NDR

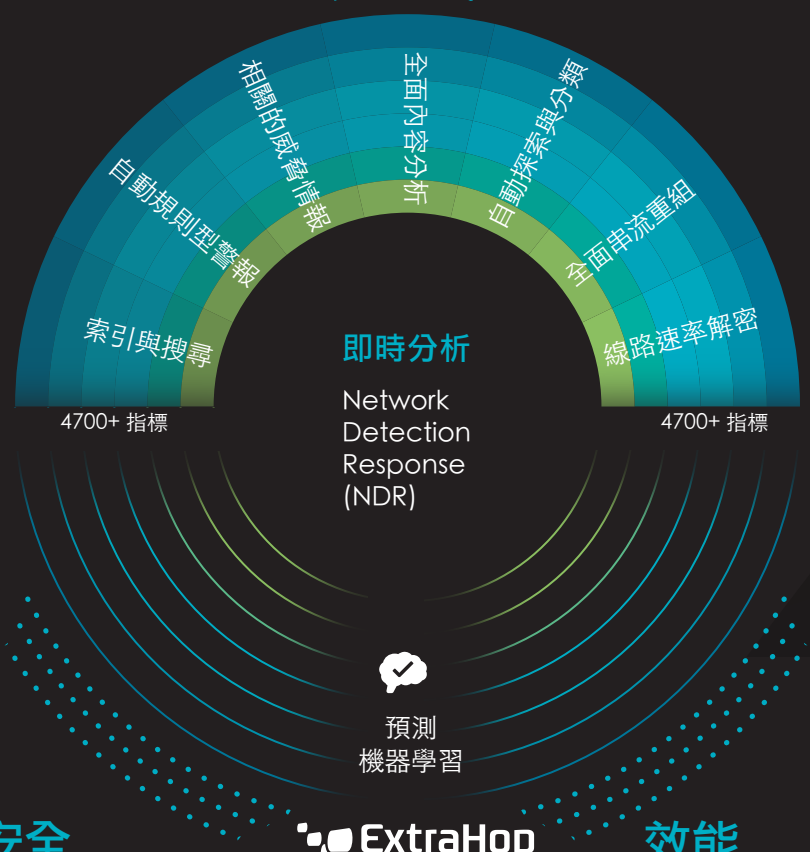
ExtraHop Reveal(X) NDR 平台

透過機器學習網路流量來分析關鍵資產

你知道嗎？平均入侵時間不到兩個小時即可從初始攻擊點轉向最終目標。過去，大部分的 IT 或安全團隊，可能需要等到有一些典型的跡象或症狀，例如 IT 基礎架構性能下降或資料外洩等事件發生才能意會已被入侵。通常等到安全團隊發現時，入侵者已經在你的環境中待了幾個月甚至更長的時間？

所以，當發現網絡攻擊時，安全運營中心（SOC）團隊有兩個緊迫的目標：迅速了解威脅，及採取行動予以補救。

ExtraHop 創造了一種全新方法，分析網路上發生的每一個數位交易，將之轉化為資安團隊，所需可付諸行動的情報，我們稱之為 Wire data，也就是即時分析的決定性來源。Extrahop Reveal(X) 通過利用有線數據解決安全程序中的差距，該數據包含應用程序事務中包含的所有信息。它可以自動發現，分類並優先處理網絡上的所有設備，客戶端和應用程序，並利用機器學習立即提供高保真的洞察力。



異常與攻擊鏈直接相關，突出了難以察覺的活動，包括：

- **內部偵察** 掃描開放端口和活動主機，暴力攻擊，嘗試登錄和異常訪問模式。
- **橫向移動** 從原始入口點重新定位，權限提升和勒索軟件傳播。
- **命令和控制** 網路中受感染主機與目標資產或外部主機之間的通信。
- **滲透行為** 直接或通過中途停留主機，從資產中進行大型文件傳輸，異常讀/寫模式以及異常應用程序和用戶活動。

根據 Gartner 2019 年的前7大安全和風險管理趨勢其中趨勢之一『新世代安全運營中心，重點是威脅檢測和響應』。

Gartner

安全

高傳真威脅偵測
衛生情況與遵循法規
關鍵資產探索
一鍵式威脅調查
透過SOAR的自動化回應

ExtraHop
Reveal(x)
網路安全分析平台

效能

即時應用程式分析
機器學習驅動的異常偵測
應用程式相依映射
端對端可視性與衛生情況
引導式調查

ExtraHop Reveal(x) 識別違反政策並滿足合規性要求

通用數據保護條例（GDPR）

- 通過檢測對個人信息的未授權訪問來增強數據處理標準。
- 儘早發現規避安全防禦措施的網路行為。
- 使用有關網路攻擊的豐富背景信息和證據，滿足72小時通知時間範圍。
- 持續監控所有雲/數據中心、用戶端及IoT設備中進行影響評估。

CIS關鍵安全控制

- 被動監視和分析所有網路流量，以識別授權和未授權的設備。
- 即時檢測主要範圍內資產中可疑的使用者，其未經授權的憑證和數據。
- 儘早發現勒索軟體中其他惡意軟體變種和隱藏的攻擊者行為。
- 在隱藏的 DNS、HTTP、HTTPS 及加密的流量中檢測網路攻擊者。

聯邦金融機構考試委員會（FFIEC）

- 優先考慮風險最高威脅並範圍內已遭到破壞的資產做關聯分析。
- 儘早發現勒索軟件，其他惡意軟體變種和隱藏的攻擊者行為。
- 即時檢測主要資產中可疑使用者，其未經授權的憑證和數據。
- 不間斷地檢測所有的雲/數據中心、用戶端及IoT設備的攻擊行為。

國防聯邦採購條例補充（DFARS）

- 通過監視所有的雲/數據中心、用戶端及IoT設備來基準系統行為。
- 檢測對管理員憑據的可疑使用行為和對管理協議的濫用。
- 通過行為演算法分析網路數據，以即時檢測威脅。
- 檢測網路攻擊並確定其威脅等級，向安全團隊觸發即時通知。

支付卡行業數據安全標準（PCI DSS）

- 即時利用已知/未知的安全性漏洞，也可檢測出SQL injection跡象。
- 識別設備和用戶帳戶訪問持卡人數據的可疑嘗試。
- 即時檢測受損的用戶憑據和共享訪問信息。
- 即使IP位址更改並且被多人使用，也可以隨時追蹤設備的活動。

醫療保健合規要求

- 可早期確定與勒索軟體、Zeus、Citadel等惡意軟體變種行為。
- 檢測已被受感染的醫療物聯網設備，對其他設備進行攻擊。
- 公開試圖竊取 PHI，PII 和信用卡信息的行為。
- 支援醫療保健合規性要求，包括PCI DSS，HIPAA 和 HITECH。

ExtraHop

NetFOS 逸盈科技

ExtraHop 代理商 逸盈科技
台北 02 6636-8889　新竹 03 621-5128
台中 04 3606-8999　高雄 07 862-8889
網站服務：www.netfos.com.tw

ExtraHop 產品方案諮詢專線 02-66368889#803 周小姐