資安作為監管
以PT-ABC 架構實作分享為例
2018/12/13

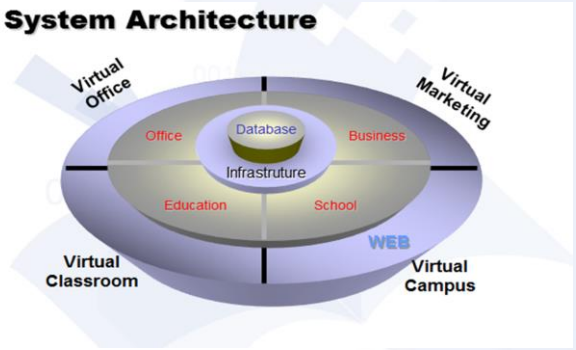
Agenda:

- 聲明與緣起-大考中心的資安經驗
- 檢視架構-監管
- CIO (資訊長)又愛又恨的滲透測試
- 資安攻防演練中心攻防架構
- PT – ABC 架構實作
- PT – ABC 成果報告與檢討
- APP PT – ABC 成果報告與檢討
- Next : PT - AABC
- 結語與建議

[Creative excellent @ SCE]

中國文化大學
推廣教育部
資訊長
資訊管理學系
助理教授 陳仁偉
Eric Chen

陳仁偉 博士
Eric Chen



- ✓ 中國文化大學推廣教育部 資訊長
  資訊管理學系 助理教授
- ✓ 大學入學考試中心
  2011.-2014 第二處(考務與資訊) 處長
- ✓ 中國文化大學
  推廣教育部
  2007-2009 資訊長辦公室 專案總監
  2002-2009 校園科技研發中心 主任
  1997-2001 系統開發組 組長
- ✓ 2005-2008 連續三年獲選微軟最有價值專家 Microsoft MVP
- ✓ 重要資訊專案經歷

2017.8-2018.7 慈濟大學教務系統轉移案
2017.9-12 資安攻防演練中心先導實作PT-ABC(已申請專利)
2017.9-2018.3 資安攻防演練中心先導實作案
2017.1-2017.7 台北市政府資訊企業架構(EA)先導研究案
2015-2017 Qubo 空間智能管理機研發
2011-2014 製卷高速掃描比對自動化品管系統
2012-2014 大學不同管道入學學生學習表現之資訊平台
2011-2014 取得 ISO 27001、 9001、 BS10012 資安、服務與個資認證
2011-2012 大學校院系所與招生資訊服務整合平台開發計畫
2011-2012 推動高中英語聽力測驗、開辦大陸考場
2011-2013 建置綠色節能資安機房、資安網路與虛擬化專案
2008-2009 RFID 旗艦計畫 – 文化、清雲、 育達
2007-2008 經濟部科專-NFC行動支付平台建置案
2005-2006 台灣創意中心資訊系統建置案
2005 交通大學IC電子錢包學生證專案
2005.12 國立台北教育大學課業輔導平台建置案
2004.3-2005.8 中國文化大學電子公文系統
2004-2006 台北市教育大學校務系統建置案
1997-2007 規劃開發中國文化大學推廣教育部EduRP資訊系統

聲明

不是駭客

我是挨踢(IT)人

防範資安挨踢分享

你現在將一個大學資訊化做好了，只是一個大學，
你如果到大考中心來，影響的是台灣所有的大學

- 前大學入學考試中心主任 牟宗燦

提升大考中心的資訊安全

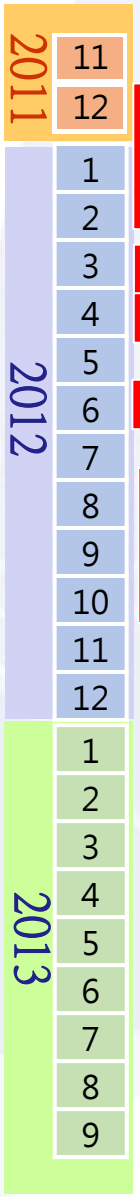
內心OS：
這是一個無法容忍絲毫錯誤的地獄場域
更可怕的是，你不知道問題何時發生，令人逼逼(Bee & Bird)
跟資安人一樣，不知道何時會發生問題，何時會挨踢

求助 HITCON 核心成員

防不勝防

資訊安全改善計畫

0 綠色節能資安機房



1. 建置應用程式防火牆(AP Firewall)與網路紀錄器
2. 資料備份儲存暨網路效能提升計畫
3. 聘請資安專家定期協助檢視資安問題與進行弱點掃描
4. 資安電子事件簿
5. 進行虛擬網路(vLan)建置
6. 分兩階段進行虛擬化主機建置
7. 完成辦公室網路建置
8. 建置點對點加密線路
9. 網路管理實務訓練
10. 進行高資安環境與網路建置
11. 架設網路流量統計MRTG
12. 研擬公布「個人資料使用告知事項」
13. 完成網路骨幹建置與結構化布線專案
14. 個人資訊管理BS 10012 主導稽核員認證課程
15. 資安區虛擬主機建置計畫
16. 網管與主機監控系統

持續改善，完成16個專案

考務與資安的共同點

都是利害關係人眾多，且程度落差很大的情境下
要推動與執行一套作業程序
近乎苛求地要求
零缺失

要達成零缺失的檢視架構
監管

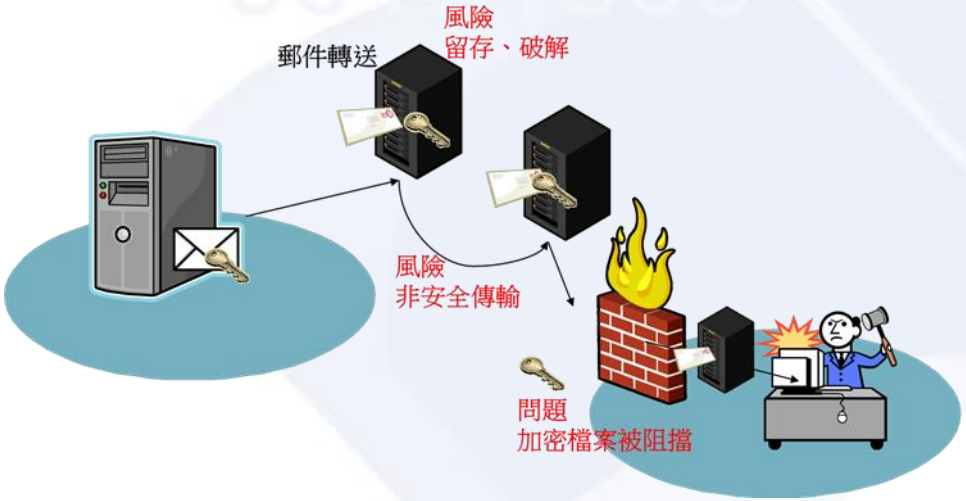
由試務零缺失的壓力而發展出的檢視架構 - 監管概念

規定：
有三等親參加考試者，不得擔任閱卷委員

新郵件架構

建置郵件伺服器
提供郵件帳號
以此帳號
透過安全通道登入網頁郵件
直接存取加密檔案
在使用者取得檔案之前，檔案均在中心伺服器中
可有效降低資安風險

現行郵件寄送個資之問題與風險



資安作為監管案例

觀念釐清
稽核、驗收與監管

- 稽核(查核)

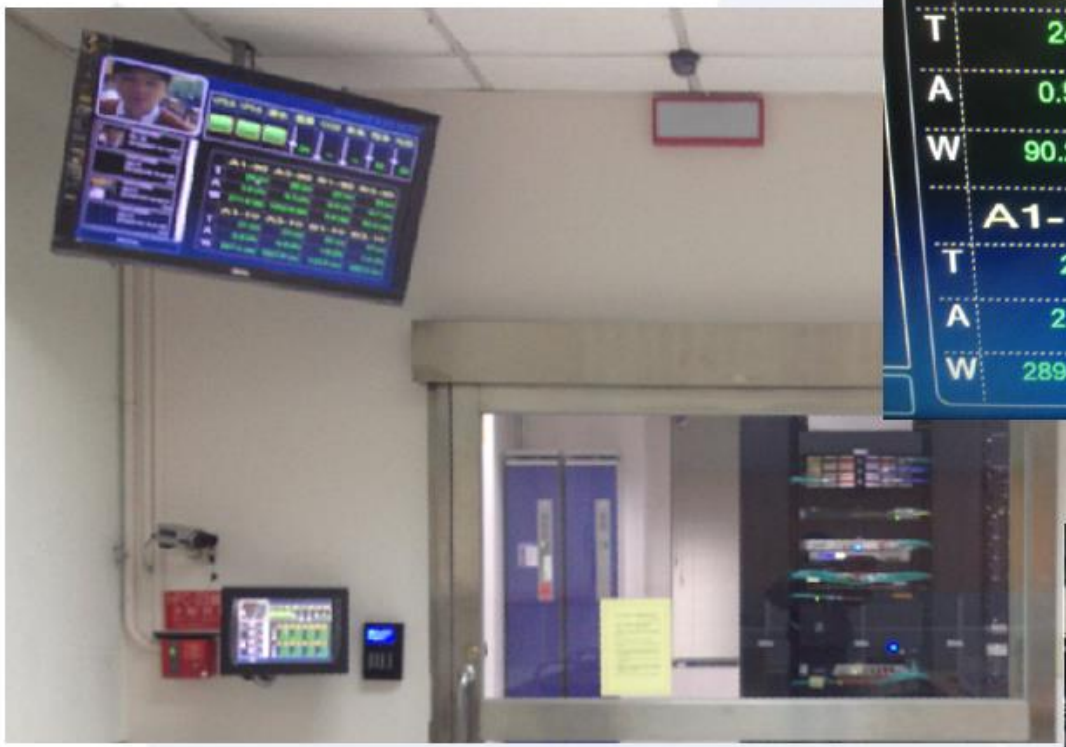
  - 定期抽樣檢查
  - 未檢查出問題，不代表沒有問題

- 驗收

  - 一次性確認符合規格標準

- 監管：監督管理的積極作為
  - 常態性確保運作機制符合消極作為(法規)
  - 全程監督，確保所有作業符合SOP，並且達到管理目標的要求
  - 透過監督管理作為來達成零缺失的目標

資安作為監管案例
資安電子事件簿



資安規定：
進出機房需要管制與登記工作事項
規定要定期檢視機房環控狀態

資安作為監管案例

- 要求：防範駭客攻擊與竊取資料
  - 實體隔離考務作業區網路(工作機)與行政作業上網區(上網機)
  - 60個員工的組織，佈署了880網點，每個員工預設提供四個網點
- 規定：使用者不得自行安裝規定清單外的軟體，要定期抽驗
  - 使用者的工作機與上網機均C槽還原卡管控，每日重新佈署；D槽設定加密
  - 導入虛擬桌面基礎架構(VDI)
  - 開發軟體與存取監控常駐小程式，自動回報系統清單與經USB傳送檔案之紀錄
- 要求：防止駭客一夜情
  - 內部服務主機夜間備份後， 上班前自動開機
  - NAS 區域儲存裝置備份後夜間自動關機，上班前自動開機

- 要求：....

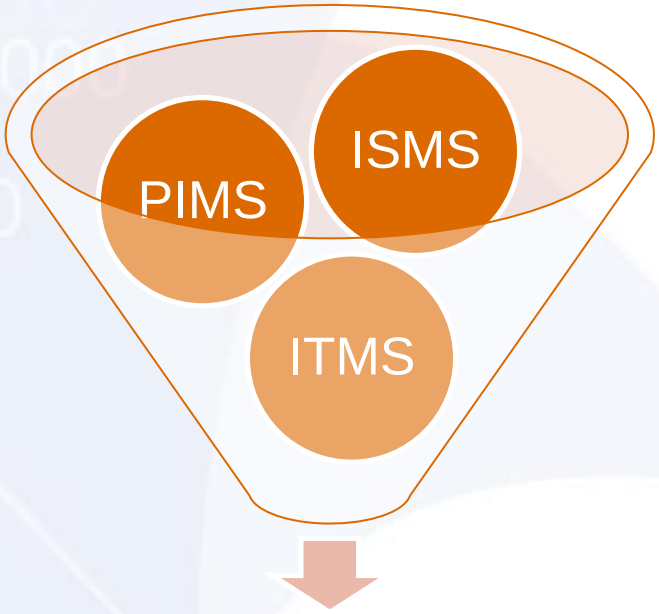
iSEC

IT Service and Security Enabling Capacity (1)

iSEC 系統結合IT 服務管理、資訊安全及個資保護管理

iSEC 系統功能

- 整合管理（提升有效性）
  - ISO 27001（資訊安全）
  - PIMS（個資保護）
  - ITMS（ IT 服務管理）
- 整合資訊
  - **iSEC 將資訊整合至單一系統**

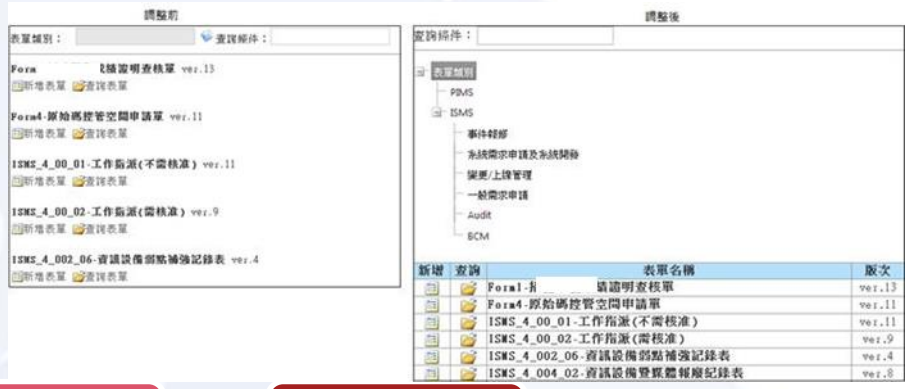


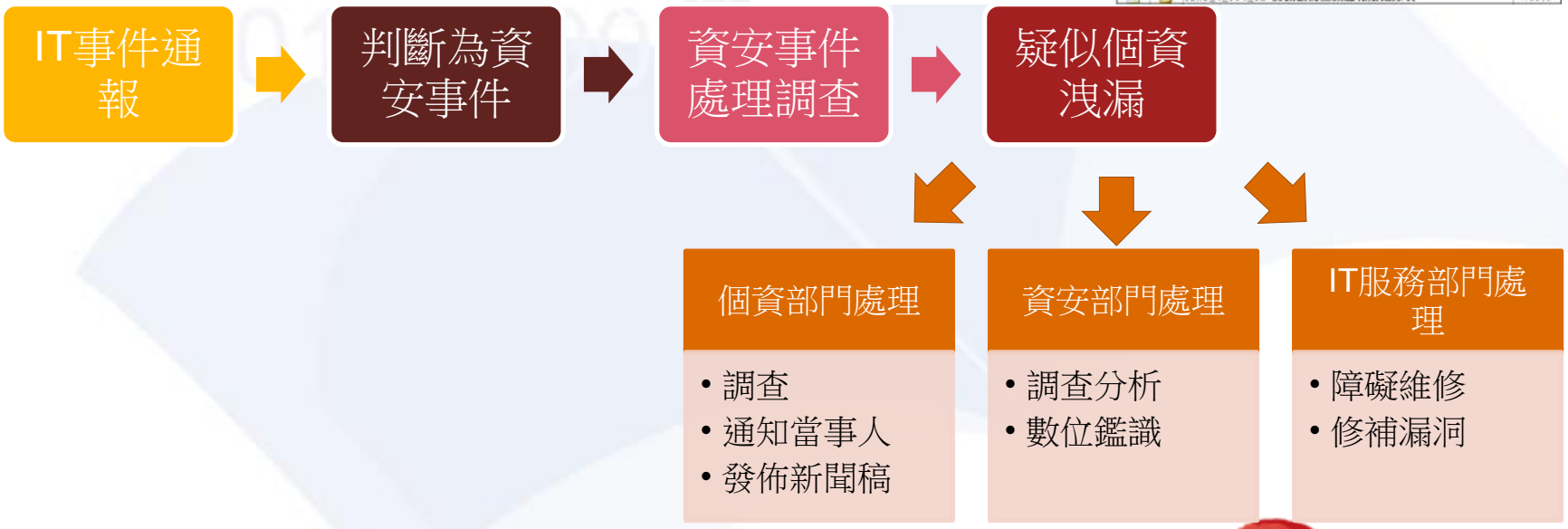
iSEC

IT Service and Security Enabling Capacity (2)

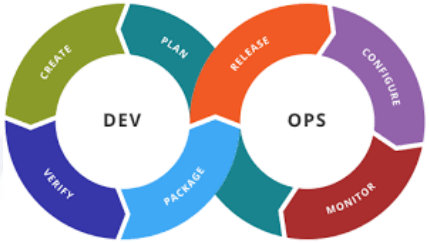
iSEC

- 整合平台案例





資安作為監管
DevSecOps



Category	Opensource tool name
漏洞評估 Vulnerability assessment	• NMAP • OpenVAS
靜態安全分析 Static security analysis	• FindBugs for Java • Brakeman for Ruby on Rails • Infer for Java, C++, Objective C and C • Cppcheck or Flawfinder for C/C++
網站安全 Web security	• OWASP dependency check • OWASP ZAP • Archni-Scanner • Burp Suite • SQLMap • w3af
通訊 Communication	• Nmap • NCAT • Wireshark • SSLScan • sslyze

資料來源：Hands-On-Security-in-DevOps

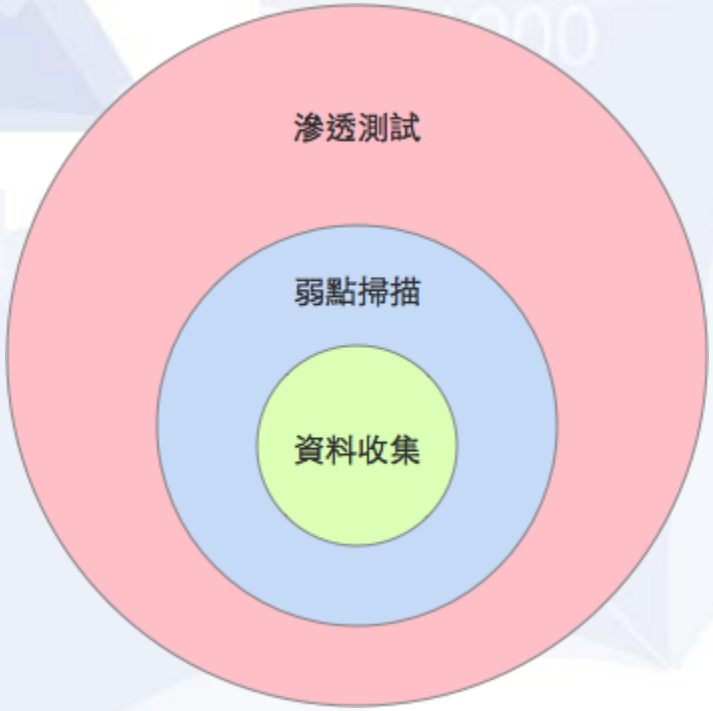
C2.1.2 靜態代碼審查
Static code review

- C2.1.2.1 靜態應用程序安全測試（SAST）
  - 靜態代碼掃描。 開發人員可以將該工具用作IDE插件的一部分，或者與每日構建一起觸發掃描。 為基本的代碼掃描工具。
  - FindSecbugs, Fortify, Coverity, klocwork.
- C2.1.2.2 動態應用程序安全測試（DAST）
  - DAST直接在運行時，由Web應用程序發送攻擊來識別安全問題
  - OWASP ZAP, Burp Suite
- C2.1.2.3 交互式應用程序安全測試（IAST）
  - IAST = RASP Agent + DAST
  - CheckMarks、Varacode
- C2.1.2.4 運行時應用程序安全保護（RASP）
  - 類似WAF的測試方式，RASP（Runtime Application self-protection）是一種在運行時檢測攻擊並且進行自我保護的一種技術
  - OpenRASP

	目的	開源工具
常見漏洞和風險（CVE）	了解雲服務中是否存在任何公開已知的漏洞。參考	OpenVAS, NMAP
誠信監控	它確定主要系統配置文件是否已被篡改	OSSEC
安全配置合規性	安全配置以滿足行業最佳實踐。	OpenSCAP

Category	Opensource tool name
基建安全 Infrastructure security	• OpenSCAP • InSpec
VM工具集 VM Toolset	• Pentest Box for Windows • Kali Linux • Mobile Security Testing Framework
安全監控 Security monitoring	• ELK • MISP—Open source Threat Intelligence Platform • OSSCE—Open source HIDS Security • Facebook/osquery—performant endpoint visibility • AlienValut OSSIM—opensource SIEM

資安作為監管
滲透測試監管
PT-ABC 架構實作分享



CIO (資訊長)又愛又恨的滲透測試

- 真正凸顯出還有哪些資安作為的不足
- 可依據最新駭客技術攻擊演練

- 項目
  - 要滲透測試那些項目
  - (~~OS：敢測什麼~~)
- 真實
  - 滲透測試結果報告到什麼程度
  - (~~OS：滲透測試結果，有多少是能浮上檯面~~)
- 涵蓋
  - 委託的資安廠商有沒有完全告知一切
  - (~~OS：廠商有沒有留一手，會不會開門揖盜~~)
- 掌握
  - 如何掌握資安廠商做了多少、做了什麼
  - (~~OS：沒缺失! 廠商到底有沒有測試啊~~)

The only thing we can do is *TRUST* !?

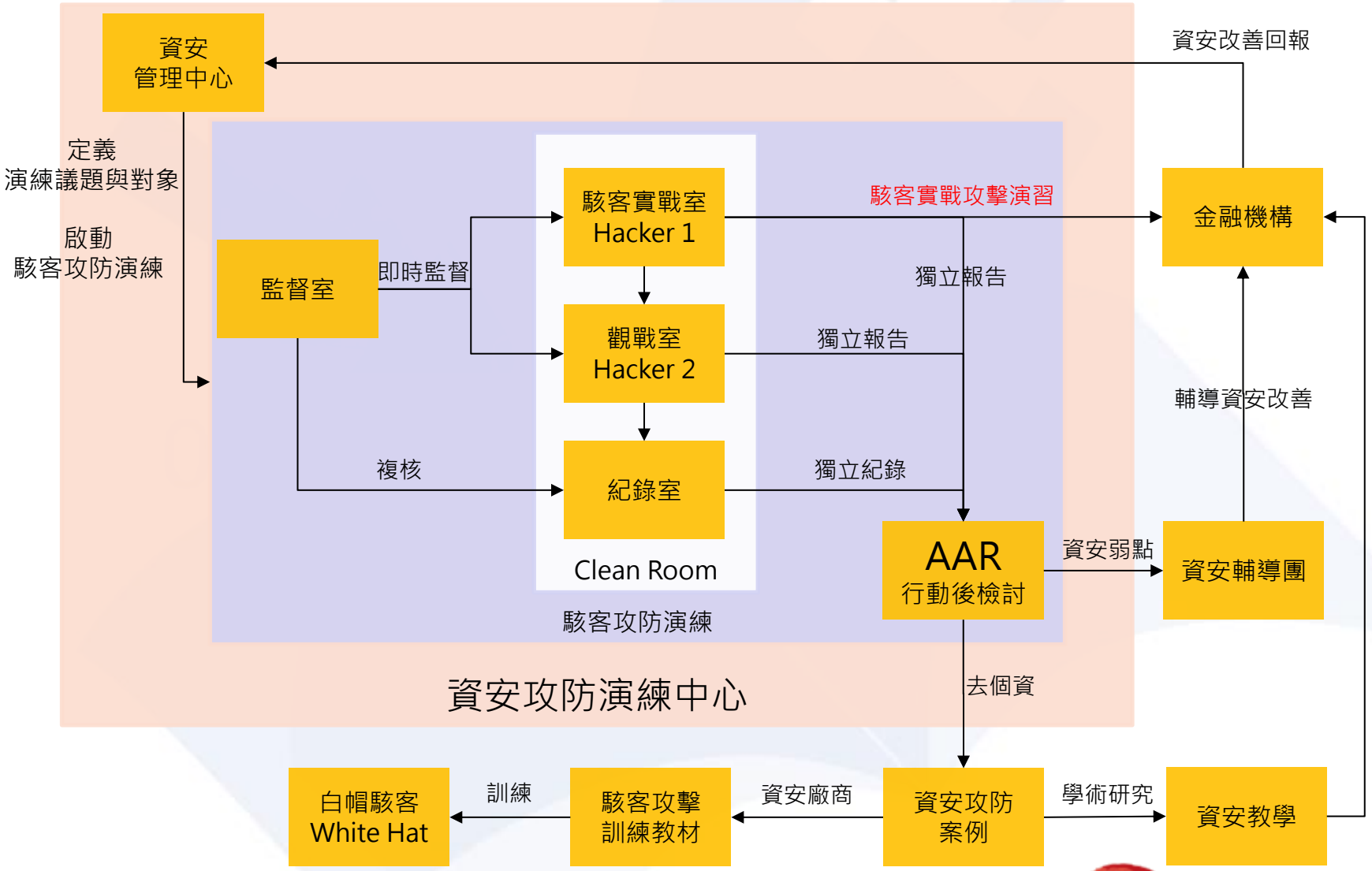
資安假想敵部隊攻防架構緣起

資安攻防演練中心

金融機構(必須匿名，請見諒)

董事會提出要求提升資安，具體掌握防駭量能

資安假想敵部隊攻防架構



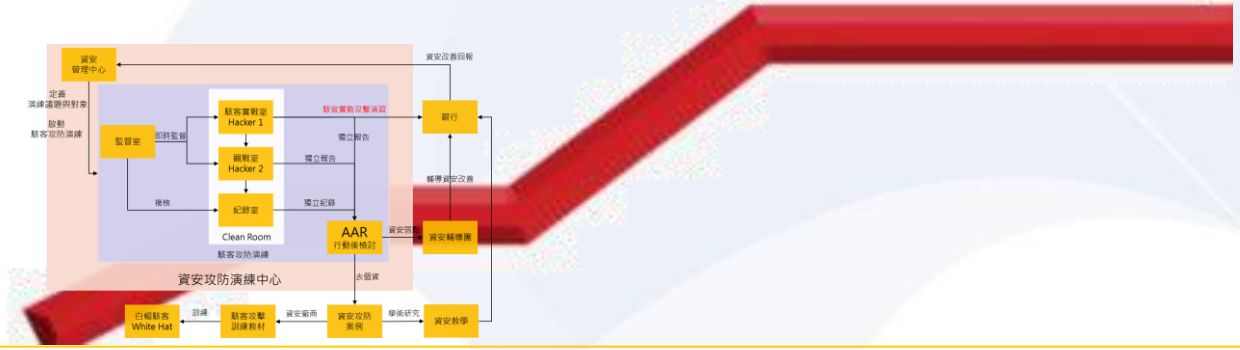
天時地利人和

- 蔡政府對資安的重視
- 主事者新上任
- 資訊與資安團隊的自信
- 董事會的支持

受委託籌畫紅隊滲透攻擊

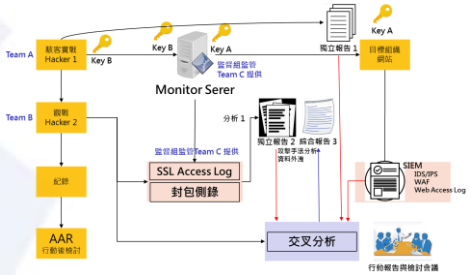
理想與實際的落差

- 觀戰
- 業務機密
- Peer
- Trust

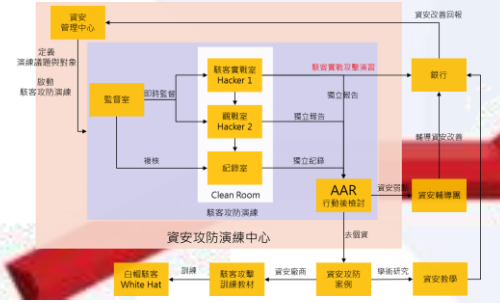


理想與實際的落差

- 觀戰
  - Packet Sideview
- 業務機密
  - Process Isolation
- Peer
  - Skill Segmentation
- Trust
  - Untrusty make trust



PT - ABC



PT – ABC 架構

PT – ABC 架構

- PT – Penetration Test
- ABC – Basic concept

團隊架構的不信任設計，產生可信任的結果

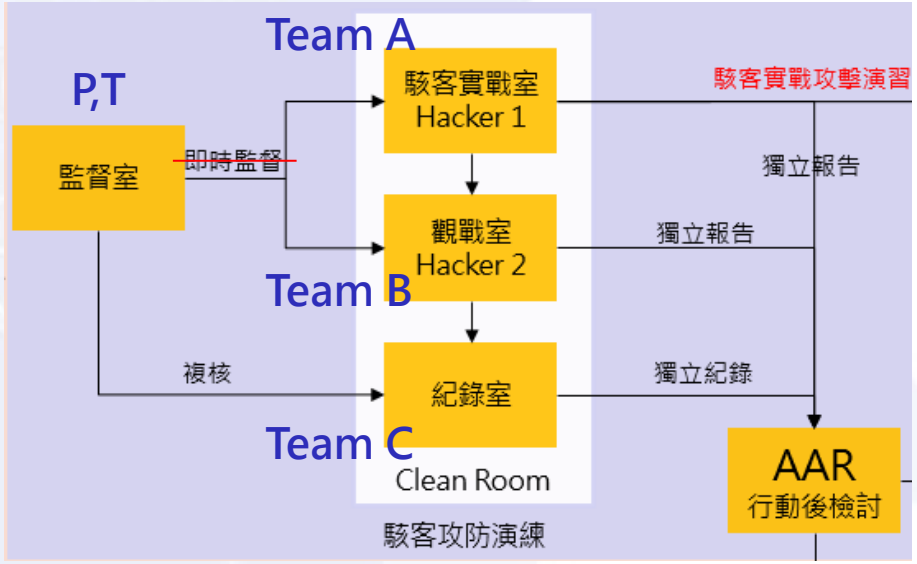
Untrusty design make trusty result

- P –業主 (Proprietor)
- T –公正第三方 (Third Party)
- A - Hacker 1 (Team A)
- B - Hacker 2 (Team B)
- C – 記錄管理服務組: (Team C)

資安攻防演練中心先導實作
PT-ABC 架構對應

- 業主 (P)
  - 金融機構指派
- 公正第三方 (T)
- Hacker 1 (Team A)
- Hacker 2 (Team B)
- 記錄管理服務組: (Team C)

對應關係

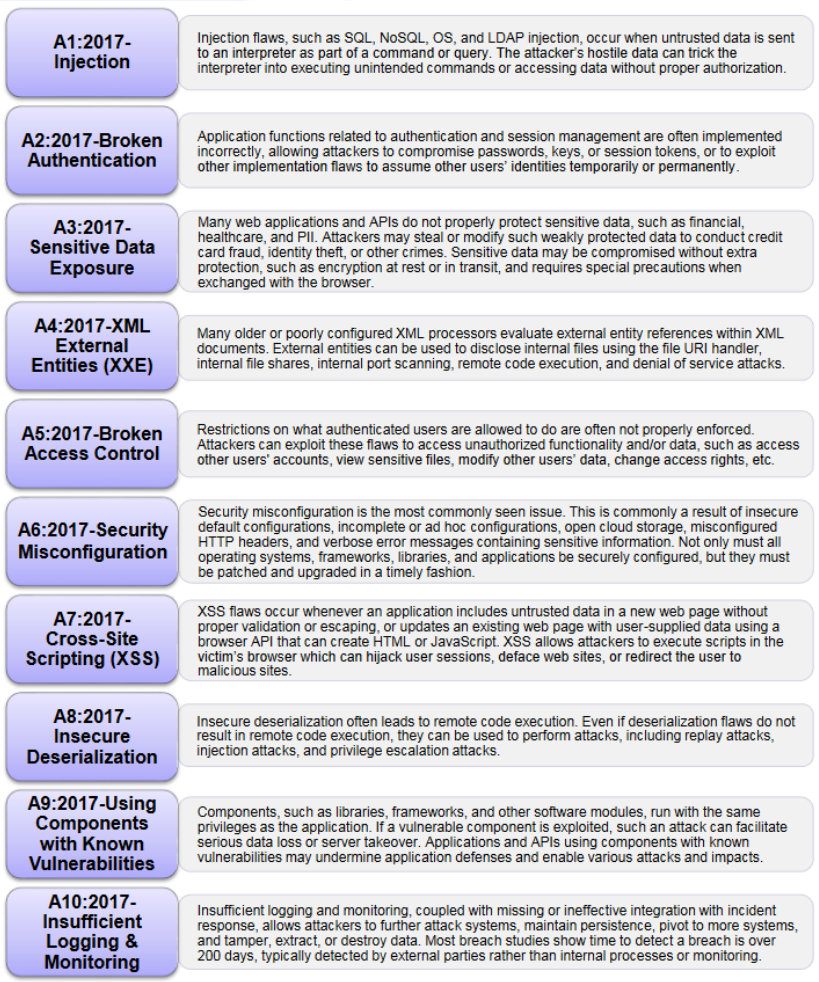


PT - ABC架構設計原則

- 團隊作業的不信任設計，產生可信任的結果
- 業主網域的全面紅隊滲透攻擊
- 有效監管
- 最少必須檢測項目與弱點報告分類
  - 議定以 2017 OWASP Top 10 為共同基礎
- 共同弱點風險等級定義

OWASP TOP 10 - 2017

- A1 注入攻擊
- A2 失效的驗證與連線管理理
- A3 跨站腳本攻擊
- A4 失效的存取控制
- A5 不當安全組態設定
- A6 敏感資料暴暴露
- A7 對攻擊手法的防禦不足
- A8 跨站請求偽造
- A9 使用已知漏洞洞元件
- A10 防護不足的API



共同弱點風險等級定義

- 重大風險
  - 具有可被立即入侵、服務中斷或機密資料洩露之風險
- 高風險
  - 可能會被入侵取得系統權限、服務中斷或機密資料洩漏之風險
- 中風險
  - 具有可輔佐或間接於入侵之風險
- 低風險
  - 潛在威脅，未來來可能提升為中、風險或是測試結果無法確認成功
- 無風險
  - 僅測試，其結果不存在風險

有效監管

- 跳板、監控主機
  - 業主提供硬體設備，事後回收
  - Team B 規劃軟體需求
  - Team C 負責、金鑰提供、安裝整合
  - T 監管

- 獨立網路
  - 中華電信光纖直接連接

- 機房監控、獨立資安機櫃，實體隔離彌封

- P資安與稽核會同彌封、T監管

業主須配合事項

- NTP 對時
  - 實戰前各相關設備、SSL Proxy Server 需做好校時工作，以利紀錄分析工作
- SSL Proxy Server
  - 專案期間只監管SSL Proxy Server IP 活動
  - 不要直接封鎖或阻擋 SSL Proxy Server IP 活動
- SIEM
  - 必須是解密、去機敏資料
  - 依照Team B要求提供該時段、型態的紀錄

建議事項

- 免責
  - 滲透測試旨在主動找出潛在問題，建請免除本次滲透測試所找出漏洞之相關資訊、資安人員的責任，以利本計畫的進行。

- 獎勵
  - 依找出弱點數量獎勵
  - 依找出弱點嚴重度獎勵

PT-ABC Team A
獨立報告 1

- D + 2 日 Team A 就找出高風險弱點，依合約規定兩小時內立即通知業主 P，並提供修復建議與協助修補弱點。
- Team A 在兩周的測試期間，找出[redacted]個重大風險、[redacted]個高風險、[redacted]個中風險弱點，共十二個弱點
- 風險等級會在行動報告與檢討會議時，再確認、共同重新定義

12個弱點，保護業主，後述僅以編號顯示

第一案AAR建議事項

- 弱點處理機制
  - 確認Team B可充分掌握 Team A攻擊行為，建立機制信任關係後
  - 建議調整重大弱點處理機制，仍然須於兩小時內通知，但不急著修補，待Team A已完整檢測此弱點影響程度後，再通知修補。
  - 發現重大弱點後，啟動通報與監管機制

- 免責
  - 滲透測試旨在主動找出潛在問題，建請免除本次滲透測試所找出漏洞之相關資訊、資安人員的責任，以利本計畫的進行。

第二案
Mobile APP PT-ABC

第二案
Mobile APP PT-ABC

- 源起
  - 第一階段PT-ABC，有優異的成果，業主 P 主動要求其即將上線的APP ，也進行APP滲透測試檢測，稱為第二案 Mobile APP PT-ABC
  - 讓PT-ABC 架構驗證能涵蓋到APP，更周延

- 依據
  - OWASP
    - Open Web Application Security Project
  - MASVS：OWASP 行動應用安全驗證標準 v 0.9.4
    - MASVS ：The OWASP Mobile Application Security Verification Standard

OWASP Mobile Top 10 2016

M1
作業系統平臺使用不當

M2
不安全的資料存儲

M3
不安全的通信

M4
不安全的認證

M5
加密不足

M6
不安全的授權

M7
用戶端程式碼品質問題

M8
竄改APP程式內容

M9
逆向工程

M5
多餘的功能

Mobile APP 攻防項目異同

- 相同
  - APP 網路服務主機攻防

M1
作業系統平臺使用不當

M2
不安全的資料存儲

M3
不安全的通信

M4
不安全的認證

- 增添
  - APP 逆向工程解析
  - APP 資料傳送解析

M5
加密不足

M6
不安全的授權

M7
用戶端程式碼品質問題

M8
竄改APP程式內容

M9
逆向工程

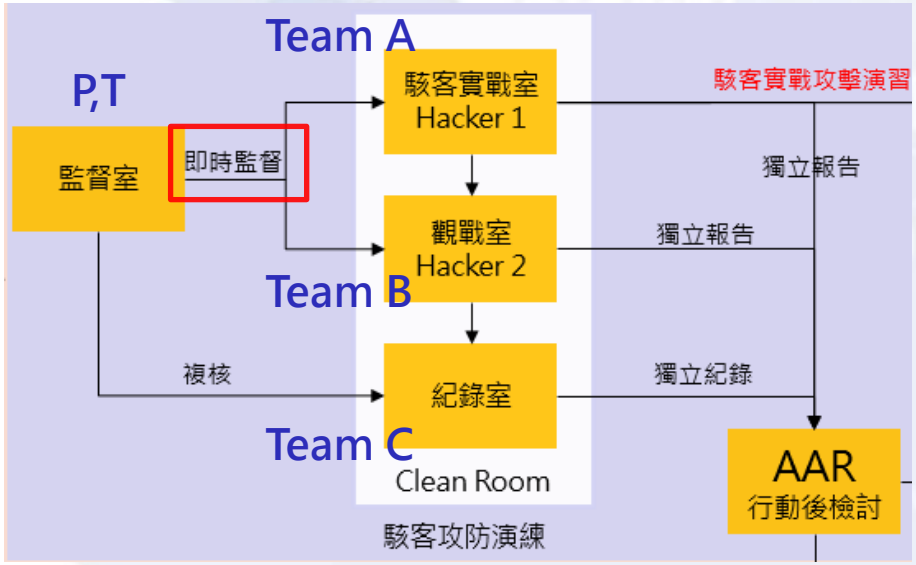
M5
多餘的功能

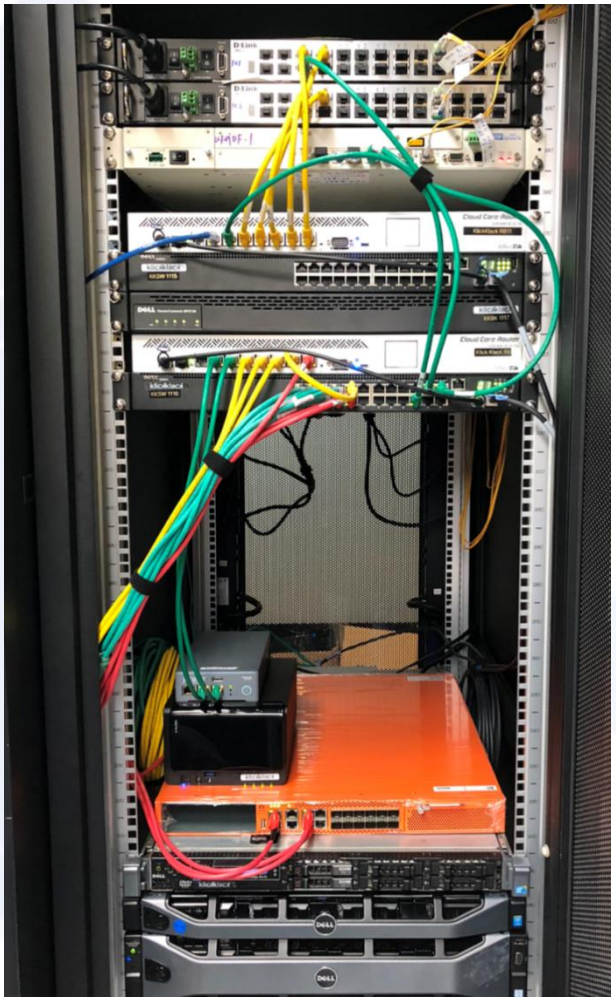
APP PT-ABC 架構設計原則

- 團隊作業的不信任設計，產生可信任的結果
- APP 動態與靜態測試
  - 動態APP網路連線功能弱點測試
  - 靜態APP逆向工程分析弱點測試
- 最少必須檢測項目與弱點報告分類
  - 議定以 OWASP Mobile Top 10 2016為共同基礎
- 共同弱點風險等級定義

第二案 APP PT-ABC 架構改善

對應關係





第二案
APP PT-ABC Team A成果

- Team A 在兩周的測試期間，找出[redacted]個高風險、[redacted]個中風險、[redacted]個低風險弱點，共十一個弱點

- 風險等級會在行動報告與檢討會議時，再確認、共同重新定義

第二案
APP PT-ABC 獨立報告3

APP 測試環境，業主沒有提供SIEM資料

第二案
APP PT-ABC AAR檢討事項

- Team B監管盲區
  - 由於APP下載到手機端，非連線型(靜態)PT、B隊無法監管

- 雙盲滲透測試
  - 第二結案會議時，提案取得同意，針對APP進行靜態分析雙盲測試
  - 稱為第二案+

第二案 +
Mobile APP PT-ABC +

B 隊
APP PT-ABC +測試規劃

- 雙盲測試
  - B 隊APP 靜態測試完全不知A隊的測試報告，獨立進行測試
- 相同PT規範
  - PT 規範重點不同，會造成不同的PT重點與結果
  - B隊也採取與A隊相同 OWASP Mobile 2016 Top 10 分析規範與風險等級定義
- 駭客擬真
  - 由APP Store下載正式的APP進行靜態分析
  - 測試結果可代表相同程度的駭客攻擊結果
- 符合保密規範
  - 測試者為B隊，第一、二案協助監管參與者，仍在保密規範要求中

B 隊
APP PT-ABC + 靜態測試結果

- 均為低風險
  - 多數弱點攻擊者需取得被滲透者手機，方能進一步取得攻擊成果
- 相同結果
  - 找出三項與A隊相同的結果
  - 此三項結果係受原第三方界接之限制，所呈現難以改善的弱點
- 差異
  - 有三項主要是Cache 型弱點
  - 三項冗餘功能
  - 容易改善

A, B 隊
APP靜態PT雙盲測試差異原因

- 焦點差異(動態與靜態測試)
  - A 隊主力測試網路連線動態弱點測試
  - B 隊主力關注非連線型 APP 靜態弱點測試
- 測試時間
  - 滲透測試結果與滲透測試時間有高度正相關
  - A 隊兩周測試時間，需分配在動態測試與靜態測試上
  - B 隊由於測試架構設計，全力在靜態測試
- 技術差異
  - 不同的駭客團隊有不同的PT技術專長

第二案 + AAR 建議事項

- 低風險
  - APP PT的結果雖然是低風險
  - 但技術上的低風險，可能是媒體操作議題上的高風險
  - 仍建議要處理
- 瀏覽器Cache
  - 這次APP PT發現三個Cache弱點，由於本案APP採包裝瀏覽器的架構
  - 建議檢查瀏覽器上是否有同樣Cache弱點
- API 界接
  - 應考慮跳脫 Web 包裝成APP的架構
  - 針對無法改善的第三方界接，改用直接APP API 界接技術

第二案 + AAR 建議事項
PT-AABC

- AABC 架構
  - 不同駭客有不同的工具、測試時間、測試方法，會產生不同的結果
  - 雙盲測試可讓PT更周延，也產生駭客技術切磋的效果
  - A隊也建議未來可考慮採用AABC架構，樂見AABC成形

- 已經獲得業主同意後續規畫滲透測試時，再進行採用PT-AABC架構

結語與建議

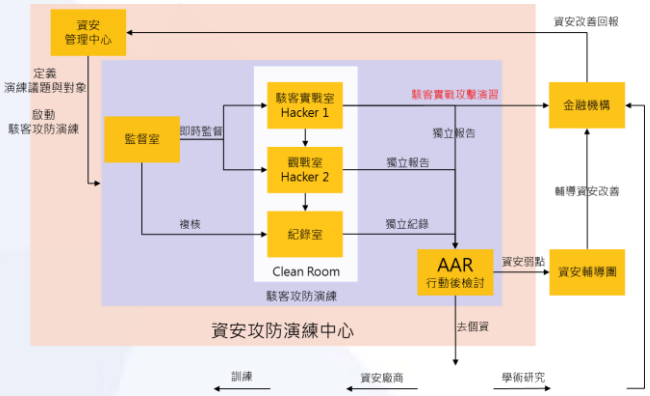
建議導入檢視架構

監管

資安零缺失

資安攻防演練中心的趨勢

- 現狀：
  - 組織各自進行資安防護與滲透測試的風險
  - 資安防護已非單一金融機構可以獨立支撐
- 機會
  - 美國國防部將駭客變成夥伴
    - Katie Moussouris
- 概念
  - 攻擊是最好防禦，藉由假想敵攻擊訓練來提升資安防禦能力
- Cyber Range 資安攻防演練
  - 已有多家資安攻防中心
  - 已定義好的狀況，適合學習，
- 資安攻防演練中心
  - 以駭客技術來實戰，同時保有稽核管控機制
  - 未來有機會發展成虛擬攻防



資訊安全

是金融機構 CIO、CISO 心中永遠說不出的痛

時代轉變

趨勢觀察

- 駭客攻防演練中心的出現是必然
- 駭客攻防演練中心將會是個資安產業鏈的一環
- 等待英雄

從架構概念提出到PT-ABC架構實戰驗證，已證明是這是可行且正確的方向，將是 CIO、CISO 都可依賴的資安解決方案之一

建議可規劃設立
共同PT-ABC 或 PT- AABC 監管中心

- 可採此監管機制，不需個別採購
- 此中心可勾稽所有測試結果
- 可評估滲透測試廠商的專業能力，進而提升資安產業
- 可精進中心同仁的專業能力
- 提供攻防演練監控環境
- 未來漏洞懸賞可以利用此機制，開放全球參與
- 並且依據實戰趨勢，提供跟得上時代的教育訓練

如能跨出這一步
影響的是
台灣所有企業與政府組織的資訊安全
是金融機構 CIO、CISO的救星