

網管經驗分享

中國科技大學 網路組

陳世賢

2024/06/27

防火牆設定

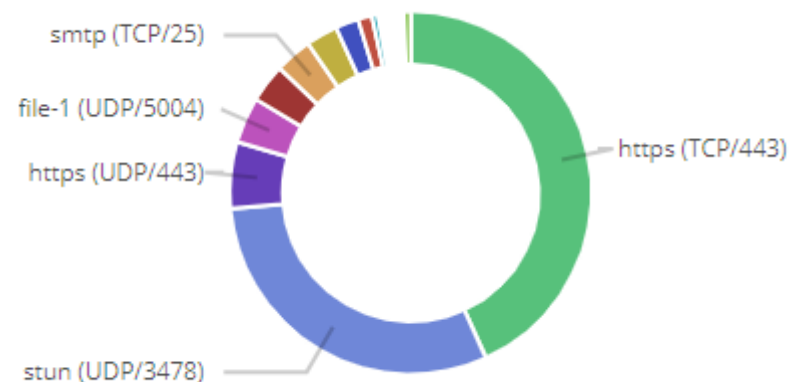
- 對外網路服務port太多，許多網路服務刻意避開傳統port number 服務方式，改用443,53port 加上封包加密機制，難以進行監控，中國科大 80/443 平時封包佔比約八成

- 建議整體關掉的網路服務..

TELNET、FTP、SSH、RDP

均改由VPN內網認證後服務

網芳早就全面封鎖就不提了..



建議這些也應該封鎖

- WinRM (5985,5986) – 以前版本win server內建開啟..
- VNC (5900) – Mac電腦開啟無帳號可暴力破解..
- Redis(6379) – 老是外面暴力試，關掉安靜些..
- Rsync(873) – 為什麼有這個?? 使用者都不知道...外面打得很開心..
- **Printer (IPP/631、LPD/515、SLP/3658、Discovery/5357-8、Bonjour/6330)**


















印表機預設開啟服務，直接變成網路伺服器了...

資安預警事件!! 都先關掉80,443了!!

- 開放HTTP、DNS、Mail之後，再考慮鎖國...
 - 私校對國外不用太多服務...僅供參考...



IoT的問題...電腦教室內的一台小米攝影機

2 minutes ago	10.80.79.200	 220.181.38.251		Ping	✓ 84 B / 84 B
2 minutes ago	10.80.79.200	 220.181.38.251		Ping	✓ 84 B / 84 B
2 minutes ago	10.80.79.200	 161.117.194.68	443	HTTPS...	✓ 26.25 kB / 16.96 kB
3 minutes ago	10.80.79.200	 47.241.62.86	10001		✓ 19.64 kB / 5.02 kB
3 minutes ago	10.80.79.200	 47.241.183.6	10001		✓ 19.64 kB / 5.02 kB
3 minutes ago	10.80.79.200	 47.241.11.101	10001		✓ 19.64 kB / 5.02 kB
3 minutes ago	10.80.79.200	 47.241.31.191	10001		✓ 19.61 kB / 5.02 kB
3 minutes ago	10.80.79.200	 47.241.171.174	10001		✓ 19.61 kB / 5.02 kB
3 minutes ago	10.80.79.200	 47.241.4.35	10001		✓ 19.61 kB / 5.02 kB
3 minutes ago	10.80.79.200	 161.117.194.68	443	HTTPS...	✓ 26.23 kB / 17.85 kB
3 minutes ago	10.80.79.200	 220.181.38.251		Ping	✓ 84 B / 0 B
3 minutes ago	10.80.79.200	 220.181.38.148		Ping	✓ 84 B / 84 B
3 minutes ago	10.80.79.200	 168.95.1.1	53	DNS	✓ 4.25 kB / 6.84 kB
4 minutes ago	10.80.79.200	 220.181.38.251		Ping	✓ 84 B / 84 B
4 minutes ago	10.80.79.200	 220.181.38.148		Ping	✓ 84 B / 84 B
5 minutes ago	10.80.79.200	 47.241.183.6	10001		✓ 18.61 kB / 4.75 kB
5 minutes ago	10.80.79.200	 47.241.11.101	10001		✓ 18.61 kB / 4.75 kB
5 minutes ago	10.80.79.200	47.241.62.86	10001		✓ 18.61 kB / 4.75 kB

校內IoT設備連出去外面伺服器

建議封鎖 Inside → Outside部份

- MQTT (TCP 1883)
- WebCam (TCP 6011、32110)
- MI-Cam (UDP 10001) ---- 擋下去, 小米攝影機會失效哦!!
- 現在CN製品的webcam都刻意避開防火牆，要找出來很花眼力...

防火牆的新要求...C2 黑名單

- 依據27001:2022版要求

A.5.7 威脅情資(Threat intelligence)

控制措施

應蒐集並分析與資訊安全威脅相關之資訊，以產生威脅情資

目的

提供對組織威脅環境之認知，以便採取適切的減緩措施

實務指引

- 蒐集(例如CERT、ISAC、CVE)並分析有關既有或新出現威脅之資訊，以防止或降低威脅對組織造成傷害與衝擊(例如作為防火牆、IDS/IPS之輸入)

- 結果是....有新要求，就是有新商機!!!
- 無法即時取得最新技服C2黑名單，只能先自力救濟...

分享社群即時Blocklist collection

- <https://firebog.net/>
 - 設定請小心，IP數量太大會吃效能，web的DN過濾封鎖很吃效能..
 - Firehole名單有名氣，但是會封鎖private IP 如有需要使用前先避開..
 - https://iplists.firehol.org/files/firehol_level1.netset (L1擋很大)
- PRI1 Feeds - IP
 - Talos_BL <http://www.talosintelligence.com/documents/ip-blacklist>
 - ET_Block <https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt>
 - Abuse_SSLBL <https://sslbl.abuse.ch/blacklist/sslipblacklist.txt>
 - CINS_army <https://cinsarmy.com/list/ci-badguys.txt> (IP多，部份FW使用)
- DN
 - Prigent_Malware <https://v.firebog.net/hosts/Prigent-Malware.txt>
 - Prigent_Crypto <https://v.firebog.net/hosts/Prigent-Crypto.txt>

其他屬於商業領域...

情資交換與分析ISAC解決方案

- 符合標準的自動化情資交換分享能力
- 主動式聯防派送，統一納管多種品牌防火牆，於收到情資的第一時間進行阻擋防禦
- 自動接收並彙總各 ISAC 及中華資安國際提供之高品質惡意中繼站黑名單
- 提供黑名單訂閱功能，符合各場域應用情境

主動聯防派送

接收威脅情資後，如何快速進行聯防至為重要。本平台可自動接收彙總各 ISAC 及中華資安單，亦可自動抽取情資內容提及的惡意IP位址，快速加入自訂黑名單中。

管理者可選擇全自動或是手動一鍵快速派送黑名單至支援的聯防設備。若聯防設備具備讀取供黑名單訂閱服務，以符合各場域應用情境。

聯絡我們



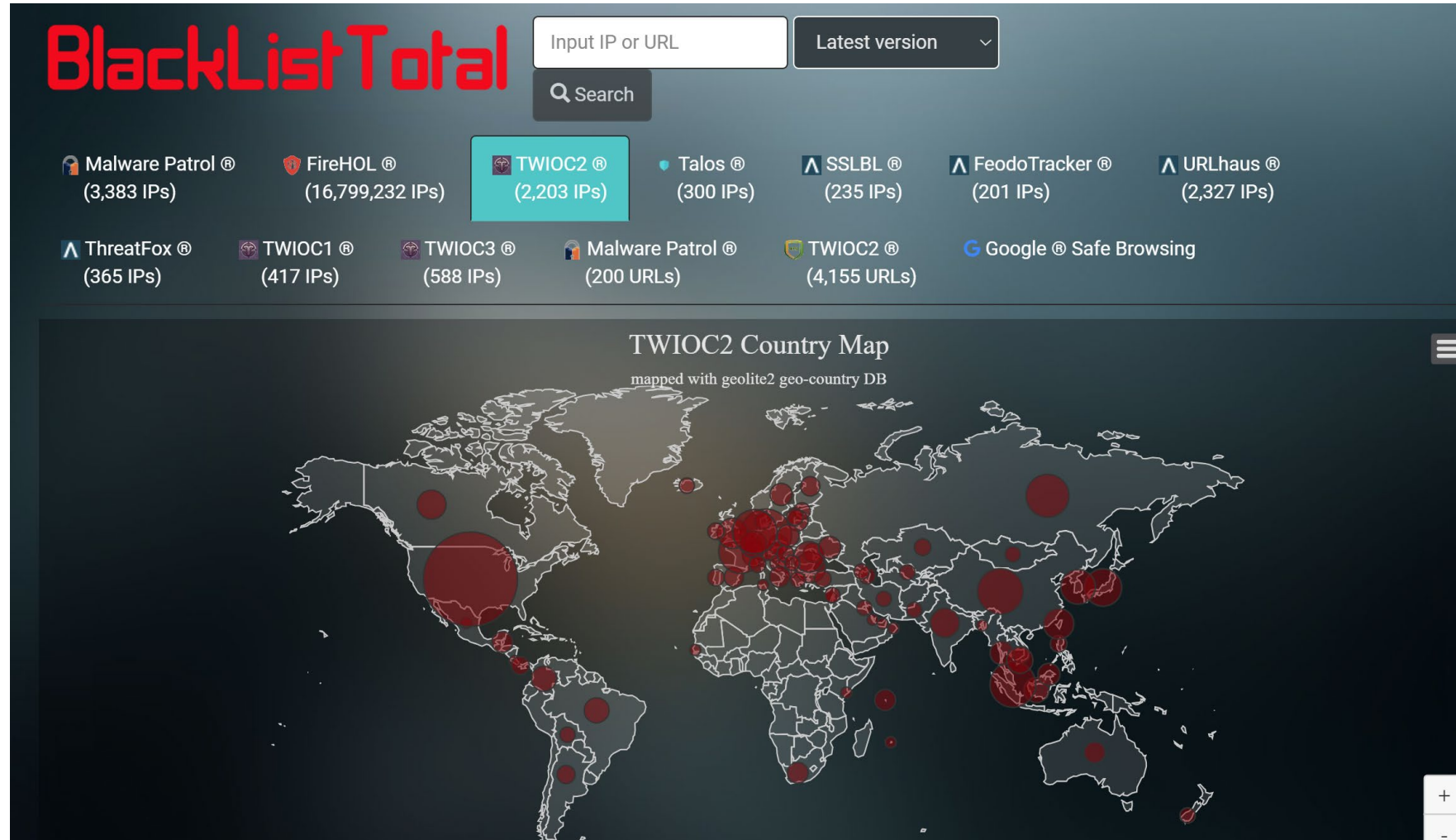
威脅情資 (threat intelligence) 指的是與網路攻擊相關的資訊，經由專業團隊收集、轉換、分析、解釋等處理過程，提供資安決策過程所需要的基礎。

ISO 27001: 2022 之「A.5.7 Threat intelligence」控制措施建議企業與組織應收集、分析資訊安全威脅相關之資訊，以產生威脅情資，並確定企業將可能面臨哪些威脅，與進一步採取防禦措施。

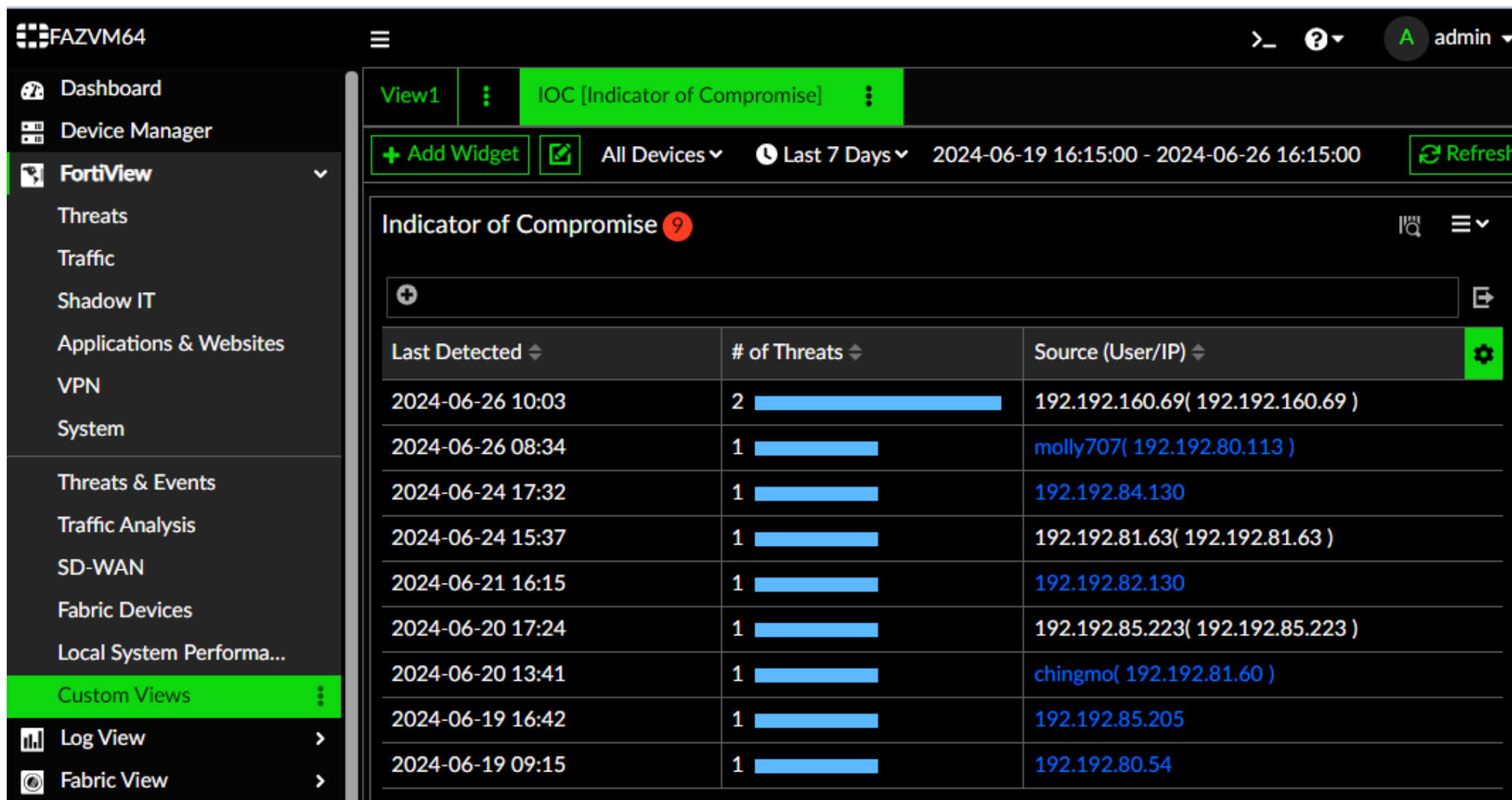
為了遵守此項要求，企業與組織應執行下列事項：

- 定期檢查企業所處的威脅環境（藉由查看政府機構和其他組織的報告達成）。
- 應確定威脅來源（如：內部人員、競爭對手、犯罪者、恐怖組織）。
- 根據當前事件和過去的事件，確定可能的新型攻擊面向和趨勢。
- 建立有助於減輕企業組織的資訊安全威脅之防禦措施。

某業者平台看來有提供技服C2..



有商機，設備商也來湊一腳...



The screenshot displays the FortiView interface for monitoring Indicators of Compromise (IOC). The left sidebar shows navigation options like Dashboard, Device Manager, and FortiView. The main content area is titled 'Indicator of Compromise' and shows a table of detected threats. The table has three columns: 'Last Detected', '# of Threats', and 'Source (User/IP)'. Each row includes a timestamp, a count of threats with a corresponding blue bar chart, and the source information. A search bar and a refresh button are also visible at the top of the table area.

Last Detected	# of Threats	Source (User/IP)
2024-06-26 10:03	2	192.192.160.69(192.192.160.69)
2024-06-26 08:34	1	molly707(192.192.80.113)
2024-06-24 17:32	1	192.192.84.130
2024-06-24 15:37	1	192.192.81.63(192.192.81.63)
2024-06-21 16:15	1	192.192.82.130
2024-06-20 17:24	1	192.192.85.223(192.192.85.223)
2024-06-20 13:41	1	chingmo(192.192.81.60)
2024-06-19 16:42	1	192.192.85.205
2024-06-19 09:15	1	192.192.80.54

明明已經有黑名單，又要搞個IOC (感染指標)

The screenshot displays the Fortinet FortiGuard interface for an Indicator of Compromise (IOC). The main header shows the IP address 91.195.240.123:443. A circular gauge indicates a risk level of 100, labeled as 'High Risk'. Below this, several tags are listed: 'BumbleBee C2', 'DGA', and 'Malware CnC'. A 'FortiGuard Live Rating' section shows 'WebFilter: Malicious Websites' and 'IOC: Malware CnC'. The 'Insights' section provides details for the ASN 47846 SEDO-AS (SEDO GmbH) in Munich, Bavaria, Germany, and includes a navigation bar for Recon, Weaponization, Delivery, Exploitation, Installation, and C&C. It also shows a Reputation Rating of 1, Version 8, and ID 207. Two risk profiles are displayed: a 30 Day Domain Hosting Risk Profile with an Average Risk of 90 and 7,714 total domains, and a 30 Day Domain Parental Control Profile with 56 total PC domains. The 'Events' section on the right lists creation and update dates. At the bottom, the 'Indicator List' tab is active, showing a table of indicators.

Type	Title	Confidence	Stages Seen	Related Objects	Created on
IP	91.195.240.123:80 FormBook C2 Malware CnC	High	Command & Control	1	2023-06-27 02:11:19
IP	91.195.240.123:443 BumbleBee C2 DGA Malware CnC	High	Command & Control	1	2023-12-02 10:24:05

<https://ioc.fortiguard.com/>

自行註冊輸入IP比對是否存在

- END -