# 次世代校園的
# 安全網路維運平台

從「收到通報」轉成「提前發現、快速處置、持續證明」

## Cisco Secure IPS

朱育民 | 台灣思科系統

2026 年 7 月 31 日

WHY THIS MATTERS

# 校園資安的壓力，不是告警數量；是通報時鐘

01

## 事件發生

學生、研究設備、對外服務
任何一點都可能成為入口

02

## 上游看見

區網／教育部偵測異常
通知落到校方

03

## 校內追查

找來源、找責任單位
確認是否仍在持續

04

## 回覆與舉證

提出處置、影響範圍
與改善措施

現在

**上游通報後，校內才開始追查**

**把判斷點往左移**

目標

**校內出口先看見、先處置**

目標不是「沒有事件」，而是「更早發現、更快收斂、更容易交代」。

THE NEW REALITY

# 傳統資安維運的前提，正同時被三件事改寫

AI

## 攻擊速度變快

AI 降低攻擊腳本與變形成本。

只靠固定特徵，比對速度可能追不上變化速度。

需要：規則 + 機器學習的互補偵測。

TLS

## 流量越來越看不見

TLS 1.3、QUIC 與 ECH 逐步壓縮可觀察範圍。

全面解密有隱私、效能與憑證管理成本。

需要：加密流量的風險能見度。

↗

## 規避工具更普及

加密 DNS、私人 VPN、多跳代理不一定惡意，卻會會繞過既有政策。

校園的開放性讓這類流量更常見。

需要：先辨識「刻意躲藏」。

10.0

次世代 的校園安全維運 必須同時回答：未知攻擊、加密能見度、規避流量

CAMPUS DEFENSE MODEL

# 沿用區網既有防護語言，補齊校內最後一哩


**共同防護語言**　同一套 Talos 情資、Snort 規則與事件語意

校內不是再建一座孤島，而是讓上游與校內更容易對得上訊號、事件與處置。

對外網站　研究設備

師生裝置　宿舍網路

對計中資安維運同仁的價值：縮短「這是誰、在哪裡、還在不在」的確認時間。

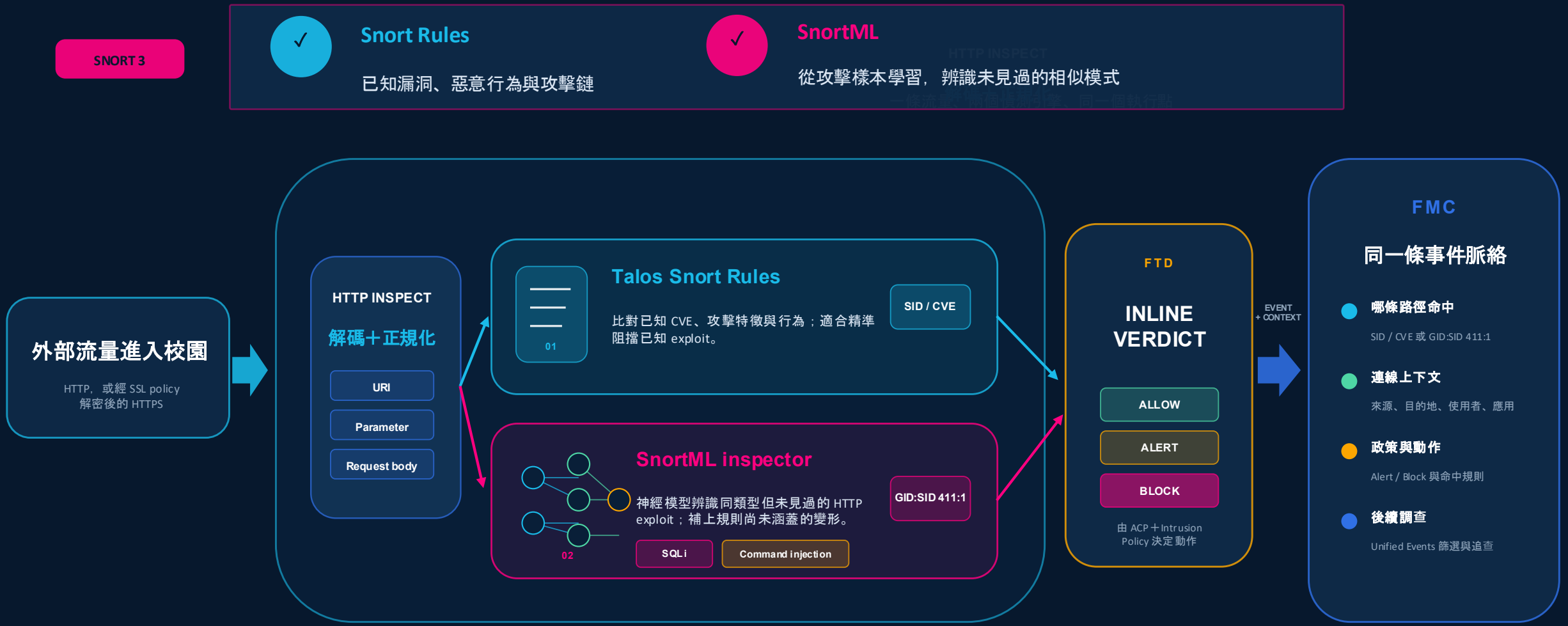
PLATFORM, NOT A BOX

# 從買一個資安設備，走向一條從訊號到證據的維運鏈


**平台價**值不在「擋了多少」，而在每一次判斷都能被管理、被追溯、被改善。

# 第一層：已知與未知攻擊，都在落地前處理

同一份 HTTP payload 先由 Snort 3 解碼與正規化，再交給 Talos 規則與 SnortML；FTD 執行 verdict，FMC 留下可追查的事件脈絡。



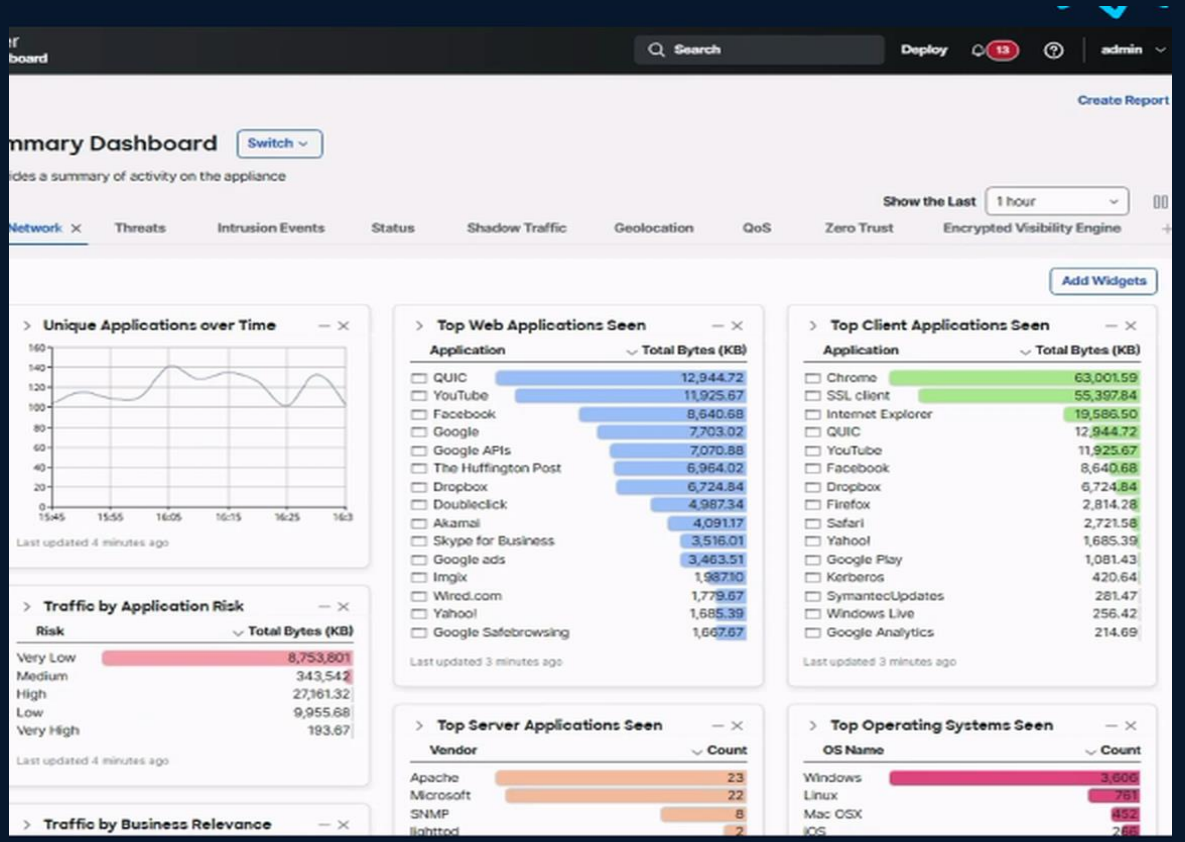
# 第二層：看見加密流量，不必全面解密

EVE

## 不讀內容，辨識連線的「外觀」

- **TLS／QUIC 指紋** — 用戶端程序、來源 OS 與連線特徵
- **目的端脈絡** — 結合網域、位址與連接埠提高判斷信心
- **Monitor → Protect** — 先觀察分布，再只對高信心威脅執行阻擋

**校園原則：先用 Monitor 建立基線；誤擋的成本可能是一堂課。**




Encryption Visibility Engine(EVE) 讓全面解密不再是唯一選項；全新的風險訊號，讓你對加密流量的可視性大幅提升。

ENCRYPTED VISIBILITY | HOW EVE WORKS

# EVE 不是流量排行榜：它用握手指紋與目的地脈絡，判斷「誰發起、風險多高」

不解密 payload，也能從 TLS / QUIC 連線建立階段產生 Process、OS 與 Threat Confidence；結果進 FMC，依 Monitor / Protect 決定記錄或阻擋。

## 01 OBSERVE

### 只看初始握手


TLS ClientHello / QUIC Initial

- TLS version
- Cipher suites
- Extensions
- ALPN / SNI

**看不到 payload 內容**

URL path / 表單 / 檔案仍是加密的

## 02 FINGERPRINT + CONTEXT

### EVE 在 FTD 本機比對

**握手指紋**
ClientHello 結構

**目的地脈絡**
IP / SNI / Port

EVE

- 形成 fingerprint
- 比對 VDB 指紋 / 模型庫
- 計算 Process＋Threat Confidence

模型與惡意程序指紋隨 VDB 更新下發；
不是每條連線送到雲端判斷。

## 03 DECIDE

### 每條連線產生判斷

EVE RESULT | EXAMPLE

| | |
|---|---|
| Process | malware_upatre |
| Process confidence | 99% |
| Client OS | Windows |
| Threat confidence | VERY HIGH |
| Fingerprint | tls/1/(0303)/... |

**這才是 EVE 的輸出：**
**程序、信心分數與威脅判斷。**

## 04 ENFORCE + INVESTIGATE

### FMC 把判斷變成動作

**MONITOR** 辨識應用 / 程序、記錄 EVE 欄位、產生 IoC

**PROTECT** 威脅信心超過門檻即阻擋；可建立 EVE exception

**UNIFIED EVENTS** 篩選、Cross-launch、追查同指紋連線

需要在 ACP rule 開啟 logging，FMC 才會顯示完整結果。

**EVE 回答的不是「QUIC / SSL Client 有多少」；而是「哪個 process 建立這條加密連線、判斷有多確定、它是否像惡意 process」。**

**啟用路徑**

**Policies > Security Policies > Access Control > EVE > Monitor / Protect > Deploy**

前提：有效 IPS license；對相應 ACP rules 啟用 logging。

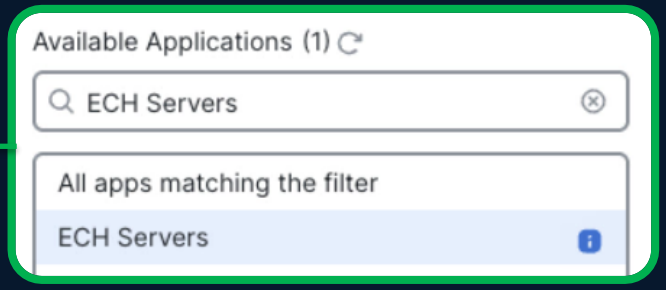
**FMC 要看的欄位**

**EVE Fingerprint | Process Name | Process Confidence | Threat Confidence | Detection Type**

位置：Events & Logs > Analysis > Unified Events，或 Connection Events。

# 不解密的可視性: 透過Client Hello洞悉 TLS 指紋與目的端情境

# Encryption Client Hello(ECH) 流量的異常偵測




| Event Type | Action | Destination IP | URL | Web Application | Encrypted Visibility Process Name | Encrypted Visibility Process Confidence Score | Encrypted Visibility Fingerprint |
|---|---|---|---|---|---|---|---|
| Connection | Allow | 172.67.135.44 | https://cloudflare-ech.com | ECH Servers | chromium browser | 98% | quic/(00000001)(0303)(130113021303 |

……但真實目的地被 ECH 隱藏
(https://pig-in-the-middle.pl)

EVE 可判定這條連線
由 Chrome 發起……

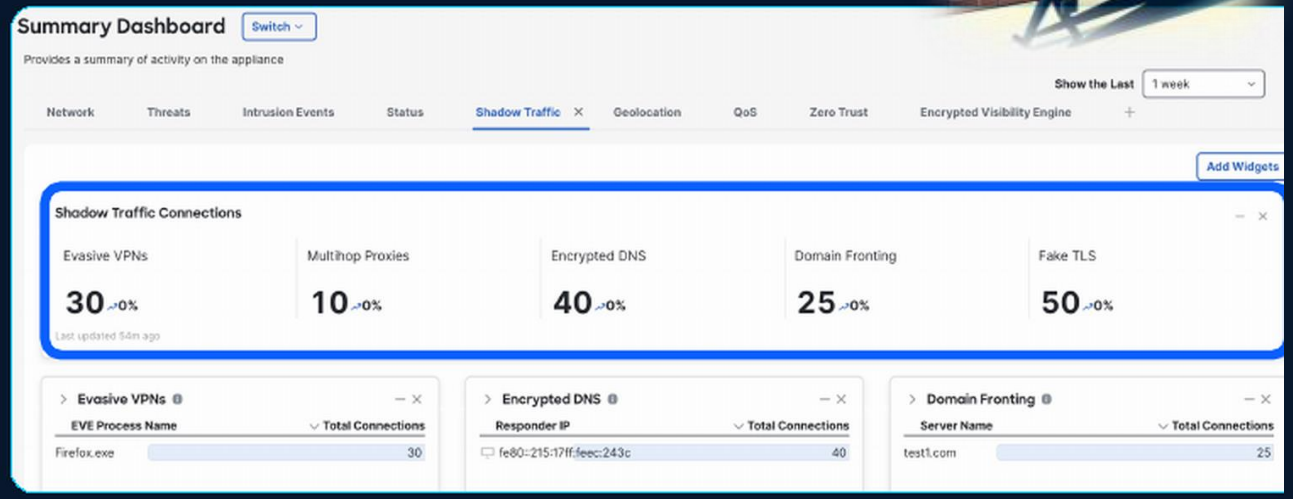
真實目的地仍然未知,但 EVE 給出強烈的可疑訊號:

| | Time | Event Type | Action | Source IP | Web Application | Destination IP | Destination Port / ICMP Code | URL | Encrypted Visibility Process Name | Encrypted Visibility Proces… |
|---|---|---|---|---|---|---|---|---|---|---|
| › | 2025-10-30 14:39:01 | Connection | Allow | 198.19.10.103 | ECH Servers | 104.18.11.118 | 443 (https) / tcp | https://cloudflare-ech.com | generic dmz process | 65% |
| › | 2025-10-30 14:36:46 | Connection | Allow | 198.19.10.103 | ECH Servers | 104.18.10.118 | 443 (https) / tcp | https://cloudflare-ech.com | rancher desktop | 100% |
| › | 2025-10-30 14:36:30 | Connection | Allow | 198.19.10.21 | ECH Servers | 172.67.135.44 | 443 (https) / udp | https://cloudflare-ech.com | chromium browser | 98% |
| › | 2025-10-30 14:36:20 | Connection | Allow | 198.19.10.21 | ECH Servers | 104.21.26.24 | 443 (https) / tcp | https://cloudflare-ech.com | firefox browser | 100% |

來自非標準瀏覽器的 ECH 流量,本身就是異常的徵兆。

# 第三層：把「刻意躲藏」的流量先標出來

- **Encrypted DNS** 加密 DNS
- **Evasive VPN** 規避型私人 VPN
- **Multi-hop Proxy** 多跳代理
- **Domain Fronting** 網域前置
- **Fake TLS** 偽裝 TLS




| Event Type | Action | Client Application | Web Application | Destination IP | Destination Port / ICMP Code | Shadow Traffic Type | TLS Client SNI |
|---|---|---|---|---|---|---|---|
| Connection | Allow | SSL client | XVPN | 35.205.176.240 | **443** (https) / tcp | Evasive VPN | 8v9m.com |
| Connection | Allow | X-VPN | Web Browsing | 130.211.50.202 | **20005** / tcp | Evasive VPN | |
| Connection | Allow | X-VPN | Web Browsing | 35.205.250.171 | **20005** / tcp | Evasive VPN | |
| Connection | Allow | Firefox | DNS over HTTPS | 172.64.41.4 | **443** (https) / tcp | Encrypted DNS | mozilla.cloudflare-dns.com |
| Connection | Allow | Firefox | DNS over HTTPS | 172.64.41.4 | **443** (https) / tcp | Encrypted DNS | mozilla.cloudflare-dns.com |
| Connection | Allow | Tor | | 185.220.101.192 | **443** (https) / tcp | Evasive VPN, Multihop Proxy | www.4vq22c3cvbm7v6bq |

**不是每一條規避流量都是攻擊**　但它們是最值得先釐清的流量：誰在使用、從哪裡來、是否違反校內政策。

註：Domain Fronting 偵測需 TLS／QUIC 解密；Fake TLS 需啟用 EVE。支援條件與限制請依 10.0 文件確認。

# Shadow Traffic 的五種樣態

**Shadow Traffic Connections**

| Evasive VPNs | Multihop Proxies | Encrypted DNS | Domain Fronting | Fake TLS |
|---|---|---|---|---|
| 30 ↗0% | 10 ↗0% | 40 ↗0% | 25 ↗0% | 50 ↗0% |

Last updated 54m ago

## Evasive VPNs

已知的規避型 VPN 應用,企圖繞過防火牆管控。


70+ 種 VPN 應用

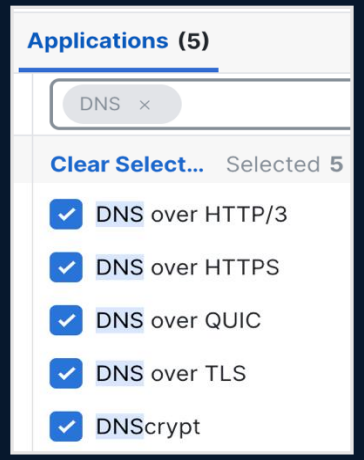
## Multi-hop Proxies

以多層跳板匿名化網路活動。

Tor .....以及更多

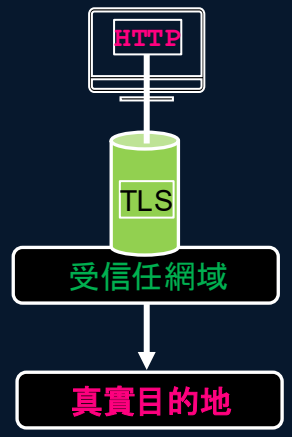
## Encrypted DNS

隱蔽的網域解析與通道化。




## Domain Fronting

HTTP header 主機名與 SNI/憑證不一致
偽裝真實目的地。




## Fake TLS

非標準或不安全的 TLS/QUIC 加密套件,或網域偽造。

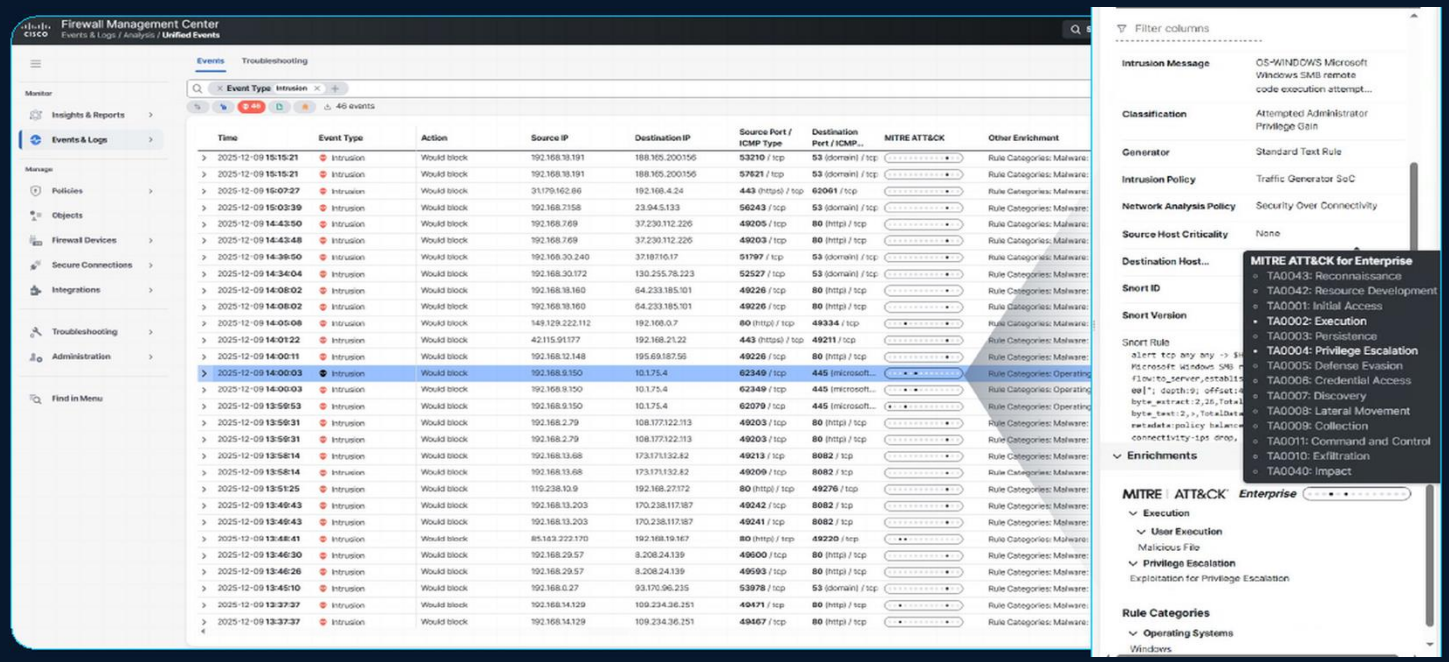
# 維運平台不是更多告警，而是更少判斷成本

**事件**
大量原始訊號

**關聯**
收斂成情境

## 思科安全管理平台 (FMC)

| | |
|---|---|
| **Unified Event Viewer** | 同一處檢視連線、入侵與脈絡 |
| **Correlation Policy** | 將大量事件收斂成少數需要處理的情境 |
| **Automated Response** | 依規則觸發 Email、Syslog、SNMP 或整或整合動作 |



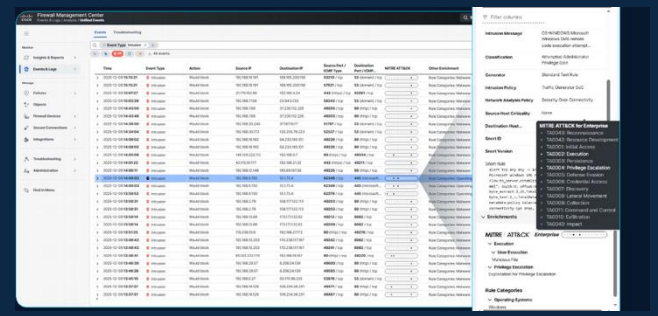

把「找訊號」的時間，移到「做判斷」與「採取行動」。

# 從收到通報到完成回覆：在 思科安全管理平台(FMC) 的實際操作鏈

每一步都對應一個介面、一個動作，以及一份可放進通報回覆的證據

| | | | | |
|---|---|---|---|---|
| 01 | 接住事件 | Events & Logs > Intrusion | 以通報時間＋來源 IP 找到 IPS event；確認 action、SID、CVE 與命中規則。 | 事件紀錄 |
| 02 | 補齊脈絡 | Unified Events > Connection | Cross-launch 連線事件；補上使用者、主機、應用、目目的地與 EVE／Shadow Traffic。 | 影響範圍 |
| 03 | 立即圍堵 | Policies > Access Control | 由 inline IPS drop、Security Intelligence block 或暫時性時性 ACP rule 阻擋持續活動。 | 處置紀錄 |
| 04 | 確認收斂 | Connection Events > Same Filter | 用相同條件確認 last seen；檢查是否還有其他來源、目目的地或校內主機持續命中。 | 收斂證明 |
| 05 | 匯出回覆 | Advanced Logging / Splunk Wizard | 針對指定規則保留協定紀錄與入侵封包；輸出至 Splunk Splunk／SIEM 組成事件時間線。 | 回覆附件 |

## FMC 把通報所需證據集中到同一條事件脈絡



### 回覆時直接帶出的 6 個欄位

- 來源 IP／使用者
- 目的地／應用
- First／Last Seen
- SID／CVE／攻擊
- 阻擋動作／Policy
- 封包／協定證據

**FMC 能幫你把散落在設備、Syslog中的資訊，整理成可直接填入回覆的證據。**

# AI 做整理與建議；治理流程保留決定權

**01** **政策異常**

找出被遮蔽、重複、過期與可合併規則

**02** **最佳實務落差**

依 Cisco 建議檢查組態，保留趨勢與報告

**03** **升級與生命週期**

看見 CVE、建議版本與 EOL 風險

**04** **變更治理**

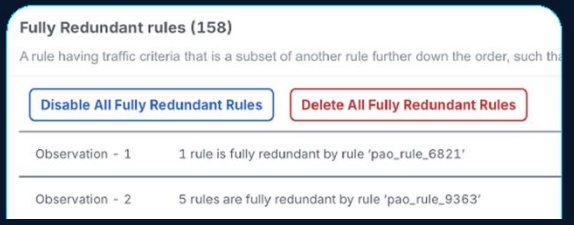
複製政策、審核變更、保留 audit trail

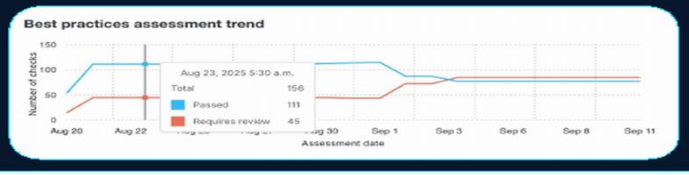
Policy Analyzer & Optimizer 為雲端服務，需整合 Cisco Security Cloud；採用前應先確認資料治理與變更審核要求。

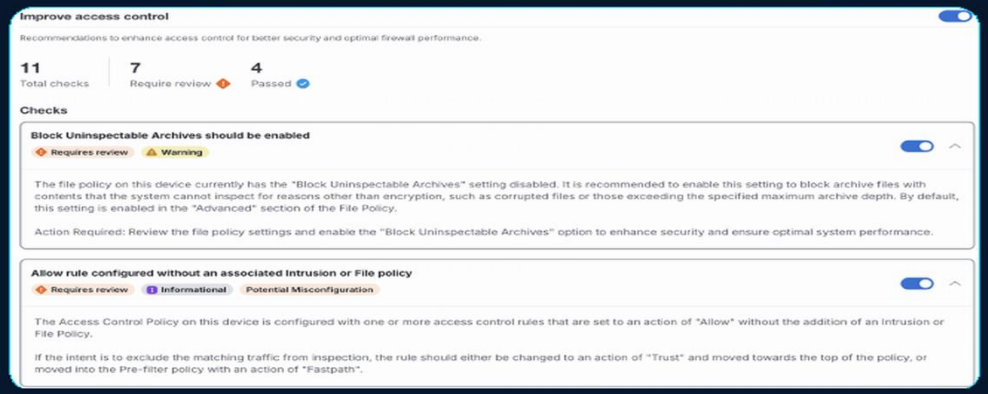
Technical Overview – Duplicate rules


**Identifies shadowed rules that will never process traffic** - these rules are blocked by higher-priority rules and can be safely removed

**Finds redundant rules that duplicate existing protections** - removing these simplifies management without affecting security coverage



# 現在的選擇，必須留得住今後的加密升級路徑


真正的問題不是「Q Day 哪一年來臨」

**而是今天買的設備，屆時還有沒有可升級的路徑。**

# 少收一張通報，我們不靠運氣

## 思科透過實打實的技術
## 將 偵測、處置與證據 放到同一個資安維運平台

01 Snort 3 + SnortML：已知與未知攻擊互補

02 EVE + Shadow Traffic：找回加密與規避流量能見度

03 FMC：把事件、政策與回報變成可重複流程

# Talos 到底管理多少開源安全社群與專案？

三種數字的口徑不同：社群 ≠ 官方工具目錄 ≠ GitHub repository；不能相加，也不能把 77 說成 77 個安全產品。

**2** 旗艦開源社群 / 引擎
Snort IDS/IPS · ClamAV anti-malware

**26** 官方 Open-source Tools
包含 2 個旗艦引擎＋24 項專用工具

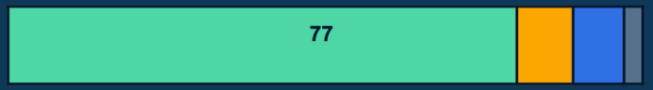
**77** Cisco-Talos 公開 repositories
62 原生未封存；其餘為封存專案與 forks

## 官方 Open-source Security Tools 目錄 | 26 項

以下為官方目錄完整名單；分類為簡報整理，不代表 Talos 的正式產品線。

| | | |
|---|---|---|
| 2 | 旗艦社群 / 引擎 | Snort • ClamAV |
| 7 | 網路防禦 / 流量 | Synful Knock Scanner • Cisco Smart Install Scanner • Daemonlogger<br>Decept • Mutiny Fuzzer • File2pcap • Re2Pcap |
| 8 | 惡意程式 / 簽章 / 解密 | PE-Sig • BASS • MBR Filter • PyLocky Decryptor<br>TeslaCrypt Decryption Tool • Thanatos Decryptor • LockyDump • Flokibot Tools |
| 8 | 逆向 / 漏洞研究 / 保護 | FIRST • Dynamic Data Resolver • Moflow • FreeSentry<br>ROPMEMU • PyREBox • GhIDA • IDA Pro TileGX Plugin |
| 1 | 建置 / 依賴自動化 | Mussels |

## GitHub footprint | 77 repos




- 62 原生 / 未封存
- 7 原生 / 已封存
- 6 Fork / 未封存
- 2 Fork / 已封存

**不要把 77 當成「持續維護中的產品」**

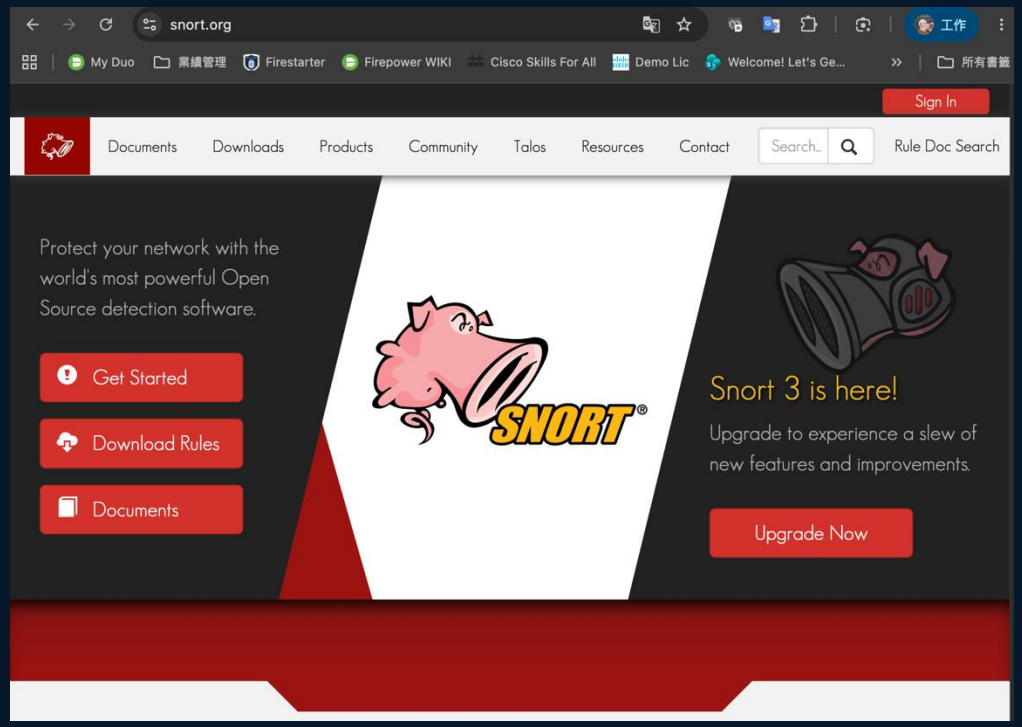
repository 可能是文件、套件、研究 PoC、fork 或歷史工具；未封存也不等於有維護 SLA。

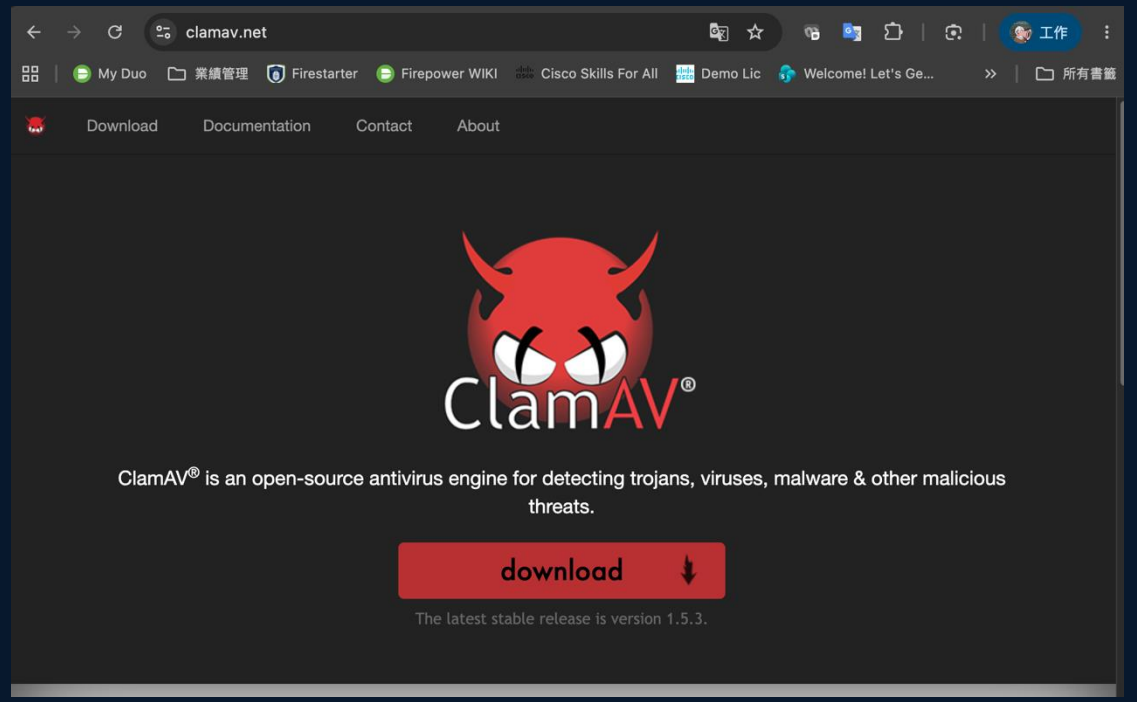
Snort >450K systems

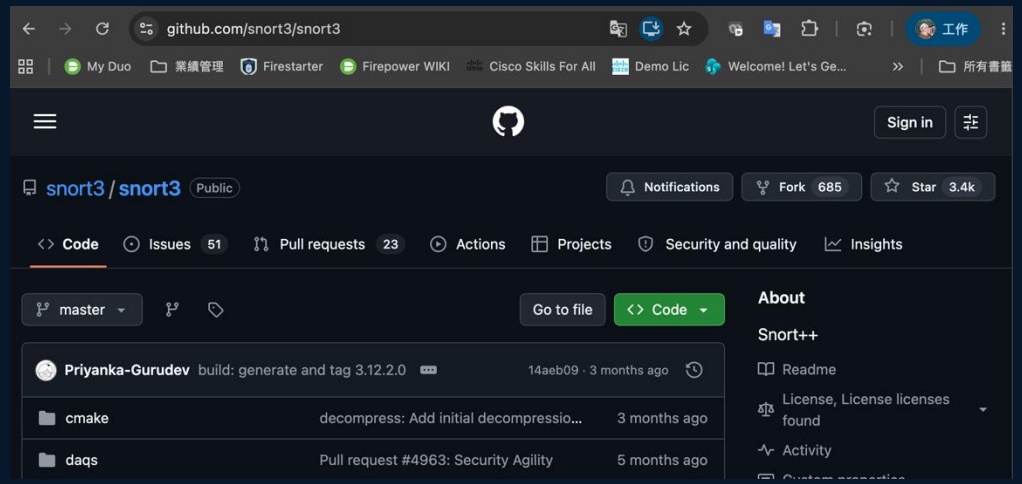
ClamAV >18M installs

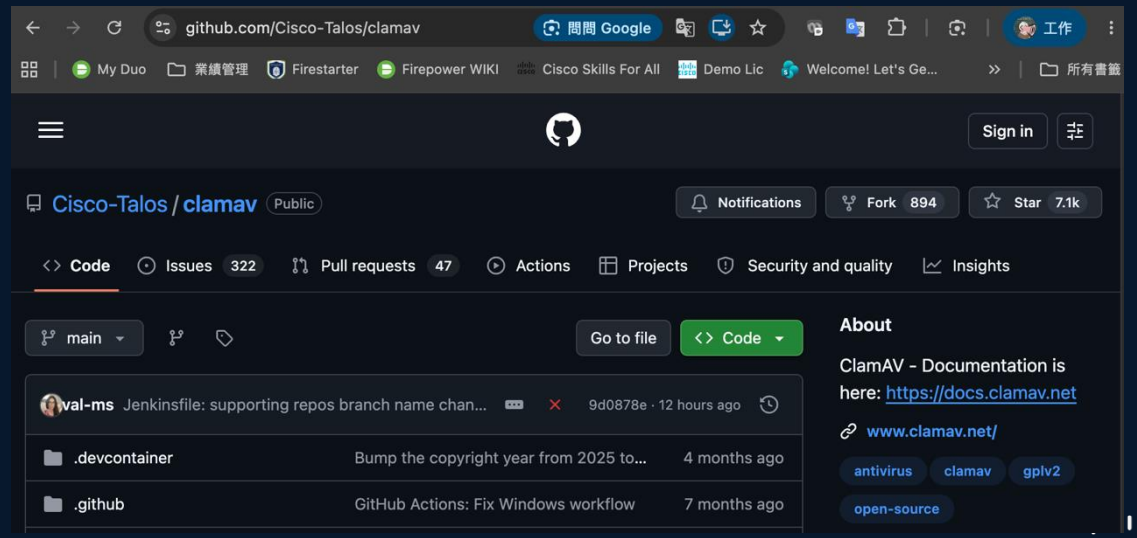
口徑：2＝Talos 明確稱為「our open-source」的旗艦引擎 / 社群；26＝Talos 官方工具目錄；77＝Cisco-Talos GitHub org API（2026-07-31）。SpamCop / SenderBase 為服務或情報社群，不列為開源程式專案。

影響力：Snort 授權部署 >450,000 系統 | 規則發布下載者 >60,000 | ClamAV 已知安裝 >18,000,000（Talos，2024-08）。



# Snort.org：Cisco 與大專院校共創資安能力的開放接口

不是把免費軟體送進教室；而是讓同一套開源引擎，從課堂、研究一路走到校園 SOC，再把成果回饋全球社群。

## CISCO TALOS／SNORT.ORG

### 公開、可重現的技術底座

01 **Snort 3 開源引擎**
Source code、LibDAQ、plugins 與文件

02 **Community Ruleset**
社群開發、Talos QA、免費下載

03 **規則撰寫與測試方法**
Rule guide、PCAP replay、inline test

04 **全球威脅研究脈絡**
Talos advisories、coverage request、社群回饋

## SNORT.ORG | JOINT SECURITY LAB

### 同一套引擎，形成三條產學合作軌道

| | | |
|---|---|---|
| 01 TEACH 教學 | PCAP → 規則 → Alert<br>學生看見偵測如何發生 | 課程 |
| 02 RESEARCH 研究 | 資料集 → 指標 → Detector<br>比較準確率、效能與誤報 | 論文 |
| 03 OPERATE 維運 | Monitor → Tune → Evidence<br>把成果帶回校園 SOC | 防禦 |

成果可回饋：規則／setup guide／bug report／coverage request／匿名化案例

## 大專院校

### 真實問題、研究方法與人才

01 **課程與 Capstone**
網路安全、惡意流量、事件調查

02 **研究題目與評估方法**
ML、加密流量、IoT／OT、規則效能

03 **校園真實情境**
入口網站、SSO／VPN、研究主機與宿網

04 **學生人才與社群成果**
作品集、規則貢獻、技術報告與研究論文

**共同價值：學校取得可重現的教材、研究題目與人才成果；Cisco／Talos 擴大規則驗證、社群知識與在地威脅理解；校園 SOC 得到可執行的偵測與證據。**

# 感謝蒞臨