CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

Product Security Forum

PRODUCT SECURITY FORUM

台灣電子產品安全嗎？

從呼叫器爆炸案談ICT產品資安

TEAM CYBERSECURITY

龔化中 Dennis Kung

國家資通安全研究院 副院長

dennis.kung@nics.nat.gov.tw

黎巴嫩呼叫器爆炸案

繪圖：ChatGPT

產品資安對 ICT 廠商有重大影響

Product Security Forum

產品行銷與政府採購	• 美國 Cyber Trust Mark, 聯邦 “物聯網網路安全法” • 日本 JC-STAR, 新加坡 CLS
市場准入法規限制	• 歐盟 CRA (Cyber Resilience Act) • 英國 PIST(產品安全與電信基礎設施法)
主管機關處罰	• 歐盟 GDPR 個資洩漏罰款 (違反32條資料安全義務) • 美國聯邦貿易委員會 FTC 提告
商譽損失與客戶求償	• Crowdstrike 全球大當機事件 (2024) • Amazon Ring (2019), Philips 智慧照明 Hue (2020)

資料來源：網路新聞整理。

產品資安也會影響國家安全

360数字安全
数 字 安 全 的 领 导 者

3000名駭客巔峰較量，100+漏洞震撼突破！矩陣杯決賽落幕

2024-07-01

矩阵杯 | ISC ISC平台 | SecOps

6月28日，由360數位安全集團、華雲安主辦，ISC平台、SecOps 平台承辦，賽寧網安、永信至誠、紅客社區協辦的首屆「矩陣盃」網路安全大賽，經過48小時激烈拼賽，在青島國際會議中心落下帷幕。大賽設置通用產品漏挖賽、國產軟硬體安全檢測賽、原創漏洞挖掘賽、人工智慧（大模型）挑戰賽、戰隊攻防對抗賽五大賽事，吸引了來自全球多個國家的1000餘支戰隊、近3000名選手共同向2000萬獎金發起衝擊。

中國國家互聯網信息辦公室 (CAC) 在 2021 年 7 月發布了《網絡產品安全漏洞管理規定》，要求所有漏洞都必須向工業和信息化部 (MIIT) 報告，並禁止公開披露漏洞，包括向海外組織。

專家指出，這項法律可能會讓中國政府幾乎獨家地早期獲得大量的零日漏洞資訊，包括可能存在於美國國防部和情報部門使用的技術中的漏洞。

Read in the Substack app | Open app

The Prototype: A.I. driven cyber offense

A rare find on the "China Net" provides an exclusive look into the future of Chinese offensive cyber operations. Meet "The Prototype": a conceptual AI cyber offensive tool from China.

NETASKARI
MAR 21, 2025

一個名為「AI驅動的網路攻擊原型」的工具被發現，其主要功能是尋找並利用台灣物聯網設備中的漏洞 。這表明該原型很可能被設計用於攻擊性的網路行動

https://netaskari.substack.com/p/the-prototype-ai-driven-cyber-offense

資料來源：網路新聞整理。

我的工作經驗: 電子通訊 + 網路資安

任務: 結合政府和業者的力量做好ICT產品安全

產品資安問題來源(一) 供應鏈攻擊

Product Security Forum

更新

後門

仿冒

遙控

資料來源：網路新聞整理。

產品資安問題來源(二) 駭客攻擊

Product Security Forum

實體改機
硬體破解

香港01

科技玩物 / 遊戲動漫

Sony PlayStation Portal遭工程師成功破解！可直接玩PSP舊遊戲

ETtoday新聞雲

首頁 | 小遊戲 | 影劇 | 生活 | 詐騙警世錄 | 社會

PS5驚傳遭人破解「越獄」 可裝非官方軟體還能裝《P.T.》

▲ PS5 驚傳遭到破解。（圖／取自免費

實體改機
韌體置換

連線攻擊
竊取資料

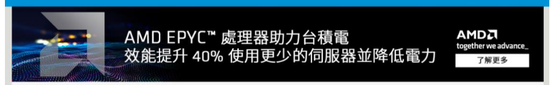
iThome

新聞

中國駭客藉由殭屍網路Quad7竊取帳密資料

前幾個月殭屍網路Quad7被資安業者發現而浮出檯面，因為當中綁架TP-Link、兆勤（Zyxel）、華碩、Ruckus等多個廠牌網路設備，而受到注意，但這股惡勢力並未完全消失，微軟近日提出警告，該殭屍網路活動再度出現升溫的現象

iThome



新聞

歐洲最大雲端服務供應商揭露自身面臨的大規模DDoS攻擊，這些惡意流量竟源自近十萬臺MikroTik路由器

連線攻擊
癱瘓破壞

資料來源：網路新聞整理。

針對ICT產品的惡意程式非常多種

- Mirai 開源惡意程式
- WannaCry 台積電的傷心往事
- Stuxnet 破壞伊朗核設備離心機
- Silex 讓設備變”磚塊”
- Mozi 防不勝防的P2P

一魚多吃!!!!

繪圖：ChatGPT

ICT 產品的漏洞是 APT 級駭客的最愛

SPY×FAMILY

- 中國 Salt Typhoon：針對電信商的核心路由竊取機密
- 俄羅斯 APT28：透過 Cisco 路由器攻擊歐洲各國政府
- 伊朗 APT：利用 Fortinet 漏洞攻擊美國和以色列
- Water Barghest：侵入大量物聯網設備當犯罪工具出租

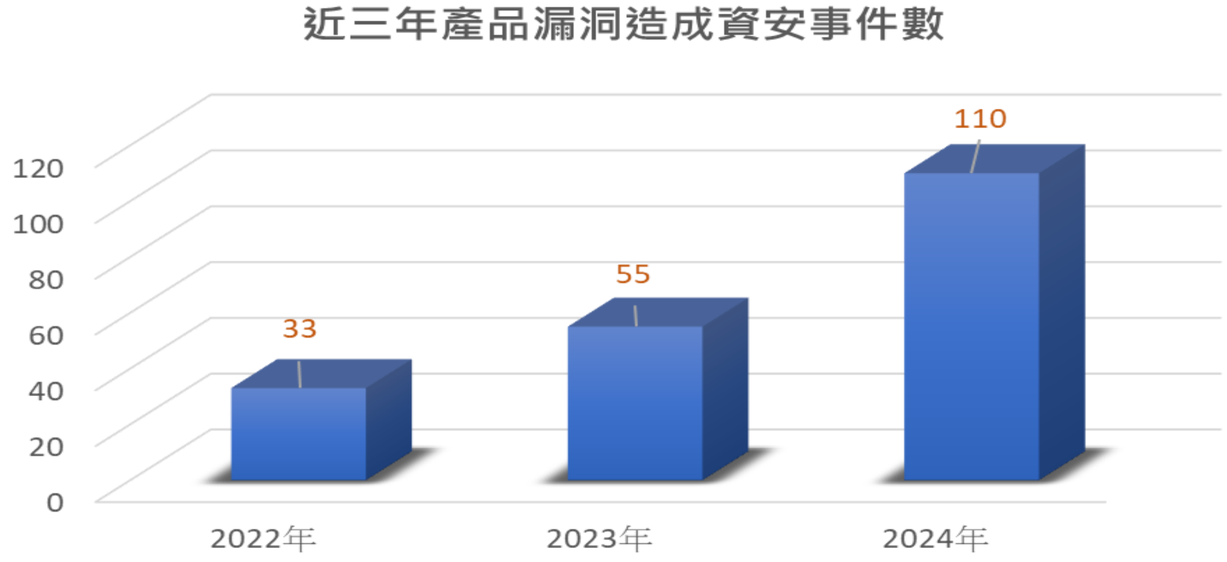
買回家研究不怕被逮到!!!!

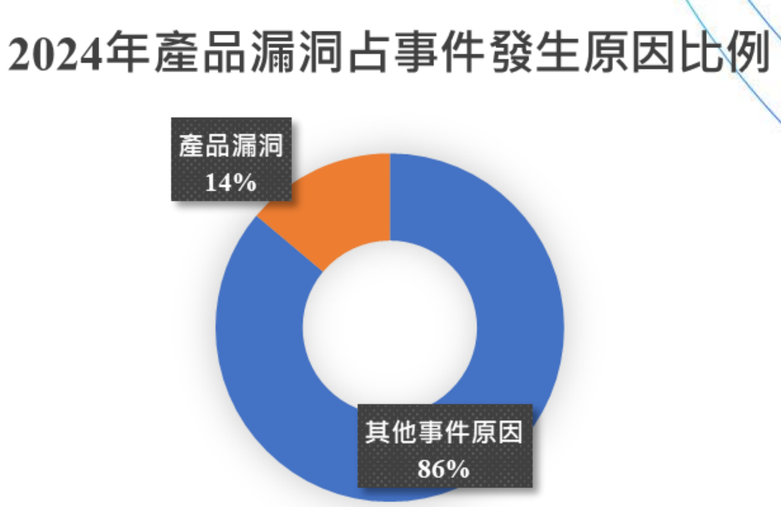
資料來源：網路新聞整理。 繪圖：ChatGPT

台灣 ICT 產品資安現況與各家廠商的改善作法

台灣政府 ICT產品資安相關的事件統計

- 統計2022至2024年間，台灣政府因 ICT 產品漏洞所引發的資安事件逐年上升，政府資安防護方面存在重大挑戰
- 觀察2023年至今，駭客鎖定邊際設備、網通設備發動攻擊為主要趨勢，歸納其攻擊模式大部分以CVE弱點利用入侵
- 透過政府資安通報，通知其他機關即時修復漏洞，避免擴散，才能大幅減少重複的攻擊





資料來源：資安院整理

台灣主要網通品牌資安漏洞CVE通報統計

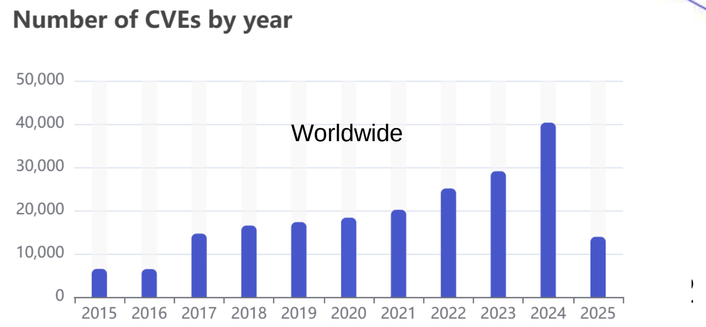
Product Security Forum

廠牌	2019	2020	2021	2022	2023	2024	2025 Q1	總計
Asus	11	6	40	24	13	7	1	102
D-link	4	4	1	0	1	25	5	40
DrayTek	2	14	6	2	4	43	3	74
QNAP	5	23	37	19	21	58	7	170
Synology	11	6	14	19	5	17	8	80
Zyxel	6	3	2	11	26	11	7	66
台灣品牌總計	39	56	100	75	70	161	31	532
Cisco	301	428	400	208	149	108	14	1608
Fortinet	17	21	60	40	76	35	40	289
Netgear	13	431	87	42	35	21	2	631
TP-Link	14	13	6	28	17	15	7	100
國外品牌總計	345	893	553	318	277	179	63	2628

* 資安院整理 本表數據綜合 NVD、CVE Details、廠商公告等多方來源

** ODM 廠牌的 CVE 漏洞是由品牌廠處理, 不列入統計

** CVE 通報多, 代表積極處理, 不代表品質不良



ICT產品資安風險的源頭

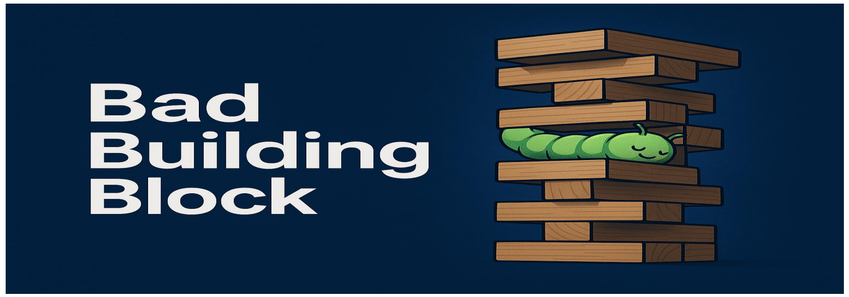
產品用的作業系統
或軟體元件有弱點

軟體設計不良
或設定不嚴謹

CVE (common vulnerability)

CWE (common weakness)

ICT產品資安風險的對策



- SBOM 管理
- 弱點掃描
- 即時的韌體更新

➔ 解決 CVE

- SSDLC 安全軟體設計
- 源碼掃描 滲透測試
- 完善的通報修復系統

➔ 避免 CWE

* 感謝 DELTA 提供資料

台達電集團的例子: 完整 SSDLC 解決方案

產品資安合規服務
compliance and testing: **TMRA, PT, VT, etc.**

產品資安管理輔助工具
AFA (SBOM)

產品資安強化方案
security software components : **AWL/RADAR**

Concept
- PVM

Design
- TMRA / TARA
- CRAFTS

Implementation
- AWL / RADAR
- AFA
- SCA

V&V
- PT / VT / FT
- Threat Mitigation Test
- Requirement Test

Operation
- PVM
- Issue Response
- AWL / RADAR

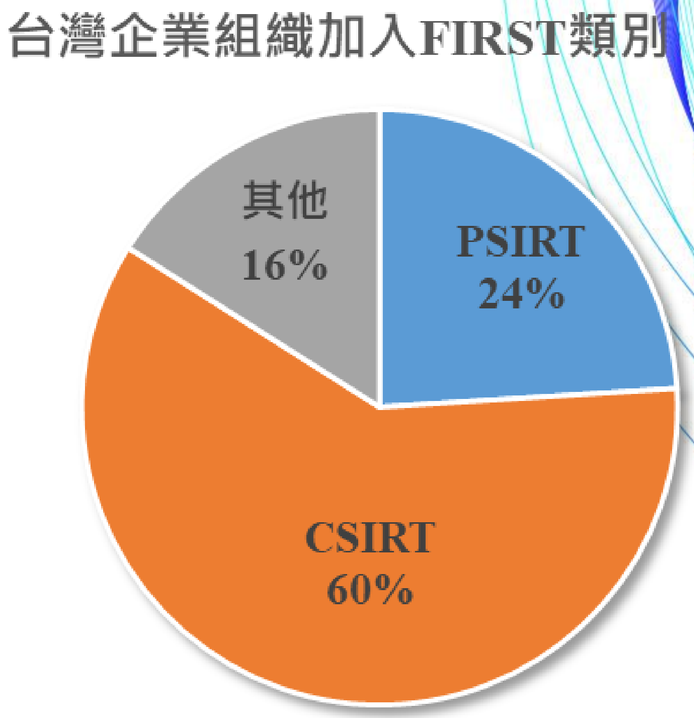
- Security Defense
- Security Tools
- Assessment

VT: Vulnerability Test
PT: Penetration Test
FT: Fuzz Testing
SCA: SW code Analysis
AWL: Application Whitelisting
RADAR: Ransomware Resist Data Backup and Recovery
AFA (SBOM): Automatic FW/SW Analysis
TARA: Threat Analysis & Risk Assessment
TMRA: Threat Modeling and Risk Assessment
PVM: Proactive Vulnerability Management
CRAFTS: Cybersecurity Risk Assessment Framework for Threats and Solutions

台灣企業產品資安通報處理團隊 PSIRT

PSIRT專注產品安全，CSIRT專注組織資安風險

- PSIRT負責主動檢查、處理來自使用者或內部的產品漏洞通報管理，防止漏洞被駭客利用
- 國際資安事件緊急應變小組論壇 FIRST (Forum of Incident Response and Security Team) 有定義 PSIRT 處理標準程序: *PSIRT Services Framework*
- 2024年總計有25個台灣企業與組織成為FIRST成員，其中 24% 有PSIRT團隊



資料來源：資安院整理

企業的資安漏洞通報系統的例子

資料來源：企業官網蒐集整理

資安名人堂 鼓勵資安研究員通報漏洞

Product Security Forum

ProArt | ASUS IoT | Gaming

ASUS | Mobile / Handhelds | Laptops | Displays / Desktops | Motherboards / Components | Networking / IoT / Servers | Accessories

ASUS Product Security Advisory

We take every care to ensure that ASUS products are secure in order to protect the privacy of our valued customers. We constantly strive to improve our safeguards for security and personal information in accordance with all applicable laws and regulations, and we welcome all reports from our customers about product-related security or privacy issues. Any information you supply to ASUS will only be used to help resolve the security vulnerabilities or issues you have reported. This process may include contacting you for further relevant information.

Hall of fame

We would like to thank the following people have made responsible disclosures to us. They were very first reporters to notified qualifying vulnerabilities which consented to be fixed by ASUSTek Computer Inc. Thank you and congratulations for demonstrating your technical skill, security knowledge, and responsible behavior.

~~2025 ∇~~

March 2025:

1. Thomas 'TKYN' Keefer

February 2025:

1. Marcin 'Icewall' Noga
2. leeya_bug
3. Mounir Elgharabawy

2024 ∇
2023 ∇
2022 ∇
2021 ∇
2020 ∇
2019 ∇
2018 ∇
2017 ∇
2016 ∇

ZYXEL NETWORKS | Products | Solutions | **Support & Learn** | Where to Buy | Sign in

Zyxel really appreciates your finding and attempt in making the internet a safer place.

Security Advisories | Report Vulnerability | Hall of Fame | PSIRT Policy

2025

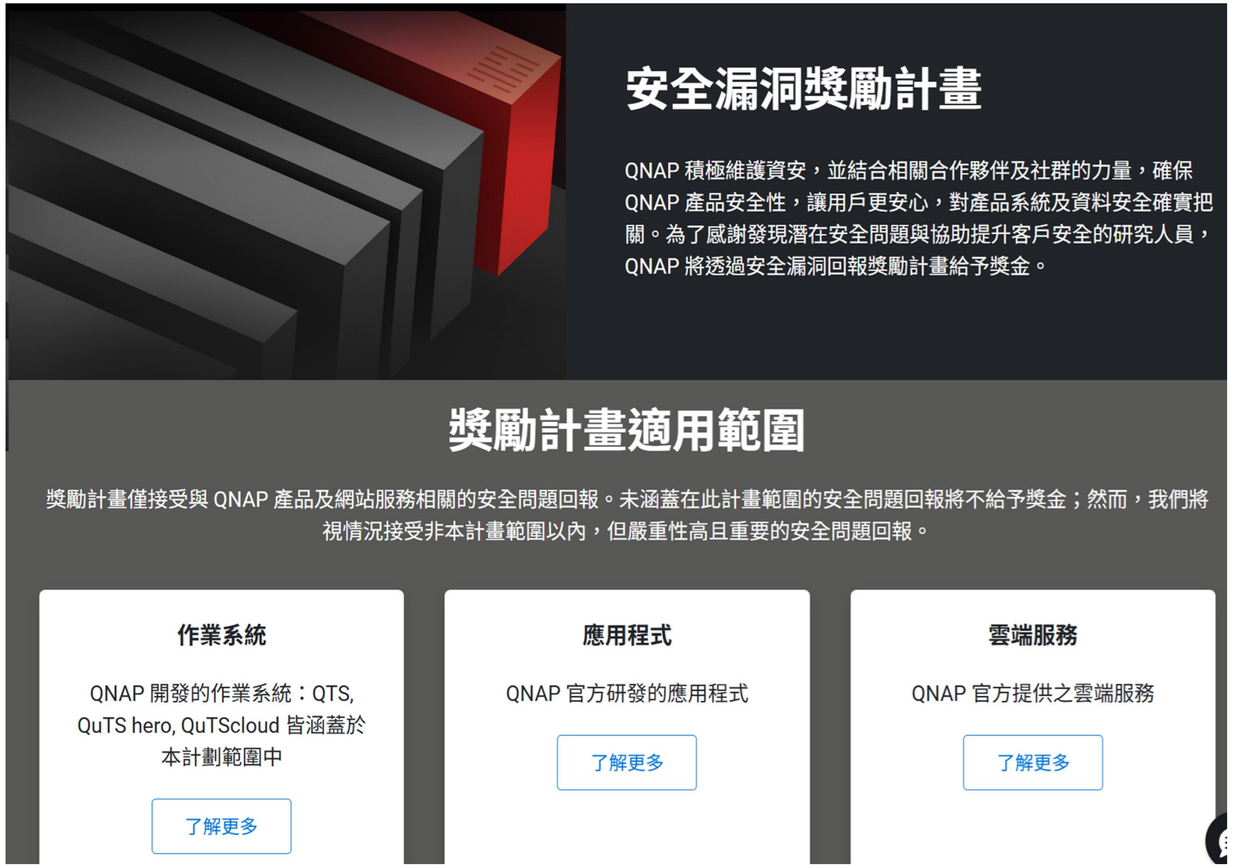
CVE ID	Company/Organisation	Contributor
CVE-2024-11253		Erik de Jong
CVE-2024-12009		Dawid Kulikowski
CVE-2024-12010	ONEKEY	
CVE-2024-12010	Digitec Galaxus AG	Martin Wrona
CVE-2024-12398	HackerHood	Alessandro Sgreccia

2024
2023
2022

資料來源：企業官網蒐集整理

賞金獵人計畫 鼓勵資安研究員通報漏洞

Product Security Forum



資料來源：企業官網蒐集整理

企業內部的漏洞探測實驗室

以Panasonic威脅情資平台為例

- Panasonic網路安全實驗室建置威脅情資平台(ASTIRA)
- 將自家IoT設備安裝成蜜罐，刻意使用寬鬆的設定值吸引駭客攻擊
- 自動化誘捕IoT惡意程式並進行動態與靜態分析
- 將分析結果提供予開發部門參考，據以改善產品資安

資料來源：CYBERSEC 2024 資料 經原作者同意引用

導入資安法規認證: D-Link 的例子

* 感謝 D-LINK 提供資料

2013 通過TRUSTe 認證

2014 導入認證ISO 27001

2016 導入 BSIMM V7，隔年通過稽核

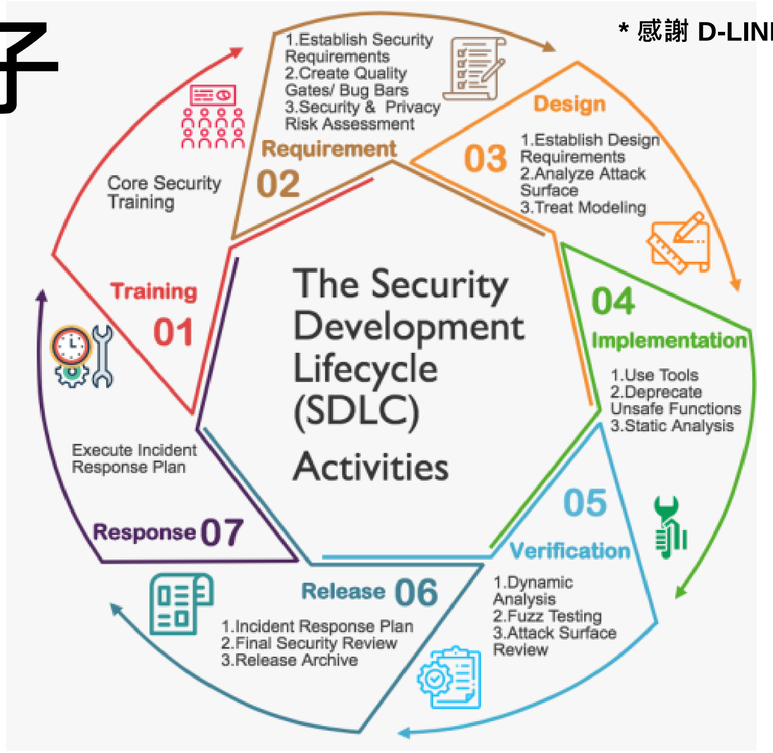
2018 導入 IEC 62443-4-1

2020 取得認證 IEC62443-4-1

2021 取得認證 BS 10012（GDPR）

2023 全台網通第一取得EN303645 認證

2025 導入歐盟 CE RED-DA 法規 EN 18031，4月取證



IEC 62443-4-1 是目前各國安規必要參考的重要法之一，例如EN 303645就是基本要求的版本，而新加坡CSA的IOT法規跟EN 303645重疊性又很高。基本上，IEC 62443-4-1就是一個完整版的SSDLC的流程規範。

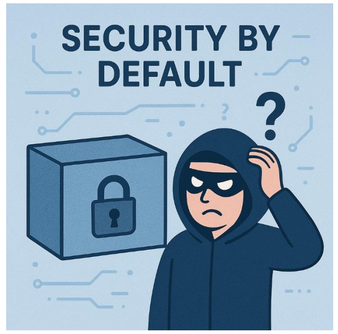
歐盟委員會 無線電設備指令授權法案(RED-DA；Radio Equipment Directive - Delegated Act)，並將於2025年8月生效。該法案要求必須遵守 RED(2014/53/EU)第3.3條(d)(e)(f)的資安要求，旨在確保此類設備具有更高水準的網路安全.

D-Link

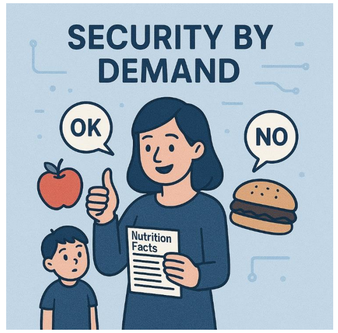
資安院推動產品資安的計劃

資安院推動 ICT 產品資安的行動計劃

- 推動 Security by Design 資安設計教育訓練



- 推廣 P-SIRT 及產品漏洞獵捕計畫



- 研究並推進台灣電子產品資安法規與標章 接軌國際

齊力提升資安
建立產業共識

培育產品資安人才 做好 Security by Design

- 以資安人才角色類別出發，參考美國NICE Framework中產品資安人才相關角色，結合職能研析、課綱與鑑測開發與實務專家經驗，開發2類產品資安人才培訓機制：
  - 安全軟體開發工程師(Secure Software Development)
  - 軟體安全檢測工程師(Software Security Assessment)

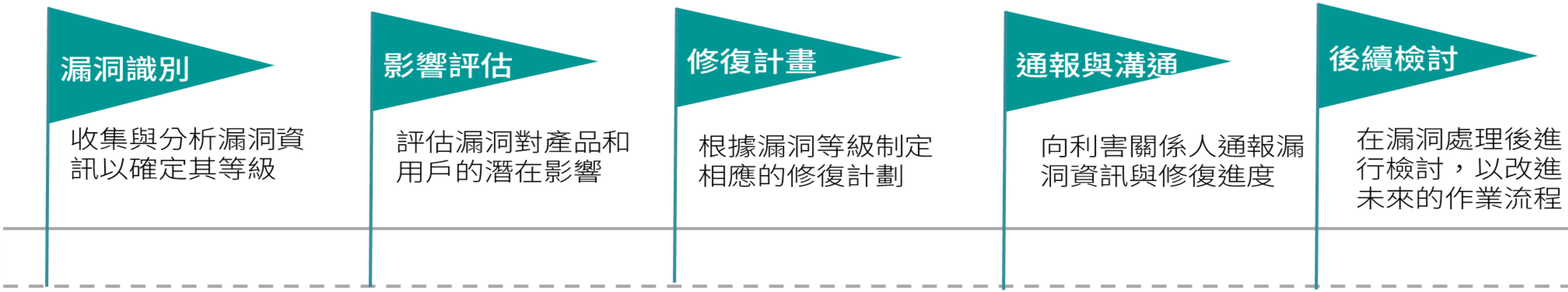
	定義角色職能	設計課綱教材	發展鑑測方式	彙集共識
工作任務	• 研析框架職能(任務、知識、技能)，減少用詞模糊性、使用控制詞彙與調整譯文語意 • 舉辦專家諮詢工作坊，經真實世界實務專家覆核人才職能 • 以疊智精神針對覆核結果外部書審	• 以2類人才職能參考基準框架為準，轉化為課綱與課程主題，並與人才所須具備之知識、技能對齊	• 運用職能框架中的職能元素與課綱內容，開發多元評核人才方式與項目建議，以驗測其知識與技能表現 • 訂定相關能力指標、評分量表與判定基準	• 召集各界產品資安專家辦理課程架構共識會議，針對產品資安2類角色之職能課程與培訓鑑測機制進行研討
預期產出	2類人才TKS職能框架	2類人才培訓課綱/教材	2類人才鑑測方法	確立課綱與鑑測方式用以未來培訓運用

推動 PSIRT 機制 確保漏洞即時通報修正更新

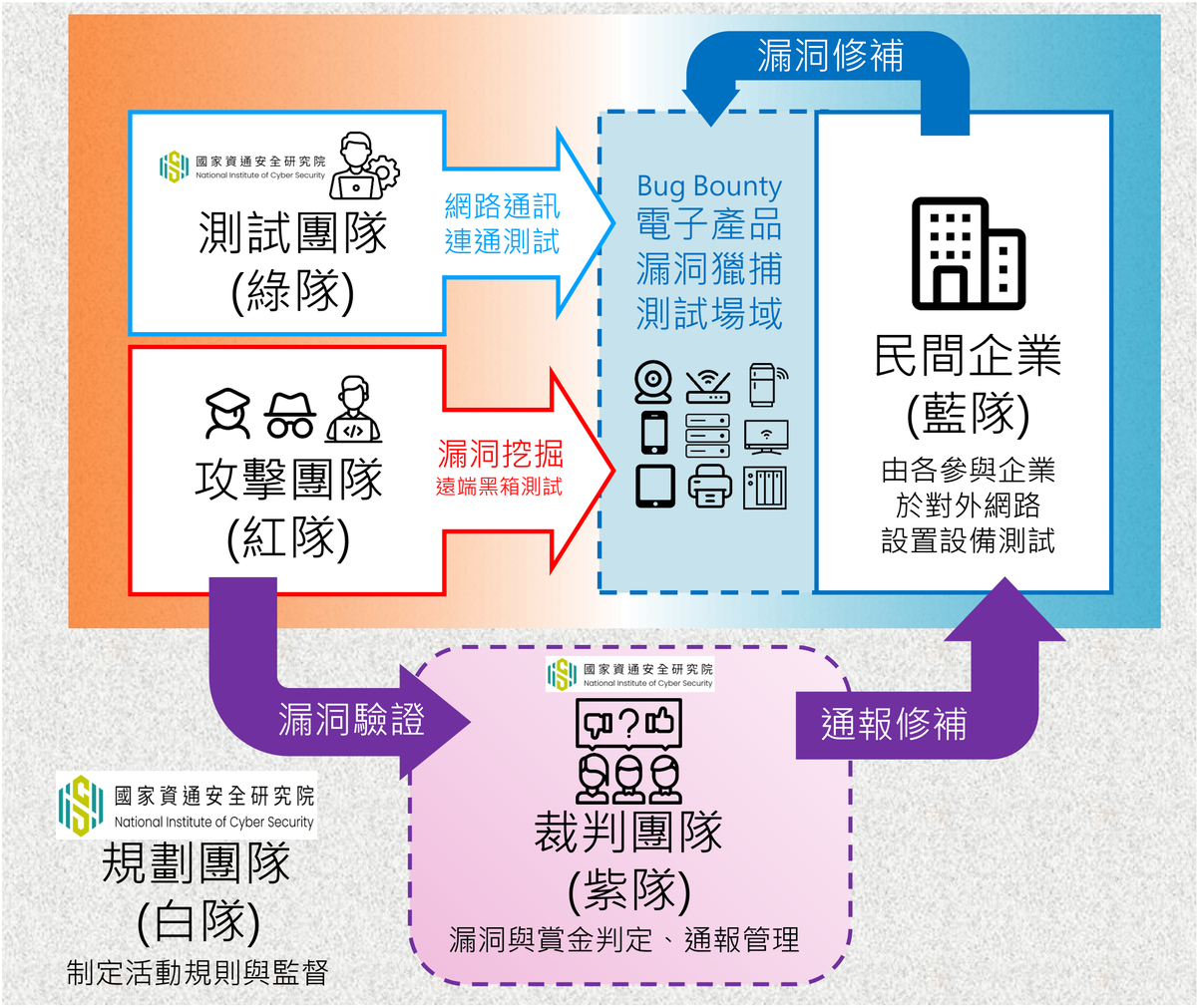
- 透過 TW-CERT 組織，規劃並推動企業成立PSIRT負責產品漏洞管理，建立雙方聯繫管道，確保企業能及時接收、評估、回應並修補產品漏洞，減少資安風險
  - 制定PSIRT guideline文件草案
  - 規劃PSIRT漏洞通報/修補程序
  - 評估PSIRT 納入政府採購規範

推動 PSIRT 機制 確保漏洞即時通報修正更新

- 漏洞處理機制初步規劃方向
  - 建立TWCERT/CC與企業PSIRT間雙向聯繫溝通管道，以利漏洞資訊及時傳遞修補與損害控管
  - 透過管道分享相關情資以利聯防
  - PSIRT自行評估漏洞情況，向TWCERT/CC提出申請CVE編號



台灣 ICT 產品 Bug Bounty 漏洞獵捕計畫



- 資安院擔任公正第三方單位，建立SOP 並擔任裁判以提升公信力
- 邀請國內共契廠商與國內主要資通廠商提供產品為標的物
- 安排管理資安院審查認可之攻擊手進行攻擊演練
- 結合產業場域與教育訓練，並與政策對接(如PSIRT機制推廣)

○ 白隊(規劃者)：制定活動規則、監督活動進行

● 紅隊(攻擊者)：挖掘設備漏洞，模擬真實攻擊

● 藍隊(建置者)：建置測試場域、提供賞金、修補漏洞

● 綠隊(維運者)：確保漏洞獵捕測試場域設備可用性

● 紫隊(協調者)：驗證與評估漏洞，判定賞金與通報

各類 Bounty Program 機制比較表

項目	HackerOne	BugCrowd	ZDI (Zero Day Initiative)	資安院Bounty Program
平台特點	Bug Bounty	Bug Bounty	Bug Bounty，僅提供漏洞回報機制，不開放雙向互動	除Bug Bounty外，結合產業場域與教育訓練，並與政策對接(如PSIRT機制推廣)
平台性質	商業平台	商業平台	趨勢主導的漏洞回報計畫	非營利、政府第三方角色
標的物取得	平台依駭客分級指派對應場域	平台依駭客分級指派對應場域	駭客自行尋找標的	由廠商提供受測標的
駭客角色	駭客主動參與	駭客主動參與	專家駭客主動提報給ZDI	召集白帽駭客、資格審核
回報對象	回報給廠商	回報給廠商	回報給ZDI，由ZDI通知廠商	回報給資安院，再轉交廠商
獎金來源	廠商提供	廠商提供	ZDI(趨勢科技)出資給回報者	廠商提供
回報流程	駭客 → 廠商 → 審核回應	駭客 → 廠商 → 審核回應	駭客 → ZDI → 廠商 → 修補	駭客 → 資安院 → 廠商 → 修補
技術審查	廠商自行處理	BugCrowd可協助	ZDI技術團隊審查	資安院技術團隊(紫隊)審查
媒合駭客與企業	是(雙方直接溝通)	是(雙方直接溝通)	否(由ZDI中介處理)	是(資安院扮演丙方媒介)
公開性	可建立名人堂增加曝光度	可建立名人堂增加曝光度	不一定署名，偏低調	公開，並串接CVE審核作業
在地化	無(國外平台)	無(國外平台)	無(國外平台)	國內廠商

協助推廣與接軌國際產品資安法規

全球產品資安要求正變得更具約束力，廠商不只要設計安全產品，還要負責產品生命週期，包括更新、通報、回應漏洞，而且法規適用範圍擴大，供應鏈包括中小型設備商都「有義務」

	歐盟 《網路韌性法》（CRA）	英國 《產品安全和電信基礎設施法案》（PSTI）	美國 《物聯網網路安全法》
適用產品	含數位元素的產品*	消費性連網產品**	聯邦採購用 IoT 裝置***
市場範圍	歐盟市場內銷售的連網產品	在英國市場銷售的連網產品	聯邦政府採購使用的 IoT 裝置
規範對象及其責任	**只要參與產品流通就須配合 CRA 的安全與漏洞處理要求** • **製造商責任最重**，產品的設計安全、風險控管、更新支援與漏洞處理機制都須從源頭承擔法規要求 • **進口商與經銷商**則要「把關有CE標章」與「通報漏洞」確保市場流通產品的安全 • 如進口或經銷商**「修改或掛自己品牌，責任等同製造商** • **製造商**是從頭到尾都要負責的角色，從安全設計 → 產品合規 → 公告支援年限→ 主動通報→ 保存紀錄 → 漏洞修補全包 • **進口商與經銷商**須確保產品附有合規聲明（SoC），發現問題要通報供應商與政府機關 • 如進口或經銷商**「修改或掛自己品牌」責任等同製造商** • **聯邦政府機構**責任最重，需確保採購設備符合 NIST 安全標準、建立並執行漏洞通報與協調流程 • **承包商與其供應商**負有「間接責任」，但須提供符合 NIST 標準的產品（才能參與聯邦採購）、建立漏洞揭露與通報機制；若產品不合規，會失去採購合約資格	

資料來源：資安院整理。
註：*含數位元素之產品包括硬體、軟體、IoT裝置；**PSIT包括智慧家電、智慧手機、遊戲主機、連網音響或玩具等；***泛指所有能連網且具備感知、處理、資料傳輸能力之設備。

接軌國際產品資安法規：以漏洞通報為例

歐盟《網路韌性法》規範最嚴格、要求廠商發現漏洞要在時限內主動通報；英國著重製造商提供通報管道，美國則規定了指引。國際法規力道各有不同，但漏洞通報機制已成為全球產品資安法規的標配！

	歐盟 《網路韌性法》	英國 《產品安全和電信基礎設施法案》
漏洞通報規範	**製造商**就已遭實際利用(actively exploited)的漏洞，須**採取下列通報措施**： • 即時通知**受影響之使用者**並提供可用的緩解措施 • 於一定時程(24hrs、72hrs、採取矯正措施後14日內)，分別以早期預警通知、漏洞通知以及最終報告的形式，分階段向單一通報平台(含CSIRT與ENISA)	**製造商**須提供產品資安問題**通報方式的相關資訊**，包含： • 至少一個聯繫管道 • 相關時程，說明通報確認以及進度更新的時程
漏洞通報是否為強制性	☑	☑
評析	強制要求製造商於一定時限內通報漏洞，監理力度高	有鑑於製造商需要建立通報之聯繫管道，故此規定具推動製造商建立PSIRT之效力

資料來源：資安院整理。

產品資安規範推動與國際合作(相互承認協議)

我國除密切關注各國實體規範外，也觀察到國際發展產品資安標章或認驗證機制之趨勢，將尋求透過與他國對話，商討、制定適宜之產品資安標準，並尋求簽訂MoU和MRA等方式，進行國際合作，共同建立產品資安生態

英國

英國PSTI雖未有產品資安標章與認驗證，但曾研議推動相關制度；PSTI亦採用ETSI EN303645為基礎

歐盟

- 「資安認證框架」 (Cybersecurity Certification Framework) ：由歐盟網路安全局(ENISA)監督，分為EUCC、EUCS以及EU5G三個計畫
- 歐盟《韌性法》得考量第三國的技術發展與符合性評估方式，與第三國簽署MRA

美國

「美國網路信任標章」（U.S. Cyber Trust Mark）

- 由聯邦通訊委員會(FCC)監督
- 未來可能與歐盟《韌性法》相互承認，惟就此尚未見公開具體規劃

韓國

「IoT資安認證」(CIC)

- 由網路振興院(KISA)監督，分為3級
- 與新加坡簽署MRA；與德國簽署MRA意向書

資安院將協助相關機關推動與國際接軌之產品資安標章及認驗證機制

我國前已有物聯網資安標章機制，如台灣資通產業標準協會「物聯網資安標章驗證證書」（經濟部與NCC）及行動應用資安聯盟「物聯網資安驗證合格證書」，**未來將參考既有之基礎及國際發展，推動得以與國際對接之產品資安標章與認驗證機制**

日本

「Japan Cyber STAR」(JC-STAR)

- 由獨立行政法人情報處理推進機構(IPA)監督並分為4級，規劃與他國簽署MRA

新加坡

「資安標章計畫」(Cybersecurity Labelling Scheme)

- 由新加坡網路安全局(CSA)監督，分為4級
- 已與芬蘭簽署MoU並與德國、韓國簽署MRA

資料來源：資安院整理。

*註：相互承認協議(Mutual Recognition Arrangement, MRA)指於國內取得產品測試或驗證結果的業者，可直接獲得對方國家政府的承認，不須進行額外的測試或驗證。其效力是促進產業之國際貿易，尤其減輕企業在技術標準和測試認證方面之成本，實質有助減少貿易壁壘並促進該國之產業發展

形成產業共識 齊力推動產品資安

與台灣資安主管聯盟全面合作

*特別感謝聯盟 會長 ASUS 金慶柏資安長
及副會長 ZYXEL 游政卿資安長

台灣資安主管聯盟
Taiwan Chief Information Security Officer Alliance

聯盟願景及推動目標

* 感謝聯盟提供資料

願　景　提升台灣產業資安韌性，促使企業永續發展

目標1：專業資安人才培訓整備

透過資安人才培訓機制，辦理資安長研習課程、產學交流、企業實習、人才媒合等活動，並建置虛實學習平台，促使企業完善專業資安人才。

目標2：供應鏈資安韌性建立

運作供應鏈資安機制，辦理資安個案、資安治理分享活動，及資安威脅情資分析與示警，強化產業資安韌性。

目標3：資安管理制度合規建立

辦理政策法規宣導、法遵諮詢服務等活動，協助企業建立資安管理制度符合相關規範。

目標4：重大資安事件應變協助

因應資安事件發生之應變諮詢、協處，並發展事前示警情資服務。

目標5：資安服務資源鏈結

結合資安專業服務資源，辦理資安事件個案研析、資安治理顧問諮詢、資安解決方案引介等，有效排除資安問題。

目標6：推動產品安全

強化產品開發與供應鏈安全管理，落實安全標準與檢測機制，提升產品安全性與市場信任度。

台灣資安主管聯盟
Taiwan Chief Information Security Officer Alliance

* 感謝聯盟提供資料

產品安全及技術委員會

- 本委員會致力打造「產官學協作平台」，匯聚各界專家，共同制定並推動符合國際標準的產品安全與資安規範
- 擔任 CISO 聯盟與政府政策間的橋樑，促進跨領域對話，整合產業資源，提供企業實務指引，全面提升產品安全，打造可信賴的數位生態
- 採「季度會議制」運作，每季召開全體會議，由產業、政府、學界與顧問組成的 18 位專家小組推動重點議題

委員會構想與推動方向

* 感謝聯盟提供資料

- 構想：建立產官研合作平台，整合資源與專業知識，共同因應全球產品安全與資安規範變動帶來的挑戰與機遇
- 四大工作方向

遵循國際產品資安法規：掌握歐盟 CRA、RED、英國 PSTI 等法規

推動 PSIRT：建立產品安全事件應變團隊，統一的漏洞應變機制

實施 Bug Bounty Program：實施安全漏洞懸賞計畫，強化市場信任

導入 SBOM：建立軟體物料清單標準流程，提升供應鏈軟體安全

四、推動 SBOM (軟體物料清單)

* 感謝聯盟提供資料

- **目標：建立完整軟體組件透明度文件，確保產品符合國際資安法規，強化台灣產業在全球供應鏈的競爭地位**

協助企業導入 SBOM

確保產品供應鏈軟體組件的透明化，符合國際法規要求（如美國 Cyber Trust Mark、歐盟 CRA 等），提升合規性與信任度

建立 SBOM 監控機制

強化供應鏈安全管理，有效降低供應鏈攻擊風險，全面提升產品的安全性

推動 SBOM 實務落地

協助企業在產品開發與維運過程中落實 SBOM，增強市場信任度與競爭力

做好產品資安

國家安全

廠商賺錢

Bounty 議題
PSIRT 機制調查

產品資安問卷

TEAM CYBERSECURITY