

AI應用在資安研發： 趨勢科技 經驗分享

趨勢科技 全球研發副總：
周存賡

趨勢科技的 AI 經驗

- 變臉詐騙阻擋
- 垃圾郵件阻擋
- 惡意巨集偵測
- 客戶續約可能性預測
- 跨世代的威脅防護 X-Gen



趨勢科技是一個 AI 公司

資安相關



影像辨識



惡意網站



垃圾/詐騙郵件



物聯網



惡意程式



事件調查

40+

營運相關



自動客戶服務



社群評論品牌形象



客戶忠誠度預測



行銷業務提升



變臉詐騙阻擋

財務長收到 CEO 寄的email 要求電匯25萬美元
給供應商, 怎麼判斷是不是變臉詐騙 (BEC) 呢?

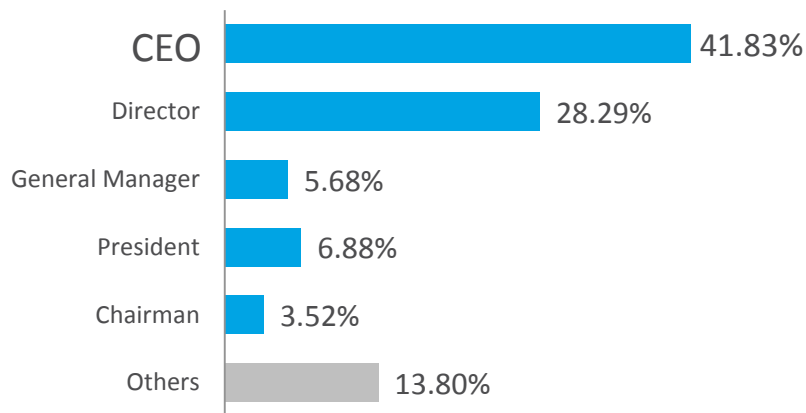
商務電子郵件詐騙損失

\$53 億美元

全球受害企業

>22000

最常偽造的寄件者



● CEO

Immediate Wire Transfer

收件人: Chief Financial Office

2015年2月3日 上午8:09

C

Please process a wire transfer payment in the amount of \$250,000 and code to “admin expenses” by COB today.

Wiring instructions below...

書寫風格異常!!



詐騙者偽裝成高階主管要求財務人員匯款

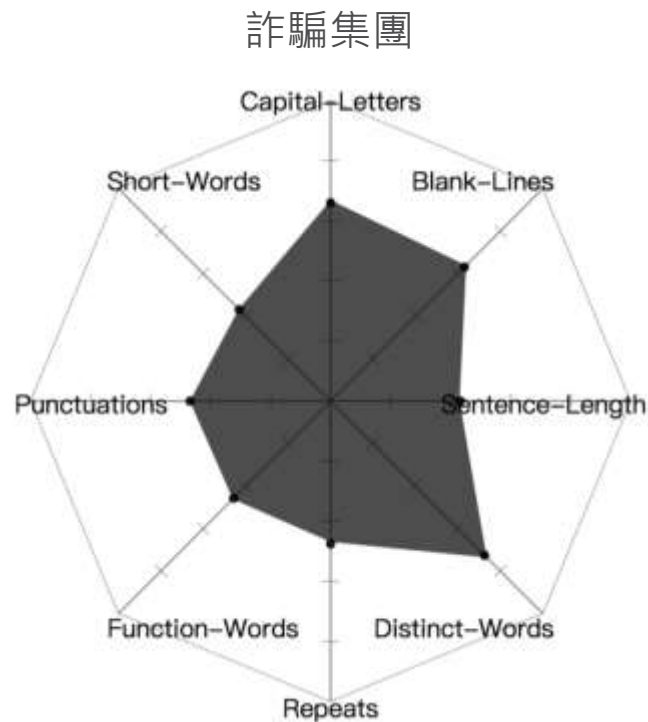
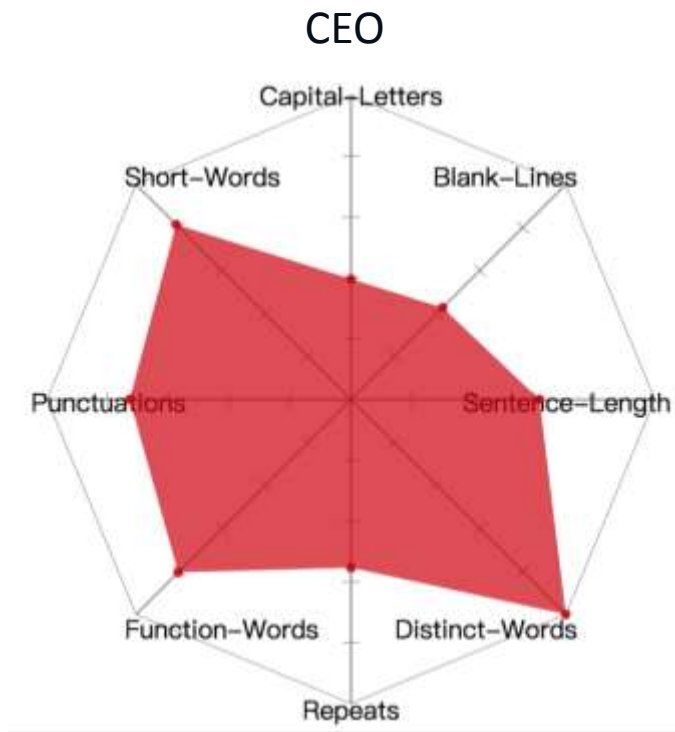


財務人員將款項匯到詐騙者指定的帳戶



詐騙者成功拿到錢

利用 AI 學習 CEO 書寫風格，判斷信件內容是否為詐騙

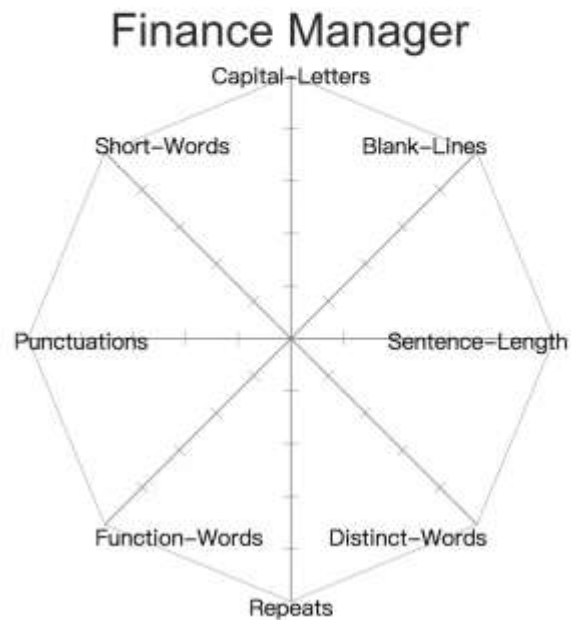
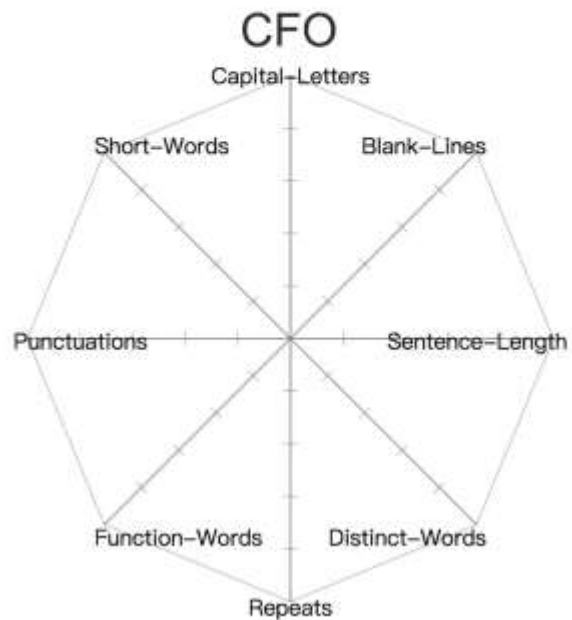
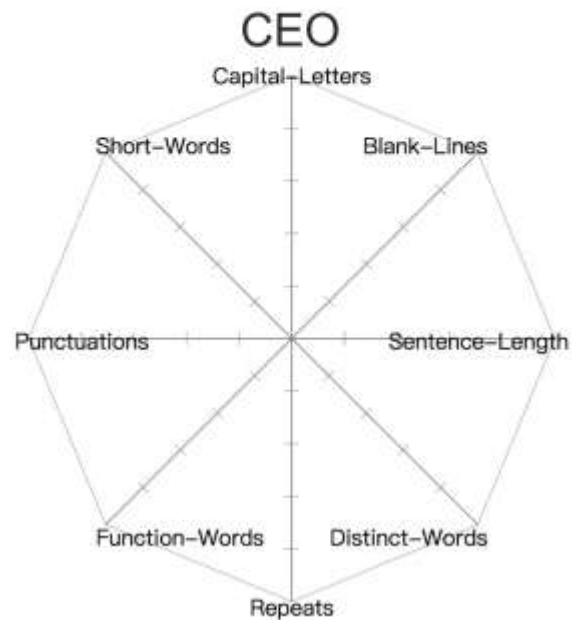


Postman Training Model Demo



Mail number : 0

Performance Variance : 0



趨勢科技主動式雲端截毒技術 (SPN)

2017年上半年阻擋的威脅總數

38,451,584,224



阻擋垃圾郵件

每天有成千上萬封的垃圾郵件, 如何有效率的過濾郵件?
和降低人力成本?

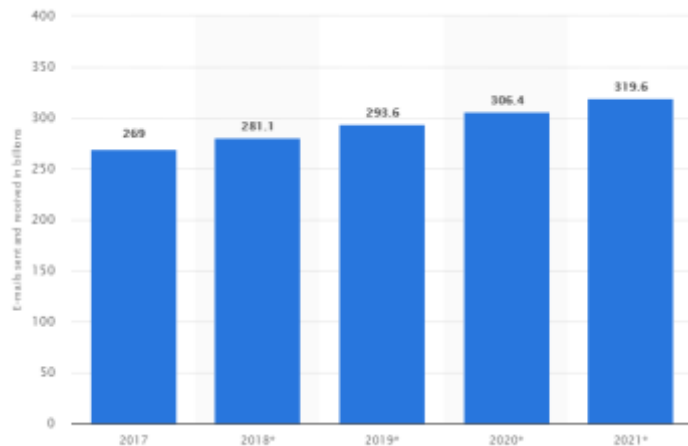
2017全球每天發送和接收
的電子郵件總數

2690 億

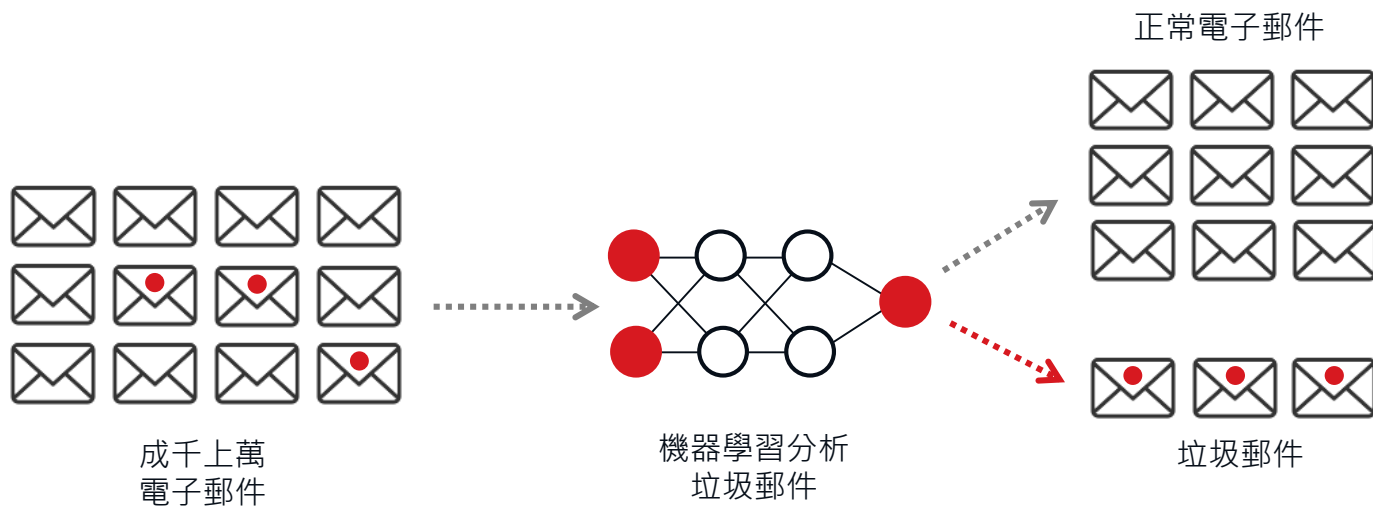
預計到2021年全球每天發
送和接收的電子郵件總數

3196 億

2017年至2021年全球每天發送和接收
的電子郵件數量



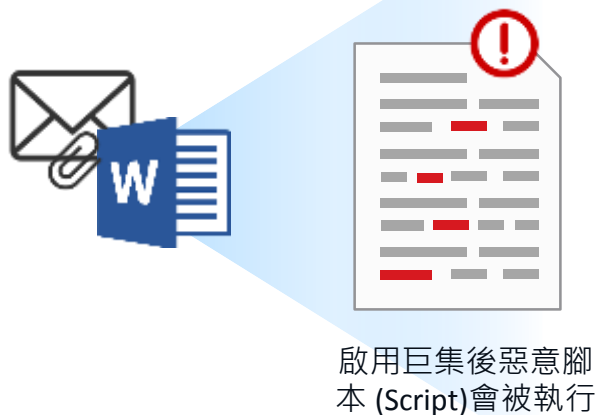
透過 AI 的訓練過濾掉 99% 垃圾郵件 大幅降低人力成本





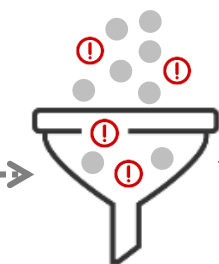
惡意巨集偵測

如何快速的發現夾帶惡意巨集的電子郵件？
和降低雲端沙盒 (sandbox) 處理成本？

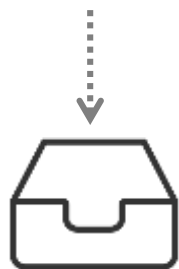


雲端沙盒
Sandbox

過去要在Sandbox
中執行巨集才知
道是否為惡意, 但
成本高速度緩慢



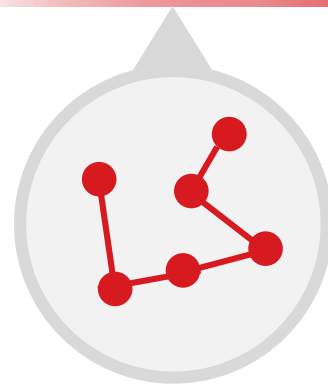
先利用機器學習
分析找出特徵



雲端沙盒
Sandbox

- Obfuscation to hide real command code !
- Get EXE from dangerous URL !
- Save to local script !
- Delete script after execution !
- Hide window while running !

Bad



組成 Macro DNA, 透
過不同 DNA比對, 判
定是否是惡意巨集

大幅減少檔案數量
進到 Sandbox
使成本降低速度變快



客戶續約 可能性預測

每個業務負責多個客戶, 客戶資料量龐大, 業務過去通常依靠直覺來判斷客戶明年是否會續約, 怎麼知道直覺判斷和結果是否有落差?

利用機器學習找出顯著影響客戶續約意願的因素

聯繫回覆率

客戶滿意度

產品使用率

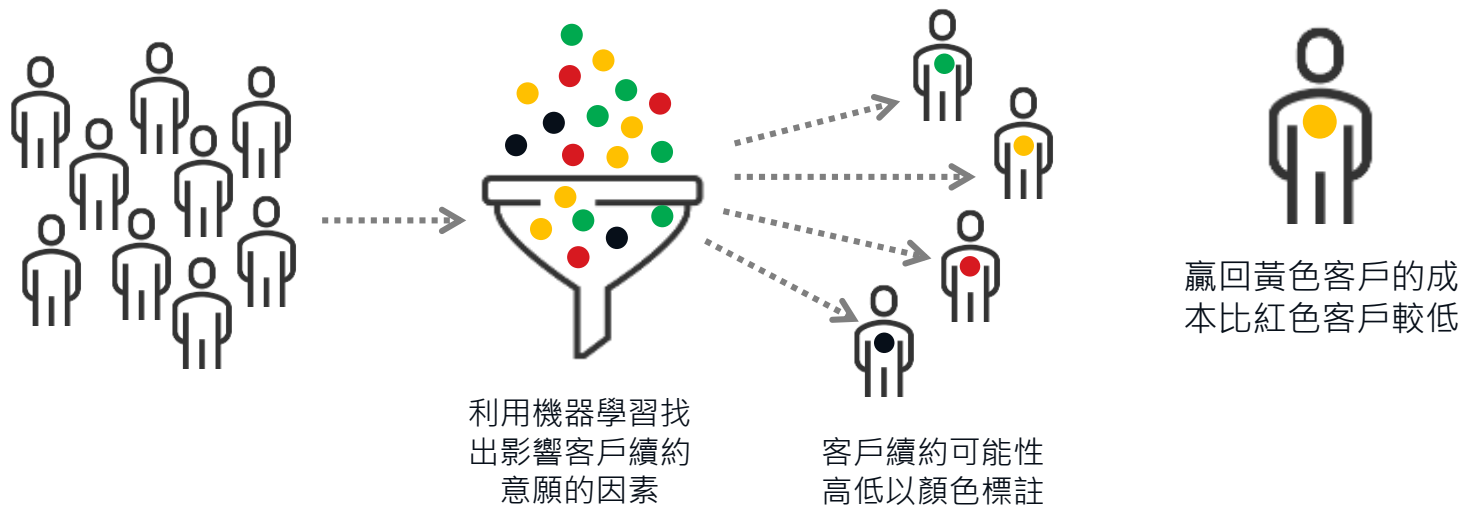
客服案件數與嚴重程度



計算出客戶續約可能性
並以顏色標註

- 續約可能性高
- 續約可能性中等
- 續約可能性低
- 不續約

透過機器學習分析更能精準預測客戶續約可能性 化被動為主動，避免客戶流失，提高客戶忠誠度





XGen 融合了跨世代的威脅防護技巧、全新整合高準度機器學習技術與領先市場的全球威脅情報。

高準度的機器學習融入威脅防禦當中，消除資安上的漏洞，為今日和明日的威脅提供最大防護，保護端點和使用者。

資安不該拖慢您的速度，XGen 端點防護能在適當時機採用適當技巧來提供最佳效能。還能集中掌握及掌控，進而節省系統管理時間。

<http://www.trendmicro.tw/tw/business/xgen/>

經驗分享 – AI 應用

AI+ (AI 產業化)

+AI (產業AI化)





為什麼是 +AI？

- 我們可以使用 AI 減輕工作量並加速客戶服務嗎？
- 現有的結果可以成為機器學習的數據集嗎？
- 用 AI 打敗競爭對手？



AI 並不是一切...

- 技術只是解決方案的一部分
- 預測速度並不是一切
- 用戶界面/製作/支持/定制/全球化/...是我們需要考慮的事情
- 不斷改進

如果我們不做 AI 呢？

很多 AI 項目失敗了...

為什麼公司的業務迅速萎縮？

很多 AI 創業公司失蹤了.....

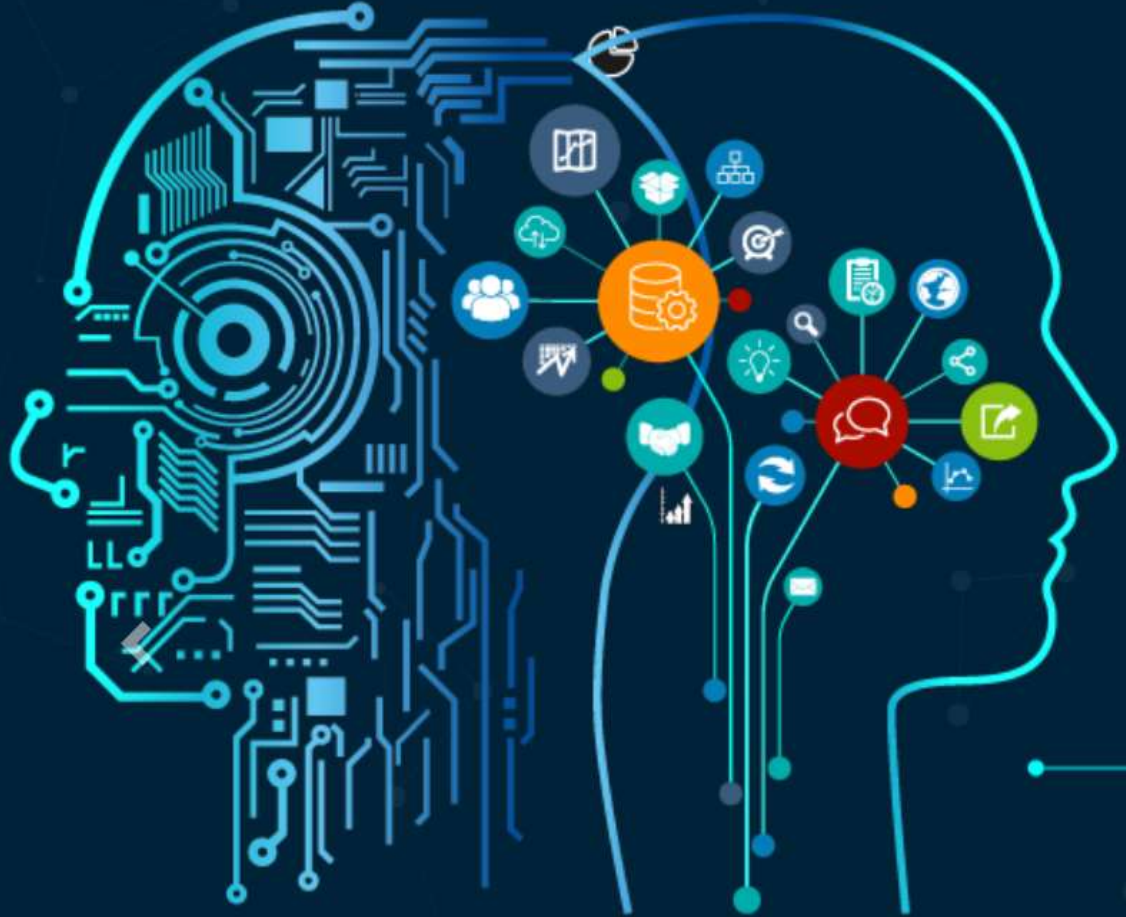
為什麼這家新創公司正在侵吞我們的市場？

很幸運，我們當初沒有做 AI ...

當初我們應該早點做 AI ...

T-Brain 競賽介紹





TBrain

Machine Learning Contest Platform



為何要做 T-Brain

• 業界 •

有資料
沒人才

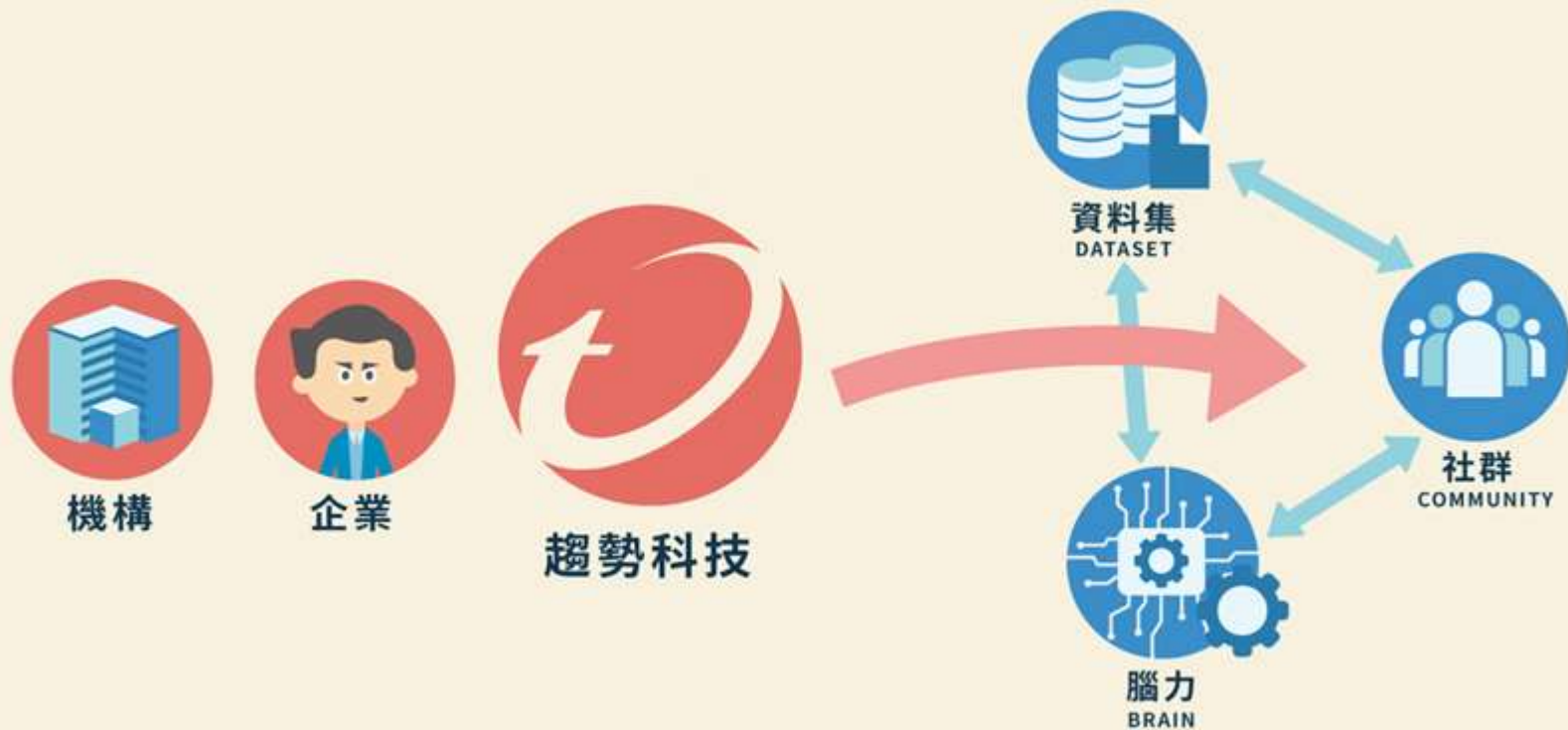


• 學界 •

沒資料
缺少交流平台
既有平台彈性不足
缺乏具商業價值的主題



T-Brain 是甚麼



T-Brain 競賽是甚麼

- 趨勢科技邀請業界提供 Dataset 一起設計比賽題目 以及 評分標準
- 比賽題目及比賽實況會在 T-Brain 平台上
- 各大學學生可參加比賽
- 從2018年開始 預計每兩到三個月辦一次
- 詳細辦法會在題目公佈實頒布

T-Brain 競賽 對業界有何好處

- 業界如果沒有AI人才，可以藉由競賽接觸到學界的AI專家。
- 業界如果有AI的想法，可以藉由競賽來驗證想法的可行性，減少投資新專案的風險。
- 業界可以藉由比賽，提升公司品牌能見度。

T-Brain 競賽 對學界有何好處

- 學生可以藉由競賽提升自己的AI專長
- 學生可以了解到業界真正的需求是甚麼
- 學生有機會可以進入業界工作
- 學生有機會可以找到創業的點子
- 學生可以賺獎金
- 學校可以藉由競賽提高學術地位

T-Brain 競賽 趨勢科技會提供

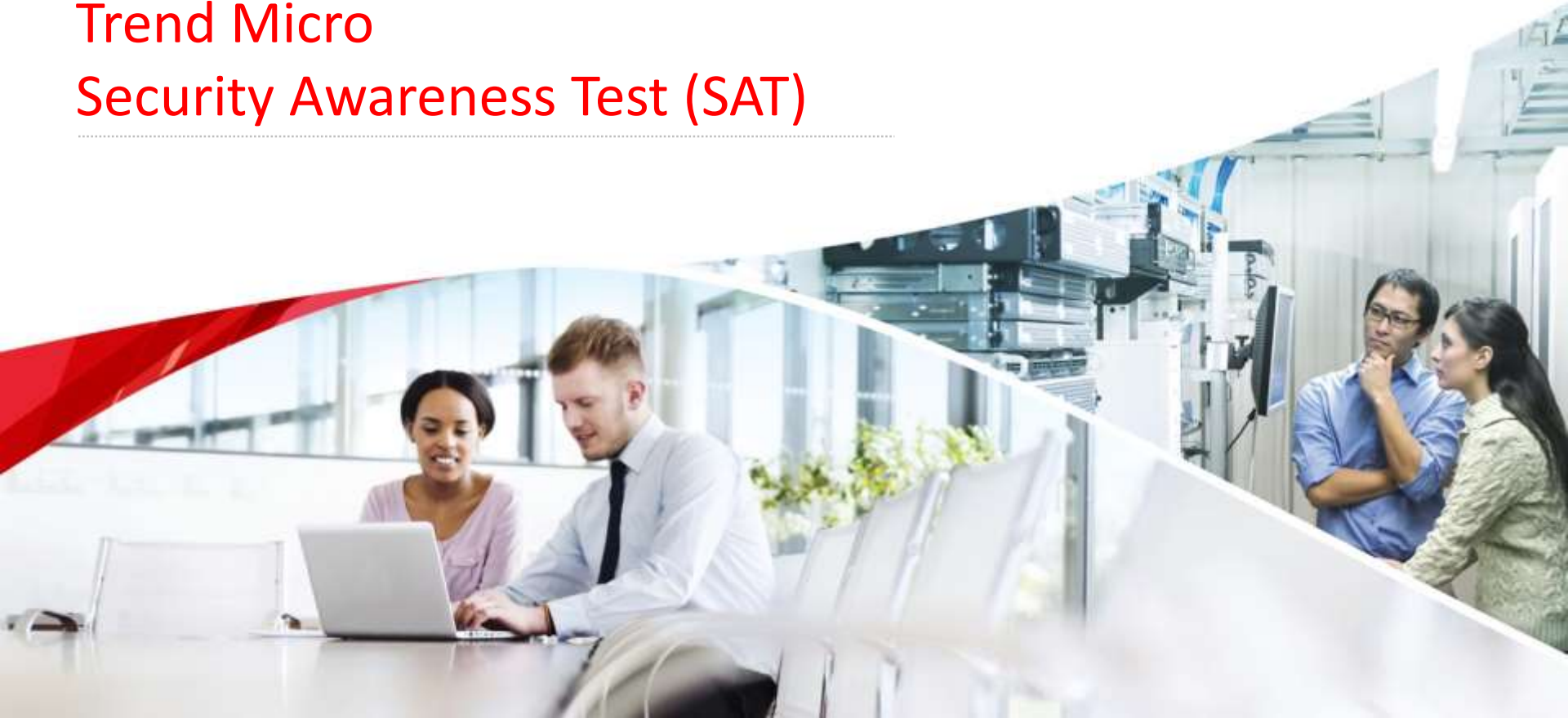
- 競賽獎金 (每次競賽總獎金預計20萬)
- 趨勢科技預聘書 (競賽前幾名的隊伍)
- 介紹參賽隊伍給業界認識
- 趨勢科技AI經驗的分享
- 參賽隊伍成果的智慧財產權都還是屬於參賽隊伍

T-Brain 競賽 範例

- 垃圾郵件分類預測競賽：
 - 趨勢科技提供垃圾郵件及合法的公開正常郵件 (Dataset 分為 Training set and Testing set)
 - 競賽隊伍下載 Dataset
 - 用 機器學習 分析 Training set 並預測 Testing set 結果
 - 上傳預測結果
 - T-Brain 會顯示目前所有參賽的預測分數
 - 比賽最後一天 T-Brain 會公佈最後得獎隊伍

T-Brain 競賽 歡迎業界跟學界共襄盛舉

Trend Micro Security Awareness Test (SAT)



TMSAT

- 透過考試來提升台灣軟體工程師基本資安常識，避免寫出有資安漏洞的產品
 - 很多資安漏洞都是很簡單的錯誤。
 - 很多台灣軟體工程式因為時間的壓力，寫出有漏洞的程式。
 - 一些簡單的資安設計架構，並不被重視。
 - 不知道利用簡單的 資安OpenSource
 - 考試對象不是將來要靠資安為生的人，而是有可能寫程式賣到世界各地的軟體工程師。

TMSAT 架構



TMSAT 歡迎業界跟學界提供意見或題目