零信任物聯網資安防護推動機制

工研院資通所 雷穎傑

公衛思維，循序漸進，協助產業深化資安

基層醫療服務

醫生問診

抽血、超音波、X光

診斷/對症下藥

衛教/回診追蹤

保險給付

企業資安評級 → 資安外部掃描/內部檢測 → 事件通報/強化資安措施 → 資安培訓 → 資安演練 → 研發補助

Art Of Cyber War ACW

計畫單一窗口

- 外部曝險分析
- 內部資安健診

- SECPAAS國產資安平台
- 資安服務試用

- 資安人才培訓課程
- 資安長交流
- 紅隊演練

- 產創10-1投資抵減
- Digital+資安主題式補助
- 場域實證計畫

ACW SOUTH 數位產業署沙崙資安服務基地

沙崙資安基地

產業資安強化推動工作小組(SIG)

企業資安檢測補助

紅隊演練補助

SECPAAS Security Platform as a Service

國產資安整合平台

零信任物聯網補助計畫(草案)

數位信任場域服務實地驗證計畫

推動公協會成立產業資安強化推動工作小組

申請時間：即日起至4/25

聯絡人：張小姐/sharonchang100@itri.org.tw /(02) 25159665 分機 164

SIG計畫：FY113年度推動重點

		擇定產業範疇	設定SIG機制 推動輔導	評級推動	紅隊推動	成果發表
			SIG會員輔導	顧問團推動	紅隊演練輔導	資安Day展示
112年度	推動作法	• 從製造業擴增至數位產業等其他業別	• 免費體驗資安外部掃描	• 提供非SIG會員免費申請自我評量 • 聯合moda服務團提供顧問諮詢服務	• 推動電商產業進行紅隊演練	
113年度	推動作法	• 全產業受理	• 自評評級問券，參考NIST SP800-171制定的171題完整版問券 • **新增ISO27001和零信任資安問券**，滿足企業國際合規需求 • **免費提供資安曝險分析**，自動化外部掃描工具協助企業掌握外部風險	• **CDM資安防護矩陣**宣導 • 提供**資安體驗方案**，如UTM整合情資端點防護等 • 聯合moda服務團提供顧問諮詢服務	• 受理**紅隊演練**補助	

企業資安成熟度評級的五大功能

除了NIST SP800-171外，今年新增ISO27001、SP800-207問券供業者填答

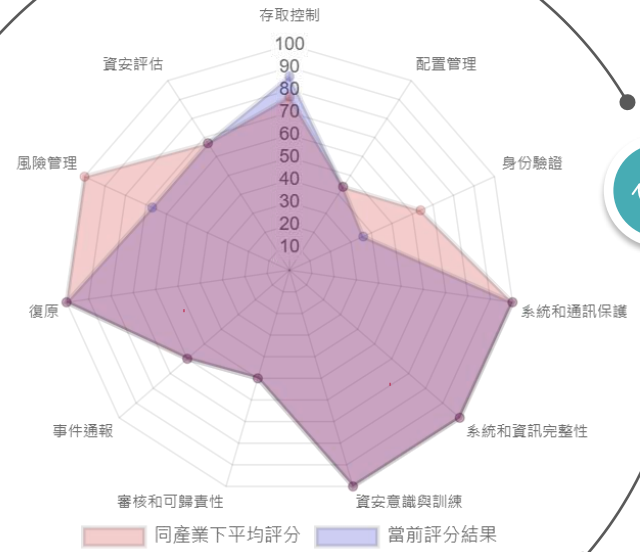
幫助CISO進行內部溝通

防護指引

平衡資安防護組合

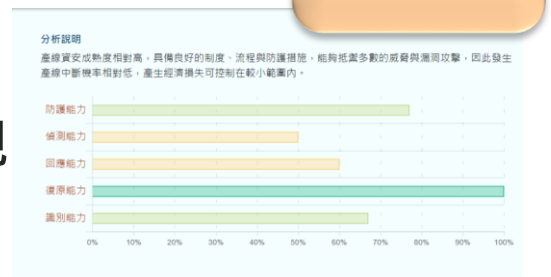
進行產業標竿分析

差距分析



提供資安現況

現況檢視



建議資安升級藍圖

幫助資安投資決策

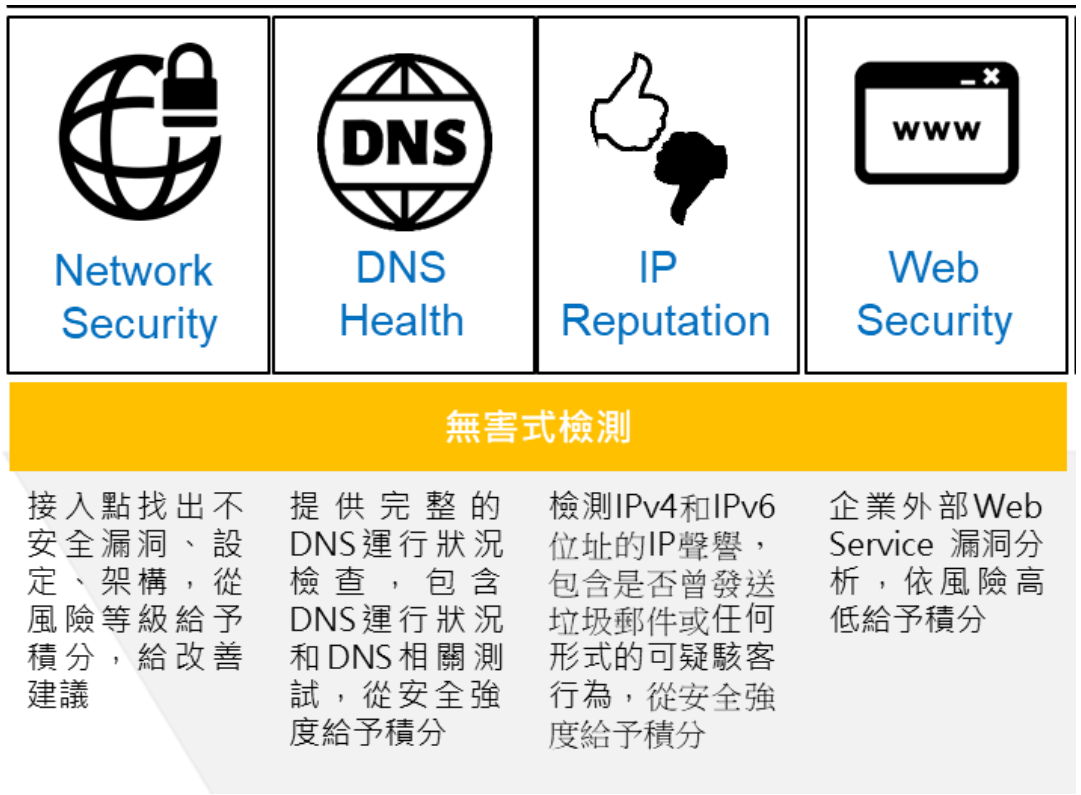
改善排序

缺口快篩

資安健診-外部曝險服務

針對企業對外網路(Public IP)提供四大面向無害式資安檢測。

- Network Security、DNS Health、IP Reputation、Web Security四大面向



表格 1: 外部節點潛在風險數量統計

網域	主機	高風險數量	中風險數量	低風險數量	潛在風險總數
123.com.tw	123.123.123.1	23	40	30	93
www.123.com.tw	123.123.123.1	0	0	0	0
auto.123.com.tw	123.123.123.3	0	0	0	0
auto.123.com.tw	123.123.123.5	0	0	0	0
auto.123.com.tw	123.123.123.6	0	0	0	0
auto.123.com.tw	123.123.123.7	0	0	0	0
ccc.123.com.tw	123.123.123.8	11	9	1	21
dns1.123.com.tw	123.123.123.9	40	77	15	132
dns2.123.com.tw	123.123.123.10	20	52	81	153
ftp1.123.com.tw	123.123.123.12	50	36	62	148
yyy.123.com.tw	123.123.123.15	40	77	15	132
service.123.com.tw	123.123.123.13	24	14	0	38
time.123.com.tw	123.123.123.30	40	77	15	132
vpn.123.com.tw	123.123.123.25	0	0	0	0

資料來源：本報告整理

資安健診-外部曝險服務

透過工研院自動化工具，以外部人角度看公司在網路世界中呈現的樣貌

功用：

1. 看外顯的DNS名稱，是否有公司不知道的子域名
   - www.itri.org.tw是正常，但Aa1BwF.itri.org.tw可能就不正常
2. 看公司顯示在外的主機，是否有非公司認知的主機
   - 140.119.1.1是認可的主機，但140.119.1.2可能是同仁私開的主機，或你的DNS有不認識的IP，就需要去檢查DNS是否已遭利用
3. 看公司主機所開啟的Port，是否有非必要的Port，或自己不知道的Port(後門)
   - 80,443是web網站常見的port，但port 21(FTP)是否該開？
4. 看每個Port所顯示的服務是否有風險
   - Port 80顯示出Apache 版本號2.2.4→版本號讓hacker容易去找漏洞

以上的問題，您需要外部掃描來告訴你

紅隊演練補助申請

計畫目的

- 擬以紅隊演練補助，協助廠商驗證識別入侵途徑，驗證其資安解決方案的有效性
- 協助藍隊解決重要弱點，提高偵測弱點的效率及資安防護與應變機制，促進企業落實資安韌性提升。

申請規定

1. 申請資格：由獲選產業資安強化推動工作小組(SIG)推薦企業成員申請
2. 提案組成：採聯合提案，由一家場域驗證企業代表和紅隊資安廠商(須為SECPAAS或具備資安能量登錄廠商)合作申請
3. 需提供合作意向書，或簽署合約或報價單等合作證明

補助金額

每案最高100萬元，每案補助比例不超過50%
即專案金額達 200 萬或以上，補助最高100萬元

資安檢測診斷服務

申請時間：尚未開放，預計五月底
聯絡人：中華軟協

資安檢測診斷服務(內部檢測，預計五月底)

◆透過「企業資安評級」、**「主機系統弱點掃描」、「目錄伺服器或設備組態檢視」、「網路封包側錄分析」、「惡意程式或檔案檢視」及「防火牆連線設定檢視」**等檢測項目，協助受測企業掌握組織內部資安防護現況

推動產業資安檢測

結合產業公協會
共同推動會員申請資安檢測

客製化檢測類別與項目

依產業要求調整檢測項目
提供符合需求的資安檢測

促成產業提升資安防護能力

提供企業資安防護(改善)建議
降低未來受駭風險

1.企業資安評級評估報告
2.主機系統弱點掃描報告
(含初掃及複掃)
3.資安檢測服務報告
(含資訊設備組態檢測、網路封包側錄分析、惡意程式或檔案檢視及防火牆連線設定檢視)

零信任物聯網補助計畫規劃(草案)

申請時間：即將公開

計畫目標

中心場域帶頭，驅動資安業者投入研發，帶動供應鏈廠商導入資安治理，共同提升資安能量

具備資格

- 國際供應鏈廠商
- 受國際/大廠客戶資安稽核要求者
- 受資安法規要求者

✓ 驅動資安業者投入利基型零信任解決方案

資安產業深耕-研發臺灣產業所需的零信任技術整合解決方案

✓ 打造供應鏈安全的零信任資安示範場域

產業資安深化- 打造零信任資安示範場域

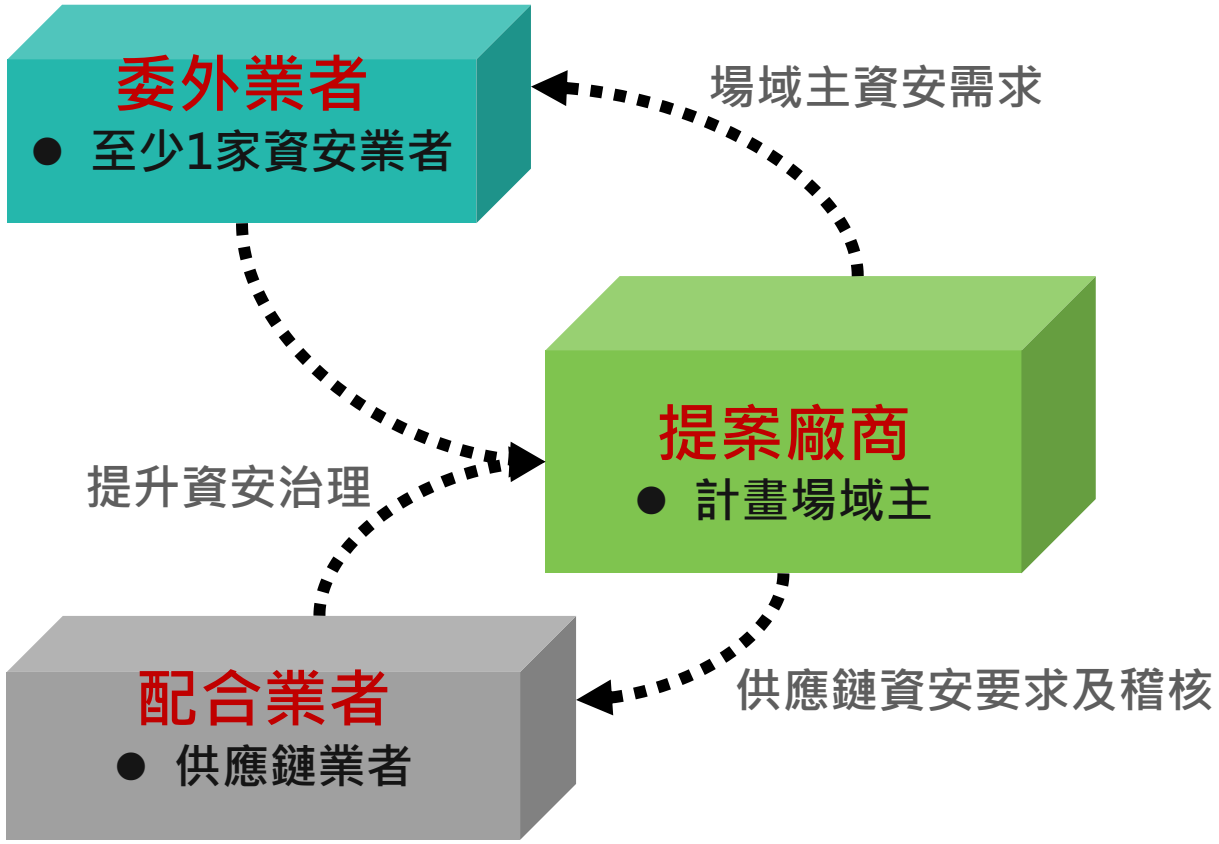
產業資安協力-資安曝險、評級提升資安治理

✓ 帶動供應鏈提升資安治理

產業資安擴散- 帶動供應鏈廠商一起參與

補助範圍

開發零信任自主技術整合方案



研發零信任資安自主技術整合解決方案

透過場域試煉，發展對企業有價值效益的資安需求解決方案，帶動零信任資安方案自主技術整合研發

打造物聯網零信任資安示範場域

輔導企業建立零信任的資安示範場域，透過場域驗證，深化資安技術能量，擴散至供應鏈廠商，帶動資安強化風氣，產生資安良性循環，建立資安生態圈

推動供應鏈資安治理

輔導供應商導入零信任方案，以資安成熟度評級+客觀資安曝險分析，完善供應鏈資安治理，並規劃稽核制度，落實管理執行面及實現可持續性

後面講者會有更詳細的介紹....

數位信任場域服務實地驗證計畫

申請時間：至113年4月19日(五)下午5時截止
聯絡人：
02-7754-2616 #200 鞠小姐
02-2577-4249 #271 張先生

申請類別有哪些？

4技術類別，每案300萬元 (上限)

※執行期限:申請日起至10/18日前完成

隱碼

- ✓ **模組設計**
  系統架構、介面及資料整備程序
- ✓ **模組隱碼**
  隱碼/物流業者API

10萬人次驗證/家

FIDO

- ✓ **導入情境**
- ✓ **系統架構設計**
- ✓ **聯盟認證**
  預計今年取得者，附規劃

3萬人次驗證/家

電子簽章

- ✓ **導入情境**
- ✓ **技術與註冊**
- ✓ **系統架構設計**
- ✓ **驗證與使用流程**

5萬人次驗證/家

區塊鏈

- ✓ **導入情境**
- ✓ **系統架構設計**
- ✓ **其他**
  使用效益、網站/APP介接架構、介面等

2萬人次驗證/家

後面講者會有更詳細的介紹....

感 謝 您 的 聆 聽

Thank You

數位發展部 數位產業署
Administration for
Digital Industries, moda