

CYBERSEC 2025
臺灣資安大會

4/15 - 4/17
臺北南港展覽二館

AIoT & Hardware
SECURITY ZONE

AIOT & HARDWARE SECURITY SUMMIT

從地端到雲端： 企業監控資安的全面防護策略

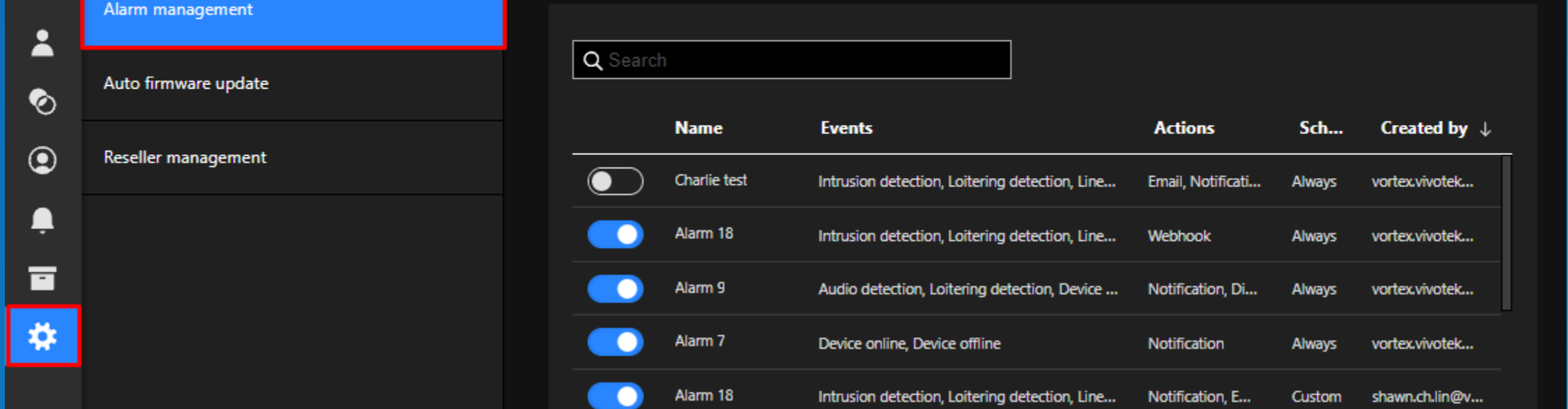
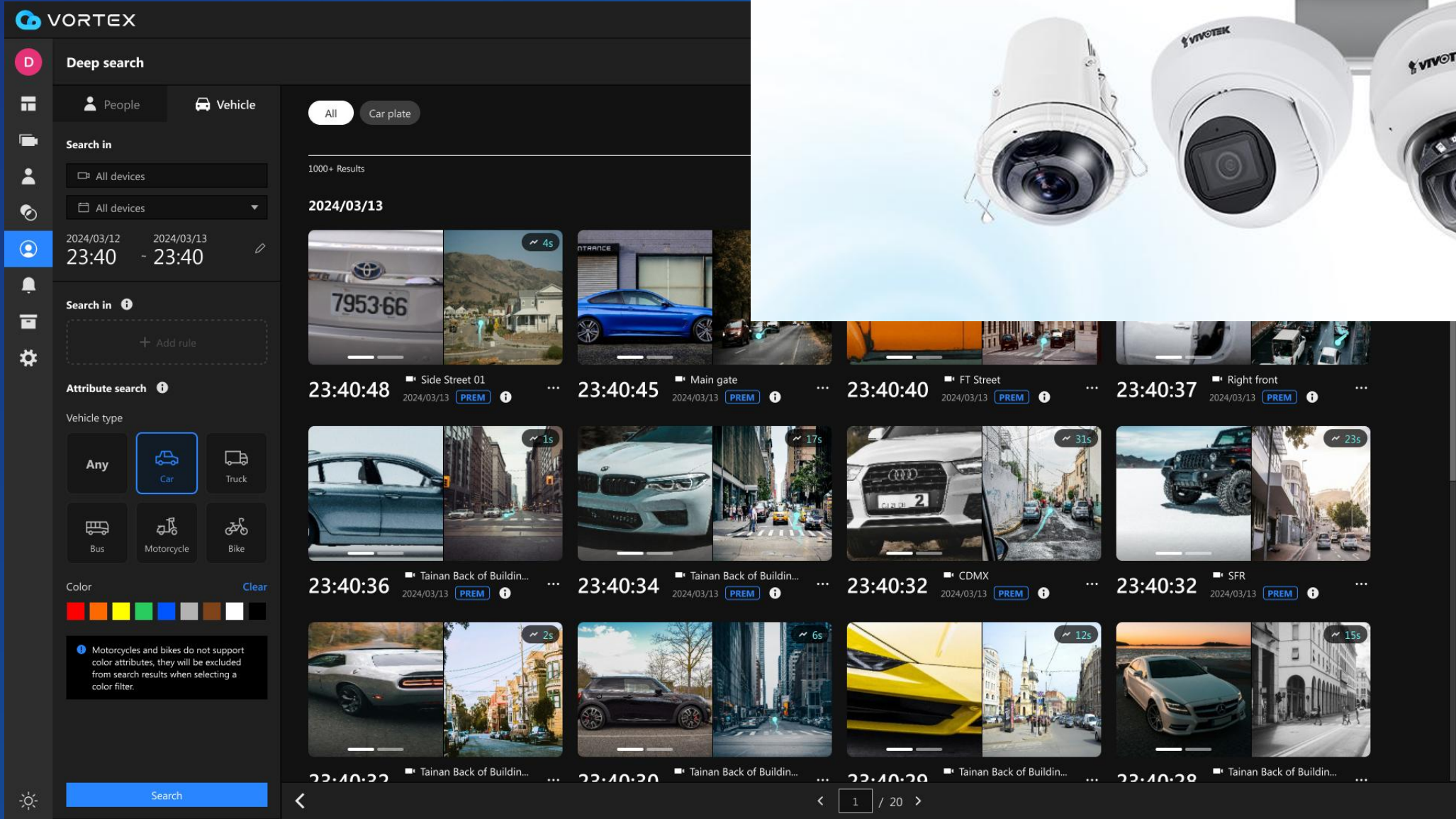
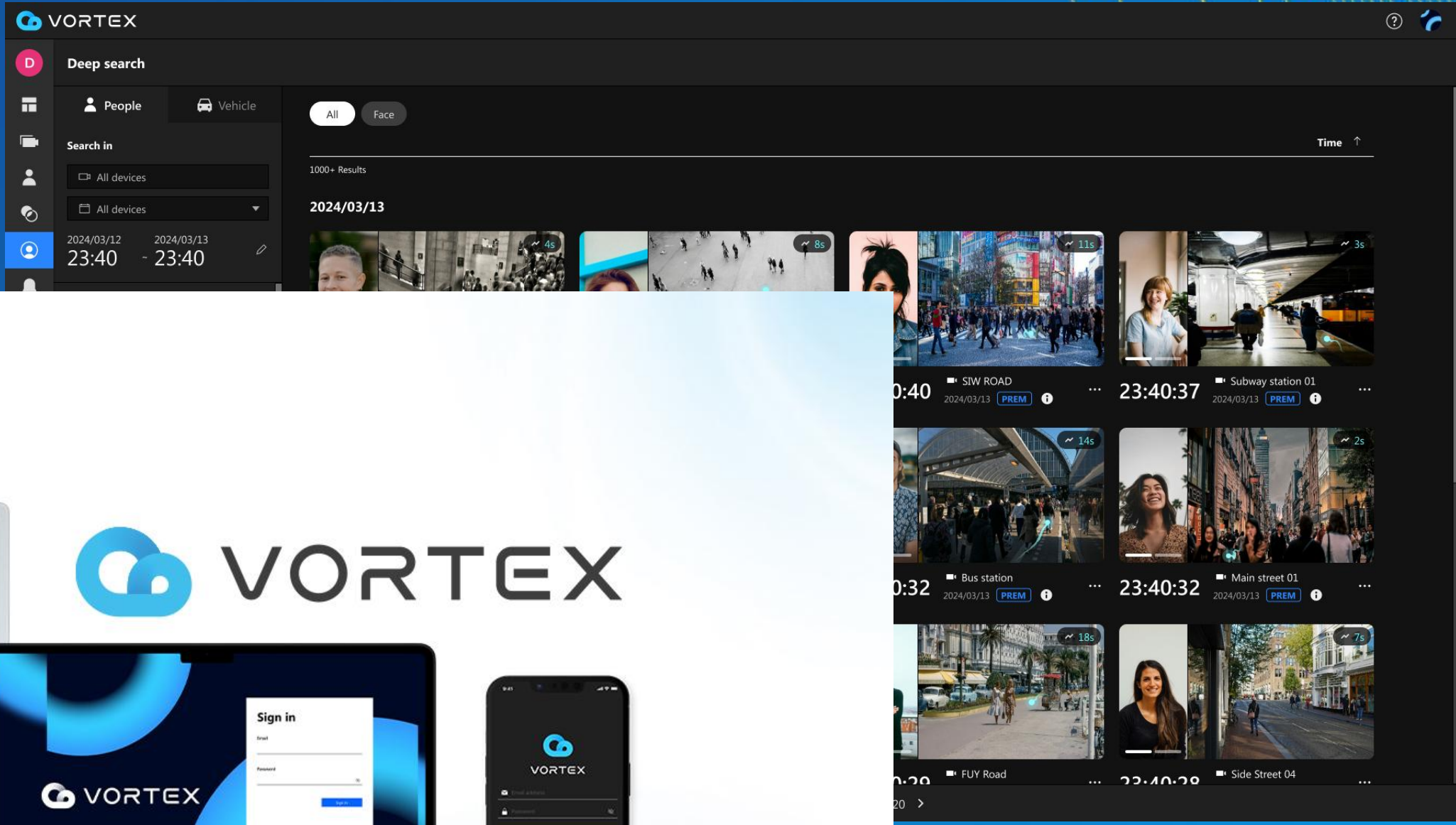
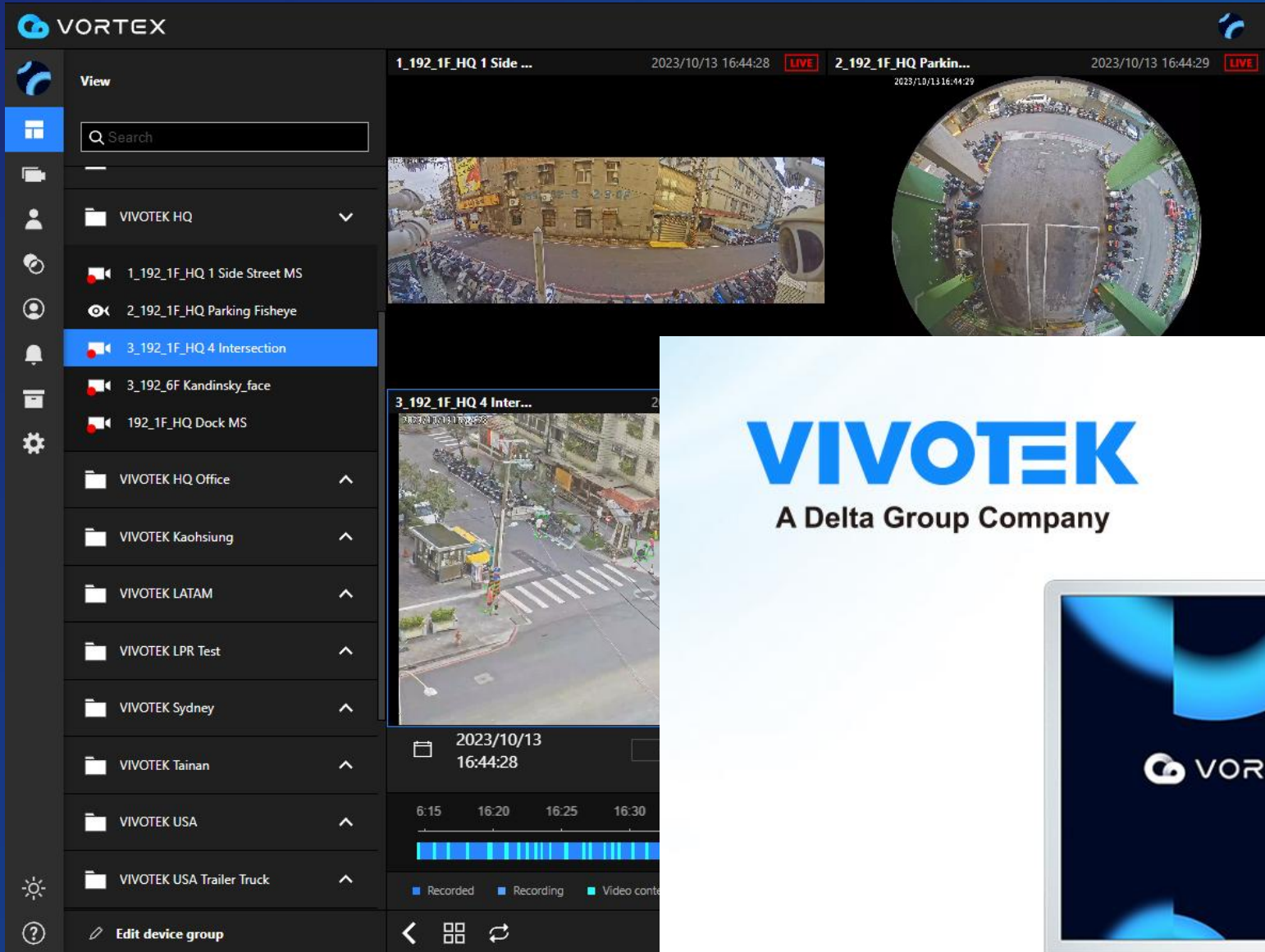
周建嘉 Hector

晶睿通訊 / 雲端服務技術一部

經理

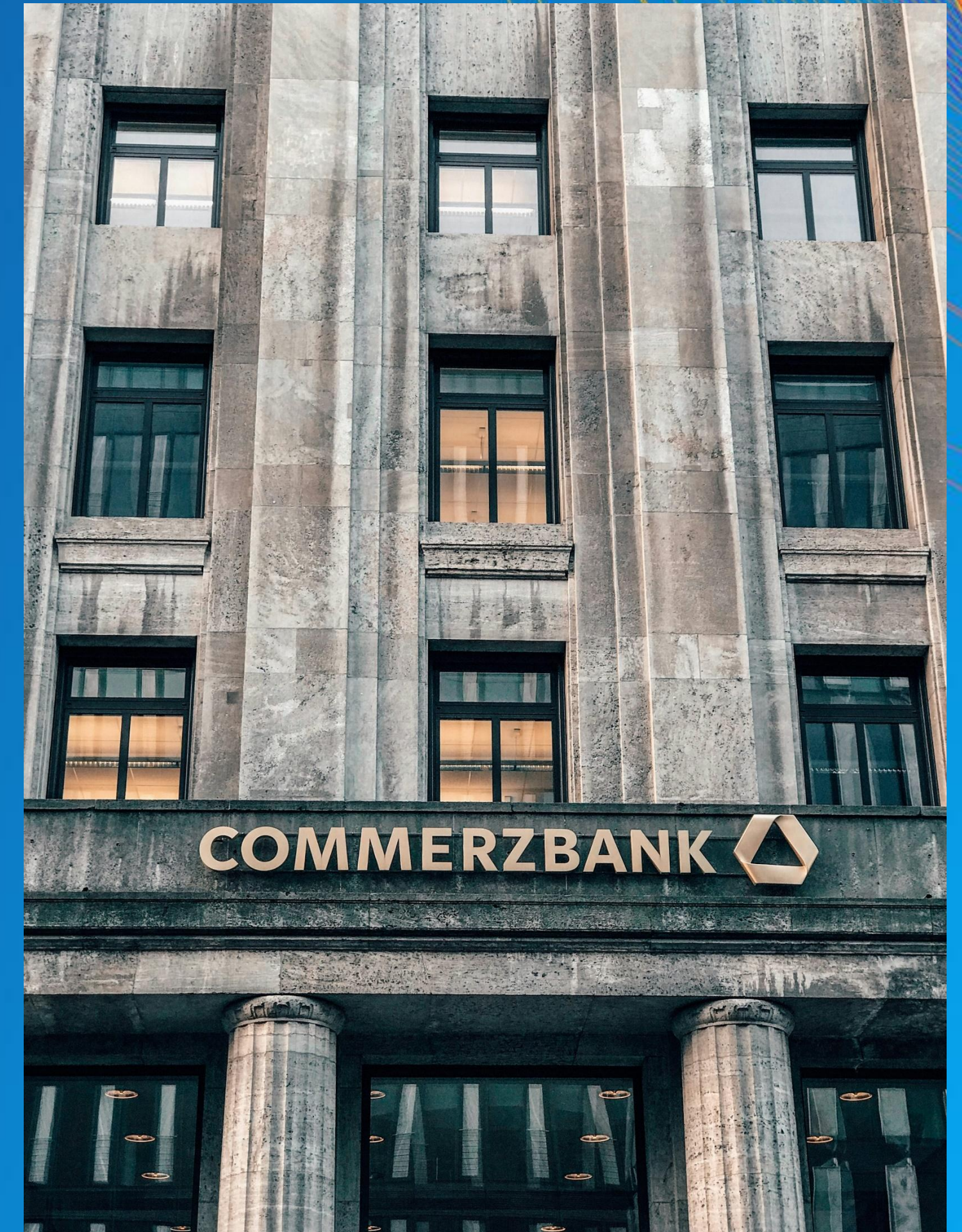
TEAM
CYBERSECURITY





它，安全嗎？
必須安全。

0. 雲地之別 – 本質上的安全性差異

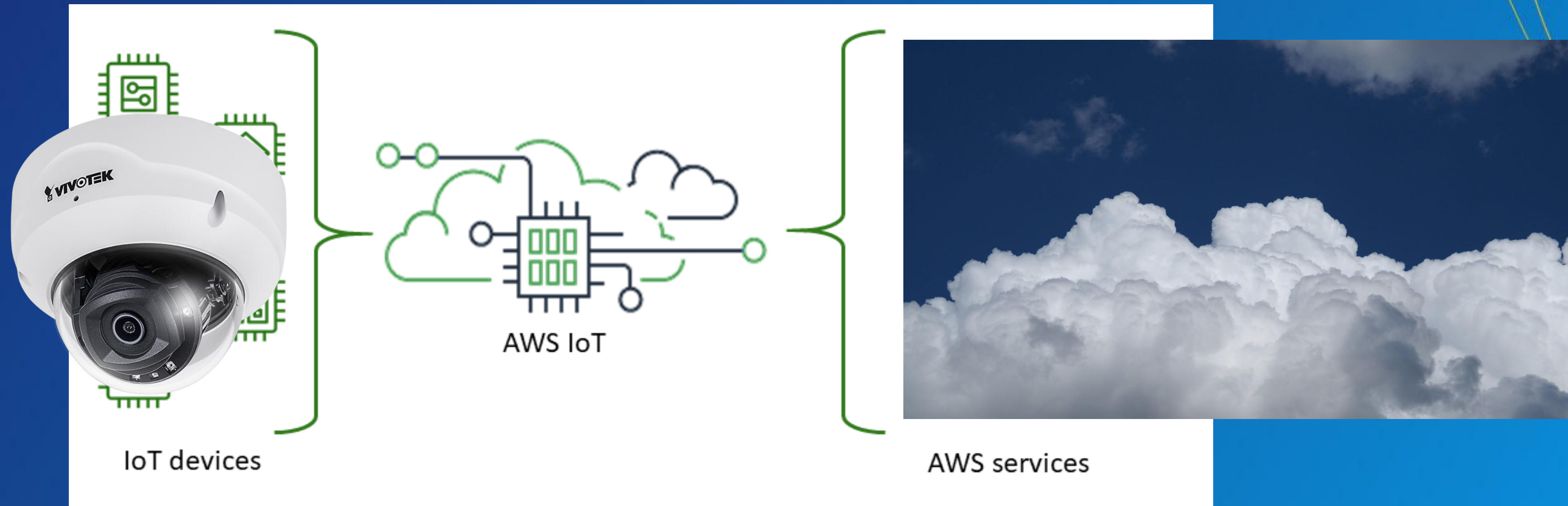


1. 從源頭安全起 – 保護前線的裝置

- Signed Firmware
 - 防止韌體被篡改
- Secure Boot
 - 防止開機過程遭惡意的程式碼侵害
- Secure Console
 - 防止遠端存取的擴權行為
- Secure SD card
 - 把卡片拔走也看不到資料
- FOTA (Firmware-Over-The-Air)
 - 資安永不過時



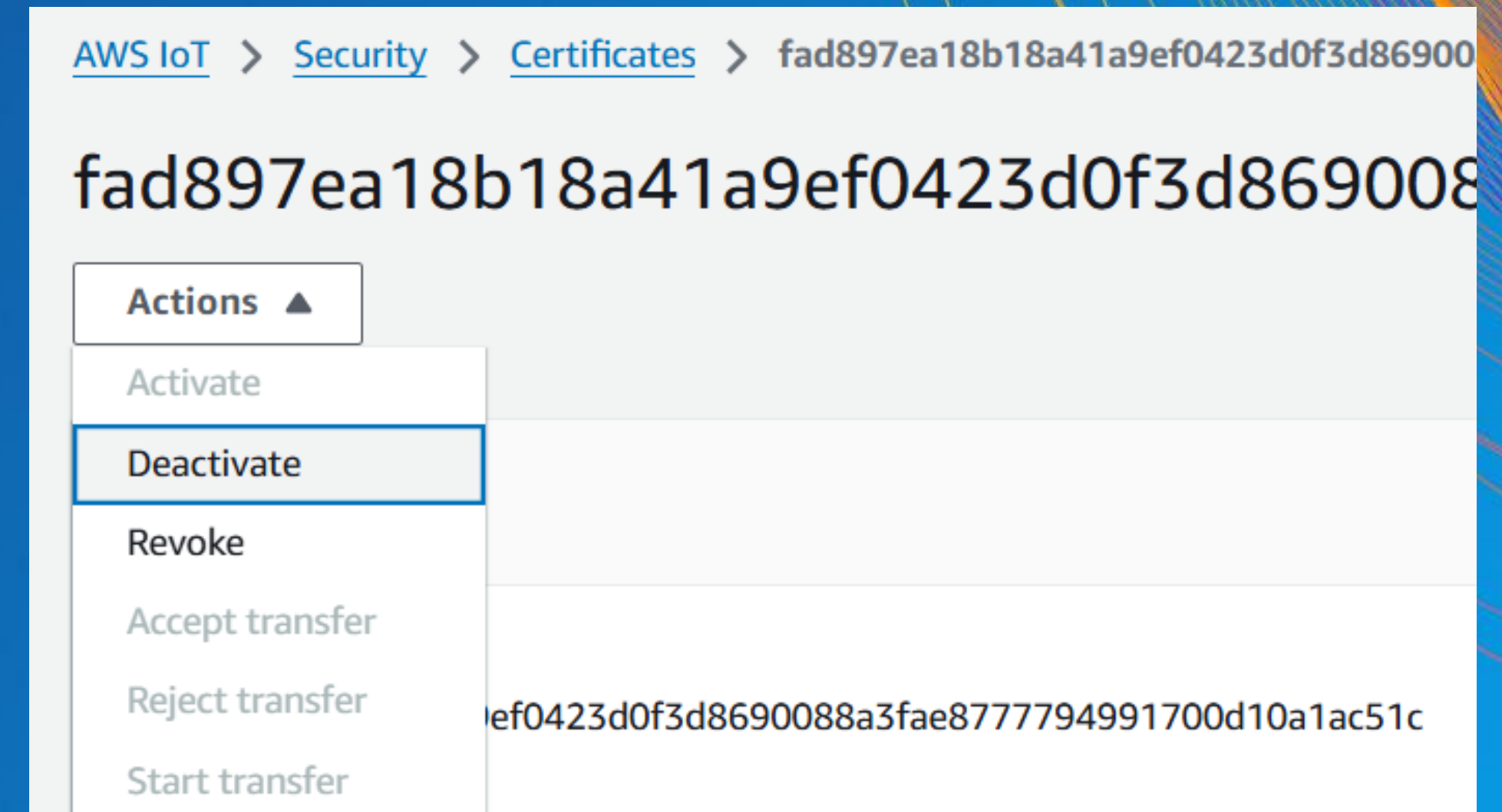
2. 安全地上雲 – Mutual TLS Authentication



- 在建立雙向安全連線的同時，也確保彼此的身分皆可信。
- 雙方都必須持有對應的 X.509 憑證及金鑰，以確認身分及訊息的有效性。
- 通過認證後所建立起來的連線乃加密傳輸。

3. 安全地活動 – IoT 裝置的管理

```
{
  "Effect": "Allow",
  "Action": [
    "iot:Publish"
  ],
  "Resource": [
    "arn:aws:iot:us-west-2:57EXAMPLE833:topic/test/dc/pubtopic",
    "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/job/*",
    "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/events/jobExecution/*",
    "arn:aws:iot:us-west-2:57EXAMPLE833:topic/$aws/things/uniqueThingName/jobs/*"
  ]
},
```



- 即便是已認證的裝置，也只能做授權範圍內 (由雲端決定) 的事情。
- 裝置若試圖進行違規操作，會立刻被雲踢下線。
- 若持續發現異常行為，將在雲端進行熔斷、停權甚至撤銷憑證。

4. 安全的存儲 – 連 VORTEX 的開發者都碰不到

- 影像是監控系統最重要的資產，VORTEX 的雲端存儲有多重防護措施：
- Access Control – 所有操作皆受存取政策的限制。
- Encrypted at Rest – 所有資料皆以加密形式儲存，就算硬碟被拔走，也不會外洩。
- 僅使用加密傳輸。
- No Public Endpoint – 即便是可公開下載的內容，也一律經 CDN 取得，無法直接碰觸存儲本身。
- Backup & Versioning – 預防災損與覆蓋。



5. 安全的串流 – 無論從攝影機或雲



- VORTEX 與攝影機之間採用 WebRTC 通訊協定：
 - End-to-End Encryption – 端對端的加密，而且是強制的。
 - Secure Signaling – 連線建立前的信令也都以加密通道進行。
 - DTLS – 防止中間人攻擊 (MITM)，避免影像遭竊聽或篡改。
- 對於播放在雲上的影像，例如雲端備份或封存等，則採用雲生態最普及的 HLS 串流協定，基於 HTTPS 進行輸出。

6. 安全的身分 – 密碼與登入

- 這真的很簡單 – 我們沒有您的密碼，所以我們沒辦法洩露您的密碼。
- VORTEX 持有的，是以密碼學領域的高強度雜湊演算法、加上亂數因子之後的計算結果，已經跟您的密碼完全不相干了。
- 該值無法被預測、也不可逆，且在系統的整個生命週期中、任何操作下都不會離開雲。
- VORTEX 也支援 MFA，及基於業界標準 SAML 2.0 的 SSO，讓您的登入更安全便捷。



We Armed to the Teeth

標準、合規、智慧監控



- ISO 27001 – 我們會保護敏感資訊、管理風險並維護安全和信任。
- FIPS 140-2 Level 2 – 我們具有良好的資訊安全及加密技術水平。
- AWS Partner & AWS Qualified Software
 - 通過 FTR (Foundational Technical Review)，表示我們的雲服務乃是基於 AWS Well-Architected 最佳實踐所建構的。
 - 我們也利用 AI 技術與行為分析，無時不刻地主動偵測系統中的潛在威脅與異常行為。

Closing Remarks



- 在數位轉型浪潮下，企業面臨的不僅是監控管理的挑戰，更是資安威脅的考驗。
- 如何在向雲遷移的過程中，運用 AI 與雲平台技術，強化資安防護，打造安全有效的監控解決方案？
- VSaaS 不是一個功能、一套軟體，而是監控時代轉折的一個樞紐。
- 如何把握住它？

感謝
各位的參與
辛苦的展場同仁
VORTEX 團隊

TEAM
CYBERSECURITY