CYBERSEC 2024 臺灣資安大會 | 5/14 Tue – 5/16 Thu 臺北南港展覽二館

Generative Future

Supply Chain Cybersecurity Forum

供應商安全管理

產品導入前的安全性測試

PD Lee

Freelancer

Pedro[ㄟ特]pdcyber.com

Agenda

- 前言
- 產品導入
  - 為消化預算而導入
  - 為時尚潮流而導入
  - 因需求而導入
- 供應商評比
  - 功能評比
  - 技術評比
  - 安全性評比
    - 產品安全性測試
    - 供應商弱點修復能力
- 結語

為消化預算而導入

- ~~錢太多~~預算充裕
- 該買的都買了
- 但...不該買的是不是也買了?

為時尚潮流而導入

- 非迫切性需求
- 因業務推廣而導入
- 因為是市場主流產品

因需求而導入

- 法規面(最優先)
  - 法遵需求
  - 產業標準需求
- 業務面
  - 配合企業發展藍圖
  - 新業務&市場的拓展

上市上櫃公司資通安全管控指引

第一章 總則

第一條、 為協助上市、上櫃公司(以下簡稱公司)強化資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業，特擬定本資通安全管控指引。

第二條、 名詞定義

一、 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、 核心業務：公司維持營運與發展必要之業務。

四、 核心資通系統：支持核心業務持續運作必要之資通系統。

五、 機敏性資料：依公司業務考量，評估需保密或具敏感性之重要資料，如涉及營業秘密資料或個人資料等。

第二章 資通安全政策及推動組織

第三條、 成立資通安全推動組織，組織配置適當之人力、物力與財力資源，並指派適當人員擔任資安專責主管及資安專責人員，以負責推動、協調監督及審查資通安全管理事項。

因需求而導入

- 資安面
  - 解決現有資安威脅
  - 整體資安環境評估後的規劃

Agenda

- 前言
- 產品導入
  - 為消化預算而導入
  - 為時尚潮流而導入
  - 因需求而導入
- 供應商評比
  - 功能評比
  - 技術評比
  - 安全性評比
    - 產品安全性測試
    - 供應商弱點修復能力
- 結語

功能評比

- Root Cause(莫忘初衷)
- 導入設備的最主要原因？
- 哪些是必須滿足的功能面？

技術評比

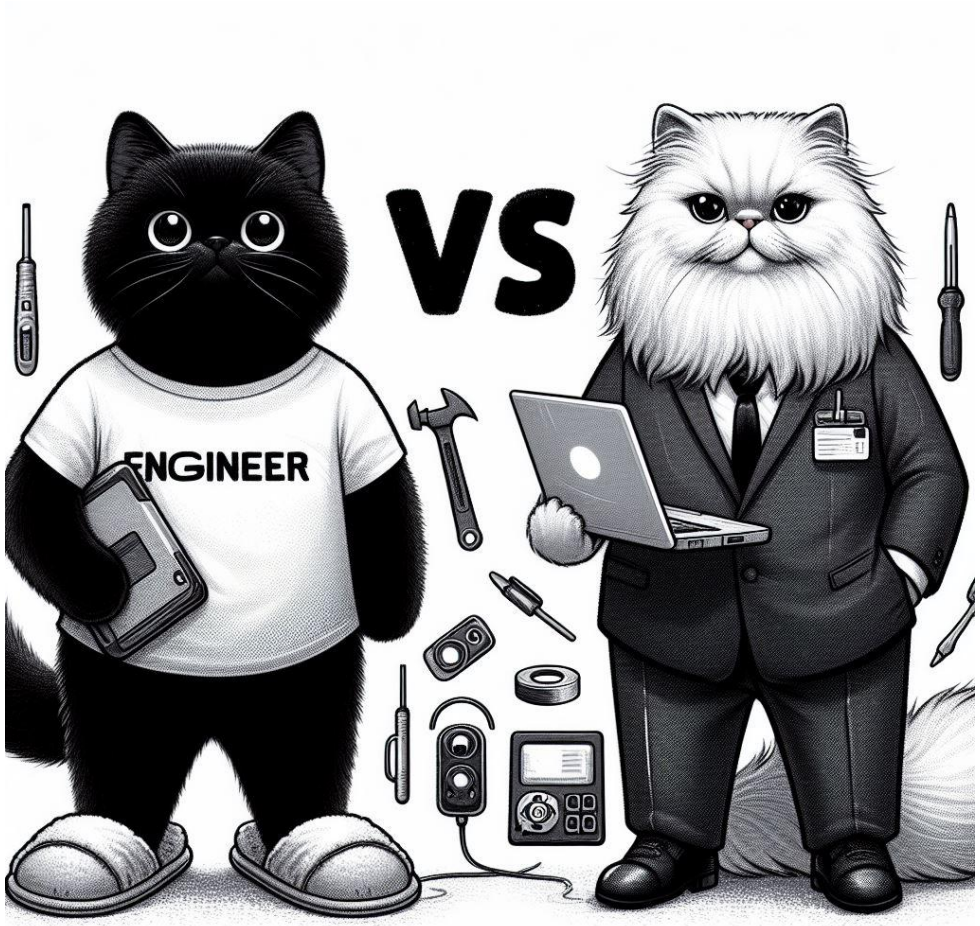
- 產品本身的技術評比
  - 國際大廠或本土廠商?
  - 產品導向或服務導向
  - 產品版本差異
- 環境相容性評比
- 供應商技術評比

供應商技術評比

- 服務品質
- 技術能力
- 調校/除錯能力
- 客製化能力

盲點

- 資訊不透明
  - 資安專案多有簽署NDA
  - 少有公開資訊可查詢
- 採購的壓力



Agenda

- 前言
- 產品導入
  - 為消化預算而導入
  - 為時尚潮流而導入
  - 因需求而導入
- 供應商評比
  - 功能評比
  - 技術評比
  - 安全性評比
    - 產品安全性測試
    - 供應商弱點修復能力
- 結語

安全性評比

- 產品安全性測試
  - 一般安全性檢測
  - 漏洞挖掘

一般安全性檢測

- 自動化工具檢測
  - 透過單位採購的自動化資安檢測工具
  - 自行架設開源弱點檢測工具
- 配合廠商檢測
  - 重要系統上線前可評估委託資安服務廠商進行檢測
- 弱點情資蒐集
  - CVE
  - Exploit-db
  - Hitcon zeroday
  - TVN (Taiwan Vulnerability Note)
  - ...etc

黑箱檢測

- 優勢
  - 誤判率低
  - 不受程式語言限制
  - 可檢測網頁伺服器弱點
  - 不需提供原始碼
- 劣勢
  - 中繼處理的弱點
  - 管理層面的弱點
  - 無法檢測商業邏輯漏洞
  - 難以檢測權限提升漏洞
  - 檢測路徑不夠完整
  - 檢測速度較慢

白箱檢測

- 優勢
  - 檢測速度相對較快
  - 與開發流程整合容易
  - 程式覆蓋率完整
  - 明確指出程式問題點
- 劣勢
  - 中繼處理的弱點
  - 管理層面的弱點
  - 無法檢測商業邏輯漏洞
  - 難以檢測權限提升漏洞
  - 必須取得原始碼
  - 受程式語言限制
  - 難以判斷自訂的過濾函式

自動化檢測工具盲點

- 中繼處理的弱點
- 管理層面的弱點
- 無法檢測商業邏輯漏洞
- 難以檢測權限提升漏洞

滲透攻擊與漏洞挖掘的差異

- 滲透攻擊
  - 配合既有環境進行滲透攻擊
  - 受限於測試範圍與限制，無法含括所有情境

- 漏洞挖掘
  - 盡可能模擬各種情境
  - 不受測試範圍限制，可以自由模擬各種情境

案例分享

- 某開源Log收集與分析工具

informationsecurity.com.tw/article/article_detail.aspx?aid=7236

資安人 INFO SECURITY

圖6、嘗試撈取/etc/passwd檔案失敗。

看起來似乎有進行簡單過濾，改變一下作法繞過去好了。（圖7）。

圖7、動了一下手腳來繞過限制。

果然順利撈出系統檔案，而且反覆測試過後，發現多個頁面皆存在SQL Injection問題，甚至還有部分頁面不需要管理者權限即可逕行注入。上述流程只是一個簡易的檢測流程，目的是要提醒企業必須做好資安檢測，以PhpLogCon例，企業在導入前若能發現其存在的安全性問題（表1），就可以針對此部份做修正或規劃其他補強機制，如此才能確保IT環境不會因為Opensource工具導入而帶來更多的安全風險。

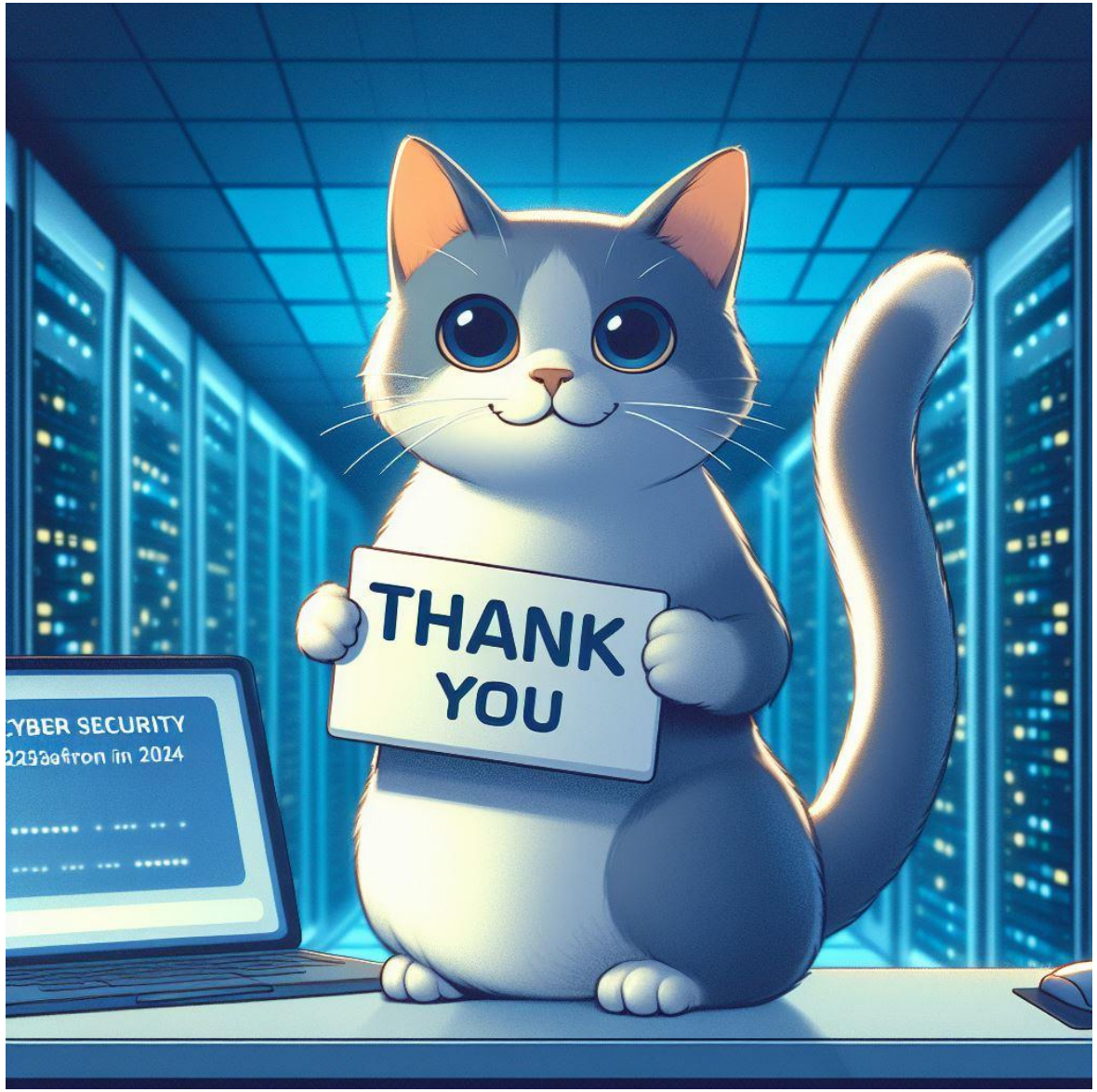
Ref:https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7236

案例分享

- 安裝模式
  - 不安裝SQL，Log檔案存放在個別file
    - 有XSS漏洞
  - 安裝SQL，Log檔案存放在SQL，無須登入可操作
    - 有SQL Injection和XSS漏洞
  - 安裝SQL，Log檔案存放在SQL，有帳號權限管控
    - 有SQL Injection和XSS漏洞，而且可提權

供應商漏洞修補能力

- 人非聖賢，孰能無過
- 有漏洞無可厚非，後續的處置能力才是關鍵


THANK
YOU