Panasonic
Cyber Security Lab

產品安全的守護神 - PSIRT 的角色與培訓

松下網路安全實驗室 負責人 陳谷傑 (Kyo)

Agenda

01 產品安全漏洞給企業帶來的影響

02 產品資安事件應變小組 (PSIRT)

03 產品威脅分析

04 產品漏洞通報情境演練

講者簡介

陳谷傑 (Kyo)

松下網路安全實驗室 (Panasonic Cyber Security Lab) 負責人
chen.kyo@tw.panasonic.com

松下集團產品安全中心專案
中國地區產品資訊安全推進
松下網路安全實驗室管理

專長：資安事件應變 (IR)、安全系統設計、威脅情資研究

Panasonic
Cyber Security Lab

Panasonic

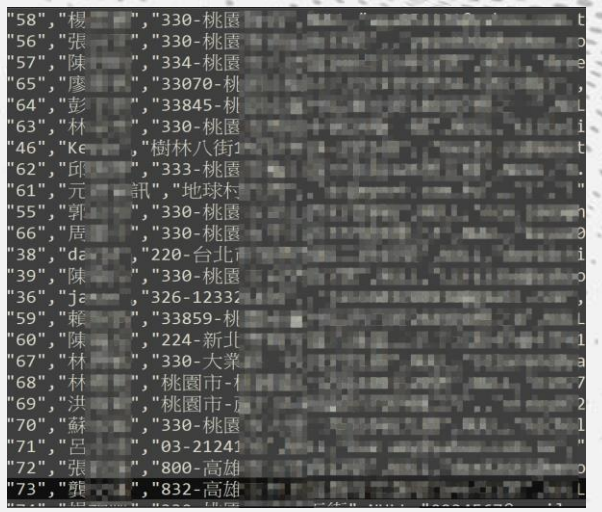
Product Security

Panasonic Cyber Security Lab

Panasonic PSIRT

1. 推動全球松下集團產品安全專案
2. 產品資安事件應變
3. 產品資訊安全測試
4. 產品安全人員培訓

產品安全漏洞給企業帶來的影響



1. 商業機密

- 產品遭逆向工程 => 透過漏洞獲得產品最高權限 => 產品設計資訊外洩
- 雲服務遭滲透入侵 => 透過漏洞取得雲服務管理權限 => 系統架構、客戶資料外洩

2. 品牌商譽

- 產品資安事件 => 客戶資料外洩 => 客戶失去信心 => 企業丟失訂單
- 企業機密外洩 => 投資人失去信心 => 股價下跌

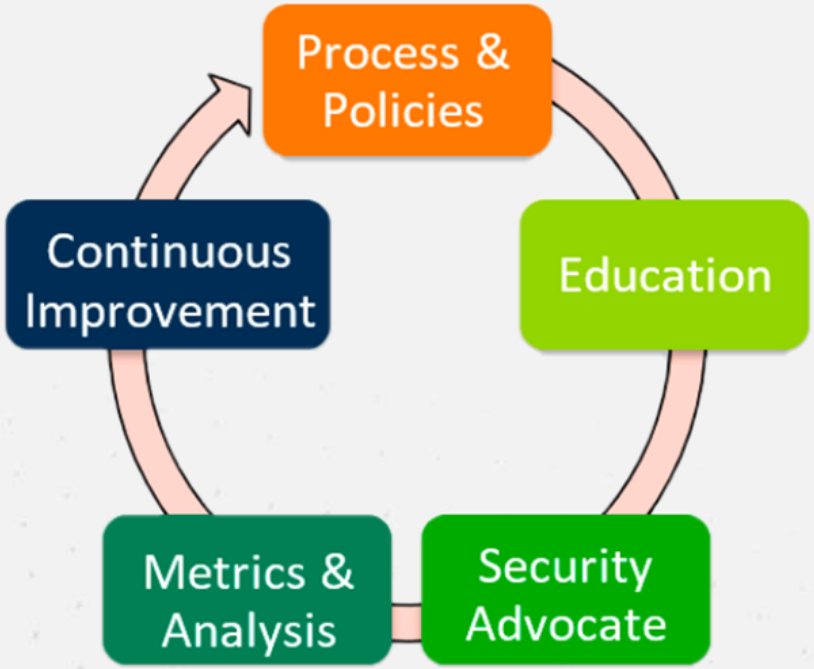
3. 罰則

- 產品資安事件 => 客戶資料外洩 => 觸犯個人資料保護法
  => 賠償 2,000 萬歐元或前一會計年度全球年營業額 4%
- 經抽查發現不符合安全規定 => 產品招回、停售

產品資安事件應變小組 (PSIRT)

職責與活動

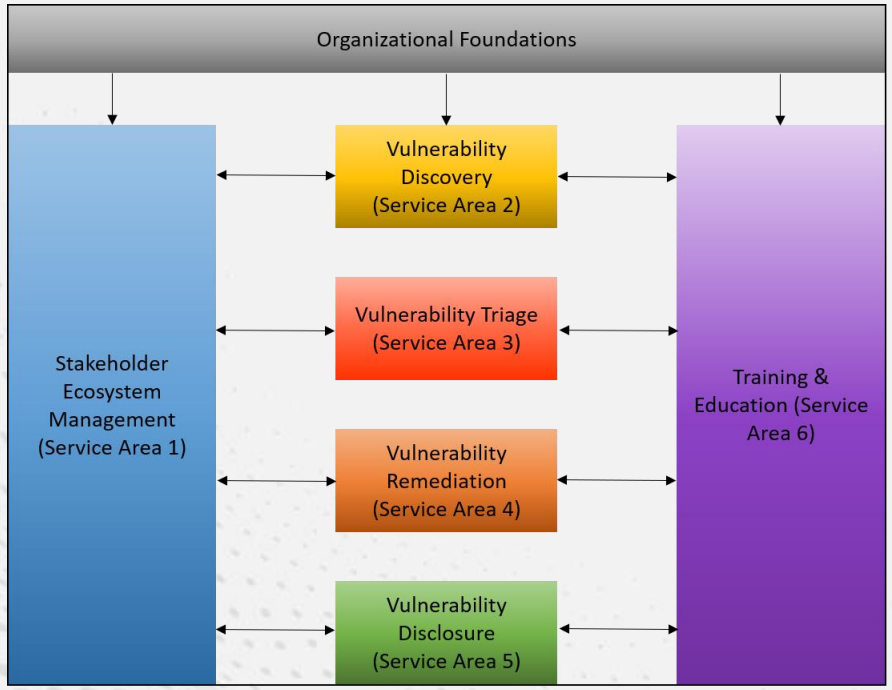
- 識別、評估和處理組織內與產品相關的**安全漏洞風險** (包括產品、解決方案、組件以及服務)。
- 非獨立運作的一群人，而是整個企業或組織中**產品安全工程**的一部分。
- 產品資安事件應變，通常會發生在安全開發生命週期的維護階段。但在產品需求收集、架構、設計、計畫和風險建模階段，仍需提供產品安全問題的指導和監督。



資料來源：https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

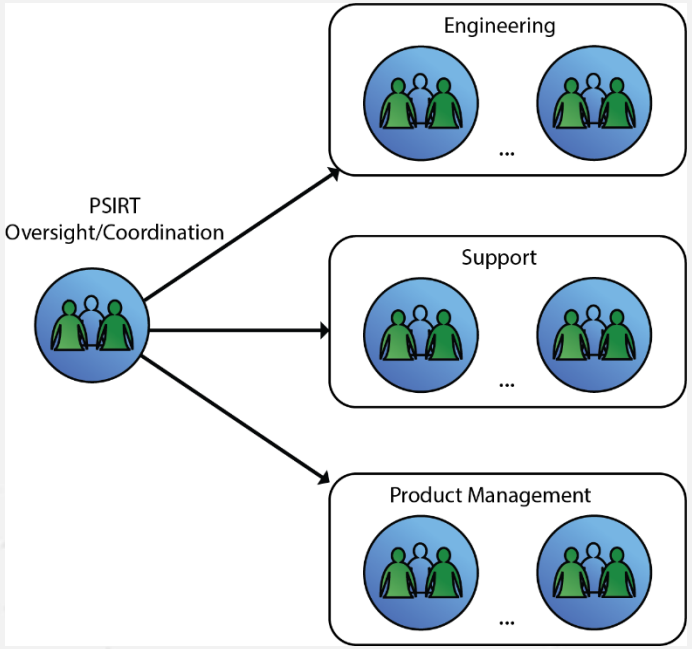
產品資安事件應變小組 (PSIRT)

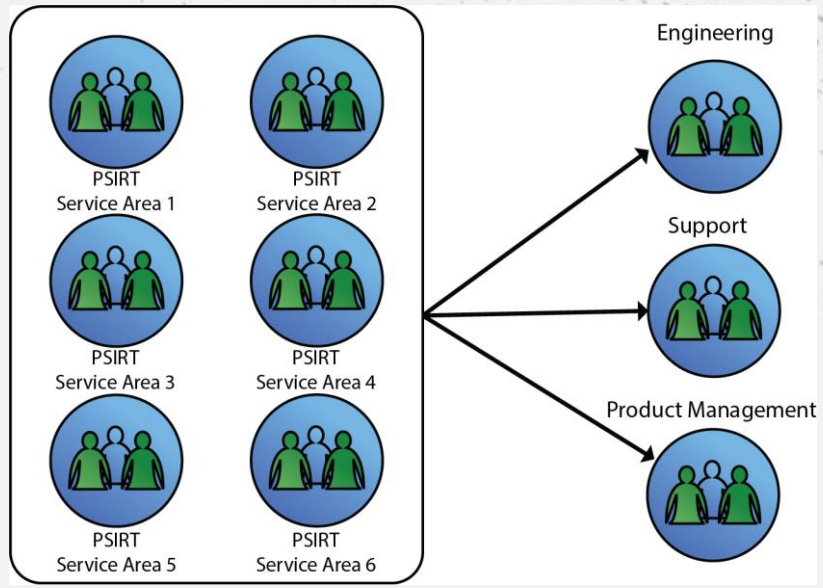
架構與模型



分散式模型

小型核心的 PSIRT，與產品團隊的代表合作解決產品中的安全漏洞。





集中式模型

擁有更多的 PSIRT 員工，他們來自多個部門，向負責組織產品安全的一名或多名高階主管報告。

資料來源：https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

產品資安事件應變小組 (PSIRT)

所需人才/技能

1. 安全漏洞通報應變管理人員

- 跨部門協調安全漏洞通報及應變流程 => 專案管理、政策及流程制定
- 上下游供應商產品及組件管理 => 專案管理

2. 資訊安全法律與政府事務合規人員

- 各國產品安全法律 => 產品安全法律、外語
- 各國政府產業規範 => 產業合規、外語

3. 產品軟韌體、硬體及通訊安全漏洞研究人員

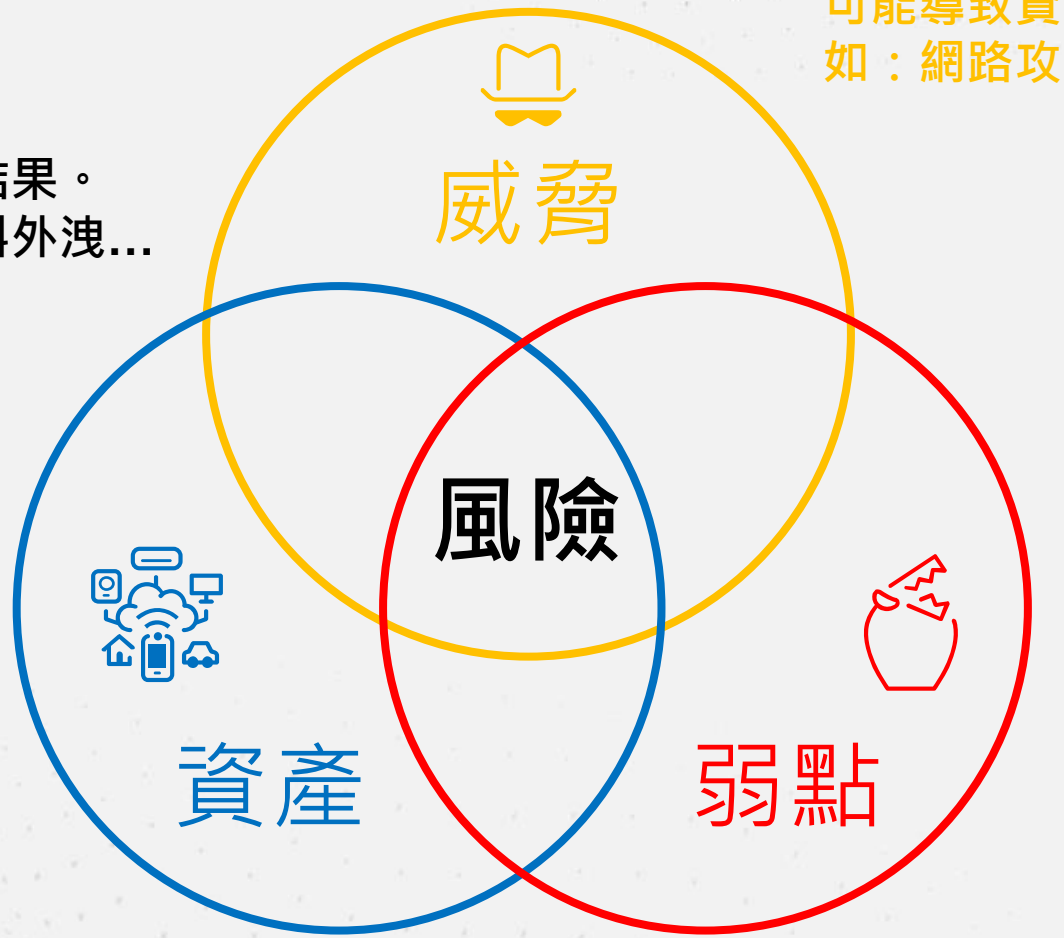
- 產品安全設計 => 軟韌體工程、硬體工程、通訊工程
- 產品漏洞利用及重現 => 軟韌體、硬體、通訊資訊安全
- 追蹤最新的產品安全威脅 => 威脅分析
- 產品安全培訓 => 教育

產品威脅分析

威脅、資產、弱點及風險

可能導致資產損壞/意外事件的潛在原因。
如：網路攻擊、實體攻擊、用戶不當的操作...

導致產品產生不確定事件的結果。
如：產品受到控制、用戶資料外洩...



應保護免受威脅的對象。
如：產品設計、用戶資料、運算資源...

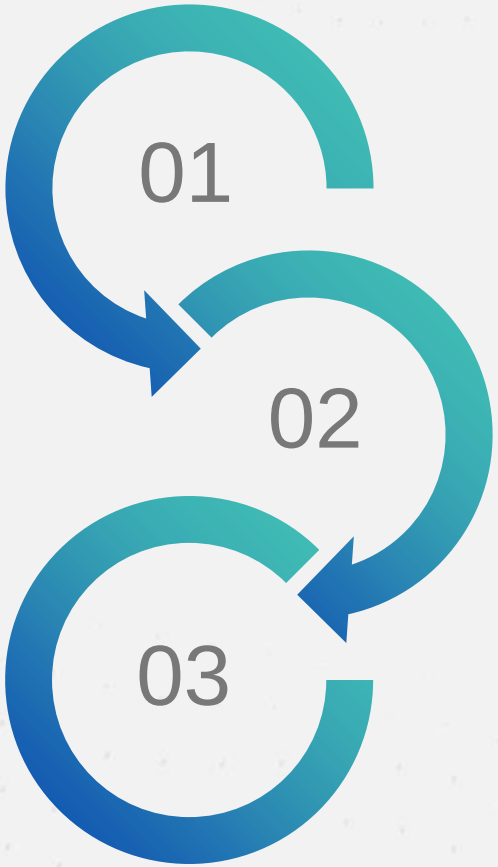
產品中可被利用的缺陷導致產品安全的負面影響。
如：緩存區溢出、登入驗證失效...

產品威脅分析

威脅分析過程

1. 資產識別

識別產品生態中，資產的範圍、種類及處理方式。



2. 威脅識別

識別產品生態中，可能導致設計缺陷的使用方式，並評估防範威脅的對策。

3. 威脅觸發

評估防範對策是否有效、威脅是否觸發，判斷威脅分級。

產品威脅分析

威脅分析情境演練

產品：

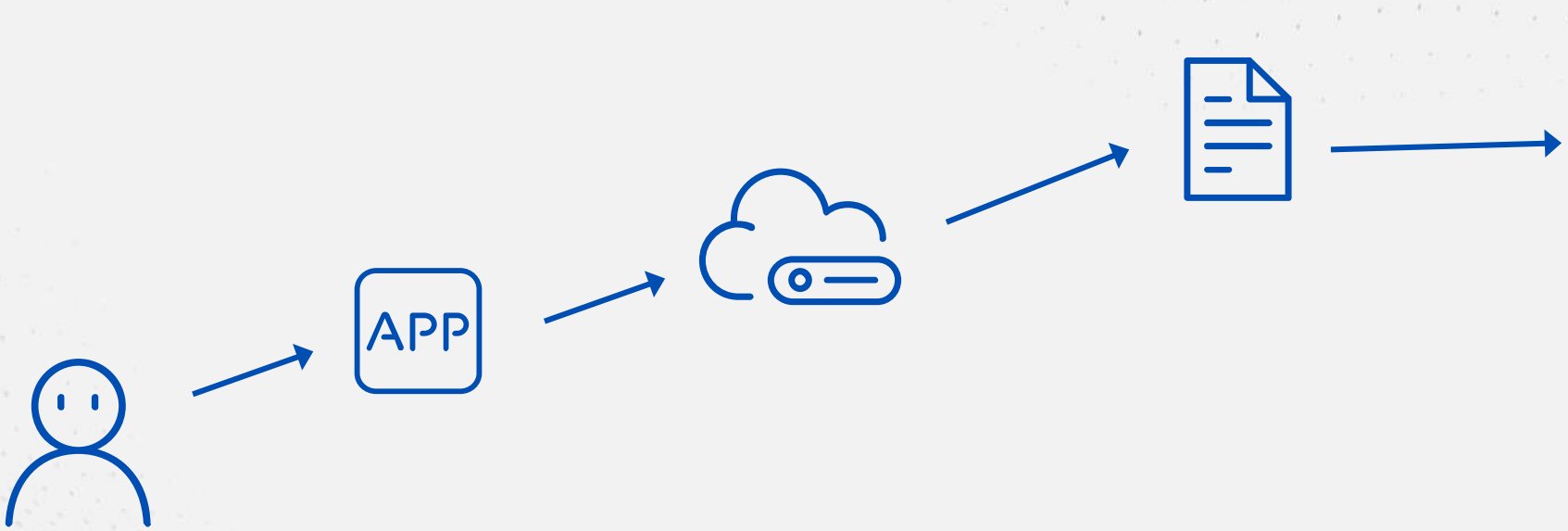
AI 機器手臂系統

功能：

1. 客戶用手機 APP登入雲端系統輸入文字，系統自動產生設計圖。
2. 雲端系統上傳設計圖至機器手臂，自動製造商品。
3. 客戶可遠端遙控調整商品參數。

產品威脅分析

威脅分析情境演練 - 資產識別



這樣的產品有哪些資產?

產品威脅分析

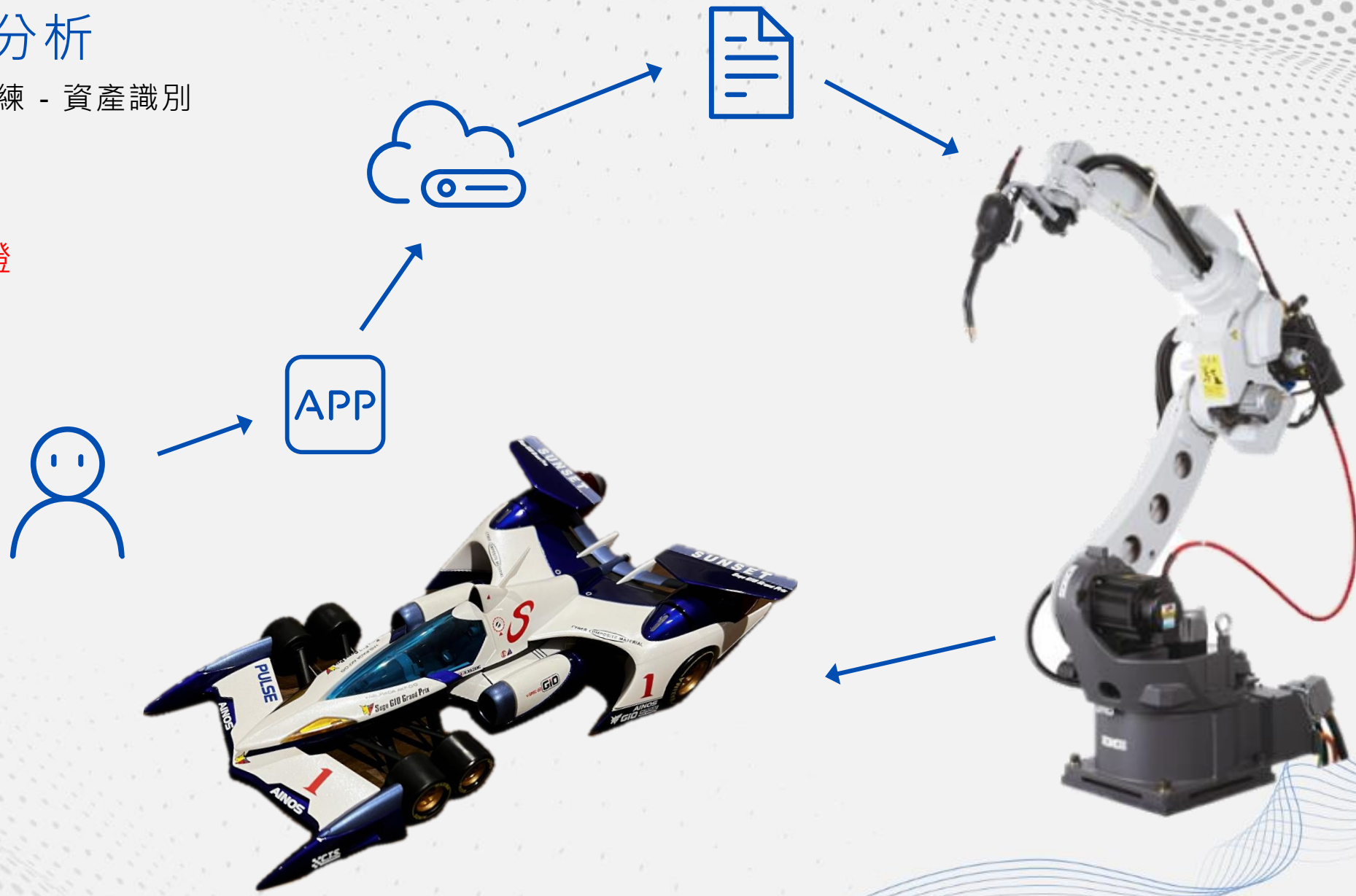
威脅分析情境演練 - 資產識別

資料類資產：

1. 客戶登入憑證
2. 設計圖
3. 商品參數

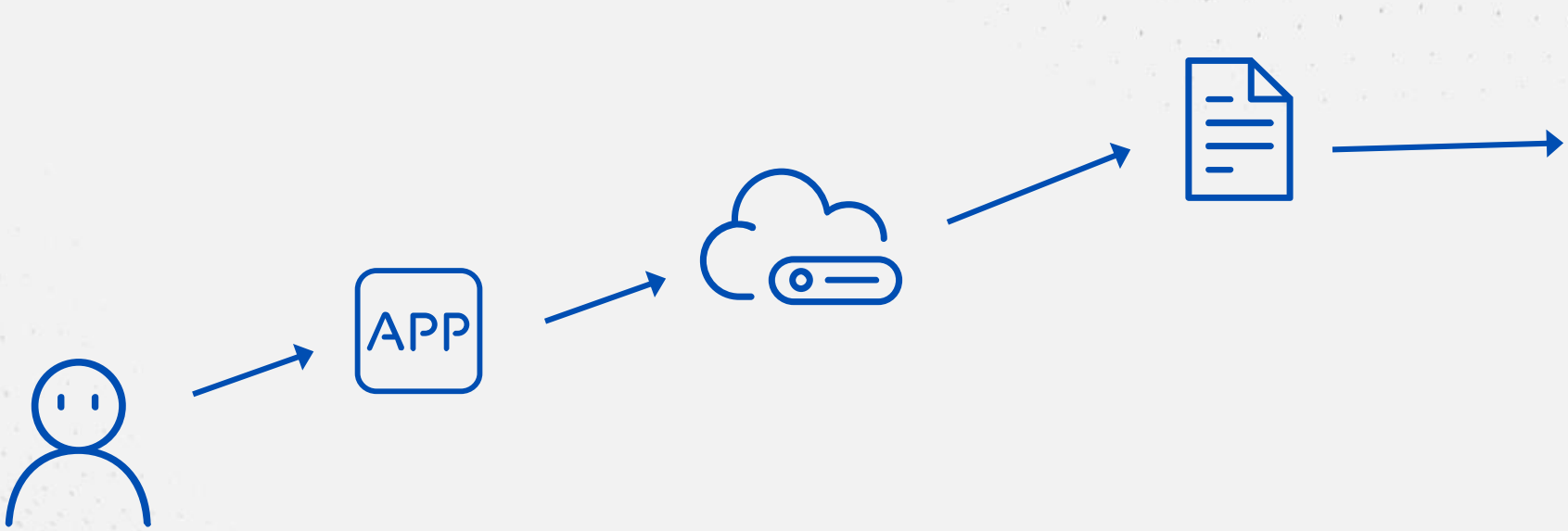
功能類資產：

1. 手機 App
2. 雲服務
3. 手臂硬體
4. 手臂韌體
5. 商品



產品威脅分析

威脅分析情境演練 - 威脅識別



這樣的產品有哪些威脅?

產品威脅分析

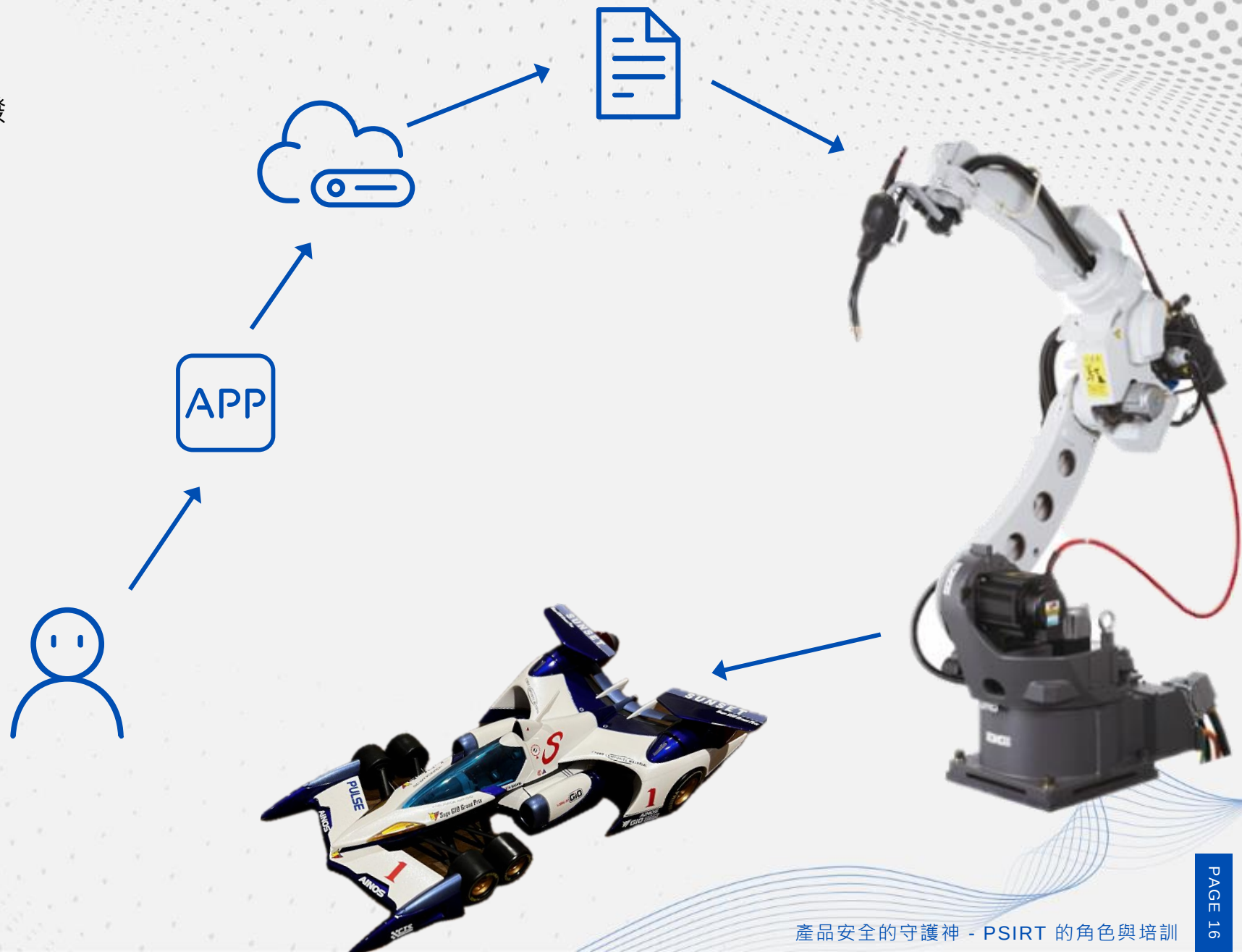
威脅分析情境演練 - 威脅識別

- 偽造客戶登入資訊
- 竄改商品製造參數
- 設計圖外洩
- 客戶權限控管不當
- 雲服務系統登入憑證外洩
- 手機 APP 停止服務

產品威脅分析

威脅分析情境演練 - 威脅觸發

- 偽造客戶登入資訊
  => 入侵雲服務系統
- 竄改商品製造參數
  => 商品製造異常
- 設計圖外洩
  => 商業機密外洩
- 客戶權限控管不當
  => 客戶資料外洩
- 雲服務系統登入憑證外洩
  => 雲服務遭到入侵
- 手機 APP 停止服務
  => 機器手臂失去控制



產品漏洞通報情境演練

模擬產品安全漏洞通報過程

模擬 PSIRT 的成員收到一則來自駭客十分有份量的通報信及檔案.....

01

漏洞通報

收到通知信了!
傳球?

02

漏洞分析

這個洞怎麼用?
有什麼影響?
威脅等級?

03

漏洞修補

把洞擦掉不留痕跡

04

漏洞揭露

適當的通知用戶威脅
不透漏敏感資訊

產品漏洞通報情境演練

漏洞通報

收件者: psirt@tw.top1manufactory.com

poc.docx
287 個位元組

Hello PSIRT，
我有發現一款智慧電視有 pre-auth RCE漏洞。

==========
Sincerely,
Kyo

Mail: chen.kyo@tw.panasonic.com
Tel: +886-2-6666-6666
==========

收到漏洞通報的第一步?

產品漏洞通報情境演練

漏洞通報

1. 確認信件來源以及檔案安全

2. 檢查漏洞資訊是否提供完整 (使用表格)

- 目標產品型號
- Serial Number
- 韌體/作業系統版本
- 漏洞利用流程
- Proof of concept
- ….

收件者: psirt@tw.top1manufactory.com

poc.docx
287 個位元組

Hello PSIRT，
我有發現一款智慧電視有 pre-auth RCE漏洞。

==========
Sincerely,
Kyo

Mail: chen.kyo@tw.panasonic.com
Tel: +886-2-6666-6666
==========

產品漏洞通報情境演練

漏洞分析

1. **漏洞目標**
   - 硬體元件、軟體元件、作業系統...?
2. **漏洞種類**
   - 服務阻斷 (DoS)、提升權限、資料外洩...?
3. **漏洞影響程度(評級)**
   - CVSS 分數、嚴重或者輕微...?
4. **漏洞影響範圍**
   - 特定型號產品、系列產品、跨產品線...?

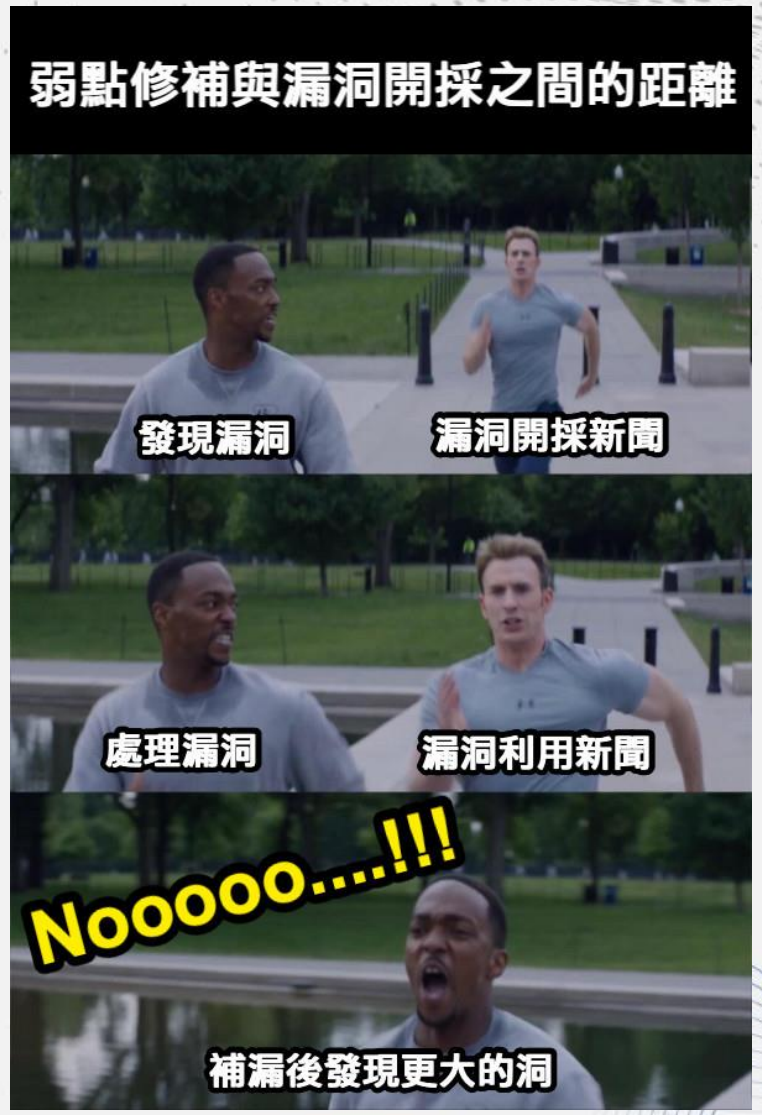
確認完成才能傳給產品負責單位

產品漏洞通報情境演練

漏洞修補

1. **漏洞修補方式**
   - 添加安全機制、更新元件...?
2. **漏洞更新方法**
   - OTA、網頁下載、App store更新...?
3. **漏洞修補日期**
   - 預計修補時間、時程...?

規劃完成傳給通報人員確認



產品漏洞通報情境演練

漏洞揭露

1. **漏洞揭露方式**
   - 官方網站、CVE...
2. **通知通報者**
   - 驗證漏洞是否仍存在、發送漏洞發現證明...
3. **漏洞獎勵**
   - 賞金、紀念品、獎品...

Takeaways

1. 產品安全漏洞，能對高科技製造業造成很大的危害。
2. PSIRT 並非僅是一個資安應變團隊，而是產品安全工程的一部分。
3. PSIRT 角色技能有三大方向，各方面人才都非常缺乏。
4. 企業可透過各式各樣的模擬與情境演練，培養 PSIRT 人才。

THANK YOU

chen.kyo@tw.panasonic.com

Product Security

Panasonic PSIRT

Panasonic Cyber Security Lab