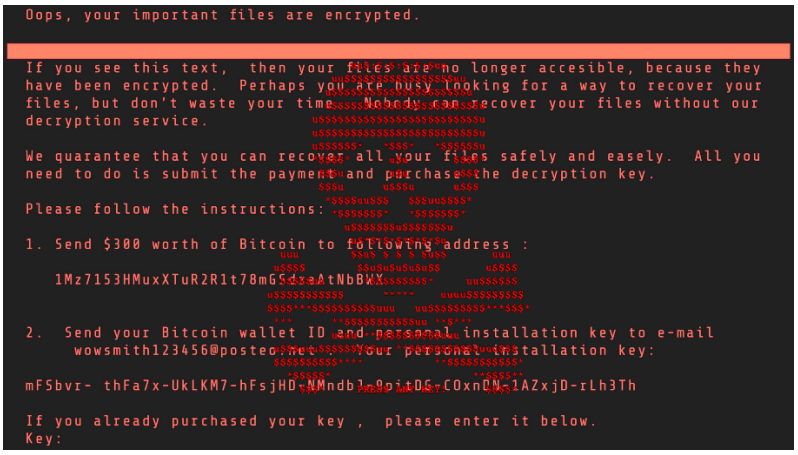
Smart X / OT 安全驗測服務及解決方案

隨著物聯網（IoT）導入工業製造與自動控制環境，工控物聯網（IIoT）時代來臨，公司營運資訊與工業控制系統（ICS）透過網路結合，得以將製造系統以傳統技術無法達到的整合性進行自動化、最佳化，大幅提高產能；甚至進一步與大數據及統計分析結合，利用資料的特性提出策略性改善，即近年極夯的話題：工業 4.0。

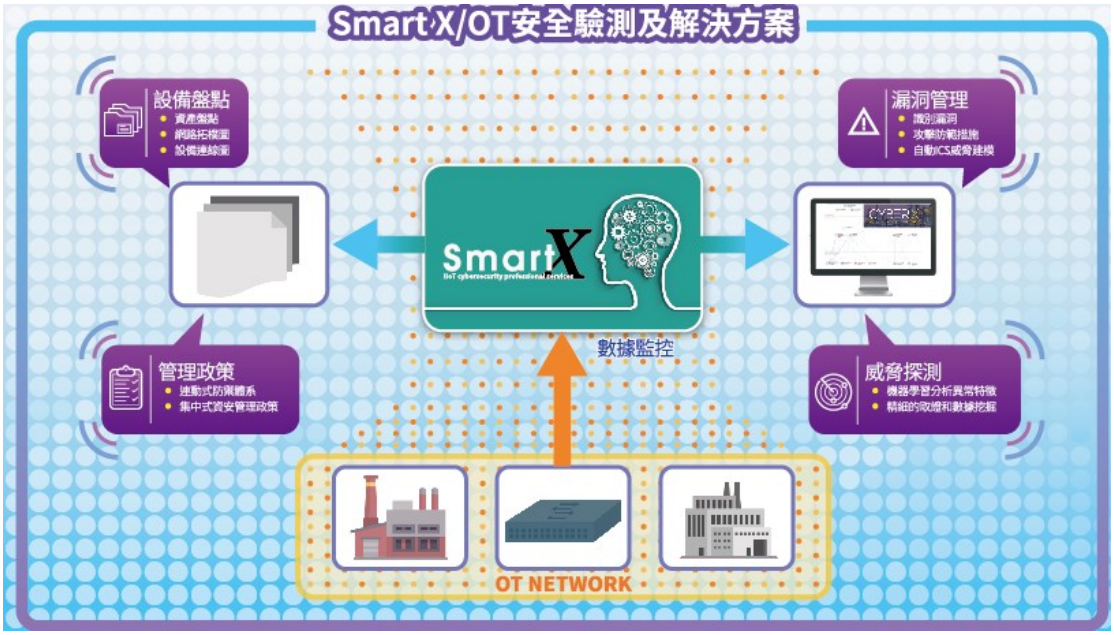


工控物聯網能讓工廠產能及運作效率大幅提升，同時，駭客的攻擊管道與危害程度卻也隨之增加：在部署的連網設備及感測裝置達到數百甚至上千的數量時，包括資料蒐集及傳感器監控系統（SCADA）、人機處理介面（HMI）、可程式化邏輯控制處理器（PLC）…等等 OT（Operation Technology）環境，大量原來在封閉且隔離 OT 環境的控制設備，也因連結網路而暴露在資安風險的危害中。而根據近年案例，工控物聯網的資安事件一旦發生，損害的程度遠遠超越過去純 IT 的時代。



華電聯網提供**針對 OT 的安全解決方案**，採用 CyberX、Nozomi 等實戰型工控網路安全方案，針對 OT 環境特有的網路脈絡規劃準確的安全防禦計畫，專業

顧問提供客製化檢測及顧問分析服務，協助企業快速建立製造環境的安全領域。



Smart X IIoT 資安解決方案五大面向

1. 資產及資安可視化風險分析：

幫助企業深入了解 IT/OT 資產狀態及網路拓樸，準確控管工控環境的安全漏洞及外洩途徑，同時專業顧問提供現有工業網路的配置建議，改善公司整體安全防禦效率。

2. 情資體系：

連線全球的安全情資，快速更新 OT 環境惡意軟體、駭客活動紀錄和攻擊手法，透過大數據精確判斷並即時識別環境中的失當行為及潛在威脅。

3. 預判攻擊路徑：

以情資餵養的機器學習系統可預判未來駭客入侵可能的管道，先期設定客製化安全政策，構築威脅模型並建立事件回應，以精細的取證步驟與挖掘工具保留證據。

4. 整合防禦系統：

整合邊際設備，將既有的網路防火牆、監控分析、雲端服務在內的防禦體系一併規劃，制定統一且高效率的 IT/OT 資安政策，提升防禦反應速度。

5. 非侵入式部署：客戶無須改變架構，以旁路側錄方式，進行深層分析，快速識別可疑資安風險。

Smart X 服務的內涵跨越 IT 與 OT 界限，以 ISO27000 國際資安管理標準及 IEC 62443 作為服務框架參考，以 PDCA 及 OODA 的持續改善的管理循環，逐步提高 IT/OT 資安成熟度，可提供企業全面識別及管理智慧製造、智慧城市及關鍵基礎設施風險，確保達成企業營運目標。