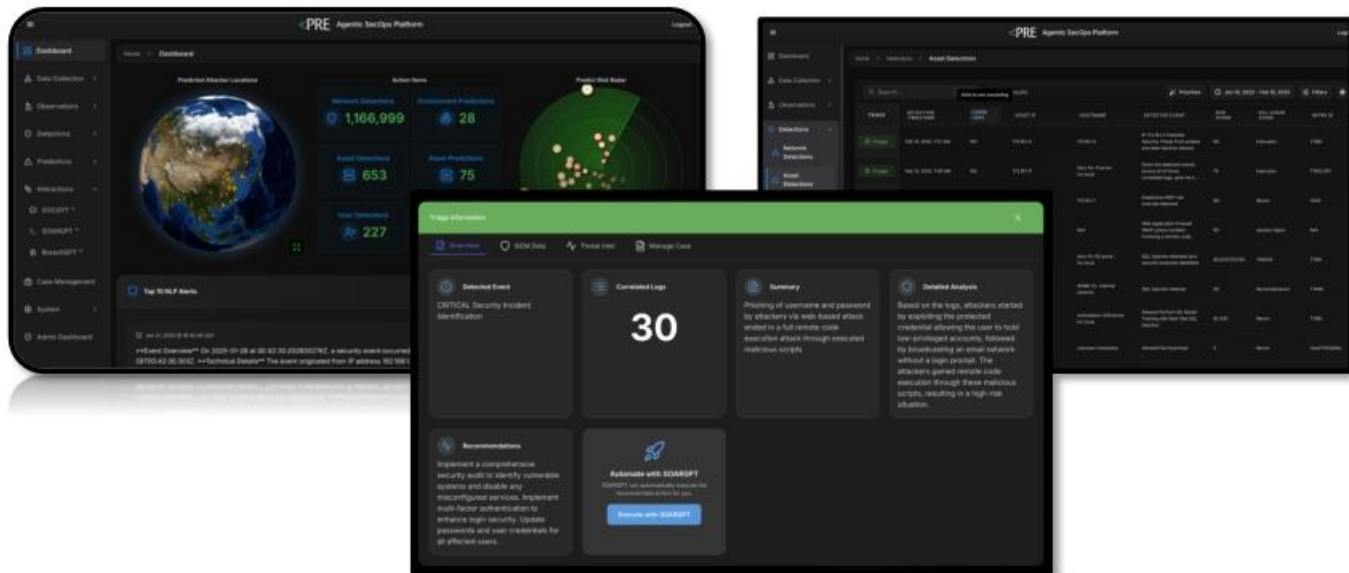


AI 原生 SecOps，實現預測性和主動式資安

PRE Security 推出 AI 原生 SecOps 解決方案，運用預測式、生成式與代理型 AI 技術，徹底革新現代資安運作模式。PRE 提供完整的資安作業流程能力，解決傳統「手動建構」架構中長期存在的各種問題——從整合各種資料來源、跨環境關聯分析，到提供進階的生成式偵測與預測，並自動化回應與預防措施。透過專為資安打造的大型語言模型，PRE Security 能加速並強化整體數位基礎架構中的威脅偵測、事件回應與防禦行動。透過 PRE Security，您的 SecOps 將從被動應對轉變為主動預防，進而增強您對不斷變化威脅情勢的防禦能力。



立即使用 PRE Security 強化或替換您現有的 SIEM 或 XDR！

傳統的 SIEM 和 XDR SecOps 架構需要持續更新規則、手動調整和維護，才能跟上新興威脅的步伐。即使定期更新，這些系統本質上仍屬靜態的，故往往會錯過新的攻擊模式，或無法及時應對快速發展的威脅，尤其是結合 AI 驅動的攻擊者。

PRE Security 的 AI 原生平台透過持續從與環境的每一次互動中學習，隨著威脅態勢不斷演進，徹底解決了這項問題。系統能動態理解貴組織獨有的漏洞、風險與威脅模式，確保偵測與回應能力隨時間推移不斷提升——而無需每個階段進行手動設計或輸入。

< **為何這很重要：**透過 PRE Security 專為資安打造、可持續學習的 AI，您的資安運作將變得更加智能化——無需頻繁人工更新或調整規則，就能領先下一波攻擊手法。

WHAT IF YOU COULD PREDICT
BAD ACTORS AND INCIDENTS
BEFORE THEY CAUSE HARM?



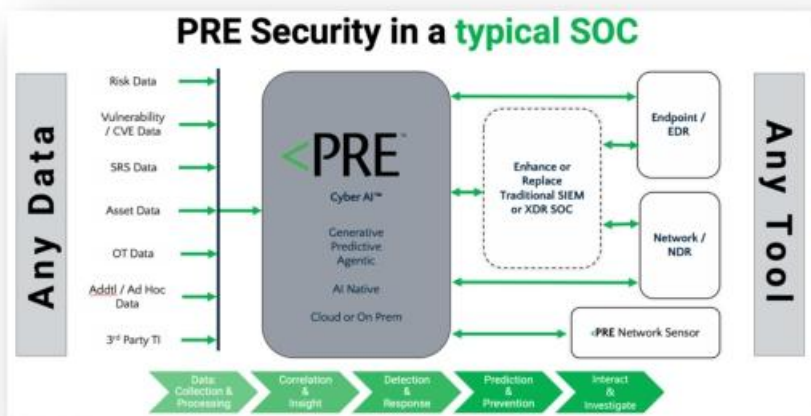
來自 Open XDR 的發明者

為什麼選擇 PRE Security ?

傳統以 SIEM 為基礎的 SecOps 架構，已無法應付現今複雜、多變且不斷演進的威脅。這些過時的解決方案範圍有限、本質被動，還常導致回應延遲和威脅漏報。此外，它們多採用昂貴的「依資料匯入量計費」模式，為了控制成本，反而限制了可提供情境脈絡的關鍵資料匯入。

PRE Security 以 AI 原生架構重新定義 SecOps，旨在解決真正的 SecOps 挑戰：

- < **生成式 AI (Generative AI)**：創意、動態的關聯分析、意外性偵測、無解析器™資料匯入等功能。
- < **預測式 AI (Predictive AI)**：既然可以「預測並防範™」，何必等到被入侵後才進行「偵測與回應」？
- < **代理式 AI (Agentic AI)**：自動化、具邏輯推理的行動、回應與自動化作業。



多種使用案例：

< 替換 SIEM

使用 PRE Security 全新 AI 原生 Secops 升級您的舊基礎架構。

< 強化 SIEM

預先處理日誌，降低 SIEM 匯入需求，提升資料標準化品質。

< 生成式 XDR 與預測分析

將 XDR 升級為生成式偵測，並導入 PRE 的預測分析功能。

使用案例

替換舊版 SIEM 解決方案

情境：某家全球企業由於營運挑戰，希望透過 AI 原生解決方案提升資安能力，進而汰換現有的 Splunk 或 QRadar 部署。

- 挑戰：確保在多樣、複雜的網路環境與以傳統架構建立的資料孤島中，實現一致的安全監控與事件回應。
- 解決方案：PRE Security 的無解析器通用資料收集器可完美整合，從任何來源匯入資料，實現具完整情境脈絡的關聯分析與威脅偵測。
- 透過 AI 原生技術，可以為長期存在的 SecOps 挑戰提供獨特的解決方案，並啟用新型應用，包括預測式分析、以自然語言為基礎的互動，以及創新回應與防禦能力。

強化傳統以 SIEM 為核心的 SOC

情境：某大型政府機構無法移除現有的 SIEM 系統，但須面對「依資料匯入量計費」所帶來的成本壓力。

- 挑戰：傳統 SIEM 架構因定價與儲存方案的限制，限制了資料匯入量。當資料匯入受限時，也會導致情境脈絡不足，讓使用者在實際預算與管理挑戰的制約中陷入兩難。
- 解決方案：PRE Security 可部署於現有 SIEM 之前，先行進行資料預處理與分析，只將與安全偵測相關的關鍵日誌儲存至 SIEM，藉此大幅降低成本與複雜性，同時維持合規性與既有作業流程。
- 另一個強化方式是部署在現有 SIEM 之上，將偵測結果取出後，把產生的偵測結果和預測結果回傳給 SIEM。

生成式 XDR 與預測分析

情境：某全球 MSSP 使用現有的 XDR 解決方案時，仍面臨過多誤報與偵測效能不足的問題。

- 挑戰：攻擊者同樣利用 AI 快速演化攻擊策略與手法，使傳統依賴預設規則的偵測方式難以偵測威脅。
- 解決方案：PRE Security 的生成式 XDR 由我們的 CyberLLM™ 驅動，透過訓練 MITRE ATT&CK、CVE 及其他資安框架與資料來源進行偵測，但不受限於既定的偵測規則，能透過多維度關聯分析持續學習與調整。
- 將預測分析導入 SecOps，可實現全新的主動式防禦方法，有助於在造成損害之前堵住漏洞，達成預防與先制防禦。

主要特色與效益摘要：

特色	效益
匯入任何資料 - 通用資料匯入機制，可從任何來源擷取資料。 - 正在申請專利的「無解析器 (Parserless)」技術。 - 支援無限制的資料格式與資料儲存系統。 - 可透過 PDF、Excel、Word 等文件上傳額外的環境脈絡資訊。 - 將日誌儲存成本與分析成本分離。 - 採固定資產定價模式。	- 提供所有數位基礎架構的全面可視性。 - 無需客製解析器或複雜的整合，縮短導入時間並降低營運負擔。 - 協助 SOC 團隊快速分析關鍵資料，提升回應品質與速度。 - 降低維護客製解析器與整合模組的成本與複雜度。 - 能快速導入新的資料來源。 - 採非匯入量計費的方式可有效降低成本，並可用低成本方式儲存日誌。
全方位關聯分析 - 跨任何資料來源自動關聯資料。 - 資料豐富的多維告警。 - 可上傳組織特有內容作為額外情境脈絡。 - 可輕鬆加入額外的威脅情報來源與資安相關資訊。	- 提供具完整情境脈絡的多維度告警，整合來自各種來源的資料。 - 讓 SOC 團隊能專注於最關鍵的威脅，而非被無關的告警與誤報淹沒。 - 透過篩除低優先等級事件，降低警報疲勞，聚焦於最高風險的威脅。 - 為資安分析師提供所需的洞察，加速決策並提升判斷品質。
以自然語言互動與調查 - 讓 SOC 團隊能透過 SOCGPT™支援的自然語言查詢與安全資料互動。 - 提供即時、具完整情境脈絡的調查回應。 - 透過 AI 快速辨識難以發現的異常活動與行為模式。	- 分析師可透過簡單提問即刻取得複雜洞察，縮短調查時間。 - 提升對資安經驗較少的分析師的可操作性，無需熟悉傳統查詢語言或複雜日誌。 - 提供每次查詢結果的關鍵情境脈絡，強化決策能力。 - 分析師無需切換工具或介面即可立即採取行動，簡化整體事件回應流程。 - 提升整體效率，讓 SOC 團隊能在更短的時間內識別與處理嚴重事件。
生成式 XDR 偵測 - PRE Security 專為資安打造的 CyberLLM™可動態偵測已知及新興威脅。 - 自適應威脅偵測，可隨新的攻擊手法持續演進。	- 威脅資料持續適應與演進，即時偵測新型威脅。 - 不再依賴靜態規則與特徵碼。 - 大幅提升偵測準確性並降低誤報率。 - 加快平均偵測時間 (MTTD) 與平均回應時間 (MTTR)，縮短暴露時間。
預測分析 - 專屬的「Predict & Prevent™」功能，可分析歷史與即時資料，在威脅與漏洞被利用前進行預測。 - 主動降低風險，改善安全態勢。 - 透明、一致的預測。	- 讓組織能採取主動行動，而非被動應對。 - 透過預測特定攻擊模式，降低零時差漏洞的暴露風險。 - 根據威脅發生的可能性，幫助確定優先順序。 - 讓組織能夠提前部署緩解措施，降低入侵風險。 - 在攻擊者攻擊前識別並解決漏洞，降低整體攻擊面。
規範化回應與防護行動 - 自動化工作流程提供即時、規範化的威脅回應指引。 - 整合 AI 自動化，有效緩解威脅。 - 可透過 Prompt 與自動化執行回應行動。	- 透過自動化回應最小化損失（例如：偵測到入侵即隔離受感染系統，防止網內橫向移動）。 - 透過減少事件回應中手動流程時間，大幅縮短回應時間。 - 透過自動化重複性任務，減輕 SOC 團隊的營運負擔。 - 確保對事件做出更一致、可靠的回應。

客戶成功案例

「自從導入 PRE Security 平台以來，我們的 SOC 團隊回應時間縮短了 45%，在威脅對網路造成影響前的偵測能力提升到了 60%。預測威脅的能力讓我們能主動加強防禦，降低整體風險態勢。」

< 全球金融機構 CISO

彈性部署選項 / 可預測的固定定價模式

PRE Security 可依您的營運需求，靈活部署於各種環境：

- < 雲端 (SaaS)：完全在雲端託管，簡化部署並實現可擴展性。
- < 本機部署 (On-Premises)：將虛擬設備安裝在您的硬體伺服器上，實現完整內部控制。
- < 混合部署 (Hybrid)：結合您現有的雲端服務供應商（如 AWS 或 Azure）或與本機部署相結合。

與業界普遍依匯入量或變動計費不同，PRE Security 提供以 IP 數量為基礎的固定合約定價。

- < 入門方案：最多支援一萬個資產。
- < 以一萬到十萬個資產為增量區間的額外資產：以 IP 數量為區間劃分，簡化資產計算方式。

軟體功能特色：

- 無解析器 (Parserless™) 資料匯入
- 通用資料收集器 / 匯出器（專利 Log2NLP™與 NLP2Log™流程）
- SearchGPT™以自然語言與資料互動
- 數據編織 (Data Fabric) 過濾、標準化與豐富化
- 多維度生成式資料關聯分析
- 生成式 XDR，由 CyberLLM 驅動的情境化自然語言告警
- 使用自動分類代理操作進行風險和優先評估
- 預測分析
- 自然語言威脅獵捕 (SOCGPT™)
- 網路與異常偵測（次世代 SIEM / XDR）
- 威脅情報，包括預測情報
- 代理型 AI 自動化與 SOARGPT™
- 內建 BreachGPT™的入侵和攻擊模擬器
- 以及更多功能

技術規格

*最低配置為 1 個 GPU，最高配置為 4 個 80GB GPU。建議使用搭載 NVIDIA 驅動程式的 Nvidia A100，亦支援 AMD、Intel 及 Apple GPU。

組件	vCPUs	RAM	Storage	GPU
Cyber LLM™ 伺服器虛擬設備	24+	128GB+	200GB+	40GB nVidia (16GB+ VRAM)*
預測伺服器虛擬設備	8	64GB	200GB	
網路感測器虛擬設備	8	1GB	100GB	

關於代理商 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，我們以守護客戶的資訊為首要考量，代理銷售不同領域之領導品牌，協助客戶在駭客攻防之中提早預防取得先機，且以欺敵技術降低駭客攻擊突破率，打造堅韌的資安防護網。欣盟科技亦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。