Fidelis Elevate™

Active XDR 平台

資訊安全和其所保護的現代化運算基礎結構一樣，隨時都在改變。環境變化的速度雖快，但威脅變化的速度更快，企業隨時都得面對更為複雜的敵人、全新的攻擊戰術以及不斷被找出的漏洞。

Fidelis Elevate 是業界第一個 Active XDR (主動式威脅誘捕偵測及回應) 平台，專為以更快的速度偵測並抵禦敵人而設計。這個平台整合了欺敵技術與端點 (EDR)、網路 (NDR) 和雲端上的偵測與回應，讓 SOC 分析師可以更容易快速尋找和阻擋先進的網路威脅，減少可能導致重大損失的停留時間。

Fidelis Elevate XDR 可提供整個 IT 環境豐富的脈絡見解與可見性。欺敵技術讓使用者可以重塑網路地形，以在攻擊生命週期的初期與敵人交戰和對抗。威脅情資與見解可用來協助使用者領先敵人，有效防止未來的攻擊。

Fidelis Elevate 會儲存元數據 (Metadata)，可以讓使用者透過簡單的查詢搜尋過去的資料，以判斷系統是否遭到新辨識的攻擊活動成功入侵。歷史元數據 (Metadata) 可以讓資安團隊追蹤攻擊者的動向，判斷哪些其他系統遭到入侵，驅逐攻擊者並還原業務運作。

Fidelis Endpoint

以無與倫比的調查、鑑識與回應功能來保護網路內外的裝置

Fidelis Network

以更快的速度偵測與回應網路上任何位置的威脅 (包含電子郵件)

Fidelis Deception

重塑攻擊面，並在攻擊生命週期的初期引誘、偵測和防衛

以完整的情況認知領先敵人

網路地形知識可協助防衛者更為妥善地保護其環境。Fidelis Elevate 整合先進的技術，可提供跨越託管和非託管端點、網路流量以及雲端資產與服務的脈絡可見性和動態網路地形映射。藉此協助資訊安全分析師快速偵測和阻擋攻擊、對環境進行深度檢測 / 分析以評估是否有任何系統遭到入侵，並讓受影響的系統迅速地返回正常的業務運作。

Fidelis Elevate 提供：

- 可排除盲點和消弭資安缺口的完整地形映射與風險分析。
- 收集自所有資料來源的 360 度全方位見解。
- 整個 IT 環境的全方位脈絡可見性。
- 對於內嵌內容的深度網路可視性，包括跨越所有連接埠和通訊協定的加密流量(連入與連出)。
- 透過針對系統記憶體和檔案系統的鑑識能力，讓您深入了解每個處理程序的使用者和電腦行為。
- 在您的網路中的託管和非託管裝置的漏洞與即時監控。
- 南北流量偵測、橫向動作與資料外流。

加快決定和回應週期的速度

Fidelis Elevate 可以改善告警的準確性和可行性，並且讓 SOC 團隊在敵人的 OODA (觀察 - Observe、調整 - Orient、決定 - Decide、行動 - Act) 循環中作業，以高效率偵測與回應進階威脅。

有了 Fidelis Elevate 使用者可以：

- 主動偵測與驗證整個企業的惡意軟體。
- 利用歸納後的資料，以更快的速度制定更明智的決策。
- 利用和網路摘要整合的端點資料更妥善分類問題。
- 利用簡化的分析將劇本自動化。
- 利用準確的資料，有助於做出更好決策以採取回應行動。
- 利用所儲存的元數據 (Metadata) 進行即時與追溯性分析，以大幅減少攻擊者的停留時間與損害。

在敵人讓商業運作停止之前即與其交戰

Fidelis Elevate 中的欺敵技術可以讓資安團隊重塑網路地形、誘捕敵人，並以更快的速度尋找、抵禦和對抗先進的網路威脅。

有了 Fidelis Elevate 使用者可以：

- 主動強化防衛，包括可以從紅軍與藍軍的角度提供資安弱點見解的「風險模擬」。
- 利用以威脅和行為為主的分析，以更強大的信心更早偵測攻擊且更少誤判。
- 利用強大的威脅情資，更快速地進行偵測與回應。
- 透過攻擊路徑風險模擬深入了解潛在的攻擊途徑。
- 利用業界頂尖的欺敵技術動態控制並管理整個攻擊面。

以自動化行動回應

敵人可以在數分鐘內入侵網路並建立立足點。針對偵測結果自動回應，在同一時段內為防衛者提供應對工具。回應可以在網路上透過封包捨棄和電子郵件隔離進行，但也必須包括在遭到入侵的主機上進行的回應。當自動化劇本不足或無法使用時，有時需要分析師立即做出回應。

Fidelis Elevate 提供：

- 內含調查、破壞和補救行動的指令碼，可以對偵測結果做出回應的自動化劇本。
- 以來自 NDR、EDR、偵測以及電子郵件平台功能的偵測結果為根據的劇本回應。
- 支援 Windows、Linux 及 Mac 系統的 100 多個指令碼。
- 可增加回應的自訂指令碼，可以由現場的分析師建立，或是複製自我們的 Fidelis Hero 使用者分享網站。
- 主控台介面具備可以管理所有託管主機的程序檢視器和檔案介面，因此分析師可以採取任何必要的行動，以及撰寫可以在其他主機上重複這些行動的指令碼。

透過會學習和成長的平台情資取得優勢

有了 Fidelis Elevate，資安團隊便能對抗當前的威脅，並為未來的攻擊做出更妥善的準備。在威脅造成業務上的損害之前，持續的調查與發現過程可以針對這些威脅的防衛和抵禦提供需要的見解。

Fidelis Elevate 讓使用者可以更容易：

- 自動部署威脅情資。
- 利用誘餌、麵包屑及陷阱來引誘和干擾敵人。
- 主動分析誘餌活動，了解活動的來源與戰術、技術和程序 (TTP)。
- 將偵測結果轉換為 IOC。
- 輕鬆辨識與回應重新出現的攻擊。
- 讓回應自動化以防止攻擊重新出現。

放大現有的資安投資

Fidelis Elevate 在設計上係做為整合式「主動防衛 (Active Defense) 平台銷售。針對想要利用現有投資的使用者，Fidelis Elevate 也整合了許多第三方解決方案，為可能已是資安產品組合一部分的資安解決方案與工作流程提供銜接的管道。

讓 Fidelis Elevate XDR 立即發揮作用

了解如何利用 Fidelis Elevate XDR 以更好的方式跨端點、網路到雲端保護貴組織。如需詳細資料及免費示範，現在就透過［電子郵件］、撥打［電話］或是造訪 FidelisSecurity.com 與我們聯繫。

資安長的工作通常涉及隨時持續監控改善方法和尋找正面的趨勢，例如改善資訊安全、縮短平均偵測或回應時間，以及隨時降低風險。為了建立一個可以支援企業抵禦敵人的安全狀況，資安長每天都要考慮三個問題：

我現在是否比過去更安全？

Active XDR 平台提供持續威脅評估和風險評估。持續評估有助於找出弱點、強化企業資訊安全、隨時展現資安改善方法，以及協助量化與特定資安計畫相關的投資報酬率 (ROI)。

我目前是否遭到攻擊？如果是，會有什麼影響？

Active XDR 可以將整個 IT 環境中的告警進行整合、建立關聯並排定優先順序，藉此減少告警疲勞和誤報。因此可以針對最有可能影響到企業的威脅提供高可信度的可行性告警。利用歸納及調查工具快速驗證告警、遏制並緩解威脅，將對於企業營運所造成的影響降到最低。

我是否暴露在最新的威脅之中？如果是，會有什麼影響？

供應鏈入侵和勒索軟體攻擊等每一個新威脅都會揭露新的入侵指標 (IOC)，並啟動判斷企業是否遭到入侵的調查，可以輕鬆判定您是否暴露在威脅之中，並回覆關鍵的「主使者」、「事件」、「地點」、「時間」和「方式」等問題。

FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市三民區民族一路80號27樓之2 A08室

想了解更多訊息，請與我們聯繫

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity

Fidelis Cybersecurity combats the full spectrum of cyber-crime, data theft and espionage. A leading provider of threat detection, hunting and response solutions, Fidelis provides full visibility across hybrid environments, automates threat and data theft detection, empowers threat hunting, and optimizes incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense.

For more information go to www.fidelissecurity.com. Fidelis Cybersecurity is a portfolio company of Skyview Capital.