DATASHEET

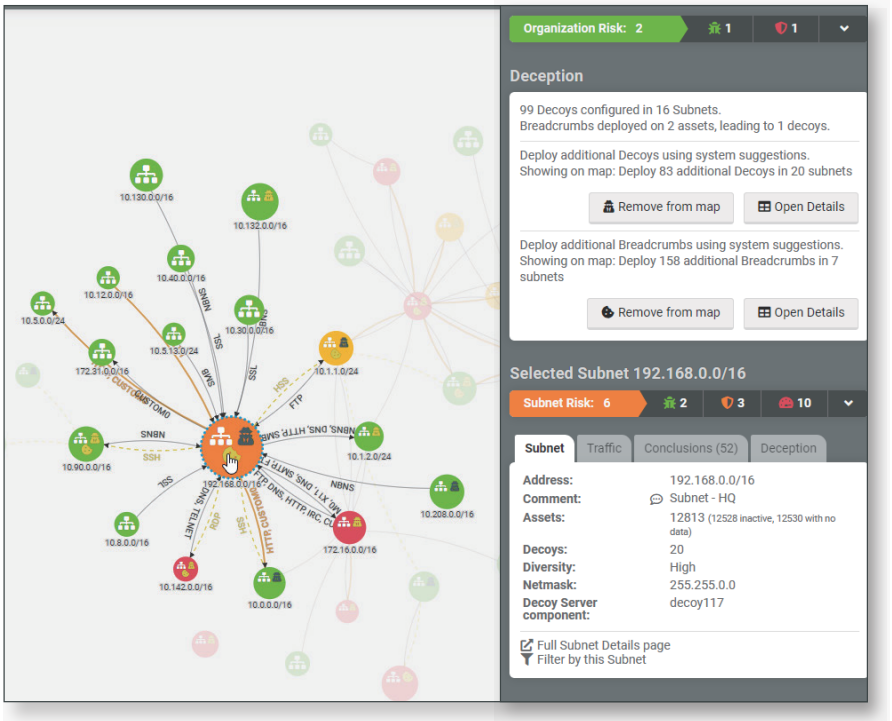
Fidelis Deception®

從 Real OS 到模擬式誘捕設備的多種誘餌選擇提供高精確度警報

動態欺敵的駭客誘捕科技

駭客誘捕科技給予分析師藉由改變自身網路環境的攻擊面，而大幅減少攻擊者於網路環境內停留的時間。此做法可以讓攻擊者不自覺地被減緩其橫向移動能力，消耗駭客進攻時間及增加攻擊者被發現的風險，給予分析師更多時間了解 TTP 並最終根除來自環境的威脅。

Fidelis Deception 可以使組織快速且精準的偵測已經存在於網路中的攻擊者、惡意的內部人員及軟體，與攻擊者交戰並壓制進階式網路威脅。分析師能自動建立真實互動作業系統誘捕設備，包括企業物聯網設備在內的擬真服務及作業系統。於是攻擊者會被不斷更新的麵包屑引誘至誘捕設備進而觸發告警。通過智慧誘敵、自動地形學習及可視性的獨特組合， Fidelis 使得攻擊者不斷盲目猜測並協助分析師將事件解決時間由數周或數個月顯著地縮短為數小時甚至數分鐘。



Fidelis Deception 利用改變組織的網路地形自動建立誘捕設備及麵包屑，改變被攻擊面。

核心優勢

- ✓ 智慧告警系統偵測網路內部威脅，以減少攻擊者停留時間
- ✓ 偵測外部攻擊及內部人員，以偵查其橫向動作
- ✓ 詳細瞭解攻擊路徑、重要資產及初始攻擊手法
- ✓ 老舊系統、企業物聯網設備及影子 IT 等在內的未知資產消除盲點
- ✓ 持續識別及分類資產設備，以生成具吸引力的誘捕設備
- ✓ 全自動佈署誘捕設備並持續適應網路環境變化
- ✓ 符合客戶需求的誘補設備選擇包括真實作業系統、golden image 作業系統及具備與攻擊者互動 ， 並提供檔案上傳的低風險模擬式誘捕設備
- ✓ 真實資產及 Active Directory的麵包屑來轉移攻擊者注意力，達成防禦效果
- ✓ 大幅減少無意義告警，產生高精確度告警
- ✓ 啟動紅隊及藍隊的風險模擬，以決定增強誘捕設備及麵包屑放置
- ✓ 整合 Fidelis Network® 及 Fidelis Endpoint® 的無縫式工作流程

關於駭客誘捕科技

藉由在真實資產上的麵包屑引誘攻擊者、 惡意的內部人員及自動惡意軟體將被引導向誘捕設備，使欺敵策略效益最大化。取代在大量資料中徒勞無功地搜尋惡意執行者，駭客誘捕科技從誘捕設備、 AD 驗證資訊與流量分析中傳送可執行的告警及事件。這些告警具有極高的精確度。
使用有新活動資料的欺敵策略可以建立有說服性的誘捕設備，包括拖延攻擊者進攻時間的機制、資料和監控活動行為。他們追尋誘餌至誘捕陷阱，讓您可以偵測及防禦。

誘餌

- 硬體 - 工作站、伺服器、路由器、交換器、監視器、印表機、企業物聯網裝置等等
- 軟體 - 作業系統、應用程式、埠、服務等
- 誘捕設備理應是用戶環境內未知的存在，員工不該存取及使用
- 高度及中等互動式誘餌，分散對真實資產注意的方式來消耗攻擊者的時間

麵包屑及陷阱

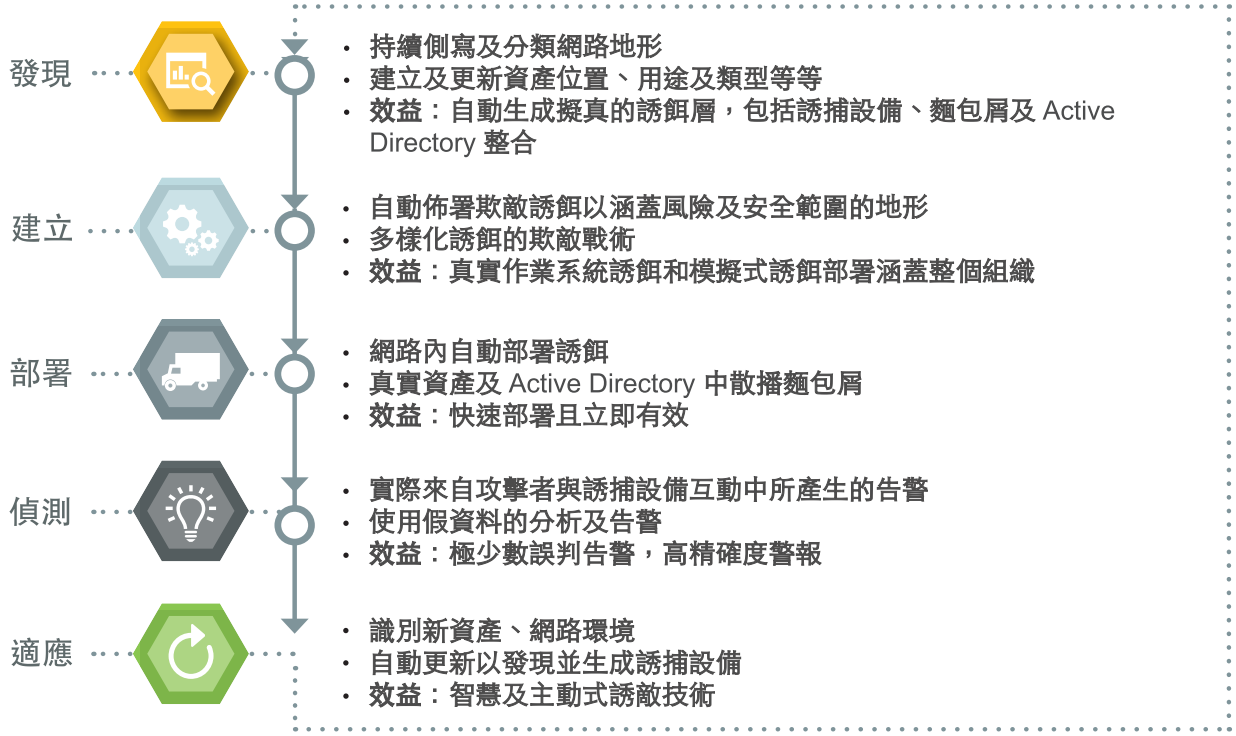
- 陷阱：檔案、應用程式、網路或驗證資訊
- 麵包屑：檔案、文件、電子郵件或是系統資源等
- 誘惑攻擊者所使用的假資料、驗證資訊及簡介

入侵後的攻擊偵測

- 資料分析顯示使用了假的資料 (例如驗證資訊)
- 以誘捕設備及麵包屑監控攻擊者行為
- 誘餌及資料告警相關的網路分析

主動式欺敵

- 誘捕設備及麵包屑的自動化及適應部署
- 偵測橫向感染，攻擊者的偵查及活動
- 學習 TTP (戰術、手法及進程)資產可視性與鑑識
- 擁有分析、獵捕及行動的完整欺敵科技的控制台
- 對營運及用戶沒有影響，對資料及資源沒有風險



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