



SecuTex Network Protection

先進資安威脅防禦系統



資安環境說明

The collage features several news snippets:

- 福斯汽車 Volkswagen 供應商 資料庫 資料外洩 個資外洩**: 福斯汽車宣佈稱是合作廠商將未做好安全防護的資料庫放上網路，才導致用戶資料外洩，時間點從2019年8月到2021年5月。 (2021-06-14)
- 麥當勞驚傳全球系統遭駭，臺、韓部分歡樂送資料外洩，臺灣麥當勞表示將通知受影響者，並提醒慎防詐騙**: 麥當勞全球網路系統在11日傳出遭未經授... (2021-04-08)
- 駭客賤賣價值近4千萬美元的禮物卡資料，疑自禮物卡交易網站竊得**: 威脅情報公司Gemini Advisory發現駭客在俄羅斯論壇上出售近90萬張、價值3,800萬美元的禮物卡資料，隨後又賣出... (2021-04-08)
- Have I Been Pwned開放外界以電話號碼查詢是否被臉書外洩個資**: 揭露臉書2019年高達5億筆資料外洩事件的資安業者Hudson Rock則表示，有107萬名用戶受害，臺灣地區有70多萬名... (2021-04-07)
- 富士通代管平臺被駭，影響眾多日本政府單位**: 駭客攻擊富士通代管的ProjectWEB專案資訊共享平臺，導致日本國土交通省、外務省等使用單位資料外洩... (2021-05-28)
- Line宣布將召開資料治理委員會，以進行後續相關處理**: 日本Line上傳傳出資料外洩，母公司Z Holding預計於3月23日舉辦第一次資料治理委員會，並公布將會報告核實結果... (2021-03-22)
- 美國起訴外洩微軟、英特爾、Adobe與監控業者Verkada機密資訊的21歲瑞士駭客**: 根據美國司法部訴狀，瑞士人Tillie Kottmann參與了眾多的駭客事件，過去2年間與同夥駭進數十家企業及美國政府... (2021-08-16)
- 客正在兜售來自T-Mobile的1億用戶資料**: 其他board證實T-Mobile大量用戶資料確流入地下論壇，對此T-Mobile正調查這起資料外洩原因... (2021-08-16)
- 歐盟將調查臉書5.3億用戶資料外洩**: 影響5億多名臉書用戶，最早追溯到2017年、近來更被免費公開於駭客論壇的臉書資料外洩事件，歐盟資料保護委員會決定... (2021-04-07)
- 審判官裁定：駭客、電腦詐欺、網路犯罪、英特爾、微軟、adobe、聯發科、Verkada | 資料外洩**
- 烏地阿拉伯國家石油公司資料外洩，1TB資料在市叫賣**: 據發現駭客在暗網兜售Saudi Aramco公司內部資料，這間沙國公營石油業者宣稱是供應商安全缺失，導致該公司資料外洩... (2021-08-16)
- THIS DOMAIN HAS BEEN SEIZED**: The domain for WELKAM.NB has been seized by the Federal Bureau of Investigation pursuant to a seizure order.
- VERKADA**: A screenshot of the Verkada website showing a security alert.

資料外洩事件頻傳



美國財政部 | 勒索軟體 | 洗錢 | 加密貨幣交易
 中心 | Suex | 黑色產業鏈

美國制裁幫勒索軟體駭客 洗錢的加密貨幣交易中心 Suex

根據美國政府以及華爾街日報的資訊，公司及成員位於東歐的Suex，是墨西哥當地知名的加密貨幣交易中心，至少協助8
 2021-09-22



New Cooperative | 農業 | 合作社 | 勒索軟體
 | BlackMatter | Darkside | 資安 | 網路攻擊

美國穀物合作社New Cooperative遭 BlackMatter攻擊，被勒索 590萬美元

美國愛荷華州的穀物合作社New Cooperative遭到勒索軟體攻擊，犯案的
 2021-09-21



Windows MSHTML漏洞 | 勒索軟體 |
 CVE-2021-40444 | 資安 | 修補 | Patch
 Tuesday

微軟：Windows MSHTML漏洞已有勒索軟體 開採

微軟在8月已經偵測到數個攻擊行動開採MSHTML引擎中的CVE-2021-40444漏洞，透過惡意Office文件散布勒索軟體
 2021-09-17



Olympus | BlackMatter | 網路攻擊 | 資安
 事件 | 勒索軟體 | 資安

相機大廠Olympus疑遭勒索 軟體BlackMatter攻擊

Olympus坦承在9月8日發生網路安全事件，影響該公司位於東歐、中東及非洲
 (EMEA) 據點的IT系統
 2021-09-16



2022 iThome臺灣雲端大會 敬候啟動！ 推薦報名獎券大會再抽 HomePod mini SRE

新聞 華碩子公司NAS設備遭DeadBolt勒索軟體攻擊

華碩集團旗下華芸科技 (Asustor) NAS設備遭DeadBolt勒索軟體攻擊，官方發出公告，呼籲遭攻擊用戶立即
 拔除乙太網路連線，長按電源鍵關閉NAS，同時不要啟動NAS以免資料被刪除，並聯絡華芸提供技術支援
 文/ 林妍潔 | 2022-02-23 發表 324



資安 | 供應鏈 | 目標式攻擊 | 零信任 | 勒索
 軟體 | iThome 2021臺灣資安年鑑

【資安教戰守則：因應雙 重勒索之道】目標式攻擊 瞄準供應鏈脆弱環節，該 如何因應？

發展已久的目標式攻擊，儼然讓駭客的勒索敲詐行徑取得更有效且豐碩的成果，而由於SolarWinds事件所引發出供應鏈
 2021-05-28



conti | FBI | 攻擊指標 | 勒索軟體 | 勒索攻擊
 | 醫療 | 政府 | 美國

FBI警告：美國占Conti全 球受害單位一半以上，公 布感染指標

FBI發現駭客對美國的行政、醫療與警消單位頻繁發動Conti勒索軟體攻擊，當地受害組織數更居全球之首，因此公布
 2021-05-26



愛爾蘭健康服務管理署 | HSE | conti | 勒索
 軟體 | 資安 | 雙重勒索

攻擊愛爾蘭健康服務管理 署的駭客要詐，給解密金 鑰後仍威脅出售民眾個資

遭到勒索軟體攻擊的愛爾蘭健康服務管理署 (HSE) 雖然獲得解密金鑰，但狡猾的駭客仍然以盜走內部資料為要脅，試圖迫
 2021-05-21

美國物流公司Expeditors遭勒索軟體攻擊，全 球營運受波及

目前無法確定系統何時恢復正常的Expeditors，坦言這次網路攻擊事件恐嚴重衝擊其業務及營收

文/ 陳穎莉 | 2022-02-22 發表 69



遭
 運

與勒索
 駭客鎖
 定了泰
 1-05-17

Appointment and service updates - HSE IT system cyber attack

There has been a ransomware attack on our IT systems. We have shut them down as a precaution.
 This has caused some disruption to our services. Most healthcare appointments will get ahead as planned but a few appointments are being affected.
 We will keep this page updated to let you know about any changes to our service.

資安 | 勒索軟體 | 愛爾蘭健康服務管理署 |
 Health Service Executive | HSE

愛爾蘭健康服務管理署遭 「重大」勒索軟體攻擊

愛爾蘭健康服務管理署 (Health Service Executive, HSE) 因遭勒索攻擊，關閉所有IT系統並切斷網路，有媒體指出，
 2021-05-17

勒索軟體盛行，產業哀鴻遍野

資安威脅日增

- COVID-19疫情造成工作方式改變，企業開放網路邊界讓員工WFH，開放意味著更多的風險
 - 當發生資安事件時，企業想在短時間之內了解的事：



駭客如何入侵？

哪些主機受駭？

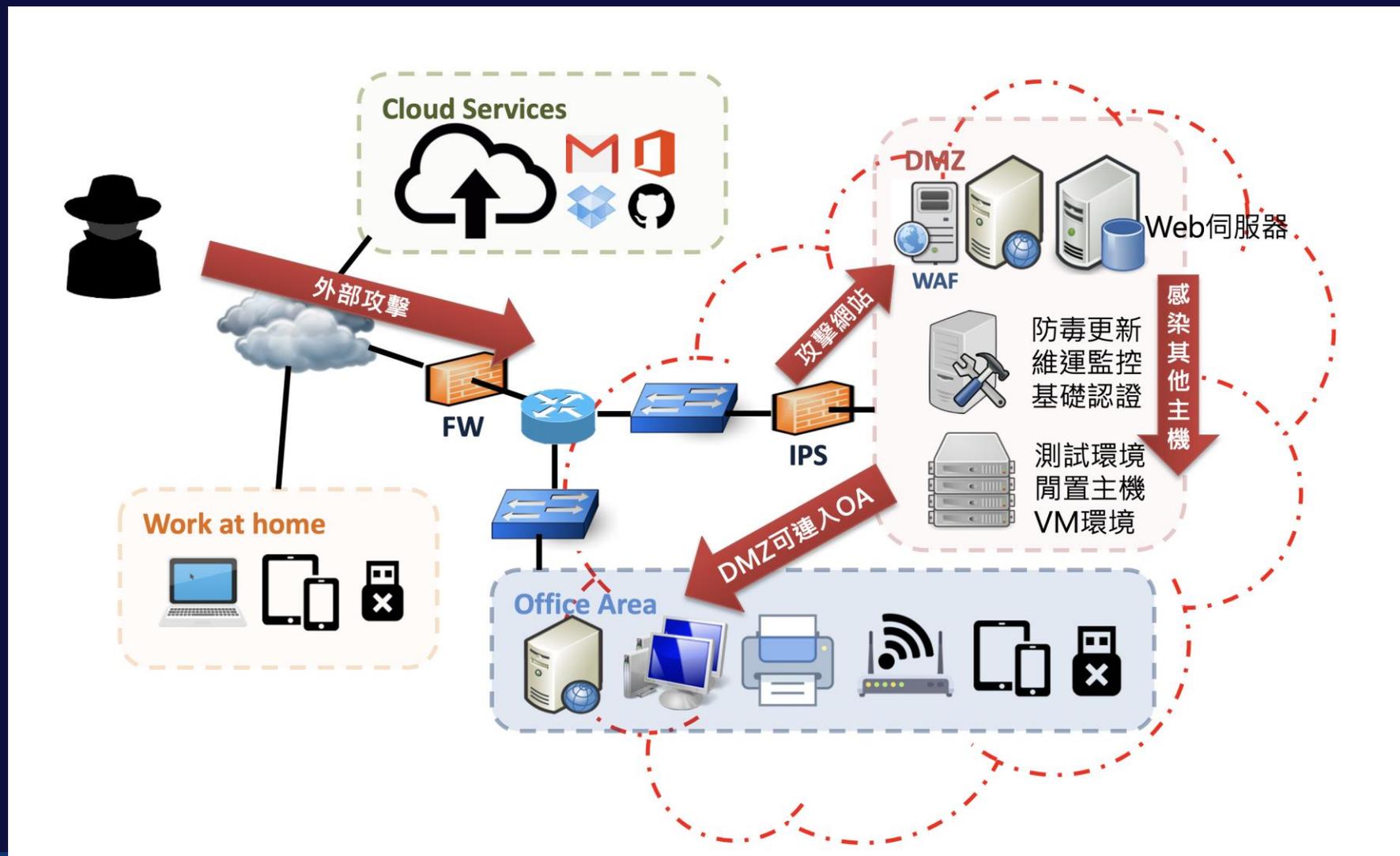
攻擊持續多久？

哪些資料外洩？



MIS要花多少時間才能回答上面的這些問題？

企業被駭客入侵時...



事件調查取證區域

當進行資安事件調查時，我們通常仰賴以下的資料來源：

防護死角/盲點

Firewall Log

大型企業可能會匯出Netflow或是Traffic log到SOC或是內部資料倉儲供調閱，但數量龐大，可能只包含Layer 3-4資訊，較不利於快速檢索

IDS/IPS Log

僅包含特徵名稱、風險等級與標的等，無法呈現具體觸發的內容，原因以及伺服器回應

Web 伺服器/OA主機 Log

保留了存取的相關軌跡，但資料量多時檢索不易，且在實務上很常日誌會因為設定、攻擊者竄改而失真或是資料遺失

Web Application Firewall Log

針對Web應用程式提供更深層的檢測與保護，但若設定不當可能無法完整保護網站

僅有資安偵測設備，無完整保留流量紀錄，難以重現攻擊內容及影響範圍



安全閘道



警衛



24小時監控錄影

- 偵測到攻擊時才開始保留證據
 - 沒有事前的證據
- 保留的證據不是Raw Data
 - Syslog 文字證據力有限
- 不同系統的證據需要時間彙整
 - 跨不同平台,無法即時同步調閱
- 端點跡證難以保留
 - 加密型或APT攻擊最後會消除攻擊足跡



SecuTex先進資安威脅防禦系統介紹

產品功能說明



全時側錄

- 封包全速抓取
- 完整封包保存

即時檢索

- 支援連結層到應用層的封包解析
- 高達300種以上的檢索條件

即時偵測

- 即時偵測異常網路行為
- 即時惡意黑名單偵測

資安聯防

- 支援CEF日誌即時匯出
- 支援在地資安威脅情資訂閱

產品優勢

SecuTex

1 **全時側錄**，保存所有payload而不只metadata

2 具備**攻擊偵測能力**，可偵測異常網路行為及惡意黑名單

3 可擔任**即時鑑識分析平台**，即時採證封包匯出

4 **最完整情資**，掌握即時國內網路威脅與第一手網軍攻擊樣本

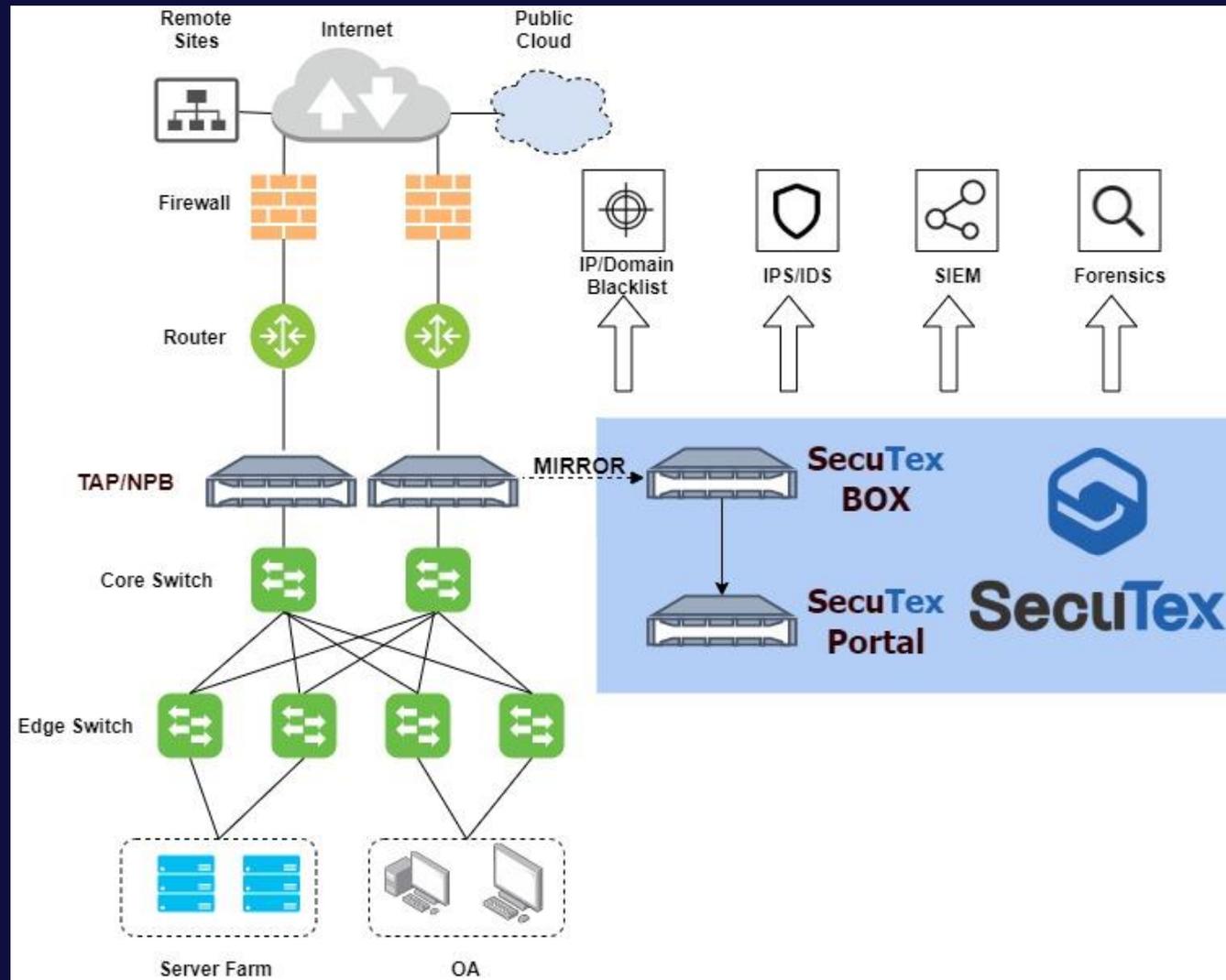
5 **SOC整合**，完整之服務流程

6 **國內自主研发團隊**，快速回應國內客戶需求

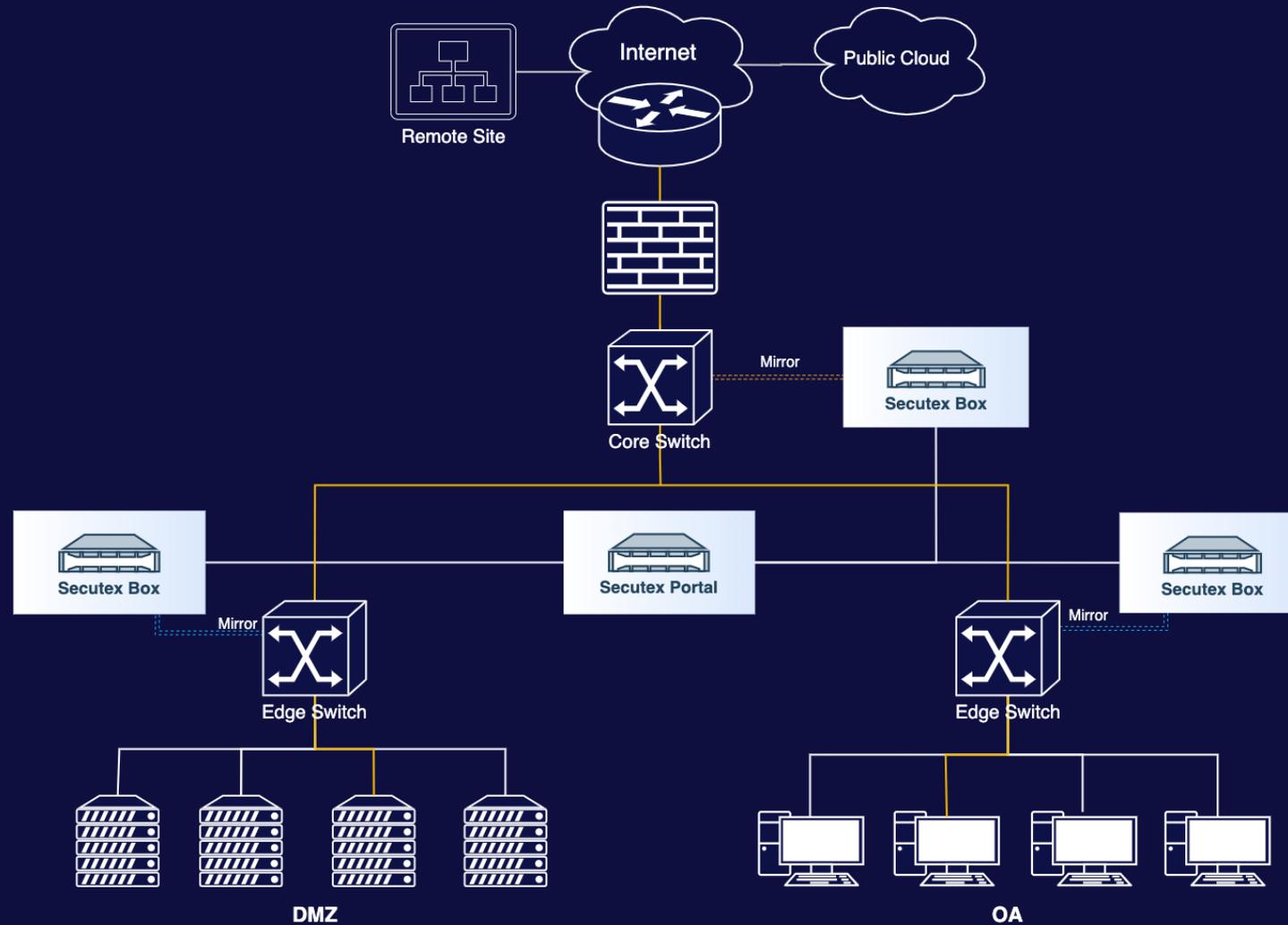


產品佈署架構

SecuTex NP – 產品架構



SecuTex NP – 部署架構示意圖 – 南北向側錄





產品介面展示

風險儀表板

- 儀表板提供視覺化的風險係數、資安地圖、告警資訊、流量資訊，使用者可以輕鬆了解一日的網路風險概況，並可通過選擇不同的日期，回溯查詢過往的風險概況資訊。



謝謝您的聆聽