第二屆產品資安漏洞獵捕活動簡介

國家資通安全研究院 檢測防禦中心

115年6月30日

大綱

01　首屆執行成果

02　第二屆活動規劃說明

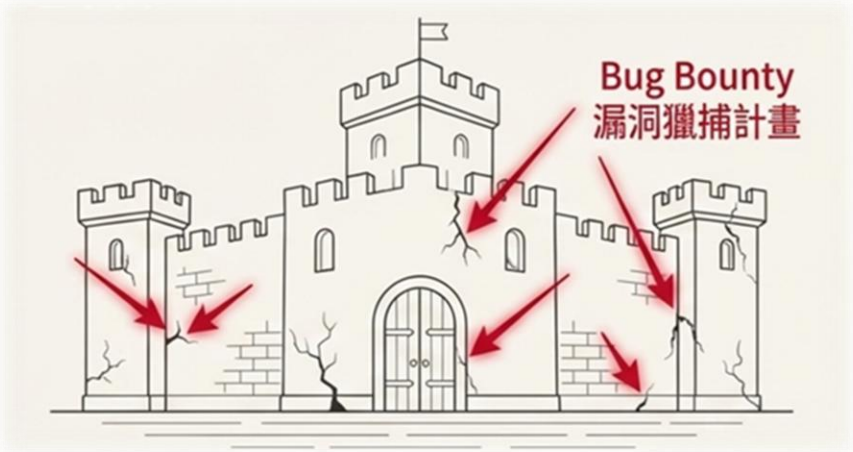
01 首屆執行成果

已完成標準檢測，真的就安全了嗎？

上市前-標準測試

合規性　被動防禦　照圖檢查

逐項檢查大門與主結構
確保符合設計藍圖安全合規的要求



持續性-漏洞獵捕

韌性　主動挖掘　尋找縫隙

產品持續營運期間，邀請經驗老道的老師傅
尋找設計圖看不到的隱性縫隙與瑕疵

首屆產品資安漏洞獵捕活動

114年12月正式開始・活動圓滿完成

資料來源：漏洞獵捕活動網站

資安院首屆漏洞獵捕找出20項有效漏洞　助攻廠商提前修補產品風險

2026/4/27 下午 02:05:45

數位發展部資通安全署指導國家資通安全研究院辦理首屆「產品資安漏洞獵捕活動」已圓滿結束，資安院今(27)日公布首屆「產品資安漏洞獵捕活動」成果，活動共集結11家國內指標性資通訊大廠、179 位本土資安研究員，針對網通設備、網路儲存設備（Network Attached Storage, NAS）及工業網通等 20 組產品進行測試，最終確認20項有效漏洞，其中包含3項嚴重等級與6項高風險漏洞。結果顯示，產品在上市前若能透過外部測試驗證，有助提前發現潛在風險、縮短修補時程，進一步強化整體產品安全。

找出20 項有效漏洞(含3 項嚴重等級)，發出新台幣53.9 萬元獎金，成功協助國內11家 網通科技大廠在產品上市前修補潛在風險、提升MIT 產品競爭力。

漏洞獵捕試辦成果：產業與社群共同參與

社群參與

179 位

本土資安研究員參與

企業投入

11 家

指標品牌廠商參與

機制驗證

20 組

設備投入驗證

研究員挖掘 → 企業修補 → 第三方驗證

打造產品資安正向循環

推動「被動防禦」邁向「主動賦能」

全面提升產品資安韌性

主動發現風險

補足弱點掃描盲點
提前發現安全漏洞

資安能力提升

強化安全設計能力
建立漏洞應變能力

制度生態建構

建立漏洞揭露機制
串聯產業與社群

滿意度實證：參與之藍隊廠商 100% 表示願意再次參與後續計畫

02 第二屆活動規劃說明

第二屆漏洞獵捕活動・推動重點

由試辦邁向制度化，聚焦軟體供應鏈資安

- **從硬體走向軟體**｜聚焦高風險供應鏈
- **從場域走向場景**｜導入政府採購實務
- **從活動走向機制**｜建立持續運作模式

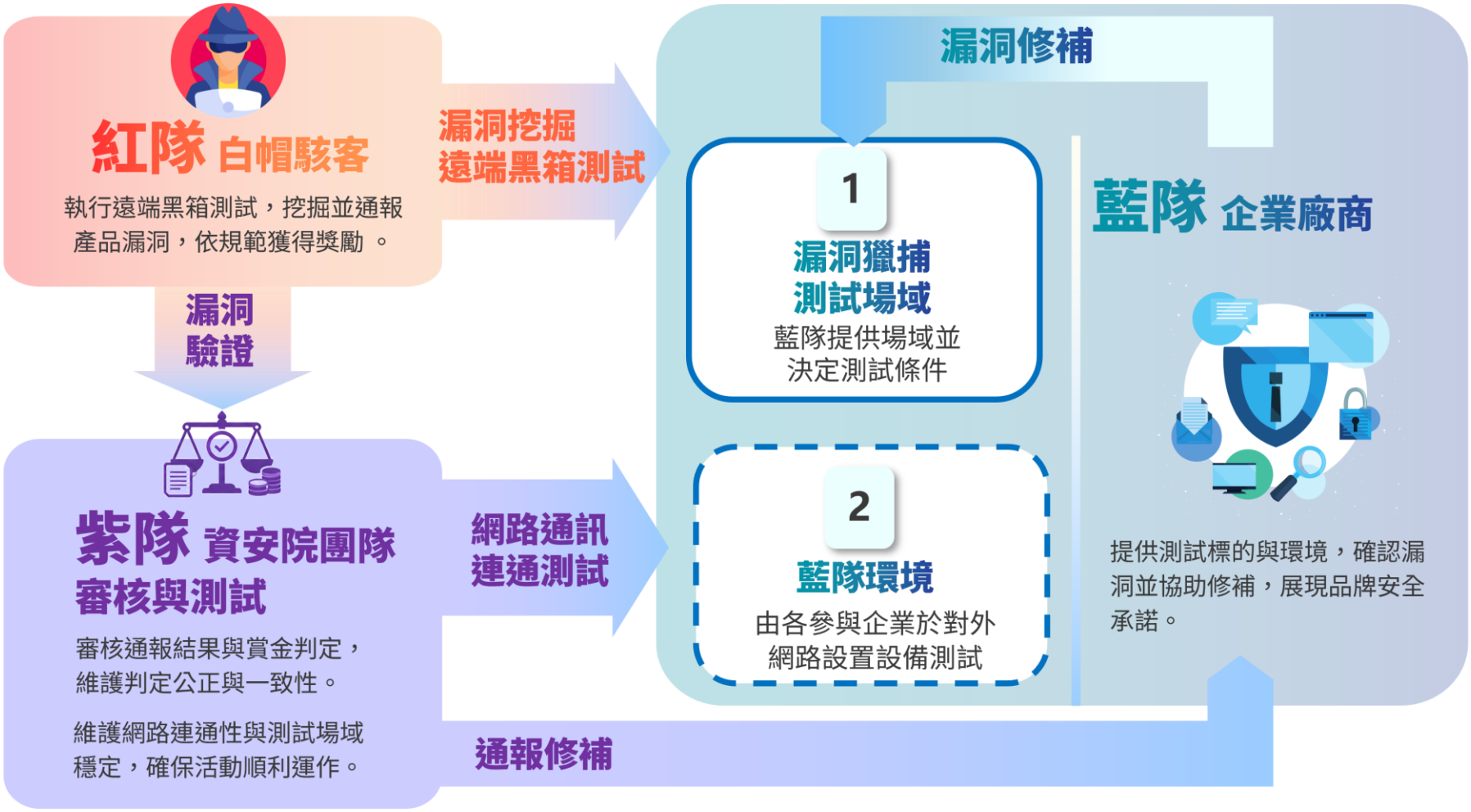
階段性任務躍升：從硬體轉向核心軟體

	第一屆漏洞獵捕活動	第二屆漏洞獵捕活動
活動時間	114年12月~115年1月	預計115年**9月~10月** 預計7月起於TWCERT/CC網站公告受理報名
總獎金池	720萬元	預計募集 **800萬元** 由參與廠商提供
目標領域	硬體與網通設備	**軟體**供應鏈安全驗證
測試標的	工業網通設備、 NAS、網通設備	**政府機關常用軟體** 高使用、高風險、關鍵資安軟體(如VANS、GCB等)
藍隊數量	11家 國內硬體製造廠商	**邀請廠商** + **開放報名**

因應政府採購需求演進
全面檢視務實環境中的
軟體供應鏈安全

鼓勵運用 AI 輔助
挖掘漏洞
並以可驗證結果
作為認定依據

第二屆產品資安漏洞漏洞獵捕活動合作模式



第二屆產品資安漏洞獵捕活動時程規劃

活動 網站公告	藍隊 報名	公告 獎金	紅隊 報名	活動 正式開始
115/6/30	115/7/1~8/31	115/8/31~9/1	115/9/1~9/30	115/10/1~11/30

測試環境建置作業整備 115/7/1~9/30

軟體產品測試情境規劃

產品類型	測試情境規劃	測試環境/正式環境	紅隊可知的資訊
地端軟體	廠商部署伺服器到資安院測試環境，並提供使用手冊與測試帳號供資安院確認可用性	●資安院測試環境 ●廠商提供測試帳號	1.測試網站入口點 2.測試帳號(可分階段提供) 3.使用手冊
地端軟體含Agent	廠商部署伺服器到資安院測試環境，並提供使用手冊與測試帳號與Agent供資安院確認可用性	●資安院測試環境 ●廠商提供測試帳號	1.測試網站入口點 2.Agent取得與安裝說明 3.測試帳號(可分階段提供) 4.使用手冊
SaaS服務	廠商提供使用手冊與測試帳號供資安院確認可用性	●廠商提供環境(正式或clone) ●廠商提供測試帳號	1.網站入口點 2.測試帳號或帳號命名規則(無需綁定信用卡) 3.使用手冊
APP	廠商提供安裝與使用手冊與測試帳號供資安院確認可用性	●廠商提供環境(正式或clone) ●手機下載APP進行測試(是否可用模擬器待確認)	1.網站入口點 2.測試帳號或帳號命名規則 3.使用手冊
網站 (如e-commerce)	對上線服務中的網站直接測試	●廠商提供環境(正式或clone)	1.網站入口點 2.測試帳號或帳號命名規則 3.使用手冊

若為資安院測試環境，待詢問廠商的環境需求

賞金管理機制

透過合理獎勵機制與嚴謹漏洞管理流程，鼓勵高品質漏洞回報，協助企業提升產品資安韌性

不予獎勵情形
- 非本活動範圍內項目
- 無法重現或資訊不足
- 造成系統中斷或破壞
- 違反活動規範行為
- 重複或已知漏洞

1. 風險賞金基準對照表

風險等級	CVSS v4.0	賞金
嚴重	9.0–10.0	NT$100,000
高	7.0–8.9	NT$30,000
中	4.0–6.9	NT$10,000
低	0.1–3.9	NT$3,000

800萬元

第二屆目標獎金池總額

2. 獎勵原則與認定標準

（一）以影響程度為導向

依漏洞對機密性、完整性及可用性之影響程度進行分級與獎勵。

（二）需可驗證且可重現

漏洞需提供足夠資訊、驗證步驟及PoC，以利主辦單位與廠商確認。

（三）最小揭露原則

僅取得足以證明漏洞存在之最小必要資料量，避免過度存取或資料蒐集。

（四）不重複給獎

相同漏洞以最先有效回報者為主，不重複發放獎勵。

活動流程與廠商參與方式

通報收斂・責任清楚・揭露可控

1	2	3	4	5	6	7	8	9	10
廠商確認受測標的	**界定範圍禁止事項**	**場域部署與測試**	**紅隊依規範測試**	**平台通報漏洞**	**資安院初審分級**	**正式通知廠商確認**	**廠商修補與回覆**	**協調揭露獎金核定**	**漏洞修補完成**
廠商報名後，選定測試標的產品	廠商指定 聯絡窗口	準備測試環 境	限定範圍內進行	統一資安院受理	CVSS 評級	廠商協同確認	回報資安院漏洞修補進度與預計完成漏洞修補日期	廠商發放獎金給紅隊研究員，確認成果揭露範圍	資安院協助CVE申請

通報收斂於平台與資安院窗口，廠商不必直接面對多頭聯繫，確保資訊集中、責任清楚、揭露可控

- 事前確認可測試範圍與禁止事項，降低測試過程的商譽風險
- 漏洞由資安院初審後正式通知，指定單一內部聯絡窗口，流程收斂、避免多頭聯繫
- 揭露內容與時程須與資安院協調確認

參與漏洞獵捕・提前發現風險・強化產品資安韌性

提升品牌聲譽

展示企業對安全的承諾，將「負責任揭露」轉化為品牌信賴資產，提升市場競爭力。

PSIRT 實戰演練

在資安院導引下建立漏洞通報與處理 SOP，低成本導入國際級資安治理流程。

早期預警與防範

在黑市利用漏洞前即時掌握並修補，避免動輒數百萬的事故損失與法律罰鍰。

展現產品資安治理能力

透過受控式漏洞獵捕，累積產品安全驗證與修補實績，作為企業對外展現資安治理能力之具體佐證。

公私協力 守護產品資安

誠摯邀請參與漏洞獵捕活動

主辦單位
數位發展部資通安全署
Administration for Cyber Security, moda

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

Made In Taiwan = Make It Trusted

逐步形塑 MIT 為全球信任標誌

主動發現 —— 韌性提升 —— 國際認可

主辦單位
數位發展部資通安全署
Administration for Cyber Security, moda

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