

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」

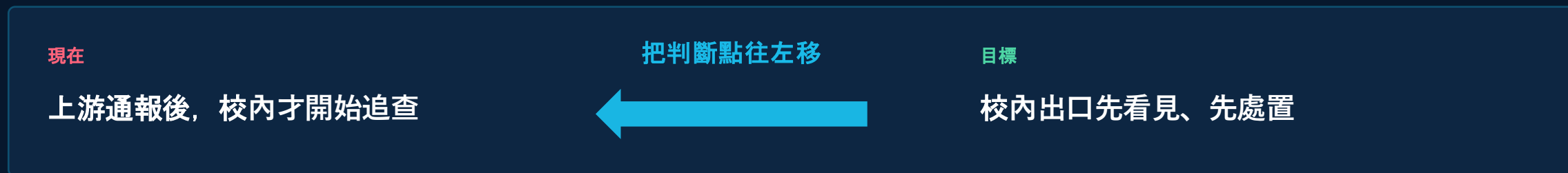
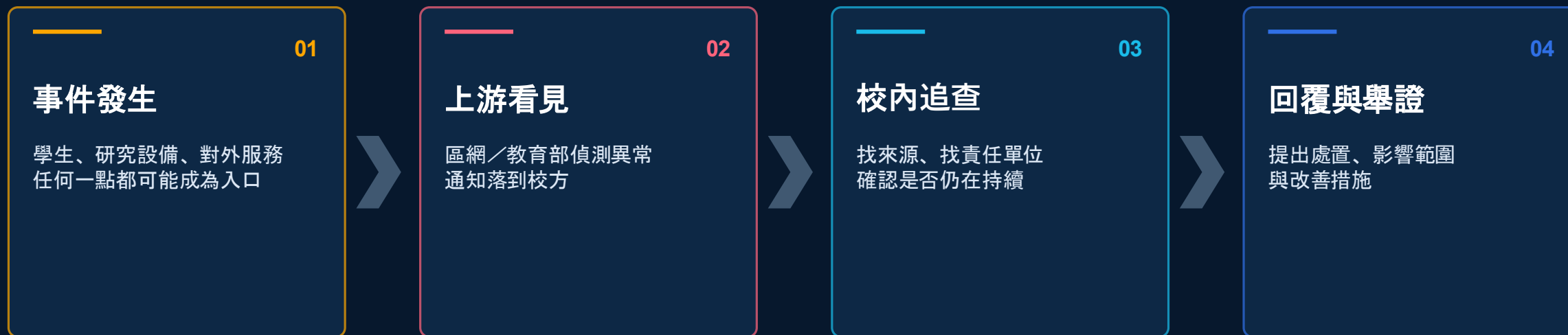
Cisco Secure IPS

朱育民 | 台灣思科系統

2026 年 7 月 31 日



校園資安的壓力，不是告警數量；是通報時鐘



目標不是「沒有事件」，而是「更早發現、更快收斂、更容易交代」。

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

沿用區網既有防護語言，補齊校內最後一哩



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。

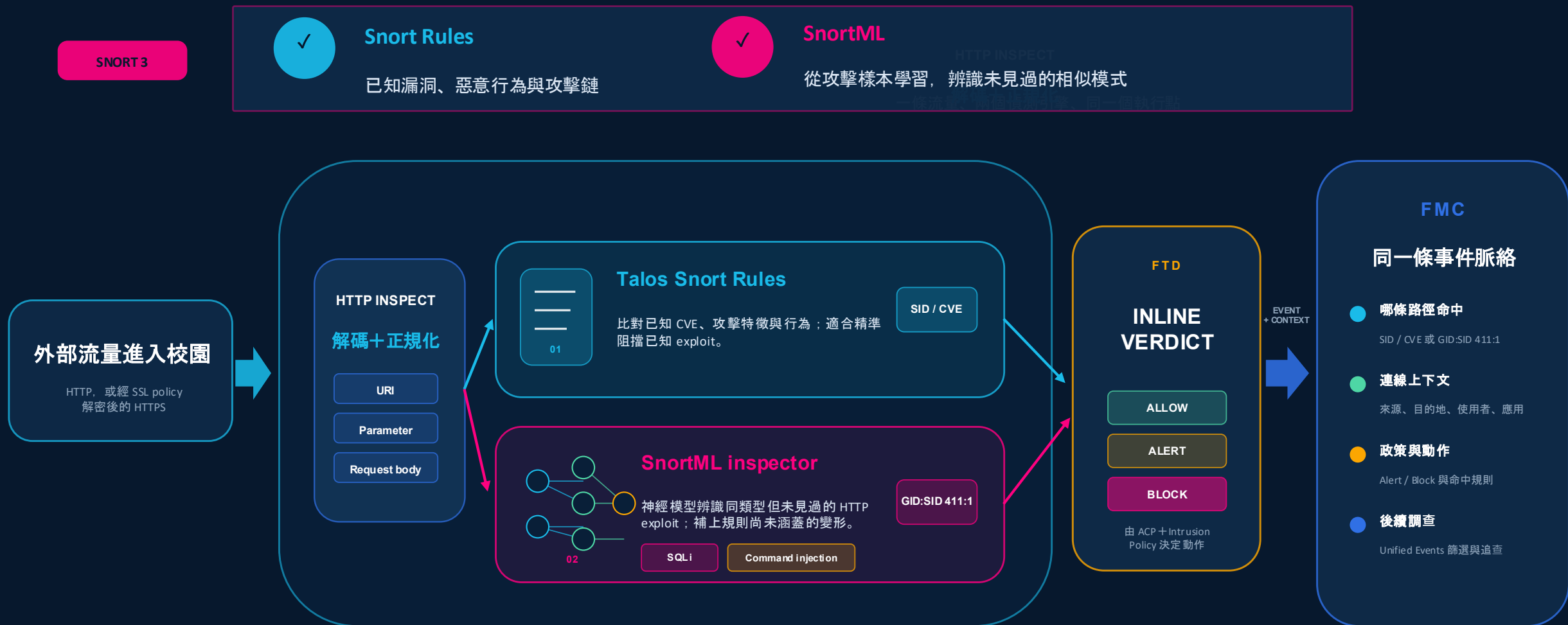
從買一個資安設備，走向一條從訊號到證據的維運鏈



—— 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

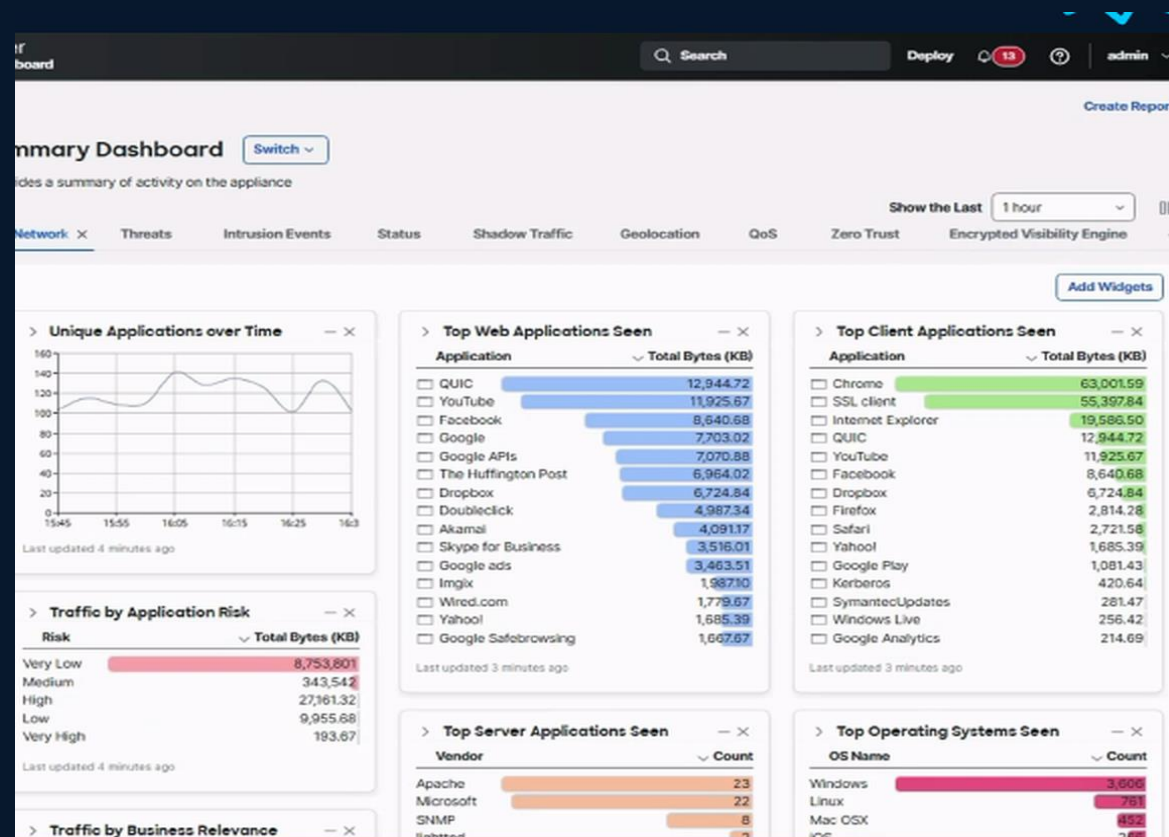
目的端脈絡

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。

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。



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

TLS ClientHello

```
✓ Cipher Suites (18 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```



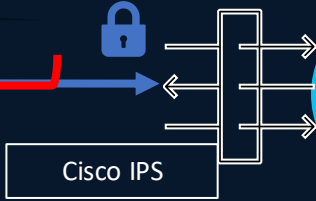
TLS 指紋



TCP/TLS 192.168.2.110/34624->172.16.45.200/443 (SNI cisco.com)



目的端資訊



信心度:99.94%
程序:firefox.exe
版本:76.0.1
類別:browser
作業系統:Windows 10 19041.329
常見 FQDN:cisco.com

依 TLS 與目的端中繼資料,為每個用戶端應用產生唯一指紋

Encryption Client Hello(ECH) 流量的異常偵測

Available Applications (1)

All apps matching the filter

ECH Servers

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



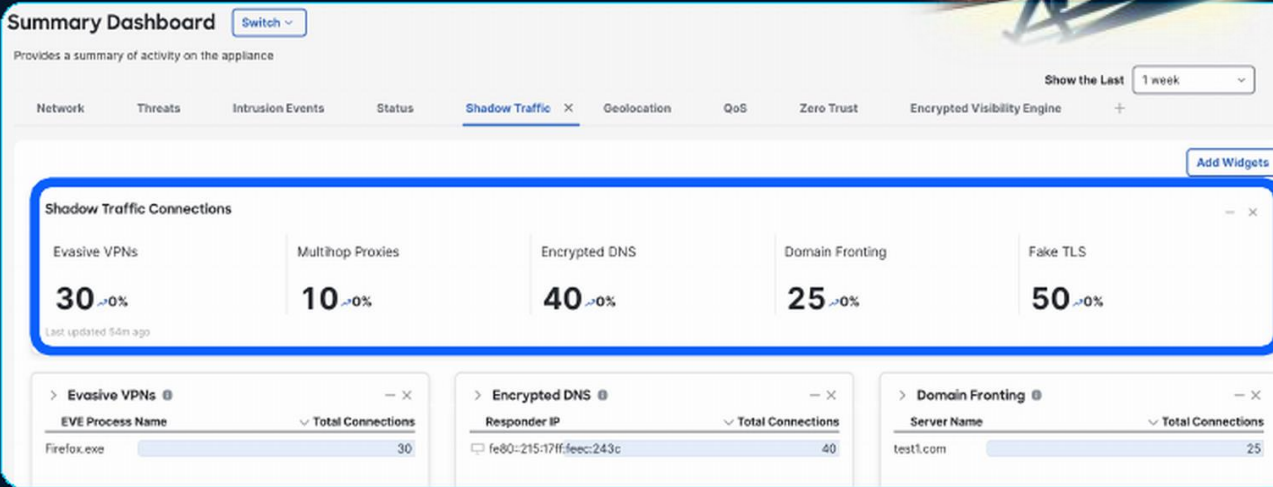
Encrypted DNS 加密 DNS

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

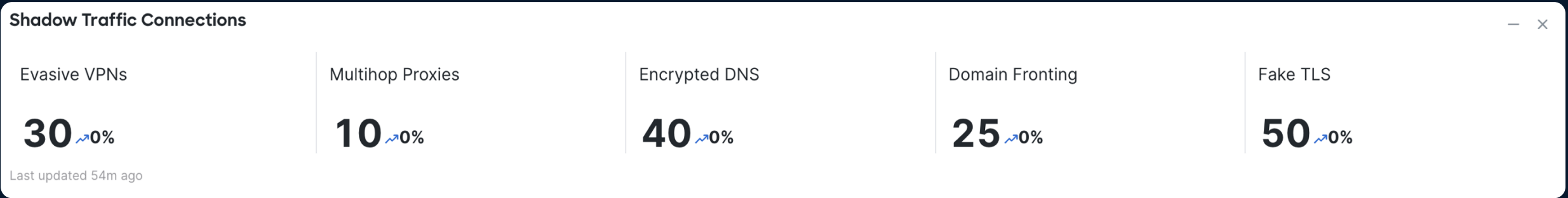


Event Type	Action	Client Application	Web Application	Destination IP	Destination Port / ICMP Code	Shadow Traffic Type	TLS Client SNI
Connection	Allow	SSL client	XVPN	35.205.176.240	443 (https) / tcp	Evasive VPN	8v9m.com
Connection	Allow	X-VPN	Web Browsing	130.211.50.202	20005 / tcp	Evasive VPN	
Connection	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.4vo22c3cybm2v8bo

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



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

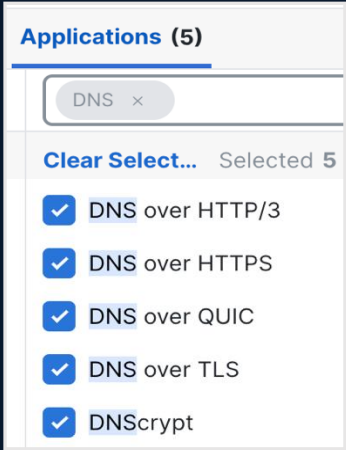
Multi-hop Proxies

以多層跳板匿名化網路活動。



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 或整合動作

The screenshot displays the Cisco FMC 'Events' page. The main table lists intrusion events with columns for Time, Event Type, Action, Source IP, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Type, MITRE ATT&CK, and Other Enrichment. A sidebar on the left contains navigation links like Monitor, Insights & Reports, Events & Logs, Policies, Objects, Firewall Devices, Secure Connections, Integrations, Troubleshooting, and Administration. On the right, a detailed view of a selected event shows its classification, generator, network analysis policy, source host criticality, destination host, and a list of MITRE ATT&CK techniques mapped to the event.

Time	Event Type	Action	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Type	MITRE ATT&CK	Other Enrichment
2025-12-09 15:15:21	Intrusion	Would block	192.168.18.191	188.165.200.156	53210 / tcp	53 (domain) / tcp	...	Rule Categories: Malware
2025-12-09 15:15:21	Intrusion	Would block	192.168.18.191	188.165.200.156	57821 / tcp	53 (domain) / tcp	...	Rule Categories: Malware
2025-12-09 15:07:27	Intrusion	Would block	31.179.162.66	192.168.4.24	443 (https) / tcp	42001 / tcp	...	Rule Categories: Malware
2025-12-09 15:03:39	Intrusion	Would block	192.168.7158	23.94.5.133	56243 / tcp	53 (domain) / tcp	...	Rule Categories: Malware
2025-12-09 14:43:50	Intrusion	Would block	192.168.769	37.230.112.226	49205 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 14:43:48	Intrusion	Would block	192.168.769	37.230.112.226	49203 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 14:36:50	Intrusion	Would block	192.168.30.240	37.187.16.17	51797 / tcp	53 (domain) / tcp	...	Rule Categories: Malware
2025-12-09 14:34:04	Intrusion	Would block	192.168.30.172	130.255.78.223	52527 / tcp	53 (domain) / tcp	...	Rule Categories: Malware
2025-12-09 14:08:02	Intrusion	Would block	192.168.18.160	64.233.185.101	49226 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 14:08:02	Intrusion	Would block	192.168.18.160	64.233.185.101	49226 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 14:05:08	Intrusion	Would block	148.129.222.112	192.168.0.7	80 (http) / tcp	49334 / tcp	...	Rule Categories: Malware
2025-12-09 14:01:22	Intrusion	Would block	42.115.91.177	192.168.21.22	443 (https) / tcp	49211 / tcp	...	Rule Categories: Malware
2025-12-09 14:00:11	Intrusion	Would block	192.168.12.148	195.69.187.56	49226 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 14:00:03	Intrusion	Would block	192.168.9.150	10.1.75.4	62349 / tcp	445 (microsoft...) / tcp	...	Rule Categories: Operating
2025-12-09 14:00:03	Intrusion	Would block	192.168.9.150	10.1.75.4	62349 / tcp	445 (microsoft...) / tcp	...	Rule Categories: Operating
2025-12-09 13:59:53	Intrusion	Would block	192.168.9.150	10.1.75.4	62079 / tcp	445 (microsoft...) / tcp	...	Rule Categories: Operating
2025-12-09 13:59:31	Intrusion	Would block	192.168.2.79	108.177.122.113	49203 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 13:59:31	Intrusion	Would block	192.168.2.79	108.177.122.113	49203 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 13:58:14	Intrusion	Would block	192.168.13.68	173.171.132.82	49213 / tcp	8082 / tcp	...	Rule Categories: Malware
2025-12-09 13:58:14	Intrusion	Would block	192.168.13.68	173.171.132.82	49209 / tcp	8082 / tcp	...	Rule Categories: Malware
2025-12-09 13:51:25	Intrusion	Would block	115.238.13.9	192.168.27.172	80 (http) / tcp	49276 / tcp	...	Rule Categories: Malware
2025-12-09 13:49:43	Intrusion	Would block	192.168.13.203	170.238.117.87	49242 / tcp	8082 / tcp	...	Rule Categories: Malware
2025-12-09 13:49:43	Intrusion	Would block	192.168.13.203	170.238.117.87	49241 / tcp	8082 / tcp	...	Rule Categories: Malware
2025-12-09 13:48:41	Intrusion	Would block	85.143.222.170	192.168.18.167	80 (http) / tcp	49220 / tcp	...	Rule Categories: Malware
2025-12-09 13:46:30	Intrusion	Would block	192.168.29.57	8.208.24.139	49600 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 13:46:26	Intrusion	Would block	192.168.29.57	8.208.24.139	49593 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 13:45:10	Intrusion	Would block	192.168.6.27	93.170.96.215	53278 / tcp	53 (domain) / tcp	...	Rule Categories: Malware
2025-12-09 13:37:37	Intrusion	Would block	192.168.14.129	109.234.36.251	49471 / tcp	80 (http) / tcp	...	Rule Categories: Malware
2025-12-09 13:37:37	Intrusion	Would block	192.168.14.129	109.234.36.251	49467 / tcp	80 (http) / tcp	...	Rule Categories: Malware

MITRE ATT&CK for Enterprise

- TA0043: Reconnaissance
- TA0042: Resource Development
- TA0001: Initial Access
- TA0002: Execution
- TA0003: Persistence
- TA0004: Privilege Escalation
- TA0005: Defense Evasion
- TA0006: Credential Access
- TA0007: Discovery
- TA0008: Lateral Movement
- TA0009: Collection
- TA0010: Command and Control
- TA0011: Exfiltration
- TA0040: Impact

Enrichments

- MITRE ATT&CK Enterprise
- Execution
- User Execution
- Malicious File
- Privilege Escalation
- Exploitation for Privilege Escalation
- Rule Categories
- Operating Systems
- Windows

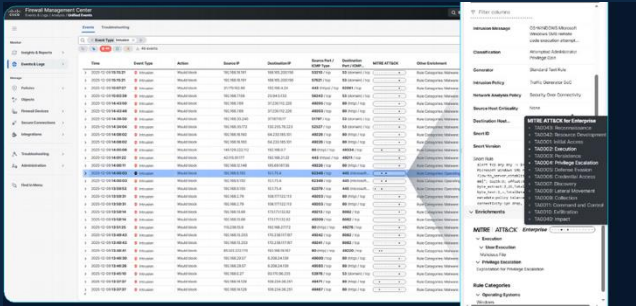
把「找訊號」的時間，移到「做判斷」與「採取行動」。

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



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

Fully Shadowed rules (296)

A shadowed rule is a rule that will never evaluate network traffic because the traffic matches a higher-priority rule. [Learn about Shadowed Rules](#)

Disable All Fully Shadowed Rules

Delete All Fully Shadowed Rules

Observation - 1	1 rule is fully shadowed by rule 'pao_rule_443'
Observation - 2	1 rule is fully shadowed by rule 'pao_rule_182'
Observation - 3	1 rule is fully shadowed by rule 'pao_rule_6807'

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

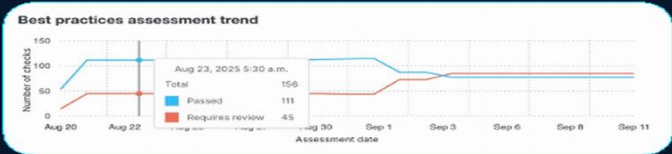
Fully Redundant rules (158)

A rule having traffic criteria that is a subset of another rule further down the order, such that the rule will never be evaluated.

Disable All Fully Redundant Rules

Delete All Fully Redundant Rules

Observation - 1	1 rule is fully redundant by rule 'pao_rule_6821'
Observation - 2	5 rules are fully redundant by rule 'pao_rule_9363'



Improve access control

Recommendations to enhance access control for better security and optimal firewall performance.

11

7

4

Total checks

Require review

Passed

Checks

Block Uninspectable Archives should be enabled

Requires review

Warning

The file policy on this device currently has the "Block Uninspectable Archives" setting disabled. It is recommended to enable this setting to block archive files with contents that the system cannot inspect for reasons other than encryption, such as corrupted files or those exceeding the specified maximum archive depth. By default, this setting is enabled in the "Advanced" section of the File Policy.

Action Required: Review the file policy settings and enable the "Block Uninspectable Archives" option to enhance security and ensure optimal system performance.

Allow rule configured without an associated Intrusion or File policy

Requires review

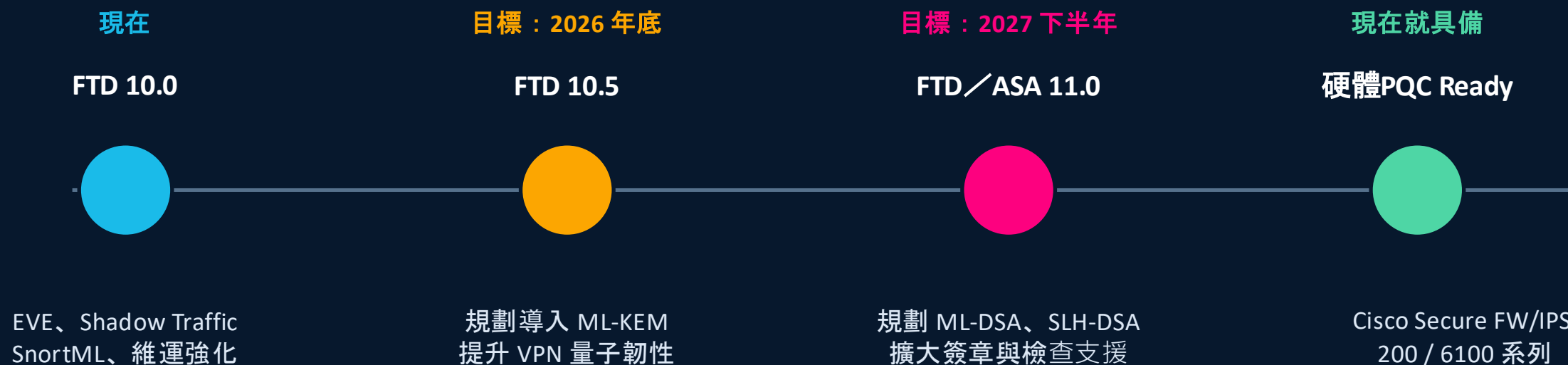
Informational

Potential Misconfiguration

The Access Control Policy on this device is configured with one or more access control rules that are set to an action of "Allow" without the addition of an Intrusion or File Policy.

If the intent is to exclude the matching traffic from inspection, the rule should either be changed to an action of "Trust" and moved towards the top of the policy, or moved into the Pre-filter policy with an action of "Fastpath".

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
Decept · Mutiny Fuzzer · File2pcap · Re2Pcap

8

惡意程式 / 簽章 / 解密

PE-Sig · BASS · MBR Filter · PyLocky Decryptor
TeslaCrypt Decryption Tool · Thanatos Decryptor · LockyDump · Flokibot Tools

8

逆向 / 漏洞研究 / 保護

FIRST · Dynamic Data Resolver · Moflow · FreeSentry
ROPMEMU · PyREBox · GhIDA · IDA Pro TileGX Plugin

1

建置 / 依賴自動化

Mussels

GitHub footprint | 77 repos

77

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」

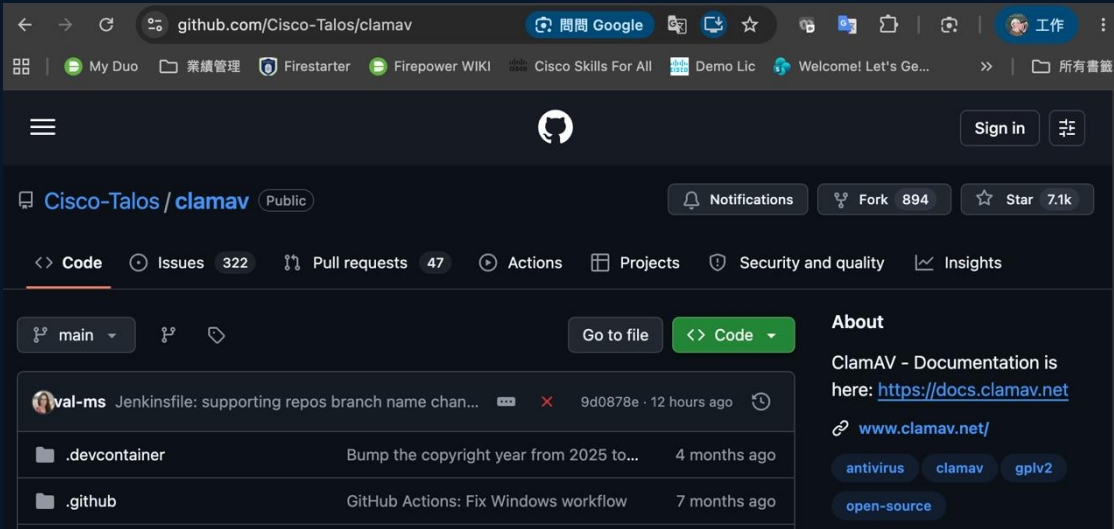
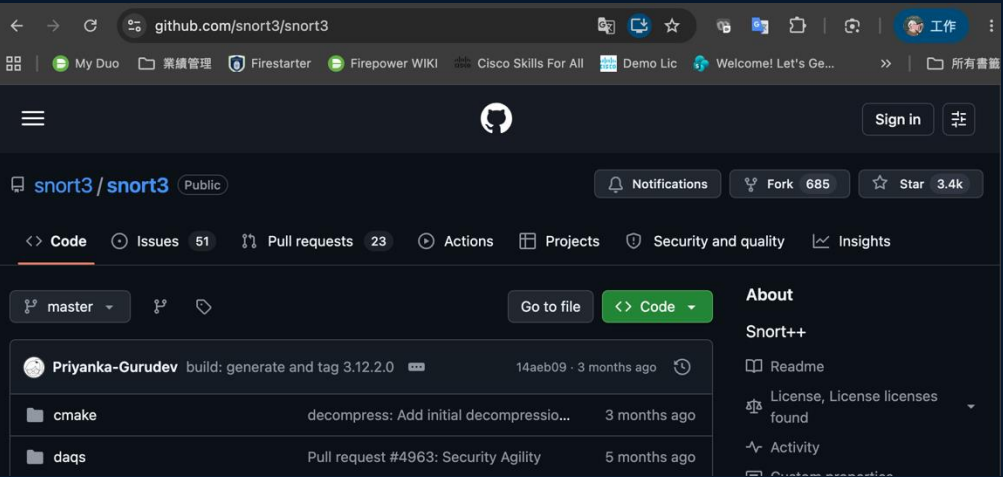
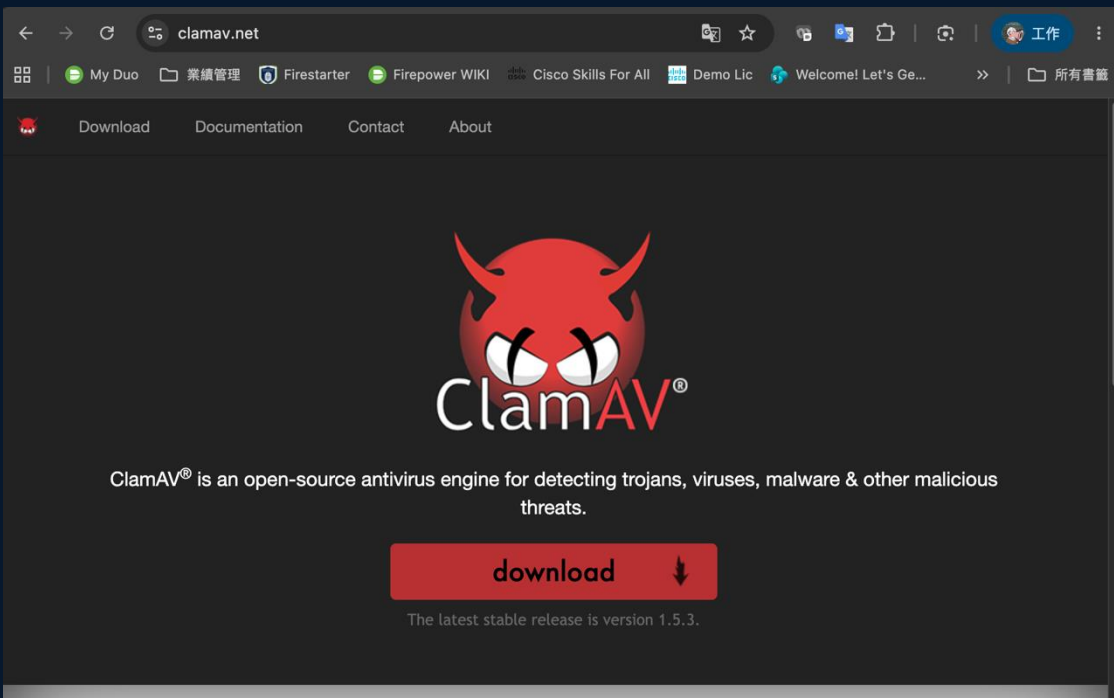
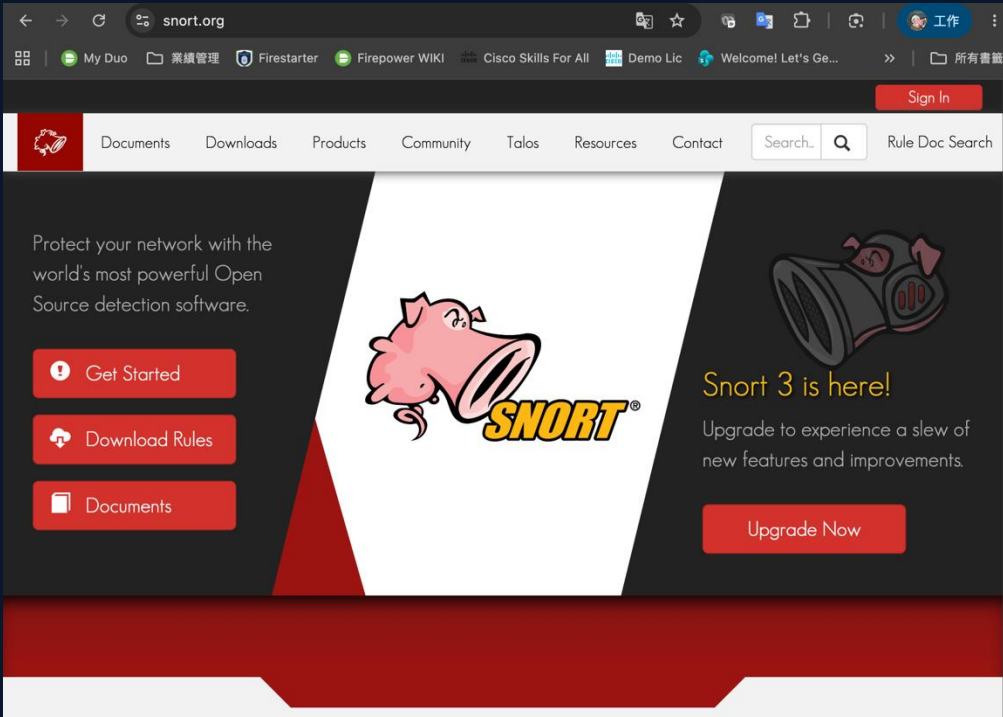
repository 可能是文件、套件、研究 PoC、fork 或歷史工具；未封存也不等於有維護 SLA。

Snort >450K systems

ClamAV >18M installs

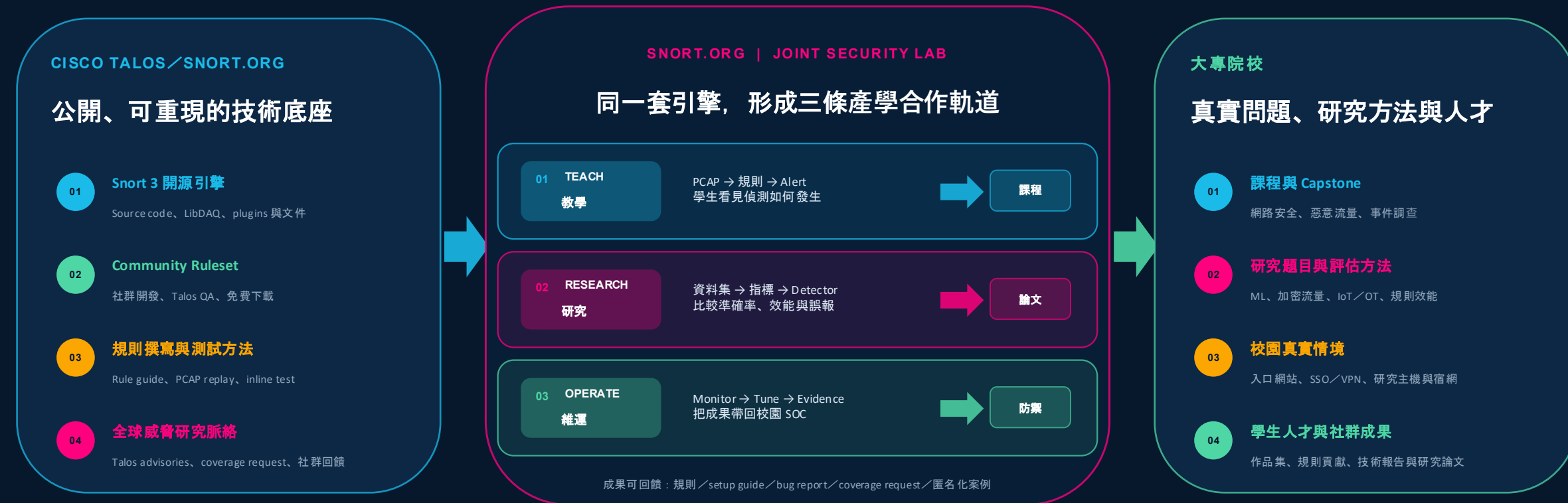
口徑：2=Talos 明確稱為「our open-source」的旗艦引擎 / 社群；26=Talos 官方工具目錄；77=Cisco-Talos GitHub org API (2026-07-31) · SpamCop / SenderBase 為服務或情報社群，不列為開源程式專案。

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。



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



思科參訪回饋問卷

研討會圓滿結束

感謝您今日參與！

作為後續規劃與辦理活動參考，還請
您協助填寫本次問卷，您所提供的寶
貴建議，我們會虛心接受並加以精進，
只為創造更好的研討會品質！



中華民國大專校院資訊服務協會
Information Service Association of Chinese Colleges