企業網路資安保全

為了提升營運績效、達成業務目標，我們已用盡了全力，但駭客總潛藏在暗處伺機而動，培養專業資安人才並非易事，加上對安全基礎設施所需的專業化程度不斷提高，在企業資安設備與服務都需要不定期更新與維護的情況下，投入大筆預算培養資安人才對企業來說會是一筆龐大的支出與負擔，是否能用較有效率的方式，建立企業資安防護屏障？

欣盟企業網路資安保全服務，最大化您的資安預算效益

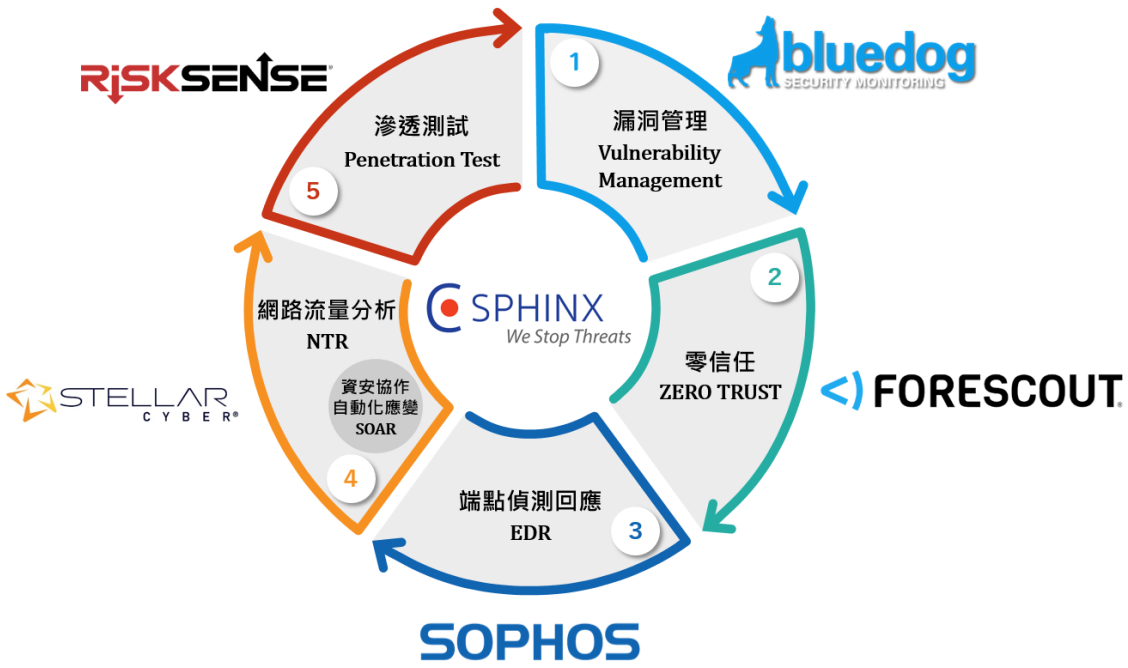
為您的網路進行資安監控，偵測駭客行為，透過蒐集的日誌資訊結合威脅獵捕系統中多種威脅偵測機制，以大數據分析、AI 機器學習提前發現威脅、持續追蹤，並協助您即時進行回應。

基本方案說明

說明	租賃 Stellar Sensor P300 乙台	
優勢	✓ AI 全年無休監控內外網威脅 *適用網路節點最大 500 Node ✓ 偵測威脅事件，並依嚴重等級進行分類 ✓ 提供資安遠端 / 到場協助服務 *適用所有訂閱服務範圍	✓ 系統 Log 紀錄保存 180 天 ✓ 5X8 小時資安分析師專屬服務，為您篩選、調查高風險事件 ✓ 高風險事件即時通報機制 ✓ 提供高風險事件詳細資訊與處理建議

網路資安保全服務可搭配多樣解決方案

進階的安全性 / 多面向的防護 / 更完善的資安架構



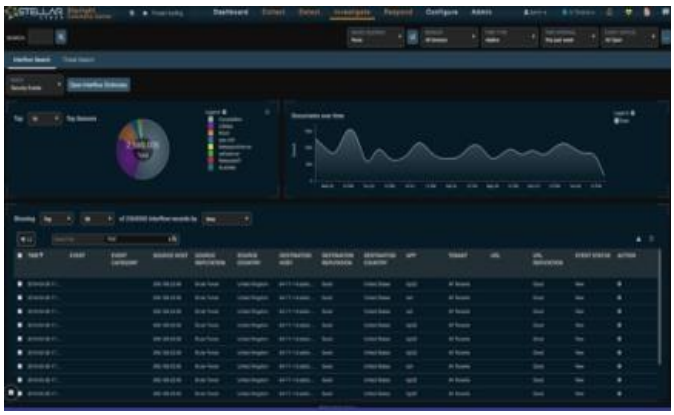
進階持續性威脅 (APT) 被發現前的潛伏時間都非常久，這類攻擊難以被發現，而攻擊手法的隱匿性及多樣化，為資安防護工作應對增加困難度。相較於傳統的事前預防，我們應更重視侵入過程的主動偵測，透過情資分析找出威脅趨勢，在駭客入侵前就發現其蹤跡，有效進行威脅早期預警、事件調查與回應。

廣泛蒐集資料來源

高度整合各項資安工具，串接各種情資來源，為您解決威脅來源過多，無法有效查找威脅的痛點，實現整體攻擊面的可見性。

偵測真實威脅

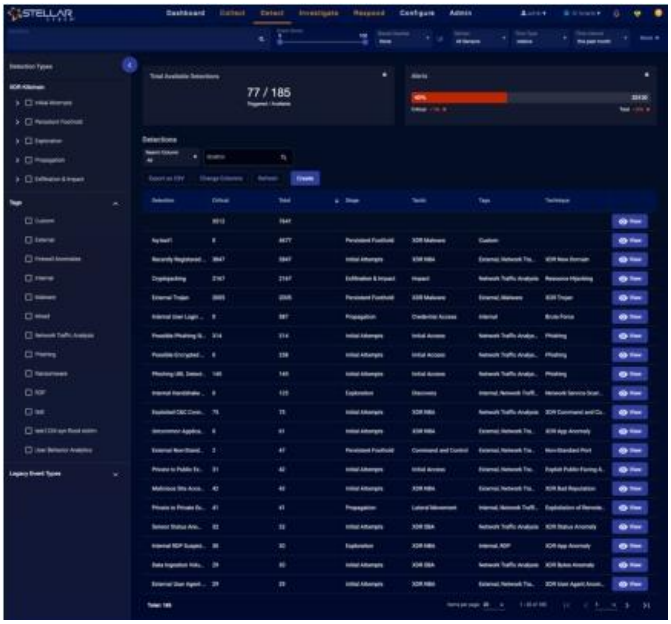
AI 大數據機器學習以使用者行為偵測、釣魚偵測、沙箱、網路封包等多樣方法偵測威脅，將威脅投射在 MITRE ATT&CK 攻擊鏈，為您找出隱藏在暗處伺機而動的真實威脅。



威脅調查分析

專屬資安分析師為您深入調查高風險事件，藉由可視化報表為您掌握威脅態勢，並提供您解決方案建議。

- **重大威脅事件即時通報**
- **每周提供「中高風險威脅報告」**
- **每月提供「資產風險報告」**
  - 資產威脅概況
  - 當月事件調查結果
  - 惡意 IP 清單



SPHINX We Stop Threats

欣盟企業網路資安保全

http://www.sphinxtec.com/
新竹縣竹北市嘉豐十一路一段 100 號 4 樓之 2 | 03-6682708 | CustomerCare@sphinxtec.com