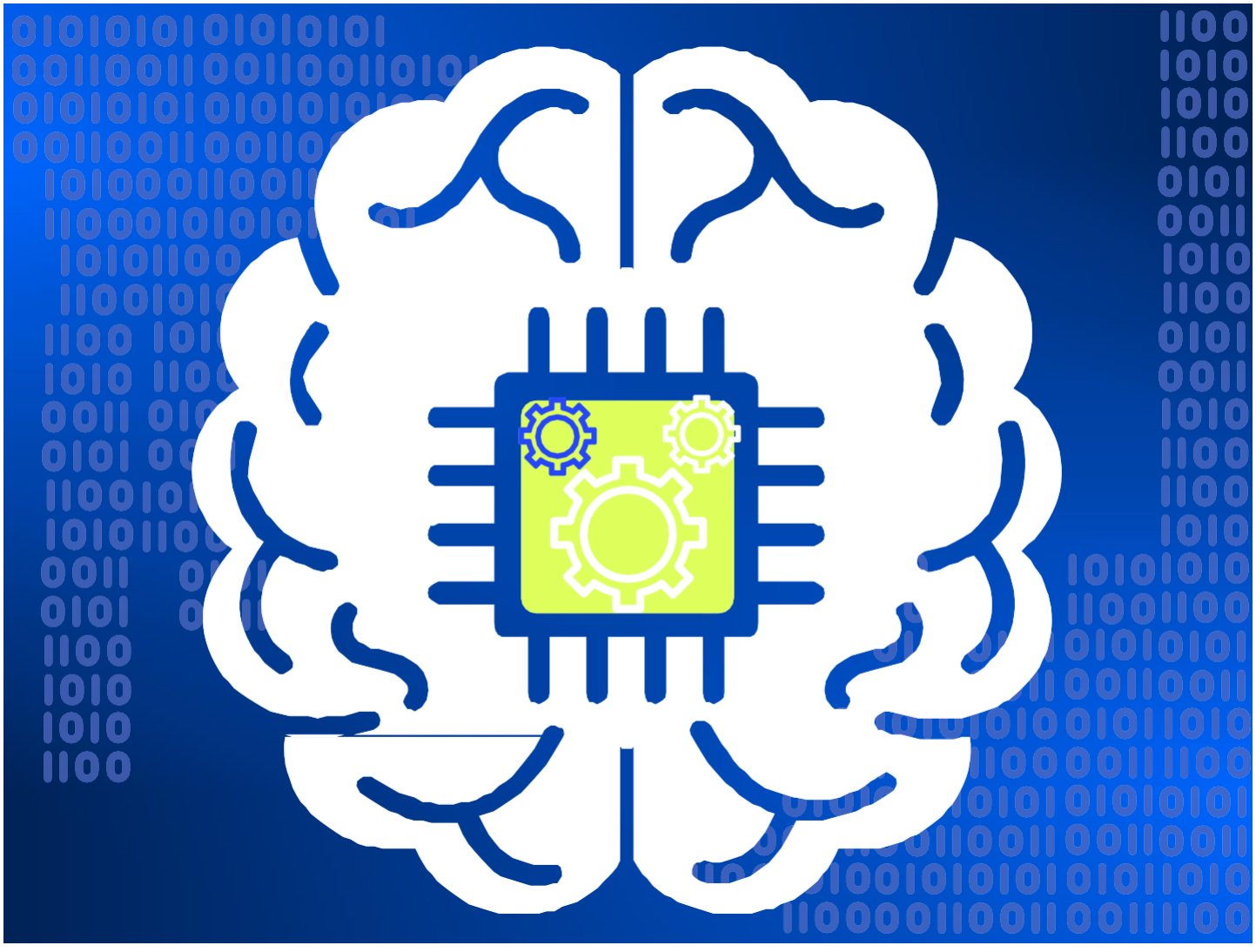
MIT Technology Review
Insights

Produced in association with

deep instinct

企業需要開始以不同的角度思考資訊安全，才能領先於惡意行為者。

深度學習提供主動的網路防禦



網路安全專業人員不斷尋找新的創新方法，以領先駭客一步。 然而，根據身分盜竊資源中心的數據，光是2022 年第一季度，美國就發生了 404 起公開報告的資料外洩事件，比2021年第一季度增加了 14%。特別引人關注的是勒索軟體攻擊的急劇上升，根據2022年Verizon資料外洩調查報告（DBIR）的數據，僅一年內增加了13%，增幅超過了過去五年的總和。

越來越多的組織開始探索深度學習及其模仿人腦的能力如何智取並超越世界上最快、最危險的網路威脅，這件事也已經不足為奇了。

深度學習是人工智慧 (AI) 技術最先進的形式，也是機器學習的一種，它利用神經網路本能地、自主地預測和預防未知惡意軟體和零時差攻擊，避免它們在 IT 環境上造成嚴重破壞。

大多數資訊安全技術，如端點偵測與回應（EDR）解決方案，通常**僅能在威脅已經進入環境後進行識別**、追蹤、記錄和封鎖它。基於機器學習的資訊安全解決方案也是所有安全策略的重要一環，它們使用預先標記的資料，將其分類為良性或惡意，以偵測危險的行為模式。

但是，這兩種網路安全解決方案都無法在不經過人為調整的情況下主動防禦複雜的攻擊。幸運的是，深度學習可以模仿人類腦神經元的功能和連接性，使神經網路能夠獨立地從原始和未經整理的資料中學習，並自動識別未知威脅。

重點

1. 在2022年第一季度，美國的資料外洩事件較2021年第一季度增加了14%。
2. 深度學習提供了一種自主、高度準確的方式，可以識別複雜的攻擊模式並在它們發生之前預測對手的威脅，無需高度熟練的資訊安全專家。
3. 如果公司要在對抗惡意行為者方面取得進展，他們需要**從檢測轉向預防**的思維方式。隨著網路攻擊變得更加技術複雜，使用像對抗性人工智慧這樣的技術，更高級的工具如深度學習來防止資料外洩是必要的。

資訊安全公司Deep Instinct的創始人兼首席聯盟官Guy Caspi表示「深度學習是唯一一種能夠在原始數據上以無與倫比的速度和精確度識別資訊安全威脅的演算法」。

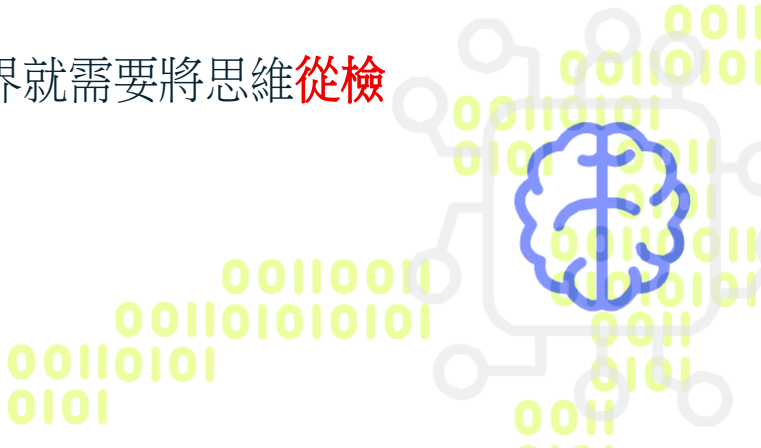
一個強大的解決方案，可以以前所未有的速度精確識別高度複雜的攻擊模式。

是時候採取不同的防禦策略了

儘管深度學習技術自1940年代以來就存在，但高昂的圖形處理單元（GPU）成本和其複雜性使許多組織難以應用該技術。不過，隨著圖形晶片處理能力不斷增強和成本降低，情況正在發生改變。

「如果我們要超越我們的對手，世界就需要將思維**從檢測轉變為預防**。」

- Guy Caspi，Deep Instinct 創辦人兼首席聯盟官



此刻正是最好的時機。勒索軟體即服務提供的增加，如勒索軟體工具包和目標清單，使惡意行為者甚至是那些經驗有限的人，更容易發動勒索軟體攻擊，在感染的第一刻就造成嚴重損害。其他複雜的攻擊者使用有針對性的攻擊，將勒索軟體放置在網路內，以便在命令下觸發。

另一個令人擔憂的問題是隨著雲端計算存儲和資源轉移到邊緣運算，IT環境的邊界日益模糊。International 安全與信任研究副總裁Michael Suby 表示，當今的組織必須保護終端用戶設備（如桌上型電腦、筆記型電腦和移動設備）的端點或入口，以防止它們被惡意駭客利用——這是一項具有挑戰性的任務。他說：“攻擊不斷演進，端點本身和使用其設備的終端用戶也在變化。這些動態情況為惡意行為者的入侵以及在任何端點上建立存在並使用該端點來發動攻擊序列創造了三重優勢。”

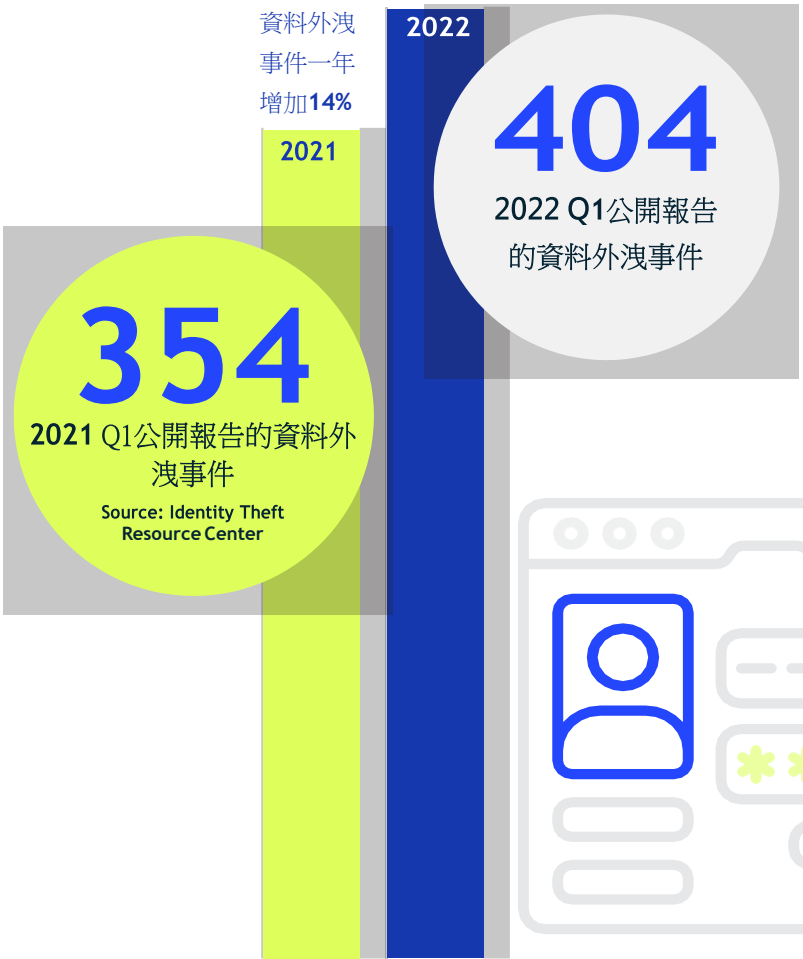
高調威脅（例如勒索軟體）的增加速度高達二位數（15.8%）的增長。結果顯示一條危險的路徑，最有可能導致那些成為網路攻擊受害者且沒有獲取任何防禦能力的組織持續損失，事實上，IBM和Ponemon研究所於2021年公佈的一份資料外洩報告顯示，資料外洩平均造成 424 萬美元的損失。

除了財產上的損失之外，網路攻擊還可能對公司的品牌、股價和日常營運造成不可挽回的損害。 根據德勤最近的一項調查，32% 的受訪者將營運中斷視為網路事件或入侵事件造成的最大影響。
該公司提到的其他影響包括智慧財產權竊盜（22%）、股價下跌（19%）、聲譽損失（17%）和客戶信任的喪失（17%）。

考慮到這些重大風險，組織根本無法接受保護數位資產的現狀。 卡斯皮說：“如果我們想要領先對手，世界就需要改變思維方式，**從檢測轉向預防**。” “組織需要改變他們執行安全和打擊駭客的方式。”

美國資料外洩事件不斷增加

從過去兩年的第一季來看，資料外洩事件的發生將逐年上升。



深度學習可能會有所不同

到目前為止，許多網路安全專家都將機器學習視為保護數位資產的最具創新性的方法。 但深度學習更適合改變我們預防網路安全攻擊的方式。 任何機器學習工具都可以被理解，理論上可以進行逆向工程，以引入偏見或漏洞，從而削弱其防禦能力。

惡意行為者也可以使用他們自己的機器學習算法，以假數據集污染防禦解決方案。

幸運的是，深度學習解決了機器學習的限制，它避免了高度熟練和有經驗的資料科學家手動提供數據集的需求。相反，專為資訊安全而開發的深度學習模型可以吸收和處理大量的原始數據，以全面訓練系統。這些神經網路在經過訓練後變得自主，不需要持續的人工干預。這種基於原始數據的學習方法和更大的數據集的結合意味著，深度學習最終能夠以遠快於機器學習的速度精確識別更複雜的行為模式。

"Honeywell Building Technologies (HBT)的副總裁和總經理Mirel Sehic表示： “深度學習勝過任何阻擋清單、啟發式或標準機器學習方法。

Source: Cost of a Data Breach Report 2021 by IBM and the Ponemon Institute

深度學習在企業應用中

由於深度學習技術能夠由人類執行的任務轉成有效自動化，企業應用程式是豐富多彩且越來越普遍。**STX Next**進行的一項針對**500**名首席技術官的全球調查發現，**20.7%**的首席技術官已將深度學習技術納入其技術堆棧。

常見的企業應用案例

自然語言處理. 這項技術推動了機器人、虛擬助手、翻譯工具和文本應用，如自動校正和情感分析。大多數人每天都會與這項技術互動，執行諸如過濾電子郵件、搜索網站和瀏覽網際網路等任務。

異常檢測.深度學習在各行各業中的這個應用非常重要且廣泛。它用於檢測詐騙交易，識別製造系統中的故障，檢測網路基礎設施的入侵，協助解釋醫學影像等多種應用案例。

電腦視覺. 影像和模式識別技術在各行業提供廣泛的應用。 例如，在製造業中，它們可以幫助檢測裝配線上的產品缺陷。 他們可以查看靜態或即時影像和影片以進行分類或標記，或識別修改後的影像或深度偽造影像。 其他應用程式包括圖像和影片審查，以識別客戶或員工的盜竊行為； 確保員工遵守安全措施，例如在餐廳洗手或在建築工地使用安全帽； 甚至促進風力發電等行業的遠端預防性維護。

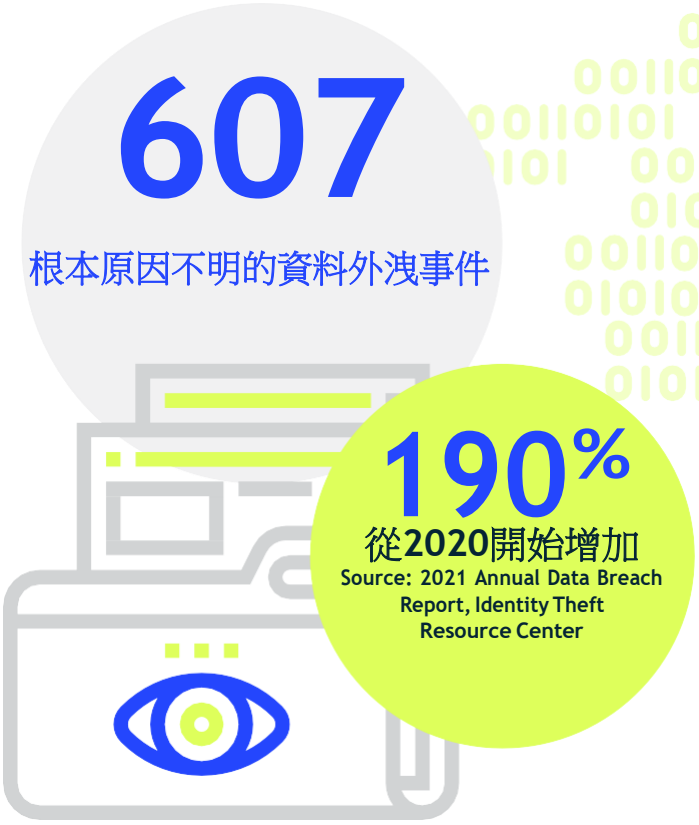
這些應用程式僅代表企業中潛在的深度學習用例的冰山一角。 根據最近的市場研究，“**2021** 年全球深度學習市場價值為 **29.9** 億美元，預計到 **2029** 年將達到 **687** 億美元。” 確定的主要驅動因素包括數位化趨勢的上升、網路攻擊的增加以及與先進技術的整合的增加。

基於深度學習的方法檢測特定威脅所需的時間比這些元素所需的總合要快得多。" HBT是一家跨國公司，提供航空航天、性能材料和安全及生產力技術。"

深度學習的另一個優勢是它能夠預測對抗性人工智慧的威脅。對抗性機器學習是一種技術，通過提供欺騙性數據來欺騙AI模型。從本質上講，攻擊者故意利用基於機器學習的傳統解決方案的工作方式，找到一種偏見，繞過他們的檢測能力，欺騙他們將惡意檔案視為良性檔案。然而，由於深度學習網路不依賴於特徵工程，因此威脅行為者更難創建能夠理解和利用系統運作方式的惡意軟體。

此外，深度學習模型可以使用極少的處理資源且部署在任何端點上。
深度學習的其他技術優勢包括識別惡意軟體和其他無檔案威脅的準確率大幅提高以及誤報率低得多。 而且由於深度學習與檔案類型無關，因此它可以應用於任何檔案格式，甚至適用於任何作業系統，無需進行大量修改或調整。

Mirel Sehic表示： "機器學習在很大程度上依賴於手動任務，您必須自行推斷並手動指導特徵以教授機器學習算法模型。" 然而，如果一個無監督的深度學習模型經過適當和有目的的建立，它可以應對大量的數據，主動預測和檢測資訊安全攻擊。



相反，深度學習的「低接觸性」使其對資源匱乏的組織特別有吸引力。Sehic 說「你不需要盯著螢幕，也不需要高技能的網路安全專家來梳理大量數據。相反的，深度學習與改進的網路安全威脅偵測相關，就是能夠以極少的人機互動來偵測新的威脅，同時不需要不斷更新該特定模型。 當你將這些因素與深度學習的低誤報率結合起來時，它在業界是無與倫比的。"

利潤成長是有可能的

除了技術實力之外，深度學習還可以帶來顯著的商業效益和成本節約。 卡斯皮說「不可能將原始資料直接輸入機器學習模型，網路安全團隊必須分析數據並確定其最重要的特徵和屬性。"
他說，這種情況的問題在於，僱用和保留必要的人才來執行特徵提取可能既昂貴又困難，特別是在當今緊張的勞動力市場中。

投資於人才、最佳實踐和合作夥伴

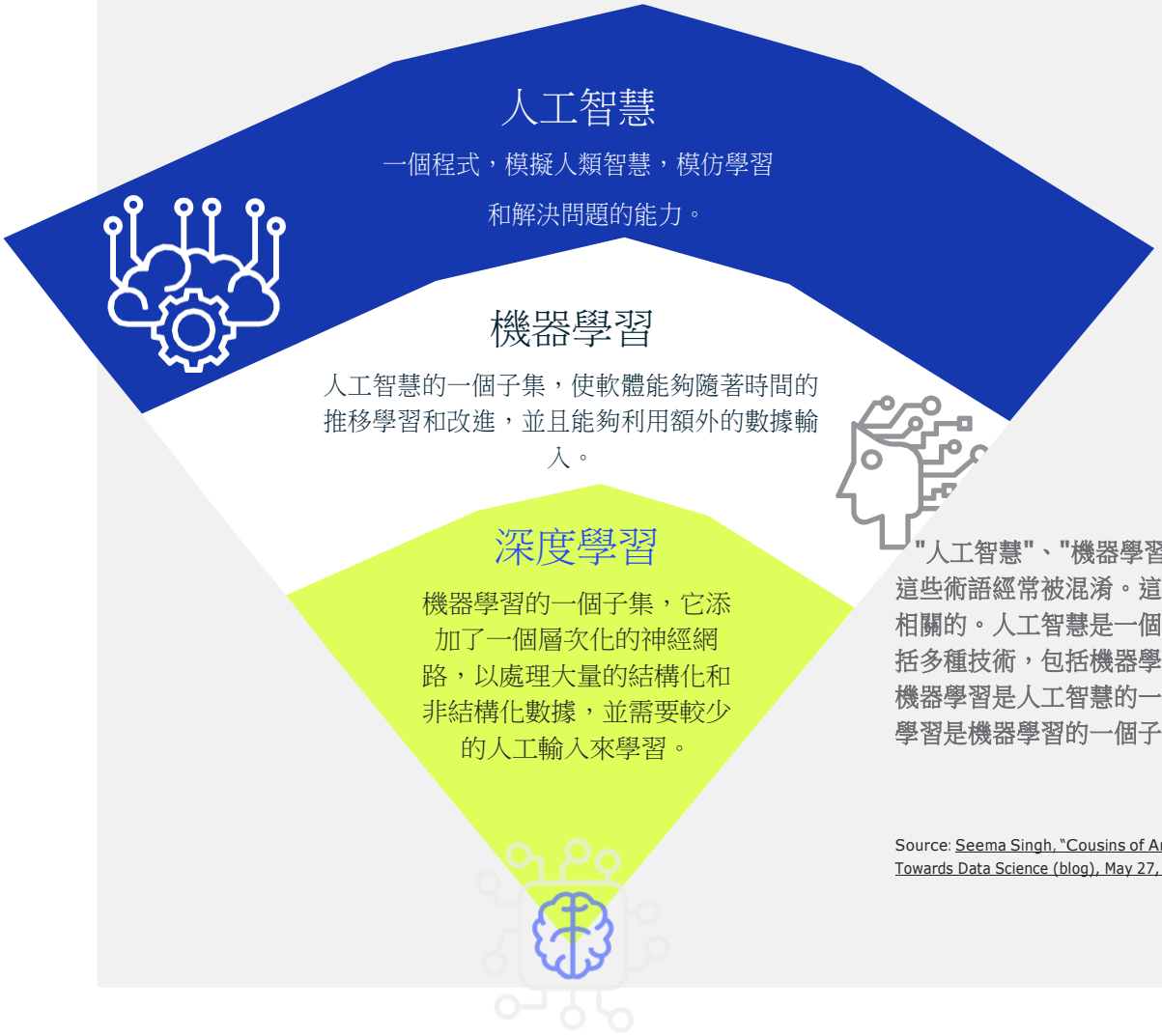
儘管存在重大的商業優勢，但在全面採用深度學習之前，組織必須採取一些重要的措施。首先，Caspi表示，資訊安全團隊必須仔細考慮培訓數據的數量和品質。這是因為培訓數據的品質越好，深度學習模型的性能就越好。

充分利用深度學習的另一種方法是將其與其他技術結合使用，例如自然語言處理和動態網路分析。 這樣做可以顯著提高保護和預防能力。 使用深度學習建立專注於即時預防的一流網路防禦系統，可確保快速偵測日益複雜的攻擊向量和元件。

然而，即使是最強大的資訊安全防禦工具，也需要熟練的IT專業人員來操作。Honeywell的Sehic表示：“作為一個整體，人是良好安全架構和安全實踐的關鍵。對我們來說，真正重要的是擁有合適的團隊，專注於解決關鍵基礎設施環境中的運營技術挑戰。"

> “深度學習勝過任何黑名單、啟發式或機器學習方法”
>
> **- Mirel Sehic，Honeywell的資訊安全主管**

人工智慧 vs. 機器學習 vs. 深度學習



"人工智慧"、"機器學習"和"深度學習"這些術語經常被混淆。這些技術是獨立但相關的。人工智慧是一個廣泛的領域，包括多種技術，包括機器學習和深度學習。機器學習是人工智慧的一個子集，而深度學習是機器學習的一個子集。

Source: Seema Singh, “Cousins of Artificial Intelligence,” Towards Data Science (blog), May 27, 2018

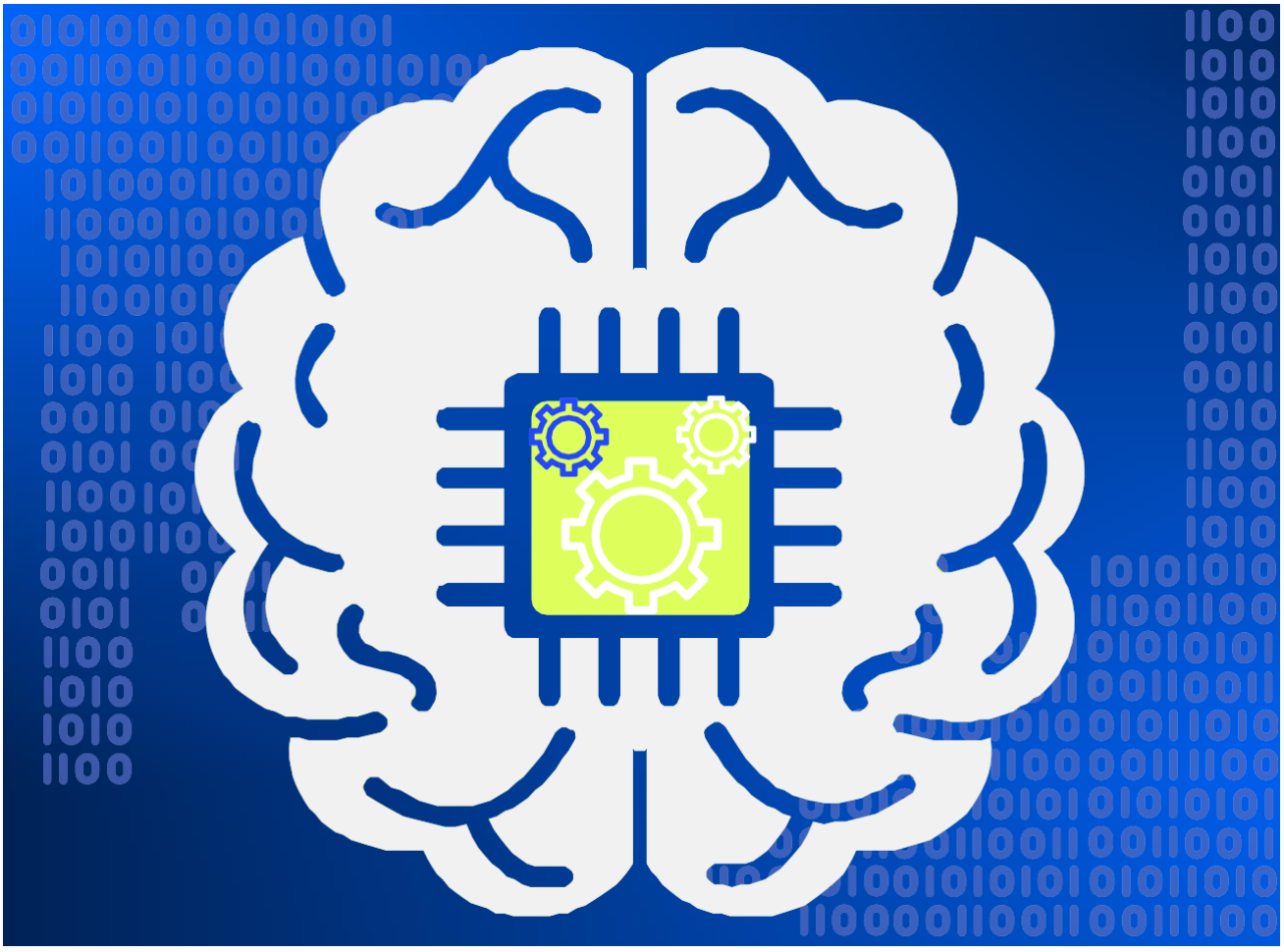
Sehic表示，組織必須花時間不斷教育那些從事資訊安全和深度學習系統介紹的人，同時提高非安全角色員工的資訊安全意識。教育計劃包括幫助員工認識攻擊對組織財務狀況的潛在影響、資訊安全威脅不斷增加，以及能夠保護系統免受惡意行為者威脅的對策和最佳實踐。

不斷演變的資訊安全攻擊需要不斷發展的打擊犯罪網路的工具和技術來抵禦。然而，IDC的Suby表示，大多數IT團隊缺乏時間和專業知識來不斷審查新供應商和解決方案。因此，他表示:「許多組織與託管服務提供商或託管資訊安全服務提供商合作，指導他們使用的產品和技術。借助這些關係有助於確保組織擁有最優化的解決方案，以保護其環境。"

一個新的典範

透過模仿人類大腦的功能，深度學習可以以無與倫比的速度和準確性識別可疑活動，這些活動可能表明不良行為者或惡意軟體的存在。這有助於組織更好地預測和防止攻擊，以防止損害品牌聲譽、侵蝕股價或導致收入損失。然而，這並不意味著深度學習能夠單獨對抗駭客。相反，深度學習、經驗豐富的專業人才和最佳實踐的有力結合可以在快節奏的世界中提供明顯的競爭優勢。

正如Sehic所解釋的，"我們正在過渡到這種新的範式，使用深度學習的創新解決方案不再是一個只能由專業高科技人員使用的 '神奇事物'，而是現在每個人都可以使用的。"



《深度學習提供主動網路防禦》是《麻省理工學院技術評論洞察》的執行簡報。

關於麻省理工學院技術評論洞察

麻省理工學院技術評論洞察是世界上歷史最悠久的技術雜誌《麻省理工學院技術評論》的客製化出版部門，得到世界上最重要的技術機構的支持，針對當今領先的技術和商業挑戰舉辦現場活動和研究。 Insights 在美國和國外進行定性和定量研究與分析，並發佈各種內容，包括文章、報告、資訊圖表、影片和播客。 透過其不斷壯大的《麻省理工科技評論全球洞察小組》，Insights 擁有無與倫比的機會接觸世界各地的高階主管、創新者和企業家，進行調查和深入訪談。

贊助商資訊

Deep Instinct 採用以防為主的方法，使用全球首個和唯一的專用深度學習資訊安全框架來阻止勒索軟體和其他惡意軟體。我們可以在不到20毫秒的時間內預測和防止已知、未知和零日威脅，速度比最快的勒索軟體加密快750倍。Deep Instinct具有超過99%的零日準確率，承諾<0.1%以下的誤報率。

Deep Instinct Prevention Platform是每個安全系統的重要組成部分，提供跨混合環境的多層次威脅防護。

Illustrations
Cover art and spot illustrations created by Chandra Tallman Design LLC, compiled from The Noun Project.