



分散式智慧校園路燈蜜罐系統

DISTRIBUTED SMART CAMPUS STREETLIGHT HONEYPOT SYSTEM

指導教授：陳奇業、李南逸教授 專題成員：周昀軒

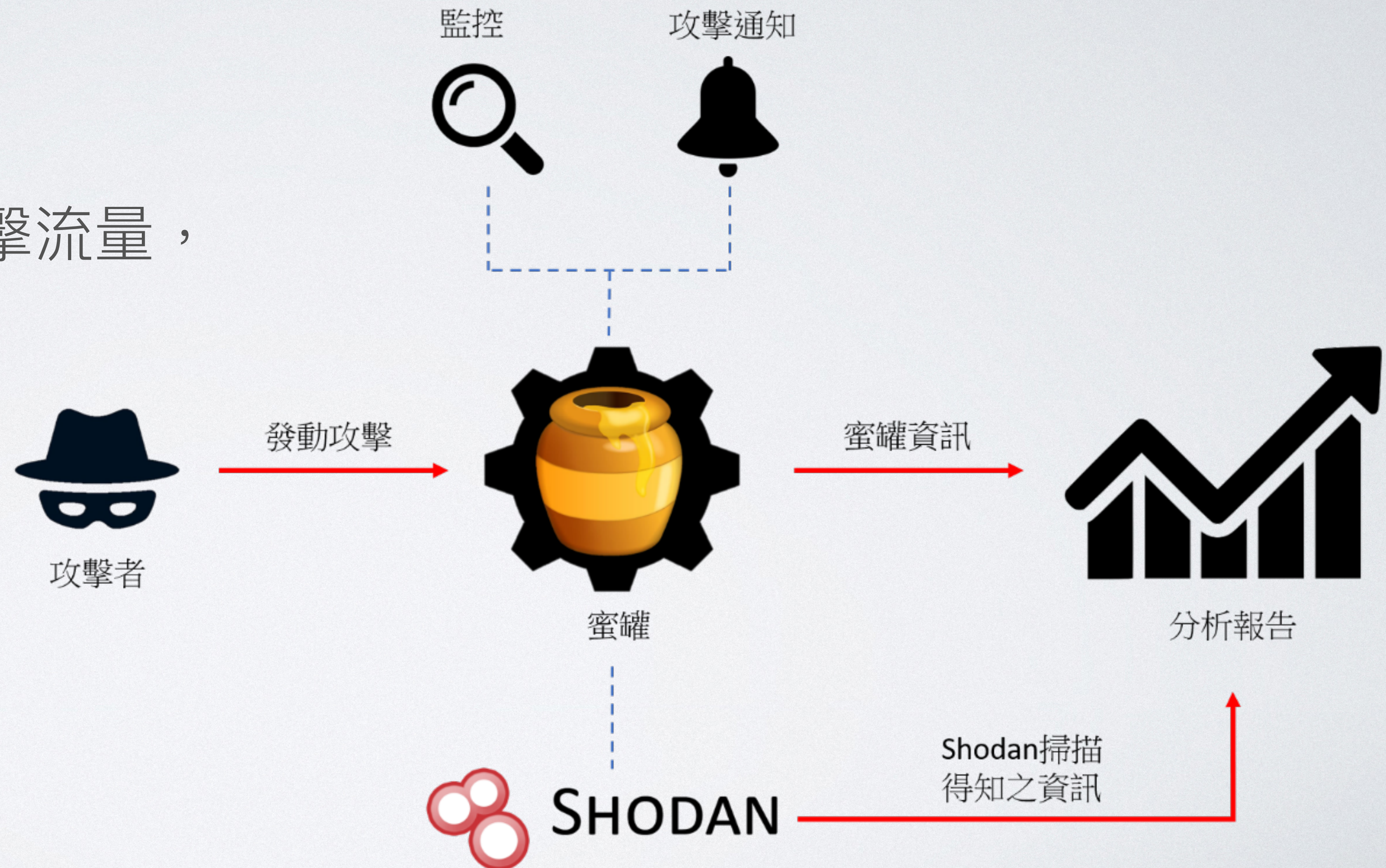
大綱

1. 專題動機
2. 架構設計
3. 成果展示
4. 結論與未來展望



蜜罐

- 誘導駭客攻擊進而搜集攻擊流量，提升防禦系統



專題動機

在 ICS 場域中，PLC、感測設備、通訊協定與後端服務之間通常存在多節點互動。然而現有許多 Honeypot 仍多著重於單一設備或單一通訊服務，並且只能部署於單一環境，用以吸引攻擊者並蒐集攻擊流量



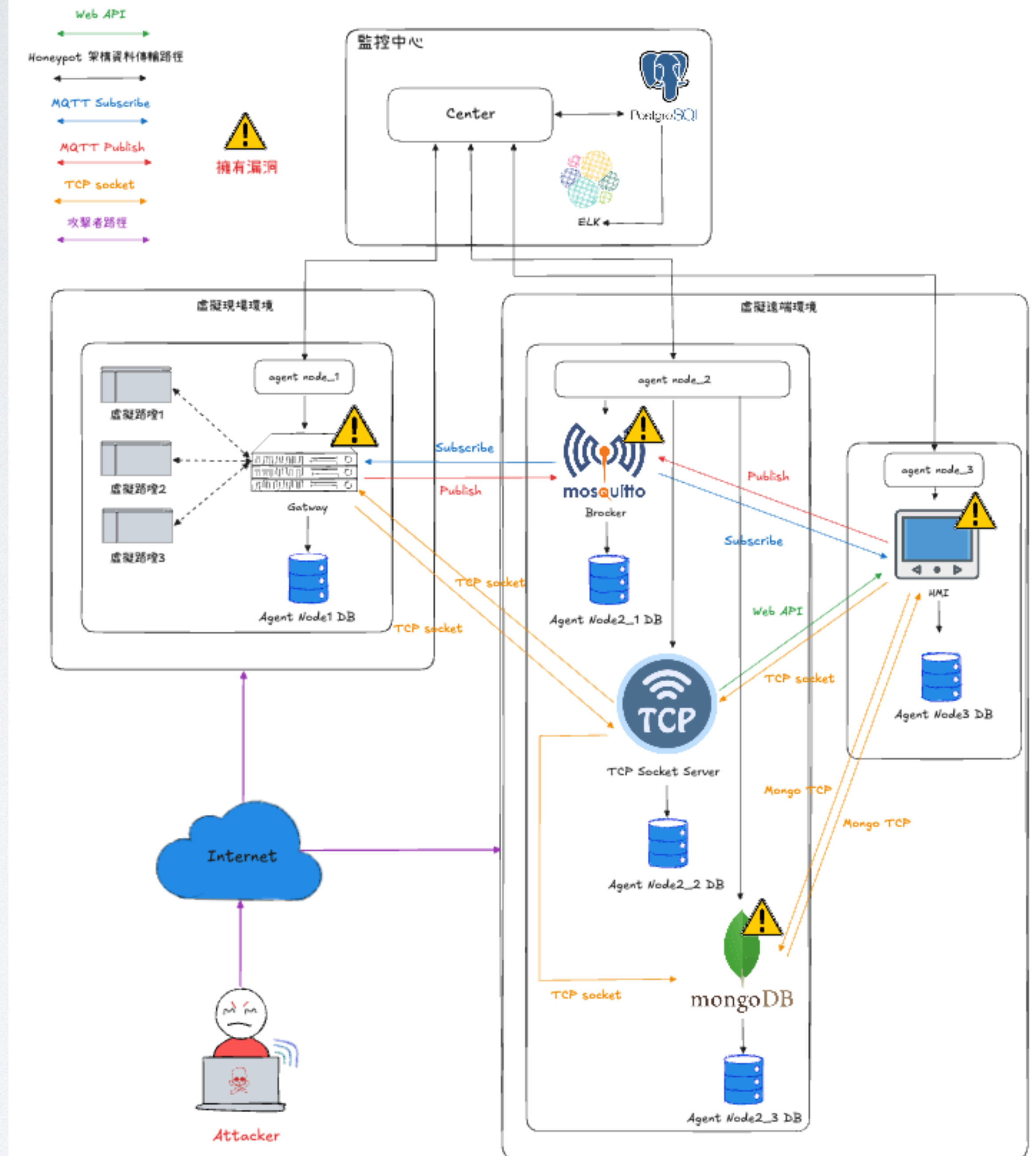
T-pot



Conpot

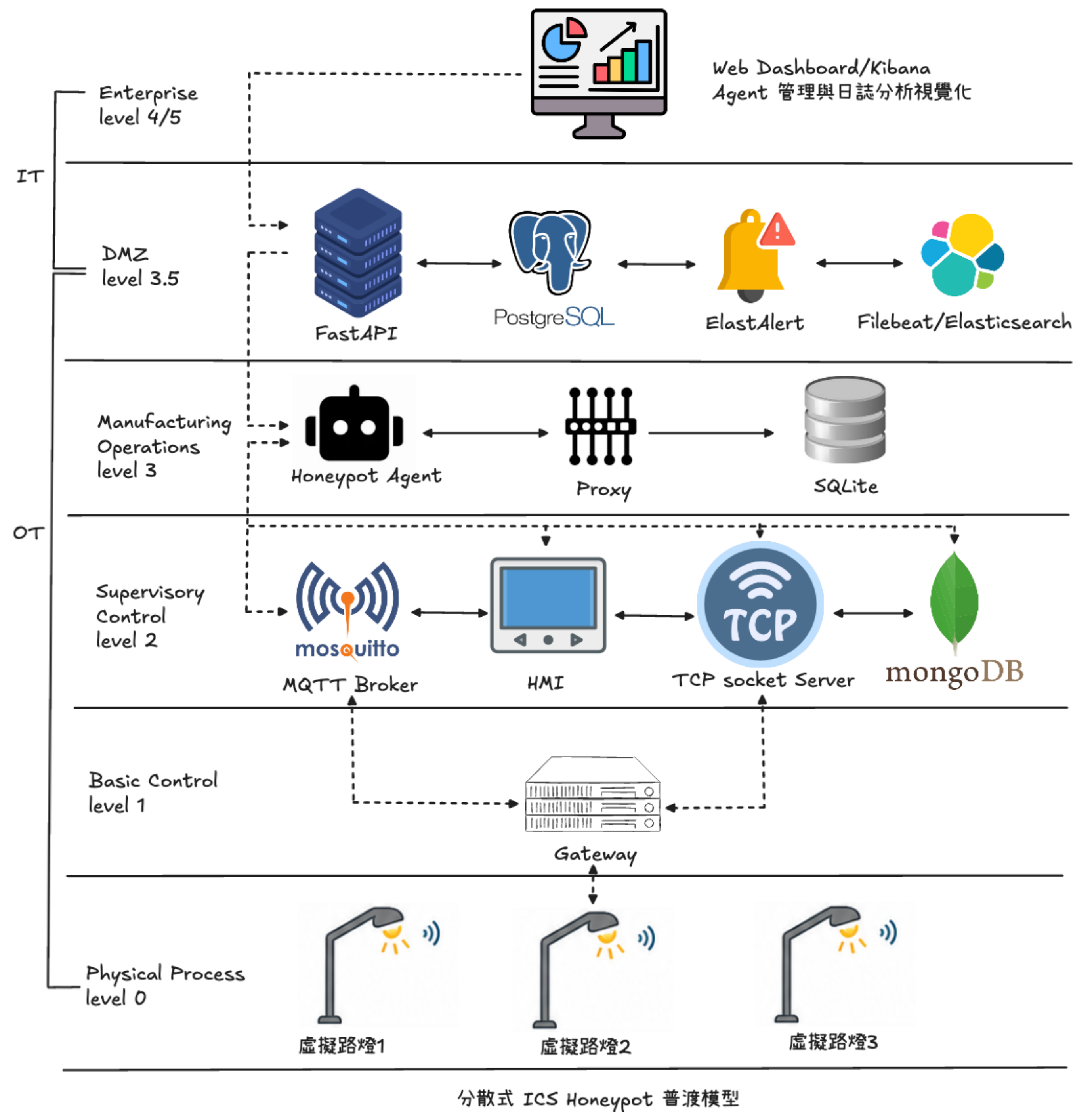
專題簡介

- 可在不同環境部署多個 Honeypot Agent，並由中央 Server 統一管理服務部署、狀態監控與攻擊流量分析。
- 模擬服務設計漏洞點引誘駭客入侵
- 以成功大學智慧路燈系統為情境，建構路燈系統架構與主要通訊流程，使蜜罐行為更貼近真實環境。



智慧路燈 Honeypot 模擬系統架構

系統架構



成果展示

成大虛擬路燈展示畫面



國立成功大學
National Cheng Kung University



主頁

路燈控制

成大校區路燈系統
使用者 admin

搜尋 MAC、校區、座標

● 已連線 登出

● 控制器正常 206

● 控制器異常 0

● 控制器離線 160

● 控制器回報 206

● 地圖標點 338

● 陣

街道圖 深色

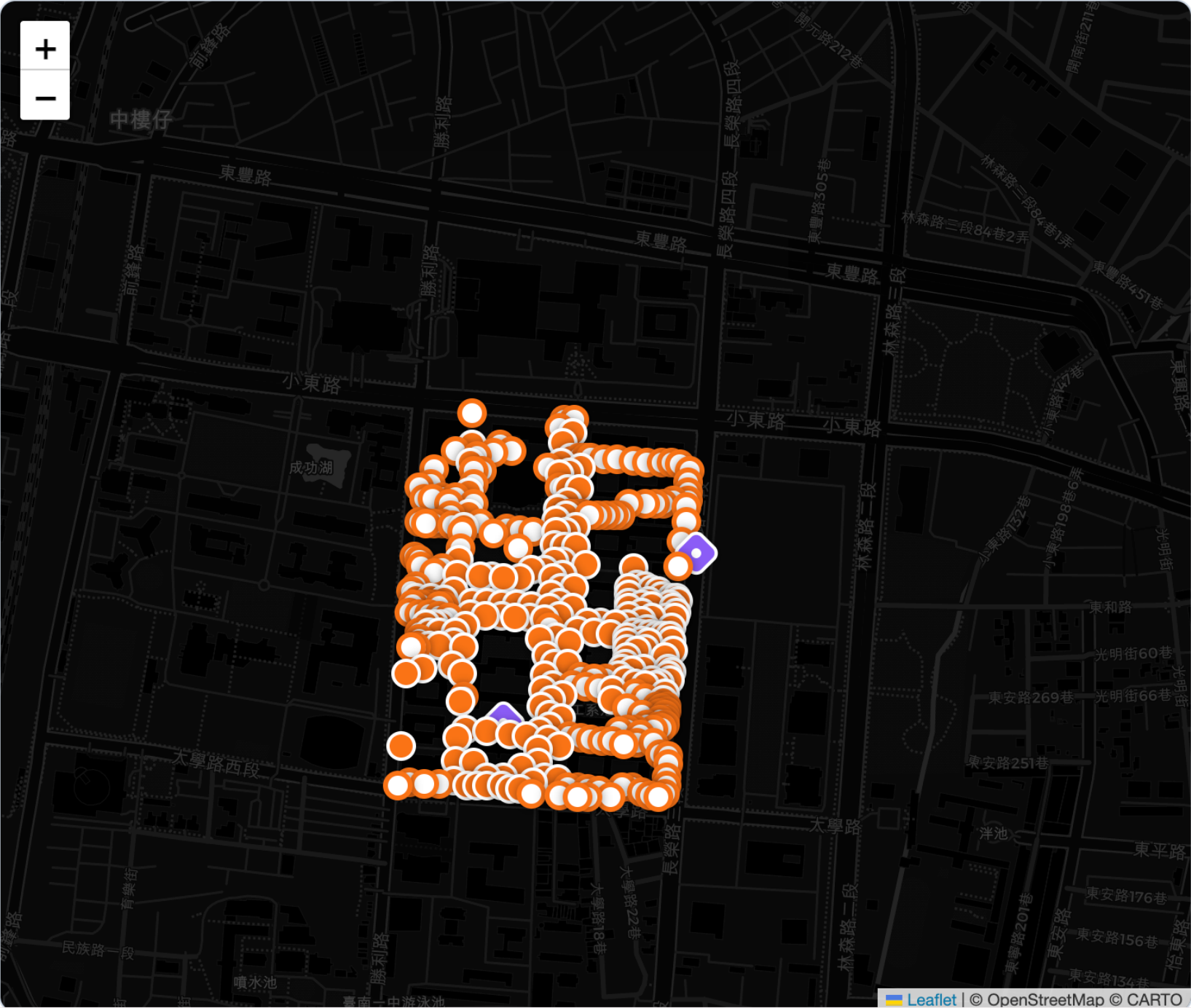
成大校區路燈地圖

校區篩選

338 / 338 個控制器標點 · 2 個閘道器 · 366 盞路燈 · 匯出 2026-06-09T08:51:45.881Z

+

-



成功校區 · 1 盞

座標: 22.998139, 120.220855

MAC: B827EB863F

最後回報: 2026-06-09T05:07:33.592983+08:00

功耗 350 W

亮度 100%

電壓 133 V

RSSI 77

控制 MAC

B827EB863F

已送出 SPW -> B827EB863F

SPW 單盞控

SGW 群控

SRA 立即回報

自訂 Hex 指令

020B523C610553B801323F

發送

成果展示

收到登入HMI 蜜罐請求

與使用socket 發送消息

140.116.247.244

Section 1, Minsheng Road, Taiwan · 1 protocol

Overview

Alerts38

Packets300

"severity": 1,

"source": "elastalert",

"attacker_ip": "140.116.247.244",

"node_id": "node_3",

"protocol": "http",

HighHTTP socket or command submission6/10/2026, 21:49:48

SID 7000303Category Potentially Bad TrafficProto HTTPDest 127.0.0.1:8080Node node_3ElastAlert

{

"signature": "HTTP socket or command submission",

"signature_id": 7000303,

"category": "Potentially Bad Traffic",

"severity": 1,

"source": "elastalert",

"attacker_ip": "140.116.247.244",

"node_id": "node_3",

"protocol": "http",

}

HighHTTP successful login to honeypot web UI6/10/2026, 21:49:35

SID 7000302Category Successful Administrator Privilege GainProto HTTPDest 127.0.0.1:8080Node node_3ElastAlert

{

"signature": "HTTP successful login to honeypot web UI",

"signature_id": 7000302,

"category": "Successful Administrator Privilege Gain",

"severity": 1,

"source": "elastalert",

"attacker_ip": "140.116.247.244",

"node_id": "node_3",

"protocol": "http",

}

成果展示

收到針對路燈進行攻擊的警報

125.228.248.22

Banqiao Road, Taiwan · 3 protocols

Overview

Alerts5

Packets259

HighTCP/custom possible buffer overflow probe

5/26/2026, 12:18:22

SID7000602

CategoryAttempted Denial of Service

ProtoCUSTOM

Dest127.0.0.1:15566

Node node_1

ElastAlert

"signature": "TCP/custom possible buffer overflow probe",

"signature_id": 7000602,

"category": "Attempted Denial of Service",

"severity": 1,

"source": "elastalert",

"attacker_ip": "125.228.248.22",

"node_id": "node_1",

"protocol": "custom",

"timestamp": "2026-05-26T04:18:22.294Z",

"-- id": "125.228.248.22"

專題貢獻

- 此架構蜜罐與蜜罐之間可以互相互動，形成**蜜網**
- 分離式架構，Server 與 蜜罐可在不同台機器上
- 高度彈性，可以架自己做的 HMI 或者模擬 PLC

未來展望

- 擴充更多 ICS 協定，如 S7、DNP3、BACnet
- 加入威脅情資搜集功能
- 加入機器學習偵測



THANKS