DARKTRACE HEAL™

DARKTRACE

組織變遷，威脅演進

面對不斷變化的威脅環境，人力資源的限制、不完善的流程和不符合實際需求的解決方案往往使資安團隊在因應新興資安事件時困難重重。
因此，各組織企業的資安長必須著重審視自身資安技術的是否完善（包括正確配置達到最有效的防禦），並檢視資安團隊應對網路攻擊的能力。隨著組織變遷，若「劇本（playbook）」的標準化流程仍維持靜態而不變，因應措施將遠不及威脅的演進。

隨著ChatGPT 普及，
2023年「新型社交工程」攻擊
增加了 **135%**

＊數據統計源於2023 年 1 月至 2 月期間Darktrace/Email部署環境中所偵測的電子郵件攻擊平均增長率（去除極端值）。

Darktrace HEALTM人工智慧深入了解企業數據，
確保組織在遭受攻擊的當下能迅速修復資安防禦，並恢復企業正常運作。

不斷進行防禦力評估，並優化您團隊和技術的事件應變能力。

我的團隊和技術是否能在必要時如期運作？

- 進行事件模擬和應變能力演練
- 產出應變能力報告

及早處理事件，並快速修復。

我該如何針對正在發生的攻擊進行超前部署？

- 由人工智慧產生的客製化標準流程「劇本（playbook）」
- 自動產出的修復和恢復措施

自動產出的報告與輕鬆上手的協作服務，幫助團隊節省寶貴的時間。

我該如何在團隊有限的時間內將效率提升到最大？

- 自動產出事件報告
- 提供安全的協作與溝通平台
- 提供技術整合

功能特色

應變能力分析｜萬全準備，隨機應變

綜合Darktrace DETECT所收集的資訊（包含裝置和通訊數據），Darktrace HEAL會透過其所建立的企業認知，分析該組織在面對資安攻擊的應變能力。當Darktrace HEAL隨著組織變遷持續提供分析評估時，企業亦可即時了解組織的資安韌性及如何有效提升自身防禦力。

事件模擬和應變能力演練｜眞槍實彈，隨時迎戰

透過模擬眞實案例的攻擊事件，確保企業有隨時迎戰的準備。模擬事件的演練和測試可幫助團隊找出應變系統中相對薄弱或有漏洞的環節。

修復決策引擎｜快速復原，維持運作

當事件發生時，Darktrace HEAL不會強制套用統一的標準流程「劇本（playbook）」，而是透過修復決策引擎根據精確的事件詳情自動調整應對措施。大部分修復流程已自動化，僅在必要時依即時動態向人員團隊提供建議，透過自動執行、委派工作和持續追蹤幫助團隊修復資產。

安全的協作與溝通平台｜找對的人，做對的事

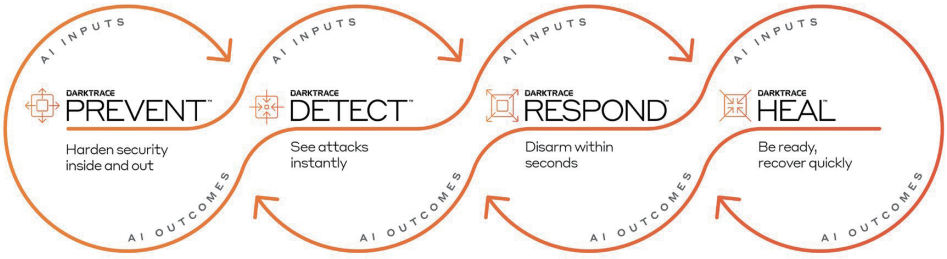
Darktrace HEAL可幫助企業集中並協調團隊溝通，快速召集相應的人員並傳達重要資訊。

前後完整的事件報告｜自動產生，省時省力

HEAL不僅可以自動記錄已完成和計劃執行的動作、決策和筆記，還可以將事件分析和封鎖資訊結合，提供可匯出PDF的詳細事件報告。

Darktrace HEAL完整了Cyber AI Loop。

在這個全年無休的資安生態系統中，各個環節透過彼此自動反饋不斷改善企業資安狀態。



Darktrace會在事件期間和事件後自動將HEAL所產出的資訊回饋給Cyber AI Loop，協助優化未來應變。

透過與資安生態系統的相互溝通，系統可以預測攻擊方可能採取的下一步行動並提前準備，強化防禦能力。

舉例：

- DETECT & RESPOND能提供關鍵的背景資訊以及正在進行的封鎖動態給HEAL，協助HEAL進行決策。
- 在事件發生後，DETECT會更緊密的監控和保護近期修復的設備。
- 在修復的過程中，HEAL會透過PREVENT所提供的背景資訊了解關鍵攻擊路徑及其潛在影響，優先處理高風險項目。

Darktrace HEAL使用需求：必須在網路、雲端、終端裝置或OT中至少其一領域部署Darktrace DETECT。

DARKTRACE

黃靖怡
台灣區業務總監

+886 972 600 229
+886 2 8729 5865

april.huang@darktrace.com
https://darktrace.com

臺北南山廣場
110臺北市信義區松仁路100號34樓