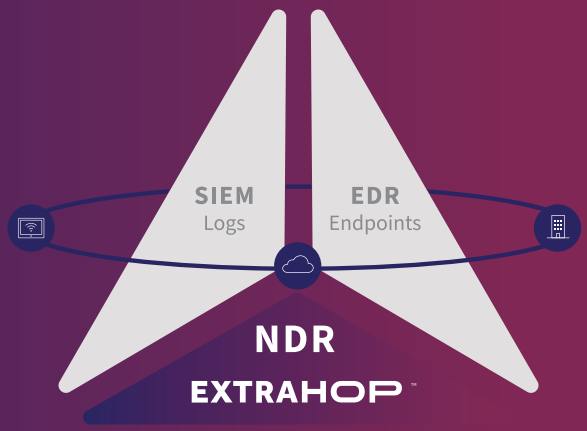
EXTRAHOP

EXTRAHOP NETWORK

網路偵測和回應 (NDR)

Reveal (X) 揭示未知並揭露攻擊



安全從業者長期以來一直在與可見性作鬥爭。 當入侵者透過加密流量橫向移動時，端點可以停用、關閉或完全避 開。 雲端和混合環境引入了不斷增長的攻擊面和外圍安全的額外盲點。

雖然許多組織依賴於像端點檢測與回應(EDR)和安全資訊與事件管理(SIEM)等解決方案，但這些工具存在限 制。EDR和SIEM缺乏所需的可視性和高保真數據，無法阻止已經進入您網絡內部的高級威脅。

信任始於真相。ExtraHop NDR 模組使安全分析人員能夠利用網絡作為資安真相和透明度的中心來源。ExtraHop Reveal(x) 平台提供他們所需的網絡可視性，以在雲端、混合和分散式環境中查看並阻止高級威脅。憑藉我們先進的 人工智能、行為分析和解密技術，安全分析人員可以比以前快 87% 的速度檢測、調查和解決威脅，其中包括幾乎 90% 的 MITRE ATT&CK 技術。

ExtraHop NDR 可透過 IDS 和網路取證模組進行增強，以提供更強大的真相來源，為即時威脅偵測和直覺的調查工 作流程，從而實現快速、自信的回應。

SEE MORE

在安全威脅成為內部問題之 前，提前識別。

在整個混合攻擊面上，從本地 部署到多雲端，再到分散的工 作人員和操作，獲得完整的情 況感知和 360 度的網絡威脅可 視性。

KNOW MORE

毫無疑問地知道入侵者將去向 以及他們曾經去過的地方。

透過雲端規模的機器學習、強大的回顧性取證以及無與倫比的解 密功能，深入了解過 去、現在和未來的威脅，透過 每一個網絡轉折點揭示資安真 相。

STOP MORE

以更快、更精確和更頻繁的速度 阻止網路攻擊者。

透過更智能的工具檢測、優先處 理和阻止更多惡意後維持行動， 這些工具消除了複雜性層次，縮 短了總體威脅應對時間並在每 個威脅檢測和解決過程中節省了 數小時。

FULL-SPECTRUM DETECTION

Hygiene

代表風險的活動:端口、協定加密合規性以及易受攻擊或不符合合規標準的服務

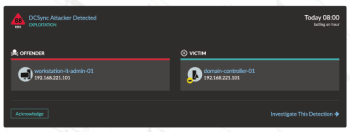
Known Attacks

過去攻擊中觀察到的IP 位址、網 域、檔案名稱、有效負載字串或協 定行為(包括情報來源)

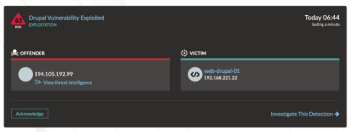
UnKnown Attacks

沒有先前已知的標識符，但表現出可與攻擊生命週期的一部分相關聯的異常行為的攻擊

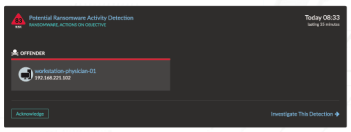
SPECTRUM OF DETECTION



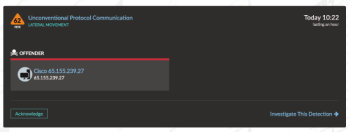
Rule-Based Detection



Robust Anomaly Detection



Sophisticated Behavioral Detection



Peer Group Detections

NIST MITRE | ATT&CK CIS Controls

NDR USE CASES

高級威脅檢測	漏洞評估	法證調查
自動化資產探索	容器防護	入侵檢測與回應
合規性與審計	威脅狩獵	解密與橫向移動可見性

COMPLETE NETWORK VISIBILITY
完整的網絡可視性

跨數據中心、雲端和校園環境的實時可視性，幫助您在單一用戶界面中更好地了解您組織的攻擊面。

ENTERPRISE GRADE PLATFORM
企業級平台

對世界上最大、最複雜的環境進行流量分析，支援 70 多種協定並與領先技術整合。

BROAD SPECTRUM DETECTION
廣泛範譜的檢測

檢測能力包括機器學習、IOCs 和基於規則的檢測，提供豐富的上下文信息，增加可解釋性並加速分類。

SIMPLIFY & STREAMLINE INVESTIGATIONS
精簡調查

Reveal(x) 提供經過精心策劃的即時威脅簡報，具有引導式的檢測和調查工作流程，使組織能夠對最關鍵的漏洞採取迅速行動。

HIGH-FIDELITY DETECTIONS
高保真檢測

Reveal(x) 雲端規模機器學習可擴展到數百萬個模型，從而產生最 複雜的偵測。

ADDRESS MULTIPLE USE CASES
應對多種使用情況

在一個工具中，為IT運維和安全運維團隊提供專用的工作流程，支 持雲遷移並保護雲工作負載，獲得寶貴的見解。

REVEAL(X) | FULL SPECTRUM DETECTION

ExtraHop Reveal(x)

揭示(X)功能

自動化庫存
Reveal(x) 透過自動發現和識別網路上通訊的所有內容，始終保持最新的資產清單。

自動化調查
Reveal(x) 通過上下文、風險評 分、攻擊背景和專家引導的下一 步，豐富了每一個檢測，以實現 自信的應對。

雲端規模機器學習
透過利用 5,000 多個 L2-L7 功能的雲 端規模機器學習和預測建 模，Reveal(x) 可以偵測對您的關鍵資 產的威脅，確定其優先順序並對其進 行背景分析。

完美的前向保密解密
Reveal(x) 可以 passively 並實 時解密具有 PFS 的 SSL/TLS 1.3，因此您可以檢測隱藏在加 密流量中的威脅。

對等組檢測
透過自動將設備分類為精確的對 等組，Reveal(x) 可以以最小的 誤報發現風險和攻擊行為。

自信的應對自動化
Reveal(x) 處理檢測和調查，同時與 CrowdStrike、Phantom、Palo Alto 等強大的整合，實現了增強和自動化 的應對工作流程。

REVEAL(X) | FULL SPECTRUM DETECTION

99% FASTER TROUBLE SHOOTING

83% FASTER THREAT DETECTION

87% FASTER THREAT RESOLUTION

適用於每個環境的 SaaS 和自我管理部署選項

Reveal(x) 平台有兩種部署模型:基於 SaaS 的 Reveal(x) 360 和具有自我管理感測器的 Reveal(x) Enterprise。 這兩種部署都提供了 NDR 的全部優勢，包括基於雲端的機器學習和威脅檢測能力。

EXTRAHOP

NetFOS 逸盈科技
詳情內容請洽代理商逸盈科技
台北 02 6636-8889　新竹 03 621-5128
台中 04 3606-8999　高雄 07 976-8909