如何透過檢測及演練提升資安防護與意識

吳啟文

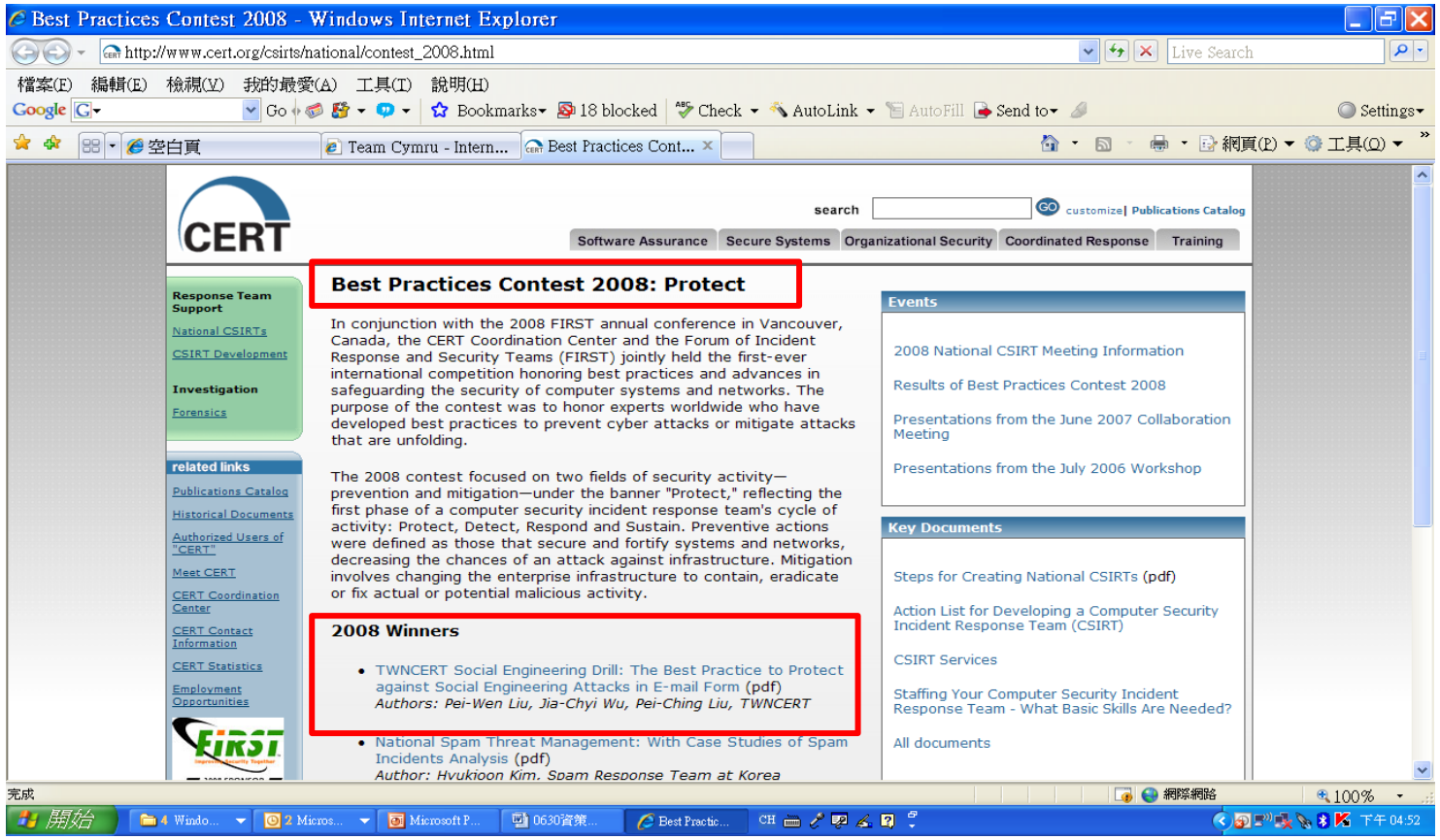
114年6月

大綱

- **緣起**
- 技術檢測
- 資安演練
- 結論

緣起(1/2)

- 前行政院國家資通安全會報技術服務中心以「TWNCERT Social Engineering Drill：The Best Practice to Protect against Social Engineering Attacks」，參加First舉辦之「Best Practice Contest 2008」獲獎



資料來源：https://www.first.org/conference/2008/contest.html

緣起(2/2)

- 以突破傳統「偵測並防堵駭客攻擊」作法，改以創新理論，結合實務演練模式，強調low cost and high efficiency，有效協助政府機關了解電子郵件社交工程攻擊，並透過認知宣導方式提升資安意識，獲得FIRST最佳實務比賽評審委員之肯定，勇奪冠軍
- 本獎項於2008/6/26 於加拿大溫哥華舉辦之FIRST大會，由當時主席Derrick Scholl親自頒發獎牌及5000美元獎金

大綱

- 緣起
- **技術檢測**
  - 安全性檢測-弱點掃描
  - 安全性檢測-滲透測試
  - 漏洞修補策略
  - 資通安全健診
  - 資安稽核技術檢測
- 資安演練
- 結論

資安應辦事項-技術面

- 依據「資通安全責任等級分級辦法」相關規定

辦理項目	辦理內容	A級	B級	C級
安全性檢測	全部核心資通系統弱點掃描	每年2次	每年1次	每2年1次
	全部核心資通系統滲透測試	每年1次	每2年1次	每2年1次
資通安全健診	1.網路架構檢視 2.網路惡意活動檢視 3.使用者端電腦惡意活動檢視 4.伺服器主機惡意活動檢視 5.目錄伺服器設定檢視 6.防火牆連線設定檢視	每年1次	每2年1次	每2年1次

安全性檢測-弱點掃描

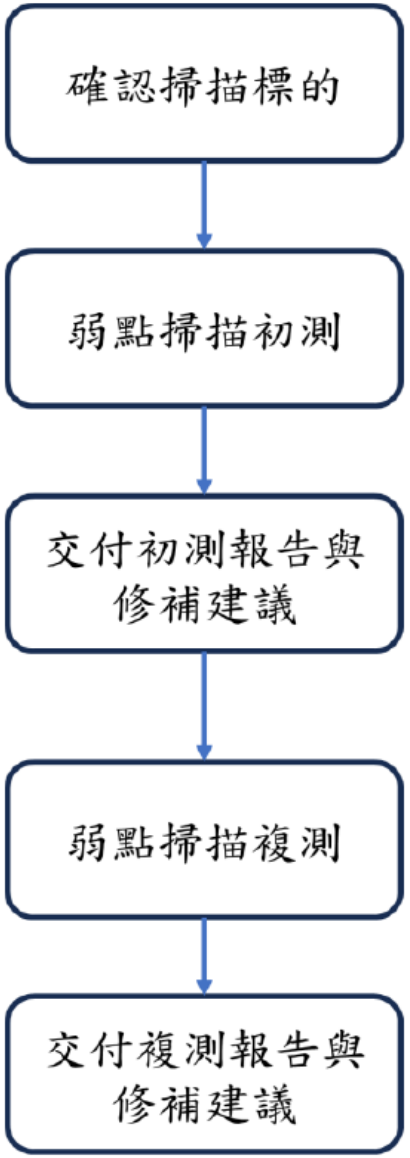
安全性檢測-弱點掃描

- 運用檢測工具進行大範圍自動化弱點探測，針對已知弱點特徵進行探查，若識別存在相關弱點特徵會搭配弱點資料庫對弱點進行風險等級判定。掃描工具可能出現誤判狀況，此時可輔以人工作業進行結果驗證

1. 主機系統弱點掃描	2. Web網頁弱點掃描 (OWASP Top 10：2021)	3. 網頁個資掃描
1.1 作業系統未修正漏洞檢檢測 1.2 常用應用程式漏洞檢測 1.3 網路服務程式檢測 1.4 木馬程式檢測 1.5 後門程式檢測 1.6 帳號密碼破解測試 1.7 系統之不安全與錯誤設定檢測 1.8 網路通訊埠檢測	2.1 Broken Access Control 2.2 Cryptographic Failures 2.3 Injection 2.4 Insecure Design 2.5 Security Misconfiguration 2.6 Vulnerable and Outdated Components 2.7 Identification and Authentication Failures 2.8 Software and Data Integrity Failures 2.9 Security Logging and Monitoring Failures 2.10 Server-Side Request Forgery (SSRF)	3.1 對外網頁之個資檔案掃描 3.2 掃描之個資特徵

弱點掃描作業流程

- 一般弱點掃描整體流程會從確認掃描標的開始，分成初測與複測階段
- 當完成初測報告後，將檢測報告提供給受測單位
- 待受測單位完成弱點修補後，再執行複測作業，以確保受測單位針對初測報告中發現之弱點已確實修補完成



安全性檢測-滲透測試

安全性檢測-滲透測試

- 模擬駭客攻擊方式，對目標主機或網路服務進行安全強度測試，以找出可能的資安弱點，並提出改善建議
- 檢測方式較專注於特定資通系統、應用程式或設備之弱點利用，通常檢測範圍為一至數個標的，主要模擬駭客攻擊行為對標的進行檢測，檢測人員透過資訊蒐集進一步挖掘標的潛在之弱點，並搭配半自動化或特定攻擊程式，實際利用弱點以達到確認弱點存在之目的

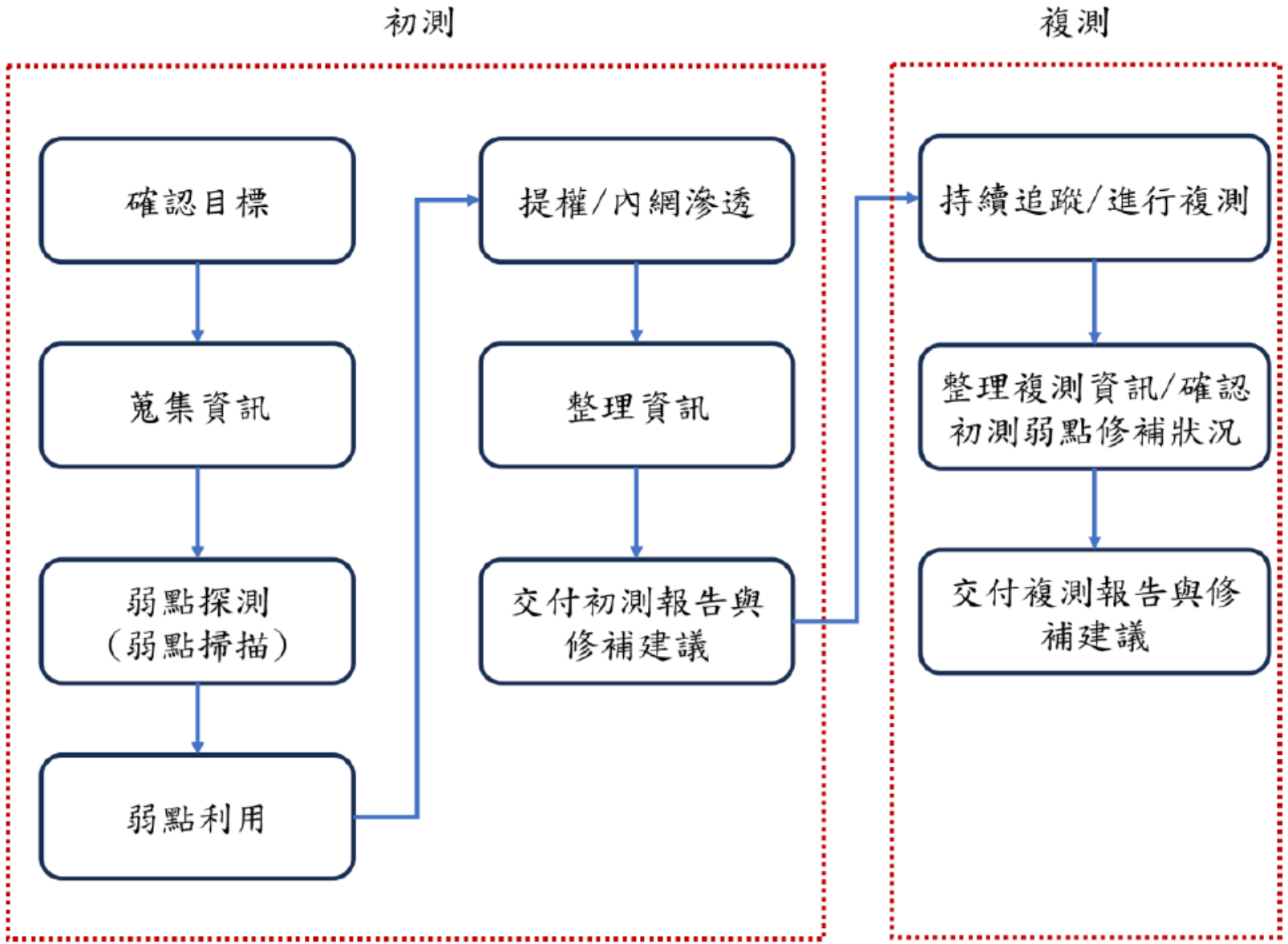
1. 作業系統測試
1.1 遠端服務
1.2 本機服務

3. 應用程式測試	
3.1 電子郵件服務	3.2 網站服務
3.3 檔案傳檔服務	3.4 遠端連線服務
3.5 網路服務	

2. 網站服務測試		
2.1 設定管理	2.2 使用者認證	2.3 連線管理
2.4 使用者授權	2.5 邏輯漏洞	2.6 輸入驗證
2.7 Web Service	2.8 Ajax	

4. 密碼破解與無線服務測試
4.1 密碼強度測試
4.2 無線服務測試

滲透測試作業流程


初測
確認目標
蒐集資訊
弱點探測
（弱點掃描）
弱點利用
提權/內網滲透
整理資訊
交付初測報告與
修補建議
複測
持續追蹤/進行複測
整理複測資訊/確認
初測弱點修補狀況
交付複測報告與修
補建議

漏洞修補策略

通用漏洞評分系統(CVSS)

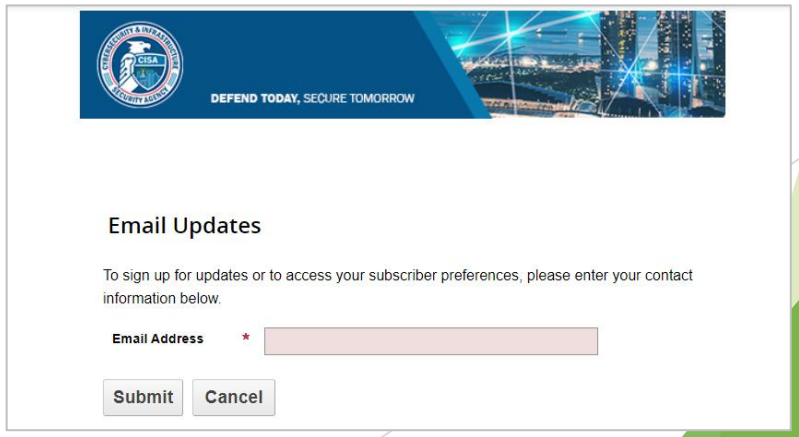
- CVSS(Common Vulnerability Scoring System)主要用於表示漏洞嚴重性
  - CVSS基準分數介於0-10分，分數越高表示嚴重性越高，分為無、低、中、高及重大5種等級
  - 建議高等級以上漏洞優先修補
- 目前共發布4個版本，最新版本CVSS v4於2023/11發布

基準分數與嚴重等級對應

CVSS Base Score	CVSS Severity Level
0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

已知遭利用漏洞(KEV)

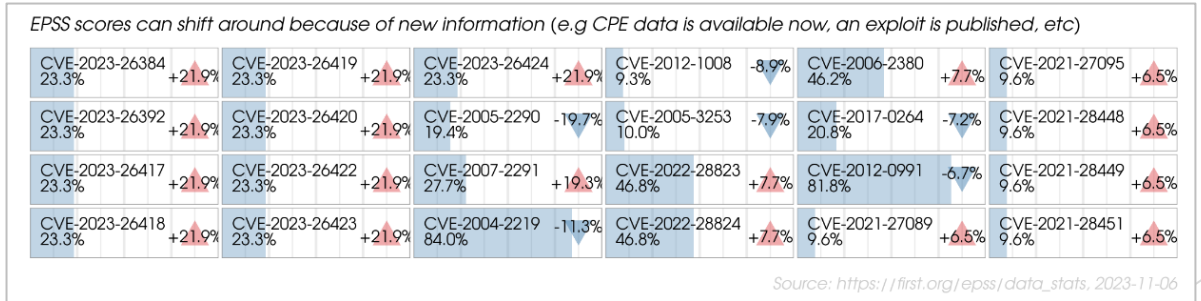
- KEV(Known Exploited Vulnerabilities)是CISA為降低重大風險提出之清單，列出目前或最近被利用之已知漏洞，納入KEV共有3個原則
  - 漏洞具有CVE ID
  - 已被積極利用於攻擊活動
  - 已有補救措施(如供應商提供更新)
- KEV不定期更新，自2021年11月公布至今(2025/6/3)已累計1,357漏洞
  - 可訂閱KEV更新的公告通知



漏洞利用預測評分系統(EPSS)

- EPSS(Exploitability Probability Prediction Score)為FIRST推動之項目，利用機器學習模型評估漏洞被利用可能性
  - EPSS利用分數介於0-1分，分數越高表示漏洞於未來30日內被利用之機率越高
  - EPSS並無考慮漏洞被利用時之影響與環境因素等，僅可做為風險分析之參考，應與其他因素如嚴重程度(CVSS)與威脅情資(KEV)，一同做為可利用性指標
- 目前共發布4個版本，最新版本EPSS v4於2025/3發布
  - EPSS分數每日更新，且提供資料下載與API介接

CVE之EPSS分數變化



可能遭利用漏洞評估指標(LEV)

- 根據研究報告，多數企業每月僅能修補影響其系統約16%漏洞，而研究顯示僅約5%漏洞會在實際環境中遭到利用。理想情況下，組織應將有限資源集中於修補這小部分但極危險的漏洞子集，但識別這些漏洞一直是業界難題
- 目前組織主要依賴「漏洞利用預測評分系統(EPSS)」及美國CISA維護的「已知遭利用漏洞(KEV)」清單進行漏洞風險評估，惟這兩種方法各有侷限性。EPSS專注於預測但不考慮過往利用情況，而KEV清單雖為確認案例，卻往往資訊不完整
- 美國國家標準暨技術研究院(NIST)近日發布全新漏洞評估指標「可能遭利用漏洞(Likely Exploited Vulnerabilities, LEV)」，目的在於解決資安界長期面臨的關鍵挑戰。從每年數千個軟體漏洞報告中，精準識別哪些已被攻擊者實際利用。LEV透過分析歷史EPSS數據，計算漏洞過去遭利用機率，有效橋接EPSS及KEV兩種方法間的差距

資料來源：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=11916

資通安全健診

資通安全健診

- 透過整合各項資通安全項目檢視服務，提供機關資安改善建議，藉以落實技術面與管理面相關控制措施，以提升網路與資通系統安全防護能力

1. 網路架構檢視
1.1 主機位置配置檢視
1.2 網路區域配置檢視
1.3 網路架構設計邏輯檢視

2. 有線網路惡意活動檢視
2.1 封包監聽與分析
2.2 網路設備紀錄檔分析

3. 使用者電腦惡意活動檢視
3.1 使用者電腦惡意程式或檔案檢視
3.2 使用者電腦更新檢視

4. 伺服器主機惡意活動檢視
4.1 伺服器主機惡意程式或檔案檢視
4.2伺服器主機更新檢視

5. 防火牆連線設定檢視
5.1 防火連線設定檢視

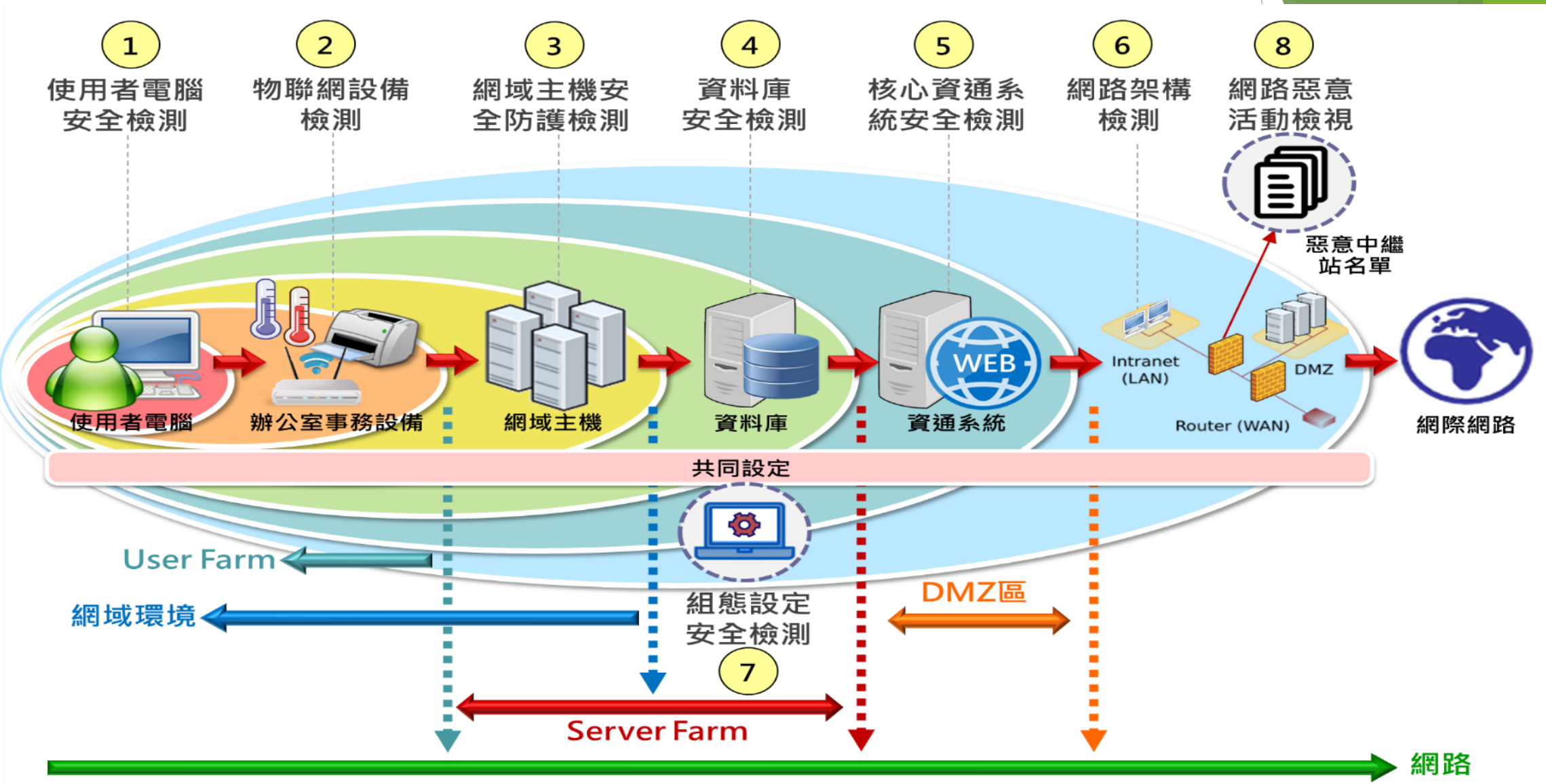
6. 目錄伺服器(AD)設定檢視
6.1 AD GCB 設定檢視

7. 政府組態基準(GCB)設定檢視	
7.1 作業系統GCB設定檢視	7.2 瀏覽器GCB設定檢視
7.3 網通設備GCB設定檢視	7.4 應用程式GCB設定檢視

8. 資料庫安全檢視
8.1 特權帳號管理
8.2 資料加密
8.3 存取授權
8.4 稽核紀錄
8.5 委外管理
8.6 備份保護
8.7 弱點管理

資安稽核技術檢測

技術檢測框架


1
使用者電腦
安全檢測
2
物聯網設備
檢測
3
網域主機安
全防護檢測
4
資料庫
安全檢測
5
核心資通系
統安全檢測
6
網路架構
檢測
8
網路惡意
活動檢視
惡意中繼
站名單
使用者電腦
辦公室事務設備
網域主機
資料庫
資通系統
WEB
Intranet
(LAN)
DMZ
Router (WAN)
網際網路
共同設定
User Farm
網域環境
組態設定
安全檢測
7
DMZ區
Server Farm
網路

技術檢測項目(1/4)

項次	技術檢測項目	技術檢測子項	執行範圍	執行方式
1	**使用者電腦安全檢測**	使用者電腦弱點掃描	全機關	針對受稽機關進行全機關網段連接埠掃描(Port scan)，藉由掃描結果挑選可能存在風險之50台使用者電腦進行弱點掃描
		使用者電腦安全防護檢測		依照弱點掃描結果之風險程度排序，挑選5台高風險使用者電腦進行深度檢測，其檢測項目包含防毒軟體、安全性修補程式更新、應用程式安裝與更新及惡意程式檢測等4項安全防護措施檢測
2	**物聯網設備檢測**	網路印表機檢測	5台物聯網設備	針對網路印表機、門禁設備、網路攝影機、無線網路基地台/無線路由器、環控系統及網路儲存裝置(NAS)等物聯網設備之身分鑑別、資料安全、系統安全及通訊安全等基準項目，透過訪談與實際檢測方式確認是否符合安全基準
		門禁設備檢測		
		網路攝影機檢測		
		無線網路基地台/無線路由器檢測		
		環控系統檢測		
		網路儲存裝置(NAS)檢測		
3	**網域主機安全防護檢測**	網域主機安全防護檢測	1台網域主機	透過實際檢視方式，針對機關之網域主機進行防毒軟體、安全性修補程式更新及惡意程式檢測

技術檢測項目(2/4)

項次	技術檢測項目	技術檢測子項	執行範圍	執行方式
4	**資料庫安全檢測**	資料庫安全檢測	1個資料庫	透過訪談及實際檢視方式，抽測10項資料庫安全檢測項目，包含特權帳號管理、資料加密、備份保護、弱點管理、存取授權、稽核紀錄及委外管理等安全機制，確認資料庫安全管理與防護狀況
5	**核心資通系統安全檢測**	核心資通系統內網滲透測試	1個核心資通系統	針對核心資通系統進行內網滲透測試，包括檢測資通系統之權限存取、應用程式及系統弱點、系統通訊保護等項目，若資通系統使用單一簽入進行權限管控，則亦納入檢測範圍
		核心資通系統防護基準檢測		依據系統等級(普、中、高)，針對核心資通系統之存取控制、識別與鑑別、系統與服務獲得、系統與資訊完整性及系統與通訊保護等控制措施進行檢測，並檢視源碼掃描、弱點掃描及滲透測試等檢測報告及修補紀錄，以及安全需求檢核結果
6	**網路架構檢測**	網路架構檢測	全機關	透過訪談及實際檢視方式，驗證網路與系統之管理控制措施、網路與系統之安全控制措施、網路與系統架構之備援機制、防火牆規則及存取控制，並確認資通系統管理及防護情形

技術檢測項目(3/4)

項次	技術檢測項目	技術檢測子項	執行範圍	執行方式
7	**組態設定** **安全檢測**	作業系統組態檢測 瀏覽器組態檢測 網通設備組態檢測 應用程式組態檢測	5台使用者電腦	• 針對作業系統(Win7、Win8.1、Win10及Win11)抽測18項政府組態基準設定 • 針對瀏覽器(IE8、IE11、Google Chrome、Mozilla Firefox及Edge)抽測12項政府組態基準設定 • 針對應用程式(Word 2016/2019、Excel 2016/2019、PowerPoint 2016/2019及Outlook 2016)抽測12項政府組態基準設定
			1台網域主機	針對作業系統(Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019及Windows Server 2022)抽測50項政府組態基準設定
			2台網通設備	抽測2類網通設備(Juniper Firewall、Fortinet FortiGate、無線網路及Cisco Firewall)各10項政府組態基準設定
			1台伺服器主機	抽測1類(Exchange Server 2013、IIS 8.5、Apache HTTP Server 2.4、SQL Server 2016、Red Hat Enterprise Linux 8及Red Hat Enterprise Linux 9)10項政府組態基準設定

技術檢測項目(4/4)

項次	技術檢測項目	技術檢測子項	執行範圍	執行方式
8	**網路惡意活動檢視**	惡意中繼站連線阻擋檢測	全機關	依照資安院每日公布之惡意中繼站名單，分別針對機關使用者網段及資通系統管理者網段進行檢測
		APT網路流量檢測		機關協助提供即時側錄之完整流量，透過部署資安院自行研發之APT流量偵測規則，針對機關內對外與外對內完整流量進行APT活動檢測

物聯網設備檢測範圍

項次	名稱	說明	範例
1	**網路印表機**	• 可使用RJ45進行控制之相關設備 • 提供紙張輸出功能	印表機、多功能事務機、影印機等
2	**門禁設備**	• 可使用RJ45進行控制之相關設備 • 提供門禁開關或設定功能	指紋機、指掌靜脈機、門禁卡機等、門禁管理伺服器等
3	**網路攝影機**	• 可使用RJ45進行控制之相關設備 • 提供影像錄製或影像顯示/儲存功能	攝影機、網路影像錄影機(NVR)等
4	**無線網路基地台/無線路由器**	• 可使用RJ45進行控制之相關設備 • 提供無線網路分享或控制功能	無線網路基地台、無線路由器、無線區域網路控制器等
5	**環控系統**	• 可使用RJ45進行控制之相關設備 • 提供監控機房溫度或濕度功能	溫度計、溼度計、機房溫度監控伺服器等
6	**網路儲存裝置(NAS)**	• 提供電子檔案儲存與讀取功能	網路儲存裝置(NAS)

物聯網設備檢測檢核內容

項次	構面	項目名稱
1	身分鑑別	管理介面存取須具備並啟用身分鑑別功能
2		管理介面通行碼具備並啟用複雜度要求
3		管理介面通行碼須具備並啟用最小長度限制
4		管理介面須具備並啟用限制錯誤嘗試之機制
5		管理介面身分鑑別不得使用預設帳號通行碼
6		資料存取須進行權限控管，並以最小權限為原則
7	系統安全	軟/韌體、作業系統及相關應用程式不得存在CVSS v3高於7分(含)之CVE漏洞
8		設備所使用之網路服務面臨不正當輸入時，產品應正常運作，且不應出現非預期異常行為
9	資料安全	設備須具備並啟用日誌管理功能
10	通訊安全	若設備具WPS功能則須關閉

資料庫安全檢測檢核內容(1/2)

項次	類別	檢測項目
1	特權帳號管理	變更資料庫預設管理帳號
2		啟用帳號鎖定次數
3		啟用帳號鎖定時間
4		啟用通行碼複雜度原則
5		啟用通行碼長度原則
6		啟用通行碼最長有效期限原則
7		限制管理者帳號透過遠端存取
8	資料加密	資料庫資料具有適當保護機制(包含加密、不可識別處理)
9		資料庫資料傳輸具有安全機制
10		資料庫加密金鑰具有適當保護機制
11	存取授權	限制資料庫主機服務埠
12		限制遠端存取來源
13		限制遠端存取帳號
14		限制遠端存取操作
15		資料庫帳號權限最小原則

資料庫安全檢測檢核內容(2/2)

項次	類別	檢測項目
16	稽核紀錄	啟用資料庫帳號變更稽核
17		啟用資料庫帳號登出/登入稽核
18		啟用資料庫結構變更稽核
19		稽核紀錄管理方式
20		資料庫主機時間校時
21		稽核紀錄分析
22	委外管理	委外廠商外部連線方式
23		委外廠商資料存取方式
24		委外廠商帳號授權方式
25	備份保護	資料庫定期執行備份
26		資料庫備份具有適當保護機制
27		資料庫備份回復測試
28	弱點管理	資料庫主機定期弱點掃描
29		資料庫主機弱點修補
30		修補資料庫主機安全性更新項目

網路架構檢測檢核內容(1/3)

項次	檢核內容	檢核結果	風險
1	**網路系統架構區域** 規劃網路區域，如伺服器區、資料庫區	未規劃網路區域	高
		未依規劃置放系統服務	中
		未明確劃分網路區域	建議
2	部署入侵偵測/防禦系統	未部署入侵偵測/防禦系統	中
3	部署系統本機安全機制 如HIDS、HIPS、本機防火牆	未部署系統本機安全機制	低
4	建立實體備援機制 從主機端至服務出口端經過的設備	重要資通設備未建立實體備援機制	中
		實體備援失效仍可維持機制	低
5	建立服務備援機制 網域名稱服務、系統服務	服務未建立服務備援機制	中

網路架構檢測檢核內容(2/3)

項次	檢核內容	檢核結果	風險
6	限制內部對外連線	未限制內部對外部連線	中
		內部對外部連線服務過於寬鬆	建議
7	**限制外部對內連線**	未限制外部對內部連線	高
8	**限制服務區域連線**	未限制服務區域連線	高
		服務區域連線過於寬鬆	中
9	**應不包含Permit All/Any於任一個規則**	包含Permit All/Any	高
10	**應定義Deny All/Any於最後一個規則**	未定義Deny All/Any	高
11	限制明文資料傳輸	與外網端點資料交換使用明文傳輸	中
		與內網端點資料交換使用明文傳輸	建議

網路架構檢測檢核內容(3/3)

項次	檢核內容	檢核結果	風險
12	網路設備存取鑑別	未配置網路設備存取鑑別	中
		管理者帳號未進行區分控管	建議
13	**網路設備存取控制**	未妥善管理邊界網路設備	高
		未配置內網網路設備存取控制	中
		已配置存取控制，但未生效	中
14	**網路設備SNMP設定**	配置可寫SNMP，使用預設通行碼	高
		配置唯讀SNMP，使用預設通行碼	中
		使用預設通行碼，但有配置存取控制	低
15	網路設備校時設定	未配置校時設定	中
		已配置校時設定，但未生效	中
		未部署校時伺服器	建議

113年資安稽核技術檢測結果

使用者電腦安全檢測

- 使用者電腦弱點掃描共發現664個高風險與117個中風險弱點
- 使用者電腦安全防護檢測顯示電腦皆未發現惡意程式，惟發現1台未落實更新病毒碼，39台未落實作業系統安全性更新，15台未落實更新應用程式

物聯網設備檢測

- 物聯網設備檢測結果共發現93項不符合項目，其中24.7%為「管理介面身分鑑別不得使用預設帳號通行碼」，20.4%為「軟/韌體、作業系統及相關應用程式不得存在CVSS v3高於7分(含)之CVE漏洞」

網域主機安全防護檢測

- 網域主機皆已部署防毒軟體且未發現惡意程式，惟發現1台未落實更新病毒碼，且2台未安裝所有安全性更新項目

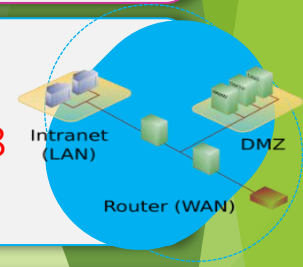
資料庫安全檢測

- 資料庫安全檢測結果共發現4項不符合項目，分別為「限制管理者帳號透過遠端存取」、「資料庫資料具有適當保護機制(包含加密、不可識別處理)」、「資料庫主機時間校時」、「修補資料庫主機安全性更新項目」

核心資通系統安全檢測

- 核心資通系統內網滲透測試結果共發現54個高風險、7個中風險及13個低風險弱點，其中52.7%屬於「無效的存取控管弱點」弱點
- 核心資通系統防護基準檢測結果共發現58個不符合項目

網路架構檢測



- 網路架構檢測共發現13個高風險、33個中風險及8個建議項目

組態設定安全檢測

- 共發現35台使用者電腦組態設定有未符合之項目
- 共發現1台網域主機組態設定有未符合之項目
- 共發現10台網通設備組態設定有未符合之項目
- 共發現4台伺服器主機組態設定有未符合之項目

網路惡意活動檢視

- 共發現184筆IP與677筆DN中繼站名單未阻擋
- 1個機關發現APT網路流量惡意行為

大綱

- 緣起
- 技術檢測
- **資安演練**
  - 網路攻防演練
  - 分散式阻斷服務攻擊演練
  - 跨國攻防演練
  - 紅隊演練
- 結論

網路攻防演練

網路攻防演練

目的

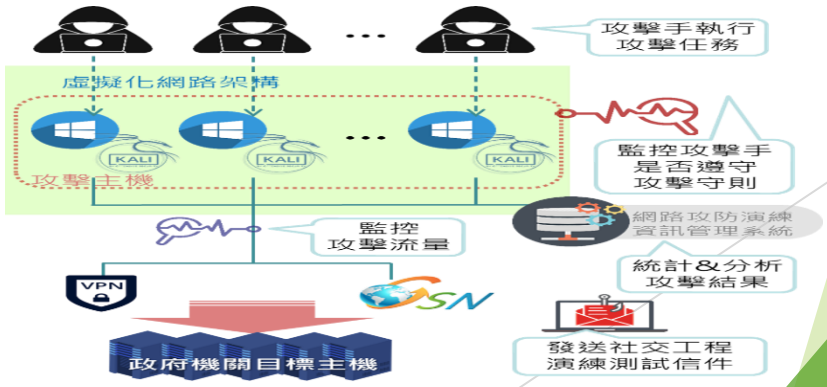
- 透過官學研界合作，邀集國內資安專業人員，檢測政府機關(構)所轄對外系統之資安防護能力
- 強化政府機關(構)所轄對外資通系統發生資安事件時之緊急應變、系統復原及協調管控等能力
- 檢視我國公務機關對外資通系統整體資安防護措施，並研議精進作為

社交工程演練

針對受測機關Email與其正副首長之公務手機門號，寄送社交工程郵件與簡訊，測試人員之資安意識

資通系統實兵演練

針對A級公務機關、直轄市政府及各縣市政府所維運之對外資通系統與連網設備模擬駭客進行攻擊



弱點衝擊性判定原則

類型	重大衝擊性	高衝擊性	中衝擊性	低衝擊性
SQL查詢	透過資料庫語法取得資料庫(明文/密文)帳密或資通系統明文帳密	透過資料庫語法取得資料庫機敏資料或資通系統密文帳密	透過資料庫語法取得資料庫欄位資料(不含機敏/帳密)或僅取得帳號	透過資料庫語法或錯誤訊息取得資料庫欄位名稱
AP讀寫權限	具有可寫入OS特權路徑之權限	具有可寫入非OS特權路徑之權限或可讀取OS特權路徑檔案	具有可讀取Web跨目錄或非OS特權路徑檔案之權限	僅可讀取當前Web非公開目錄檔案之權限
惡意內容	成功寫入攻擊語法或竄改頁面，且受影響之頁面為任一使用者並可擴散至其他系統	成功寫入攻擊語法或竄改頁面，且受影響之頁面為任一使用者	成功寫入攻擊語法或竄改頁面，但受影響之頁面限定已登入之任一使用者	成功寫入攻擊語法或竄改頁面但受影響之頁面限定該登入使用者
帳號權限	▪ 取得OS管理者權限或足以證明權限等同system、root或sysadmin之帳號 ▪ 取得資通系統防護需求為高等級之管理者(或帳號控管)權限或OS一般使用者權限	取得資通系統防護需求為中或普等級之管理者(或帳號控管)權限或OS一般使用者權限	取得資通系統(分級不限)業務單位使用者權限但不具帳號控管功能	取得資通系統(分級不限)一般使用者權限
資料外洩與存取控管	▪ 取得任一特種個資(病歷、醫療、基因、性生活、健康檢查及犯罪前科) ▪ 取得國家機密文書(未達解密條件者)	取得一般個資 取得一般公務機密文書(未達解密條件者)	取得部分一般個資	取得非機敏且非公開資料
通用漏洞	▪ CVSS 9.0-10.0 ▪ CISA KEV網站所列之高風險弱點	CVSS 7.0-8.9	CVSS 4.0-6.9	CVSS 0.1-3.9

113年網路攻防演練重要結果

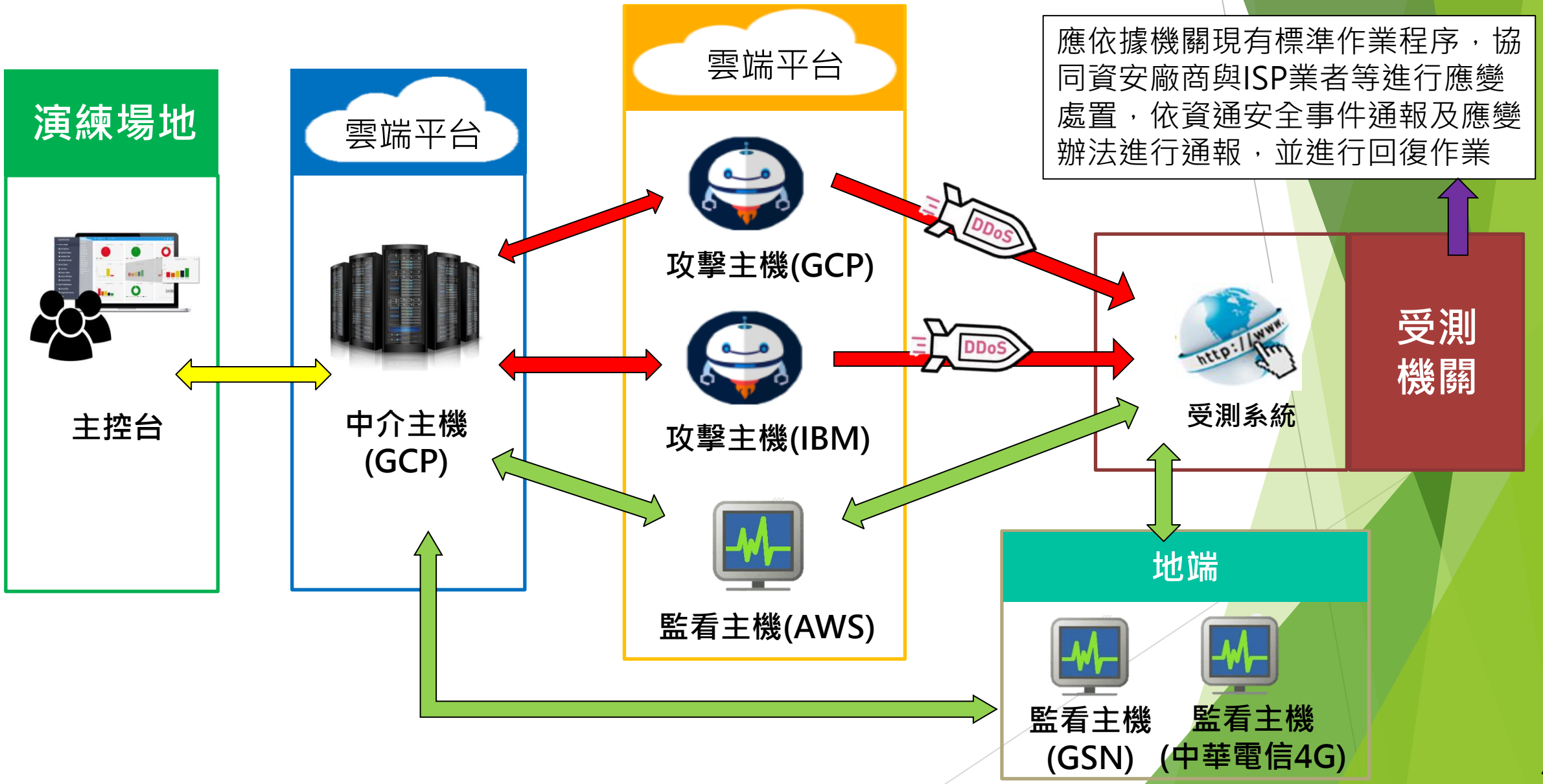
項次	弱點類型	常見攻擊手法	可能造成危害
1	**加密機制失效**	• 透過網頁原始碼或以工具攔截封包取得帳號通行碼 • 透過Adobe Reader複製圖片取得未遮罩之原始圖片 • 使用Google Hacking取得個資	• 取得系統管理權限 • 取得文件或系統儲存之機敏資訊(如個人資料)
2	**注入攻擊**	• 跨網站腳本攻擊 • SQL Injection攻擊	• 竊取使用者資訊 • 資料庫資訊外洩
3	**認證及驗證機制失效**	• 弱通行碼破解 • 透過系統手冊取得帳號通行碼資訊	• 取得系統管理權限或公開頁面修改權限 • 取得系統儲存之機敏資訊(如個人資料)
4	**無效的存取控管**	• 利用開發人員工具修改原始碼，將隱藏功能顯示於網頁上 • 透過目錄掃描或路徑猜測攻擊	• 取得系統管理權限或公開頁面修改權限 • 取得系統儲存之機敏資訊(如個人資料)
5	**不安全的組態設定**	• 使用預設之帳號通行碼登入 • 繞過檔案上傳格式限制 • 透過安全設定不足取得攻擊資訊	• 取得系統管理權限 • 被植入後門程式

分散式阻斷服務攻擊演練

分散式阻斷服務(DDoS)攻擊演練

- 針對選定之機關系統執行DDoS演練，以檢視機關防護機制對於分散式阻斷服務攻擊之抵禦及應變能力
  - 使用複合式DDoS攻擊手法，模擬駭客實際攻擊受測機關對外服務系統，嘗試造成服務異常與系統癱瘓
  - 當受測機關之對外服務系統遭受DDoS攻擊時，應依據機關現有標準作業程序，協同資安廠商與ISP業者等進行應變處置，如系統可用性遭受損害時，依資通安全事件通報及應變辦法進行通報，並進行回復作業

DDoS攻擊演練環境


演練場地
主控台
雲端平台
中介主機
(GCP)
雲端平台
攻擊主機(GCP)
攻擊主機(IBM)
監看主機(AWS)
DDoS
DDoS
受測系統
受測
機關
應依據機關現有標準作業程序，協同資安廠商與ISP業者等進行應變處置，依資通安全事件通報及應變辦法進行通報，並進行回復作業
地端
監看主機
(GSN)
監看主機
(中華電信4G)

113年DDoS攻擊演練發現

- 個別DNS伺服器遭受DDoS攻擊，皆防禦失敗
- 執行網路層攻擊時，同網段之其他主機服務亦會受到影響
- DNS伺服器遭受攻擊後，通報比率低
- 使用CDN技術分散攻擊，可有效抵禦DDoS攻擊
- 分段執行不同攻擊方式，較容易進行結果分析

DDoS攻擊防禦建議(1/2)

- 為防範DDoS攻擊，機關可採用以下設備或機制防禦DDoS攻擊，透過組合運用攻擊偵測、流量分類及回應等工具，阻擋非法流量並允許合法且正常之流量封包

防火牆	交換器與路由器	網站應用程式防火牆(WAF)與入侵防禦系統(IPS)	黑洞(Blackholing)	流量清洗	內容傳遞網路(Content Deliver Network, CDN)
可阻擋特定IP、連接埠及通訊協定，但不易防護混合式攻擊流量	透過限制速率與設定ACL等方式進行防護，部分設備還有延遲流量與入口過濾等防護功能，但皆會降低傳輸頻寬	透過特徵比對進行防護，可有效防護特定型態攻擊，但不易防護大流量攻擊或以合法流量掩飾非法流量之攻擊	將所有流量導入黑洞直接丟棄，此方式不區分合法與非法流量，可能影響系統可用性	將所有流量導入「清洗中心」進行分析，過濾非法流量後，再將合法流量導回用戶系統，若搭配骨幹級頻寬與大型資安防護設備，可有效阻擋DDoS攻擊	為一分散式網路系統，各CDN伺服器皆擁有原站伺服器網站資料，可透過近端CDN伺服器就近提供用戶服務，可有效阻擋針對網站之DDoS攻擊

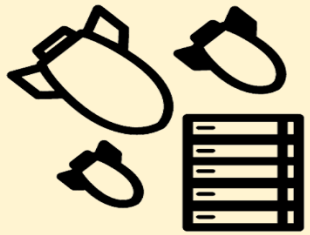
DDoS攻擊防禦建議(2/2)

- 除採用設備或機制防禦DDoS攻擊外，機關應依自身網路環境與系統服務屬性研擬DDoS應變程序，整體性規劃資源分配與配套措施
  - **內部**：事前規劃、研擬DDoS應變計畫與程序書、調校伺服器與網通設備，以及定期進行DDoS演練等
  - **外部**：規劃採用ISP業者之流量清洗服務、採用CDN服務架構

內部

事前規劃

調校設備



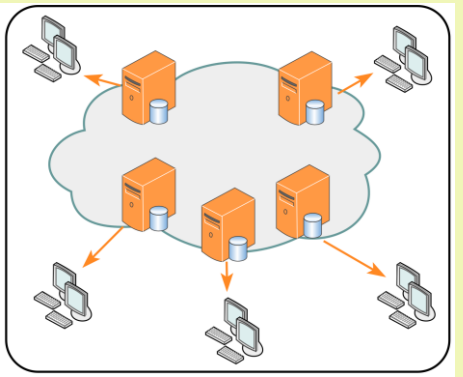
執行演練

綜合評估

研擬DDoS應變程序

外部

流量清洗



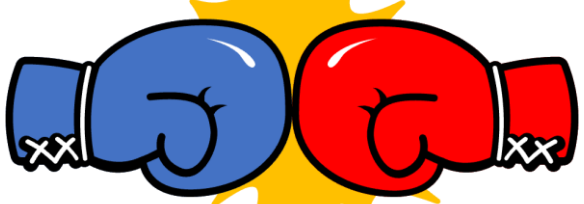
CDN架構

跨國攻防演練

跨國攻防演練

- Cyber Offensive and Defensive Exercise(CODE)

紅藍軍即時對戰



實兵演練

防禦方

攻擊方

關鍵基礎設施

金融領域

中油公司

台水公司

國內

國防部
國安局
調查局
刑事局
學研組

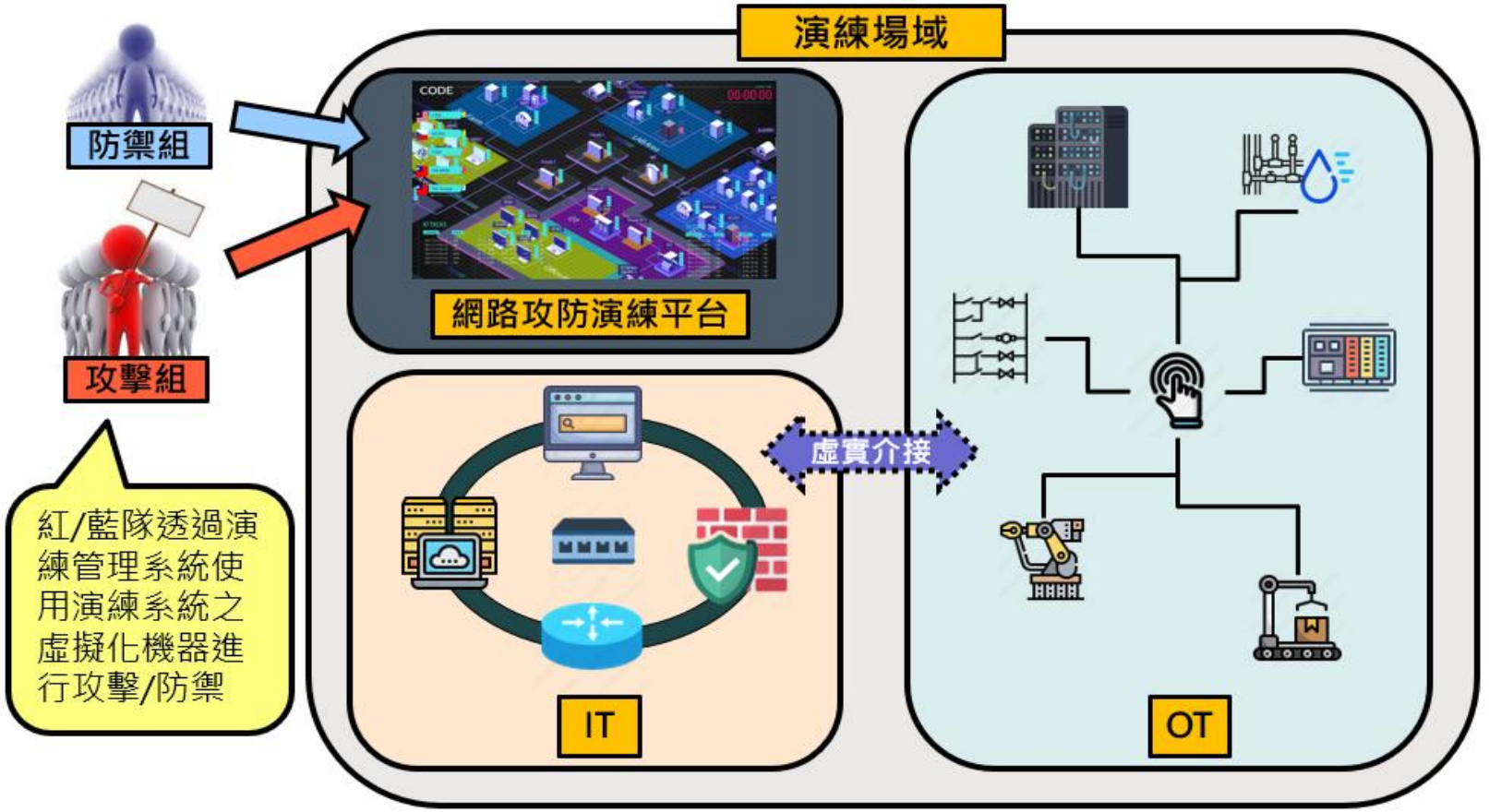
國外

政府單位
國際資安組織

CODE 2019 金融領域 DONE　CODE 2021 能源領域 DONE　CODE 2023 水資源領域 DONE

演練環境說明

- 演練場域係以CI領域工控(OT)場域為基礎，建立整合資通(IT)場域與工控(OT)場域之模擬攻防演練場域，並透過演練管理系統即時呈現演練過程



演練管理系統

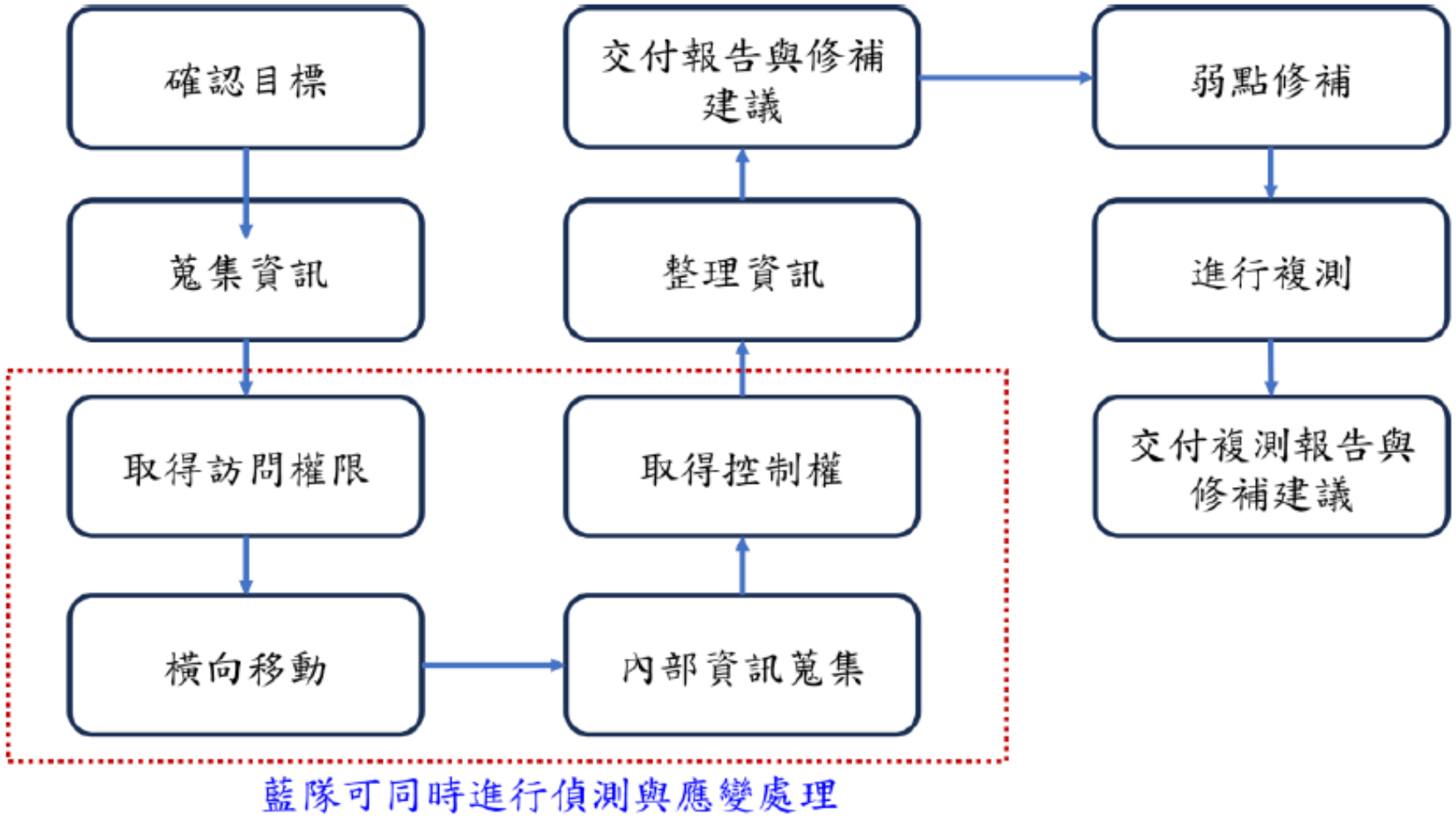
- 即時呈現演練狀況

紅隊演練

紅隊演練

- 紅隊演練之主要目的係藉由模擬實際攻擊之戰略、技術及流程(Tactics, Techniques, and Procedures, TTP)，找出整體資安問題，並確認遭受攻擊時之應變能力，藉由改善機關之人員、流程及技術，以提升資安準備度並降低整體資安風險
- 紅隊演練是更全面之檢測方法，檢測標的通常不是單一系統或設備，而是整體機關，檢測方式大都包含多個攻擊面向，包括社交工程、外部與內部攻擊及應用程式弱點等，以檢視受測目標維運上可能存在之資安風險，並檢視受測目標防禦機制之有效性，以持續提升資安防護能力

紅隊演練作業流程

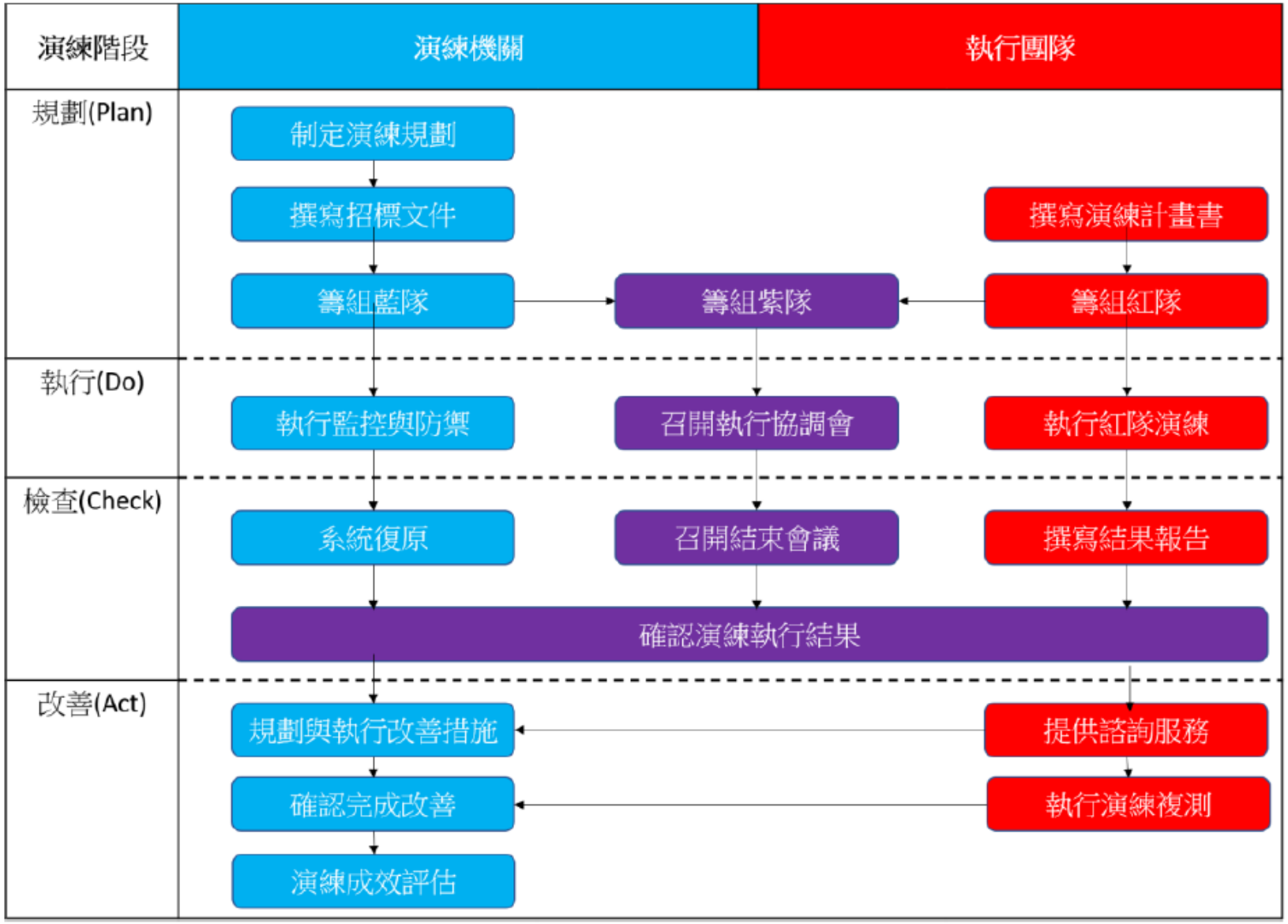

確認目標
蒐集資訊
取得訪問權限
橫向移動
內部資訊蒐集
取得控制權
整理資訊
交付報告與修補建議
弱點修補
進行複測
交付複測報告與修補建議
藍隊可同時進行偵測與應變處理

弱點掃描、滲透測試及紅隊演練比較

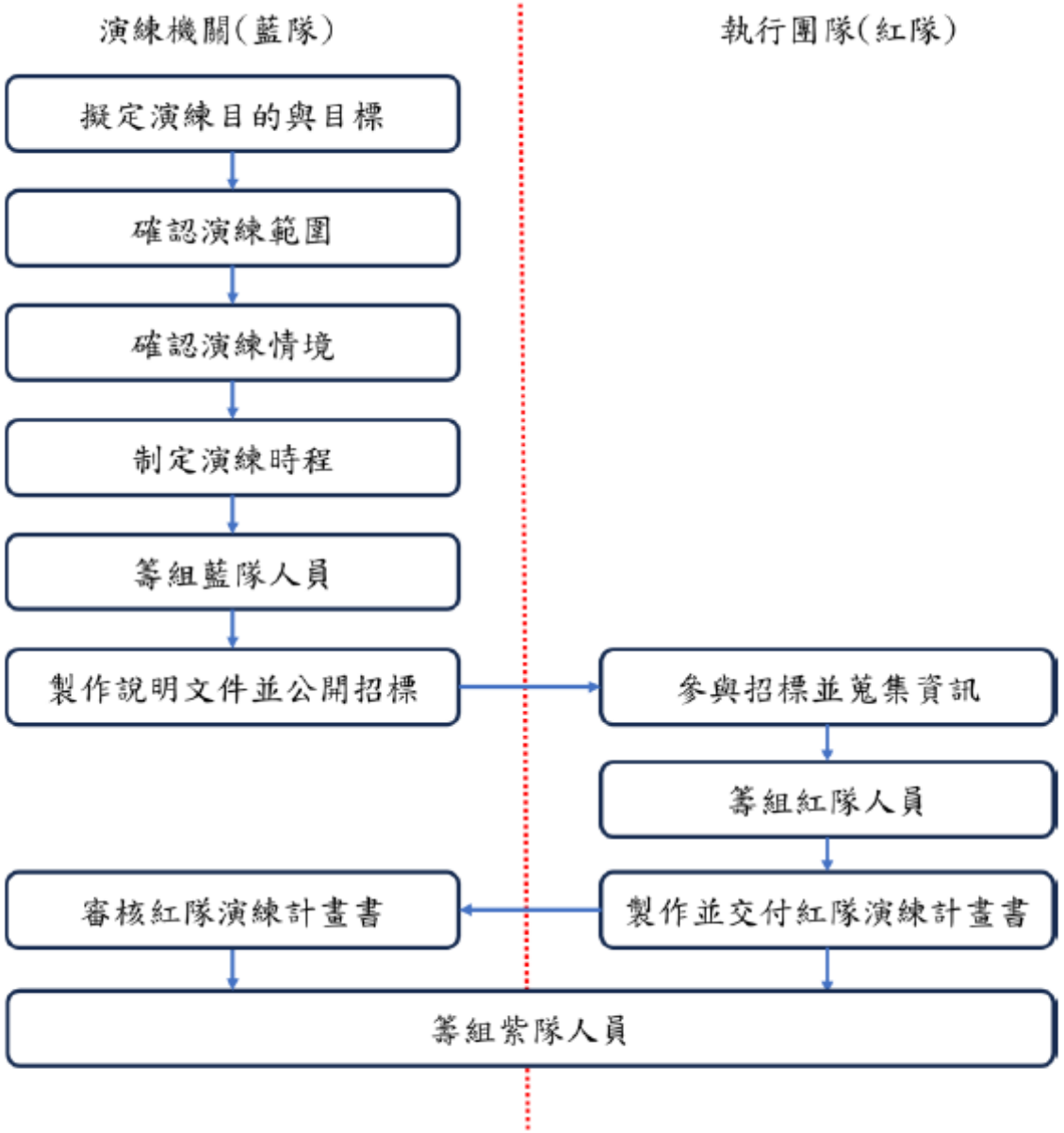
檢測方式	弱點掃描	滲透測試	紅隊演練
目的	主要用於快速且大量識別系統、應用程式或設備之已知弱點	由具駭客能力之專業人員模擬攻擊者行為，試圖找出所有已知與未知之弱點並進行弱點利用，以確認可能造成之危害	由專業演練團隊模擬實際攻擊之戰略、技術及流程，找出機關整體資安問題，並確認遭受攻擊時之應變能力，藉由改善人員、流程及技術，以提升資安準備度，並降低整體資安風險
檢測方法	執行自動化工具進行掃描	具駭客思維與能力之專業人員模擬攻擊	專業演練團隊模擬攻擊
範圍	單一系統之已知弱點	單一系統或網路之已知或未知弱點	受測機關整體(含設備、系統、網路、人員及作業流程等)
執行頻率	每季或每半年執行1次	每年執行1次	每1~2年執行1次
每次執行所需時間	數日	1~2週	1~6月

紅隊演練作業參考指引

紅隊演練流程

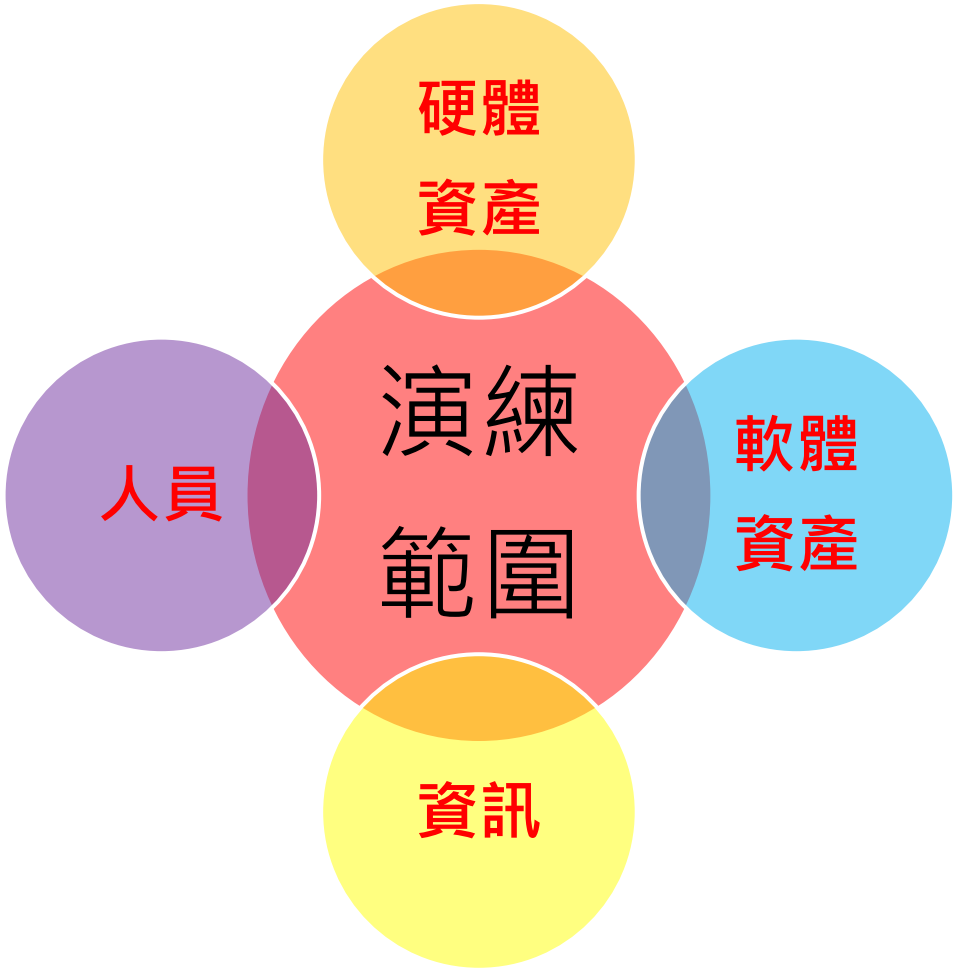


1.規劃階段細部流程


演練機關(藍隊)
執行團隊(紅隊)
擬定演練目的與目標
確認演練範圍
確認演練情境
制定演練時程
籌組藍隊人員
製作說明文件並公開招標
參與招標並蒐集資訊
籌組紅隊人員
審核紅隊演練計畫書
製作並交付紅隊演練計畫書
籌組紫隊人員

確認演練範圍

如伺服器、防火牆、入侵防護系統及員工個人電腦等



如正式員工、約聘人員及工讀生等

如作業系統、自行開發之應用程式及套裝軟體等

如數位與紙本文件資訊等

確認演練情境(1/2)

- 可根據機關需求與組織現況而採用不同之演練情境執行，至少包含外部入侵與內部網路滲透
- 如有對外服務並委外開發多項專用軟體時，建議可優先選擇結合外部入侵、內部網路滲透及應用程式弱點情境

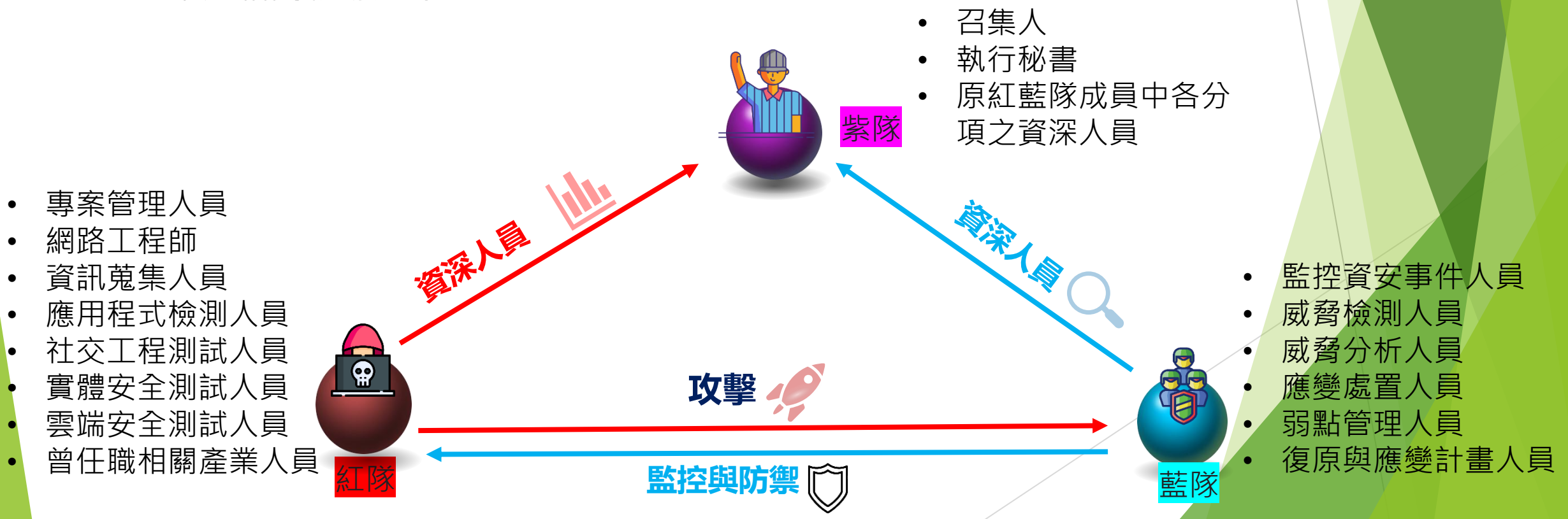
演練情境	演練方式與效果
外部入侵	模擬外部攻擊者由外部試圖入侵機關之內部網路，如透過對外服務系統之弱點或社交工程等攻擊。紅隊成員可能試圖入侵內部系統、竊取敏感資訊或取得內部使用者權限等，協助機關評估外部服務防護之有效性
內部網路滲透	紅隊可以試圖進入內部網路，然後橫向移動，試圖存取其他系統和資源，協助機關評估內部網路之安全性
應用程式弱點	紅隊可以模擬對機關應用程式之攻擊，試圖利用應用程式弱點，協助機關發現與修復弱點，以防止遭攻擊者針對應用程式弱點進行攻擊而造成之危害

確認演練情境(2/2)

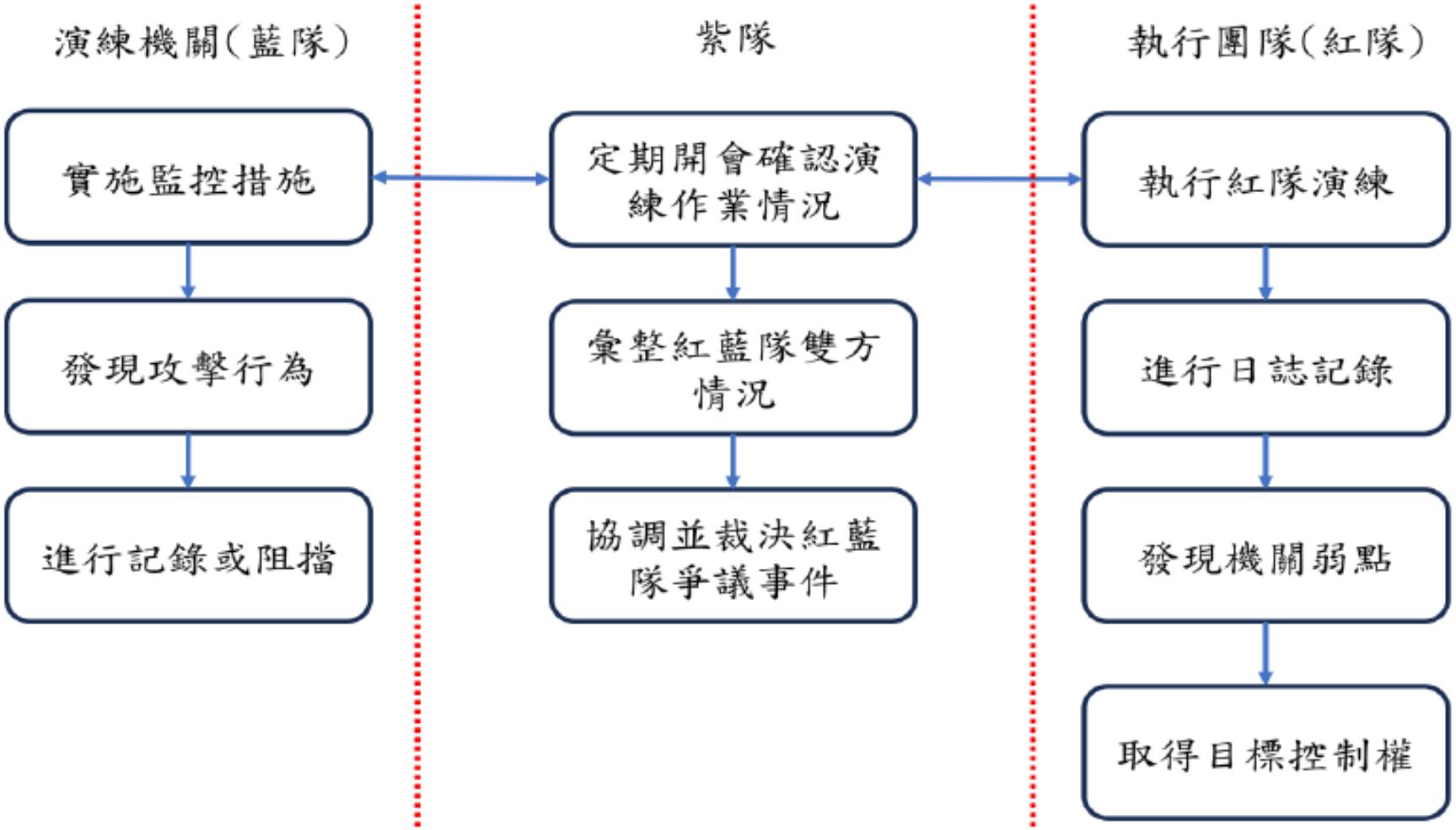
演練情境	演練方式與效果
雲端安全測試	對於使用雲端服務之機關，紅隊可以模擬攻擊雲端環境，試圖入侵或滲透雲端服務，協助機關評估使用雲端服務之安全性
社交工程攻擊	紅隊成員可以模擬釣魚攻擊、偽裝為受信任的人員或單位，或試圖誘導員工洩漏敏感資訊的攻擊，協助機關評估員工對於社交工程之警覺與資安意識
工業控制系統(ICS)攻擊	對於使用工業控制系統之機關，紅隊可以模擬對ICS與SCADA系統之攻擊，協助機關評估工業控制系統資通安全防護之安全性。若機關本身有使用該系統建議列為優先演練情境
內部威脅	模擬來自內部使用者的威脅情境進行攻擊，如員工故意或不小心洩漏敏感資訊，或試圖濫用其權限存取應用程式或資源，協助機關評估內部安全控制措施與防護偵測機制之有效性
實體入侵	紅隊可以嘗試模擬進入機關設施之攻擊，如潛入辦公區域或機房等敏感區域，協助機關評估實體安全防護措施之有效性

籌組演練團隊

- 紅隊演練團隊包含紫隊、藍隊及紅隊
  - **紫隊**：主要負責整體演練溝通協調任務，並於演練過程進行裁判工作
  - **藍隊**：主要負責演練過程中之監控與防禦，並視演練情境規劃，進行弱點修補與通報應變作業
  - **紅隊**：主要負責執行攻擊，並於演練過程中試圖達成演練目標，並記錄演練過程中之相關軌跡紀錄



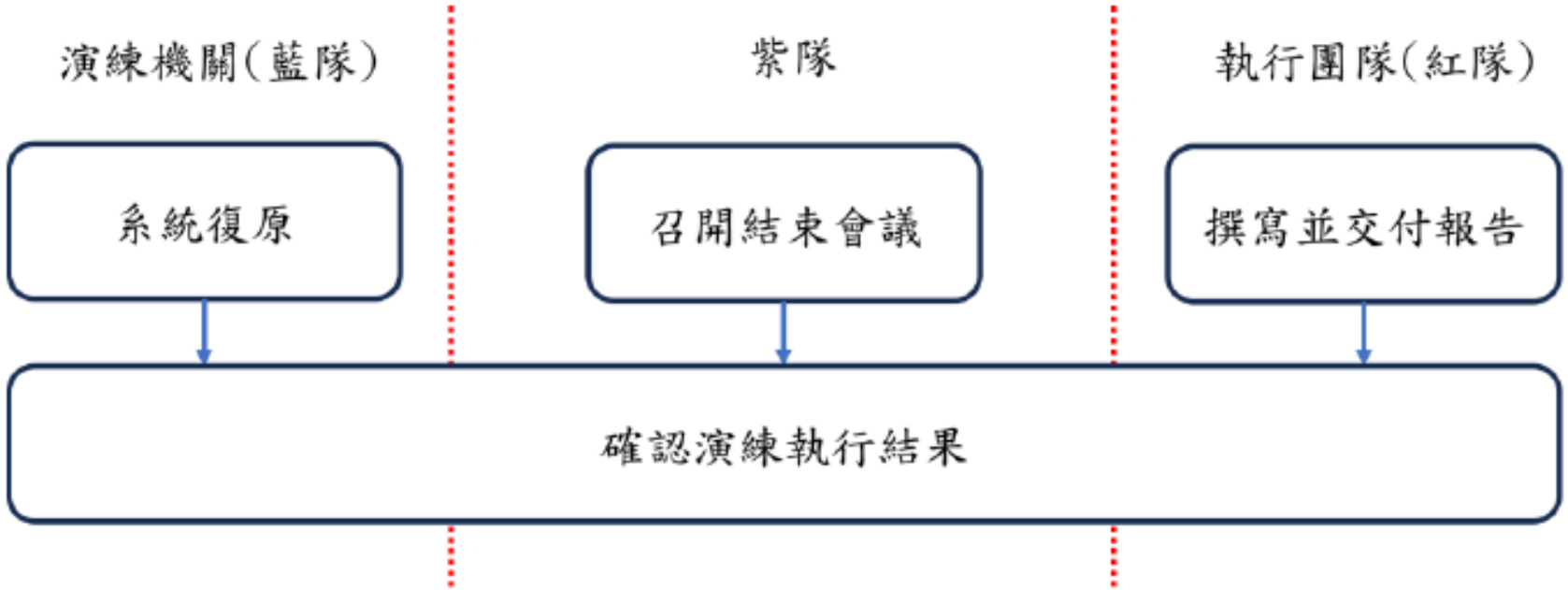
2.執行階段細部流程


演練機關(藍隊)
紫隊
執行團隊(紅隊)
實施監控措施
發現攻擊行為
進行記錄或阻擋
定期開會確認演練作業情況
彙整紅藍隊雙方情況
協調並裁決紅藍隊爭議事件
執行紅隊演練
進行日誌記錄
發現機關弱點
取得目標控制權

紅隊演練執行

- **紅隊**
  - MITRE ATT&CK提供網路攻擊戰術矩陣，包含14種網路攻擊戰術與245種技術(2025年4月發布之ATT&CK v17.1版)，紅隊可依照相關戰術與技術制定攻擊策略
- **藍隊**
  - 針對制定之演練情境，進行演練攻擊行為之監控，或執行通報應變處置及弱點修復作業

3.檢查階段細部流程

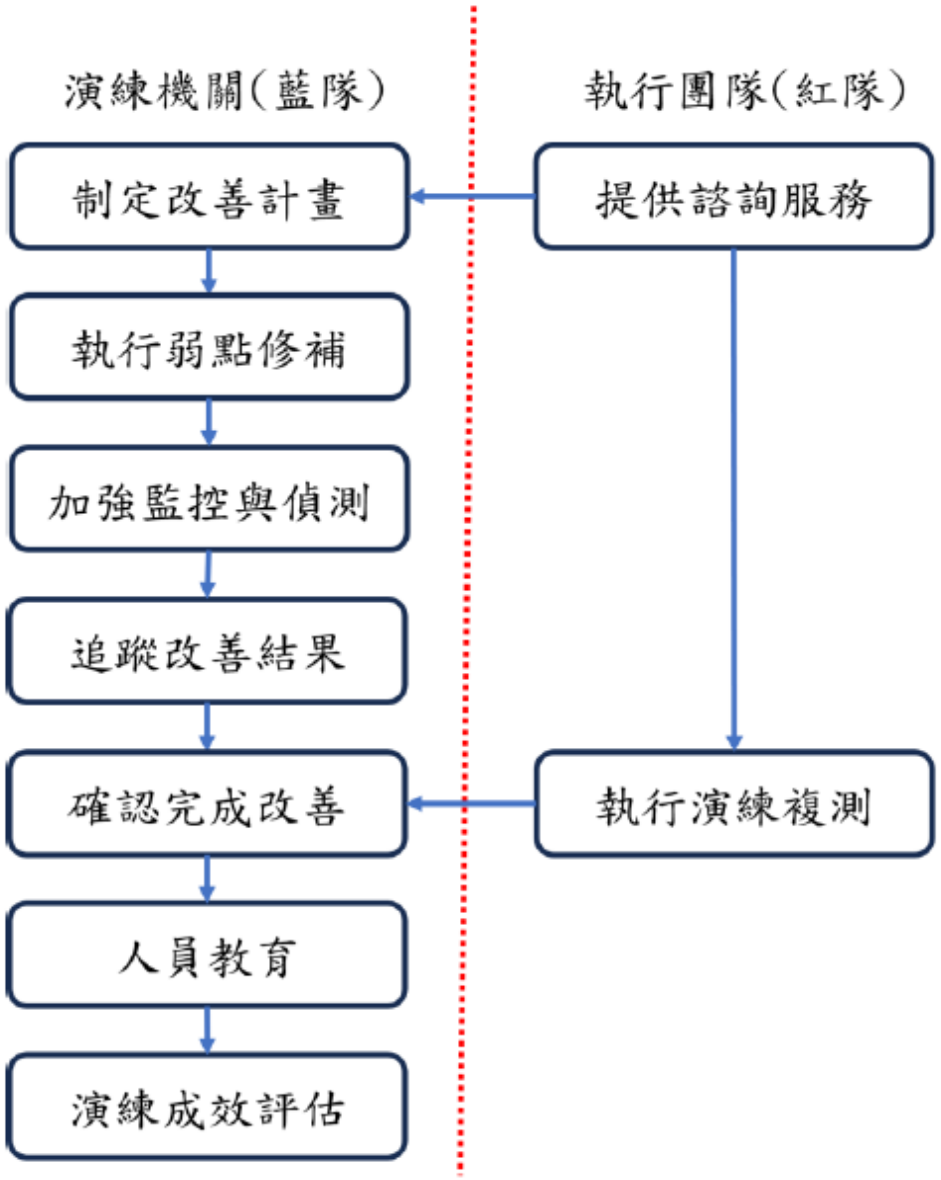


確認演練執行結果

- 演練機關收到報告後，應與紅隊針對報告發現之弱點與機關潛在之威脅進行確認，並衡量改善方式之可行性

確認項目	說明
情報蒐集	確認蒐集可供後續作業之資訊，為機關潛在但不易發現或管理之風險
社交工程攻擊資訊	社交工程攻擊成功之機關成員名單
弱點探測與利用	演練發現之系統存在已知或未知弱點
身分認證測試	弱密碼與驗證繞過等相關弱點
內部橫向移動	內部可利用橫向移動之設備或系統
偵測系統繞過	機關監控與偵測系統存在可以繞過之弱點
無法及時修補項目	藍隊偵測所轄系統受攻擊但未能及時修補之弱點

4.改善階段細部流程


演練機關(藍隊)
執行團隊(紅隊)
制定改善計畫
提供諮詢服務
執行弱點修補
加強監控與偵測
追蹤改善結果
確認完成改善
執行演練複測
人員教育
演練成效評估

制定改善計畫(1/2)

- 機關確認演練結果後，須接續訂定改善計畫，並進行追蹤與管理

改善方式	說明
弱點修復與防禦強化	根據演練發現之弱點進行修復，同時加強資安措施，如防火牆、入侵偵測系統及資安政策等，以減少攻擊成功機率
加強監控與偵測	根據攻擊紀錄修改相關偵測規則，以避免再遭受相同攻擊
進行複測	確認修復後之弱點已不存在
人員教育	提供全體員工與相關利害關係人之資安宣導與訓練，以提高員工識別與應對威脅能力

制定改善計畫(2/2)

- 針對紅隊演練規劃內容與執行情形，可參考美國國家安全專家Zenko在「Red Team: How to Succeed By Thinking Like the Enemy」一書中所提出之6個項目進行執行成效評估，並進行檢討與提出改善方案，作為未來持續辦理紅隊演練之參考

評估項目	說明
高層支持	高階管理階層應確實了解紅隊評估效益，並給予相對應之人力、資源及回報層級，才能確保紅隊執行任務順遂
若即若離	紅、藍隊於執行過程中應保持適當距離
擁有技能的專家	要依據當次任務，組成具備相關技能及經驗之團隊
足智多謀	紅隊開始執行時，應針對目標，採用「大膽假設，小心求證」之方式，逐步找出問題並提供相對應之解決建議
願意聽壞消息並據此採取行動	高層應正視及願意撥出時間來瞭解紅隊演練結果及建議
適可而止	提出演練重點發現及建議措施後，則應結束此項任務及作業，如同專案管理，沒有完美的專案，只有依計畫管理與進行之專案

大綱

- 緣起
- 技術檢測
- 資安演練
- **結論**

結論

落實執行技術檢測及資安演練，

可降低機關整體資安風險

有效提升資安防護能量與認知意識

報告完畢
敬請指教