



無聲瘟疫來襲：

工業物聯網三重防禦劍指行動網路資安漏洞

Alpha Chen 陳文雄

CEO, 昇頻股份有限公司

Proscend Communications Inc.

蓬勃發展的資安產業，

又有多少關注在物聯網資安？

IIoT工業物聯網產業應用



Power, Oil & Gas
電力石化油氣

車載應用
In-vehicle



Surveillance
安防監控

建築工程
Construction



EV Charging Station
充電站

再生能源
Renewable Energy



Parking Lot
無人停車場

環境監測
Field Monitor



Transportation
智慧交通

軌道安全
Railway Safety



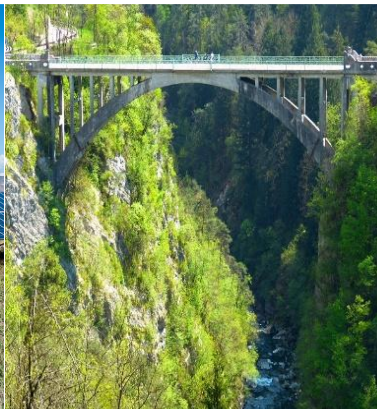
Vessel
船舶通訊

倉儲管理
Warehouse

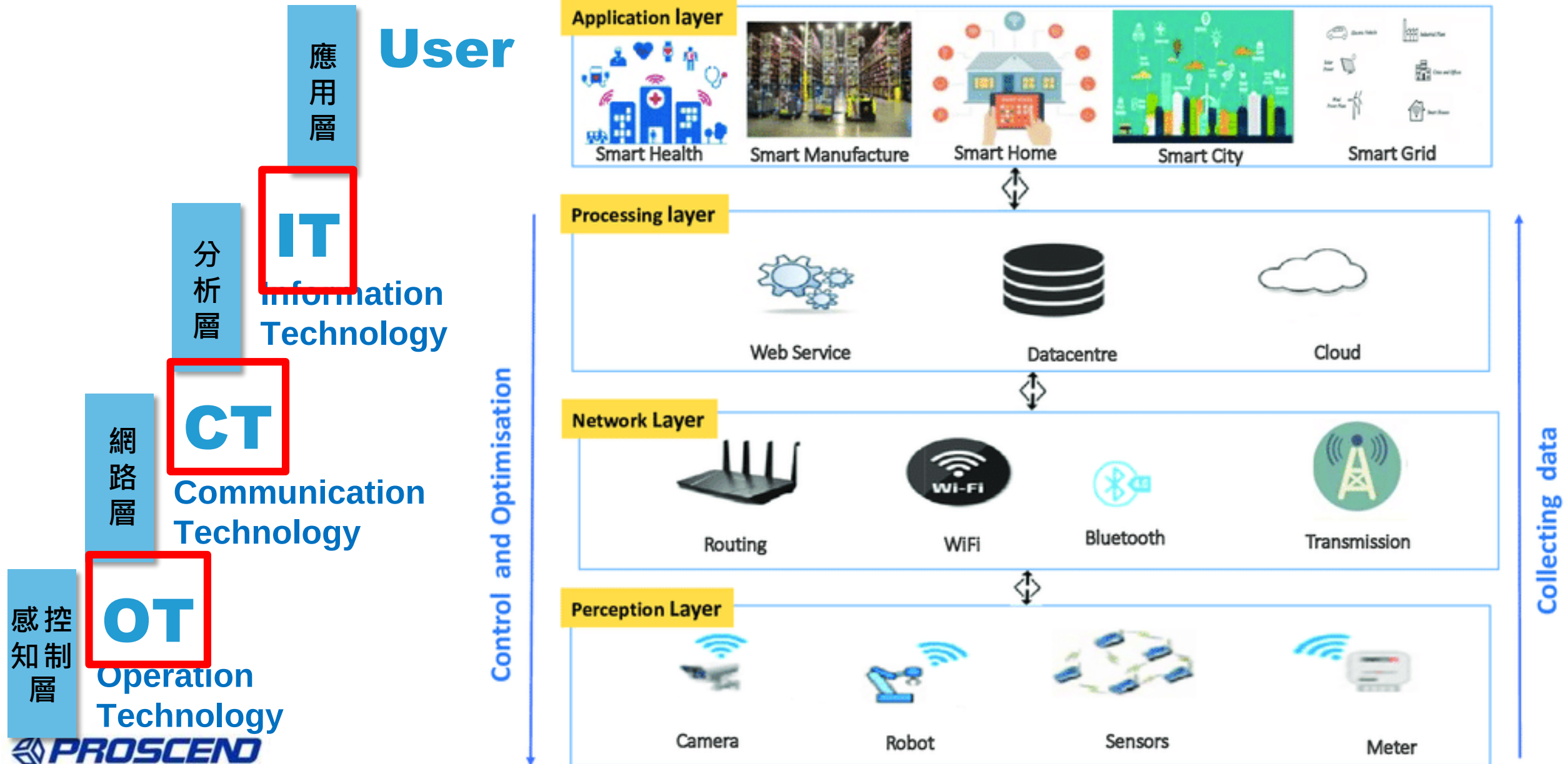


Ambulance
智慧醫療

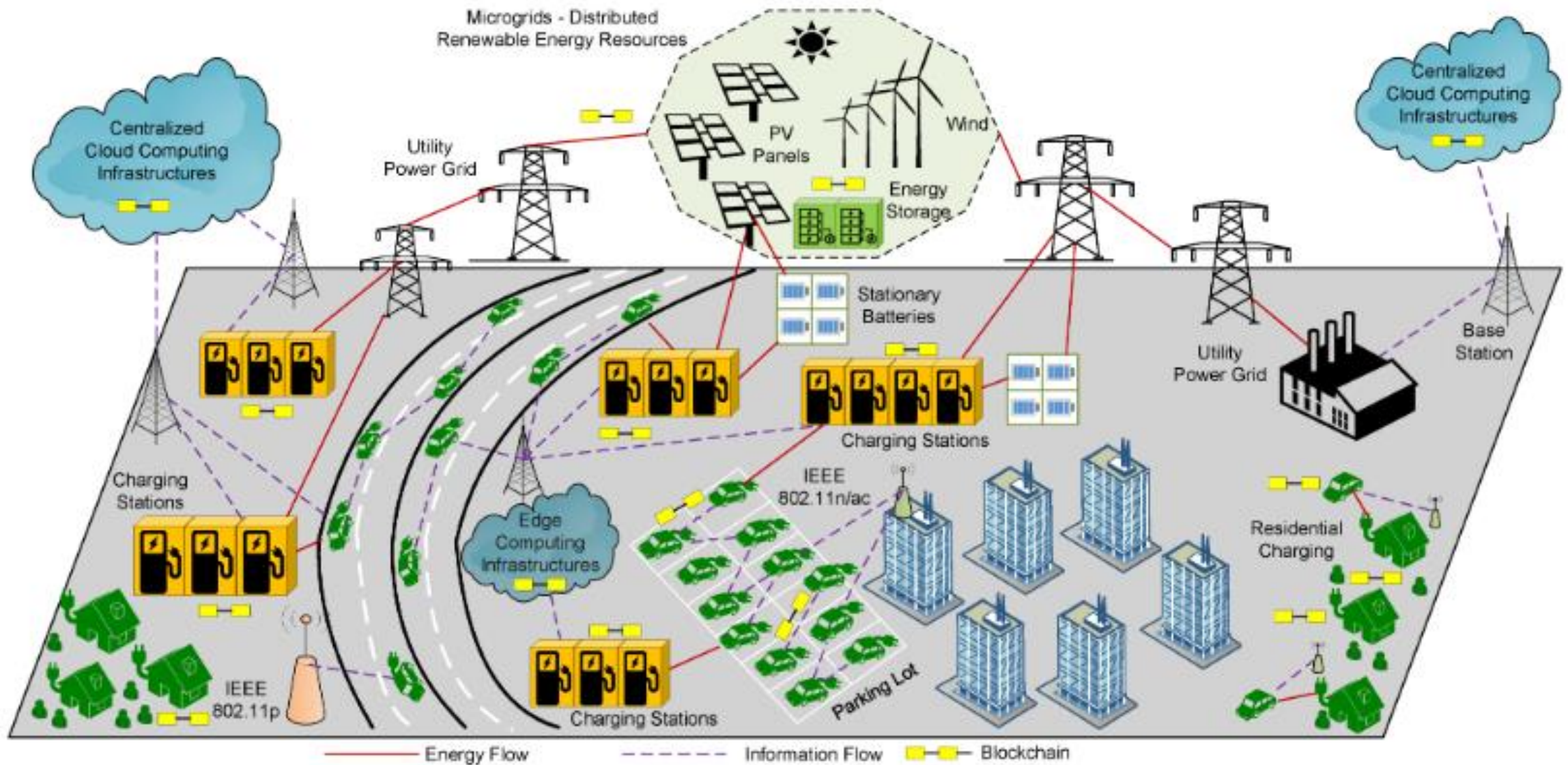
智慧移動
AGV/AMR



工業物聯網基本架構與涉及的專家領域



網上到處皆可看到IIoT的偉大應用圖



網上到處皆可看到IIoT的偉大應用圖



The background diagram shows various IIoT components: 'Microgrids - Distributed Renewable Energy Resources' with solar panels and wind turbines; 'Centralized Cloud Computing' in a cloud; and a large black box containing the equation $IT \times OT \times CT = IIoT$.

$$\underline{IT \times OT \times CT = IIoT}$$

有沒有已知的資安防禦破口？



工業4.0 風潮下的廠內聯網訴求OT and IT Convergence

很安全嗎？看看歐洲某工業自動化大廠的自省

40%



Un-patchable Windows

40% of ICS were hacked in Q1, 2018
3 out of 4 sites run a Window version no longer supported by Microsoft

60%



Weak Authentication

Default passwords in operation, no password encryption, no network access control

31Days



Loss of Production

31 days to identify and recover from cyber attack or instruction, from massive logs or even no logs

67%



The OTA Myth

2 out of 3 industrial sites are now connected to Internet, there will be more.....

基本解法：狂加IPS，細分網端，網內Firewall，管制聯外網

當OT微型化又聯上了外網變成IIoT
資安挑戰變得更加嚴峻，但廠內守護設備的招式卻使不開

Poor Computing
Resources

Miscellaneous
vendors

Lack of Patch
management

Long life spans,
hard to update

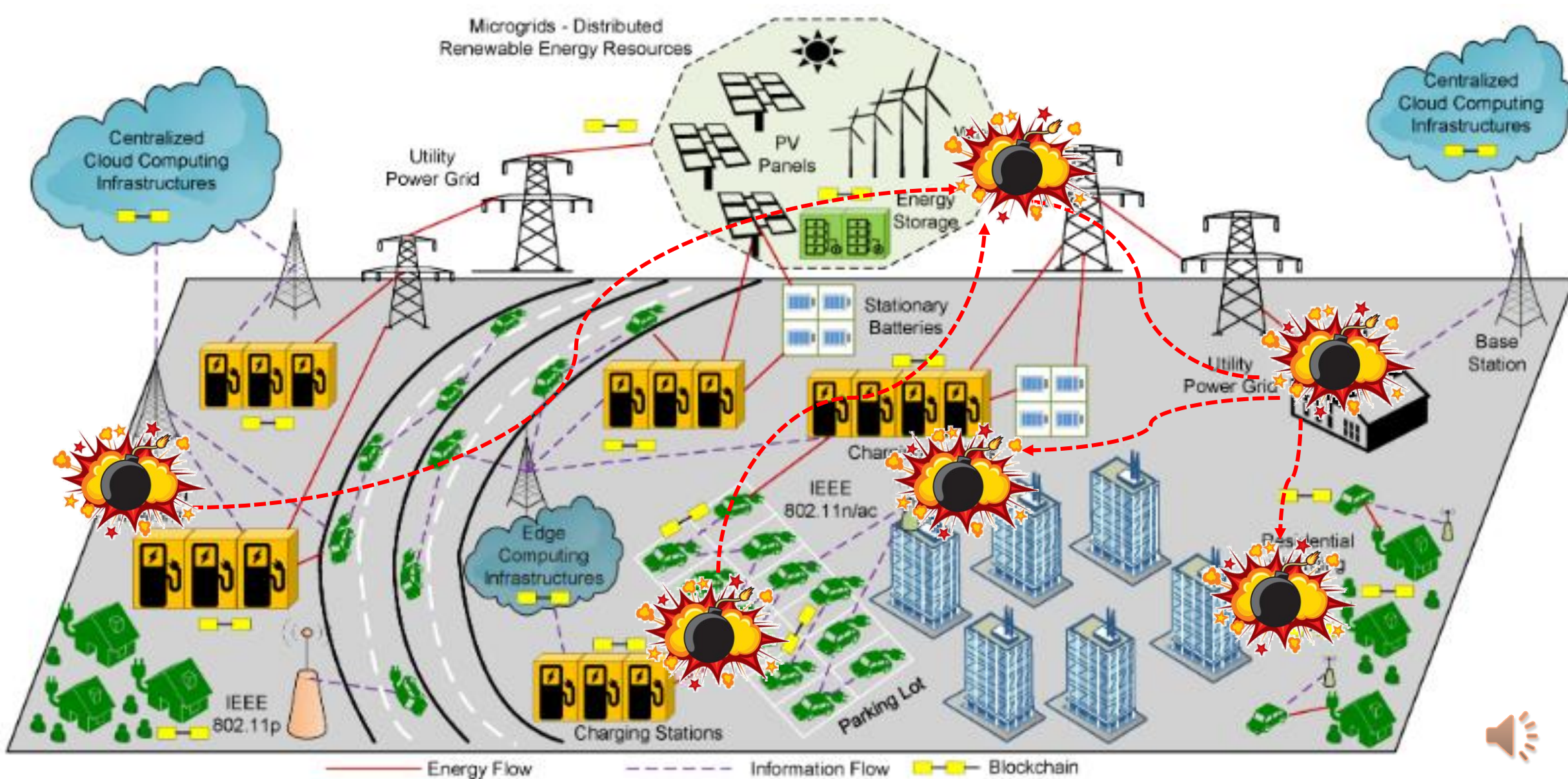
Inability to detect
security vulnerability

New Cyber Threats
from Internet

Myth: Someone else will fix the cybersecurity problems !

迷思：物聯網資安問題總會有人去解決的啦！

無聲瘟疫來襲：物聯網資安出現破口就有如地圖炮全炸開



WHO'S NEXT?

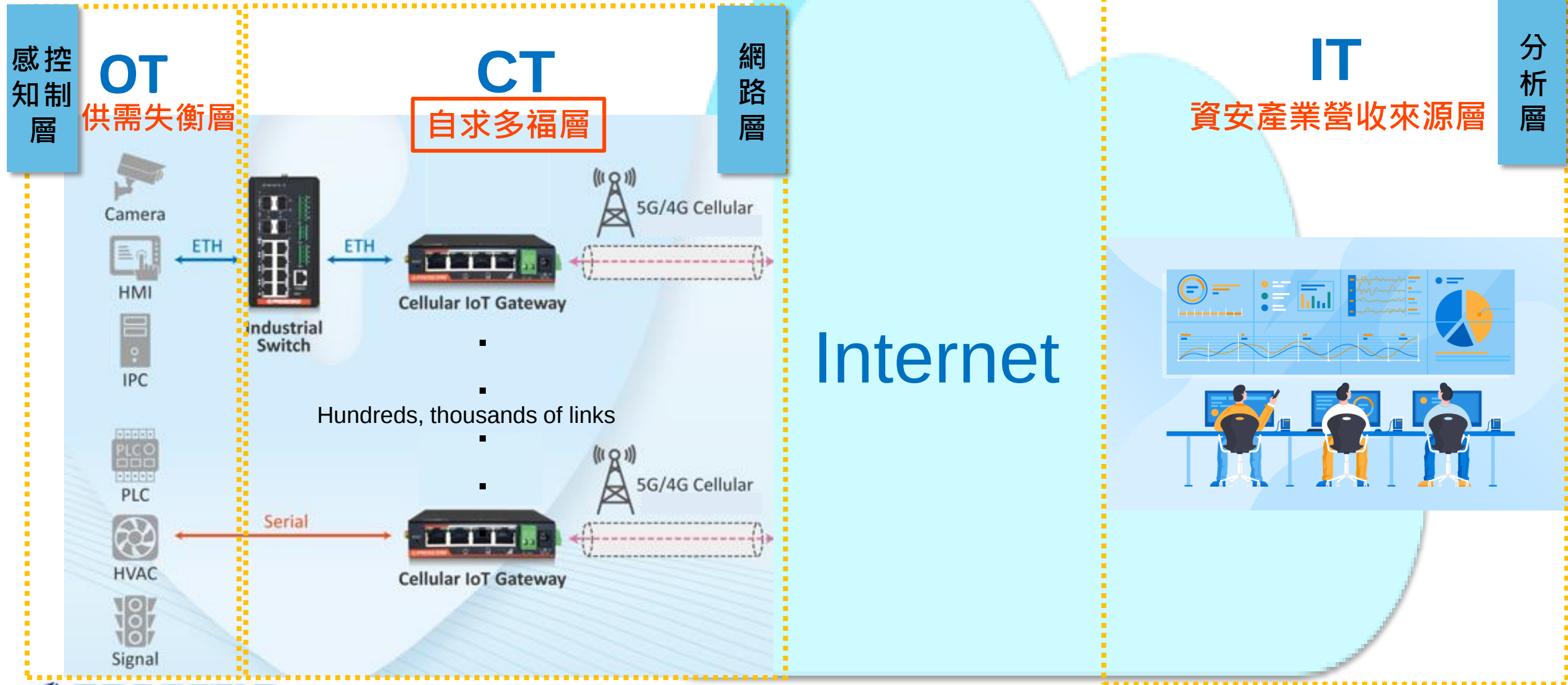


冷靜一下，讓我們重新檢視IIoT基本架構

Looking-Fine
Sec. Budget

Low Sec. Budget

High Sec. Budget



Proscend leads the CT ways

自求多福層4G/5G領導品牌

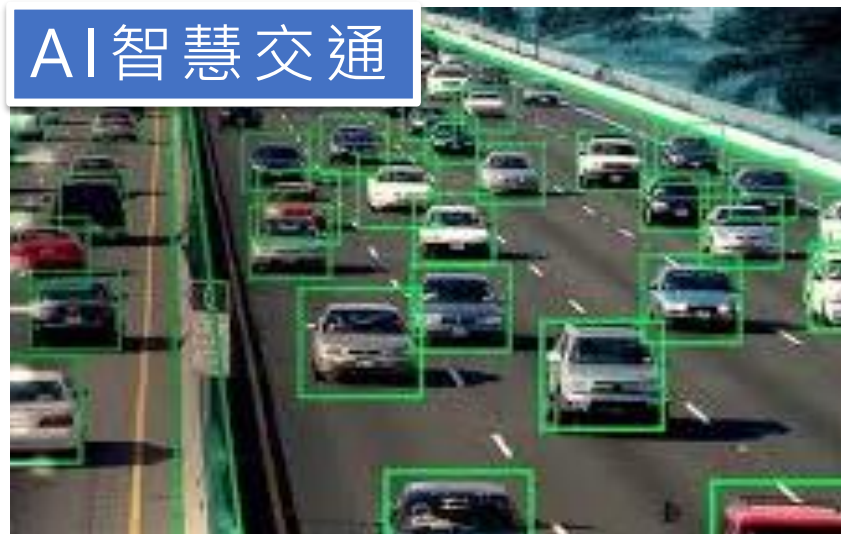


IIoT實際聯網個數從幾十個到幾千個都有

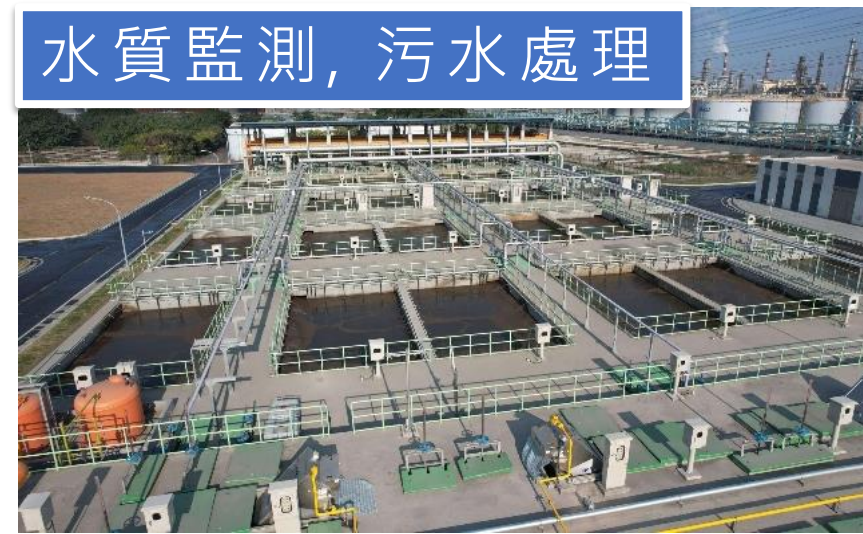
電廠，石化業



AI智慧交通



水質監測，污水處理



停車場



綠色能源



充電站



CT自求多福之餘，也樂於造福鄉里

Looking-Fine
Sec. Budget

Low Sec. Budget

High Sec. Budget

感知層
控制層

網路層

分析層

OT

供需失衡層

CT

自求多福層

IT

資安產業營收來源層



Camera



HMI



IPC



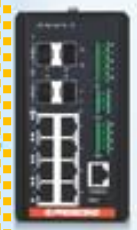
PLC



HVAC



Signal



Industrial Switch



Cellular IoT Gateway



5G/4G Cellular

1. 確保IoT Gateway
本質安全



Cellular IoT Gateway

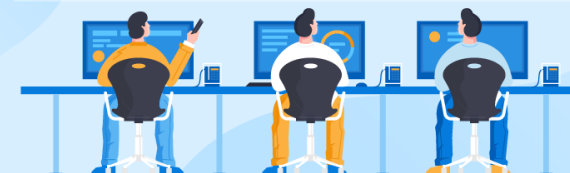
2. 阻止個別OT
小內網入侵擴散

3. 阻止IT破防擴
散至OT小內網

4. OT設備查察
並反控制設備

5. 佈建初期遠
端對OT設備作
接管控制

6. 透過API 整合
IT系統



CT不出, 誰與爭鋒

蜂巢式物聯網 (Cellular IoT) 企業網路的隱形後門

工業物聯網行動網路資安威脅

Jason Huang 黃傑笙, CEO

April 15th , 2025

CTOne 簡介



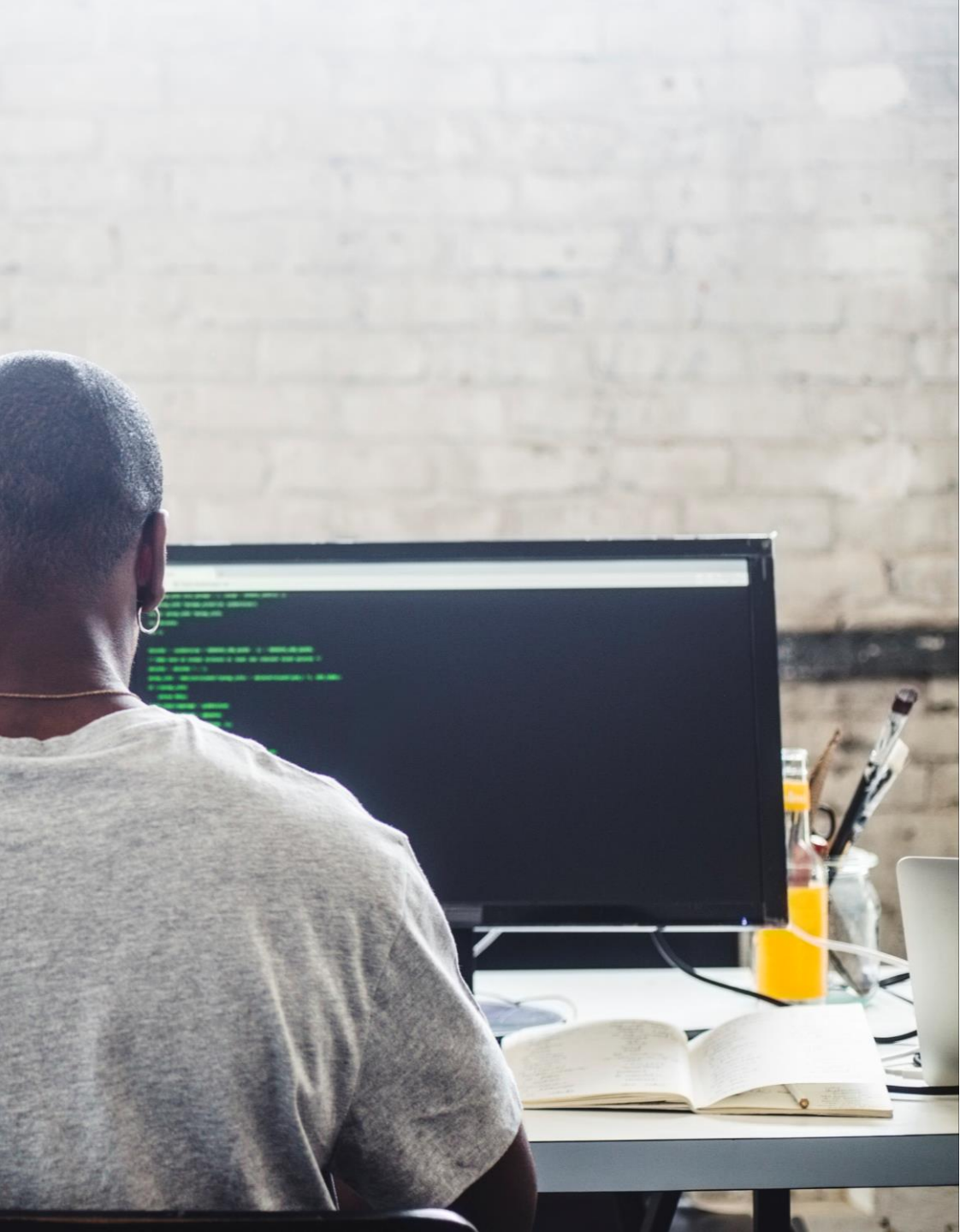
訊勢科技成立於 **2023** 一月

100% 由 趨勢科技 (Trend Micro Inc.) 投資持有

專注於 新世代通訊技術 **CT (Communication Technology)** 資訊安全領域

提供為 **5G/O-RAN/Mobile IoT** 應用量身打造的資安防禦解決方案

協助 企業客戶/移動網路運營商 守護移動網路應用的安全



新世代通訊技術資安研究



**Dedication to CT networks &
IT/OT threat intelligence**



Hands-On Approach



Pioneering Research



**Exclusive CT Database
+ Trend Micro IT/OT Database**

蜂巢式物聯網 (Cellular IoT)

CIoT 是物聯網 (IoT)設備的一種，這些設備將通過行動網絡(公網/私網)，如 4G / LTE 或 5G 進行連接及資料傳輸。



蜂巢式物聯網應用

Smart City

Smart Mining

Smart Transport

Mobile Edge AI

Smart Wind Farm

Smart Energy

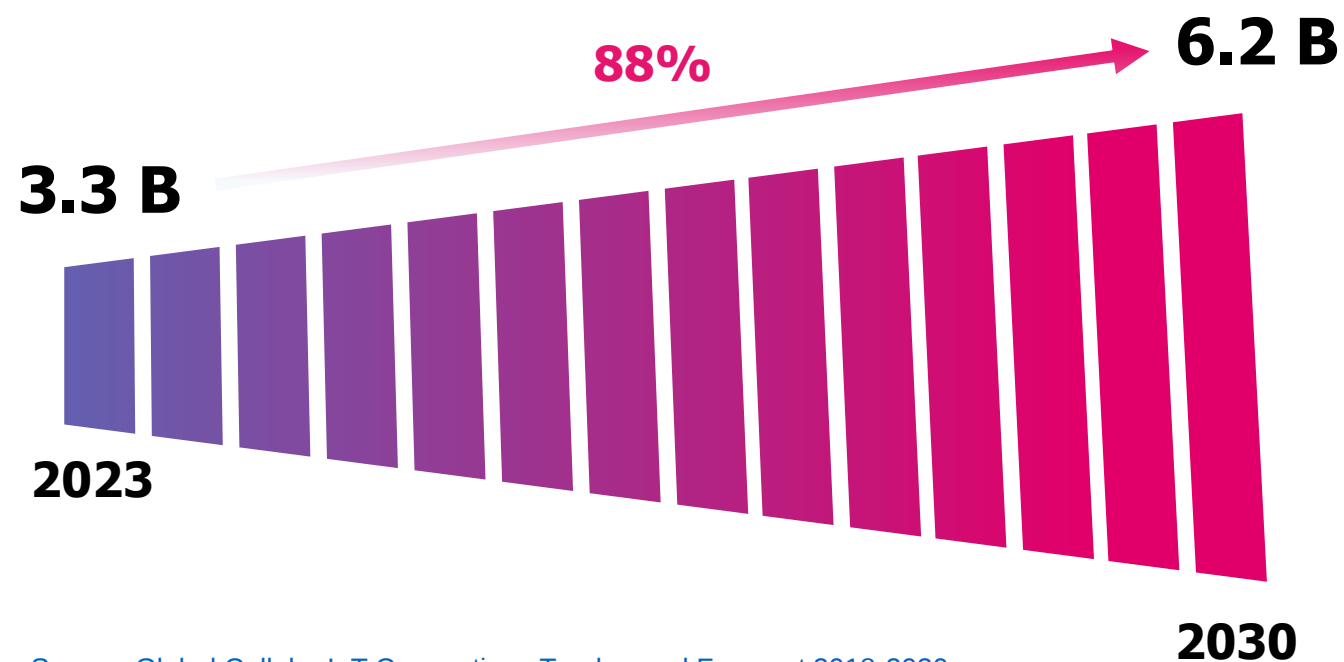
Smart Harbor

Smart Manufacturing



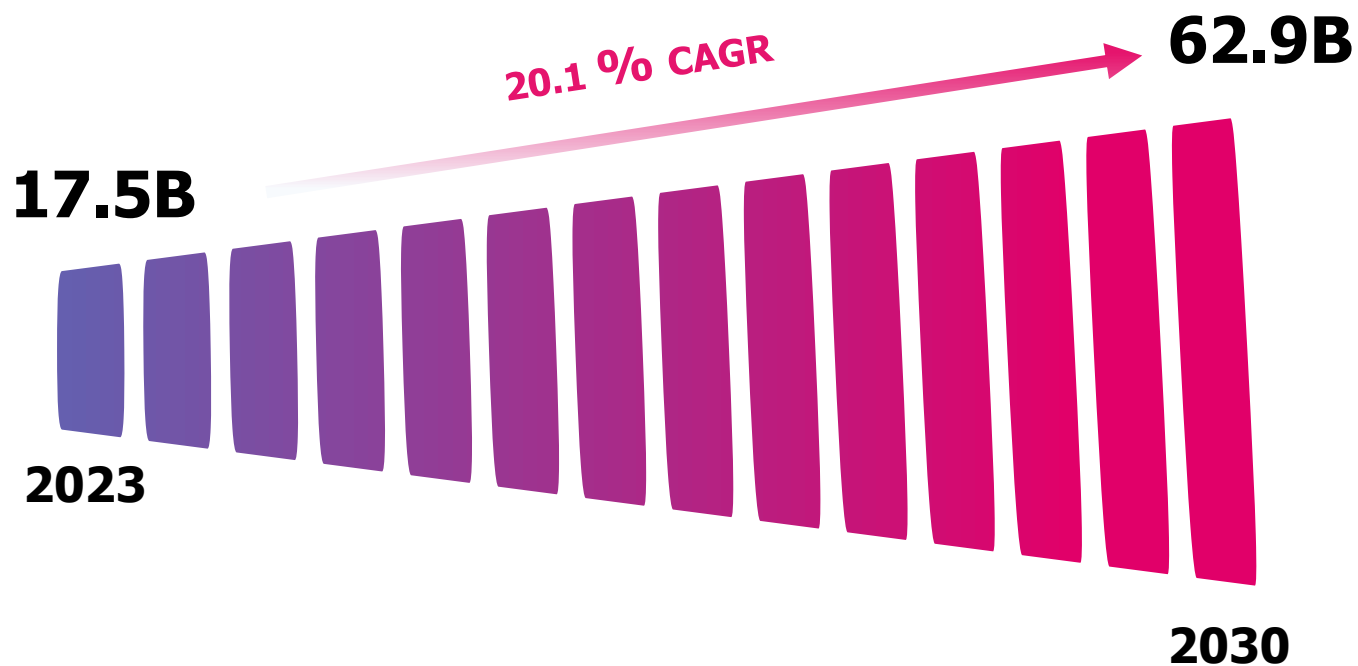


Cellular IoT (CIoT) 裝置預計將成長 88% (每年複合成長率為 10%) , 到 2030 年將達到 62 億台 (2023 年已達到 33 億台)



[Source: Global Cellular IoT Connections Tracker and Forecast 2018-2030](#)

邊緣人工智慧 (Edge AI)市場規模在 2023 年為 174.6 億美元，預計從 2024 年到 2030 年的年複合增長 (CAGR)為 20.1%，到 2030 年將達到近 629.3 億美元。



[Source: Edge AI Market: Global Industry Analysis and Forecast \(2024-2030\)](#)



針對蜂巢式行動網路的威脅面向

108

Unique Techniques



11

Attack Vector



79

CT-Specific



Source: CTOne TR2



Cellular IoT Vulnerabilities: Another Door to Cellular Networks

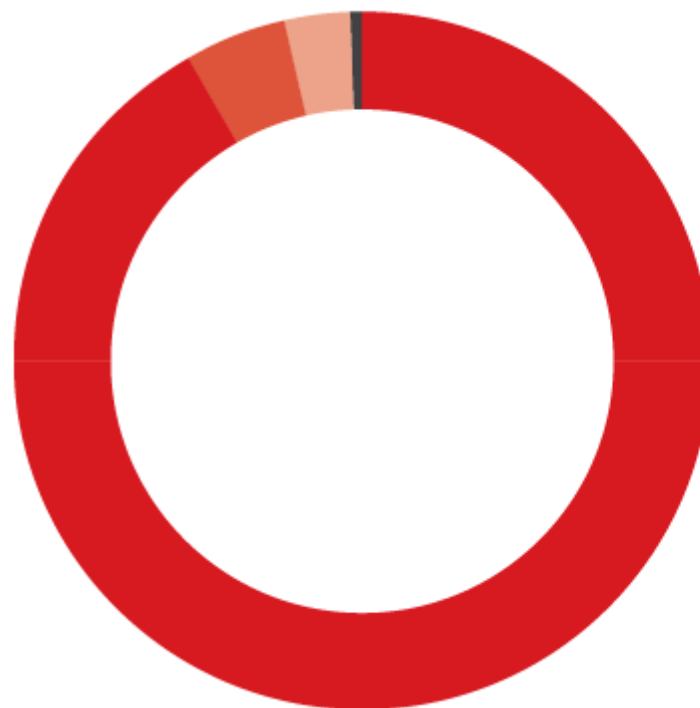
Released on 2024 Oct. by CTOne TR2 Research Team



[Cellular IoT Vulnerabilities: Another Door to Cellular Networks | Trend Micro \(PH\)](#)

資安漏洞名列前茅的 CIoT 裝置

91%

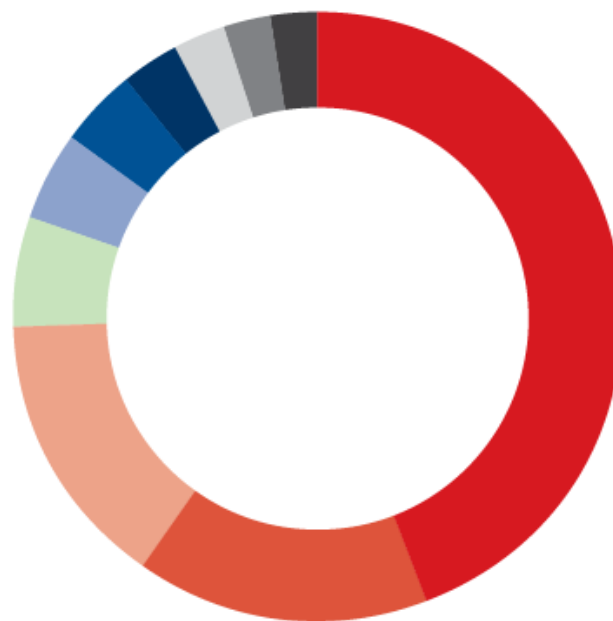


Router	91.7%
Gateway	4.9%
Home Hub	2.9%
IPcam	0.5%

Cellular Routers 是漏洞排名第一的 CIoT 裝置，與其被大量佈署有關

常見的 CIoT 裝置資安漏洞

44%



Command Injection	44.3%
Buffer Overflow	15.4%
XSS	14.8%
Path Traversal	5.9%
Null Pointer Dereference	4.7%
Hidden Fuctionality	4.1%
Information Leakage	3.0%
CSRF	3.0%
Hardcoded Credentials	2.4%
File Deletion	2.4%

Command Injection 是最常見的漏洞

光有登入密碼保護是不夠的

72%

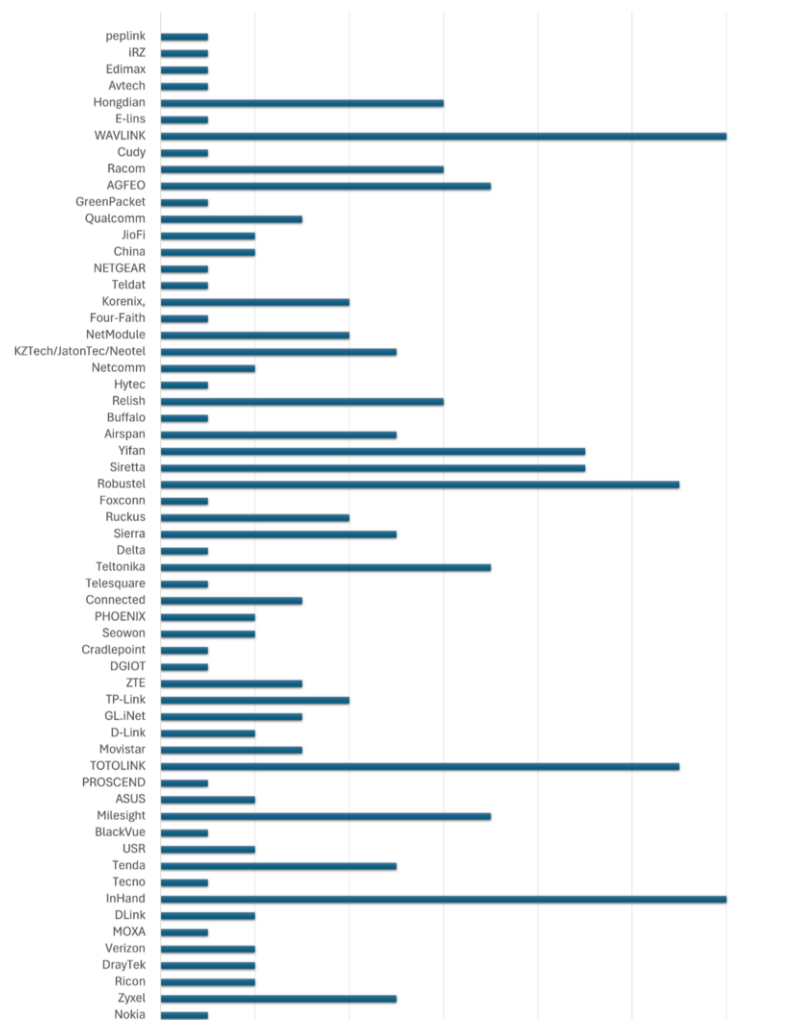


● Pre-Authentication	72.4%
● Post-Authentication	27.6%

72% 的漏洞可在未登入裝置的情況下被觸發



存在資安漏洞的供應商與漏洞數量



蜂巢式物聯網 (Cellular IoT) 端到端的資安風險

CloT 終端裝置



易受攻擊的終端裝置
及身分洩漏

無線接取網路



脆弱的 RAN 基礎設施

邊緣計算網路



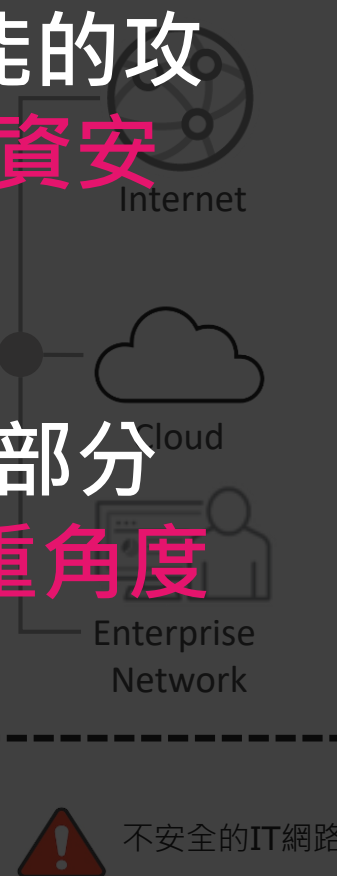
不安全的邊緣運算
系統及其應用

移動核心網路



脆弱的移動核心基礎設施
和系統

資料網路

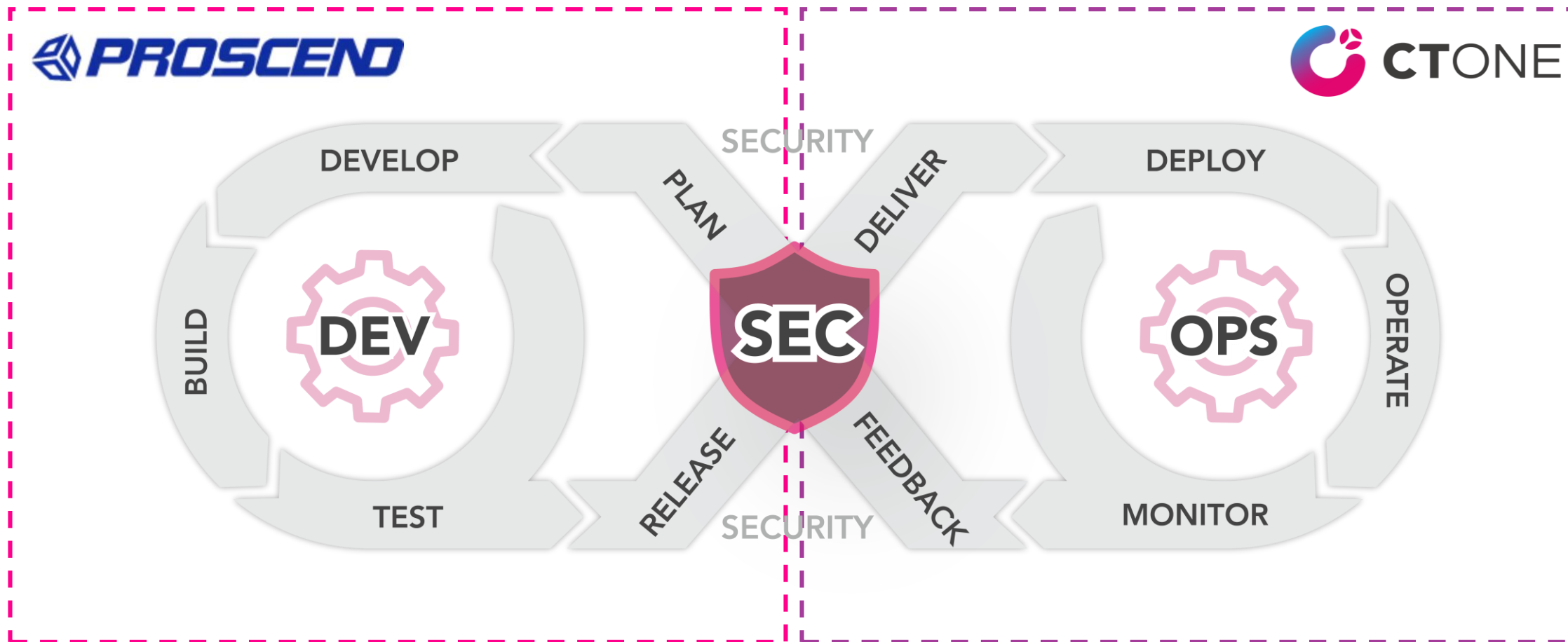


不安全的IT網路

- 作為可能的攻擊進入點，佈署於可能的攻擊傳輸路徑上，CloT 應用端到端的資安防護重要性不容小覷

CloT 裝置作為企業資訊應用系統一部分的, 企業應同時從 IT, OT 與 CT 多重角度來考慮整體資訊安防護策略的設計

構建基於安全的設計與全時運轉的安全防護網



構建基於安全的設計與全時運轉的安全防護網

01

裝置與網路的零信任管理

02

深層的封包內容檢測與過濾

03

安全加密的通訊管道進行外網與內網的整合

04

基於安全架構設計的的聯網產品

05

快速低門檻的安全佈署方案



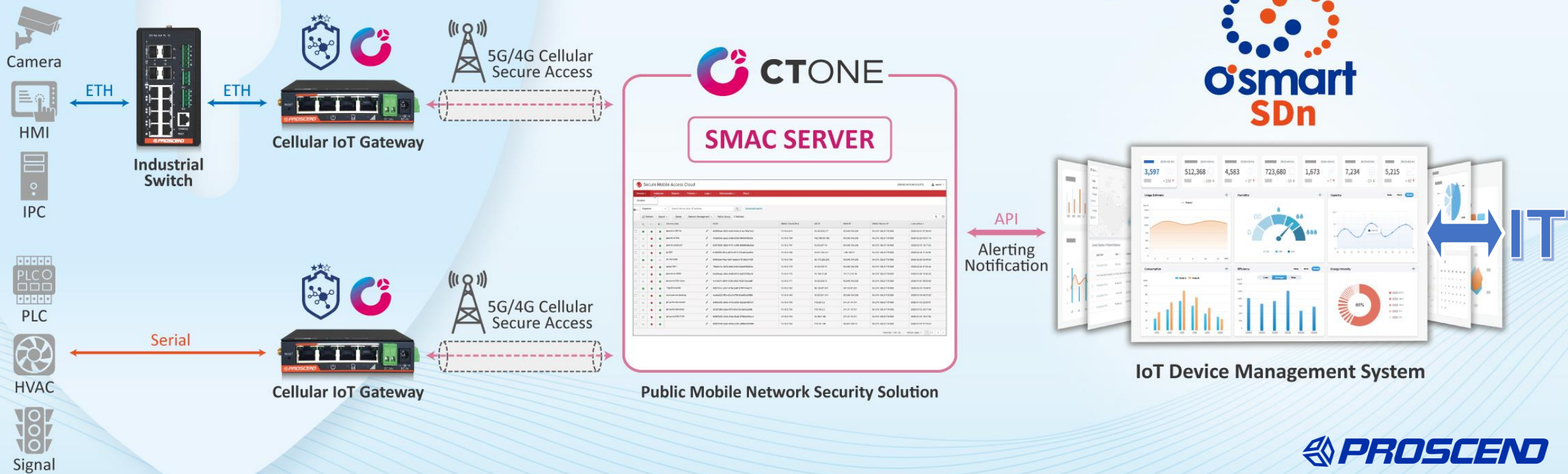
Proscend x CTOne 強固行動網路 資安防護 解決方案

安全的工業物聯網是永無止盡的任務

- Secure by Design
- IoT Cybersecurity Certification (2 Stars)
- Built-in CTOne edge agent
- Remote device control
- MQTT protocol communication

- Network Access Control List (ACL)
- Prevent network intrusion
- Stop malware downloading
- Web Threat blocking & URL filtering
- Application control

- Device cybersecurity risk management
- Inspect device cybersecurity incidents
- Filter and block abnormal device traffic
- Management capacity up to 2000 sites
- Customizable visualization dashboards



昇頻 工業物聯網智慧連結專家

為卓越而生，25年以上豐富經驗，深耕創新研發，榮獲2025台灣精品獎，
領先技術、產品，遍及60餘國，致力與生態圈夥伴共創價值鏈，共享成果。



解鎖一年一度的物聯網生態圈夥伴大會

Secure AIoT 安全未來

The logo features a blue geometric icon above the word "TEAMPROS" in large, bold letters. "TEAM" is orange and "PROS" is blue. To the right, "2025" is in blue above "TAIPEI" in blue.

主辦
單位

 **PROSCENO** 昇頻

協辦
單位

 **CTONE**

 **ShareTech**

 **VCA**
TECHNOLOGY

 **PROWAVE**
譜威科技

將於 4/21(一)開放報名!

活動日期：2025 年 5 月 7 日(三)，下午 14:20-17：30 (13:30 開始實境展示體驗互動交流)

活動地點：TICC 台北國際會議中心 4 樓貴賓廳(台北市信義區信義路五段 1 號)

主辦單位：昇頻股份有限公司

協辦單位：訊勢科技、眾至資訊、VCA Technology、譜威科技

感謝聆聽



5月7日

TICC 台北國際會議中心

Looking forward to seeing you