1.

架構:

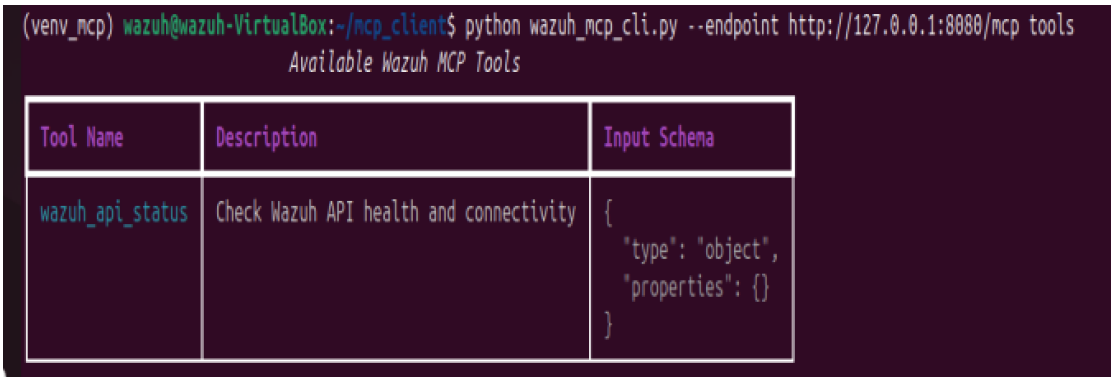
Wazuh Agent → Wazuh Manager → Wazuh MCP Server → MCP CLI

↓

OpenAI LLM

這張圖是 Mcp-WAZUH 連上畫面

這是問 wazuh 健不健康的工具



後來我又增加工具，是可以問有沒有警告的

```
(venv_mcp) wazuh@wazuh-VirtualBox:~/mcp_client$ python wazuh_mcp_cli.py --endpoint http://127.0.0.1:8090/mcp
 tools
                        Available Wazuh MCP Tools
```

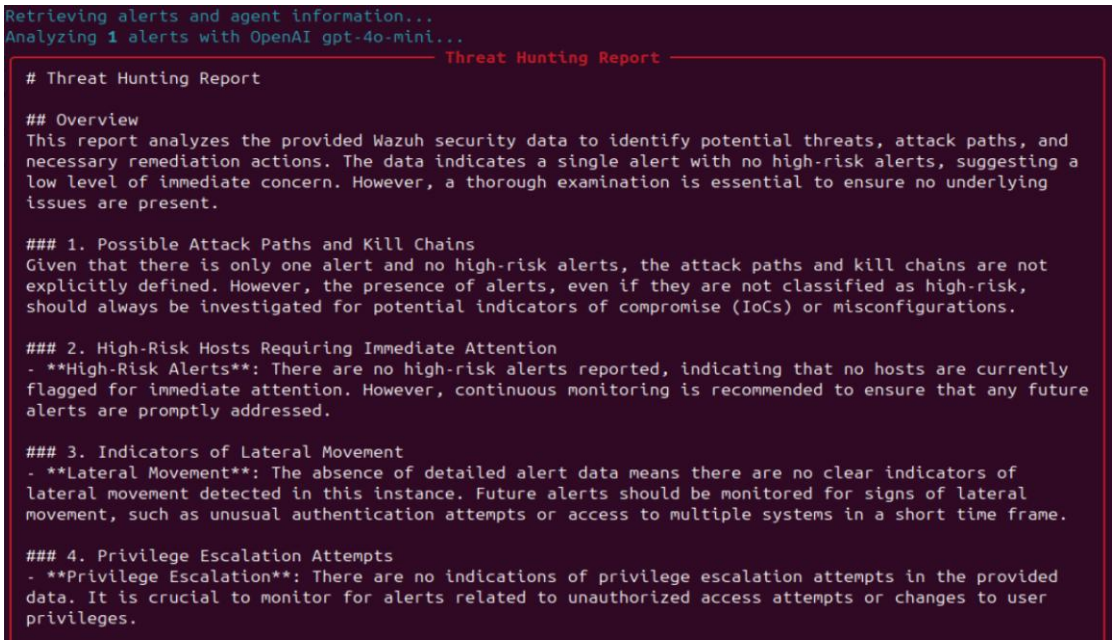
Tool Name	Description	Input Schema
wazuh_api_status	Check Wazuh API health and connectivity	{ "type": "object", "properties": {} }
get_wazuh_alert_summary	Get recent high severity alerts	{ "type": "object", "properties": { "limit": { "type": "integer", "default": 5 } } }

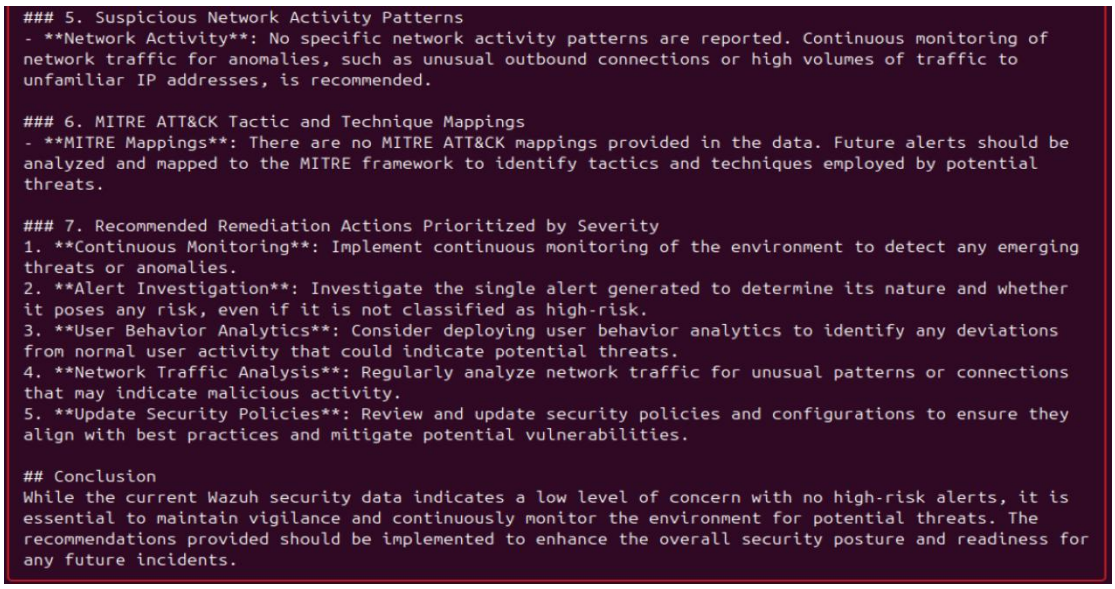
這是我原本用指令問(給我最近 24 小時的高嚴重度告警摘要，列出 top 5) ，所產生的報告

```
(venv_mcp) wazuh@wazuh-VirtualBox:~/mcp_client$  python wazuh_mcp_cli.py \

  --endpoint http://127.0.0.1:8090/mcp \

  hunt --limit 5
usage: wazuh_mcp_cli.py [-h] [--endpoint ENDPOINT] {init,tools,alerts,test,hunt} ...

Wazuh MCP CLI - Cybersecurity and Threat Hunting Tool

positional arguments:
  {init,tools,alerts,test,hunt}
                        Available commands
    init                Initialize MCP session
    tools               List all available Wazuh MCP tools
    alerts              Retrieve Wazuh alerts
    test                Run automated test routines
    hunt                Automated threat hunting using OpenAI LLM

options:
  -h, --help            show this help message and exit
  --endpoint ENDPOINT   MCP server endpoint URL (default: http://127.0.0.1:8080/mcp)

Examples:
  # Initialize MCP session
  python wazuh_mcp_cli.py init

  # List available tools
  python wazuh_mcp_cli.py tools

  # Retrieve alerts
  python wazuh_mcp_cli.py alerts --limit 20
```

```
  # Test agents
  python wazuh_mcp_cli.py test agents

  # Test high-risk agents
  python wazuh_mcp_cli.py test risks --limit 100

  # Threat hunting with OpenAI
  python wazuh_mcp_cli.py hunt --limit 50 --model gpt-4o-mini
```

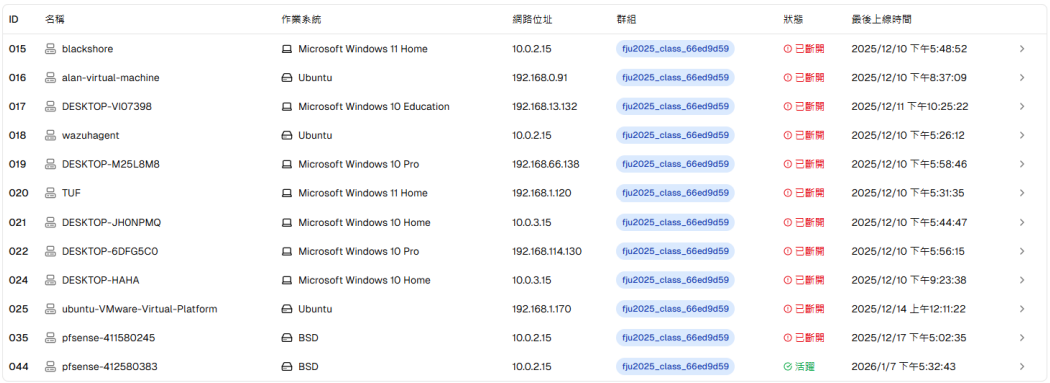
後來增加 wazuh api(去 openai 申請)，我問: 給我最近 24 小時的高嚴重度告警摘要，列出 top 5 。LLM 把它解讀完重新生成給我一報告(自然語言)





2. 用三台 vm，一台 wazuh，一台 pfsense，一台被攻擊。

   按照上次老師教的影片，順利連上(pfsense-412580383)



ID	名稱	作業系統	網路位址	群組	狀態	最後上線時間
015	blackshore	Microsoft Windows 11 Home	10.0.2.15	fju2025_class_66ed9d59	已斷開	2025/12/10 下午5:48:52
016	alan-virtual-machine	Ubuntu	192.168.0.91	fju2025_class_66ed9d59	已斷開	2025/12/10 下午8:37:09
017	DESKTOP-VIO7398	Microsoft Windows 10 Education	192.168.13.132	fju2025_class_66ed9d59	已斷開	2025/12/11 下午10:25:22
018	wazuhagent	Ubuntu	10.0.2.15	fju2025_class_66ed9d59	已斷開	2025/12/10 下午5:26:12
019	DESKTOP-M25L8M8	Microsoft Windows 10 Pro	192.168.66.138	fju2025_class_66ed9d59	已斷開	2025/12/10 下午5:58:46
020	TUF	Microsoft Windows 11 Home	192.168.1.120	fju2025_class_66ed9d59	已斷開	2025/12/10 下午5:31:35
021	DESKTOP-JH0NPMQ	Microsoft Windows 10 Home	10.0.3.15	fju2025_class_66ed9d59	已斷開	2025/12/10 下午5:44:47
022	DESKTOP-6DFG5C0	Microsoft Windows 10 Pro	192.168.114.130	fju2025_class_66ed9d59	已斷開	2025/12/10 下午5:56:15
024	DESKTOP-HAHA	Microsoft Windows 10 Home	10.0.3.15	fju2025_class_66ed9d59	已斷開	2025/12/10 下午9:23:38
025	ubuntu-VMware-Virtual-Platform	Ubuntu	192.168.1.170	fju2025_class_66ed9d59	已斷開	2025/12/14 上午12:11:22
035	pfsense-411580245	BSD	10.0.2.15	fju2025_class_66ed9d59	已斷開	2025/12/17 下午5:02:35
044	pfsense-412580383	BSD	10.0.2.15	fju2025_class_66ed9d59	活躍	2026/1/7 下午5:32:43

設定規則: tcp any any -> [private networks] 22　(內部服務嘗試存取)
tcpdump -n -i <interface> port 514 執行這行指令就可以了

3.

我用的資料是 **The Ultimate PCAP**，因為它裡面包含大量 HTTPS、TLS 1.3、QUIC 等加密流量。因為它是 pcapng 檔，所以我後來轉成 pcap 才可跑 ET-BERT，後來建立 ET-BERT 需要的資料 normal、malware 做對照，最後開始執行 ET-BERT，後來嘗試 **packet mode**、**flow mode**。

最後發現程式可以讀到 pcap，但是有效樣本數是 0，直接在資料切分階段失敗，各自原因是不符合 ET-BERT 的序列，這個資料已經是被整理過的，還有如果用 flow mode，可能還要找其他工具轉成 flow，ET-BERT 本身 沒有內建 flow 產生功能，但我知道接下來就是模型預訓練、模型微調、模型測試。

ET-BERT 是學習「流量行為模式」，從 PCAP / Flow 中判斷「這條加密流量像不像 Cobalt Strike」

LLM 而是讀取 ET-BERT 的結果 + Wazuh 告警，並產生人看得懂的威脅解釋與報告

這兩個是合作關係的。

	ET-BERT	LLM
輸入資料	封包長度、方向、時間序列（Flow / PCAP 衍生特徵）	文字、程式碼、結構化文本
是否分析 Payload	不分析(被 TLS 加密）	需要可讀文字

Token 定義	封包行為序列	詞、子詞
是否適合 PCAP	是（經 flow/sequence 轉換）	不適合
是否具語意理解	無	有
資安應用	加密流量分類、惡意 C2 偵測	SOC 告警解讀、報告生成

TeamViewer 是合法但高度加密的遠端控制流量，有固定流量行為、有模式
AnyDesk 和 TeamViewer 相似，都是合法的遠端桌面工具

Cobalt Strike 是惡意加密遠端控制，封包看起來像正常加密流量，所以只能從流量行為判斷

```
(venv) wazuh@wazuh-VirtualBox:~/ET-BERT/data_process$ python main.py --dataset_path ~/datasets/etbert
--output_path ~/datasets/etbert_output --mode flow
[Errno 2] No such file or directory: 'I:\\cstnet-tls1.3\\packet\\result\\dataset\\'
Dataset directory I:\cstnet-tls1.3\packet\result\dataset\ not exist.
Begin to obtain new dataset.

Begin to generate features.
0it [00:00, ?it/s]
all     0
read dataset from json file.
category flow
0       0
1       0
2       0
3       0
4       0
5       0
6       0
7       0
8       0
9       0
10      0
11      0
12      0
13      0
14      0
15      0
16      0
17      0
18      0
```