Darktrace Version 5： 自主 AI 升級版

Darktrace Version 5 以我們的核心 AI 引擎爲基礎，並採用了全新自動化形式，擴大了組織營運模式的防禦覆蓋範圍，增強了客戶體驗，能夠適應日益多變的工作型態。

隨着組織加速數位轉型並逐步爲未來工作做好準備，企業安全正經歷重新調整和定義的階段。多變且不可預測的工作型態已成爲數位化業務的常態，而攻擊者也相應調整他們的技術，許多組織都在努力應對以人爲中心的網路攻擊。

Darktrace 免疫系統可透過自我學習 AI 自主運行了解並適應未知和不可預測的行為。它利用人工智慧了解組織內所有員工的行為 — 無論他們在哪裡工作或是使用哪個應用程式。透過對端點和電子郵件以及雲端和協作工具提升實適應性 AI 防護範圍，Darktrace 可以積極地防止企業內部出現保護漏洞。

無論貴組織需要增加對創新技術防護領域以及優先處理運行速度的投資，還是試圖從現有技術中獲得更多的價值，Version 5 都能爲您提供很多益處。此次升級代表着在平台的三個不同但相關領域的自主功能的擴展。

AI 技術擴展應用

Antigena 自主防禦 和 Cyber AI Analyst 防護能力的增強

- Antigena 擴展
- 針對雲端和工業網路的 Cyber AI Analyst
- 針對第三方應用軟體的 AI 警報
- 使用者指定事件進行 AI 調查報告
- 與 SIEM、SOAR 和 SOC 系統共享 AI 事件報告的外部 API
- Antigena Email 的全新記述方式

員工的防護範圍

擴展跨客戶端、雲端服務和協作平台的防護範圍

- 用戶端感測器
- SaaS 介面
- 用於 SaaS 的 Antigena
- 用於 Slack、Zoom、Okta、Duo 等的全新模組
- 與零信任技術的全新整合
- 用於雲端與 SaaS 的 Cyber AI Analyst

互通性

統一的介面、靈活的整合和雲端部署

- 一鍵整合
- 統一的介面
- 系統狀態頁面
- OT 工程師介面
- 增強的模型編輯器和進階搜尋 UI 介面
- 雲端部署

Version 5 有哪些新增功能?

AI 技術擴展應用

隨著遠距工作及數位轉型帶來的風險和複雜性，安全團隊的工作充滿挑戰。 相關人員正逐步部署全新技術和服務；資料流和拓撲正在不斷變化；無論我們如何努力快速地重寫規則、特徵碼、政策和解決方法，它們已經無法適應不斷變化的使用者和工作型態。

Cyber AI 在企業環境中持續發現的攻擊技術與已知的規則和特徵碼截然不同，資訊安全的管理面臨駭客科技進步快速且複雜的挑戰，即使是最快的規則編寫者也無法對其進行預測。 我們在資訊安全產業面臨並將持續面對的挑戰是增強防禦功能的迫切需求，爲了實現這一目標，Darktrace 在平台的兩個核心領域增強了自己的自學能力：自主防禦和 AI 調查。

「Immune System 的自主性對我來說非常重要，我們無需進行手動管理，它可以自主回應，迅速阻止威脅。 Darktrace 就像是 IT 團隊中加入了一位成員，但它的意義遠不止於此。 您如果付錢給另一個人，讓他每天 24 小時坐在那裡，會發現他獲取的數值無法與 Immune System 相提並論，因爲人類的反應速度不夠快。對於 Version 5 中的新功能來說，這一點更是體現的淋漓盡致，它不僅增強了 Cyber AI Analyst 的能力，還發佈了雲端服務和協作工具的自主功能。」

Saddleback 技術與人事主管 John Wager

Darktrace Antigena：自主防禦向 SaaS 應用程式擴展了自主防禦功能

當 Darktrace 免疫系統偵測到一個新出現的網路威脅時，Antigena 會以最精準且迅速的行動中斷攻擊。透過在數秒內遏制新威脅，自主防禦功能可幫助安全團隊在攻擊數量和速度持續上升的情況下，優先處理策略性工作。

面對機器速度的威脅，Antigena 既可以採取自主行動，也可以與現有應用程式整合，作爲一種回應機制，通知第三方系統已經遭受的攻擊。透過 Version 5，Antigena 可消除 SaaS 服務中的各種攻擊 — 從 Microsoft 365 的電子郵件平台，到 Zoom 和 Teams 等雲端協作工具，也有像 SharePoint 和 OneDrive 這樣的雲端檔案儲存應用程式。

Antigena SaaS 的常見用例包括遭洩露的 SaaS 或電子郵件憑證、內部威脅和管理員遭到濫用。透過停用使用者或阻止存取，Antigena 可以在沒有人爲干預的情況下自動保護您雲端中的寶貴資料。

Microsoft 365 SharePoint zoom OneDrive Microsoft Teams Microsoft Dynamics 365

Cyber AI Analyst：AI 調查報告
將 AI 調查報告擴展至您的員工和資訊安全管理

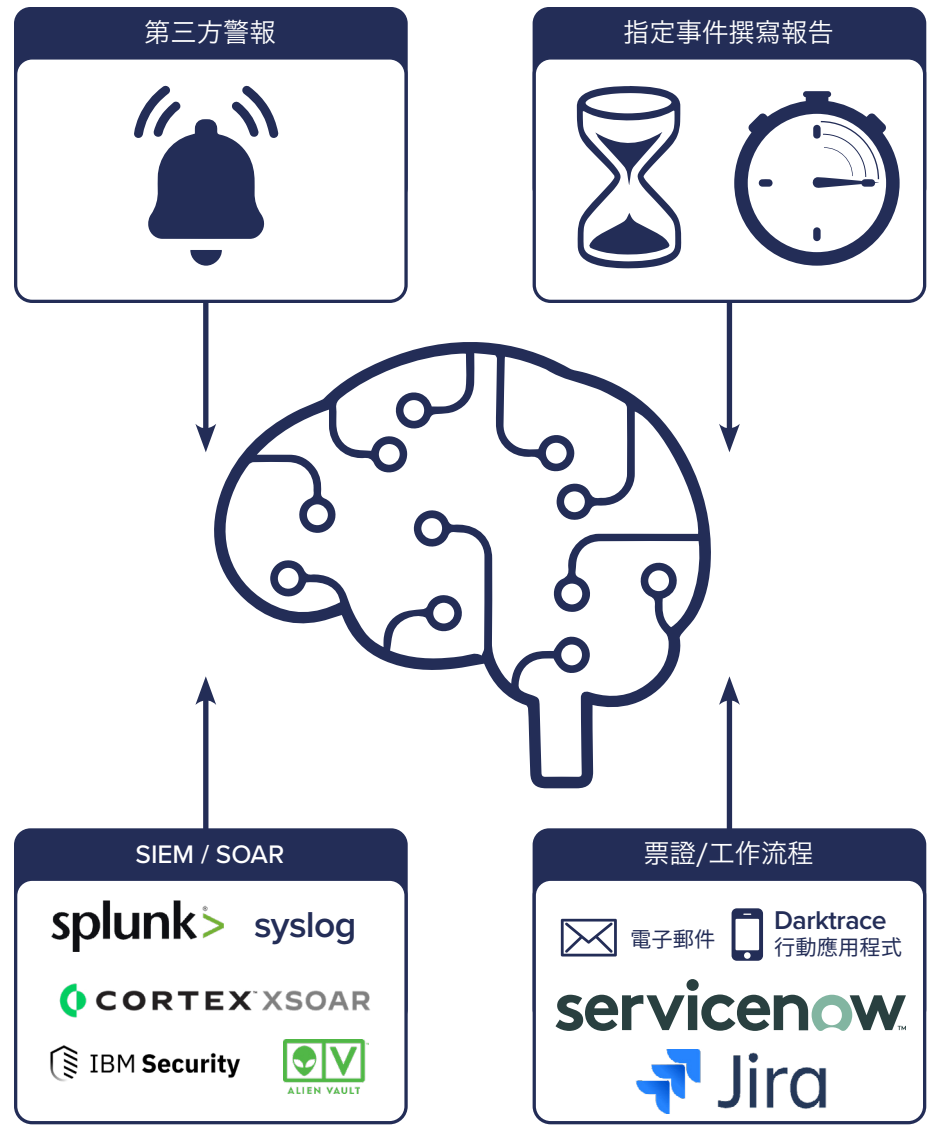
Cyber AI Analyst 是 Darktrace 的 AI 調查技術，它可針對您組織內員工的遠距工作型態進行全方位的自動分級、分析和報告。透過結合專家分析師行爲和進行專屬 AI 的訓練，Cyber AI Analyst 可將分級時間減少至多 92%，爲資源緊張的安全團隊提供了關鍵的 AI 增強支援。

透過對 Darktrace 免疫系統偵測到的所有安全事件進行持續自動調查，Cyber AI Analyst 可產生一個動態形勢儀錶板以及書面報告，可讓安全團隊快速就位，採取行動。

Version 5 將 Cyber AI Analyst 的範圍從網路事件擴展到 SaaS 應用程式、雲端基礎設施和網路實體系統。 它還有助於 Cyber AI Analyst 對感興趣的使用者和裝置進行調查，接收第三方警報以觸發新的調查，並自動向任何 SIEM、SOAR 或下游追蹤系統提供 AI 事件報告。

「Cyber AI Analyst 的新功能爲我的團隊增加了真正的價值，特別是隨時啓動事件調查和查詢 SaaS 資料或可疑裝置的能力。AI Analyst 雖然很複雜，但它提供給我們的情報既清晰又具有實操性 — 即使是我們這些沒有經驗的新手也能在一天內立即上手並從中獲取資訊。」

Calligo 首席資訊安全官 Mark Herridge



員工的防護範圍

如今，數位轉型變化快速且難以預測，組織營運模式需要因應快速的科技發展。關鍵資料和應用程式存取於不熟悉的雲端服務中，而員工的行爲通常發生在傳統防禦範圍之外，過於寬鬆的權限為網路罪犯和內部威脅提供了便利的渠道。

在這種背景下，能夠隨着組織營運模式的快速發展，且不斷提升安全策略以適應多元且多變的遠距辦公模式便顯得尤為重要，尤其是在組織長期採用零信任策略、雲端服務和更多元的工作模式的情況下。

用戶端感測器：將網路可視性擴展至中斷連線的端點

爲了覆蓋關閉 VPN 連線的分公司和遠端員工，Darktrace 現可在一系列受管理的端點上部署輕量型用戶端感測器。 這有助於系統分析遠端員工的即時流量，就像它分析網路流量一樣，將一個連接網路關聯起來，以逐步瞭解員工行為。

用戶端感測器可對關閉 VPN 連線時發生的可疑活動提供急需的可見性 — 從內部威脅和合規性問題，到潛在的惡意軟體（當員工重新連線時，惡意軟體可能會水平移動）。

雲端、SaaS 和零信任技術：擴展員工行為的防護範圍

如今，最關鍵的員工活動可能集中在 SaaS 應用程式中，因為利用雲端服務的使用者越來越多， 如 Salesforce、Google Workspace、Box、Dropbox 和 Microsoft 365。這些應用程式有助於大規模地提高效率和創新性，因此各種形式和規模的組織都將它們用於核心業務功能和操作。

然而，當我們將操作轉移到雲端時，爲 SaaS 建立的防禦機制只能提供靜態和單一封閉的保護，幾乎無法起到防護作用。

Darktrace 免疫系統透過一系列關鍵的增強功能補充了雲端和 SaaS 防禦，包括專用 SaaS 主控台、從自主防禦和 Cyber AI Analyst 調查到雲端的擴展，以及與 Zoom、Okta、Microsoft Teams 等的整合。

同樣地，新功能能擷取針對 VPN 和零信任技術的行為有助於 Darktrace 在任何工作地點為員工的資訊安全提供保護。

Darktrace SaaS 介面

互通性

統一的介面

Darktrace 免疫系統是唯一可以在您的整個數位環境中學習「正常行為」的自我學習平台 — 從雲端、SaaS 和電子郵件，到端點、物聯網和網路實體系統。

與傳統利用規則和特徵碼的解決方案不同，Darktrace 的平台利用 AI 引擎從各種資料源中學習、偵測、解釋和回應網路環境中的新威脅。

Version 5 不但為系統引入了新的功能 — 從專用 SaaS 的平台到專用 OT 工程師使用介面，總體設計原則仍然維持一貫的統一性訴求，以促進調查效率和簡化工作流程。

「Version 5 具有非常出色的創新性，從新型雲端部署的靈活性到 Darktrace 用戶端感測器端的擴展可視性，都與我們安全團隊的當前需求相契合。」

Linc Cymru Housing Association **技術主管** Peter Murphy

一鍵整合

Darktrace 平台採用開放和可擴展的架構設計，可與您現有的應用程式無痛整合。Version 5 可幫助使用者透過一鍵整合來增強和擴展他們的 Darktrace 部署。

其中包括能夠立即擴展到新型雲端服務、透過新的記錄擷取源強化平台分析，並透過與其他安全防禦的整合啟動自主防禦能力。隨着組織加速數位轉型並逐步爲未來工作做好準備，快速適應和整合其安全防禦的能力將比以往任何時候更加重要。

靈活傳送

隨着系統優化，自主防禦功能能快速適應產業變遷並且與第三方應用程式整合安全防能力一直是 Darktrace 奉行的準則。 Version 5 不僅將 Darktrace 免疫系統擴展至不同的產業領域，並且確保客戶無論從哪個應用程式開始使用平台，都能無痛整合。Darktrace 系統能夠適應各種網路環境，不論您選擇 100% 雲端部署，或是選擇覆蓋內部和雲端環境的混合式部署。

關於 Darktrace

Darktrace 是領先的自主人工智慧資安公司，以及自主防禦科技的創始者。 Darktrace 的自我學習 AI 由人體免疫系統為藍本，協助 4 千 700 多個組織抵禦雲端、電子郵件、SaaS、傳統網路、物聯網、端點以及工業系統威脅。

Darktrace 在全球擁有超過 1500 名員工，總部設於英國劍橋。每隔 1 秒鐘，Darktrace AI 自動抵抗網路威脅，防止它造成損害。

如需更多資訊

- 瀏覽 darktrace.com
- 預約 demo
- 瀏覽我們的 YouTube 頻道
- 在 Twitter 上關注我們
- 在 LinkedIn 上關注我們