TMRTEK

CYBERSEC 2024
OT Security Forum

工控協定的深度解析及行為學習

椰棗科技 **TMRTEK**

邱允鵬 博士 (Frank Chiu)

椰棗簡介

TMRTEK

- 新漢 (NEXCOM) 集團子公司，專注於工業控制系統 (Industrial Control System)、OT 資安解決方案。

椰棗簡介

TMRTEK

產品功能

1

即時威脅檢測與分析
(Threat Detection and Analysis)

- 即時監控
- 威脅檢測
- 深層封包檢測 (DPI)

2

網路安全監控
(Network Security Monitoring)

- 流量監控
- 入侵檢測
- 即時告警

3

資安數位儀表板
(Security Dashboard)

- 事件記錄
- 日誌保留

4

資料整合與分析
(Data Integration and Analysis)

- 資料整合
- 資料分析

5

保護設備資訊收集
(Assets Information Collection)

- 網路資訊收集
- 即時報告

6

機器學習和人工智能
(Machine Learning and AI)

- 用於異常檢測的機器學習算法
- 用於識別潛在威脅的預測分析
- 從新數據模式中持續學習

講者簡介

- 工作職責：嵌入式安全系統，包括入侵偵測、工業網路協定、工業網路行為異常分析等。
- 研發成果主要包括：
  - 機械手臂產線自動化 (RPA) 之資安防護，於 CYBERSEC 2020 台灣資安大會的「台灣資安館」展出。
  - 智慧製造產線資安保護平台，成功完成工業局科專「智慧製造資安強化」；本案更被選為科專亮點。

緣起

- 數位產業署沙崙資安服務基地
  - https://www.acwsouth.org/
  - 臺灣第一座資安演訓實證場域
- 產品檢測與攻防演訓
  - 其資安示範暨展示場域，可針對「智慧製造」、「關鍵基礎設施(石化/化工、天然氣、變電設備)」、「智慧綠能」、及「新興主題」進行產品驗測及攻防演訓。
  - 椰棗在2023年九月參加產品驗測，選擇的是天然氣場域。

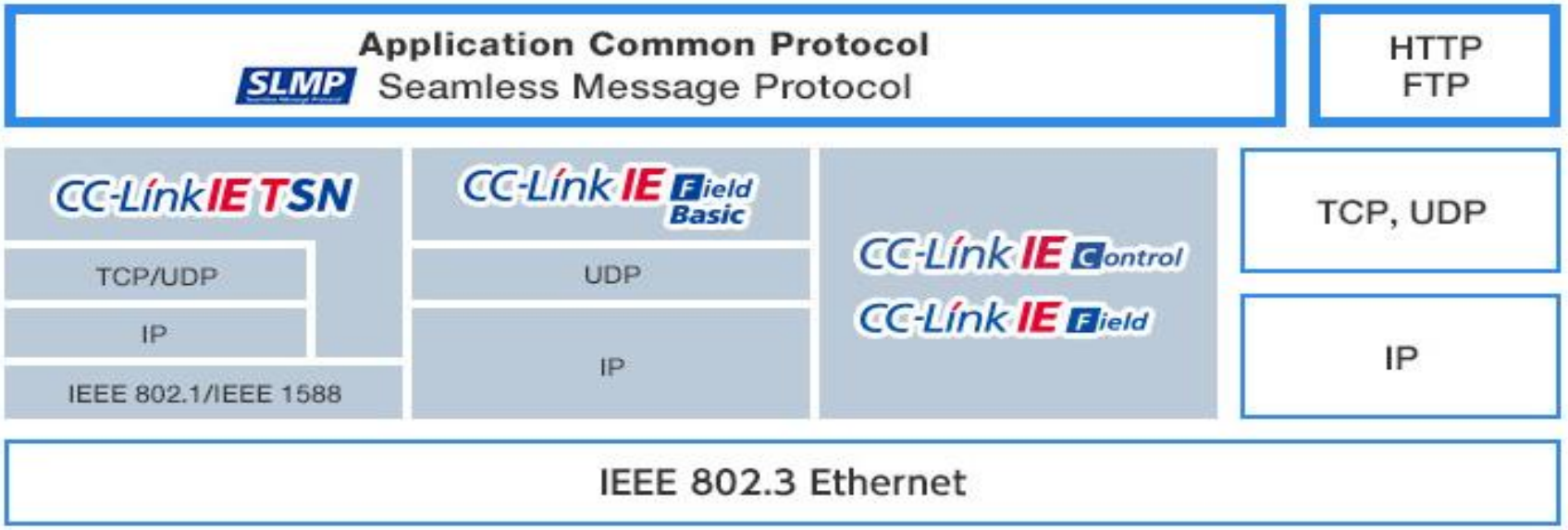
資安驗測場域架構圖

TMRTEK

Seamless Message Protocol (SLMP)

TMRTEK

- SLMP 是三菱電機（Mitsubishi Electric）2010年，制定的一種通信協議，目的實現CC-Link系列網路與乙太網路等不同設備之間的通信，且易於理解和使用且降低了開發和維護的難度。



https://am.cc-link.org/en/cclink/slmp/index

MELSEC

TMRTEK

- 三菱 MELSEC (MC) 協定也是與三菱 PLC 溝通的協定，是一種公開協定。
  - MELSEC Communication Protocol Reference Manual https://dl.mitsubishielectric.com/dl/fa/document/manual/plc/sh080008/sh080008ab.pdf
- 「部分」與 SLMP 通訊格式相容
  - 有些觀念共通
  - 但很多地方例如在封包中的位址、數值等等都不同

Melsoft Protocol

- 三菱 PLC 預設啟用之私有通訊協定
- 明文協定
- 沒有防重送機制
- 封包格式有多種版本
- 使用 PLC 不同的網路介面，封包的內容也會有些許不同。
- 此報告以三菱 iQ-R CPU 模組的 PLC 作為範例

研究方法

TMRTEK

- 硬體與軟體準備
  - 購買支援協定型號之 PLC、PLC 開發軟體、HMI 軟體
- 收集資訊
  - 獲取與 Melsoft 相關的所有官方文件、手冊和技術說明
  - 了解使用該協議的設備或系統的功能和操作方式
  - 是否有其它開發者或研究者分享關於 Melsoft 的資訊
- 通訊封包擷取
  - 執行各種命令和操作，觀察設備回應行為
  - 側錄設備與上位機 (HMI) 或其它設備間通訊之網路封包

研究方法

TMRTEK

- 工控協定分析
  - 分析側錄封包拆解封包起始暨結束標示
  - 分析側錄封包格式和結構，如資料長度、指令長度、校驗方式等
  - 嘗試識別指令與回應的類型，以及指令碼功能含義
  - 分析封包格式內容變化規律，推論參數代表狀態之意義
- 測試與驗測
  - 根據解析的協議，編寫測試程式與設備進行通訊，驗證正確性
- 分析與記錄
  - 根據分析結果，編寫協定插件，紀錄封包格式、指令碼、回應之格式等

Melsoft 封包重點欄位

TMRTEK

傳輸層以上的相對位址	說明
0	0x51（網路模組）或 0x57（CPU模組）
19~20	Payload length：負載長度
46~47	COMMAND：指令
	DEVICE NAME：資料型別
	DEVICE DATA：資料位址
	DEVICE VALUE：資料數值

Device Name List (User Device)

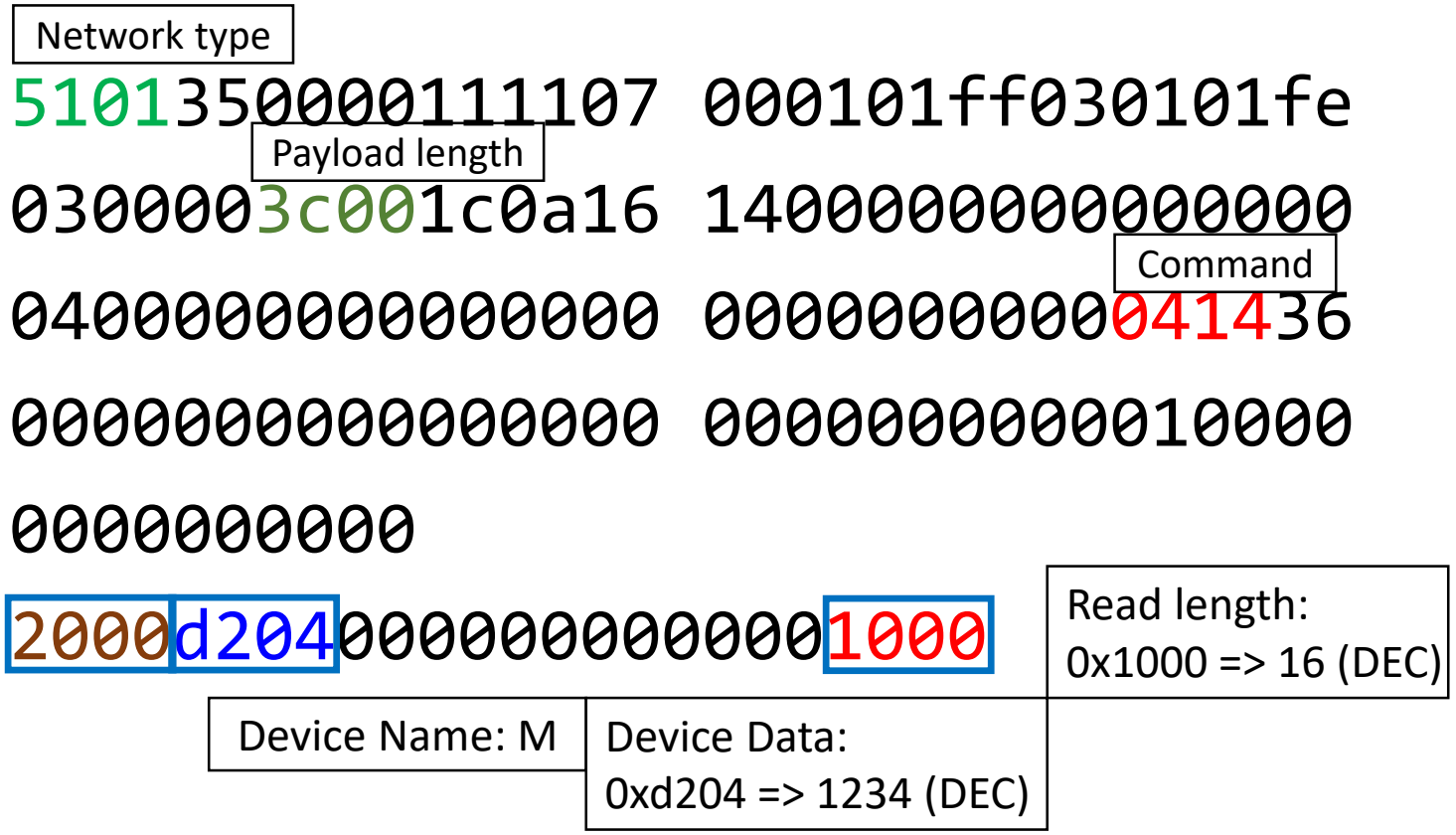
TMRTEK

- Source: MELSEC iQ-R CPU Module User's Manual (Application), p. 2.

https://www.mitsubishielectric.com/app/fa/download/search.do?kisyu=/plcr&mode=manual

Device name
Input (X)
Output (Y)
Internal relay (M)
Link relay (B)
Annunciator (F)
Link special relay (SB)
Edge relay (V)
Step relay (S)
Timer (T)
Retentive timer (ST)
Long timer (LT)
Long retentive timer (LST)
Counter (C)
Long counter (LC)
Data register (D)
Link register (W)
Link special register (SW)
Latch relay (L)

Read (0x0414)


Network type
5101350000111107 000101ff030101fe
Payload length
0300003c001c0a16 1400000000000000
Command
0400000000000000 0000000000041436
0000000000000000 0000000000010000
0000000000
2000d204000000000000001000
Read length:
0x1000 => 16 (DEC)
Device Name: M
Device Data:
0xd204 => 1234 (DEC)

Write (0x1411)

TMRTEK

Network type

5701080000111107 0000ffff030000fe

Payload length

0300004200 1c0a16 1400000000000000

Command

0400000000000000 0000000001411 09

0000000000000000 0000000000000100

0000010000

0100d204 00000000 0000000000000000

0100

Device Name: M

Device Data:
0xd204 => 1234 (DEC)

Device Value:
0x0100 => 1 (DEC)

Write (0x1411)

TMRTEK

Network type

5101080000111107 0000ffff030000fe

Payload length

0300004400 1c0a16 1400000000000000

Command

0400000000000000 0000000001411 09

0000000000000000 0000000000000001

0000010000

52000c00 00000000 0000000000000000

f24fbc00

Device Name: LT

Device Data:
0x0c00 => 12 (DEC)

Device Value:
0xf24fbc00 => 12341234 (DEC)

Write (0x1411)

TMRTEK

Network type

5101f10000111107 000101ff030113fe

Payload length

0300007800 1c0a16 1400000000000000

Command

0400000000000000 0000000001411 59

0000000000f4cc05 08b4923c8f040000

0000040000

2000 0100 00000000 0000000000000000

2000 0200 00000000 0000000000000000

2000 0300 00000000 0000000000000000

2000 0400 00000000 0000000000000000

313233343536 3738

Device Name: D

Device Data:
0x0400 => 4 (DEC)

Device Value:
"12341234" (ASCII String)

Wireshark Plugin

TMRTEK

- 有第三方開發解析 Melsoft 的 wireshark plugin
  - 但版本不同，指令及位址都不同。
    https://github.com/Zalberth/melsec_lua/blob/main/melsec.lua
- 參考並開發適合我們 PLC 最新版本韌體的 wireshark plugin

```
› Frame 528: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on inte
› Ethernet II, Src: MagicCon_c1:6a:4e (00:05:1b:c1:6a:4e), Dst: Mitsubis_d6:25:16
› Internet Protocol Version 4, Src: 192.168.200.101, Dst: 192.168.200.1
› Transmission Control Protocol, Src Port: 60304, Dst Port: 5007, Seq: 59964, Ack:
⌄ MELSOFT Protocol
    Header: 5701
    Requested Data Length: 66
  ⌄ Data Content: 1c0a161400000000000000040000000000000000000014110900000000000
      Command: 1411
      Device_Name: 0100
      Device_Name(Memory Type): Internal relay(M)
      Device_Data: d204
      Device_Data_DECShow: 1234
      Device_Value: 0100
      Device_Value_DECShow: 1
```

沙崙資安服務基地產品驗測

TMRTEK

- 椰棗在產品驗測得到100% 偵測率的高分，歸功於對協定做了深度解析。

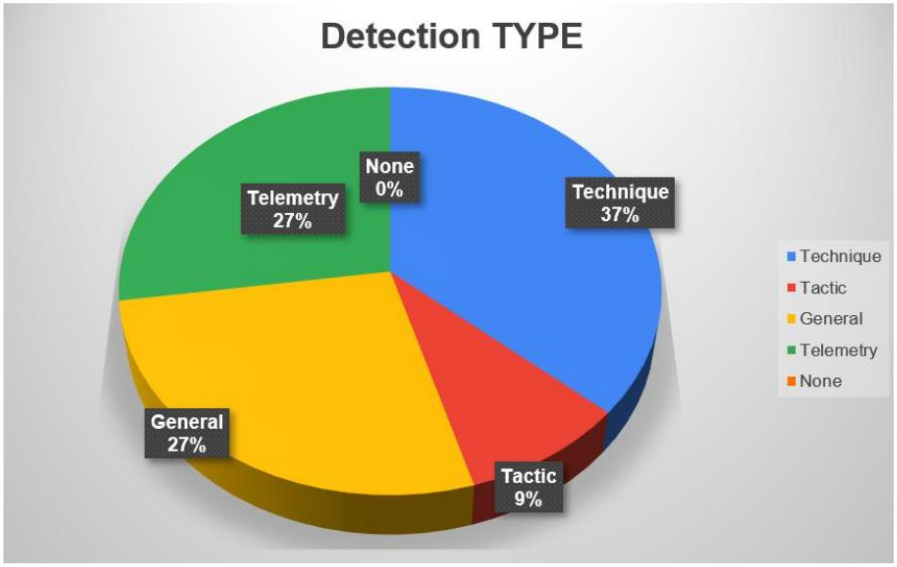
椰棗科技產品偵測率 100%

肆、 驗測結果總結

攻擊計數	偵測覆蓋率
11 steps	（100%）11 / 11 steps

類別	Technique	Tactic	General	Telemetry	None
個數	4	1	3	3	0

偵測類別結果



偵測類別分佈(圖)

AI 用在工控資安的問題闡述

- 我們希望能用人工智慧、機器學習的方式，學習到工控網路中，各種網路層面的行為變化。
- 在網路層主要的資料特徵包括連線數、連線對象數、封包大小、封包數...等等。

時序資料

TMRTEK

- 按照時間順序排列的數據集合，其中每個數據點都與特定的時間點相關聯。
- 可以分析隨著時間的推移而變化的模式、趨勢和周期性。
- 資安領域的應用
  - 日誌文件分析：資訊系統通常會生成大量的日誌文件，如登入、登出、檔案訪問等。分析這些時序日誌可以幫助檢測潛在的安全風險或異常行為。
  - 入侵檢測：通過分析系統的行為模式，可以建立正常的使用模式。當系統行為偏離正常模式時，可能是入侵或安全風險的跡象。
  - 漏洞分析：資安專業人員可以通過分析時序資料來追踪和分析系統漏洞的利用模式，以改進系統的安全性。

LSTM

- Long short-term memory 長短期記憶
- LSTM 適合於處理和預測時間序列中間隔和延遲非常長的重要事件。
- 可以根據前一段時間來得到下一個時間的預測值。
- 可以將 LSTM 比喻為一個智慧型的時間預測工具，就像一位能夠學習和理解時間序列模式的預測專家。
- LSTM 擅長處理存在順序關係並且有一定排列組合的資料。工廠產線機器的操作正符合這種特性。

LSTM 的應用

TMRTEK

- 時間序列預測：LSTM 可以被用來預測未來的數據點，透過學習歷史數據的模式，LSTM 能夠提供相對準確的預測。
- 自然語言處理：LSTM 被廣泛應用於處理時間相關的自然語言數據，如文本和語音。這可用於機器翻譯、語音識別等應用，因為 LSTM 能夠理解和捕捉語言的上下文和時間相依性。
- 行為分析：在資安領域，LSTM 可用於分析使用者或系統的行為模式，以檢測異常或可疑的活動。它可以學習正常行為，一旦檢測到異常，即可發出警報。

LSTM 與傳統統計算法比較

TMRTEK

特徵	LSTM	傳統統計分析
適用性	適用於非線性、複雜的時序模式，能夠處理長期依賴性。	適用於線性或簡單的時序模式，對於長期依賴性較不擅長。
資料量需求	對於大量資料有良好的適應性，能夠學習複雜的模式。	對資料量的需求較少，但在複雜模式上可能表現不佳。
適應性	能夠自動學習特徵，適應不同的資料模式。	需要預先選擇和設計特徵，對於資料的變化較敏感。
計算效能	在大型資料集和複雜模型下，計算成本較高。	在簡單模型和小型資料集下，計算成本相對較低。
預測能力	對於長期預測有較好的表現，能夠捕捉長期趨勢。	在短期預測上表現較好，對於長期趨勢的捕捉相對較差。
可解釋性	複雜的神經網路結構通常難以解釋，黑盒性較強。	傳統統計分析模型通常較容易解釋，能夠提供更直觀的結果。

移動平均缺點範例

TMRTEK

同類型高峰左邊的高峰會超過閥值發出警報，
右邊的高峰卻因閥值線受異常值改變不會發出警報

閥值線容易受到
異常值影響

我們將 LSTM 用於…

- 連線數異常偵測：連線數突然暴增，是很多惡意程式的特徵之一。
- 連線對象數異常預測：是否跟平常不連線的對象連線？
- 功能碼異常預測：從工控協定的功能碼層級，分析某個設備是否出現非常規的操作方式。本報告以 Modbus 為例。

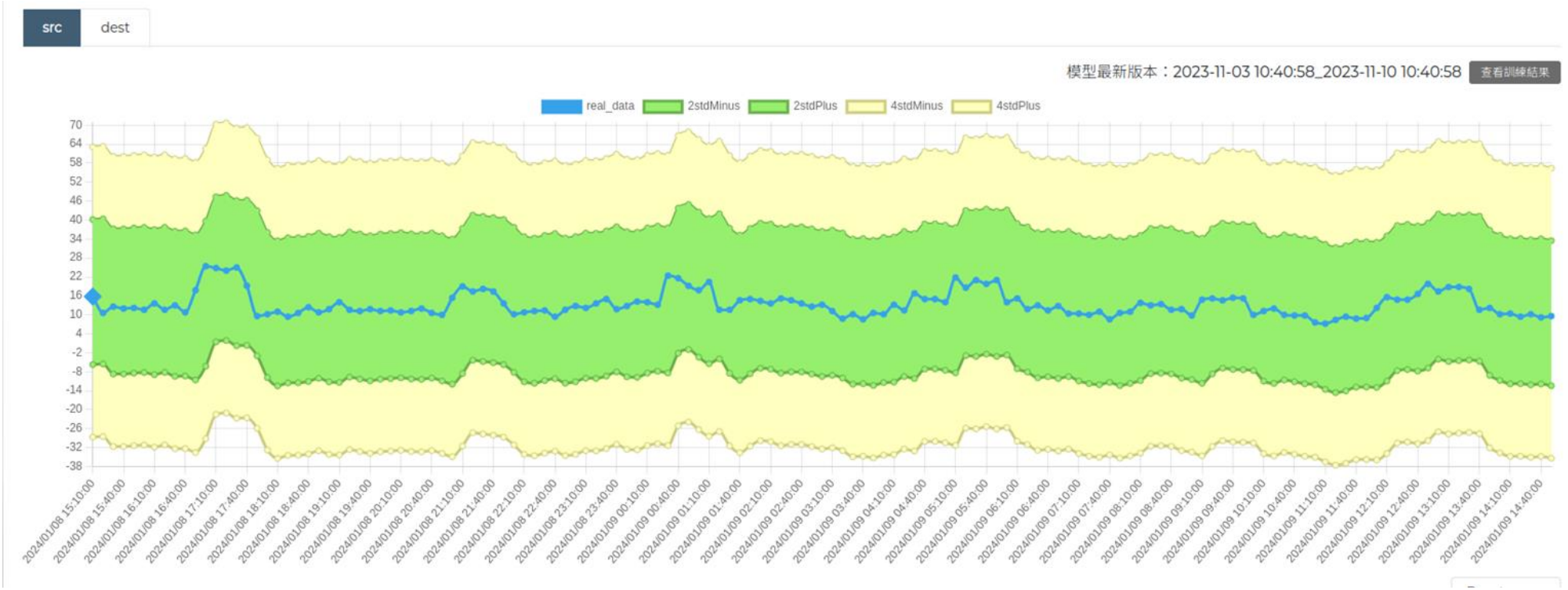
兩種連線數分析方式

TMRTEK

- 基礎：單一設備連線數分析
  - 當設備連線環境屬於比較單純時，例如 IoT 設備的電錶、溫濕度設備等，使用此功能即可。
  - 針對一個被防護設備只有一個模型。
  - 每十分鐘回報一次警告
  - 建議訓練的數據一周以上
- 進階：個別連線對連線數分析
  - 當設備連線環境屬於比較複雜時，例如一般個人電腦或伺服器等，此功能能達到更好的防護。
  - 將基礎功能的連線數資料拆分的更細緻，每一個連線對 (IP pair) 都擁有一個獨立的模型並且有分成內網、外網。外網還加上域名 (domain name) 分析。
  - 每一天回報一次警告
  - 建議訓練資料累計二個月

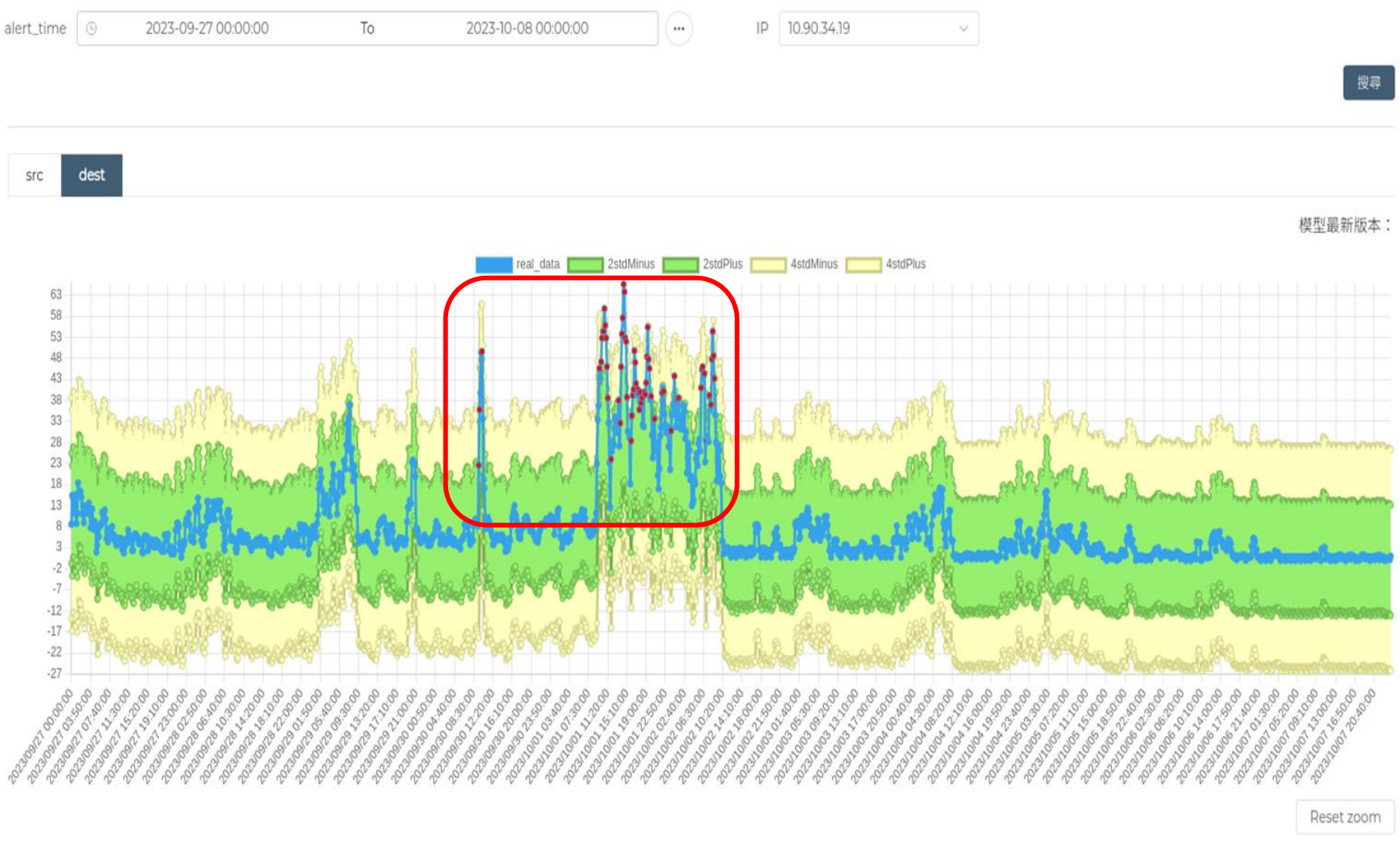
單一設備連線數分析 (destination)

單一設備連線數分析 (source)



新漢工廠資料示例

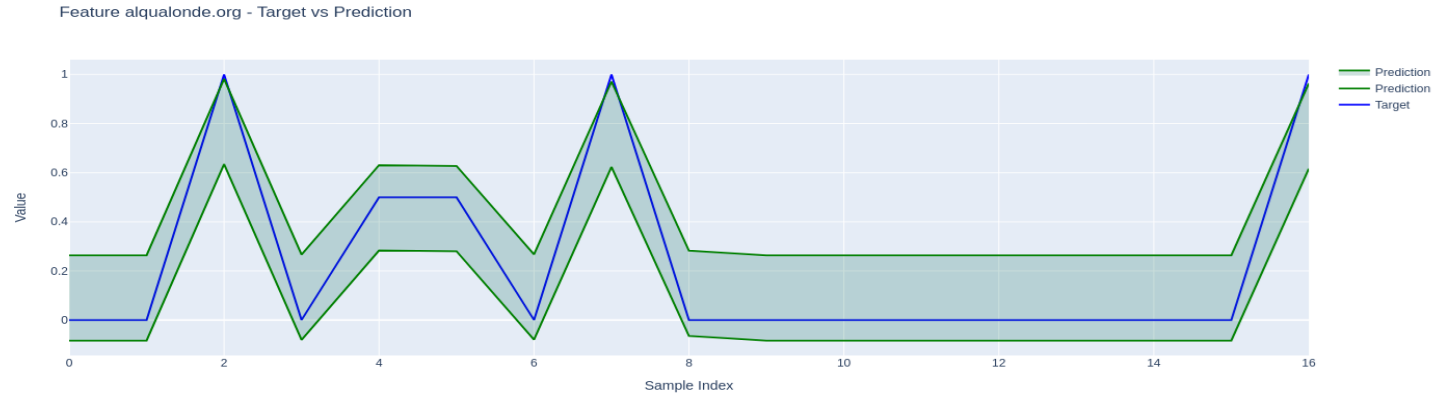
TMRTEK



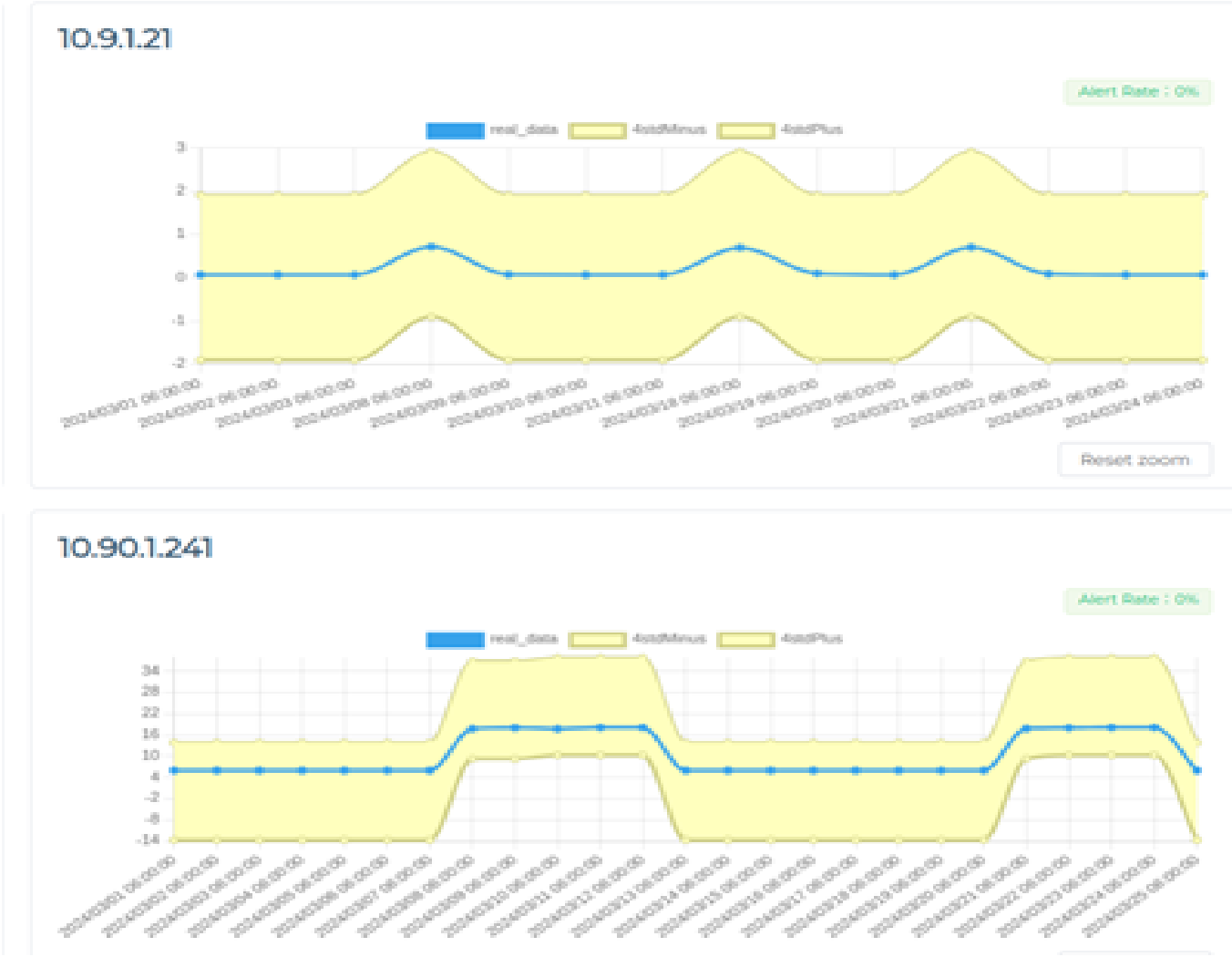
個別連線對連線數分析

- 將單一設備的連線數資料拆分的更細緻，每一個連線對 (IP pair) 都擁有一個獨立的模型並且有分成內網、外網。外網還加上域名 (domain name) 分析。
- 加上域名分析，可使跨國企業的 IP 被統整。例如 anydesk.com 的 IP address 可能分布在各國。如果只看 IP address，無法顯示出這群 IP address 其實屬於同一家跨國企業。

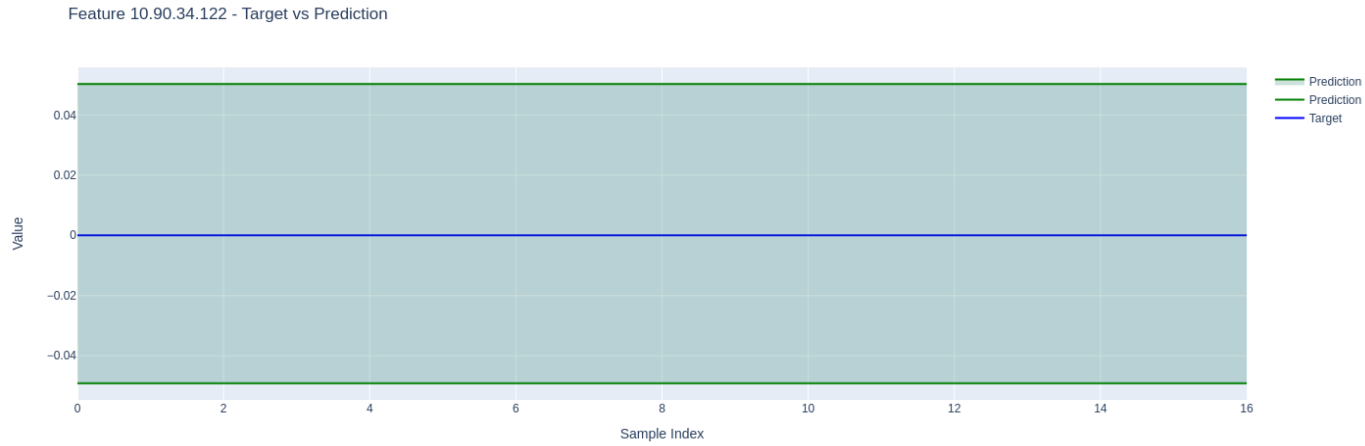
個別 IP Pair 連線數分析 (destination)(外網)

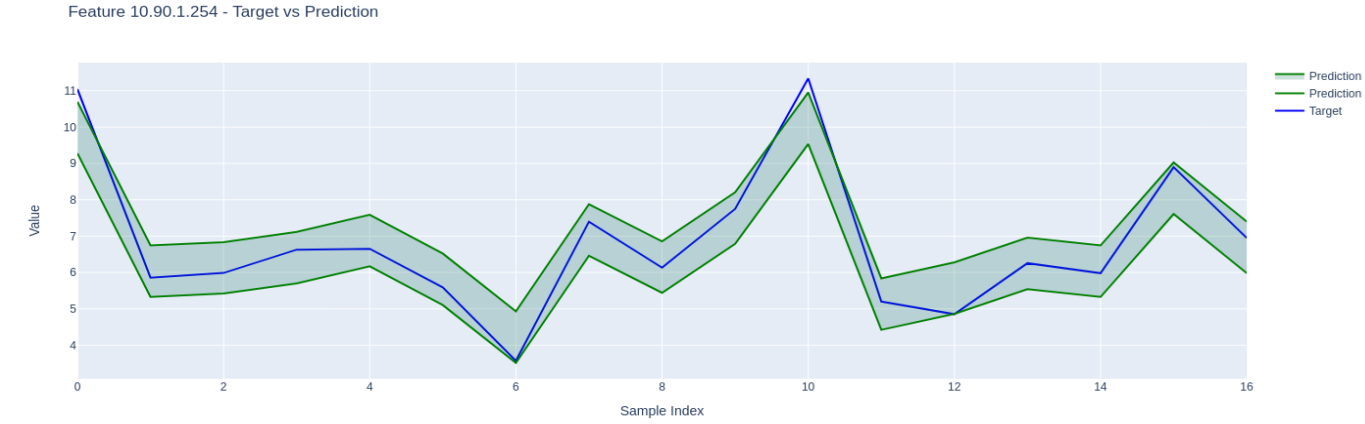


個別 IP Pair 連線數分析 (destination)(內網)

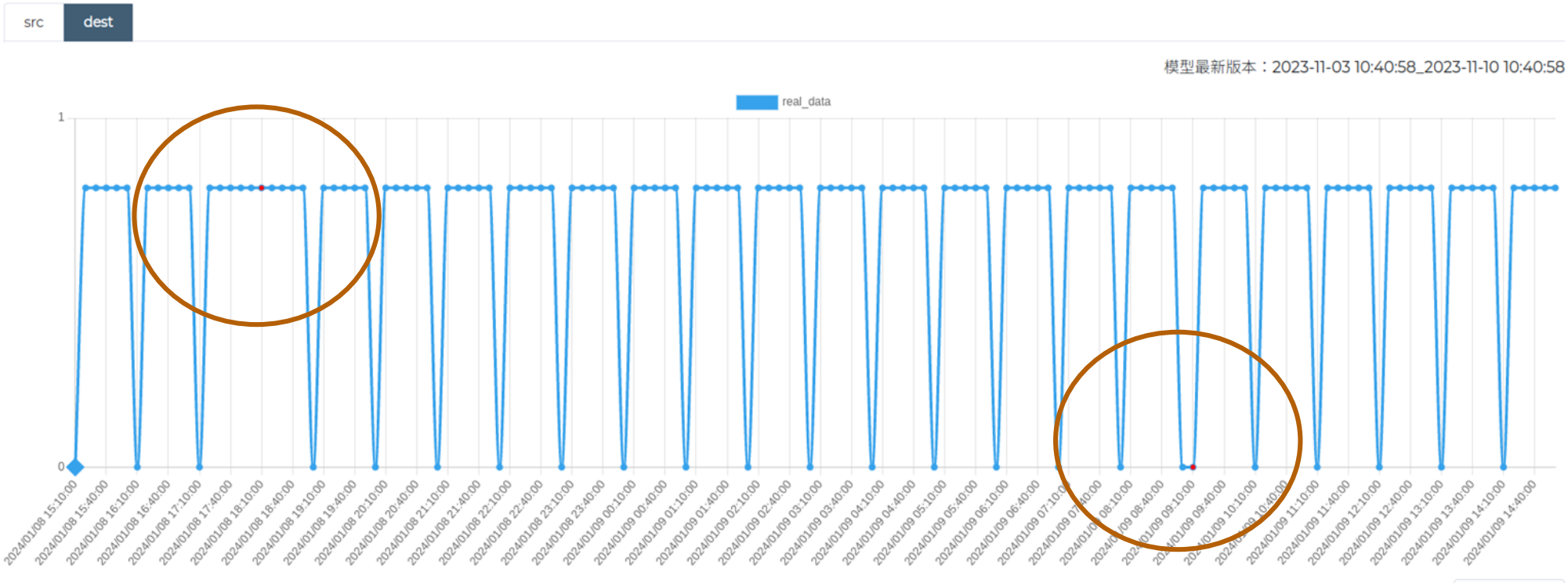


個別 IP Pair 對連線數分析 (destination)(內網)



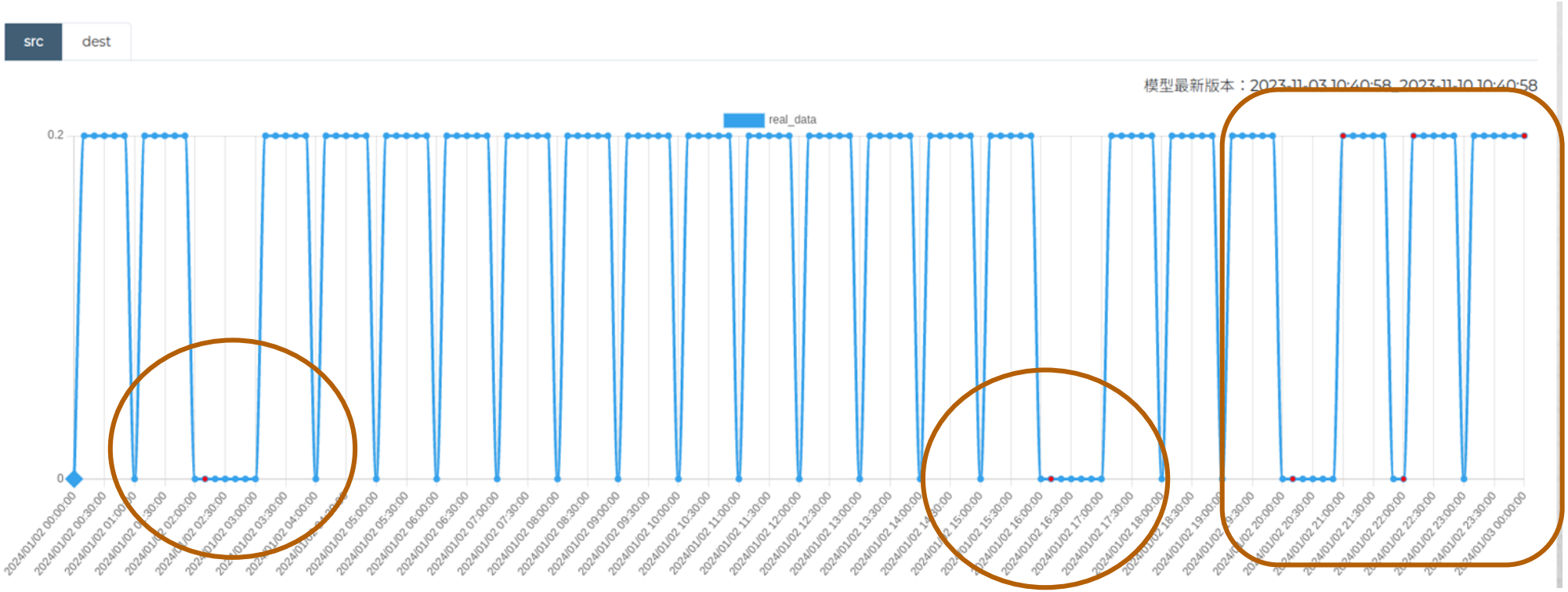


功能碼排列組合分析 (destination)



備註：因為資料有處理過，縱軸並不代表function code的實際值

功能碼排列組合分析 (source)



備註：因為資料有處理過，縱軸並不代表function code的實際值

結論

TMRTEK

- 我們分析了三菱的 Melsoft 通訊協定，可以抽出命令、資料型別及位置、以及資料數據本身。
  - 藉由分析出各資料欄位，可以對網路行為做細緻的分析。
- 我們用 LSTM 模型做網路行為的分析，包括以下幾種：
  - 基礎：單一設備連線數分析
  - 進階：個別連線對連線數分析
  - 功能碼異常預測：從工控協定的功能碼分析設備行為

椰棗聯絡方式

- 展覽攤位：四樓台灣資安館 T09
- 椰棗網址：https://www.tmrtek.com/

- 若想進一步了解，歡迎填寫諮詢問卷：