

IP Camera 資安輔導攻略

報告人：陳昶昕 技術長

中華民國 107 年 07月 24 日

CONTENT

- ◆ 資安新聞分享
- ◆ 輔導流程
- ◆ 檢測安全構面
- ◆ Privacy by Design(GDPR)

資安新聞分享



參考資料：

https://twcert.org.tw/subpages/securityInfo/loophole_details.aspx?id=4870

義籍駭客破解Master IPCAM01並取得root密碼

- (1)檔案雙向傳輸控管不周
- (2)內建寫死(hardcoded)系統密碼
- (3)無驗證Data閱讀異動
- (4)坊間已公開之IP camara帳密

```
Acta: admin / 1234567890
Appro: admin / 99999999
Avigilon: admin / admin
Axis: root / password
Basler: admin / admin
Boschs: service / service
Brickcom: admin / admin
Canon: root / (Ca...
CBC: admin / admin
CNB: root / admin
```

資安新聞分享



網路攝影機Pelco Sarix系列出現一打漏洞，
易遭遠端接管系統及檔案控制權

- (1) 訊息洩漏
- (2) Bypass身分驗證
- (3) 任意處置檔案
- (4) 擴權執行command
- (5) 緩衝區溢位

參考資料：

https://twcert.org.tw/subpages/securityInfo/loophole_details.aspx?id=4903

資安新聞分享



日本數十台同品牌網路攝影機
遭針對式入侵

據日本產經新聞報導，日本超過60台佳能(Canon)網路攝影機遭有心人士入侵，並在受影響的設備的視訊畫面上印有短語「I'm Hacked. bye2」。

因未更改攝影機的預設密碼所致

參考資料：

https://twcert.org.tw/subpages/securityInfo/hackevent_details.aspx?id=825

(二) 網路活動檢視

- 1、檢視網路設備、伺服器及物聯網設備之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。
- 2、檢視資安設備(如：防火牆、入侵偵測或防禦、惡意軟體防護、資料外洩防護、垃圾郵件過濾、網路釣魚偵測、網頁防護等)之監控紀錄，識別異常紀錄與確認警示機制。
- 3、檢視網路封包是否存在異常連線或異常網域名稱解析伺服器(Domain Name System Server, DNS Server)查詢，並比對是否為已知惡意 IP、中繼站或有符合網路惡意行為的特徵。

(三) 網路設備、伺服器、端末設備及物聯網等設備檢測

- 1、辦理網路設備、伺服器、端末設備及物聯網等設備之弱點掃描與修補作業。
- 2、檢測終端機及伺服器是否存在惡意程式，包括具惡意行為之可疑程式、有不明連線之可疑後門程式、植入一個或多個重要系統程式之可疑函式庫、非必要之不明系統服務、具隱匿性之不明程式及駭客工具等。
- 3、檢測系統帳號登入密碼複雜度；檢視外部連接密碼(如檔案傳輸(File Transfer Protocol, FTP)連線、資料庫連線等)之儲存保護機制與存取控制。

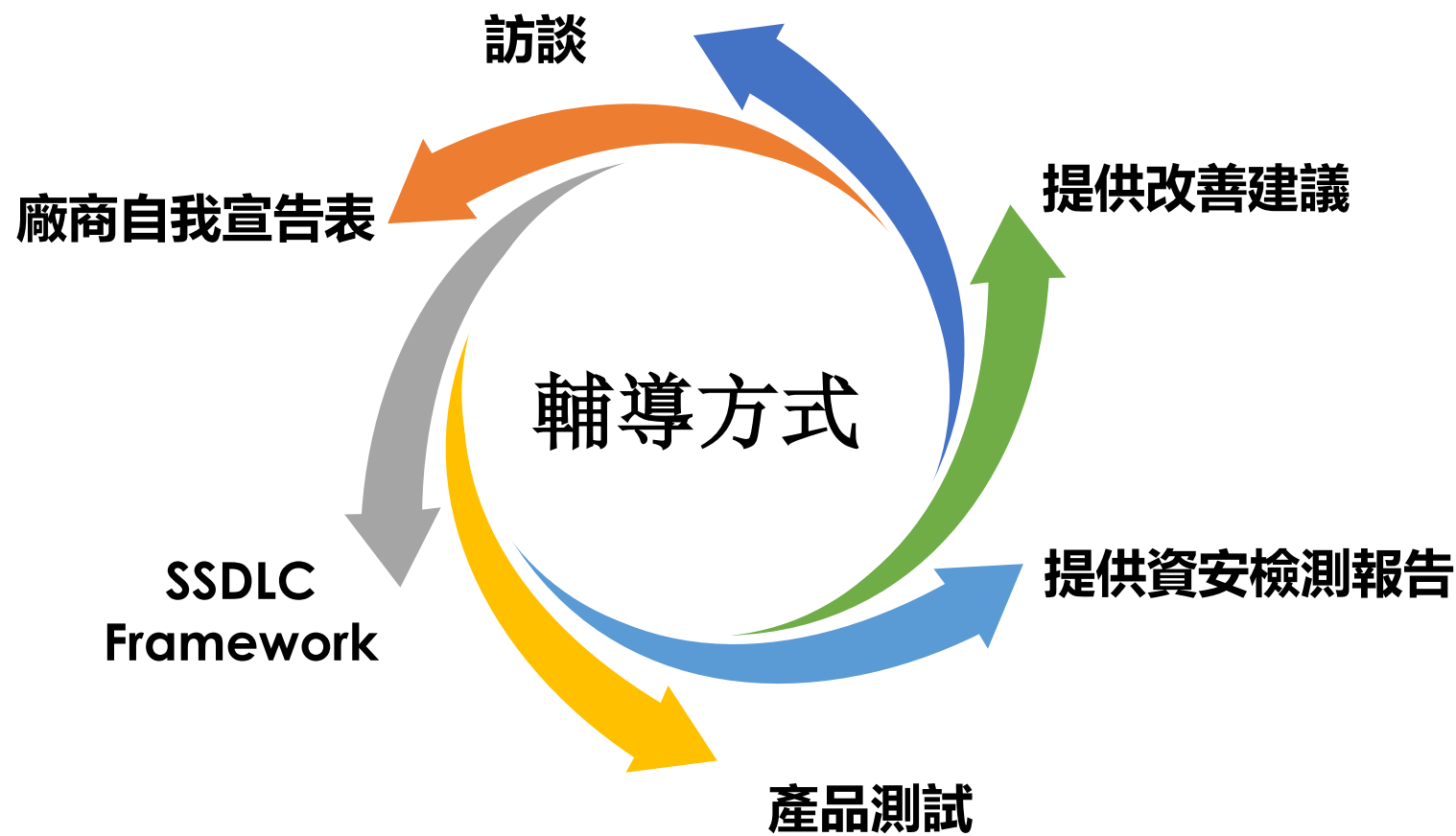
金融機構資訊安全評估辦法修正草案
- 資訊安全評估作業項目

So, IOT security is also important



影像監控系統資安標準之測試規範

- 由台灣資通產業標準協會(TAICS)公布之產業標準
 - 共通要求
 - IPCamera
 - NAS
 - NVR、DVR



訪談問題



物聯網產業標準（IP Camera）資安輔導

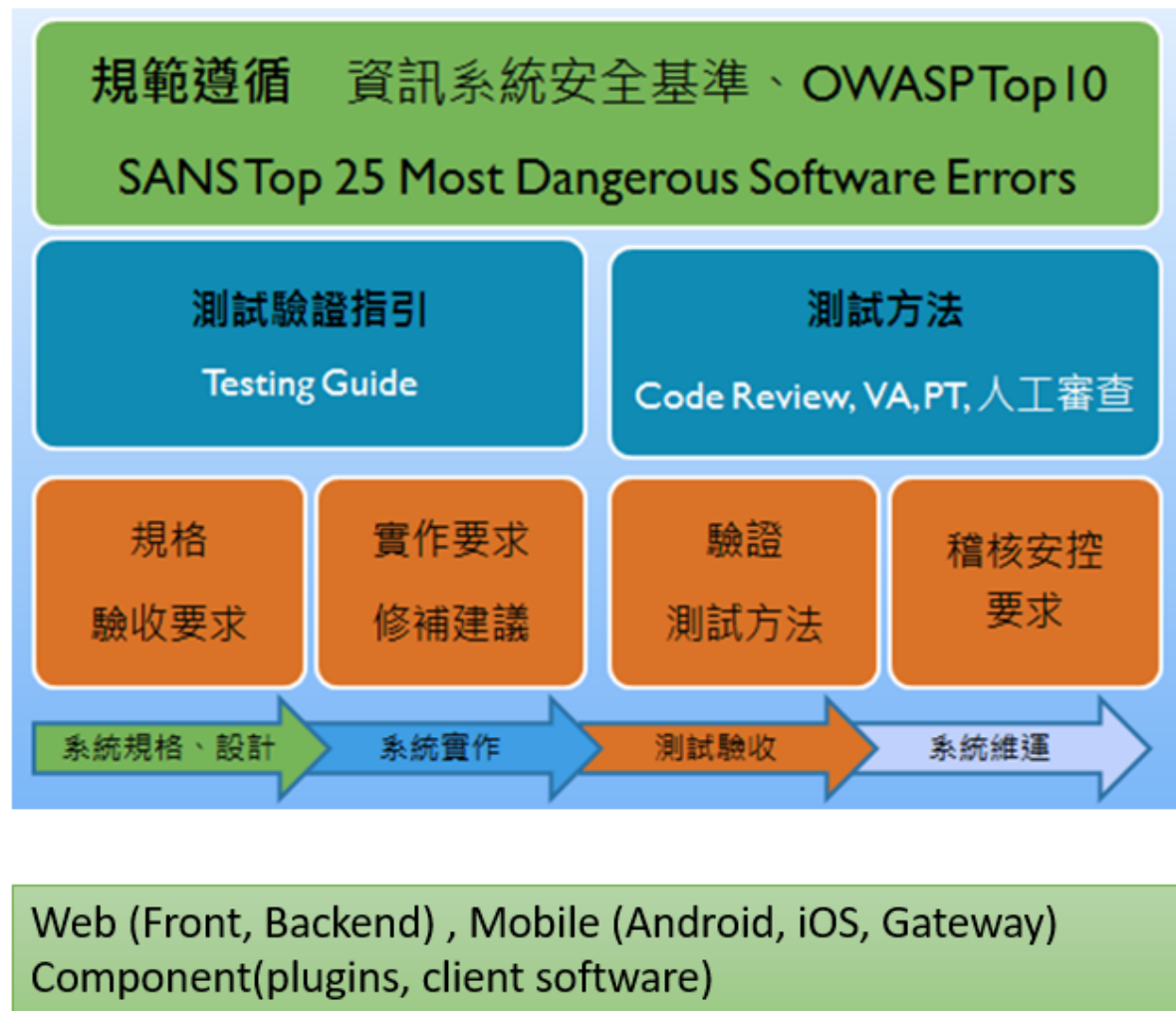


IP Camera 廠商自我宣告表

編號	項目	內容
1.	送測單位名稱	
2.	連絡資訊	
3.	物品及型號	
4.	製造廠商	
5.	作業系統版本	<input checked="" type="checkbox"/> Linux 版本 <input type="checkbox"/> 其他
6.	韌體版本	
7.	受測品 是否開啟網路埠	<input checked="" type="checkbox"/> 新申請案件 <input type="checkbox"/> 補申請案件 固定埠號(服務) : 動態埠號範圍(服務) :

8.	物 基 本 資 料	是否提供 API	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
9.		是否支援韌體更新	<input type="checkbox"/> 是，線上更新 <input checked="" type="checkbox"/> 是，手動更新 <input type="checkbox"/> 否	
10.		支援遠端管理介面	<input checked="" type="checkbox"/> 是 <input type="checkbox"/> 否	
11.		裝置 API 帳號權限說明		
12.		遠端管理介面帳號權限說明		
填表人 (簽名)			填表人 連絡資訊	電話 : 電子郵件 :

SSDLC Framework



Training: 規範；攻擊、防禦、測試手法；測試工具應用

Guideline: 因應規範之對策、系統規格(合約\SOW)、開發設計、安全測試案例abuse test case

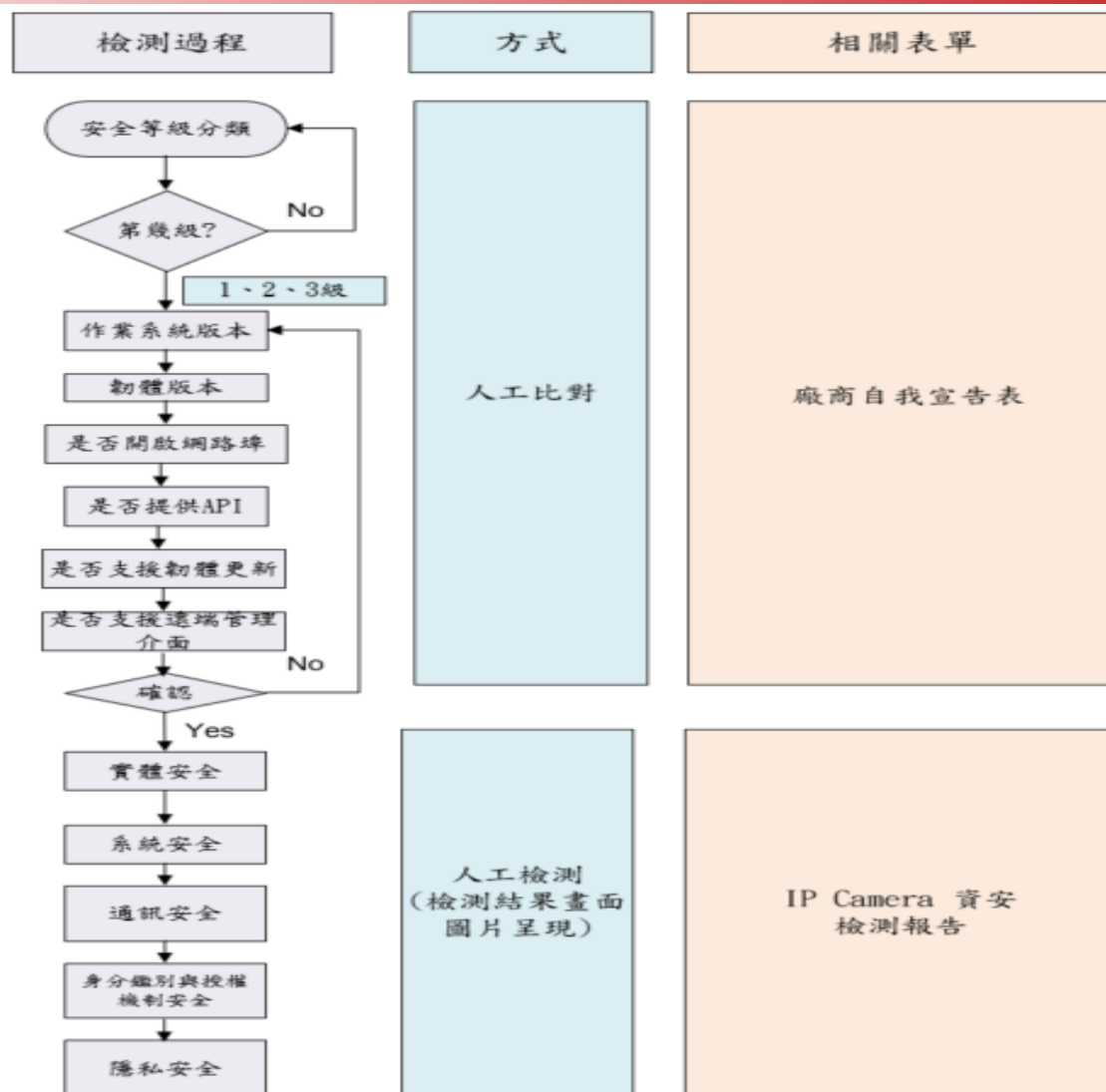
Checklist: 檢核表(需求分析、測試、驗收上架)

Security Library: 公用安全函式庫

Practice Pilot-run: 實際導入SSDLC並修正之

SSDLC 組織及維運
SSDLC 安控稽核

檢測步驟流程圖



檢測安全構面



檢測安全構面

實體

提供服務：**SD卡**

檢測方向：用這**SD卡**接到其他設備時，要經過驗證後才能進行讀寫的

系統

提供服務：**WebApp**網頁管理介面、行動**App**控制

檢測方向：網頁弱掃，韌體版本是否有**CVE**風險、系統**Debug Log**

通訊

提供服務：資料傳輸方式，採**Https**加密方式

檢測方向：建議採用**TLS 1.2**以上、是否採用安全通道建議使用之密碼套件
避免使用編碼進行混淆，**ex: Base64**

檢測安全構面

身分鑑別與授權機制

提供服務：身份認證

檢測方向：驗證方式、密碼強度、低權限帳號是否能切換成高權限、
Session / Token 是否有時效性，預設密碼更換

隱私保護

提供服務：個人資料使用

檢測方向：使用上是否有偵詢同意，若有需要儲存時有哪些保護措施

Privacy by Design

Privacy by Design的核心涵蓋：主動非被動、預防非防治；寓隱私保護於設計中；隱私保護作為預設模式；全部功能正和而非零和；尊重用戶隱私，確保以用戶為中心；自始至終的安全，遍及全程的保護；保持能見及透明度，做到保持開放。

按照GDPR第25條提到，有關資料控制者、資料處理者對於Privacy by Design落實情況，可考量採用第42條提到的認證機制證明以落實Privacy by Design。

而第42條所稱認證機制，指GDPR鼓勵歐盟各會員國的隱私保護監管機構，可實施GDPR落實情形的認證機制，作為企業或組織已符合GDPR要求之論證方法。

參考：GDPR十大重點

- ◆ 以資料為主體
- ◆ 企業必須設置資料保護長
- ◆ 個資的蒐集、處理和利用，必須先徵求當事人的同意
- ◆ 強化個人資料可攜權權利
- ◆ 新增被遺忘權
- ◆ 外洩個資，必須在72小時內通報資料保護主管機關
- ◆ 個資保護系統預設要納入隱私保護
- ◆ 賦予當事人有權反對被自動化剖析（ Profiling ）權利
- ◆ 要求企業必須落實資料保護影響評估
- ◆ 提高罰則金額，甚至以全球營業額計算罰金金額

個資定義、告知要求，歐盟比台灣嚴苛許多

——歐盟個資法與台灣比較

台灣個資法令		歐盟個資法 (GDPR)
最多新台幣 50 萬元	罰款	最高可達 2000 萬歐元或 4% 全球收入 罰金更高
19 項具體欄位，包含 • 姓名 • 出生 • 身分證 • 醫療 • 指紋 • 健檢 • 基因 • 病歷等	個資定義	• 姓名 • 身分證 • 醫療 • 健檢 • 基因 • 病歷 • 網路識別資料如 cookie 及 IP 位置等 • 敏感性個資項目 如種族、政治主張、宗教信仰及工會會員等 規範更多
• 適當位置 使當事人得以知悉其內容 • 若當事人未拒絕且已提供資料者， 即被視為同意	當事人告知及同意要求	• 須可理解及易接近 • 企業針對一般個資及敏感個資處理 當事人皆須明確同意 須經當事人明確同意
無此規範	當事人權利	新增資料可攜權和被遺忘權 當事人有更多主導權
除電信業等少數業者受規範外， 原則上無限制	國際傳輸	• 採原則禁止、例外開放方式， • 資料若欲跨歐盟境內外傳輸者， 皆須符合規定方可傳輸
無	資料保護長 (DPO)	企業若有大規模系統性監測個資時 須設立
只有主管機關或法規要求說明時， 才須向主管機關通報	個資違反通報	須於知悉後的 72 小時內通報主管機關， 不得有不當延遲，違者重罰
無	自動化處理 (剖析) 限制	• 須明確通知 • 當事人得行使拒絕權 • 須有人為干預機制 自動化技術處理從嚴規範



資料來源：KPMG 整理：黃煒軒

Thanks