產品資安升級行動
活動簡介

國家資通安全研究院 檢測防禦中心

115年9月1日

大綱

01 漏洞獵捕 從發現產品漏洞到持續管理

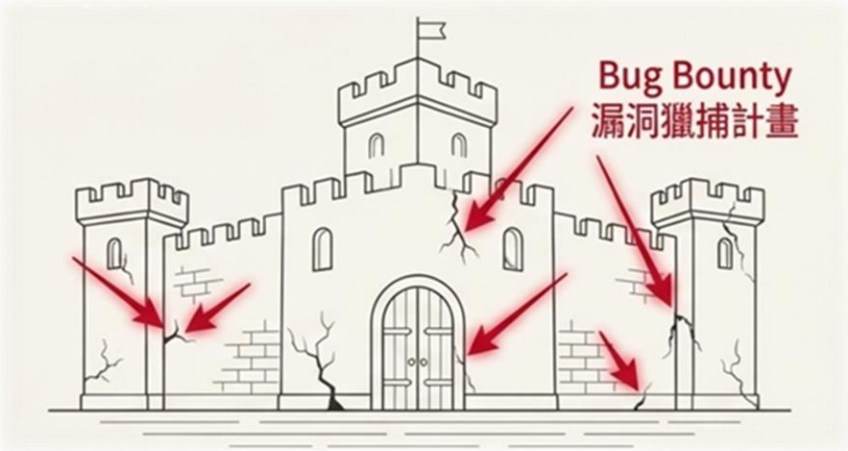
02 產品資安升級行動 第二屆活動合作模式

01 漏洞獵捕

從發現產品漏洞到持續管理

為什麼要做漏洞獵捕？

完成標準檢測，就代表產品持續安全嗎？



上市前-標準測試

合規性　被動防禦　照圖檢查

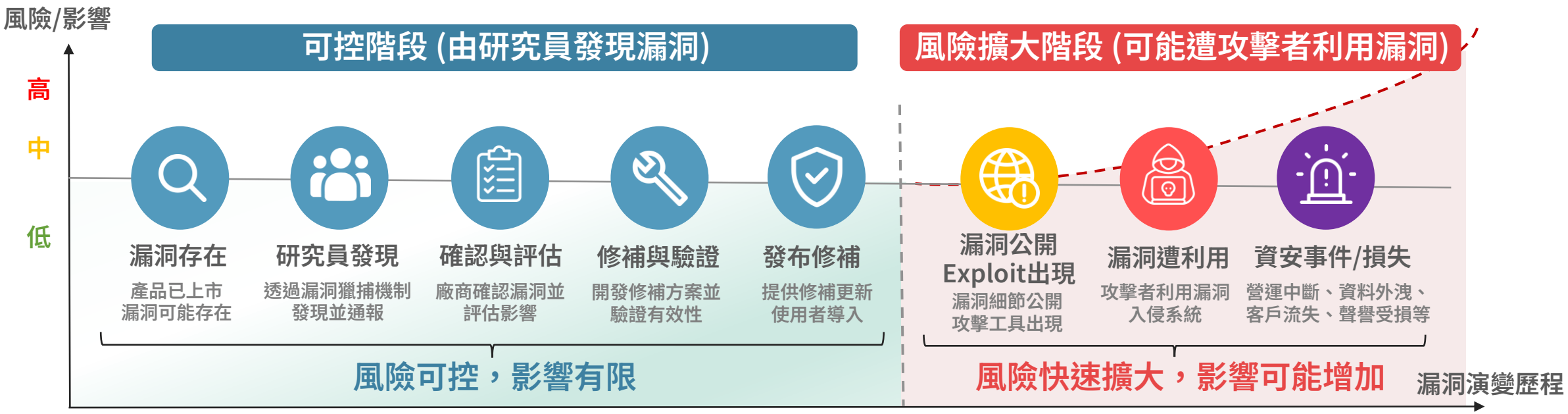
逐項檢查大門與主結構
確保符合設計藍圖安全合規的要求

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

及早發現漏洞，把風險控制在可處理的階段



及早發現漏洞的好處

01 降低漏洞被利用風險

02 爭取漏洞修補時間

03 降低事件衍生影響

延後處理漏洞的風險

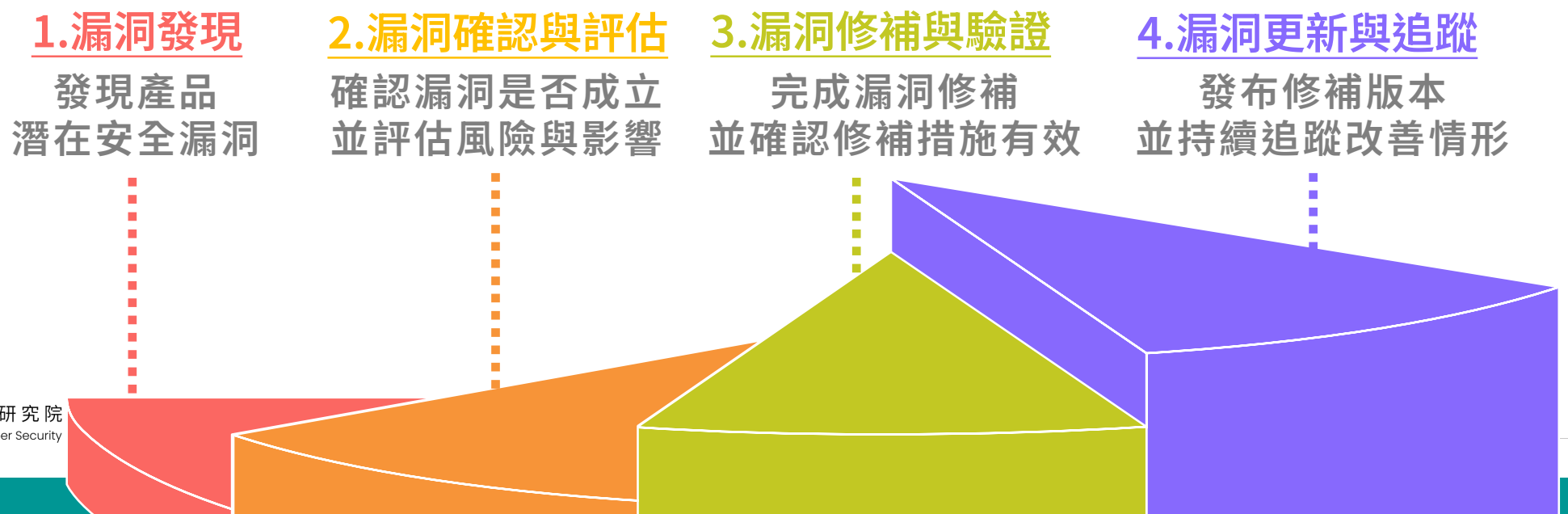
01 漏洞可能遭攻擊利用

02 事件應變壓力增加

03 營運與信任受影響

漏洞獵捕不只找漏洞，更要做好管理與修補

- **漏洞獵捕協助企業建立從「發現漏洞」到「確認與修補」的基本處理機制**
  1. **發現漏洞**：透過研究人員測試，找出產品潛在安全問題
  2. **確認與評估**：確認漏洞是否成立，判斷影響範圍與風險程度
  3. **修補與驗證**：完成漏洞修補，並確認修補措施有效
- **「產品修補與更新」仍由企業負責，並應逐步建立持續性的漏洞管理與追蹤機制**



建立PSIRT機制，讓漏洞管理持續運作

從單次漏洞處理，走向持續產品資安管理

導入產品資安概念前

僅作標準測試
被動防禦
(Compliance)

導入產品資安概念後

產品資安
應變小組
(PSIRT)

企業應變
機制手冊

企業以PSIRT為核心
統籌管理產品漏洞議題
持續改善產品安全

持續性漏洞獵捕
主動風險挖掘
(Resilience)

從漏洞獵捕，建立企業持續的產品資安能力

主動發現產品風險

導入外部研究能量
持續發現產品潛在漏洞

強化漏洞處理能力

建立漏洞接收、確認、
評估、修補與驗證流程

建立產品資安制度

透過PSIRT及漏洞揭露
形成持續改善循環

02 產品資安升級行動

以「產品資安升級行動」為主題
辦理第二屆活動
協助國內軟體業者主動強化產品安全

產品資安升級行動 協助企業導入外部研究能量

外部研究能量

發現未知漏洞

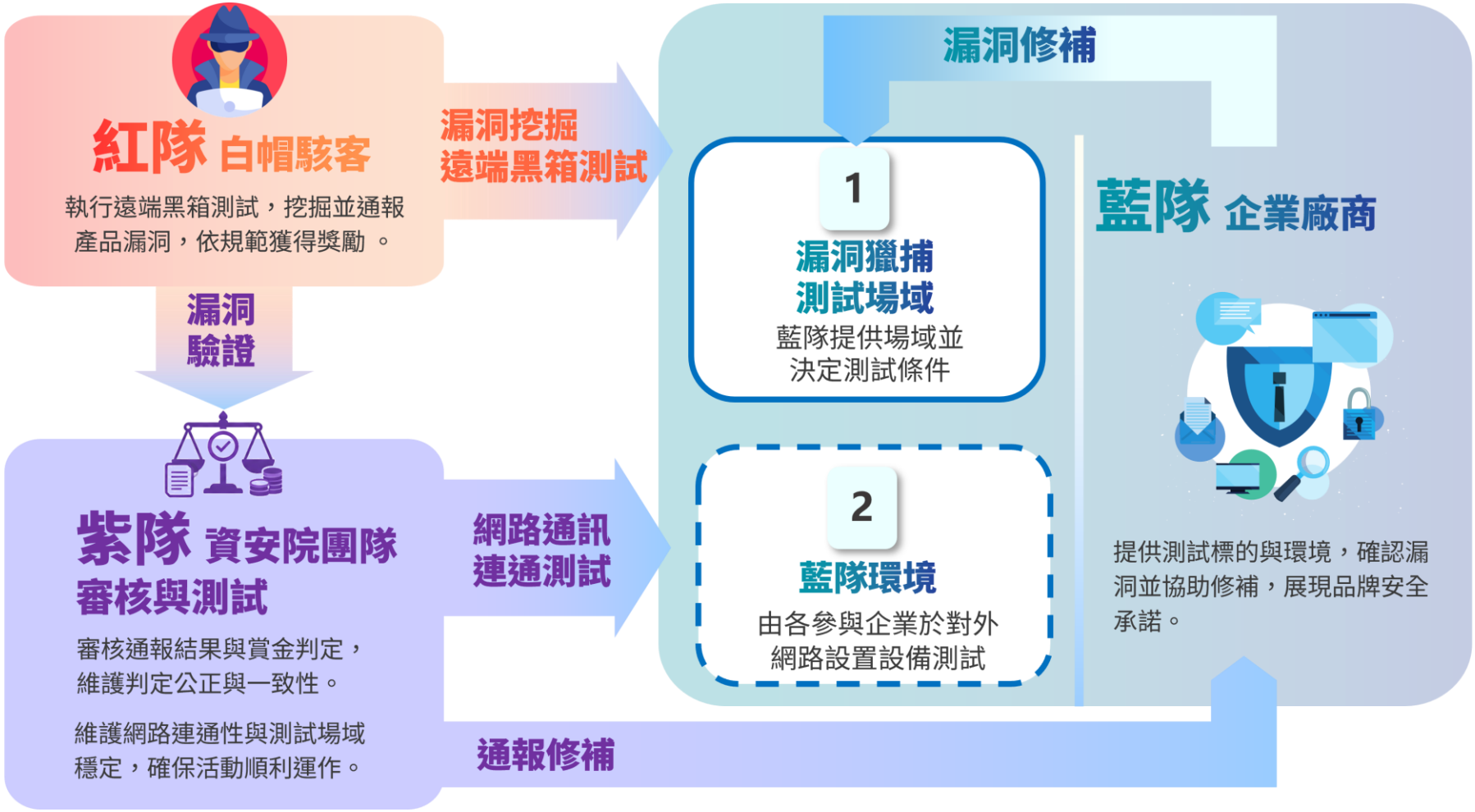
實戰處理經驗

建立漏洞管理能力

降低導入負擔

資安院協助
媒合與管理

產品資安升級行動 合作模式



哪些產品可以參加？

活動受測標的

地端軟體

部署於資安院測試環境

SaaS 服務

正式或複製環境測試

APP

行動應用程式測試

網站服務

如 e-commerce
電子商務

廠商參與準備事項

選定欲參與漏洞獵捕之產品，並確認測試範圍

設置可供研究員測試之環境及必要連線方式

指定技術窗口，協助資訊釐清、漏洞確認及後續修補

依產品特性及預算規劃獎金額度

每家廠商漏洞獎金，前5萬元由資安院支應

獎金池說明

每家廠商漏洞獎金，前5萬元由資安院支應

舉例

資安院加碼	5 萬元
＋	
廠商設定 漏洞獎金額度	50 萬元
‖	
獎金池	55 萬元

漏洞獎金

01 資安院加碼漏洞獎金
漏洞獎金前 5 萬元

02 藍隊廠商漏洞獎金
依有效漏洞核發

資安院加碼獎勵

01 前三名排名獎勵
第1名5萬｜第2名3萬｜第3名2萬

02 AI 工具應用特別獎
擇優 2–3 名，每名 5 萬元
並獲邀分享漏洞獵捕成果與經驗

廠商投入金額可控，資安院再加碼5萬元

✓ 廠商可依預算設定投入獎金額度
✓ 單一漏洞獎金依照活動辦法核發
✓ 經裁定為有效漏洞才核發獎金
✓ 前5萬元漏洞獎金由資安院補助

分工清楚，降低廠商參與負擔

企業(藍隊)負責

測試環境維護
確保研究人員可依規範進行測試

漏洞技術確認
確認漏洞是否成立及影響範圍

漏洞修補改善
規劃修補措施並完成改善

修補成果回覆
提供修補情形及必要驗證資訊

資安院(紫隊)協助

研究人員招募與管理

測試場域與活動管理

漏洞審查與風險分級

紅藍隊溝通協調

漏洞揭露與成果追蹤

從報名到漏洞修補，完成產品資安健檢

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	115/7/1~9/15	115/9/16	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

完成漏洞獵捕，累積可展示的產品資安實績

活動參與證明

Certificate of Participation

茲證明

【公司名稱】

參與數位發展部資通安全署主辦之

產品資安升級行動

於活動期間提供受測產品及技術支援，
配合漏洞驗證、風險評估及修補作業，
共同促進產品資安防護能力提升，
展現對產品安全與供應鏈資安之重視。

特頒此證，以茲證明。

活動名稱　產品資安升級行動
活動期間　115年10月1日至115年11月30日
參與角色　藍隊（產品提供單位）
參與產品　藍隊產品

中 華 民 國 115 年 12 月 01 日

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

完成活動之廠商，可取得活動參與證明及識別徽章
協助廠商向客戶展現產品資安投入與實務參與成果

產品資安升級行動

邀請藍隊企業與紅隊研究員攜手，找出產品漏洞、完成驗證與修補，一起守護軟體供應鏈安全。

找漏洞

驗證

修補

更安全

*此圖為AI輔助製作

立即參與

加入第二屆產品資安漏洞獵捕活動
成為更安全的關鍵力量！

漏洞獵捕
活動辦法

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

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

附件1：軟體產品測試情境

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

附件2：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

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

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

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。