國家資通安全研究院
National Institute of Cyber Security

產品資安漏洞獵捕計畫

抓漏洞・強資安・護產業

國家資通安全研究院

114/9/24 公開文件

沒有資安，就沒有產品安全

資安不是成本，而是進入市場的門票

市場門檻提高 | 無資安測試，難過歐美認證
出口受阻，訂單流失

修補成本加倍 | 上市後爆漏洞，修補成本高
比設計階段高10倍

品牌形象受損 | 一個漏洞，就可能大規模召回
消費者信任重挫

企業痛點・想做資安卻卡關

資安規範複雜

研發團隊專注功能開發
對國際資安規範不熟悉

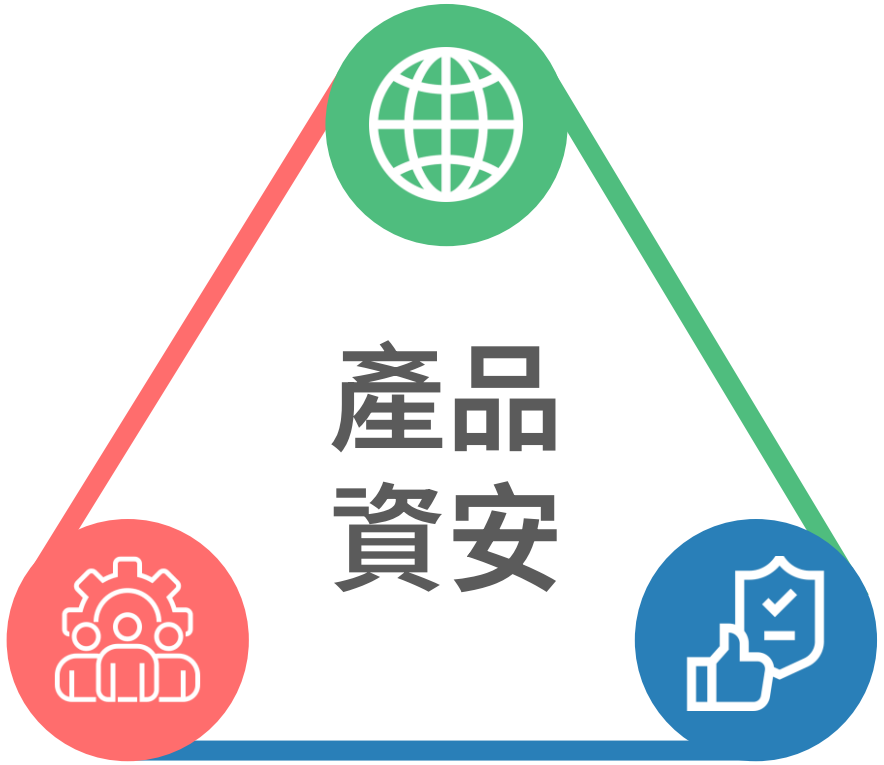
測試能量有限

外部紅隊資源昂貴
企業內部缺乏測試人力

品牌認可有限

企業單打獨鬥
難獲市場或政府認可

產品資安三大支柱



① 接軌國際資安標準
符合歐美規範・降低風險

② 協助企業測試產品
無紅隊資源・也能測試

③ 建立台灣信任形象
安全履歷・品牌信任

產品資安三大破口

電子產品
生命週期

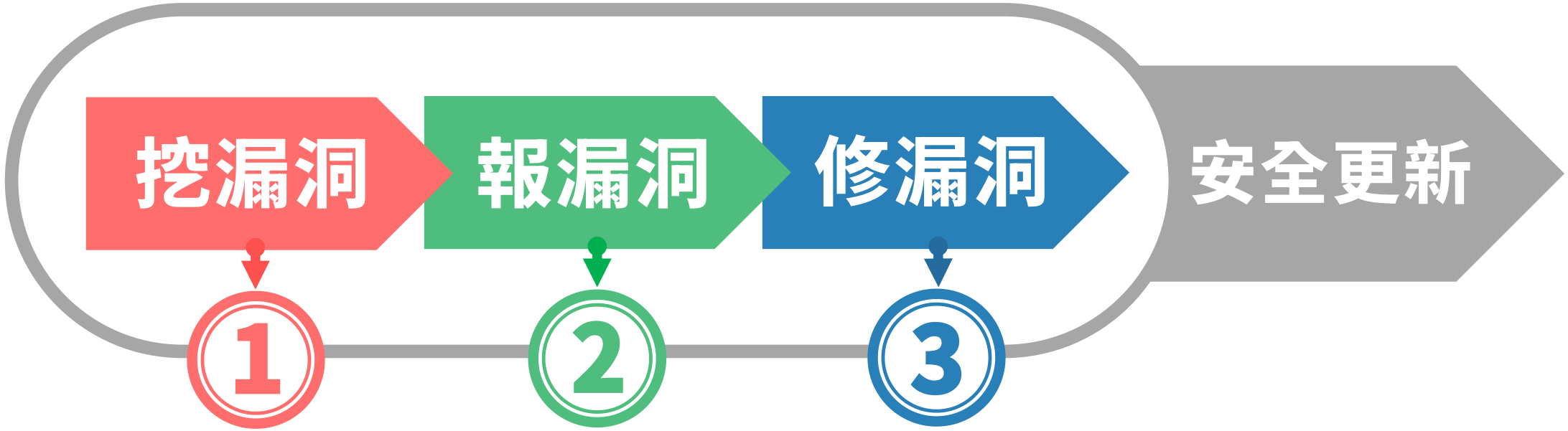
① 設計缺乏資安，出廠即帶漏洞

② 產品缺乏測試，難以察覺漏洞

③ 通報缺乏誘因，無人處理漏洞

挖・報・修・漏洞有解

挖得到・報得出・修得好
產品資安才牢靠



上市前中後・資安帶著走

設計重安全・出廠就防護・合規最安心

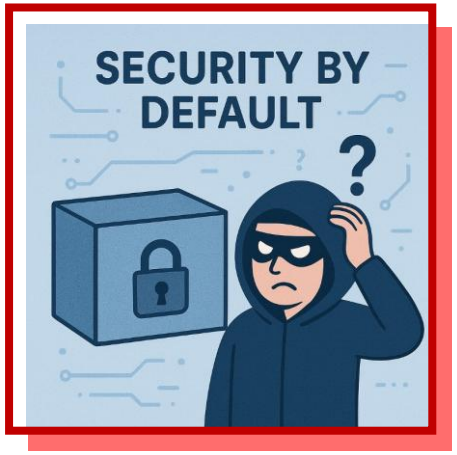
產品上市前

設計即安全

發展人才職能
設計有信心

產品上市中

出廠即安全



推動 PSIRT・漏洞獵捕
產品更安心

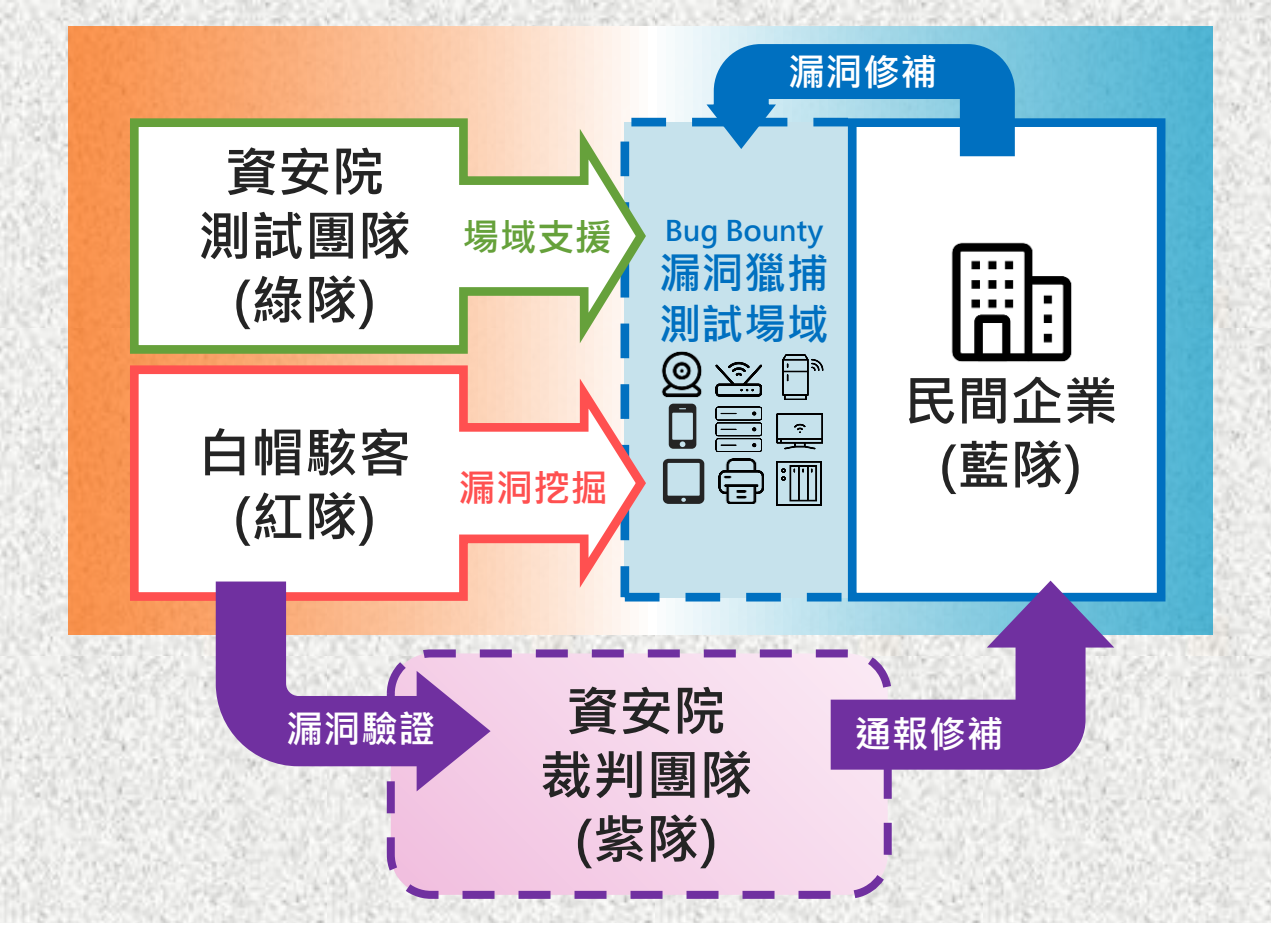
產品上市後

合規也安全

推動法制規範
信任更升級

註:本頁圖片為 Chatgpt 模型生成

漏洞獵捕機制・多方協同合作



白帽挖・廠商補
資安院來驗又來顧

白帽駭客 挖掘漏洞

企業廠商 修補漏洞

資安院 驗證漏洞

資安院 支援場域

獎金驅動挖掘・漏洞修補到位

企業廠商 設置賞金・鼓勵 白帽駭客 挖掘漏洞

賞金基準參考對照表

企業設置**總獎金**・確保預算可控

嚴重	等級(9.0-10.0)	$100,000
高	等級(7.0-8.9)	$30,000
中	等級(4.0-6.9)	$10,000
低	等級(0.1-3.9)	$3,000

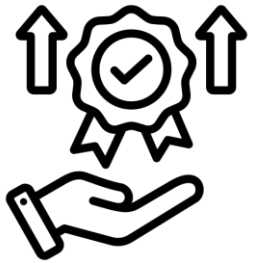
註：風險分數為CVSS v3.1，活動前參考對照表設置獎金

自定特定嚴重風險情境

網路滲透		路由器 遠端操控・惡意植入
資料破壞		NAS 備份失效・資料刪改
隱私失守		安控/攝影機 影像外洩・畫面竄改

藍隊參與效益 × 三大亮點

漏洞提早抓・通報不延誤・品牌最可靠



產品更安全

早測早安心
出廠有保障

通報更順暢

內部通報快
修補更即時

品牌更可靠

資安有投入
市場更信任

紅隊參與效益 × 三大亮點

動機更強烈・成就更清晰・認可更專業

獎金更誘人

漏洞有價值
挖掘最高獎10萬

成就更清晰

登錄名人堂
展現技術力

認證更專業

申請CVE漏洞編號
國際都認可

資安到位・國家安全・廠商賺錢

抓漏洞發獎金・顧資安接大單

漏洞獵捕
活動辦法

藍隊報名
114/9/25~
114/10/27

活動獎金揭曉
114/10/28~
114/10/31

紅隊報名
114/11/1~
115/1/25

活動正式開始
114/12/1~
115/1/31

活動採報名制・掃描QR CODE了解更多

現在就報！強化資安！信任加分不中斷