工控資訊安全顧問服務

ICS Cybersecurity Consultancy Service

技術領域

1. # Cybersecurity

解決問題

- 隨著工業生產的自動化與資訊網路化，大幅提升了生產效率，卻也增加潛在的資訊安全危機。有鑑於工業資訊安全事件頻傳，各國多已加強要求生產業者之資訊安全規範與認證**(**從設備元件、生產程序系統及整合解決方案**)**。我國工業控制設備製造業多以外銷為主要市場，如未能符合全球廠區 **OT (Operational Technology)**資訊安全之要求，可能被排除在供應鏈之外
- 一般資訊安全專家較少以 **OT** 觀點來訓練人員之資訊安全意識。即使有了資訊安全認知，多數工業生產業者也難以找到國內資訊安全專家進行整體資訊安全風險評估

主要功能

本方案提供業者建立資訊安全能力與相關輔導服務，可協助業者符合國際資訊安全認驗證要求，並維護製程可用性**(Availability)**。主要功能說明如下：

- 工控資訊安全認知與防護訓練：
  - 基礎訓練：工業資訊安全威脅趨勢、工業控制網路架構與攻擊面向、工業伺服器主機與控制設備之資訊安全防護介紹、工控網路入侵資訊安全偵防介紹
  - 進階防護：工控系統**(ICS)**網路協定介紹、工控協定操控模擬演練、封包分析與鑑識工具、建立初階 **ICS** 入侵偵測之工具**(Snort)**、**SCADA** 設備與網路弱點檢測，以上各項課程含實機操作
  - 專業攻防：實體工控 **Test Bed** 與模擬虛擬環境操控演練、**SCADA HMI/PLC** 設備滲透測試與遠端攻擊、**SCADA Malware** 分析、工控系統網路攻擊**(**偵察、命令注入、偽冒回應、**DoS** 、複合**)**、**ICS** 入侵偵測規則分析與撰寫、實體 **Test Bed** 紅藍軍攻防對抗演練
  - 工業 **IEC 62443** 國際資訊安全標準：**IEC 62443** 概述、**IEC 62443-4-1**、**IEC 62443-4-1** 與軟體專案之匹配連結、**IEC 62443-4-2** 、**62443 3-1/3-2/3-3**、**IEC 62443-2-4**
- 資訊安全風險評估建立資訊安全發展流程管理制度之顧問輔導：
  - 執行現況差異分析、輔導 **OT** 資產盤點、輔導 **OT** 風險評鑑及安控處理、制定 **OT** 管理制度規範、內部稽核顧問服務
  - 嵌入式設備網路安全保證**(EDSA)**/元件設備網路安全保證**(CSA)**、系統網路安全保證**(SSA)**、網路安全開發生命週期保證**(SDLA)**等認驗證導入顧問服務
- 資訊安全防護解決方案：
  - 深度封包分析，從 **OSI** 網路標準第二層到第七層進行全方位深度封包分析
  - 標準協定分析能力，可分析超過 **11** 種工業 **(**如 **Modbus/TCP, OPC/UA, ...)** ，以及超過

38 種網際網路服務協定 **(**如 **HTTP, FTP, SSH, Telnet, SSH, Telnet…)**。可偵測涵蓋偵查、命令注入、偽冒回應、中間人、及癱瘓服務等各式 **ICS** 攻擊

- **IEC 62443-4-2** 嵌入式設備網路安全保證**(EDSA)**/元件設備網路安全保證**(CSA)** 驗測實驗室

具體效益

- 以工業 **OT** 領域為出發點，搭配 **OT Test Bed** 進行各項資訊安全攻防實作演訓，提供不同程度的資訊安全訓練課程，包括：產業技術訓練、**OT/IT** 資訊安全整合技術、**OT** 資訊安全認知訓練、工控資訊安全基礎訓練、工控資訊安全進階防護訓練、工控 **OT** 資訊安全專業攻防訓練
- 以工業生產系統風險安全評估為基礎，加入資訊安全因子風險評估因素，重新評估關鍵風險衝擊性，輔導建立因應緩解措施；此外根據業者不同需求，提供 **ISO27001** 的資訊安全概念強化、**ISO27001** 取得驗證、**IEC62443** 為漸進式導入、與通過 **IEC 62443** 的認驗證等不同程度之資訊安全發展流程制度建立之顧問輔導
- 提供工業控制網路之多層次入侵偵測設備**(ICTD)**：
  - 具備非侵入性安裝，透過 **Switch** 同步側錄網路封包進行威脅偵測分析，不影響工業生產運作
  - 免疫式行為基準之異常偵測，自動學習建立工業生產各設備間之正常操控與網路通訊行為動作基準，可偵測未來未知之不應存在之額外命令動作或網路擴散等各式攻擊行為。為一符合國際潮流之 **ICS** 資訊安全解決方案

▲圖說：顧問輔導流程方法

相關連結

影片

- **Industrial Cyber Threat Detector (ICTD)**：**https://youtu.be/5nfufZwuvsw**
- **ICSMID-A multi-level deep intrusion detection system for industry control system (OT) network**：**https://youtu.be/meBm_vGjtf4**