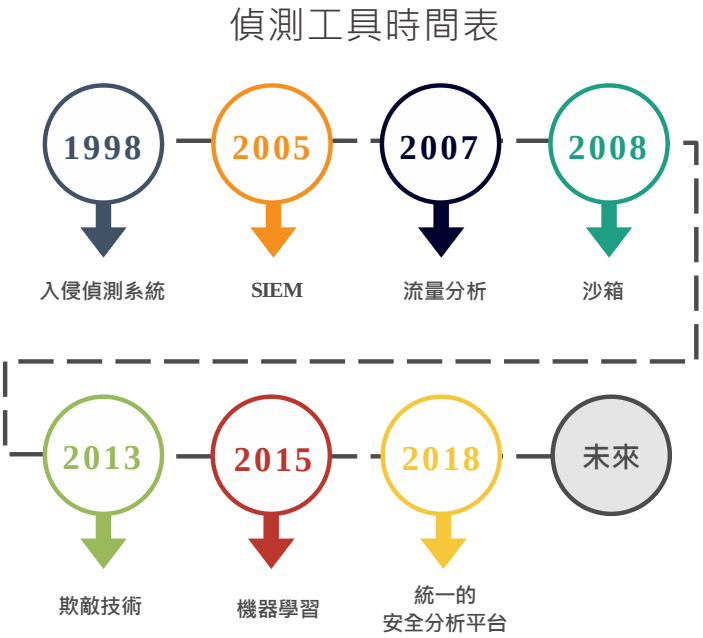
SOLUTION BRIEF

# 欣盟 提供您
# 新世代智能安全運營平台

跨雲、端點、網路、用戶、應用程式和 SaaS
將複雜的攻擊自動組合在一起




## 當今的網路安全挑戰

網路攻擊和漏洞激增，安全預算也隨之增長。到目前為止，有必要兼顧多家供應商提供的多種昂貴工具。然而並非單點解決方案就可以團結起來。它需要一個可擴展的，智能的中央平台，這個平台可提供正確的資料並具備自動響應威脅的能力。

## 為什麼現有方法失敗

那麼為什麼組織仍然遭到破壞？ 在 Stellar Cyber 中，我們認為這是因為存在盲點以及處於不同工具和警報噪音的複雜環境。現今的環境由公共、私有和混合雲中的實體、虛擬化、容器化工作負載組成，這些工作負載構成了巨大的覆蓋範圍挑戰，並且產生了無法處理的大量警報。在這種狀態下，安全團隊很難有效地應對威脅並在資料被盜或損壞之前確定關鍵威脅。因此您需要一個更好的預警偵測系統。

## 解決方案

Stellar Cyber 提供了唯一的新世代智能安全運營平台，這是第一個由開放式擴展偵測和響應（Open XDR）驅動的平台。 該平台通過機器學習結合了普適資料收集、大數據處理和人工智能的功能。

我們認為當今安全問題的解決方案是部署可以在所有環境中部署的單一技術，以提供普遍可見性。該技術應捕獲並關聯所有類型的資料，例如網路流量、日誌、伺服器命令、進程 、應用程式、用戶訊息、文件等。解決方案應該是完整的堆棧，且應該是開放的、可擴展的、可伸縮的、智能的，並提供自動化功能，以便安全人員可以更有效地進行操作。 最後，也是最重要的一點是，在 Stellar Cyber，我們認為網路安全解決方案應**將業界平均 200 天的偵測違規時間減少到幾分鐘**，同時降低資料洩露或任何其他損壞的風險。

Stellar 解決方案通過在網路、伺服器、容器、實體和虛擬主機上部署感測器和日誌轉發器來工作。感測器將原始資料轉換為 Interflow 記錄，並將其發送到集中式資料處理器和資料湖泊，該資料湖泊將對接收到的資料進行重複資料刪除、關聯、豐富、索引和儲存。接收到此資料後，它將在資料集上進行複雜分析，以識別真實違規事件。

該平台還具有緊密整合的安全功能，可在一個平台上共享資料，並具有內建分析功能，可利用機器學習消除警報干擾並提高偵測關鍵安全事件的準確性。 通過這種方法，組織可以通過使用大數據分析和人工智能來擴充安全運營團隊，從而提高人工效率。 該解決方案的使用案例在威脅調查、偵測和響應領域是無限的。

> “Open XDR 能夠消除盲點、減少偵測缺陷的時間、提高的人力資本效率。
>
> 通過**全面的資料收集、自動偵測以及調查和響應**，安全操作員的夢想得以實現。”
>
> *– Albert Li,*
> *Chief Scientist,*
> *Stellar Cyber*

## 收集正確的資料

Open XDR 平台的核心功能是資料收集和處理，而在 Stellar Cyber，我們認為首先解決資料問題是關鍵要點。 這是因為安全分析人員常在擁有太多資料，沒有足夠的資料或沒有資料關聯性的情況下苦苦掙扎。如果無法正確解決資料收集問題，則工具將遇到垃圾回收問題。Stellar Cyber 的資料收集技術稱為 Interflow。

Interflow 是 JSON 格式的資料記錄，可通過其他遙測進行標準化、縮小和豐富，以提供實際發生情況的關聯性。 Stellar Cyber 的感測器系列可捕獲網路應用程式資料、伺服器進程、命令和文件資料、威脅情報和地理位置資料。 收集後，這些資料將融合在一起形成一條記錄。

## 偵測真正的威脅

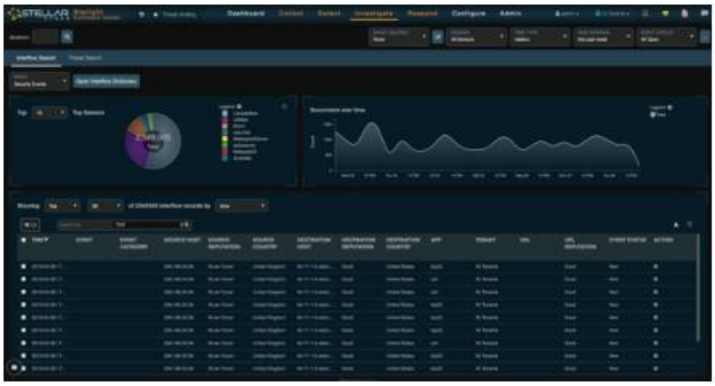
Stellar Cyber 的 Open XDR 支持定制的安全工作台，以使分析師獲得所需的工具。已知和未知行為的偵測超過 50,000 種，這些偵測被映射到網路安全狙殺鏈中，以作為預警偵測系統。與市場上其他解決方案不同，Starlight 由於其豐富的資料收集而具有完整的狙殺鏈偵測功能。

例如，在狙殺鏈交付階段的偵測需要一個惡意軟體沙箱，而在利用階段的偵測則需要 IOS 技術。

Stellar Cyber 提供了在整個狙殺鏈中進行偵測和響應的工具。該解決方案還將 IOS 等傳統技術與機器學習相結合，以提高真實度並降低誤報率。機器學習有效地創建了通常會經常觸發的簽名基線，並將其從高真實警報中消除了。

機器學習還可以偵測異常流量模式和伺服器行為。

## 調查問題



威脅搜尋已迅速成為網路安全運營中的一種流行策略，尋找未知與偵測未知一樣重要。 借助 Open XDR，組織可以通過動態創建簡單或複雜的查詢來搜索其豐富的資料集是否存在惡意活動。

就像有一個 Google 搜索引擎來處理您的資料。 例如，操作員可以調查執行—伺服器上的 Windows Powershell 命令是從具有預先存在的不良信譽公共 IP 地址啟動的。 另一個範例是運營商想要搜索特定用戶上載到網路上的伺服器的特定文件（MOS 雜湊）。

創建這些搜索查詢後，操作員可以保存它們並將其轉換為自定義可視化效果以備將來使用，並使其自動執行以生成警報和報告。

## 自動回應

對高真實度事件進行偵測和調查對於任何安全平台都是必不可少的，但是，如果該平台不具備採取行動的能力，則該平台將是不完整的。 Open XDR 具有內建的事件響應功能。 操作員可以通過其內建的案例管理系統創建故障單來響應事件，觸發電子郵件，Slack 和 API 警報，自動發送 PDF 報告並向防火牆發出信號以採取適當的措施。

除了這些內建的響應功能外，該平台還具有針對 SIEM 以及 SOAR（如 Demisto，Phantom Cyber，Swimlane 和 Siemplify）的業務流程組件。 SIEM 組件可以流式傳輸事件，而 SOAR 組件則可以使平台偵測自動觸發編排產品中的劇本，以執行各種指令，包括執行腳本或與相鄰工具整合。

## OPEN XDR 安全操作平台部署

該解決方案以軟體形式提供，可以安裝在您自己的實體或虛擬 x86 伺服器上，這些伺服器可以在 AWS、Azure 或 Google 等雲端供應商中使用，也可以作為預先安裝的硬體設備購買。

### 有多個組件可以創建整體解決方案：

- 網路感測器從乙太網路交換機收集網路流量。
- 伺服器感測器安裝在伺服器上的 Linux 和 Windows 上，以收集流量、命令、過程和文件資料。
- 容器感測器收集容器環境內部的流量。
- 欺敵感測器充當您環境中的蜜罐。
- 虛擬設備感測器可以部署在 KVM、VMWare 和 HyperV 環境中。
- 部署了資料處理器節點，並將其整合在一起，以創建可擴展的大數據平台以進行資料儲存和分析。


---

## 欣盟資安遠端監控服務 Sphinxtec, Managed Security Service Provide (MSSP)

欣盟的資安遠端監控服務結合 Open XDR 新世代智能安全運營平台與欣盟專業資安技術顧問團隊的知識經驗，提供使用者從資料收集、威脅獵捕、問題調查至自動回應的一系列流程，隨時因應駭客的威脅。

√ 透過資訊整合預防未知威脅
√ 依據使用者環境釐清威脅來源
√ 提供每月定期資安報表並分類威脅等級
√ 協助解決目前的威脅
√ 協助未來資安規劃
√ 突發重大災難時緊急到場支援

欣盟提供的資安遠端監控服務讓您不必花費鉅額成本培養資安專家，欣盟的專業團隊即是您最強力的後援。

---

## 關於欣盟科技有限公司

欣盟科技 (SphinxTec Co,. Ltd.) 以專業的技術服務為基礎，遵循資訊安全的規範，整合異質平台中央控管觀念為技術核心，代理銷售不同領域之領導品牌，產品範疇適用於網路和端點與資料中心之非結構化資料存取與稽核管理。
企業面對來自端末、網路、檔案中心之資料洩漏等持續增加的各式威脅，欣盟科技提供資安技術顧問服務可客製化企業需求去分析找出關鍵核心，提供適切的資安策略，配合使用實際的可行性分析，導入適合的企業資安解決方案。