



Built Secure. Stays Secure.

台達產品資安服務與解決方案型錄



DAA – 台達應用程式允許清單方案

Delta Application Allowlisting Solution

Delta Application Allowlisting (DAA) 是一款專為關鍵資產與 OT 場域打造的端點防護解決方案，結合多層次防護、行為學習與不中斷更新能力，實現動態信任管理，有效防止勒索病毒、惡意程式與橫向移動攻擊，在不中斷營運的前提下守護設備與工業現場的安全。



聯絡我們

www.deltaww.com

security.sales@deltaww.com



精準信任管理

僅允許受信任的程式執行，阻擋未知或偽裝合法的惡意行為

- 只允許受信任之應用程式執行
- 僅允許通過簽章、Hash 或預授權名單驗證的應用程式
- 阻擋未授權、無簽章或偽裝合法程序的惡意軟體
- 防止 Fileless 無檔案攻擊、DLL 注入與橫向移動行為



專利智慧更新機制

支援寬容模式與預授權更新，防護不中斷、作業不中斷

- 不中斷營運的自動更新設計
- 支援寬容模式與信任更新者名單
- 自動辨識合法應用更新流程，無須停機
- 確保防護不中斷、作業不中斷



老舊與封閉設備支援

支援 XP、7、IoT 與無防毒設備，降低系統重構成本

- 支援 Windows XP / 7 / 10 / 11 / IoT 與 Server 各版本
- 無須升級硬體也能部署防護策略
- 強化無法裝防毒軟體的設備安全性

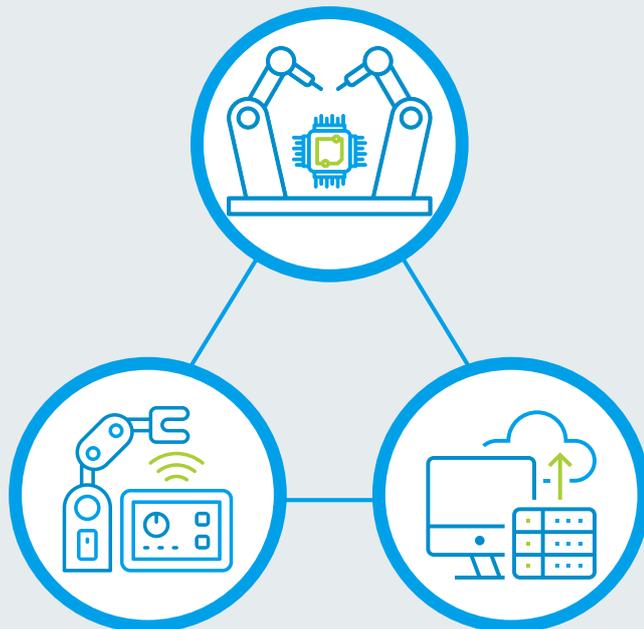
為 OT 系統打造不中斷營運的安全防護

智慧工廠產線中
無法升級的機台

封閉場域 (Air Gap) 環境
需主動防護

需通過 OT 資安稽核的
公共設施或電力單位

運作 24/7、不容許
重開機維護的設備群



建立裝置行為輪廓 主動預警異常

建立行為模型，自動判別突兀操作與系統呼叫異常

- 長期學習建立行為基準模型
- 偵測命令列濫用、系統呼叫異常與參數突變
- 提供即時告警與事件追蹤



集中可視化管理平台

多站點管理、離線支援、視覺化儀表板與稽核日誌

- 支援離線部署與合規稽核
- 支援 Air Gap 與場域化部署
- 提供視覺化儀表板、版本控管與事件日誌



稽核與合規支持

對應國際產品資安法規與標準合規需求

- 歐盟網路韌性法案 (EU CRA)
- 半導體設備資安標準 (SEMI E187)
- 工業控制系統安全 (IEC 62443)

多層式鎖定防護架構



程序鎖定

只允許授權的程式運行，任何未授權程式嘗試啟動，立即攔截並回報



資料鎖定

防止駭客竊取、竄改配方、機器參數或控管資料，也防止載入不明資料



組態鎖定

即使 USB 已感染，也無法篡改控制邏輯檔，更無法植入惡意指令或後門



USB 鎖定

不允許任何未授權 USB 存取 PLC 端、工程站、HMI，阻斷初始感染點

最低系統規格要求

支援列表

Windows

Windows XP , Windows 7 , Windows 10 , Windows 10 IoT , Windows 11

Windows Server

Windows Server 2012 , Windows Server 2016 , Windows Server 2019 , Windows Server 2022

最低效能須求



處理器
1 GHz or Faster



記憶體
4 GB or Greater



儲存空間
200 MB Available

DAFA – 台達自動化軟體韌體分析方案

Delta Automated Software and Firmware Analysis Solution

為軟體、韌體安全打造的全生命週期合規平台

DAFA 是一套結合韌體組件解析、SBOM 管理、自動漏洞監控與合規追蹤的全方位平台，協助產品在開發階段掌握供應鏈風險，實現開源授權合規與產品資安治理。



聯絡我們

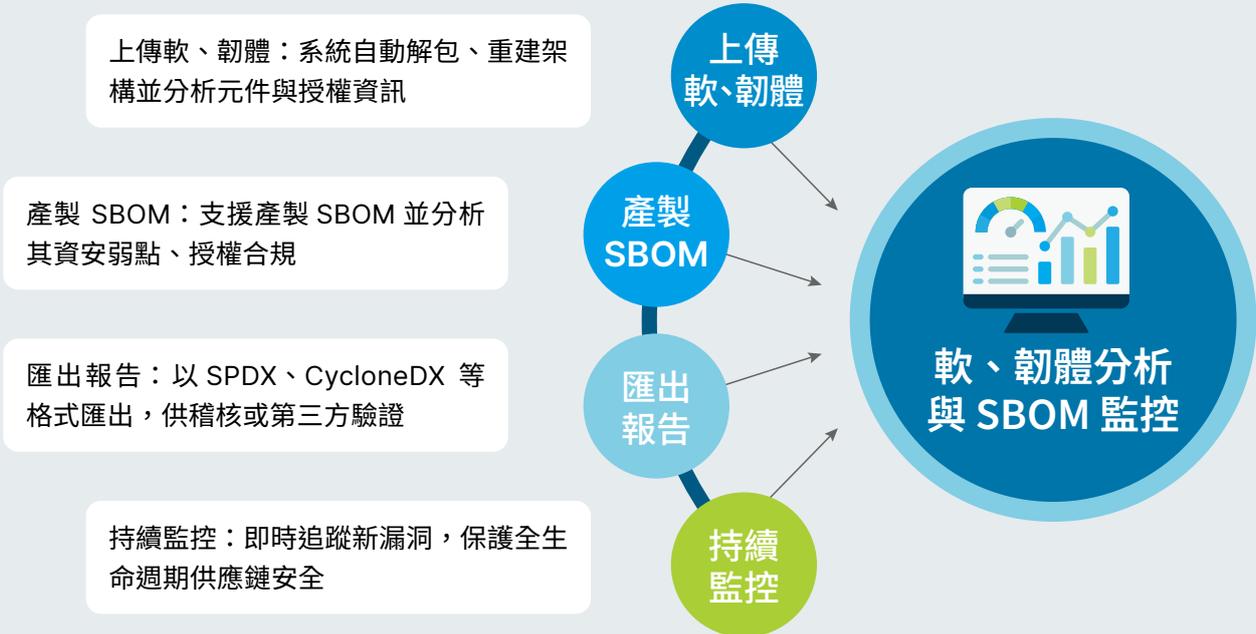
www.deltaww.com

security.sales@deltaww.com

適用於產品製造商的完整 SBOM 解決方案



四步驟完成軟、韌體分析與 SBOM 監控



SBOM 自動建構與分析

無原始碼？沒問題。

- 支援編譯後的二進位檔案韌體建構 SBOM，無需原始碼
- 自動解析元件版本、授權類型與軟體組件架構
- 相容格式：CycloneDX、SPDX 等主流標準
- 一鍵匯出完整 SBOM，支援第三方整合與法規送審



多源合併與精準比對

讓 SBOM 成為真正可信賴的資產地圖

- 合併手動 SBOM、掃描工具與第三方組件資料
- 建構豐富化 SBOM，結合漏洞資訊與授權狀態
- 專利比對技術，提升 CVE 對應精準度與版本辨識正確性
- 自動包含 VEX 描述，評估漏洞實際影響情境



弱點管理與即時監控

從被動通報到主動防禦

- 定期掃描韌體並回報最新漏洞清單
- 自動分類嚴重程度，優先處理具實際風險的項目
- 中央化儀表板：整合警示、版本紀錄
- 降低人工作業時間，強化資安回應效率

適用於產品製造商的完整 SBOM 解決方案



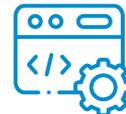
最完整的二進位檔案分析能力：
不用原始碼也能建構合格 SBOM



供應鏈風險可視化：
一目了然掌握漏洞、授權與元件變化



最短合規路徑：輕鬆符合 EU CRA、
開源授權與自證需求



支援韌體管理模式：
導入無縫，適用於 OEM/ODM



開源授權與合規治理

簡化合規 · 防止法律風險

- 自動追蹤開源套件授權變化
- 一鍵產出合規報告與稽核記錄
- 支援 EU CRA 等國際法規之聲明生成
- 完整交付報告格式，可用於供應商自證或外部稽核



自動掃描

軟韌體安全狀態

- 不需手動觸發，平台自動分析軟韌體
- 隨時掌握 SBOM 與弱點資訊
- 保證資訊同步、安全態勢持續強化
- 支援版本比對與異常差異提示



整合既有安全流程

自動化安全流程 · 嵌入 CI/CD 更簡單

- 原生整合 DevOps 工作流程與常見 CI/CD 工具
- 將資安檢查納入開發流程中，安全與交付同步進行
- 精簡流程、降低資安與開發團隊協作成本

產品資安合規服務

從制度到產品，打造符合國際標準的全方位資安合規體系

我們的合規顧問團隊由兼具多年顧問經驗、企業實務與工控產品研發背景的專家組成，熟悉 ISA/IEC 62443、EU CRA、RED-DA、TISAX 等國際資安法規與標準，成員長期服務於工控、車用、半導體及製造業，深度參與企業內部合規推動、產品研發與系統整合，具備豐富跨部門協作與資安法規實作經驗。

我們提供的不只是文件審閱與標準說明，而是根據企業實際狀況，量身打造能真正落地的資安合規解決方案，協助客戶在稽核、導入與持續維運各階段穩健推進，同時因應不同產業的特殊挑戰與風險管理需求。

聯絡我們
www.deltaww.com
security.sales@deltaww.com



Product Security
Service Platform



協助合規關鍵資安標準，打造全方位防護體系



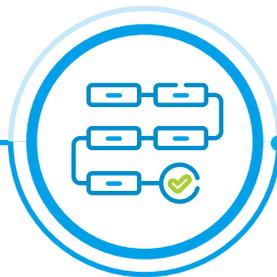
解決理論
與實務落差



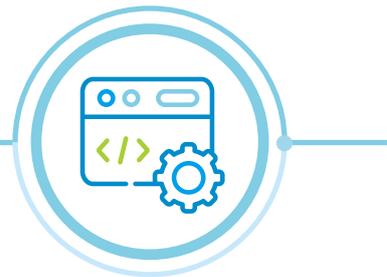
跨領域溝通力強



安全設計



資安融入開發流程



深入技術細節
與實作

IEC 62443 (工業自動化及控制系統資安標準)

IEC 62443 是由國際電工委員會 (IEC) 所制定的一套工業資安標準系列，專門針對工業自動化與控制系統 (Industrial Automation and Control Systems, IACS) 的資訊安全需求所設計。其核心目的是協助企業建構可抵禦網路攻擊與內部威脅的安全防禦架構，確保生產作業的穩定性與可靠性。



符合法規要求
提升市場競爭力



提升產品安全性
降低營運與資安風險

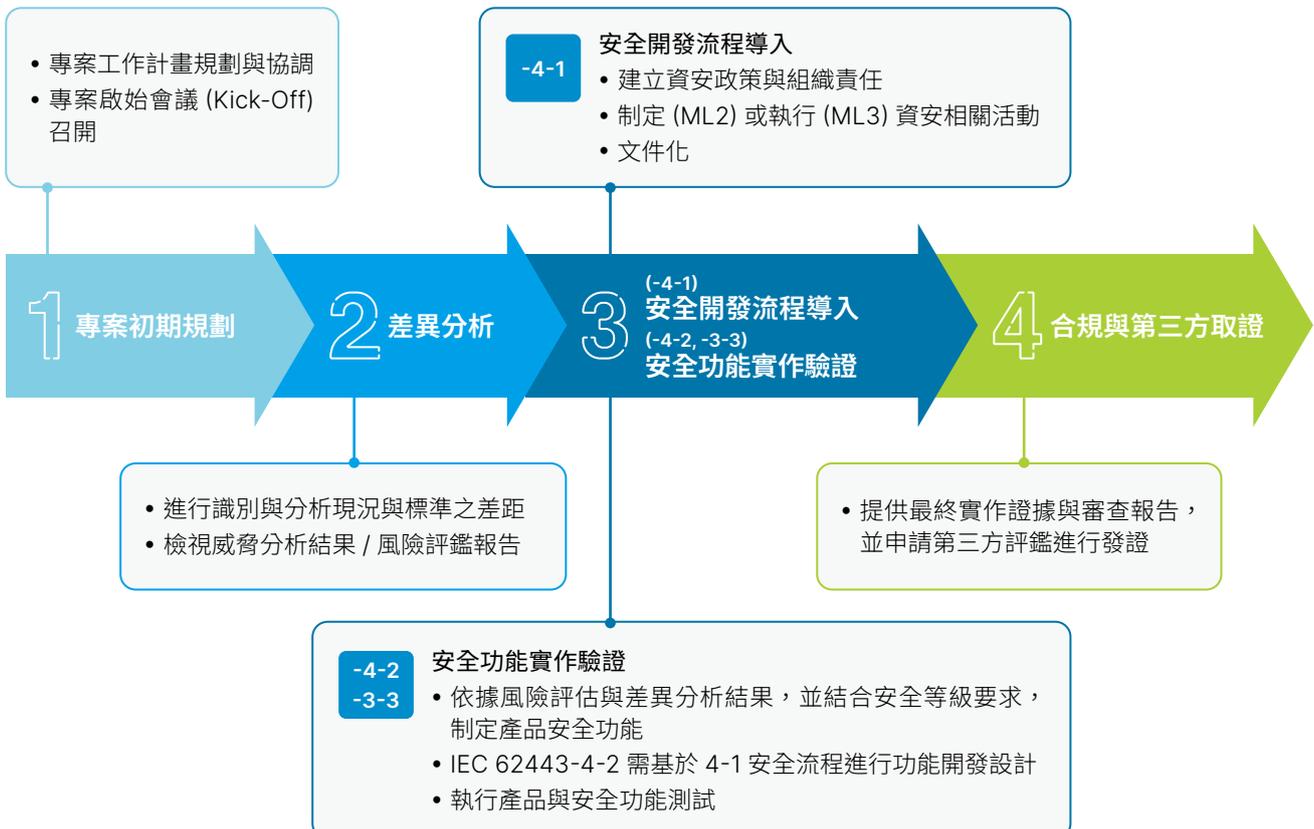


建立系統化的
資安管理機制
提升內部流程效率



增強客戶信心
獲得更多商業機會

IEC 62443 合規專案 - 執行步驟

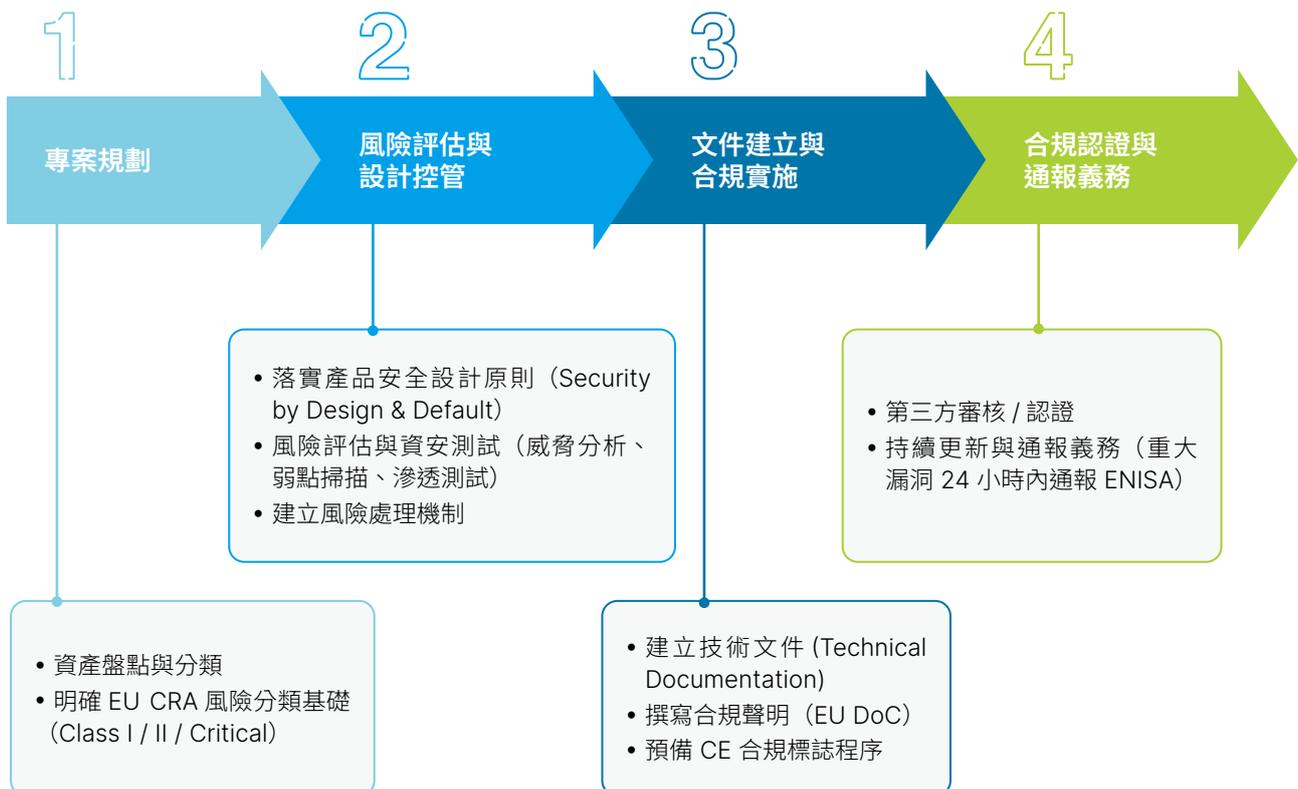


EU CRA (歐盟網路韌性法)

EU CRA 是針對涵蓋硬體與軟體的數位產品設立統一的網路資安法規，目的為提升產品在整個生命週期內的資安韌性與透明度。EU CRA 要求產品於上市前落實預設安全設計、完成風險評估與技術文件，並貼附 CE 標章；高風險產品則須經第三方評估認證。建立一套統一且具法律效力的數位產品資安要求，取代過往各成員國與產業自訂規範的分散管理模式，提升整體供應鏈資安水平與市場透明度。



EU CRA 合規專案 - 執行步驟



RED-DA (無線電設備指令授權法案)

RED-DA 是歐盟無線電設備指令 (RED) 的授權法案，旨在確保無線電設備的網路安全。RED-DA 的重點在於具備連網功能的產品，需要具備防範未經授權存取與資料濫用的能力，若產品涉及個人資料或隱私資訊的處理，則需強化資料保護與隱私設計，以及支援金流或交易功能就必須實作高度安全的加密與驗證機制。該法案要求製造商在產品設計初期就將安全性納入考量，以符合相關法規要求。



Article 3.3(d)
提升網路韌性

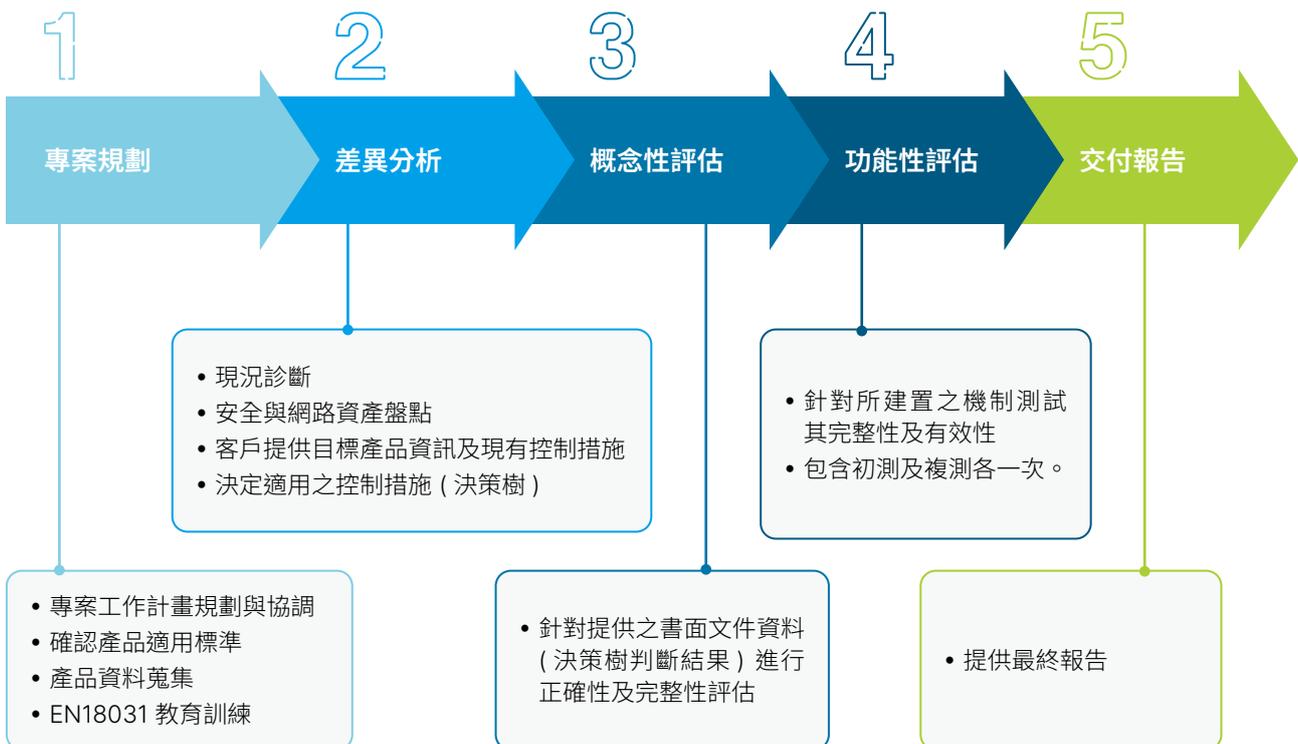


Article 3.3(e)
提高個人隱私保護



Article 3.3(f)
降低詐騙風險

RED-DA 合規專案 - 執行步驟

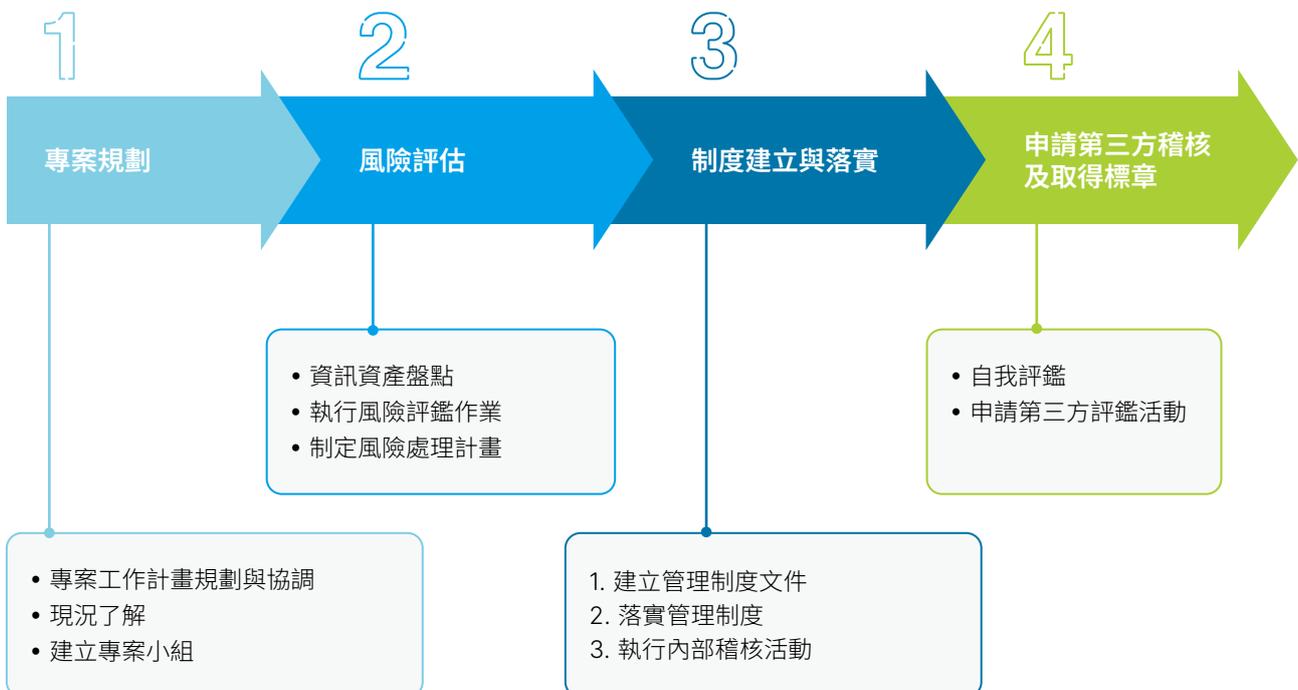


TISAX (汽車供應鏈資訊安全評估)

TISAX (Trusted Information Security Assessment Exchange) 由 ENX (ENX Association) 管理，基於 VDA ISA (VDA Information Security Assessment) 建立之評估與結果交換機制，用於驗證汽車供應鏈的資安成熟度與可稽核性。其涵蓋原型與機密資料處理等情境，已成為歐系車廠的供應鏈準入門檻，可降低重複稽核並加速專案啟動。適用對象包含 OEM、Tier-1 / Tier-2 供應商、設計試製與測試服務商、IT / 雲端與研發外包商。



TISAX 資訊安全 - 導入步驟



SEMI E187 (半導體製造設備資安)

SEMI E187 定義半導體設備的資安基礎，涵蓋作業系統強固、網路區隔 / 加密、端點防護與事件日誌 / 監控，採 OT 零信任思維，適用於以 Windows / Linux 為底層的晶圓廠設備。導入後有助於對晶圓廠以一致規格交付，降低資安風險，並強化客戶信任。



機台設備
資安標準化

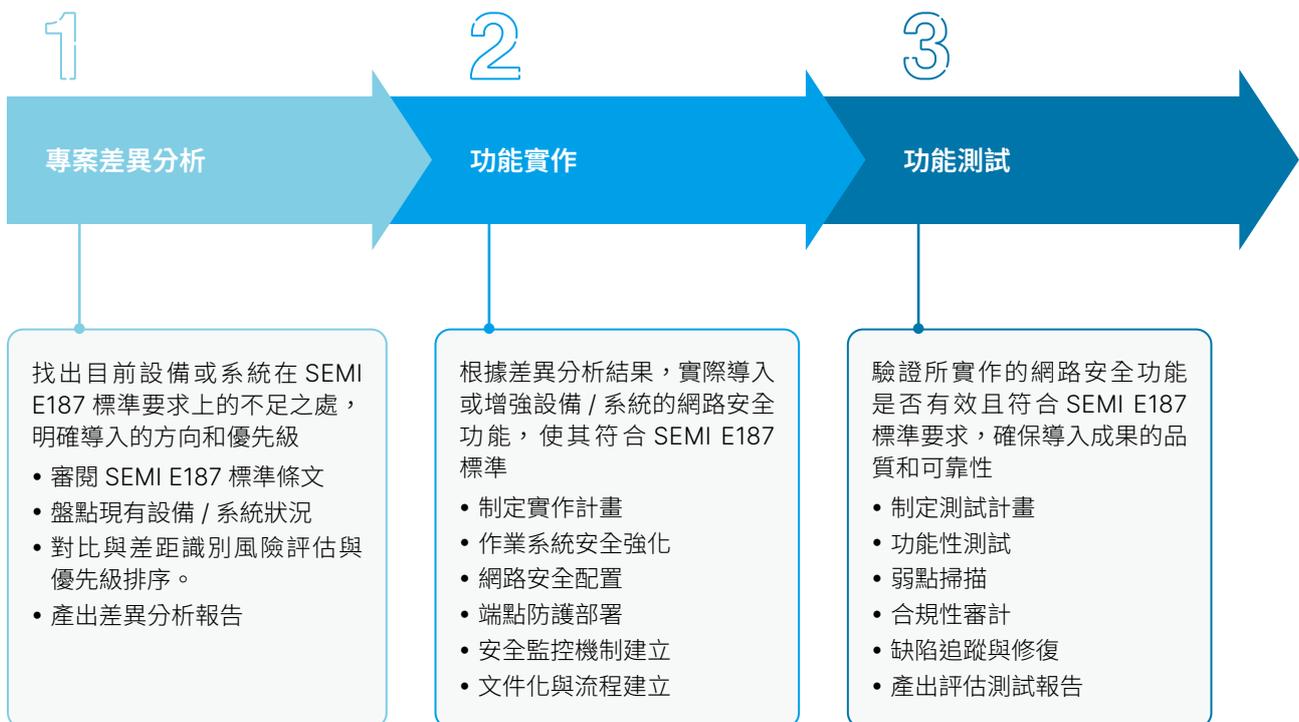


減少設備
潛在資安風險



強化設備安全
與維運韌性

SEMI E187 - 導入執行流程



產品資安評測服務

Delta Product Security Assessment Services

台達的資安評測服務以攻擊者視角＋合規導向雙軌並行，將風險轉為可度量、可驗證、可修復的 engineered work。從威脅建模切入，先鎖定關鍵資產、濫用案例與攻擊路徑，再以弱點掃描快速覆蓋面、手工滲透測試驗證真實影響，並用針對協定／韌體／介面層的模糊測試挖掘未知缺陷。對 OT/IoT 與車用／半導體設備場域皆提供情境化劇本，輸出包含 CVSS / EPSS 風險分級、攻擊路徑圖、修復優先序與重測驗證報告。所有發現與建議可對應 IEC 62443、EU CRA、RED-DA、TISAX、SEMI E187 等條款與客製驗收指標，協助產品的上市上線，或是商業運作之標案需求與外部稽核一次到位。同時，我們把測試結果回饋至研發與維運流程（SDL、SBOM、弱點管理），用最少資源建構產品資安工程。

聯絡我們
www.deltaww.com
security.sales@deltaww.com



Product Security
Service Platform



專業資安防護服務，涵蓋產品資安的每一環節



全面測試精準 揭露安全漏洞

- 威脅建模與風險分析
- 弱點掃描
- 模糊測試
- 滲透測試

產品全球合規 提升防禦能力

- 歐盟網路韌性法案 (EU CRA)
- 無線設備指令授權法案 (RED-DA)
- 工業控制系統安全 (IEC 62443)



國際標準驗證 頂尖資安測試服務

- 符合 ISO/IEC 17025 認證資安實驗室
- 針對不同產業提供專業資安測試方案
- 協助企業建立產品安全開發生命週期
- 全方位資安測試，讓您的產品保持最佳安全狀態

滲透測試服務 Penetration Testing

滲透測試以攻擊路徑為核心，利用橫向移動、權限提升與邏輯竄改驗證等手法，對 OT 資產進行測試。透過對產品硬體、介面、韌體、軟體、服務、通訊等多方面進行全面的入侵嘗試，識別可利用的漏洞和攻擊路徑，有效預防產品安全事件，避免重大損失。



符合資安標準要求



OT 產品與嵌入式設備 / 系統測試經驗



高度模擬駭客攻擊情境真實性



揭露高風險弱點

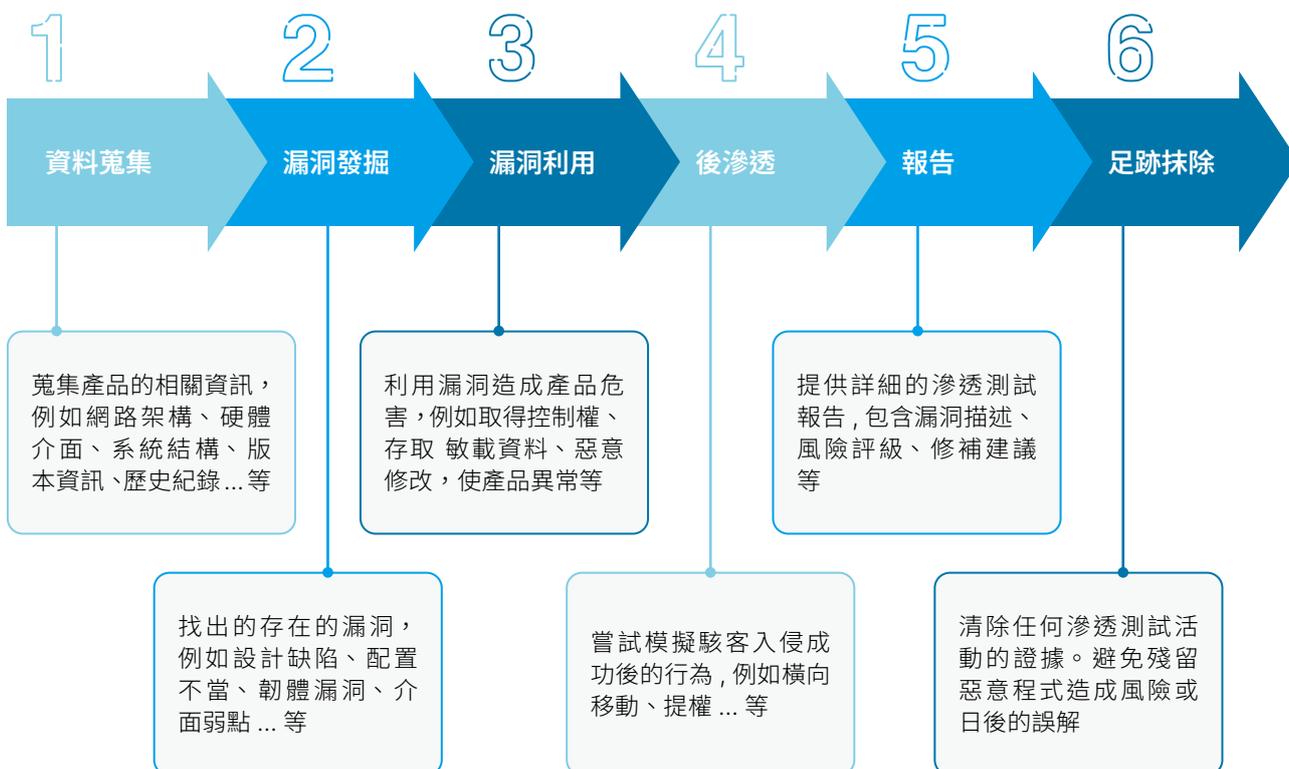


強化產品資安即設計



驗證現行防禦機制有效性

滲透測試服務 – 導入執行流程



弱點掃描 Vulnerability Assessment

弱點掃描是以自動化方式，快速找出已知漏洞、錯誤設定、過期元件、弱密碼與不必要開放服務。全程採低干擾方式，不做破壞性操作；完成後提供問題清單、風險等級與修補建議，可安排重測與週期性掃描，持續把資安基礎拉高。此服務適用於網頁、主機、App 等類型的產品。



滿足規範及
認證要求



高成本效益



易週期性執行
提升資安基準線

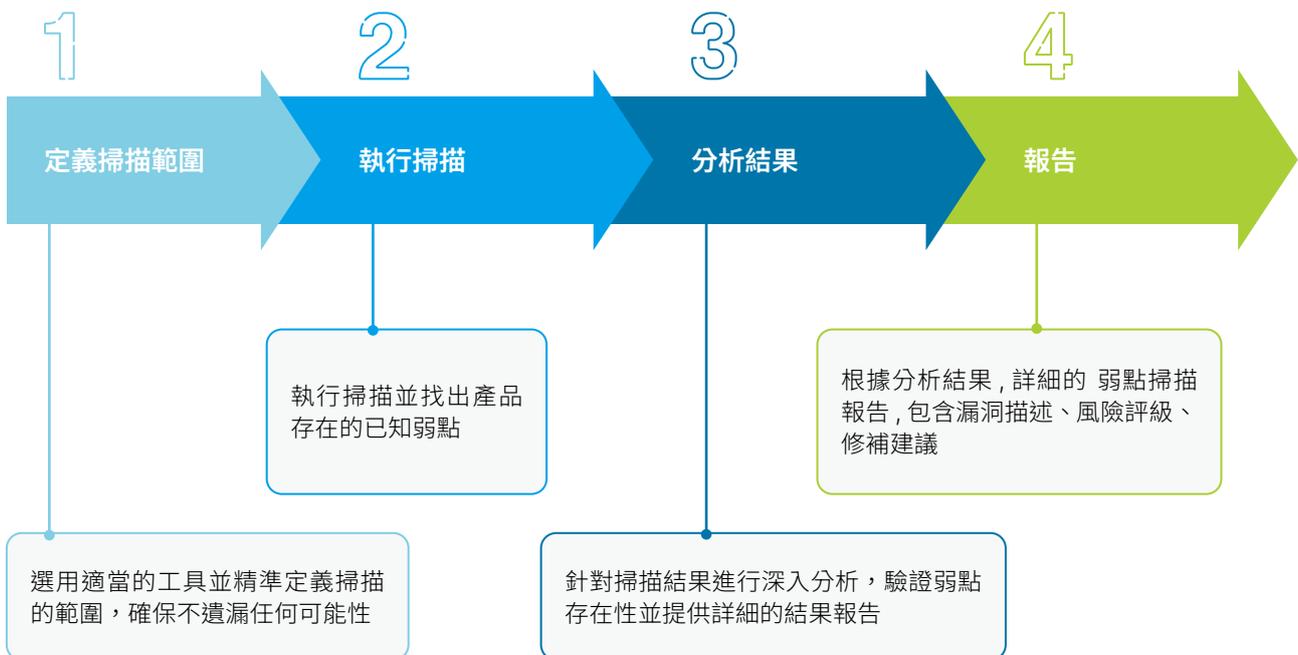


高度降低資安事故
發生率及損失



產品導向的
資安評估經驗

弱點掃描 - 導入執行流程



模糊測試 Fuzz Testing

模糊測試是一種自動化或半自動化針對產品可用性的評測服務。透過向目標傳送大量異常或非預期的封包，監控產品是否會出現非預期的狀態，揭示產品潛在的資安缺陷，有助於提升穩定性與可用性。模糊測試服務適用於嵌入式、主機設備、車用、網通等類型的產品。



發現傳統掃描無法檢出的漏洞



補強通訊協定與解析器安全



驗證設備 / 系統的抗錯能力與韌性



支援自動化測試

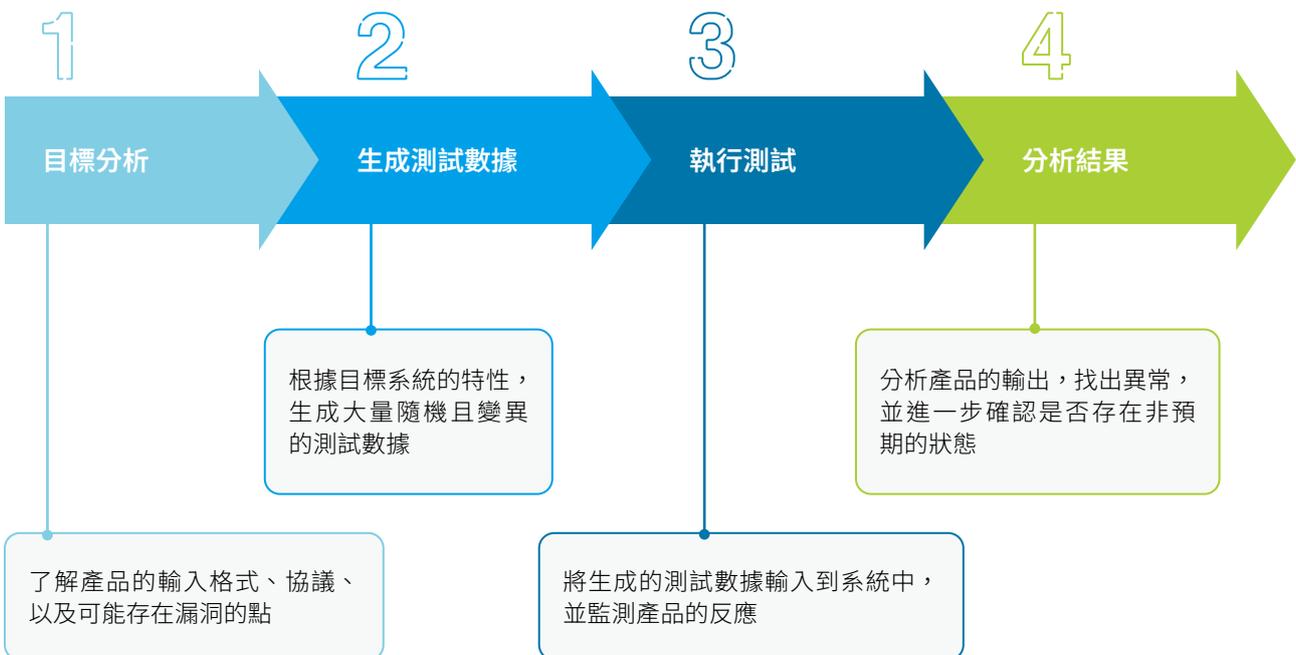


提升防禦編碼品質



加速產品安全驗證與合規準備

模糊測試 - 導入執行流程



PVM：產品安全智慧風險管理平台

Proactive Vulnerability Management: The Intelligent Risk Management Platform for Product Security

PVM 結合全球威脅情資、持續漏洞監控與風險排序。支援主流 SCA 工具與多種檔案格式（Black Duck CSV、Jenkins XML、自定義 Excel）。協助企業在產品的全生命週期中，從看見風險到預見決策，實現高效合規與全方位漏洞追蹤。



聯絡我們
www.deltaww.com
security.sales@deltaww.com



Product Security
Service Platform

從持續監控到智慧決策，打造 CRA 合規致勝引擎



持續監控 — 7×24 全球風險雷達

- 全球頂級情資即時同步（NIST / CISA / FIRST）
- 精準到版本的漏洞分析，避免誤判
- 客製化威脅洞察推送，化被動為主動
- 完整稽核軌跡，輕鬆應對合規

智慧決策 — 資安指揮中心

- 攻擊潛能排序，聚焦不到 10% 致命風險
- 團隊協作平台：即時註記、追蹤進度
- 輔助修復顧問：提供具體修補建議
- 企業知識大腦：累積修補經驗



自動化合規 — 一鍵式法規應對中心

- 將 CRA 合規流程數位化、可追蹤化
- 自動生成報告（CRA 附件、VEX 等格式）
- [可選] 專業服務團隊，支援複雜合規挑戰

PVM 產品價值

- 不僅整合 NIST，更全面匯集 CISA 與 FIRST 等多源威脅情資，深入管理第三方 套件漏洞，大幅縮短合規準備時間。
- 告別冗長的漏洞清單，自動排序漏洞優先級，開發團隊專注於真正重要的風險。
- 支援 Nessus、DAFA 及 CI/CD 工具，無需改變現有工作流程，降低總體成本。
- 能透過分析攻擊趨勢，預測潛在風險，在威脅發生前就做好準備。



**CRA 合規
自動化引擎**



智慧修補導航

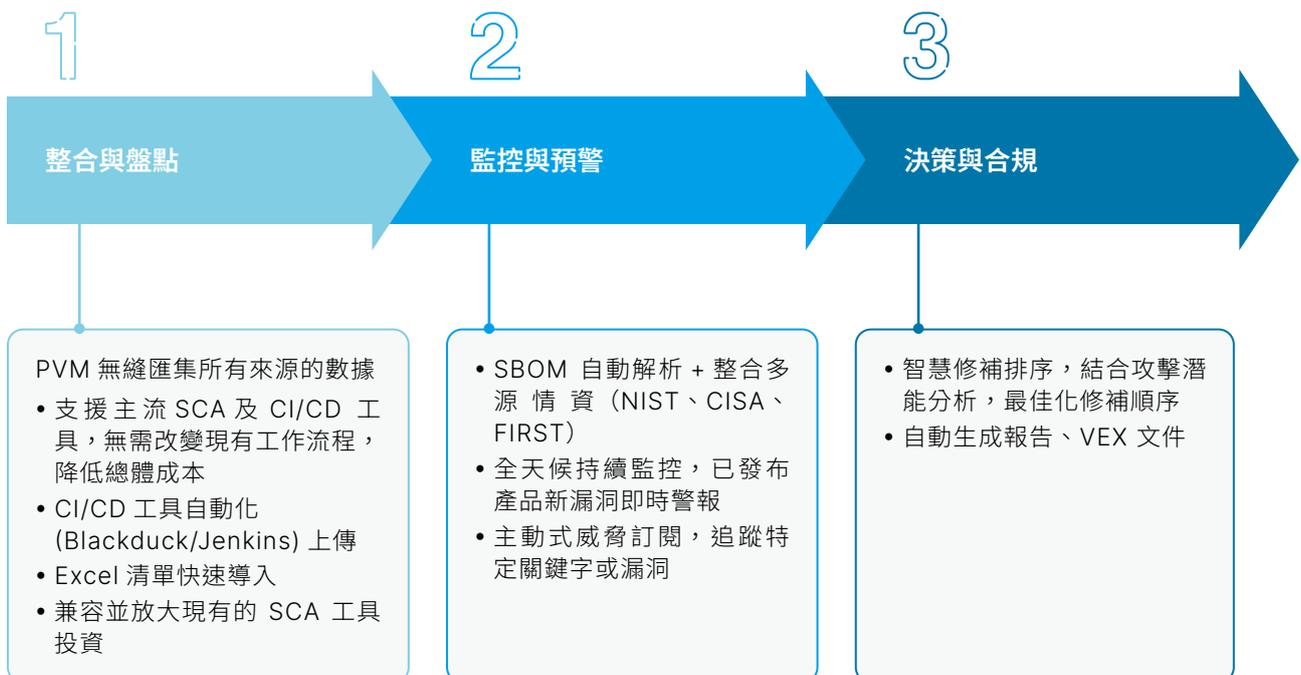


**無縫整合的
安全作戰平台**



**從被動響應
到主動防禦**

PVM 解決方案：產品安全三部曲





www.deltaww.com

114501 台北市內湖區瑞光路 186 號 台灣企業總部
TEL: +886-2-8797-2088 FAX: +886-2-8797-2120