

{ AI 時代  
為自己而學 }

親子天下 2024 教育創新國際年會  
International Conference On Education Innovation

# AI 時代的資安素養

吳章銘 Eric Wu  
Fortinet 台灣區總經理



# 後疫情時代，資安事件層出不窮

## AI 生成、GPT、深偽技術讓網路釣魚日益猖獗

iThome 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT EXPLAINED 搜尋

### YouTube平臺出現馬斯克Deepfake影片企圖詐騙加密貨幣，吸引3萬人同時收看

入侵知名企業或名人的網路服務帳號，對其支持者進行金融詐騙的手法頻傳，本周YouTube平臺便出現將特斯拉公司發布的馬斯克公開影片改造成深偽影片，企圖誘騙支持者造訪指定網站並轉出數位貨幣，影片被檢舉下架前5個小時，曾吸引至少3萬人同時觀看

文/ 林妍濠 | 2024-06-25 發表

讚 40 分享



本周傳出特斯拉公司的YouTube帳號疑似被駭，並用來發布利用馬斯克公開影片改造的深偽影片以進行金融詐騙。(圖片來源/ 特斯拉)

Share More Gain More  
2024 iThome 鐵人賽  
加入 2024 iThome 鐵人賽  
從 8 / 1 報名同時開賽

YouTube Live周一出現一則以Deepfake手法製作的馬斯克 (Elon Musk) 推銷加密貨幣的詐騙影片，一度吸引3萬人同時觀看。

科技新聞網站Engadget報導，這則詐騙影片看似馬斯克在特斯拉公司活動中發表演說，馬斯克指示用戶點選造訪某個網站網址，並將手上的比

收看 IT EXPLAINED  
線上研討會

- 場場精彩
- 滿滿乾貨
- 時時互動

線上學習不用等

馬上報名去 ▶

中華電信  
京揚國際導入中華電信5G 專頻專網  
打造優質頂尖物流服務 深入了解

即時 要聞 娛樂 奧運 運動 全球 社會 地方 產經 股市 房市 生活 節

### 透過AI成功變臉為總公司高層 騙走香港分公司8億元

2024-02-04 12:19 聯合報/大陸中心/即時報導

+ 英國



香港警方拆解詐騙集團利用深偽技術行騙的手法，提醒AI時代「眼見不一定為憑」。(圖/取自香港文匯報)



# 2024 年校園系統遭駭仍持續...

yahoo! 新聞

台視新聞網 | 6k 人追蹤 ☆ 追蹤

## 7所高中校務系統遭駭！多達2萬筆個資外洩

### 被駭客盯上！7高中校務系統遭駭、個資外洩 教育部公布學校名單

2024-03-30 17:29 聯合報 / 記者許維寧 / 台北即時報導

+ 教育部



- 全台有7所高中的校務行政系統
- 2024年3月中駭客取得個資，先是向行政系統公司勒索贖款，該公司拒付
- 學生個資外洩的資料地址大多分布在中彰投，還有1988年和1989年出生者，甚至連家長姓名、電話全都被曝光，資料多達2萬筆。
- 仍有26所學校使用相同系統



# 2023 威脅態勢分析 (依地區)

NOT FOR MEDIA RELEASE

台灣依然是資安威脅高度關注的地區

Powered by FortiGuard Labs



Total Threats Detected

970.31bn



Exploit Techniques Detected

111.78bn



Malware Distribution Detected

913.13M



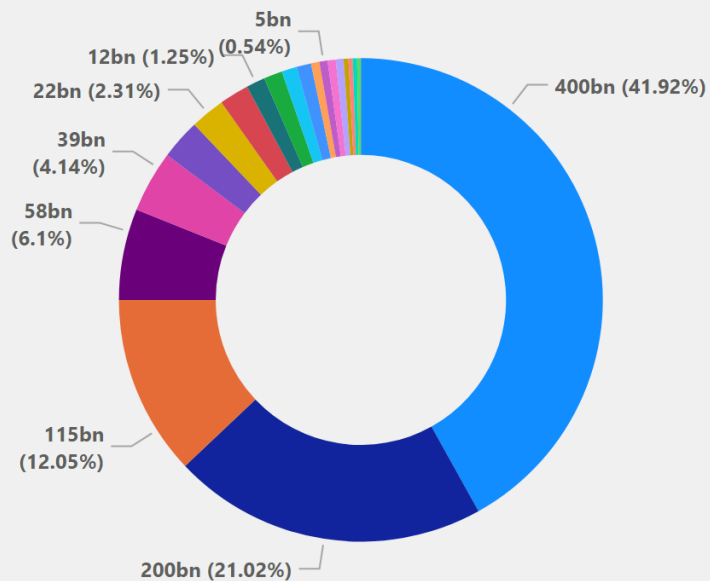
Botnet Activity Detected

2.79bn

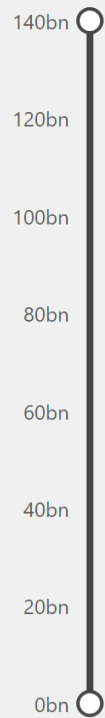
## Malicious Activity Distribution by Country

Country Name

- Taiwan
- Indonesia
- Thailand
- Japan
- India
- Korea
- China
- United Arab Emirates
- Australia
- Kuwait
- Malaysia
- Hong Kong
- Viet Nam
- Saudi Arabia
- Qatar



## Behavioral Trend Analysis by Country



台灣總年度被攻擊次數還是第一，印尼最後兩個月被攻擊數量暴增，為台灣的2倍及4.3倍

TLP: GREEN



# Total Threats Detected

## 970.31bn



# Exploit Techniques Detected

## 111.78bn

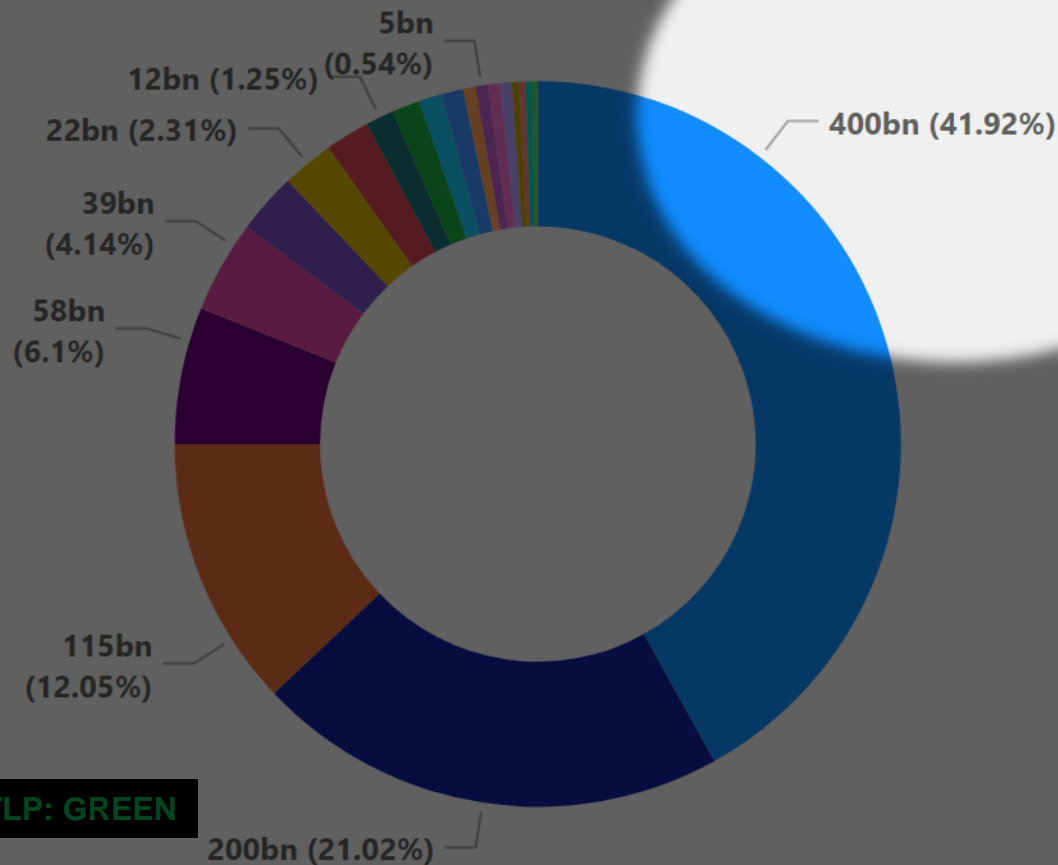


# Malware Distribution Detected

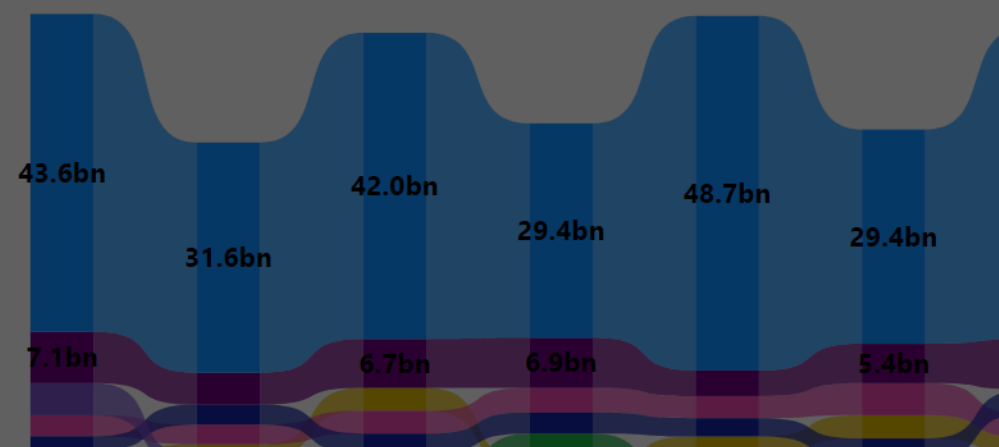
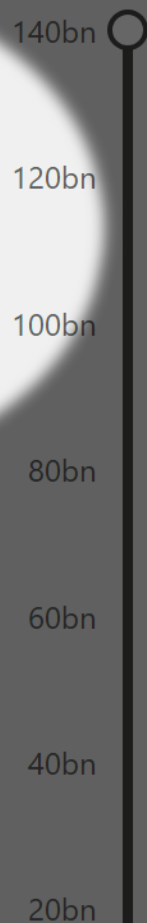
## 913.13M

NOT FOR MEDIA RELEASE

### Activity Distribution by Country



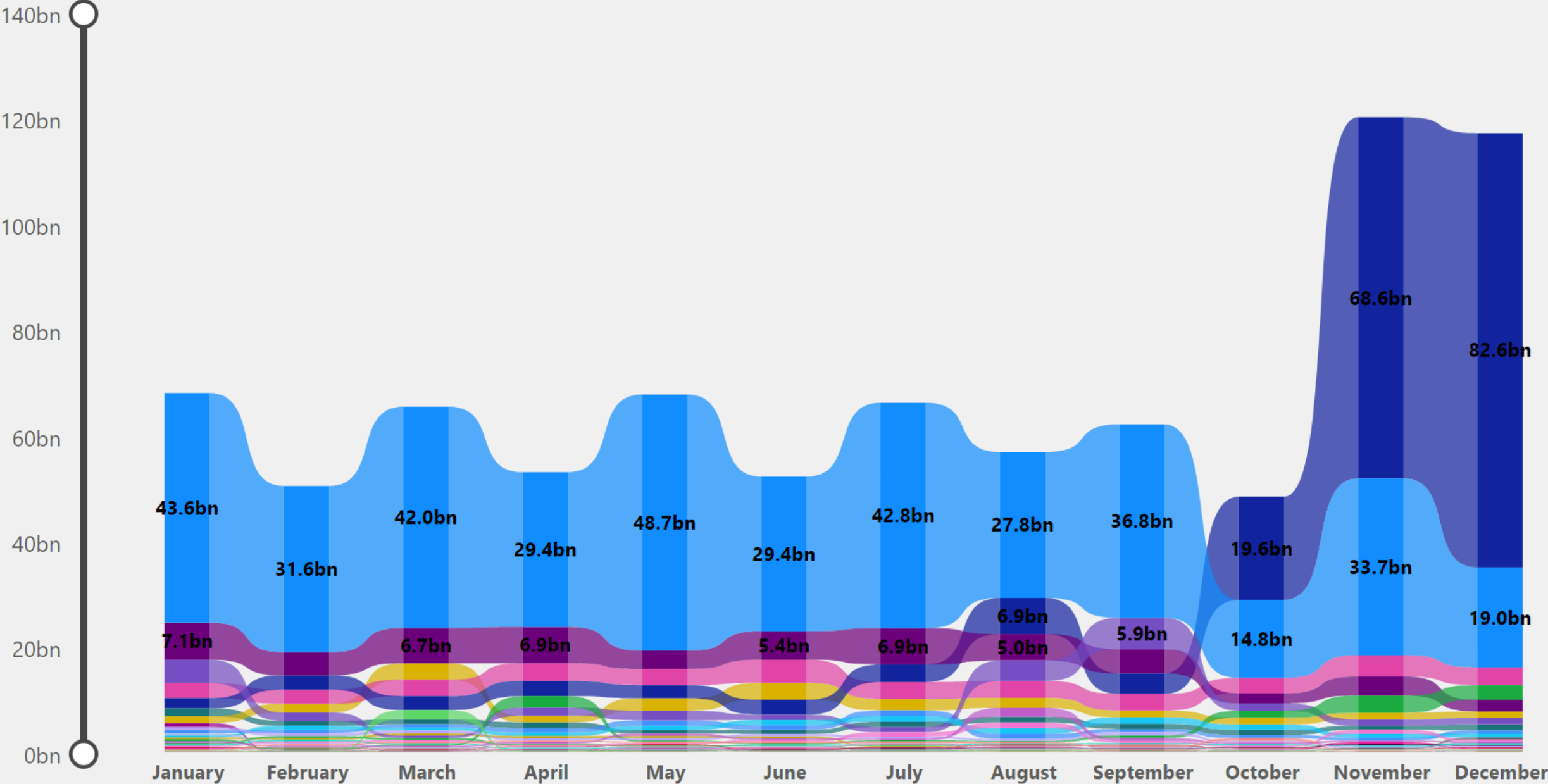
### Behavioral Trend Analysis by Country



TLP: GREEN

# Behavioral Trend Analysis by Country

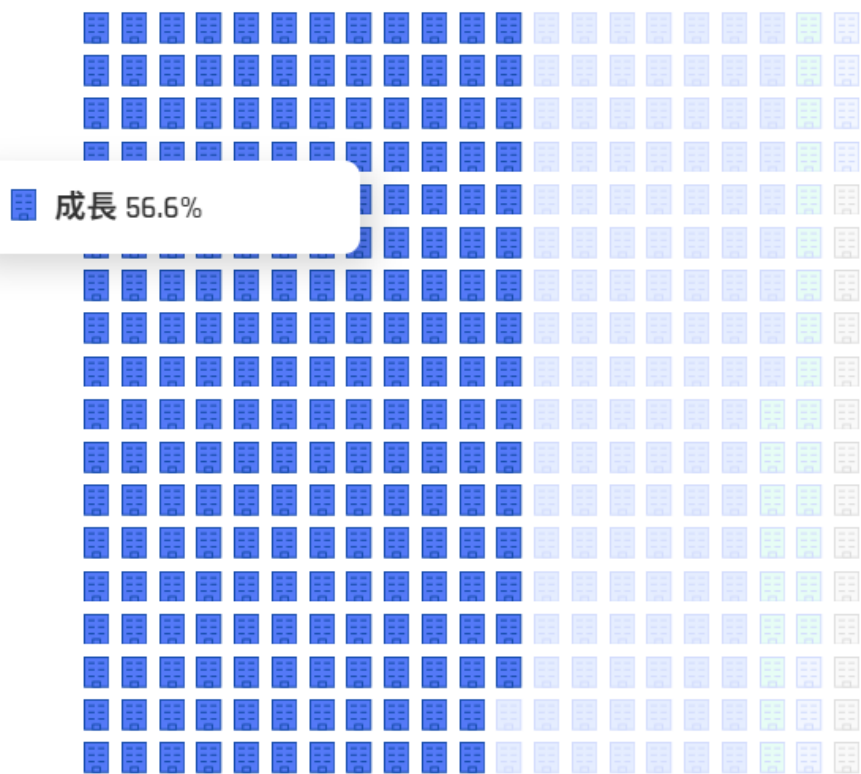
NOT FOR MEDIA RELEASE



# 企業編列的資安預算增加

資安預算是否成長 (%)

■ 成長 ■ 持平 ■ 無相關預算 ■ 減少 ■ 不知道

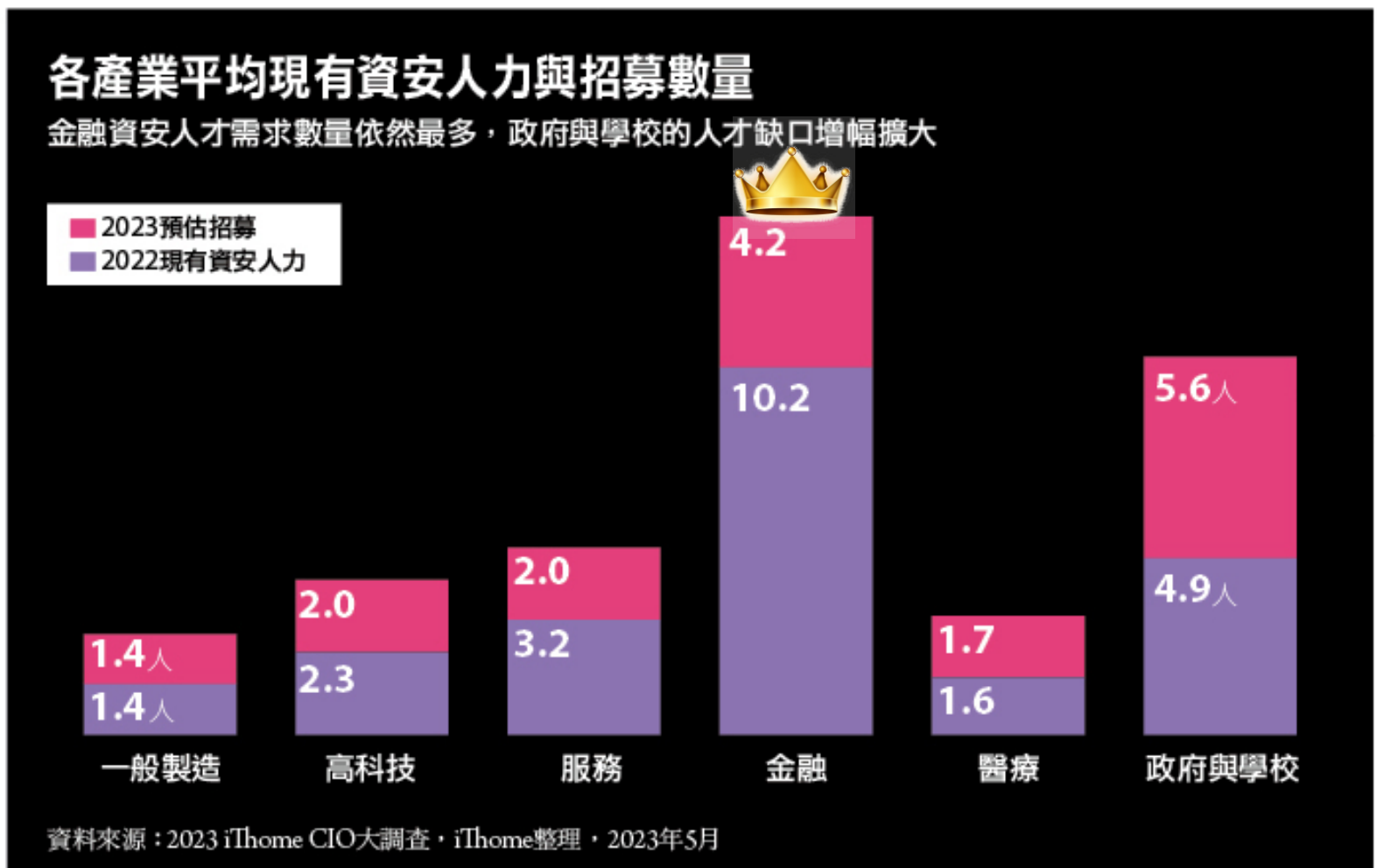


## 企業資安預算年增近三成

- **56.6%** 企業在資安所編列的預算較去年成長
- 整體成長比例平均落在 **28%** 左右 (近三成)

# 資安人力仍有很大的缺口...

2023 年臺灣大型企業平均資安人力約 3.4人，希望擴編到 6.1人，整體還要多招募 7成9 才夠用



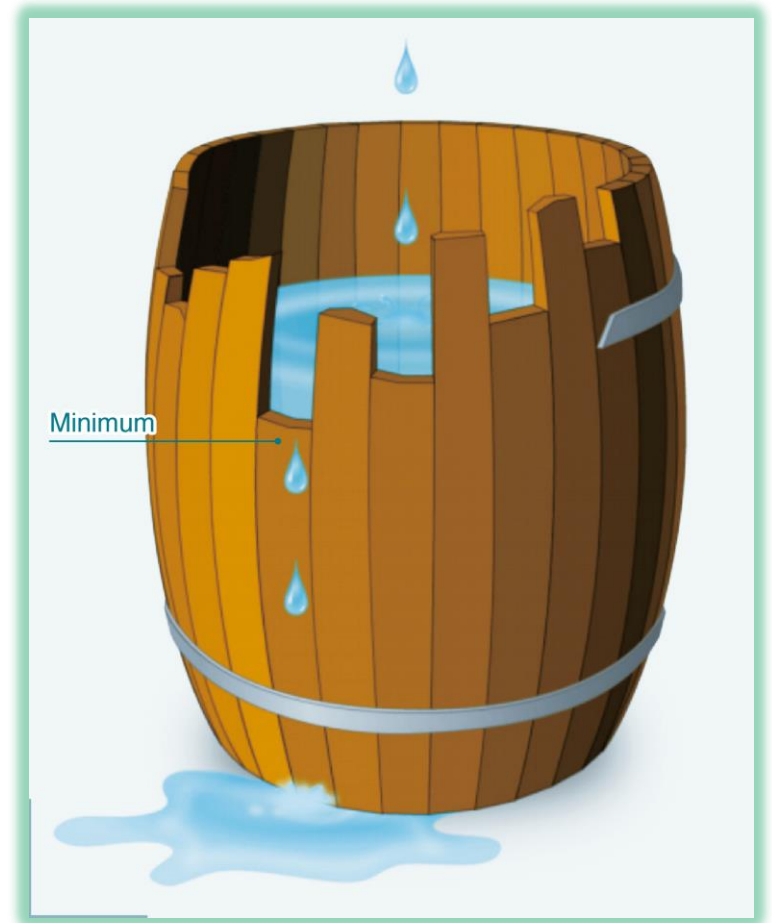
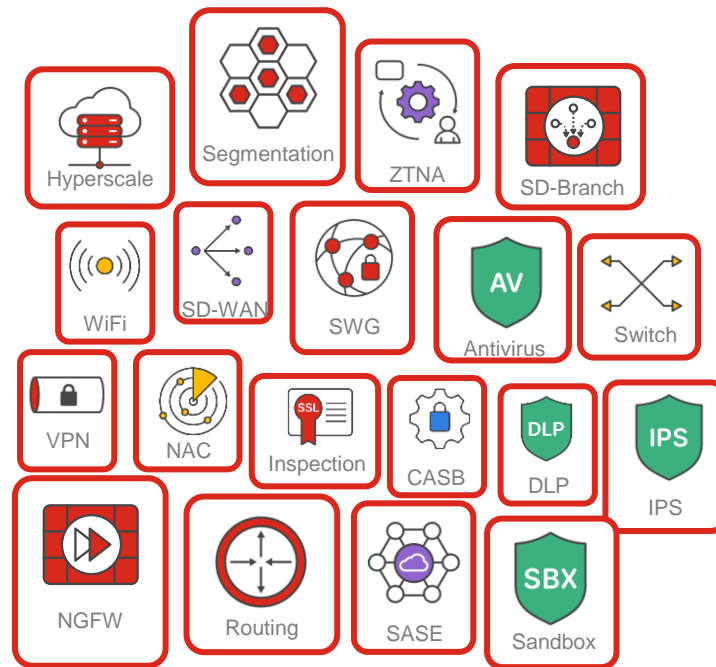
企業需招募的資安人力仍落在六成到九成之間

金融業外，組織中資安人力平均只有 3~4 人

# 木桶理論 (Cannikin Law)

資訊安全概念最基本的是「木桶原理」或「短桶理論」，也就是在木桶子裡能夠盛多少水，不是取決於最長的那一塊，而是最短的那一塊，因此系統最弱的地方就是整個系統能力的所在點

- Website
- Server
- Storage
- Endpoint
- IoT device
- Application
- Mobile User
- OT field
- Cloud
- Etc...



# 向左思考 (Shift to Left)

各種攻擊面以及資安攻擊鏈各個階段都需要更聰明、更主動的能力

## MITRE Pre-ATT&CK 先期預警

## MITRE ATT&CK 資安框架



# AI 虛擬資安分析師 加速 威脅偵測與分析



## AI 具備先進的 判斷與學習能力

使用 AI / ML 盡可能減少人工作業  
與人為誤動作

- 如：惡意軟體識別 / 安全事件分析
- 擁有 5 年經驗的資安分析師平均要花費  
1-2 周時間來分析單一資安事件始末



## 大幅降低事件 檢測時間

將企業網路流量檢測與資安  
事件分析時間從數分鐘級別  
降幅到次秒 (sub-second)  
判定級別



# AI 助手入駐 SecOps 團隊 緩解複雜未知威脅

INVESTIGATE

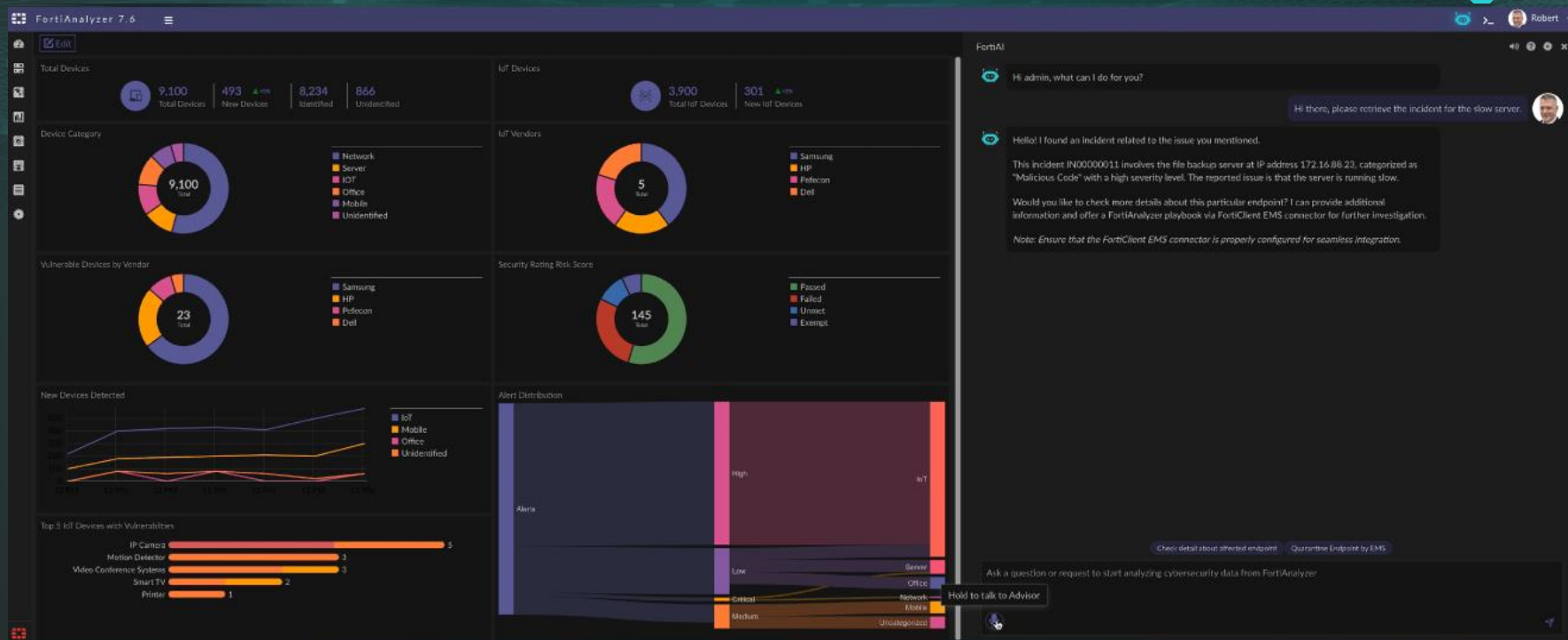
ACTION

- ✓ Retrieve incident for slow server
- ✓ Run FortiClient playbook
- ✓ Investigate public IP address
- ✓ Search for IP addresses connecting to malicious IP
- ✓ Load Threat Hunting Page
- ✓ Search for abnormal login activity
- Display log view



Hi there, please retrieve the incident for the slow server.

FortiAI, 幫我個忙, 請協助分析導致 Server 運行緩慢的事件



# 尋找校園網路安全英雄 – 跟著狗狗學資安

- 課程內容: 輕鬆的漫畫方式，講解網路與網路安全並告訴孩童如何用七大法則在網路上該如何保護自己。
- 適合對象: 中高年級
- 課程時間: 30- 40 分鐘
- 教材: 上課簡報、講義、影片、測驗試題、贈品



Cookie,  
網路上有太多太多的陷阱,  
是你不容易注意到的,  
在網路上更要小心哦!

可是 Bobee, 網路是什麼呢?



# 新北市全台首推! 15 所國中小，超過4,500 名學童



# AI時代的好處與風險

**PROS**

**V.S.**

**CONS**

**提高業務效率**

**假新聞**

**數據分析帶來正確決策**

**深度偽造 DEEPFAKES**

**做出更明智的決策**

**更猖獗的網路攻擊**

**自動化業務程序**

**創造力與社會衝擊**



# We Are Born To Be Secure Networking

吳章銘 Eric Wu  
Fortinet 台灣區總經理