Enterprise Immune System 與 Darktrace Antigena

適用雲端和 SaaS 的 Cyber AI

Darktrace 的 Cyber AI 平台以領先世界的 AI 為基底，保護各種動態雲端和 SaaS 平台，並且隨環境擴充和發展自動調適。不管是面臨內部威脅、遭洩露的身份驗證還是嚴重的配置不當，Darktrace 讓人注意到雲端中的盲點以保護無論存在何處的數據。

主要優點

- 以自我學習方式發現其他人所遺漏基於雲端的威脅
- 跨混合與多雲端環境的統一覆蓋
- 100%的即時能見度使攻擊者無處躲藏
- 自主防禦能在幾秒鐘內消除發展中的威脅

Darktrace AI 可以檢測：

- 內部數據盜竊
- 遭洩露的身份驗證
- 社交工程
- 嚴重的錯誤配置
- 供應鏈攻擊
- 橫向移動

雲端原生保護

box, salesforce, Google Cloud Platform, G Suite, OneDrive, aws, Microsoft Azure, Microsoft 365, Dropbox, SharePoint

適用雲端的免疫系統

隨著組織越來越依賴雲端來簡化操作並實現創新，保護關鍵數據的挑戰也將採取新的思維。對於傳統安全團隊而言，各種形式的雲端通常都是不熟悉的領域，網路罪犯比任何人都更了解這一點。

Darktrace 的 Cyber AI 透過從頭開始學習每個用戶、容器和虛擬機器的獨特「行為模式」，並將其與其他業務聯結來保護雲端。這種即時「自我學習」的理解，使 Darktrace 能夠偵測和防禦其他工具所遺漏的細微威脅或雲端中的配置不當。

統一和定製的保護

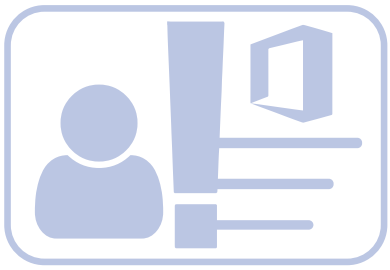
威脅行動者逐漸能夠不把一次攻擊侷限於一種技術，組織在整個數位業務中統一其防禦至關重要，諸如被洩露密碼之類的簡單事件就可能導致立刻攻擊多項設施。即時看清楚這一點極為重要，因為根據每種技術的基礎處理安全議題已不再具有意義。

經由了解整個組織獨特的「DNA」，Darktrace 的自我學習方法採取獨特的方式檢測和防禦雲端中的新型攻擊和內部威脅。如果單獨檢視一個特定攻擊，它可能看起來無害；但是透過 Darktrace 所提供定製且包含整個企業範圍的手法，則可以找到最細微攻擊的出現。

AWS、Azure 和 GCP 中的原生雲端安全

對於在 AWS、Azure 或 GCP 中架設基礎設施的組織，Darktrace 透過 AWS VPC Traffic Mirroring、Azure vTAP 和 GCP Packet Mirroring 而提供原生支援。這些系統針對 Darktrace 提供精細、即時的雲端流量存取，而且不需要任何 agent 來捕捉數量。

個案研究：Microsoft 365 中遭洩露的身份驗證



在某個國際組織中，Darktrace 發現了一起繞過 Azure Active Directory 原生控制項的 Microsoft 365 帳戶網路攻擊。雖然該組織在全球各地都設有辦事處，Darktrace AI 在 IP 位址發現一個對於該用戶及其同事群組來說均屬很不尋常的登錄名稱，因此立即向對資訊安全團隊發出警示。

接著，Darktrace 通知他們在帳戶中新建立的電子郵件處理規則將會刪除傳入的電子郵件。這顯示洩密的明顯跡象，因此安全團隊在攻擊者進行破壞之前就能先封鎖該帳戶。

客戶對我們的評語

> 當我們啟動 Darktrace 來保護我們的雲端環境，就如同在黑暗的房間裡開了盞燈。
>
> **- Director of IT, TRJ Telecom**

> Darktrace 的方法是目前市場上最好的方法，能夠在威脅升級之前找到基於雲端的威脅。
>
> **- CISO, Aptean**

> Darktrace 代表了基於 AI 的網路防禦新領域。現在，我們的團隊對我們整個 SaaS 應用程式和雲端容器具備完整的即時覆蓋。
>
> **- Director of IT, City of Las Vegas**

更多資訊

馬上預約 Demo

雲端白皮書

Darktrace 用戶心得