Crowdstrike 產品

CROWDSTRIKE

CROWDSTRIKE FALCON 端點偵測及回應 (EDR)

以快速、自動化與無可比擬的能見度，串流威脅偵測與回應生命週期

FALCON INSIGHT — 輕鬆簡單的 EDR

傳統端點安全工具有其盲點，無法偵測並阻止進階威脅。CrowdStrike® Falcon Insight™ 可提供整個組織的完全能見度，解決此問題。

Insight會持續監控所有端點活動，並即時分析資料以自動識別威脅活動，藉此偵測並防範進階威脅發生。所有端點活動均會串流至 CrosdStrike Falcon® 平台，供安全團隊快速掃描並調查事件、回應警示，以及主動搜尋新威脅。

FALCON INSIGHT 就是 EDR 方面的領導產品

Forrest Wave™ 排名第一的領導產品：端點偵測及回應，2018

在 2018 年 MITRE 國家級模擬測試中，經追蹤及偵測進階攻擊之 MITRE ATT&CK™ 框架驗證

SC Magazine的 2018 年「推薦首選」，SC Labs在所有類別均給予五星評價

在 Gartner2017 年端點偵測及回應技術與解決方案比較報告中，於所有評估的使用案例中獲得最高評分

主要優點

自動偵測進階威脅

搭配即時深度鑑識的快速調查

安心回應與修復

進行五秒企業搜尋

啟用 Falcon OverWatch™ 威脅搜尋服務

透過以 MITRE 為基礎的偵測框架，對複雜警示一目瞭然

主要產品功能

簡化偵測與解決方式

- **自動偵測攻擊者活動：**Insight使用 IOA (攻擊指標) 自動識別攻擊者行為，並將優先警示傳送至 Falcon UI，消除耗時的研究與手動搜尋作業。CrowdStrike Threat Graph™ 資料庫會存放事件資料，即便面對數十億筆事件資料，也能於五秒內回覆查詢。
- **在單一畫面徹底分析整個攻擊：**易於閱讀的流程圖可提供整體攻擊的情境資訊，讓調查快速又輕鬆。
- **加快調查工作流程：**讓警示對映 MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)框架，即便最複雜的偵測結果也能一目瞭然，藉此縮短分級警示所需時間，並加快優先順序的決定與修復。此外，符合直覺的 UI 可讓您快速切換操作，在數秒內搜尋整個組織。
- **取得情境資訊與情報：**整合式威脅情報可提供整體攻擊的情境資訊，包括事發原因。
- **果斷回應：**即時採取行動因應駭客，在發生入侵攻擊前便予以阻止。強大的回應動作可讓您遏止遭受入侵的系統並進行調查，即時回應功能可讓您直接存取受調查的端點。如此一來，安全回應者便能在系統執行動作，並以極高精準度消滅威脅。

即時獲得全領域能見度

- **即時觀察所有動作：**立即能見度可讓您檢視駭客的活動，一舉一動都難逃法眼。
- **擷取威脅搜尋與鑑識調查的關鍵細節：**Falcon Insight核心模式驅動程式會擷取超過 400個原始事件與必要的相關資訊，以反向追蹤事件。
- **在數秒內獲得解答：**CrowdStrike Threat Graph™資料庫會存放事件資料，即便面對數十億筆事件資料，也能於五秒內回覆查詢。
- **為期 90 天的重新叫用：**Falcon Insight 會將完整的端點活動保留一段時日，無論您環境中具有少於100個端點或多於50萬個端點都沒問題。

立即實現價值

- **省時、省力、省錢：**已啟用雲端的 Falcon Insight 由 CrowdStrike Falcon 平台提供，且不需要任何內部部署管理基礎架構。
- **部署只需數分鐘：**CrowdStrike客戶可一天內將雲端提供的 Falcon代理程式部署至最高 7 萬個端點。
- **馬上運作：**Falcon Insight在開始使用時即擁有無可比擬的偵測能力與能見度，無需重新開機、微調、設定基準或複雜的設定，安裝後即可執行、監控並加以記錄。
- **對端點無絲毫影響：**端點上僅有一個輕量型代理程式，且會在 Threat Graph資料庫中進行搜尋，因此不會對端點或網路造成任何影響。

防止「無聲侵略」並遏止入侵攻擊的力量

防範技術尚未完善。如果攻擊者有辦法突破貴組織的防禦，他們就能在數週或數月內隱藏蹤跡，因為安全團隊缺乏能見度與偵測工具來辨識入侵攻擊後的活動。這個「無聲侵略」的階段就是攻擊者的勝利，也是組織的潛在災難。Falcon Insight 可快速偵測、辨識，並讓您回應現有防禦措施無法偵測到的事件。

關於 CrowdStrik

CrowdStrike是雲端提供的新一代端點保護的領導廠商。CrowdStrike是業界領先唯一將新一代防毒軟體、端點偵測及回應(EDR)，以及 24小時全年無休管理式搜尋服務加以統整的公司，且僅透過單一輕量型代理程式就能提供，開創端點保護的革新局面。

如需更多資訊，請造訪
www.crowdstrike.com

數聯資安 Information Security Service Digital United
諮詢熱線：(02) 7721-1688
服務信箱：marketing@issdu.com.tw
WWW.ISSDU.COM.TW