VECTRA
SECURITY THAT THINKS®

Vectra NDR 人工智能驅動的網路檢測和響應

檢測、調查和響應網路中的攻擊

網路是企業基礎架構的基礎，需要高效的網路防禦策略。如果沒有優良的網路可視性和快速將大量數據進行前後安全比對的工具，外部攻擊者和惡意內部人員將保持優勢並讓您損失數百萬美元。

檢測未知，防範違規

Vectra Network Detection and Response (NDR) 是業界最先進的 AI 驅動的攻擊防禦，用於識別和阻止網路中的惡意策略，無額外干擾或需要解密。 Vectra NDR 利用 Security AI 驅動的 Attack Signal Intelligence™ 來確保清晰、準確和上下文的前期可視性，以消除整個可疑事件鏈中的未知因素和表面威脅、攻擊和惡意活動。借助 Vectra 您可以看到、了解並有效應對其他解決方案遺漏的威脅和攻擊，因此安全團隊可以花更少的時間進行調整、搜尋和調查，而將更多時間用於促進業務增長。

關鍵能力

- 網路可視性 - 查看、分析和存儲所有網路活動，並預先在不了解或檢測模式的情況下揭示隱藏的惡意行為。 自動跟踪攻擊者活動，包括特權憑據濫用、內部橫向移動、命令和控制以及跨網路與本地和雲端分佈式主機系統環境的遠程執行。

- AI 驅動的檢測利用安全 - AI 驅動的攻擊信號智能化 Vectra NDR 通過進階分析、深度學習、複雜行為分析和對攻擊者方法的洞察，來自動進行威脅檢測。從而像專家分析師一樣有效地從數十億個數據點中識別事件。 團隊可以查明網路上攻擊和惡意交易的威脅和源頭，包括重複或不對稱流量和封裝，以自動區分弱指標、規避和未知模式的真實性，並檢測 MITRE ATT&CK 中列出的多達 90% 的攻擊者策略技術。

- AI 驅動的分類 - 通過利用安全性 AI 驅動的攻擊信號情報優先級劃分採用 ML/AI 方法進一步分析主動檢測、每個事件的前後關聯、事件和分數之間的共性，以評估每個真實事件的緊迫性 在沒有任何人為參與的情況下進行陽性(true positive)檢測。 分析師能夠將更多時間花在緊急事件上，同時將需要審查的檢測池減少 80%。

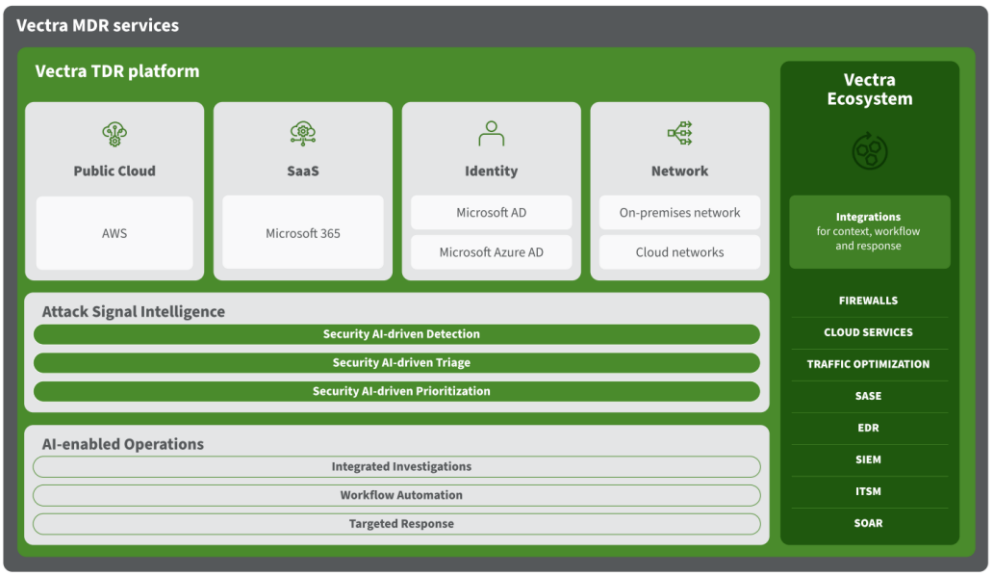
- AI 驅動的優先級利用安全性 - AI 驅動的攻擊信號情報 Vectra NDR 自動對最重要的威脅進行優先級排序，方法是在事件展開時對數以千計的事件進行評分和排名，達到近似經驗豐富的安全分析師的程度——將相關詳細信息以毫秒(而不是分鐘和小時)為單位放在您的眼前。

- 進階調查 - 不斷從持續變化的網路基礎設施中獲取知識，並提供您最需要的見解：
  - 查找異常的出站數據流，即使在加密通道中也是如此。
  - 跨主機實體關聯檢測，學習原型並識別每個對像並以各種方式呈現信息，讓您輕鬆查看關係、表徵意圖和了解業務影響。

- 內置響應操作 - 確保獲得專利的 MITRE D3FEND 對策進行強大的響應操作，用以包含、調查和補救受損系統。 您的團隊更加專注、更加高效和有效，因此可以減少分析師的倦怠和人員流動。

探索 Vectra 平台

Vectra 威脅檢測和響應 (TDR) 平台結合了跨公共雲、SaaS、身份和網路的完整攻擊面覆蓋範圍。利用 Security-AI 驅動的攻擊信號情報，獲得無與倫比的信號清晰度，讓您在防禦現代、規避進階網路攻擊者的同時掌控一切。



- 覆蓋攻擊面 - 消除攻擊面中 的未知威脅
  (cloud, SaaS, identity, networks.)
- 信號清晰度 - 利用攻擊信號情報來進行自動檢測、分類和優先處理未知威脅。
- 智能控制 - 武裝人類智能以搜尋、調查和應對未知威脅。

為什麼企業選擇 Vectra 進行 NDR

- 攻擊信號情報提供了豐富的信號，分析師可以使用這些信號來自動執行與威脅檢測、分類和優先級排序相關的任務。
- 確認您知道網路是否以及何時受到威脅，並確保您有能力管理最佳結果。
- 通過擴大覆蓋範圍、縮短調查時間並顯著降低平均響應時間 (MTTR) 來加快威脅檢測速度。
- 自動執行與第 1 層和第 2 層分析相關的手動任務，以減少總體安全操作工作量。
- 阻止正在進行的攻擊，讓安全分析師有更多時間主動搜尋和研究。
- 消除堆積如山的誤報以及相關的搜尋和調查任務，避免帶來更多風險。
- 在物理、虛擬或雲環境中隨您部署。
- 與雲網路、防火牆、XDR 安全和 SIEM/SOAR 無縫整合。

相關細節，請洽官網 ：www.vectra.ai.