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

產品資安漏洞獵捕計畫
活動辦法(115.1.22 更新)

主辦單位：國家資通安全研究院

活動信箱：bounty@nics.nat.gov.tw

目錄

1. 活動簡介

為強化國內電子產品的資安防護，國家資通安全研究院（NICS，以下簡稱資安院） 將自 114 年 9 月下旬啟動 「產品資安漏洞獵捕計畫」。本活動透過安全且正向的通報與獎勵機制，由廠商（藍隊）提供產品與測試環境，資安專業人員（紅隊）進行漏洞挖掘與回報，雙方在公平透明的機制下攜手合作，於漏洞遭惡意利用前即時完成修補。

透過紅隊與藍隊的協同合作，不僅能確保產品安全與使用者信任，更可推動產業建立完善的資安治理流程。此一合作模式將成為國內產品資安的重要典範，並為我國產品在國際市場上奠定堅實的信譽與競爭優勢。

2. 活動期程

本活動自 114 年 9 月 25 日公告起展開，依序分為藍隊報名、作業整備、紅隊報名及正式活動四個階段，以確保流程完整並維持活動品質。

- 藍隊報名期間：114 年 9 月 25 日至 10 月 27 日（資安院得視實際情況調整）
    - 資安院公告並受理報名，藍隊（電子產品廠商）需於此期間完成報名文件繳交。
- 藍隊作業整備期間：114 年 10 月 28 日至 10 月 31 日
    - 資安院將於此期間完成藍隊報名資料處理與活動準備，並於整備期結束前公告參與名單及獎金池總額，確保活動正式啟動前各項環節就緒。
- 紅隊報名期間： 114 年 11 月 1 日前至 115 年 1 月 25 日。
    - 資安院受理報名，紅隊需於此期間完成報名文件繳交。
    - 報名結果將於 5 個工作天內通知；參與者愈早完成報名並通過審查，可在活動開始時即可率先投入漏洞挖掘，掌握第一手機會，搶先挑戰高額獎金。
- 正式活動期間：114 年 12 月 1 日至 115 年 1 月 31 日
    - 正式舉辦漏洞獵捕活動，進行漏洞測試、通報與審核作業。

3. 參與對象

本活動參與者分為紅隊與藍隊兩大角色。紅隊為資安專業人員，負責進行漏洞挖掘與通報；藍隊則為國內電子產品品牌廠商，提供受測標的、獎勵與獎金。透過紅藍雙方協同合作，得以及早發現並修補產品漏洞，強化我國電子產品資安防護。

3.1 紅隊—白帽駭客、資安專業人員

紅隊成員主要由白帽駭客、資安研究人員及具備漏洞挖掘能力的專業人士組成，採自願性參與方式。紅隊負責針對受測標的進行漏洞測試與通報，並依計畫規範獲得獎勵。

3.1.1 參與資格

- 須具中華民國國籍。
- 須遵守本活動之測試範圍與相關規範。
- 未滿 18 歲者需經法定代理人同意並共同簽署相關文件。
- 參加者若經查核涉及下列情事，資安院得隨時取消其參與資格並得由藍隊追回獎勵與獎金：
    - 違反本活動相關規範。
    - 曾因內亂罪、外患罪、國家安全法、反滲透法、國家情報工作法、國家機密保護法等罪，經法院判決有罪或尚在通緝中。
    - 未經授權，與外國情治單位或大陸、香港、澳門官方機構有聯繫接觸紀錄。
    - 曾受外國或敵對勢力利誘、脅迫，從事不利國家安全或重大利益

之行為。

- 曾因洩密罪或違反安全保密規定，經法院判決或受行政處分。

3.2 藍隊—電子產品品牌廠商

藍隊成員為國內電子產品製造品牌廠商，為本活動的重要合作夥伴。藍隊需提供測試標的、獎勵與獎金，並確保產品於活動期間正常運作。透過參與漏洞獵捕，廠商能提前掌握產品資安風險，展現品牌對安全的承諾，並逐步建立資安治理機制。

3.2.1 參與資格

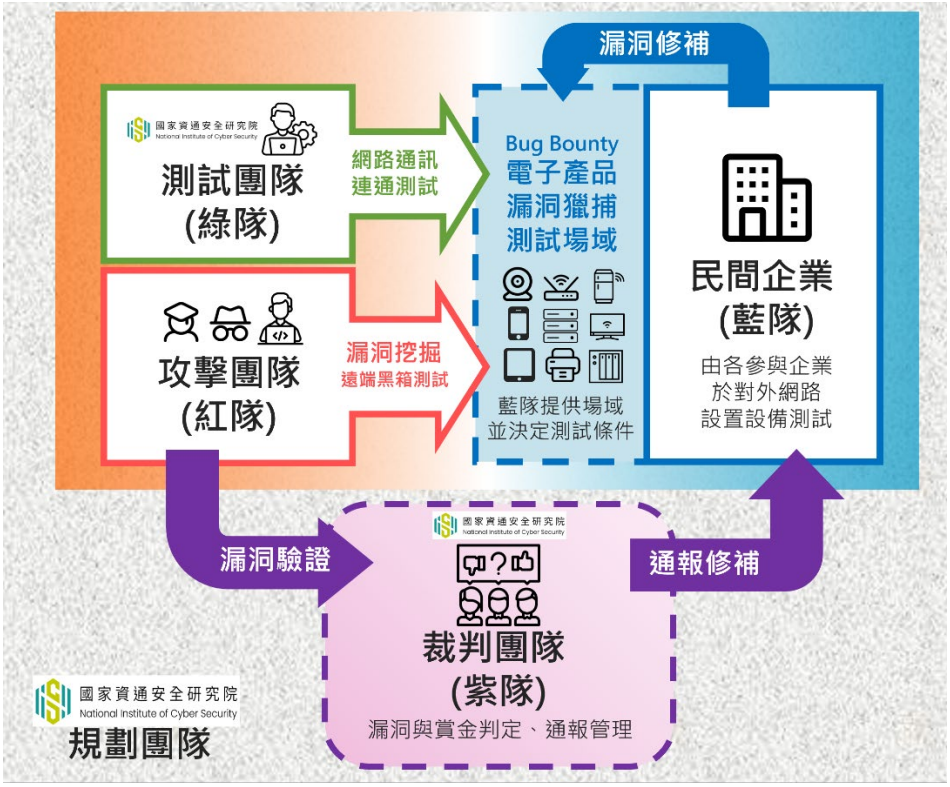
- 須為本國電子產品硬體或相關資通產品製造品牌廠商（如 NAS、網通設備、安控設備）。
- 須遵守本活動規範，並依規定完成漏洞確認並進行修補。

4. 活動辦法與相關流程規範

本活動之執行流程由多方角色共同參與，透過明確分工確保活動順利推進。主要參與角色如下：

- 紅隊（攻擊團隊）：負責執行遠端黑箱測試，挖掘並通報產品潛在漏洞。另依據說明需要，於本文件中將使用「紅隊」、「通報者」或「漏洞挖掘者」代表此角色。
- 藍隊（民間企業）：提供受測標的與必要測試環境，並確認紅隊所通報之漏洞。另依據說明需要，於本文件將使用「藍隊」、「廠商」或「標的提供者」代表此角色。
- 資安院（測試團隊）：負責進行網路通訊與連通性測試，確保受測標的與測試場域可用、穩定，協助活動順利運作。另依據說明需要，於本文件亦將以「綠隊」代表此角色。
- 資安院（裁判團隊）：負責審核、裁定通報結果與獎勵歸屬，確保判定之公正與一致性，另依據說明需要，於本文件亦將以「紫隊」代表此角色。
- 資安院（規劃團隊）：統籌計畫規範與作業制度，負責公告、受理與流程管理。

各角色於活動中之互動與責任分工如下圖所示：



本圖示意紅隊透過遠端測試進行漏洞挖掘，通報後交由藍隊確認，紫隊則負責審核與最終裁定。規劃團隊則提供制度規範與流程設計，確保整體運作透明與可追溯。

4.1 時程規範

本活動規範所稱日（天）數，依以下方式計算：

- 除另有說明外，係以工作天計算。
- 以日曆天計算者，工作天、依行政院人事行政總處所公告認定之放假日及全國性選舉投票日及行政院所屬中央各業務主管機關公告應全國放假之日，均應計入；惟活動開始前未可得知之放假日（如颱風假），不予計入。

4.2 報名流程

本活動採報名制，由資安院公告活動資訊後，參與者須於期限內下載並填寫報名文件，完成後寄送至指定信箱（bounty@nics.nat.gov.tw）。資安院將進行文件審查，必要時得通知補正；參與者需能於報名截止日前完成補正並經審查通過，始視為完成報名程序。

4.2.1 報名公告與文件下載

本活動資訊將公告於資安院（https://www.nics.nat.gov.tw/）網站，並同步於 TWCERT/CC（https://www.twcert.org.tw/）網站提供報名文件下載（如報名表、個人資料使用同意書、保密協議書等文件）。

4.2.2 報名文件繳交

- 紅隊：於報名期限內，將「報名表暨保密協議書與個人資料同意書」，寄至活動信箱（bounty@nics.nat.gov.tw）。
- 藍隊：於報名期限內，將「報名表暨保密協議書」寄至活動信箱（bounty@nics.nat.gov.tw）。
- 文件若不完整，資安院得通知補正；參與者如能於報名截止日前完成補正，始得視為有效。

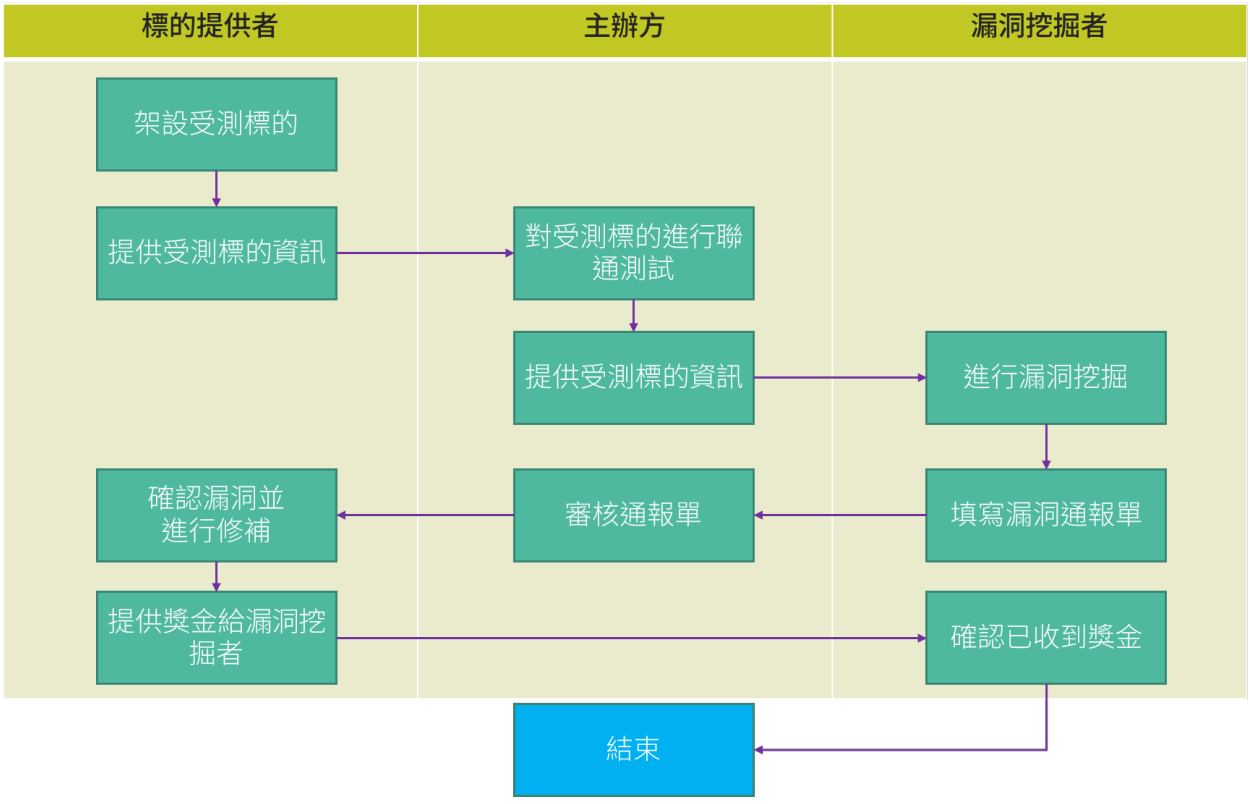
4.2.3 報名文件審查與通知

- 資安院於收件後進行報名文件審查，原則上於 5 個工作天內以電子郵件回覆收件狀況；惟實際回覆時間，得由資安院視個案情形裁量決定。
- 經資安院審查通過並以電子郵件通知後，始視為完成報名程序。
- 活動相關資訊（含漏洞挖掘受測標的）將於正式活動開始前，由資安院

以電子郵件通知合格參與者，其不對外公開。

4.3 漏洞挖掘流程

本活動之漏洞測試由藍隊廠商提供受測標的，資安院於測試開始前進行環境檢測及連通性確認，以確保測試場域之可用性與穩定性。紅隊參與者須透過「TWCERT/CC 漏洞獵捕活動資訊網頁面」（活動開始另行以電子郵件通知），取得最新標的資訊後進行測試。紅隊僅得於規定期間內依本活動規範執行遠端黑箱測試，對指定標的進行漏洞挖掘，並應避免任何破壞性行為。測試過程中，若受測標的出現重大異常或中斷，藍隊應提供必要之技術支援，以確保活動能順利進行。



4.3.1 受測標的提供

參與本活動之廠商請提供欲受測之電子產品設備做為「受測標的」，提供方式有以下 2 種。

- 廠商自行維護：將受測標的連接至藍隊自行維護之外網，供紅隊可遠端針對受測標的進行漏洞挖掘作業，並請廠商於計畫期間持續維持受測標的之可用性。

- 資安院維護：若藍隊無法自行設置網路供紅隊進行測試，可選擇將受測標的建置於資安院所選定之場域，並由場域提供對外連線方式供漏洞挖掘者進行檢測，若受測標的出現嚴重異常狀態，需請標的提供者給予必要之技術支援。選擇此方案者，每一標的需繳交資安院 5 萬元作為場域使用費用。考量本次活動屬首次試辦，免收場域使用費，但每家廠商受測標的以 3 組為限；後續活動場次之場域使用費用將另行公告。資安院完成受測標的設置後，將提供相關 IP/Port 資訊予提供者，以利確認其標的連線情形。

2 種標的提供方式皆應保持其受測標的之正常運作，以利漏洞挖掘者可於活動期間持續作業。標的提供者應於收到漏洞通報書後，確認漏洞之有效性，並依漏洞裁判書結果進行漏洞挖掘獎勵與獎金發放作業（依第 4.7 節規定辦理）。

有關廠商於活動中之配合作業項目如下：

- 於活動前選定本次受測標的，並提供其名稱、型號及連線方式或 IP 位址予資安院。

- 廠商得自行遴選公司產品作為受測標的，每一類型產品僅得選定一項，並鼓勵廠商優先提供近一年內之新產品或試產品。所提供之受測標的應具備可連線之實測環境，以利測試驗證及提升漏洞挖掘效益。

- 於漏洞挖掘執行期間，持續確保受測標的之可用性，若接獲通知受測標的已無法正常連線或執行功能，應即協助進行故障排除以利漏洞挖

掘作業持續進行。

- 收到資安院提供之漏洞通報書後，於 5 日內進行漏洞確認，若針對漏洞判定有疑慮，填復漏洞申訴書後提供資安院進行裁定。
- 完成漏洞通報審核後並於本活動結束後 30~45 日內，依照資安院提供之通報者資訊頒發對應獎金給通報者，並保留匯款紀錄。

4.3.2 受測標的資訊提供

為確保漏洞獵捕活動能順利進行，藍隊需於活動開始前完成受測標的之準備與資訊提供，並於活動全程維持標的之可用性。標的撤除或中斷僅得於特定情況下進行，以維護測試之公平性與連續性。

- 藍隊應於活動前提供本次計畫受測標的，並至 TWCERT/CC 漏洞獵捕活動資訊網頁面（活動開始另行以電子郵件通知）填寫標的名稱、型號及連線方式或 IP 位址等資訊。
- 藍隊完成系統整備後，須通知資安院進行複核，以確認受測標的之可用性與穩定性。
- 配合事項
    - 受測標的應於整個活動期間維持可用，僅於產品遭遇重大影響（如服務重大中斷、產品安全性嚴重受損等），或藍隊設定之獎金總額已達上限時，方得撤下並停止測試。
    - 資安院將不定期檢查並確認受測標的之連線狀態，若發現異常，得要求藍隊立即處置並回報。

4.3.3 受測標的資訊取得

藍隊應於活動期間持續更新標的資訊；紅隊則應透過 TWCERT/CC 漏洞獵捕活動資訊網頁面（活動開始另行以電子郵件通知）登入並下載最新版資訊，作為測試依據。

4.3.4 漏洞挖掘測試

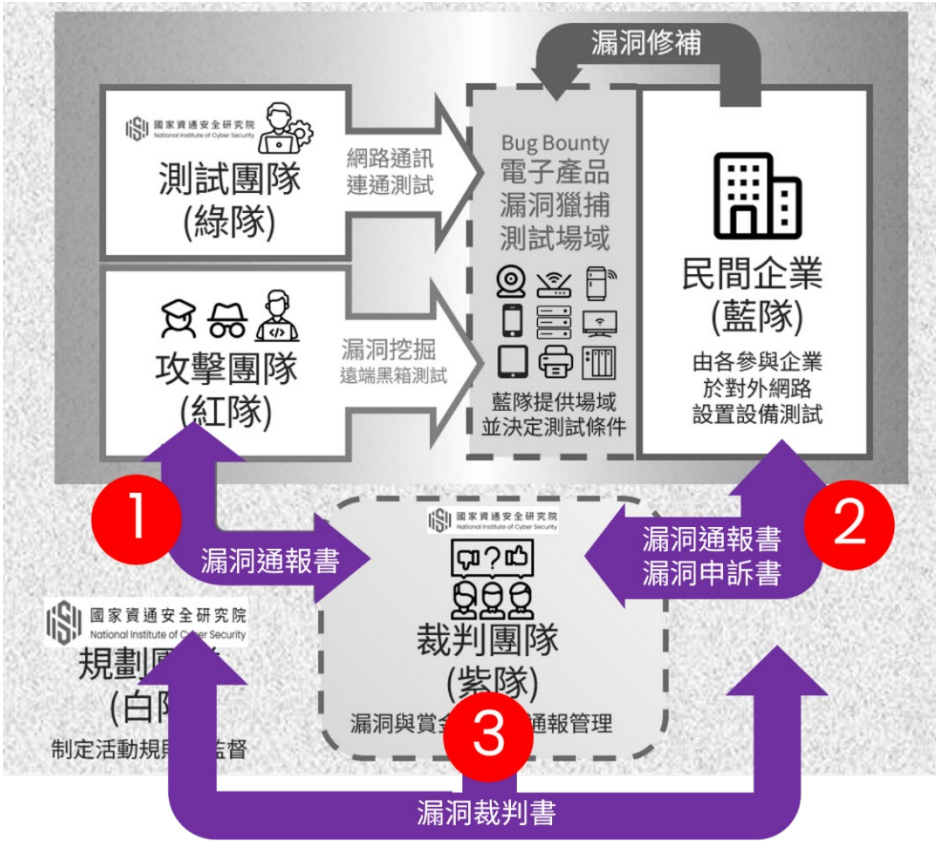
紅隊應依活動規範執行遠端黑箱測試，測試範圍僅限於本活動所指定之受測標的。

測試結果應以可重現、可驗證之漏洞為限，並須於活動結束前完成通報。有關漏洞認定排除項目，將依本活動「4.5 漏洞認定標準」辦理。若經查違反規定，資安院得取消其參與資格並追回已發放之獎勵與獎金。

綠隊將於漏洞挖掘過程中持續監測網路連線狀態，以確保標的可用性。

4.4 漏洞通報流程

紅隊完成漏洞測試後，應依活動規範填寫漏洞通報書，並以報名成功信件所提供之約定密碼加密，於期限內寄至活動信箱（bounty@nics.nat.gov.tw）。資安院將進行初審，如有缺漏得通知補正，補正次數以 2 次為限。通過初審後，其漏洞通報書將轉交藍隊確認，藍隊如有爭議得提出漏洞申訴，申訴次數以 2 次為限，最終結果以資安院裁定為準。



4.4.1 漏洞通報書下載與填寫要求

- 紅隊須透過 TWCERT/CC 平台下載官方制式漏洞通報書範本，並依範本格式完整填寫。
- 通報書內容至少包含

1. 基本資料：通報者基本資料。
2. 使用 IP：漏洞測試來源 IP。
3. 漏洞說明：成因、影響程度及建議 CVSS v3.1 評分。
4. 利用步驟：詳細操作步驟，附必要截圖作為證據。
5. 使用工具：列出所用工具與程式碼（如為自行撰寫程式碼，需提供程式碼）。

6. 修補建議：提供可行修補方式或風險緩解措施。
7. 修補複測：通報者得依意願選擇是否協助藍隊進行修補後之複測。

4.4.2 通報書送交

- 完成通報書後，須以約定密碼（隨附於報名成功信件中）加密後寄送至指定信箱（bounty@nics.nat.gov.tw）。
- 信件大小超過 20MB 者，請分次寄送。
- 信件主旨須註明：「【產品資安漏洞獵捕計畫】OO 產品漏洞通報／OO 產品漏洞申訴」。

4.4.3 初審與補正

- 資安院於收件後進行初審，若內容缺漏，將通知紅隊於 5 個工作天內完成補正。
- 補正次數以 2 次為限；逾期或未補正者，視為放棄通報。

4.4.4 藍隊確認與申訴

- 通過初審之通報書，將由資安院轉交廠商確認，並以報名成功通知信中所提供之約定密碼進行加密後傳遞。
- 廠商須於 5 個工作天內回覆是否同意漏洞內容；如有爭議，得提出漏洞申訴書。
- 廠商申訴次數以 2 次為限。

4.4.5 裁定與結果

- 資安院（裁判團隊）將依收到之通報書與申訴書，進行最終漏洞等級判定與裁定。
- 資安院（裁判團隊）裁定結果以漏洞裁判書形式提供，紅、藍隊雙方均不得對裁定結果提出異議。

4.5 漏洞認定標準

本活動之漏洞認定，係以紅隊所提交之通報書內容為基礎，由藍隊進行確認，並由資安院（裁判團隊）進行最終裁定。為確保漏洞獎勵之公正性，本章節將針對不列入認定範圍之類型漏洞進行說明，不予認定之漏洞類型亦不得作為獎勵。

4.5.1 認定原則

- 僅限本活動指定之受測標的。
- 漏洞須具可重現性、可驗證性，且對產品或使用者安全有實質影響。
- 不具實際安全風險或僅屬資訊建議者，不予認定。

4.5.2 不予認定之漏洞類型

以下情形不屬於本活動認定範圍：

- 針對標的進行破壞性測試行為如：刪除設定檔，格式化、覆蓋、加密伺服器檔案，對資料庫進行破壞。
- 社交工程（如釣魚、詐騙手法）。
- 實體安全（需取得實體存取權限）。
- 未使用之套件弱點。

- Self-XSS（僅影響自身）。
- 需中間人攻擊或實體存取始能利用之漏洞。
- 頻寬消耗型或資源消耗型之 DoS/DDoS 攻擊手法。
- 安全影響輕微的資訊洩漏（如路徑、目錄、日誌等）。
- Cookie 缺少安全標頭。
- 僅透過自動化工具掃描，未經驗證可利用性之漏洞。

4.5.3 漏洞爭議裁定

漏洞認定最終結果，由資安院（裁判團隊）裁定，並以漏洞裁判書為憑，紅、藍雙方均不得對最終裁定提出異議。

4.6 漏洞修補

漏洞修補與產品版本更新責任仍歸屬藍隊廠商。廠商得依其內部資源與產品生命週期，進行後續修補及更新。資安院不追蹤修補進度，但建議廠商善用本活動之成果，逐步建構產品資安治理流程。若廠商於修補完成後希望進行複測，可由資安院協助聯繫最初發現該漏洞之紅隊成員；是否提供複測協助，完全取決於該紅隊成員之意願。

4.7 獎勵與獎金核發

本活動採用多元獎勵機制，鼓勵紅隊積極挖掘並回報漏洞。所有通報須經資安院裁定為有效漏洞，方得獲得獎勵。獎勵內容除依漏洞嚴重程度對應之獎金外，亦包含漏洞獎金名人堂與 CVE 編號申請機會，協助通報者建立專業形象並提升技術能見度。獎金由藍隊廠商負責支付，並須於規定期限內完成，資安院僅負責審查與通知，不介入金流事宜。

4.7.1 獎金說明

- 藍隊得設定活動總獎金上限，當獎金達到總上限，將提前於活動結束前終止漏洞挖掘。
- 漏洞挖掘獎金依漏洞嚴重程度（CVSS v3.1 評分）分級，藍隊於活動前須確認獎金基準並於活動結束後支付。
- 獎金分級共分為 4 級，每個漏洞之分級標準與參考獎金如下表所示，實際金額由藍隊報名時確認，並將公告於活動網頁。

  - 嚴重等級（CVSS v3.1：9.0~10.0 分）：新臺幣 100,000 元
  - 高等級（CVSS v3.1：7.0~8.9 分）：新臺幣 30,000 元
  - 中等級（CVSS v3.1：4.0~6.9 分）：新臺幣 10,000 元
  - 低等級（CVSS v3.1：1.0~3.9 分）：新臺幣 3,000 元
- 除依 CVSS v3.1 評分分級外，藍隊得依產品特性，提出「自訂特定嚴重風險情境」（例如：資料破壞-備份失效，情境可參考下圖或自行定義），並設定對應獎金，以確保產品特有風險獲得適當重視。若紅隊通報漏洞符合該自訂情境，則獎金將依 CVSS 分級獎金或自訂情境獎金

中較高者發放，以確保獎勵符合實際產品風險。

- 獎金金額 1,001 元（含）以上者須列入個人綜合所得申報，得獎獎金在 NT$20,001（含）以上者，依法扣繳 10%所得稅。
- 藍隊須於活動結束後 30~45 個日曆日內，且最遲不得逾 115 年 3 月 31 日完成獎金支付，並保留匯款紀錄以供資安院確認獎金已交付通報者。
- 如涉及爭議案件，則於資安院最終裁定確認後，依裁定結果另行辦理獎金支付。
- 若廠商未依規定時限支付獎金，資安院得取消其後續參與資格。

4.7.2 漏洞獎金名人堂

紅隊優秀成員將登錄於活動「名人堂」頁面，顯示其漏洞通報成就與專長技能，作為資安圈能見度與信譽的重要里程碑。

4.7.3 CVE 編號申請

- 若漏洞屬於上市產品，且經廠商同意，通報者可透過平台協助申請 CVE 編號。獲得 CVE 編號後，通報者將被登錄為正式漏洞發現人，並

得選擇姓名公開或匿名，有助於提升技術聲譽與專業能見度。

- 若漏洞屬於尚未上市之產品（試產品）或廠商不同意公開該漏洞，則不得申請 CVE 編號，以避免造成未修補前的安全風險。

4.7.4 領獎原則

本活動之獎勵與獎金發放，依下列原則辦理。

- 獎金僅頒發給第一個有效通報該漏洞的通報者。
- CVE 共同發現者列名僅作為技術歸屬與公開紀錄之用，並不影響本活動獎金僅頒發給第一位有效通報者之原則。
- 漏洞須符合「可驗證、可重現、可利用」的原則，且必須在活動範圍內。
- 同一漏洞之後續重複通報，不再額外發放獎金。
- 若通報內容屬於針對同一標的之連續攻擊行為，資安院得將其視為同一筆紀錄合併審查，並以首次有效通報者為準。
- 漏洞通報書需於活動限制期間內完成補正，並經資安院審核確認其漏洞通報有效性。
- 若經資安院裁定為有效漏洞之通報者（以下簡稱有效通報者），即具領獎資格。資安院將通知藍隊並提供有效通報者之聯絡資訊（姓名、電子郵件、電話），用於後續獎金支付與聯繫事宜。獎金發放相關作業（包含銀行帳號取得、收據開立、稅務文件提供）由有效通報者與藍隊雙方直接辦理，資安院不介入金流。

5. 資訊保密與公開原則

5.1 保密義務

- 參與本活動之紅隊、藍隊及資安院，均須簽署保密協議書，確保於活動過程中取得之所有資訊（含產品資料、測試環境、通報內容、技術細節等）僅限於本活動範圍內使用。
- 未經資安院與相關廠商同意，參與者不得對外揭露或散布漏洞資訊、測試結果或其他相關資料。
- 違反保密義務者，資安院得取消其參與資格、追回獎勵與獎金，並保留追究法律責任之權利。
- 資安院於活動規劃與執行過程中，對於藍隊所提供之產品資訊、紅隊通報內容，亦負有保密責任。所有資訊僅限於本活動範圍內使用，不得作為其他研究、商業或非授權用途。

5.2 公開原則

- 本活動之參與廠商可選擇以公開或匿名方式參加，資安院將尊重廠商選擇，不強制揭露廠商名稱。
- 活動成果報告將以整體統計或匿名化方式呈現，不會揭露特定廠商之測試結果或漏洞細節。
- 資安院僅於必要時，對外公布經確認之重大成果（如總通報數量、漏洞類型分布），並確保不涉及個別廠商之專有資訊。
- 所有公開資訊將經資安院審核後發布，以避免未經授權之漏洞細節外洩。

5.3 漏洞 CVE 編號申請原則

- 若紅隊欲申請 CVE 編號，須經藍隊同意公開相關漏洞資訊。
- 若藍隊不同意，或漏洞屬於尚未上市之產品，則不得申請 CVE 編號。
- 獲得 CVE 編號後，紅隊可選擇姓名公開或匿名，以提升專業能見度，同時兼顧資訊保護。
- 若同一漏洞經多人於活動期間內獨立發現，資安院得協助將所有有效發現者列為該 CVE 編號之共同發現者，並於公開資訊中註明。

6. 法律遵循與安全港

6.1 法律遵循

- 參與者於活動期間，應遵守中華民國相關法令及本活動規範。
- 任何超出本活動範圍之外之行為，均不在活動保障範圍內，若涉及違法，參與者應自行負責，並可能被要求退還已獲獎勵或獎金，同時喪失未來參與相關計畫之資格。
- 紅隊須確認其所使用之工具、程式碼或其他技術，不得侵害第三方之智慧財產權或違反其他法律規範。

6.2 安全港條款

- 紅隊於遵守本活動規範之前提下，於活動期間內針對公告指定標的所進行之測試行為，資安院及藍隊認定其屬於授權行為，不構成《中華民國刑法》或其他適用之電腦法規所稱之「無故入侵他人之電腦或其相關設備」。
- 安全港保障範圍僅限於
    - 本活動公告之受測標的。
    - 本活動允許之測試方法。
- 若紅隊超出範圍進行測試，或對非指定標的系統進行操作，則不在安全港保障之內，並可能涉及法律責任。
- 若紅隊因依本活動規範進行測試而遭第三方（含司法單位）提起法律行動，資安院及藍隊將採取適當行動說明該行為係在本活動授權範圍內進行。

- 若紅隊對測試行為是否屬於安全港保障範圍存有疑義，應於執行前向資安院確認。
- 若本活動之安全港條款與藍隊其他使用條款或政策有所衝突，本安全港條款優先適用。
- 本安全港條款並不適用於非本活動藍隊之第三方，若紅隊的測試行為涉及第三方之基礎設施，如網路、系統、資訊、應用程式、產品或服務等，仍可能面臨第三方提起法律行動。

6.3 保密與責任限制

- 所有參與者須簽署保密協議書，活動過程中取得之資料僅限於本活動使用，不得對外揭露。
- 若紅隊依本活動規範進行測試時，無意中未經授權存取個人資料、商業機密或其他敏感資訊，應立即停止任何可能導致進一步存取前述資訊之行為，告知資安院與藍隊已存取之資料，並立即自系統中移除該資訊，不得保存、使用或對外揭露相關資訊。
- 資安院僅負責活動規劃、平台協助及裁定，惟不承擔因漏洞利用、測試行為或工具使用所導致之任何損害責任。
- 藍隊提供受測標的，對於紅隊測試環境以外之影響不承擔責任。
- 紅隊須自行承擔因測試工具或操作所生之風險，不得因此向資安院或藍隊請求補償。

6.4 智慧財產權與揭露權

6.4.1 智慧財產權

- 紅隊就其提交之漏洞報告與技術細節（通報資料），經審核通過核發獎金後視為藍隊所有，有關漏洞資訊之公開與否，由藍隊決定。
- 紅隊如提供自行開發之程式碼或工具，應確認該技術不涉及第三方智慧財產權爭議。

6.4.2 揭露權

- 漏洞資訊之公開應由藍隊與紅隊協商公開方式與時程。
- 若紅隊欲就通報之漏洞申請 CVE 編號，須先主動告知藍隊，並與藍隊協調申請方式與時程。

7. 附則

7.1 辦法效力

- 本辦法經資安院公告後施行，適用於本活動之全體參與者。
- 參與者報名並經審查通過，即視為同意遵守本辦法之全部內容。

7.2 修正權限

- 本辦法如有未盡事宜，資安院得依實際需要進行補充或修正，並另行公告。
- 修正後之內容，與原辦法具有同等效力。

7.3 優先適用

- 本辦法如與其他文件有所衝突，以本辦法為準。
- 本辦法如與現行法令牴觸，應依相關法令辦理。

7.4 緊急狀況

如遇不可抗力之事故或其他緊急狀況，資安院得單方面調整或終止活動，並公告於活動網頁，參與者同意將自行主動閱讀，資安院將不另行個別通知參與者。

7.5 解釋權利

有關本活動內容及規則，資安院保有最終解釋權利。

7.6 爭端之解決與管轄法院

因本活動所生之任何爭議，雙方應依誠信原則協商解決；如協商不成，須進入訴訟程序者，雙方同意以臺灣臺北地方法院為第一審管轄法院。

8. 附件

相關參考文件：

- （紅隊）報名表暨保密協議書與個人資料同意書
- （藍隊）報名表暨保密協議書
- 法定代理人同意書