



FreeTalk:

# 企業資安下之工程師成長歷程

LOYO@NISRA



## 問題釐清

企業資安問題層出不窮，  
為何相同的弱點卻一再被利用？

不同地方重覆被利用

不同時間重覆被利用



工程師如何面對與成長？

# 駭客張啟元買「1元車票」 遭統聯以侵占備案

TVBS-2015年11月13日 下午14:41

讚 0 G+ 0

字級： 小 中 大 特

駭客張啟元，又再度成功買到1元票券，他駭進統聯網頁，買到車票，只花1元，還搭車北上，過去都沒事，這次卻踢到大鐵方備案，雖然張啟元說只是善意提醒系統漏洞，不過統聯認為是惡意，已報警備案，決定保留法律追訴權。

駭客張啟元(2015.09.15)：「這是很嚴重的漏洞。」

他是張啟元，之前才成功駭入超商機台，上個月再度故技重施，他就是透過統聯客運的網頁購票，10月28日買台中到台北的車票，把車票改成1元，立刻搭車北上，被統聯發現。

駭客張啟元：「這封報備信好像他們沒收到，就變成說我是惡意，錯是錯在沒有確認說他們有沒有收到信，我就做這個動作。」

統聯表示，10月28日張啟元駭進系統，買到1元車票，45分鐘後，台北就連發3封EMAIL向客服反應，但是卻沒人回應，隔天他就被控侵占。

統聯台北轉運站站長甘杰：「只在28日有發個EMAIL，跟我們說，可是他並沒有得到，還沒等到我們的回覆，隔天又做這種比較誇張的動作，請警方做備案的動作。」

統聯表示，當天整理系統就發現有異狀，澄清沒漏洞，是信用卡系統問題。

駭客張啟元(2013.09.10)：「在這邊，我必須跟創辦人馬克祖克伯說聲抱歉，因為這是惡意的。」

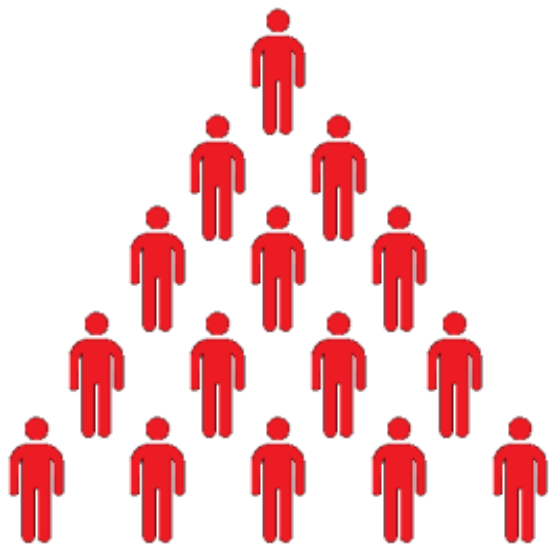
駭客張啟元曾經入侵臉書刪掉創辦人貼文，也曾破解已故藝人楊又穎的手機密碼，先前



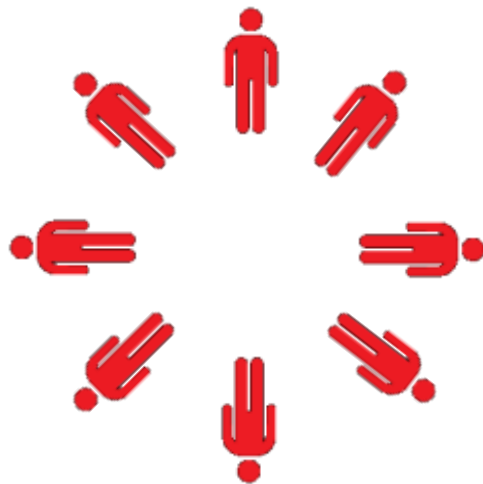
# 企業文化



# 規模分析



大型企業



中小型企业

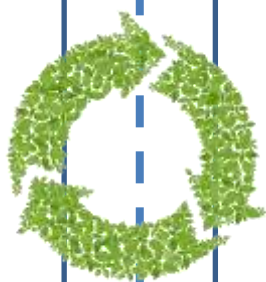
# 企業規模分析

## 大型企業

- 可用資源較多
- 階層分工較為明顯
- 各司所職
- 專案導向
- 人力組成較為複雜

## 中小型企業

- 組織較有彈性
- 服務導向
- 第三方服務整合較容易
- 敏捷



- 人力、程式碼等外包
- 共用外部整合服務 或 系統

共同性質

工程師會在這裡面輪迴LOOP...

流程

制度

溝通

人

唯一例外: 老闆!!!!



A cluster of various blue and grey icons in the top-left corner, including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a lightbulb, a gear, and a document.

# 成因

常常發生在這些地方...

A cluster of various blue and grey icons in the bottom-right corner, including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a lightbulb, a gear, and a document.





## 問題常常發生在這些地方...

- 新的流程(概念)難以導入
  - 版本管控
    - 不同專案或是不同的管控系統
  - 專案管理
    - 人比專案難管
  - 開發/設計模式
    - 需取得共識





## 問題常常發生在這些地方...

- 制度上的差異
  - 水平/垂直分工 差異性
  - 複合式的分工



## 問題常常發生在這些地方...

- 思維差異性
  - 程式撰寫習慣
  - 一分鐘十行code & 十分鐘一行code



會跑就好



會錯和我沒關係



## 問題常常發生在這些地方...

- 程式移植/重構/轉換
  - 邏輯上的修改
  - 功能上的改寫
  - 語言上的轉換





## 問題常常發生在這些地方...

- 文件
  - 彙整於不同地方(例如: 一張充滿故事的A4)
  - 格式風格的不一致
  - 沒有彙整的習慣





## 問題常常發生在這些地方...

- 資安認知不同
  - Code能跑就好
  - 我們有資安TEAM! (弱點掃描)
  - 字串我都有處理





## 問題常常發生在這些地方...

- 測試流程
  - 我們有測試TEAM!
  - 測試含蓋率
  - 對於測試的認知



誰汙染、誰治理。誰開發、誰保護。

## 自己的資安自己救...



專案性的開發，系統性的思考



認清目前的環境



正確的資安認知




重寫/重構/轉換程式時，了解特性




協同開發的共識




A cluster of small, light-blue icons in the top-left corner, including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a lightbulb, and a document.

**這是一個奇幻的過程！  
甚麼都有可能發生！！**

A cluster of small, light-blue icons in the bottom-right corner, including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a lightbulb, and a document.




## 自我能力提升

- 了解工程師思維
  - 建立自己做事情的方法
  - 對於即戰力的認知
  - 了解身邊的人
  - 沒有完美的結局
  - It is all about Making Friend!!
- 


A cluster of various blue and grey icons including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a lightbulb, and a gear, arranged in a circular pattern in the top-left corner.

## 自我能力提升

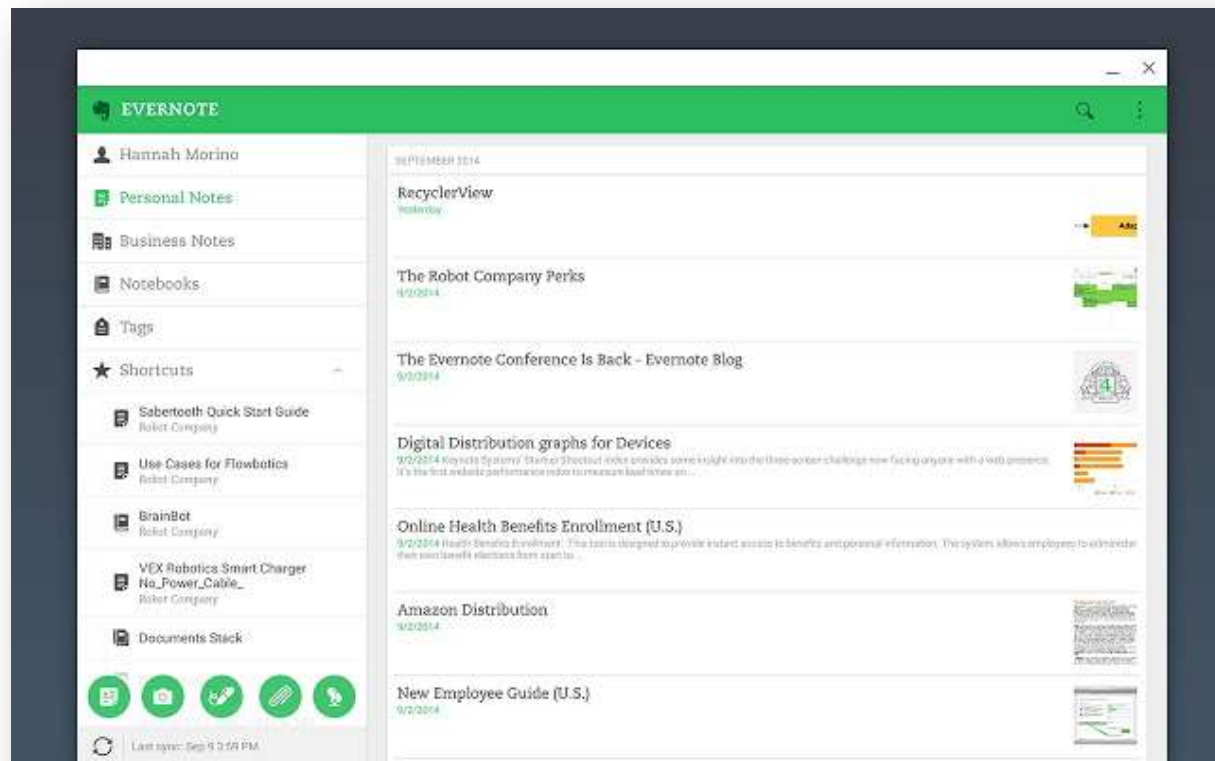
- 必然的茫然
  - 事實 = 訊息 - 立場 - 主觀
  - 善用工具來管理自己
  - 來NISRA吧!
- 
- A cluster of various blue and grey icons including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a lightbulb, and a gear, arranged in a circular pattern in the bottom-right corner.

A cluster of various blue and grey icons including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a document, and a network diagram, arranged in a circular pattern in the top-left corner.


## 工具分享



- Evernote
  - Trello
  - Redmine
  - Domain name
- 
- A cluster of various blue and grey icons including a smartphone, a laptop, a globe, a camera, a pie chart, a bar chart, a document, and a network diagram, arranged in a circular pattern in the bottom-right corner.

# Evernote





Boards 

Python   Public

### Memo

- python-packet-sniffer-code-linux
- Google Python Style Guide
- Command-line Applications
- decorator
- Add a card...

### Tool

- SSH Lib (paramiko) - for SSH2
- html2text
- SSH1 by python
- ConfigParser
- Python treelib
- System's Administration
- Console Menu(cint)
- Console Menu(Urwid)
- Add a card...

### Interesting

- Python Packet Capture and Injection Library
- Python Menu System
- 20 Python libraries you can't live without
- 30 Python Language Features and Tricks You May Not Know About
- High-performance container datatype
- KNN
- Line bot
- Add a card...

### DNS

- dnslib
- Dnssnarf
- dnsSquirrel.py
- read dns zone by python
- Unbound + Python
- dns\_attack\_mitigation.sh
- named.state parser
- Add a card...

# REDMINE



網站首頁 帳戶首頁 專案清單 問題管理 說明

日新登入 koyo 我的帳戶 登出

## 碼機咕咕 » Python玩具

搜尋:

概覽 活動 問題清單 建立新問題 封鎖欄 任務 文件 Wiki 設定

### 問題清單

➤ 篩選條件

📌 狀態  加入新篩選條件

➤ 篩選清單

✔ 關閉 ✖ 清除 📄 儲存

✔ #	問題標題	狀態	優先權	主旨	分類	更新日期
73	功能	已回應	正常	無法正常登入主權		2014-10-06 07:11
68	支援	已解決	正常	make_query() 無法設定 CD flags		2014-04-18 03:39
67	支援	新建	正常	使用treelib中node的data attribute		2014-04-07 03:18
66	功能	已解決	正常	建立 On tree 功能		2014-04-07 03:25
64	支援	已解決	正常	安裝 treelib		2014-04-07 03:23
63	異議	新建	正常	twisted 會卡住		2014-04-07 01:54
62	異議	新建	正常	decode['hex'] 有問題		2014-04-07 01:52
61	支援	新建	正常	安裝 twisted		2014-04-02 08:55
60	功能	已解決	正常	轉寫 wrapper		2014-04-18 03:32
53	異議	已解決	正常	task 在 host list 過多會報錯		2014-01-02 06:35
45	支援	已解決	正常	輸出沒有換行		2013-10-29 11:50
44	異議	已解決	正常	fabric 執行 shell 問題(會出現Unmatch ",訊息		2013-10-29 11:47
43	功能	已解決	正常	登入能關閉帳號功能		2013-10-17 07:31
37	異議	新建	正常	顏色無法顯示		2013-05-30 12:12
36	異議	已解決	正常	fespect 使用 str.format()		2013-05-30 11:08
35	異議	已解決	正常	無法import blessings		2013-05-30 12:11
34	支援	已解決	正常	安裝fespect		2013-05-30 06:26
33	支援	新建	正常	測試自動式fabric task		2013-05-30 12:03
28	支援	已解決	正常	了解fabric錯誤處理機制		2013-05-22 09:15
27	異議	已解決	正常	os.environ 無法用		2013-05-16 10:44

### 問題清單

檢視所有問題

摘要

日曆

封鎖欄



企業資安

成因

應對方法


自我修煉

骨氣



A cluster of various blue and grey icons including a smartphone, a laptop, a globe, a camera, a bar chart, a pie chart, a lightbulb, and a gear, arranged in a circular pattern in the top-left corner.

## 未來的問題

- 對 Open Source 的依賴性/安全性
  - 平台的安全性(例如: OS)
  - 自動化的取代問題(把自己取代掉)
  - 分久必合、合久必分的藝術
  - AXBXC
- 
- A cluster of various blue and grey icons including a smartphone, a laptop, a globe, a camera, a bar chart, a pie chart, a lightbulb, and a gear, arranged in a circular pattern in the bottom-right corner.

# Q&A