

1. 專案概述

1.1 專案名稱

「紅隊演練」委外服務案(以下簡稱本案)。

1.2 專案目標

XX 機關(以下簡稱本機關)為能提升本機關之資通安全防護能力並找出潛藏於本機關營運之重大資安風險，擬透過委由第三方廠商進行「XX 年紅隊演練服務」專案(以下簡稱本專案)。以攻擊者或白帽駭客之攻擊戰術、技術及程序(Tactics, Techniques, Procedures, TTPs)，在有限時間內且不影響系統運作前提下，不限制攻擊手法以達成指定目標(如外部網路環境取得核心伺服器(如：AD、防毒等)之控制權/控制特定帳號/取得特定資料)，並經由演練結果檢視現有防禦設備之有效性、管理制度及程序的落實性、監控範圍之合理性及反應時間之適切性。

1.3 專案範圍

專案範圍為本機關所有人員與擁有之資訊資產(即支援資訊相關活動所需之資產)，包含：

- 硬體資產：如伺服器、Router、AP、IPS、Firewall 等。
- 軟體資產：如作業系統、自行開發之應用程式及套裝軟體等。
- 資訊：如數位與紙本資訊。
- 人員：如正式員工、約聘人員及工讀生等。

1.4 專案期間

自簽約日起至 XXX 年 XX 月 XX 日止。

2. 專案工作項目

紅隊演練係針對機關整體安全進行評估，擬真方式以駭客思維入侵並達到演練目標，以檢視受測目標營運上可能存在之資安風險，並檢視受測目標防禦機制，持續改善受測目標資安防護之能力。

2.1 演練方式

在受測目標一般人員未知情況下進行指定受測範圍的(外網入侵/內網入侵/實體入侵)紅隊演練，受測目標之防禦機制(藍隊)採取(監控不阻擋/監控並阻擋)方式進行。

2.2 時程說明

- 專案啟動會議：得標日次日起 X 天內。
- 執行紅隊演練服務：經專案啟動會議確認內容次日起 X 個工作天內。
- 弱點修補作業：紅隊演練服務報告交付次日起 X 個工作天內。
- 執行紅隊演練複測：弱點修補作業結束次日起 X 個工作天內。

2.3 交付報告

- 工作計畫書：得標日次日起 X 天內。
- 紅隊演練初測報告：紅隊演練初測結束次日起 X 個工作天內。
- 紅隊演練複測報告：紅隊演練複測結束次日起 X 個工作天內。

3. 管理需求

3.1 廠商資格

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述：

- 3.1.1 凡在政府機關登記合格，無不良紀錄之廠商(檢附設立及登記證明、納稅證明及信用證明)且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。
- 3.1.2 本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。
- 3.1.3 投標廠商須實施資訊安全管理制度，通過 ISO 27001 或其他類似驗證，並於專案執行期間持續有效，以保護紅隊演練服務所取得之資料。
- 3.1.4 本案涉及資通訊軟體、硬體或服務等相關事務，不得提供及使用大陸廠牌資通訊產品。服務如涉及使用雲端工具，應確保機關利用服務之所屬一切資料存取、備份、及備援之實體所在地，應為我國管轄權所及之境內。
- 3.1.5 X 年內執行至少 X 件以上的紅隊演練專案。
- 3.1.6 本案團隊成員要求
 - 服務人員須年滿 18 歲以上，身體健康無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士，於履約期間不得同時於大陸地區工作。
 - 專案人員應包含至少 X 位人員，成員至少應包含專案負責人/專案經理與紅隊演練檢測人員。每位紅隊演練檢測人員應具備以下

專業要求以確保服務水準，並於建議書中檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本以供審核。

- 紅隊演練檢測人員皆須具備滲透測試、紅隊演練或漏洞挖掘相關經驗不得少於3年；惟有特殊經驗但未符合前述資格者，得經本機關同意後列入執行成員。
- 團隊之紅隊演練檢測人員應具備專業要求，至少需具備下列證照至少X張。
 - CEH(EC-Council Certified Ethical Hacker)。
 - CPENT(EC-Council Certified Penetration Tester)。
 - CompTIA PenTest+。
 - CPSA(The CREST Practitioner Security Analyst)。
 - OSCP(Offensive Security Certified Professional)。
 - 其他資安相關專業證照(需經本機關核可)。
- 其他資格限制(依需求可加入選項)
 - 具備尋找零時差弱點之能力與實績(如三年內有挖掘國際知名產品 CVE 弱點之證明或佐證，且 CVE 弱點之 CVSS 3 分數需達 8.0 分以上)。
 - 3 年內曾執行至少 5 件以上之紅隊演練專案，且專案規模至少達新臺幣 300 萬元以上。
 - 團隊成員近三年至少需有 1 位專案團隊成員曾參與國際 CTF 比賽，如 DEFCON CTF 等，且獲得前三名。
 - 具備弱點研究能力，曾於國際知名研討會發表研究成果(如

HITCON、Black Hat、DEF CON、CODE BLUE、CODEGATE 等)。

— 曾參與國際企業 Bug Bounty 計畫且獲得獎勵。

3.2 服務水準協定(SLA)與罰責

3.2.1 服務水準規範

本案各項服務水準協定(Service Level Agreement，SLA)，以必須達成該項工作服務項目要求為依據，透過客觀的證據或指標，做為品質管制，以預防各項不符合作業的事項發生，降低委外作業的風險，詳細服務水準規範如下表：

項次	項目	服務水準
1	執行時程	<ul style="list-style-type: none">▪ 初測：每次以 XX 為限▪ 複測：每次以 XX 為限▪ 檢測報告：初測與複測結束後 2 週內提供
2	日誌交付	廠商應於檢測期間應每日製作工作日誌，並於隔日交付機關，日誌中應詳實記錄工作軌跡紀錄
3	重大漏洞通報	廠商於檢測過程中如發現重大漏洞，應立即通知機關即時修補
4	清除相關異動	廠商於檢測完畢後須還原系統環境，清除相關異動(含帳號、資料及工具程式等)，相關異動須詳細記錄於每日工作日誌中，並彙整於最後成果報告中說明

3.2.2 相關說明：

- 1.承作廠商無法達成相關工作項目要求或交付文件，其罰款(違約金)計算方式為每延遲 1 日(以日曆天計，星期日、國定假日及其他休息日均應計入，不滿 1 日以 1 日計算)，本機關得按契約總價之千分之一計算懲罰性違約金，款項可自契約總價或履約保證金項中扣抵。
- 2.違約金上限依採購法之採購契約要項第四十五點規定，違約金以契約總價之 20% 為上限。如違約金逾 20% 時，本機關得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。
- 3.得標廠商應於議價後所提成本分析中，詳列各項工作項目成本，如於驗收時，經審查發現有不合格之工作項目，得標廠商應依期限予以改正。如未改正，本機關有權扣除該項工作之款項。
- 4.得標廠商指派之專案負責人及工作成員，未經本機關同意，不得更換，如有未經本機關同意自行更換時，每更換乙次得依契約總價之千分之一計算懲罰性違約金。
- 5.得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付本機關之文件經本機關審閱時，如交付項目有不符本案要求，廠商應於接獲審查意見通知後 XX 日內完成改正並送達本機關(改正以 1 次為限)再送審查，改正期限不得超過各期之履約期限。本機關再次審查結果如交付項目仍有不符要求，則逾期違約金溯至原規定交付日期之次日起算，得扣除本機關審查時間。

3.3 品質需求與驗收標準

3.3.1 品質需求

- 1.為確保專案如期如質完成，廠商應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。
- 2.得標廠商訂定品質管理流程，本機關得以稽核。
- 3.得標廠商於專案期間應辦理啟始會議與結束會議，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本機關備考。

3.3.2 驗收標準

得標廠商應依專案工作項目之服務需求，以及符合服務水準協定(SLA)中所列事項，完成專案工作，並依本說明文件所訂之交付時程，完成相關文件與紀錄之交付。

3.3.3 驗收方式

本機關將於各項工作項目交付完成後進行審查作業，得標廠商需依本機關審查意見修正交付項目，並再送至本機關複驗。

3.4 業務保密安全責任

- #### **3.4.1 廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影(音)及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽定保密協議書。**

- 3.4.2 廠商對特別以文字標示或口頭明示為機密資料者，非經本機關書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，廠商應負完全責任。
- 3.4.3 廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由廠商自訂)。
- 3.4.4 契約終止時，廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本機關或經本機關同意後銷毀。
- 3.4.5 履約期間造成保密及安全事件，得歸咎於廠商之責任時，廠商應負所有法律及賠償責任。
- 3.4.6 本機關對廠商保留實地稽核權，以確保廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

3.5 專案經費預算金額

- 3.5.1 本案 XXX 年度預算金額為新台幣 XXX 萬元整。
- 3.5.2 本案所須之人力由得標廠商自由運用調配，並於建議書中詳述計費標準與成本分析。

4. 交付項目

4.1 交付項目與時程

項次	交付項目	交付內容	數量	交付型態	交付期限
1	修正後服務建議書	依評選委員建議修正之服務建議書內容，以及執行本案細部規劃工作項目內容	X 份	電子檔\紙本	決標次日起 XX 日曆天
2	紅隊演練計畫書	<ul style="list-style-type: none">▪ 簡介▪ 演練概述▪ 演練目標與範圍▪ 準備與資源▪ 時程與計畫▪ 演練執行▪ 事後分析與報告▪ 演練評估與改進	X 份	電子檔\紙本	決標次日起 XX 日曆天
3	紅隊演練初測報告	紅隊演練檢測作業相關規劃內容 <ul style="list-style-type: none">▪ 演練期間▪ 服務人員▪ 演練過程所使用之技術與工具說明▪ 全案需詳細記錄弱點細節，包含風險等級、弱點位置、弱點描述、圖示、修補建議	X 份	電子檔\紙本	紅隊演練初測完成次一日曆天起 X 個日曆天內交付

項次	交付項目	交付內容	數量	交付型態	交付期限
		<ul style="list-style-type: none"> ▪ 演練結果統計 ▪ 演練效益說明 ▪ 檢討及建議 ▪ 演練相關佐證與軌跡紀錄 			
4	紅隊演練複測計畫書	紅隊演練複測作業相關規劃內容 <ul style="list-style-type: none"> ▪ 簡介 ▪ 演練概述 ▪ 演練目標與範圍 ▪ 準備與資源 ▪ 時程與計畫 ▪ 演練執行 ▪ 事後分析與報告 ▪ 演練評估與改進 	X 份	電子檔\紙本	廠商應於機關通知次一日曆天起 XX 個日曆天內交付
5	紅隊演練複測報告	<ul style="list-style-type: none"> ▪ 演練期間 ▪ 服務人員 ▪ 演練過程所使用之技術與工具說明 ▪ 全案需詳細記錄弱點細節，包含風險等級、弱點位置、弱點描述、圖示、修補建議 ▪ 演練結果統計 ▪ 演練效益說明 ▪ 檢討及建議 	X 份	電子檔\紙本	廠商應於機關通知次一日曆天起 XX 個日曆天內交付

項次	交付項目	交付內容	數量	交付型態	交付期限
		<ul style="list-style-type: none"> ▪ 演練相關佐證與軌跡紀錄 			

5. 伍、服務建議書製作規定

5.1 服務建議書格式

5.1.1 紙張：宜用 A4 規格。

5.1.2 繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明廠商名稱、廠商地址、本案名稱及日期，裝訂線在左側。

5.1.3 目次：應標示各章節之出處頁碼。

5.1.4 廠商投標建議書之份數為 1 式 N 份。

5.2 服務建議書內容

5.2.1 專案概述

- 1.專案名稱
- 2.專案目標
- 3.專案時程

5.3 廠商說明

- 1.廠商簡介
- 2.公司營運狀況，包含參與人員名單、能力證明及廠商經驗說明

5.4 專案計畫

- 1.專案服務內容項目
- 2.組織與人力配置
- 3.專案時程、品質、風險管理與交付項目計畫，包含工作項目、

時程規劃及查核點

- 4.本案預期效益
- 5.本案 SLA 承諾