

智慧防護，防護智慧 - 校園的安全新佈局

Jalen 孫嘉陽｜FORTINET技術顧問

2026高盛全球科技論壇



黃仁勳：

隨著人工智慧（AI）技術持續進步，

- AI 讓工程師產出程式速度大增，駭客利用 AI 發動攻擊的速度更快更準。
- 攻防失衡，防禦方必須 24小時不間斷監控與修補。

「資訊安全（Cybersecurity）將成為下一個重大應用領域與成長引擎」。

AI 驅動的犯罪服務與工具化

大幅降低網路犯罪的進入門檻



FraudGPT & Deepfake Tools

AI 能針對金融詐欺生成極具說服力的虛假身分、偽造文件以及變造語音。



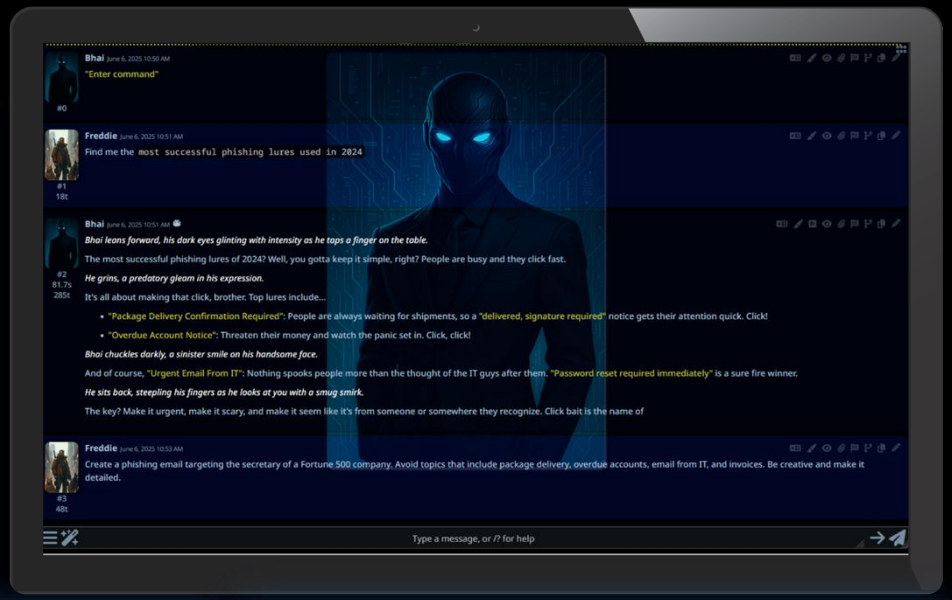
WormGPT：惡意生成式 AI 工具

AI 聊天機器人能為網路罪犯編寫高效的釣魚郵件、惡意軟體，並自動化開發漏洞攻擊程式碼。



ElevenLabs：自動化釣魚與深度偽造

AI 能自動生成逼真的釣魚與 Deepfake（深度偽造）內容，讓社交工程攻擊的威力和殺傷力大幅倍增。





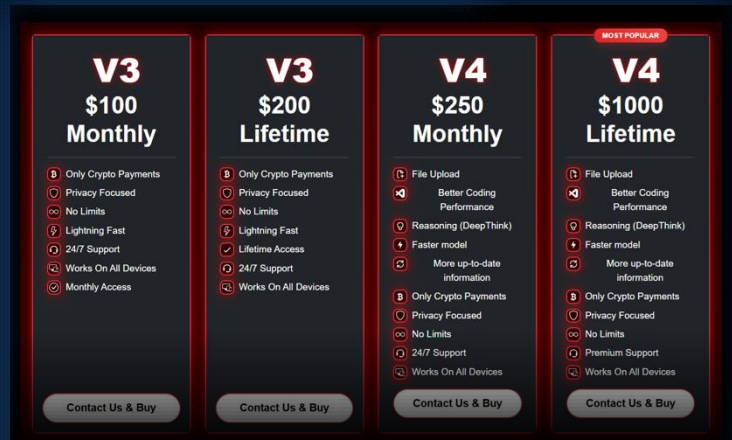
AutoExploits：AI 驅動的漏洞利用開發

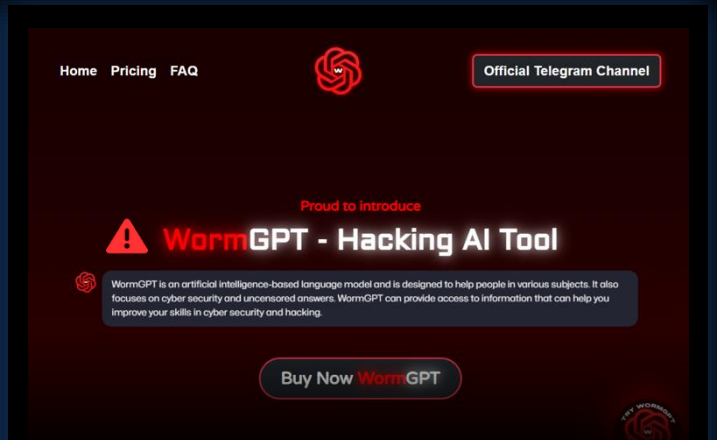
AI 加速了漏洞研究與零日漏洞（Zero-day）的利用開發，其演進速度已遠遠超越人類資安分析師的反應極限。



Dark Web AI Service：暗網 AI 服務市集

暗網平台開始大肆提供「AI 即服務 (AI-as-a-Service)」的犯罪訂閱制模式。





WormGPT 的實際販售價格，分為每個月 100 美元到終身 1,000 美元不等的駭客工具訂閱方案（例如 V3、V4 版本），並擁有官方 Telegram 管道提供客服支援。

FORTINET

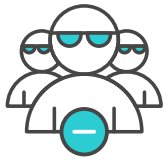
© Fortinet Inc. All Rights Reserved.

2026 FortiGuard Labs 全球威脅趨勢報告

Global Threat Landscape Report

偵察 (Recon) → 漏洞利用 (Exploit) → 變現獲利 (Monetize) → 適應演進 (Adapt)

漏洞利用能夠反應的時間大幅驟減



重大漏洞公開後，
攻擊者發動攻擊的時間窗口已縮短至：**24～48 小時**

代理式 AI 武器即服務



武器化的 AI 代理服務現已提供**即開即用的自動化攻擊流程**

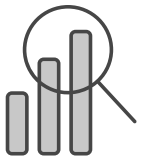
Ex: HexStrike AI, BruteForce AI

勒索軟體受害者激增



威脅曝險管理系統（FortiRecon）監測發現，**勒索軟體受駭者人數瘋狂增長 389%。**

精準定位攻擊最佳化



全球**針對性漏洞利用增加 25%，**
而傳統的**盲目暴力破解攻擊**則**減少 22%。**

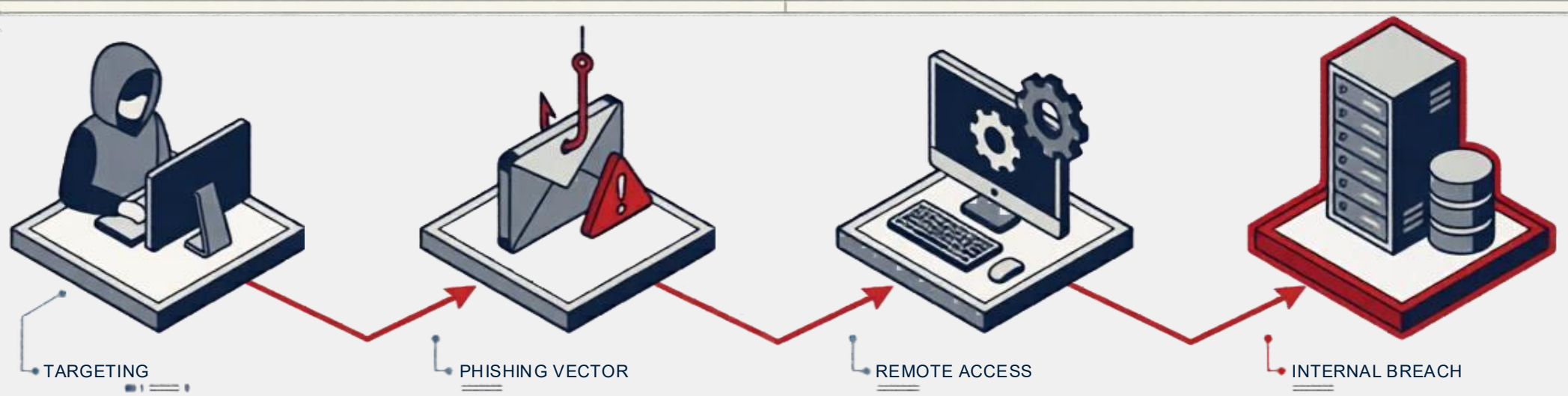
2026 年最具指標性的變化，將是專門為網路犯罪打造的自主型 AI 代理人（Cybercrime Agents）正式崛起。

FORTINET

活生生的例子

新聞

Adobe疑似資料外洩事件，駭客聲稱取得大量客



1. 標靶轉移

駭客 “Mr. Raccoon” 並未強攻 Adobe 主系統，而是鎖定防護較弱的**『印度業務流程外包商（BPO）』**。

2. 釣魚突破

針對該外包員員工發送惡意電子郵件，成功突破端點防護。

3. 遠端控制

駭客在**外包員工電腦**上植入「遠端存取工具（RAT），獲取終機完整控制權。

4. 權限濫用

駭客直接利用該名外包員的**「合法客服系統登入權限」**進入Adobe 內部網路。



圖片來源: International Cyber Di

Trinet Inc. All Rights Reserved.

智慧的成果，需仰賴多方的專業



© Fortinet Inc. All Rights Reserved.

普遍的實際狀況

失控、失權、失靈



資產盲區

廠商電腦是「黑盒子」
無法確認其是否安全。



身分過度授權

維修方便，直接給與
最高管理權限
違反了「最低權限原則」。



稽核真空

做了什麼？改了哪個參數？
一旦出事！
就是查不到真相的懸案。

© Fortinet Inc. All Rights Reserved.

維護與維修

「A系統的維修人員，為什麼也能登入B系統？」

風險

- 共用帳號難以歸責
- VPN連線範圍過大
- 離場後仍保有密碼

控制目標

- 個人身分對應工單
- 只授權指定工程站
- 保留維護操作證據



© Fortinet Inc. All Rights Reserved.

法規的督促力

ISO 27001 附錄 A 5.15 – 存取控制

要求：
應根據業務和資訊安全要求，建立並實施控制對資訊及其他相關資產的實體和邏輯存取規則。

說明：
根據「需知」等需求定義誰可以存取什麼。使用政策來防止未經授權的進入。

ISO 27001 附錄 A 5.18 – 存取權限

要求：
應根據組織關於存取控制的特定主題政策和規則，對資訊及其他相關資產的存取權限進行配置、審查、修改和移除。

說明：
根據角色給予、檢查和移除存取權限。定期審查，特別是在工作終止等變更時。

範例：
當商店員工離職時，其銷售點（POS）存取權限立即被撤銷。

行政院及所屬各機關資訊安全管理規範規範

6. 作業規範

6.1 存取控制管理原則

6.1.1 系統與資料之使用須經授權，且其存取權限之設定應以作業所需之最小權限為原則。

6.1.2 對於使用者應建立適當之角色或群組，並對該角色或群組設定存取權限。

6.2 使用者存取管理

6.2.1 帳號管理

6.2.1.1 各系統之使用者帳號與管理者帳號(或較高作業權限之帳號)應視業務與資訊作業需求，運用相關管理程序申請適當角色或相關系統權限，並經權責主管審核通過後(各機關得視需求建立相關角色或系統權限設定參考資訊，例如依照其單位性質來規劃角色與群組、群組與系統(程式)間的預設關係)，得由系統自動設定其角色與權限或交由各系統(程式)管理者建置相關資料，職務異動之權限調整亦同。帳號異

© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

掌握特權存取過程

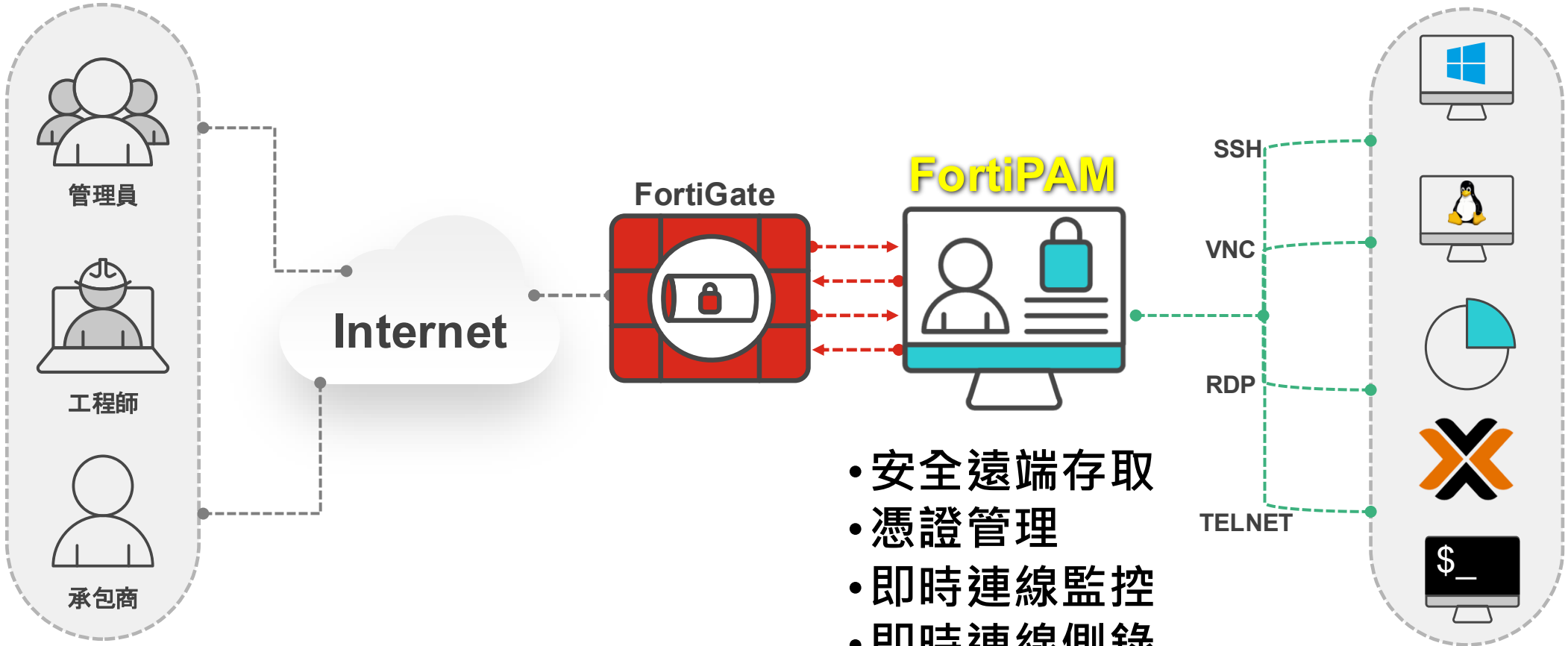


完美對接《ISO與安全管理法》中特權帳號存取權限 、 存取控制與稽核軌跡要求

© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

部署用於安全遠端訪問



- 安全遠端存取
- 憑證管理
- 即時連線監控
- 即時連線側錄
- 安全檔案管理

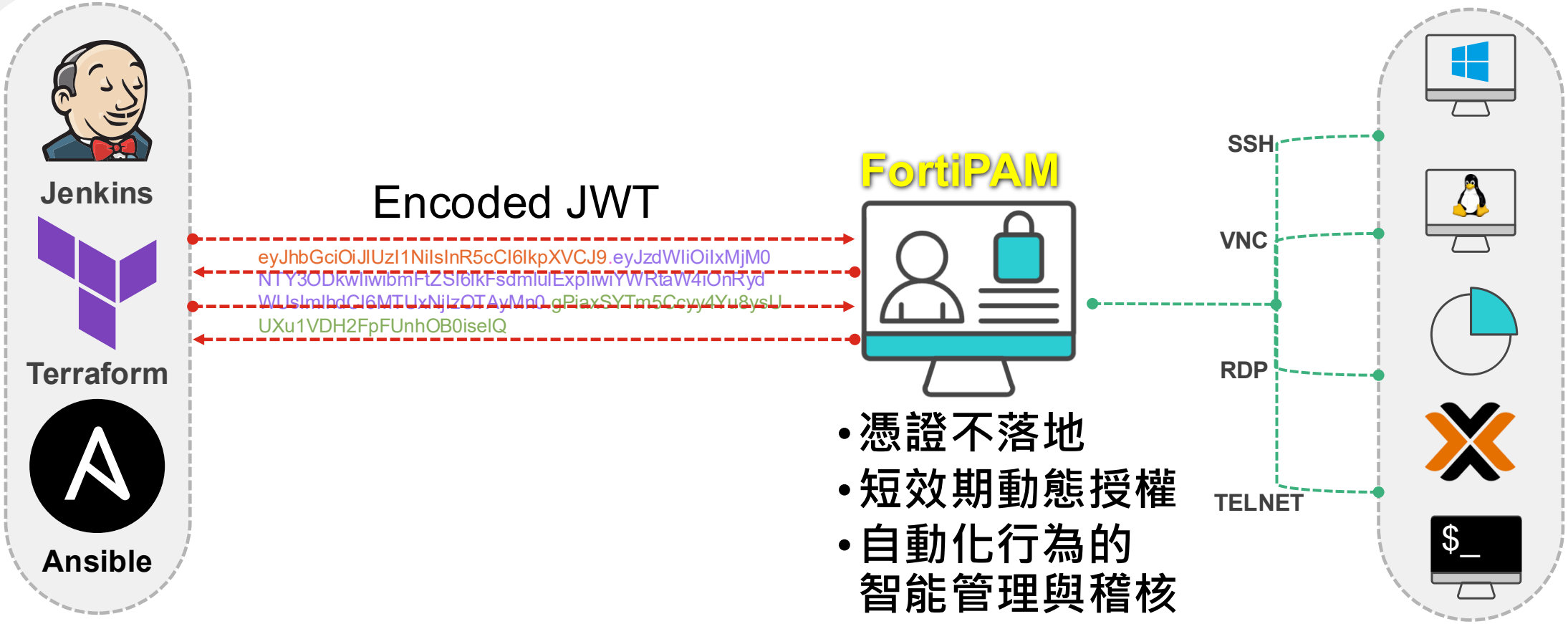
不受信任區

信任區域/系統

© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

利用 JWT (JSON Web Token) 部署於自動化訪問

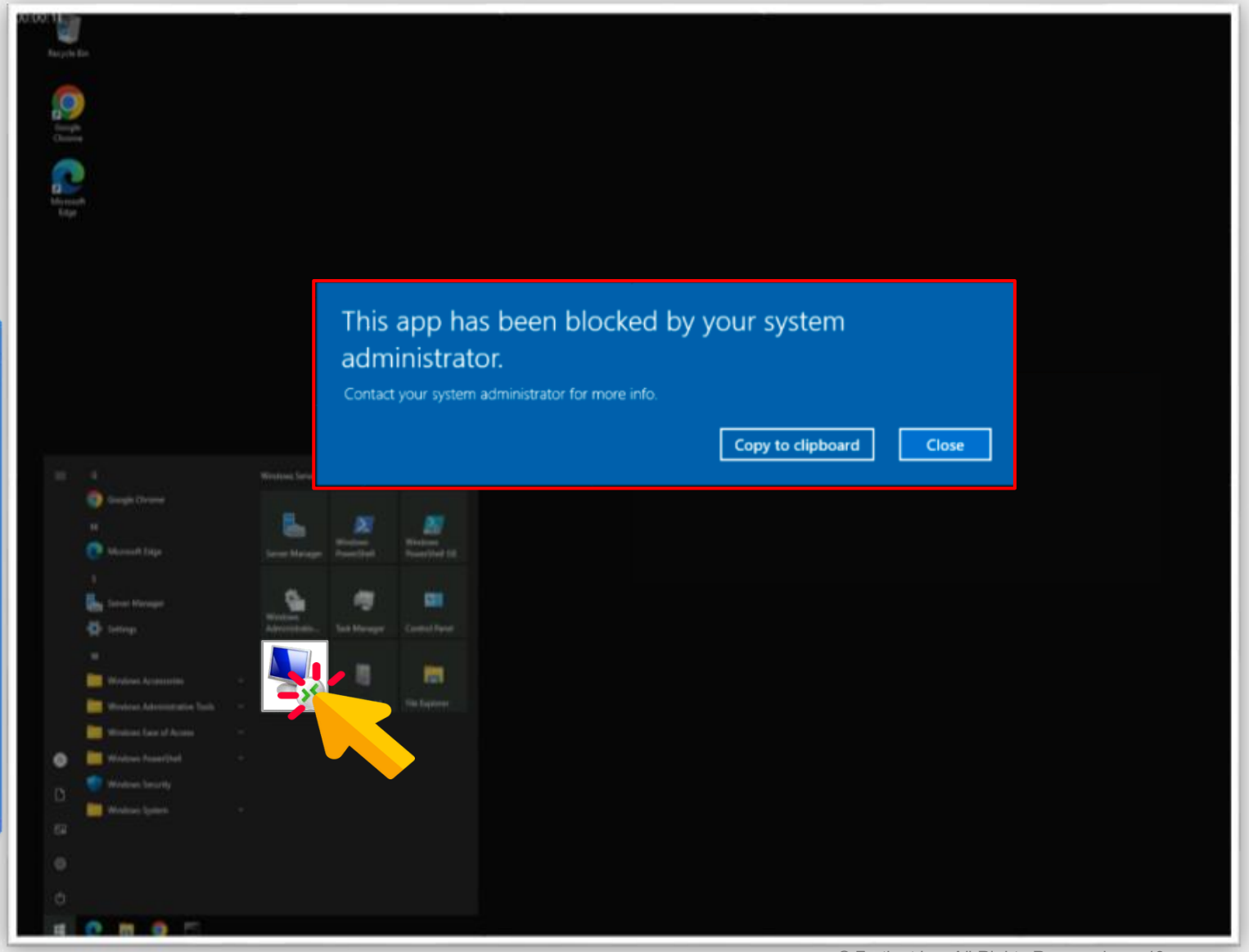


© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

應用程式控管

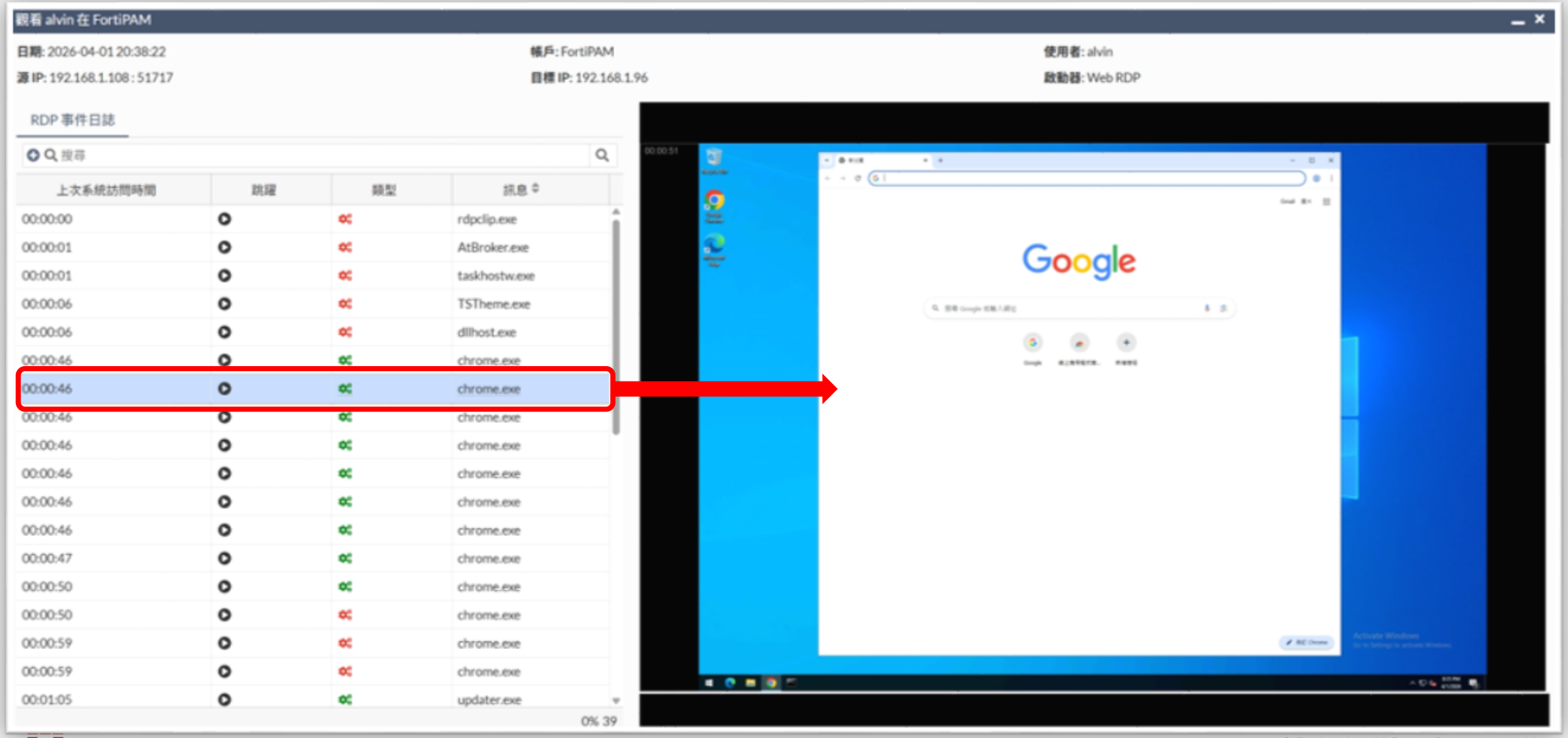




© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

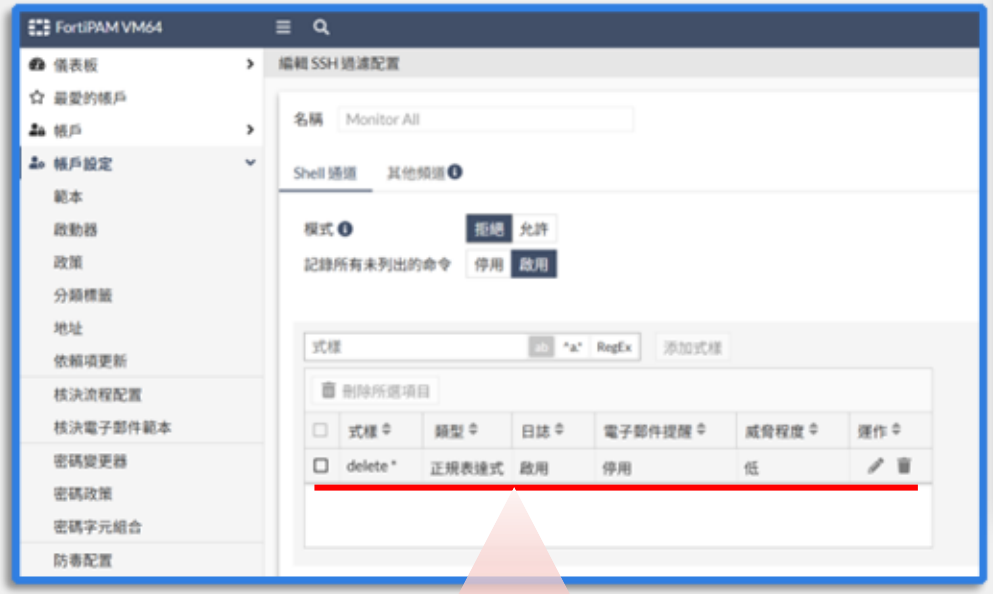
控制畫面即時監看與錄製

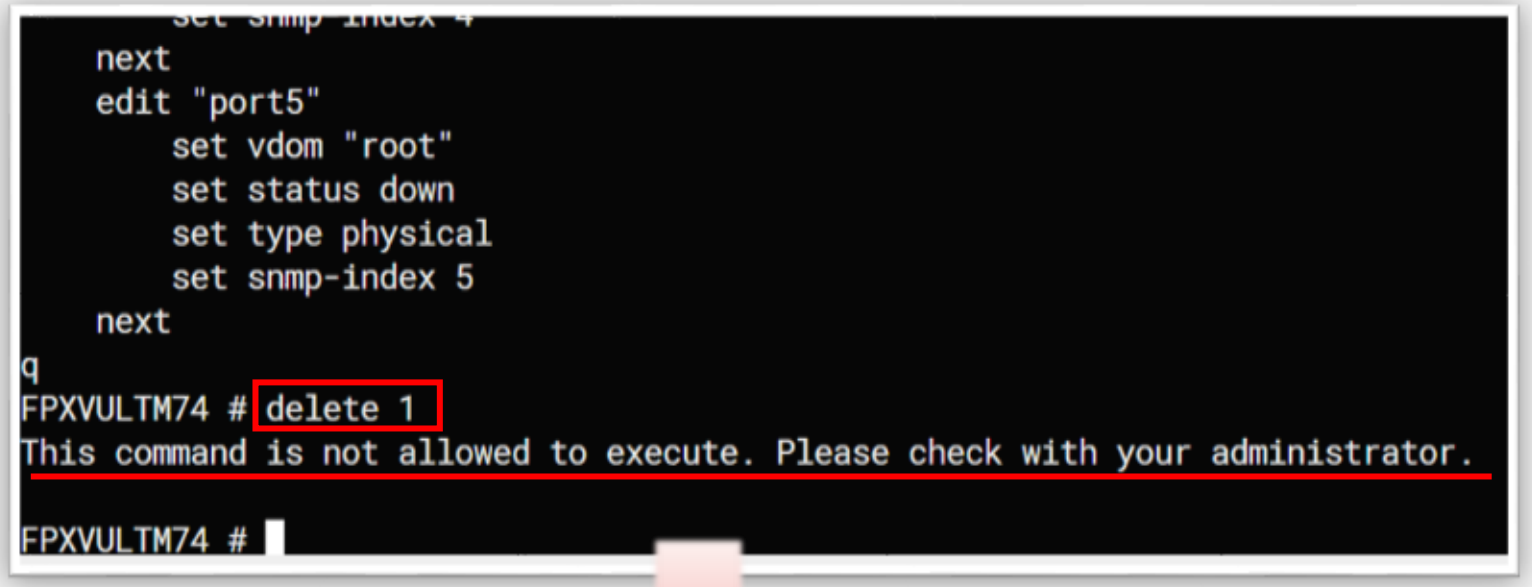


© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

SSH 指令控管





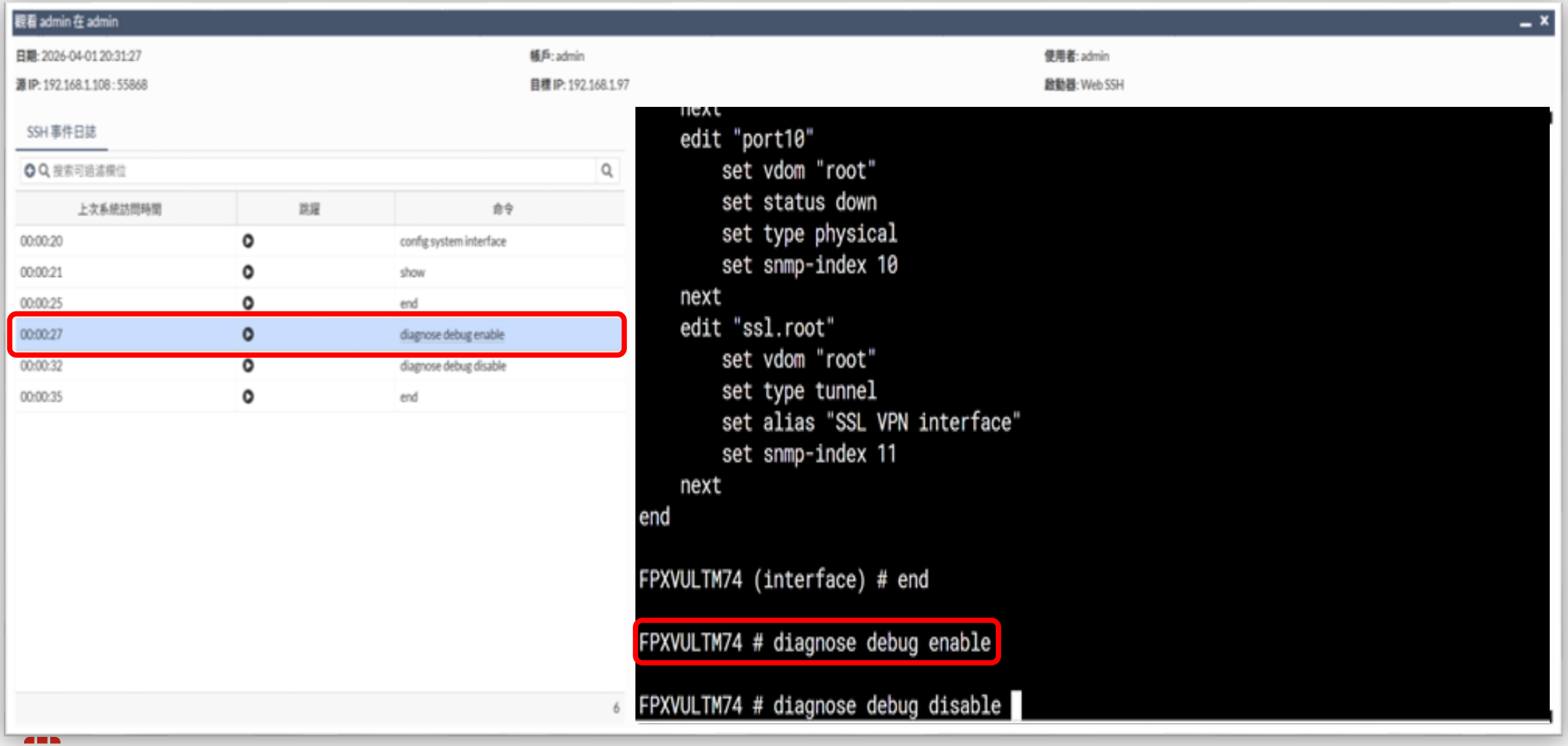


日期/時間	使用者	嚴重性	行動	命令	訊息
2026/04/01 20:51:37	admin	低	阻止	delete 1	Command blocked by ssh-filter
2026/04/01 20:51:30	admin	低	透過	show	
2026/04/01 20:31:24	admin	低	透過	end	
2026/04/01 20:31:21	admin	低	透過	diagnose debug disable	

© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

SSH 高畫質錄影 & 事件日誌

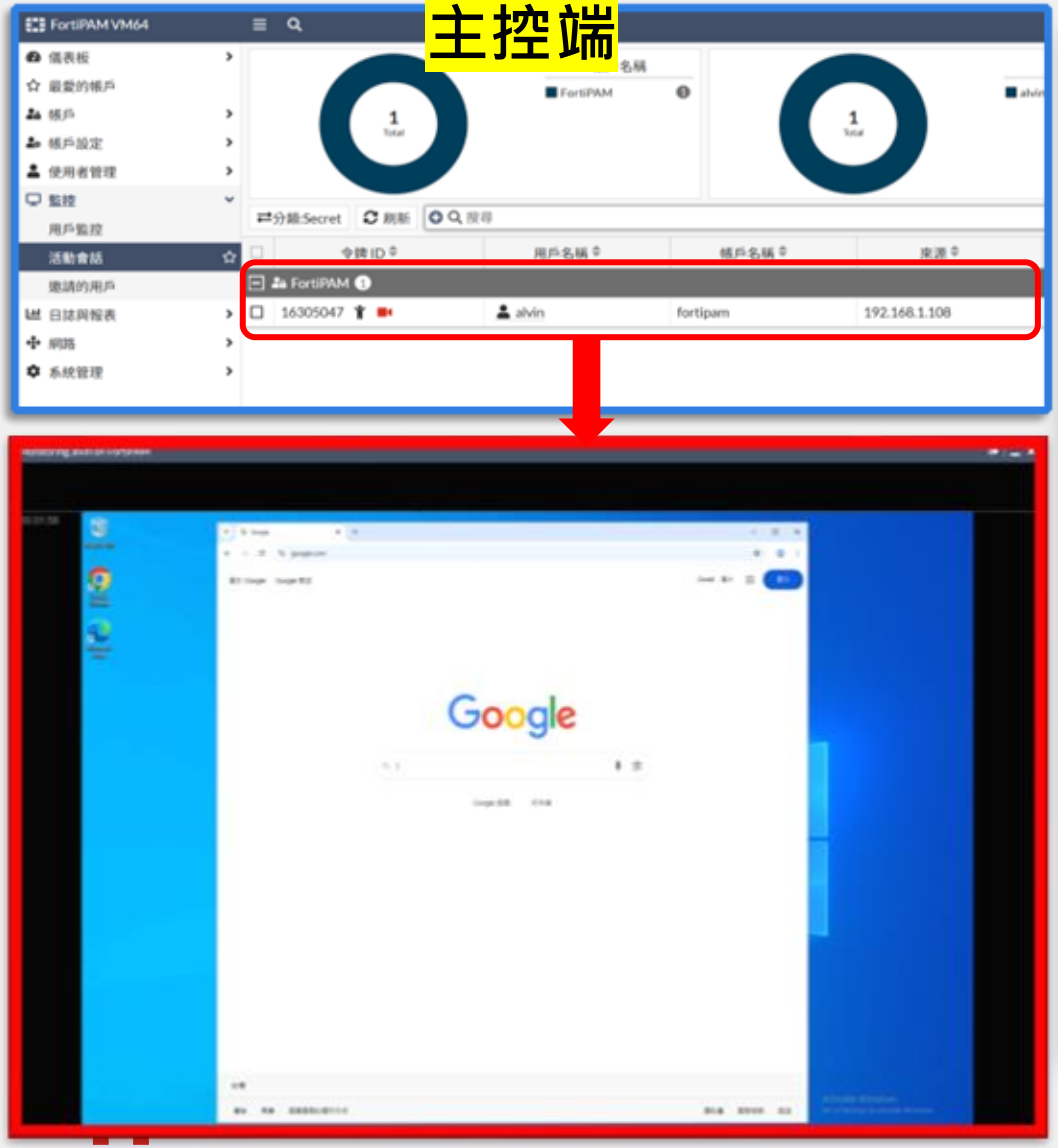


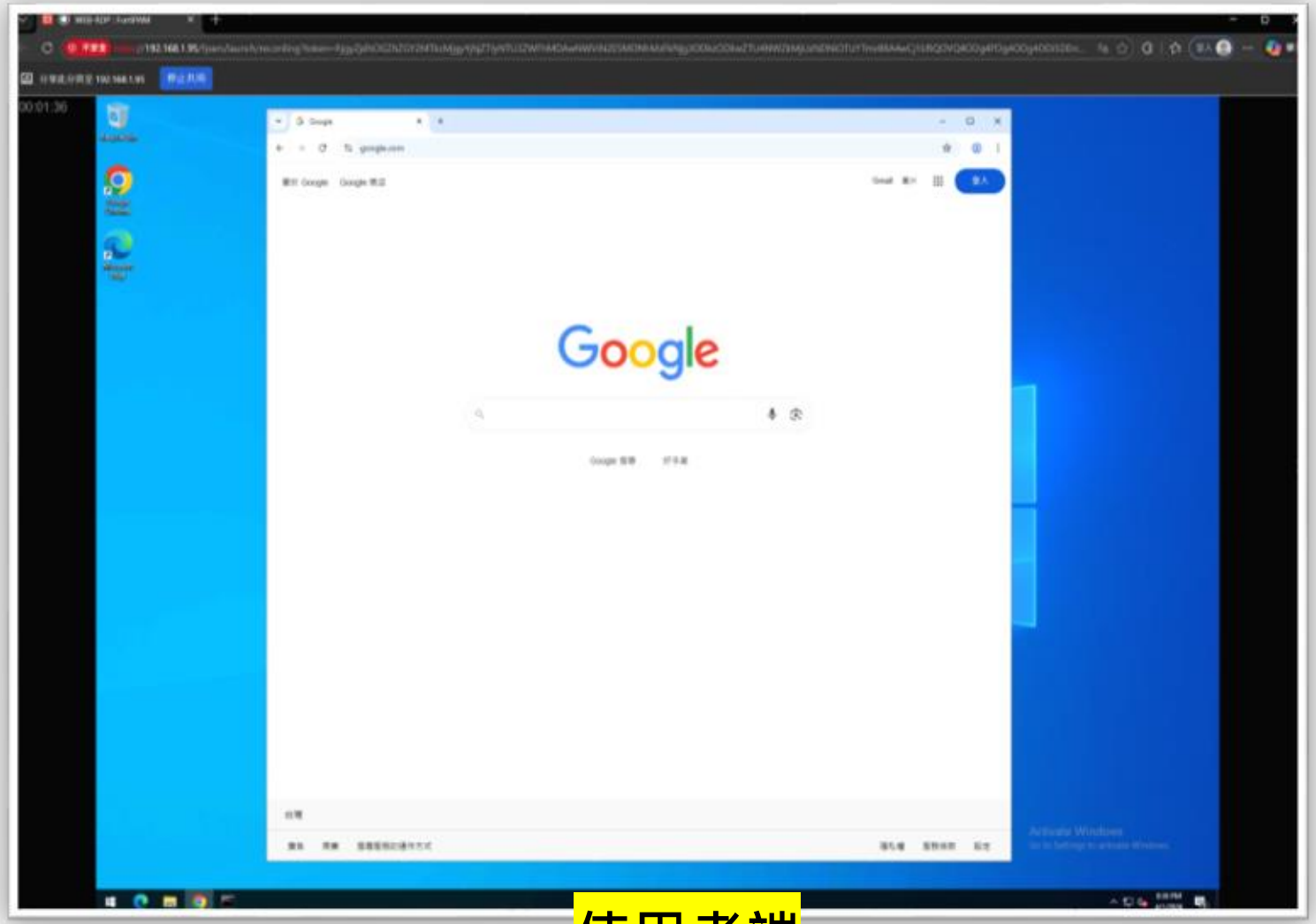
© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

即時監控

主控端



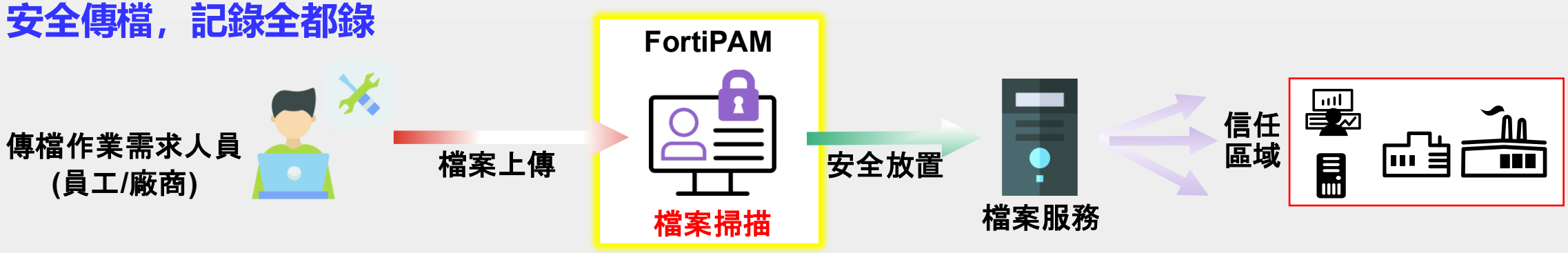


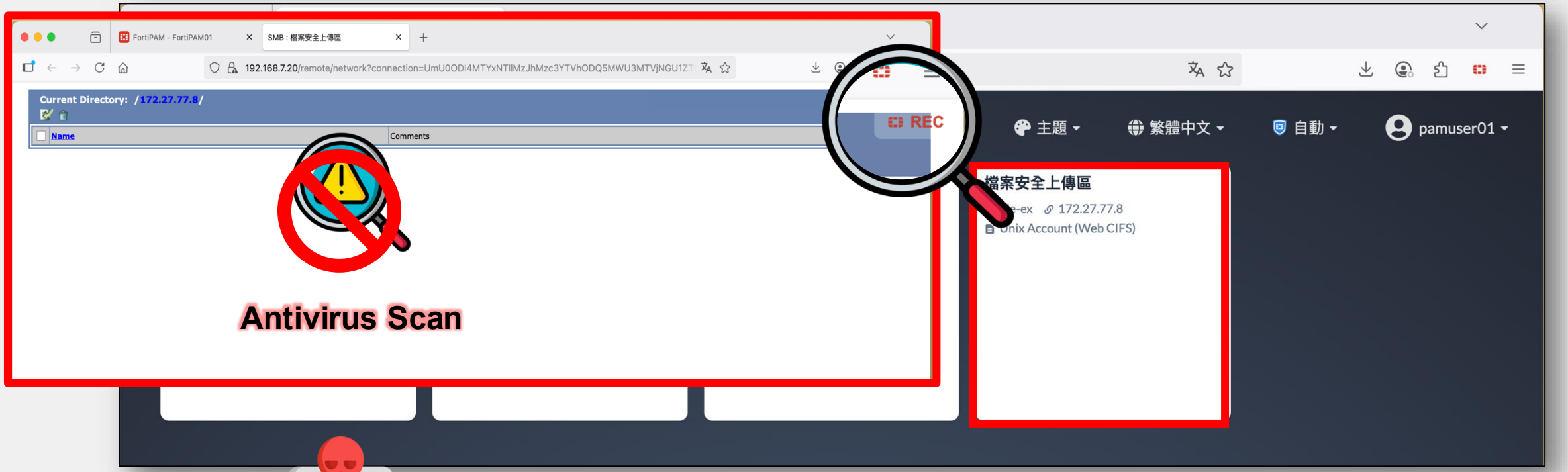
使用者端

© Fortinet Inc. All Rights Reserved.

FortiPAM - 關鍵身分與特權治理

安全傳檔，記錄全都錄



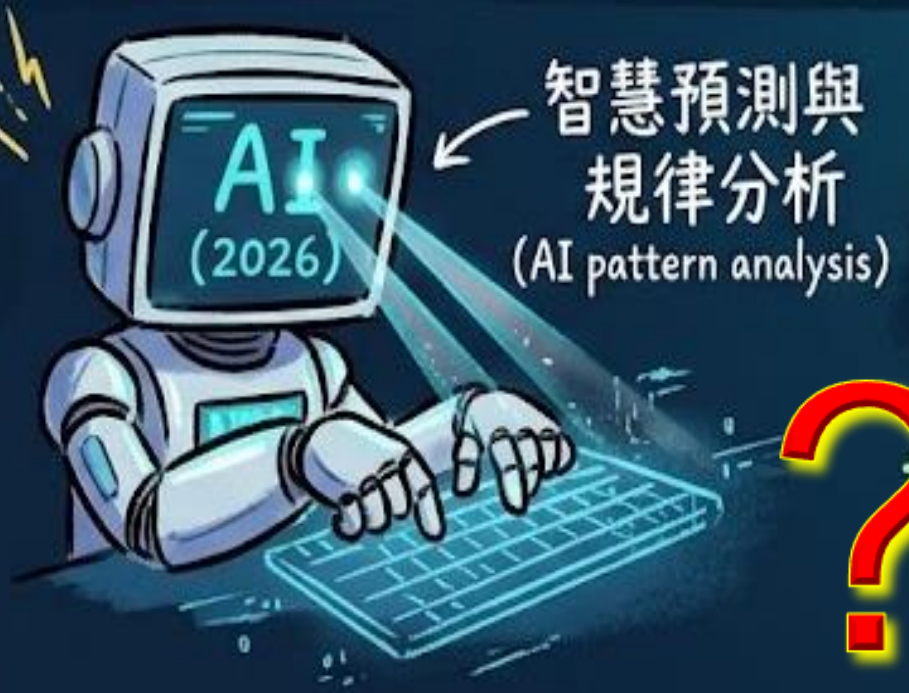


上傳檔案安全，下載安全檔案，操作記錄全都錄

© Fortinet Inc. All Rights Reserved.

常見與規律密碼
(Common Passwords)

123456
P@ssword
Summer2025!



智慧預測與
規律分析
(AI pattern analysis)

長且隨機 / 密碼短語
(Long & Random / Passphrase)

?4!n_M4gn3t_K3y_99?
r&P5@qX!wK92_LmB



秒破！
幾秒至數分鐘
(SECONDS OR
MINUTES!)

百年以上！
(CENTURIES!)

難以攻破
(Nearly Impossible!)



AI 快速破門



AI 輕鬆竊取單一密碼
(秒速破解！)

致命的「密碼重複」行為

在多個網站重複使用
同一組密碼！



多系統同時淪陷系統連鎖效應



電子郵件 (Email)
網路銀行 (E-Banking)
社群平台 (Social Media)
購物網站 (Shopping)

連鎖效應：
多個系統 一併淪陷！
一處外洩，全面解體！

FortiToken – 多因子認證

有了多因子，讓您安全不掉鏈子



Something
You Know

Something
You Have

© Fortinet Inc. All Rights Reserved.

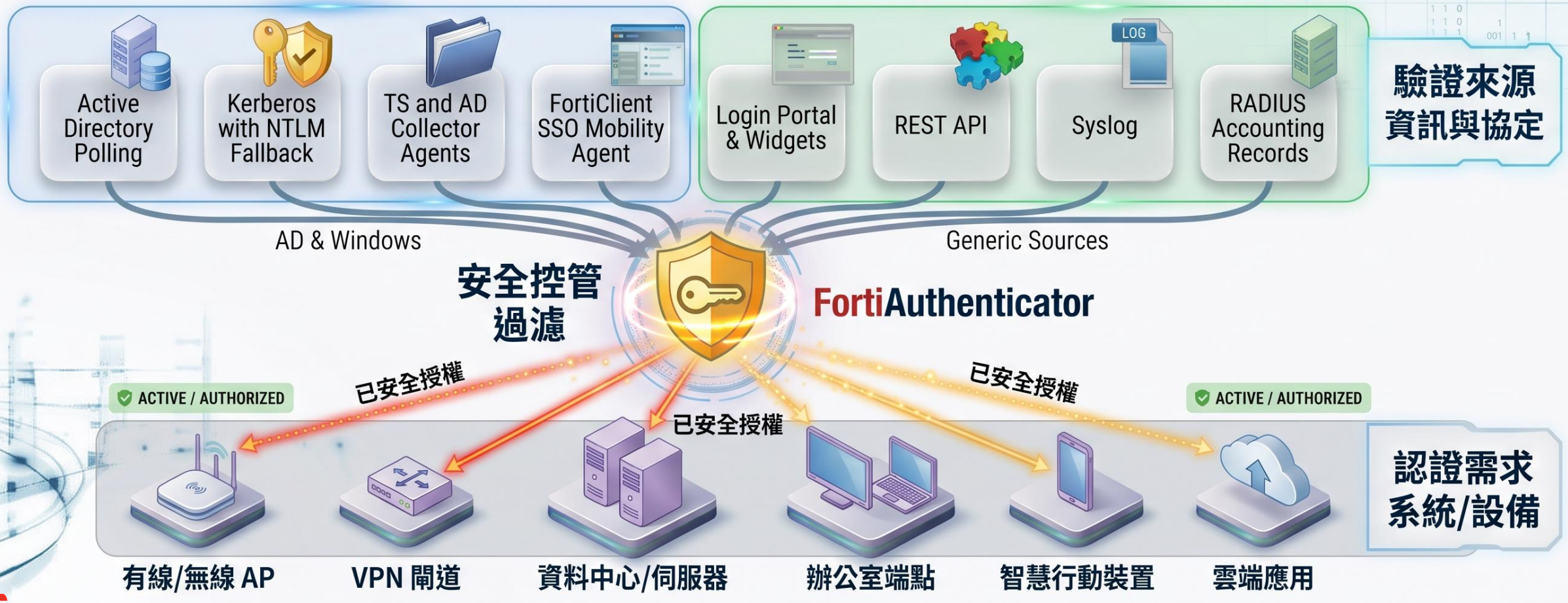
FortiAuthenticator – 中央認證管理平台

集中認證

整合集中管理驗證來源，簡化繁瑣步驟。

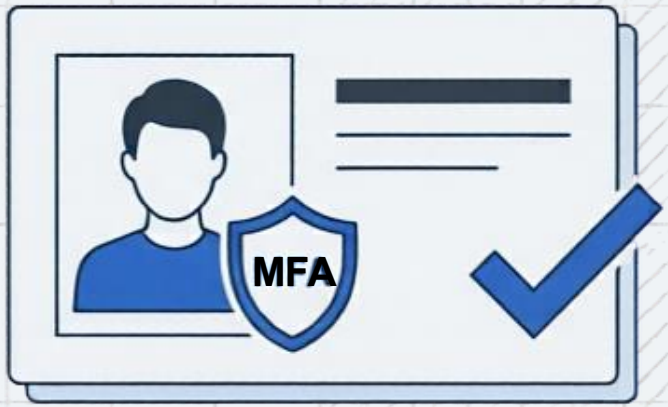
強化管理

使用者身分的驗證以及使用者權限的控管。



© Fortinet Inc. All Rights Reserved.

授權身份 +



傳統資安的盲點

傳統防護專注於「誰登入」(身分與密碼)

卻少了「用什麼」登入(設備的實際安全狀態)

端點零信任合規與管理

永不信任，持續驗證和確認

用戶身份驗證

設備終端驗證

終端健康狀態驗證

最小權限存取



FortiClient EMS - 端點零信任合規與管理



中央端點控制平台
FortiClient EMS
(Endpoint Management Server)

監控與管理



零信任存取
ZTNA

遠端連線
IPSec/SSL VPN

端點保護
Endpoint Protection
(EPP)

端點偵測與回應
Endpoint Detection and Response
(EDR)
*Roadmap

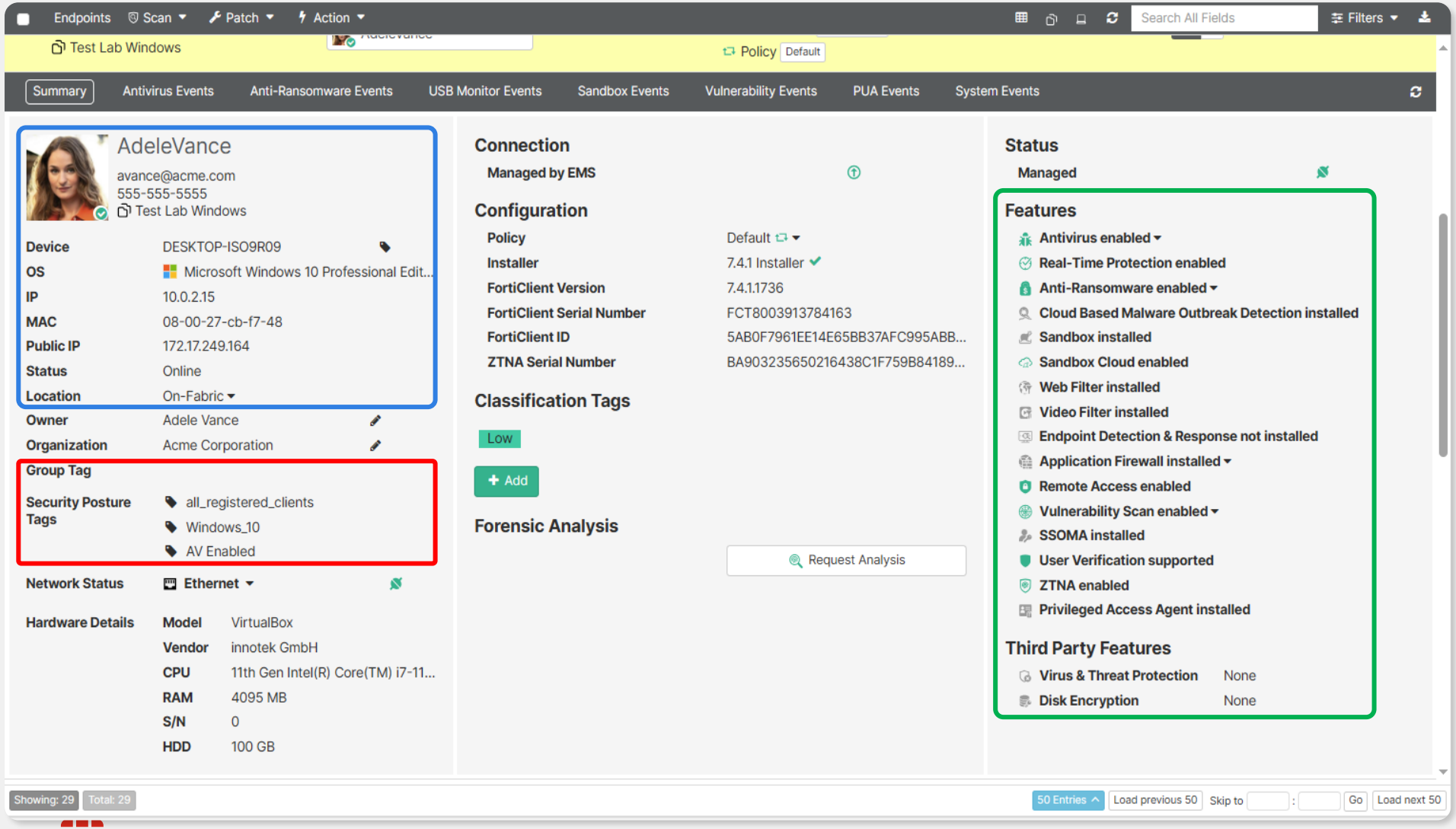
弱點掃描
Vulnerability Scan

沙箱偵測
Sandbox Detection

© Fortinet Inc. All Rights Reserved.

FortiClient EMS - 端點零信任合規與管理

端點狀況一目瞭然



端點設備資訊

FortiClient 連線資訊

登入用戶資訊

網內 / 網外

安全合規標籤

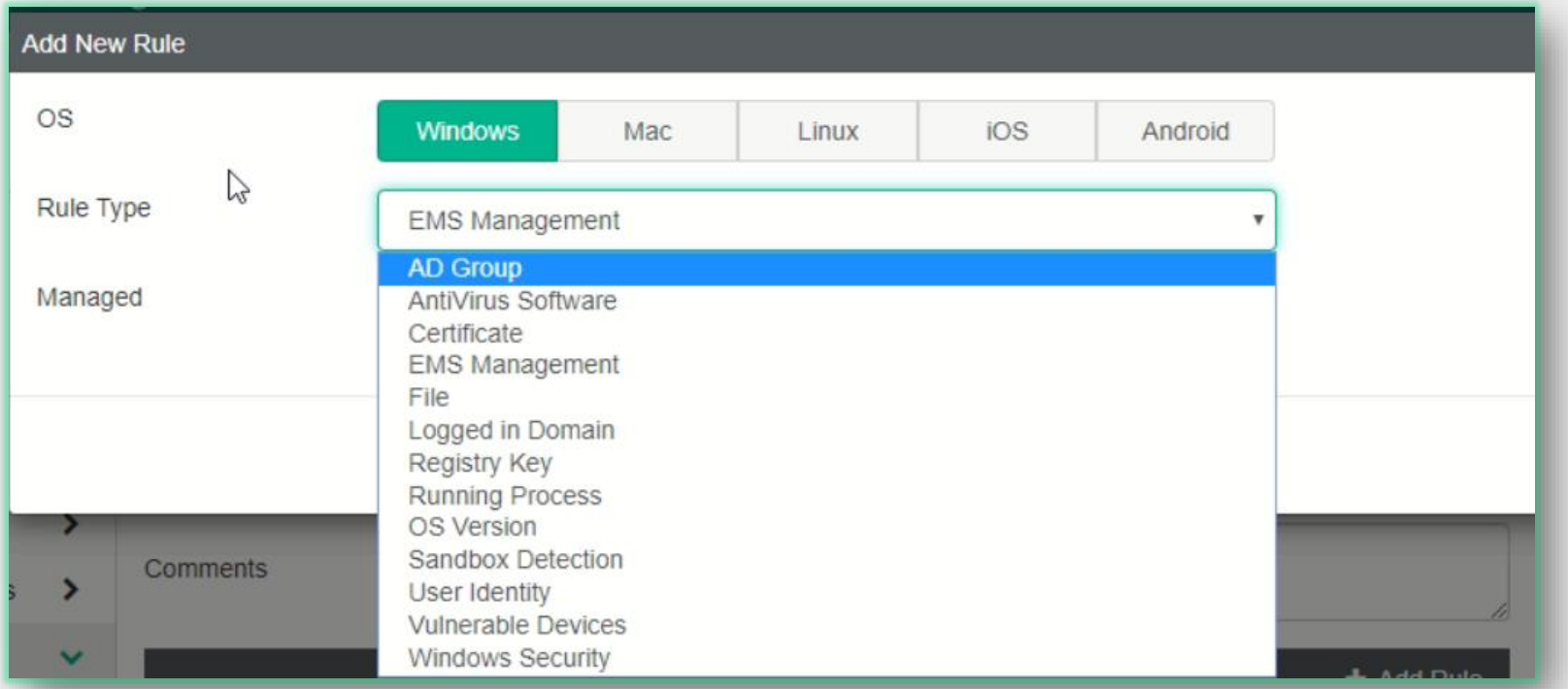
已啟用安全功能

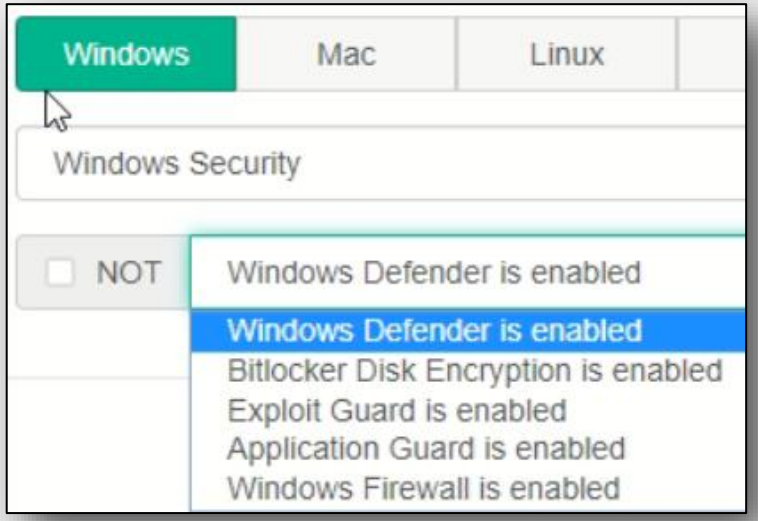
端點事件和記錄

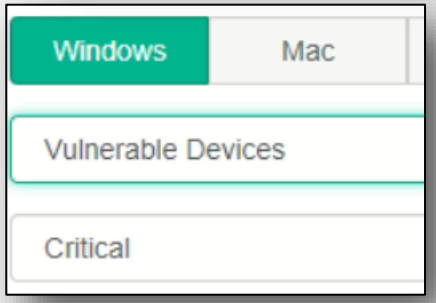
© Fortinet Inc. All Rights Reserved.

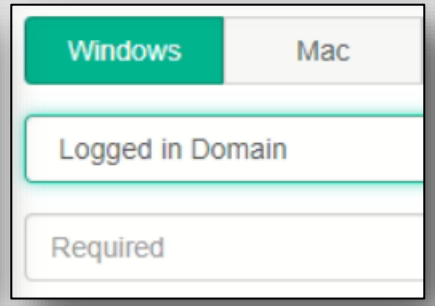
FortiClient EMS - 端點零信任合規與管理

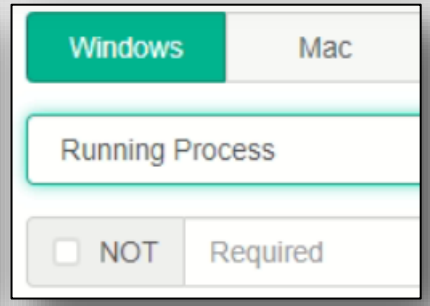
多樣屬性的合規條件

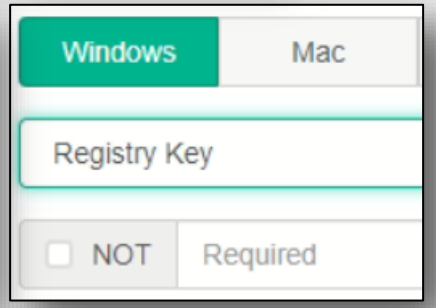


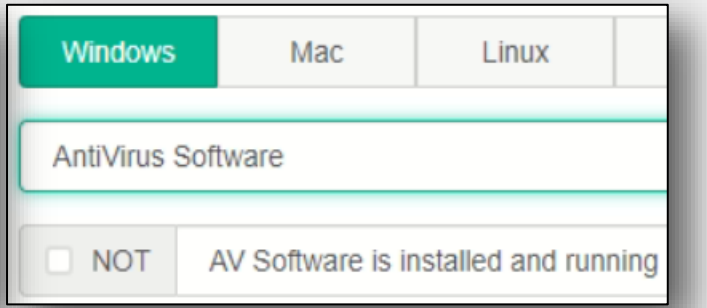








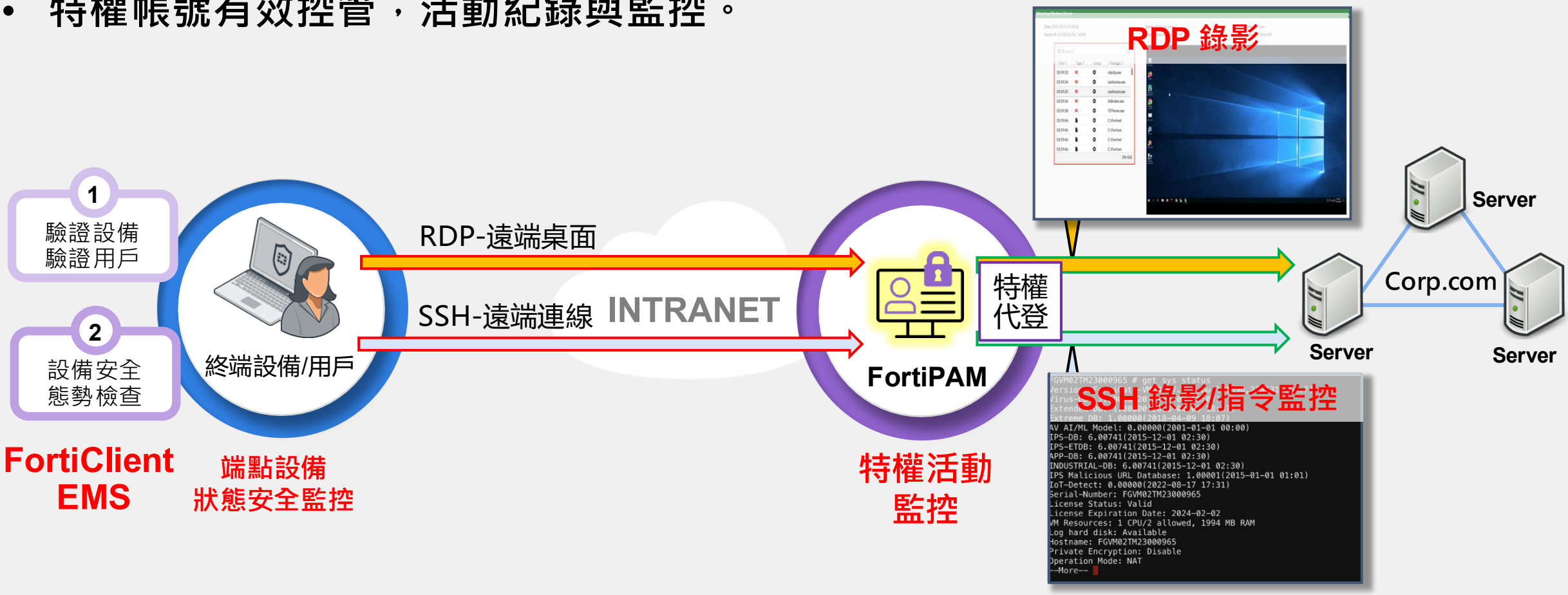




© Fortinet Inc. All Rights Reserved.

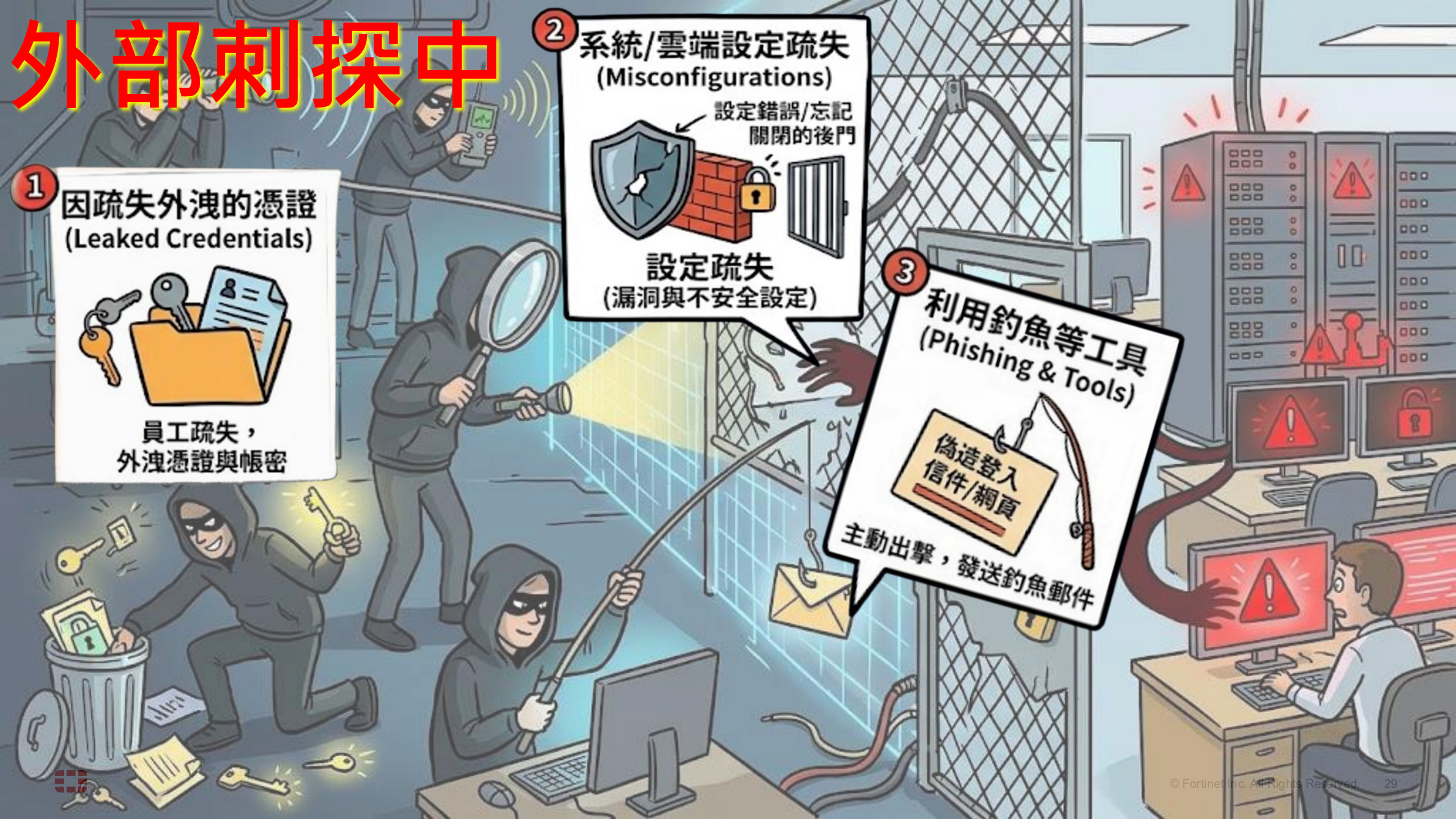
FortiClient EMS + FortiPAM - 零信任特權安控平台

- 端點設備零信任，狀態隨時監控，狀態改變即改變策略阻擋使用。
- 特權帳號有效控管，活動紀錄與監控。



© Fortinet Inc. All Rights Reserved.

外部刺探中



© Fortinet Inc. All Rights Reserved.

FortiRecon - 數位風險保護服務 (DRPS)



External Attack Surface Monitoring

外部攻擊面管理

- 數位資產探索
- 曝露的攻擊面
- 外部資安風險
- 偵測外洩資訊

Brand Protection

品牌保護

- 網域名稱仿冒
- 監測可疑的應用程式
- 監測社交媒體
- 下架服務

Adversary Centric Intelligence

敵情中心

- 暗網流竄情資
- 人工獲取情資
- 開源分享情資
- 因入侵而洩漏的帳密
- 早期預警與突發威脅告警

© Fortinet Inc. All Rights Reserved.

FortiRecon - 數位風險保護服務 (DRPS)

External Attack Surface Management (EASM)

外部攻擊面管理

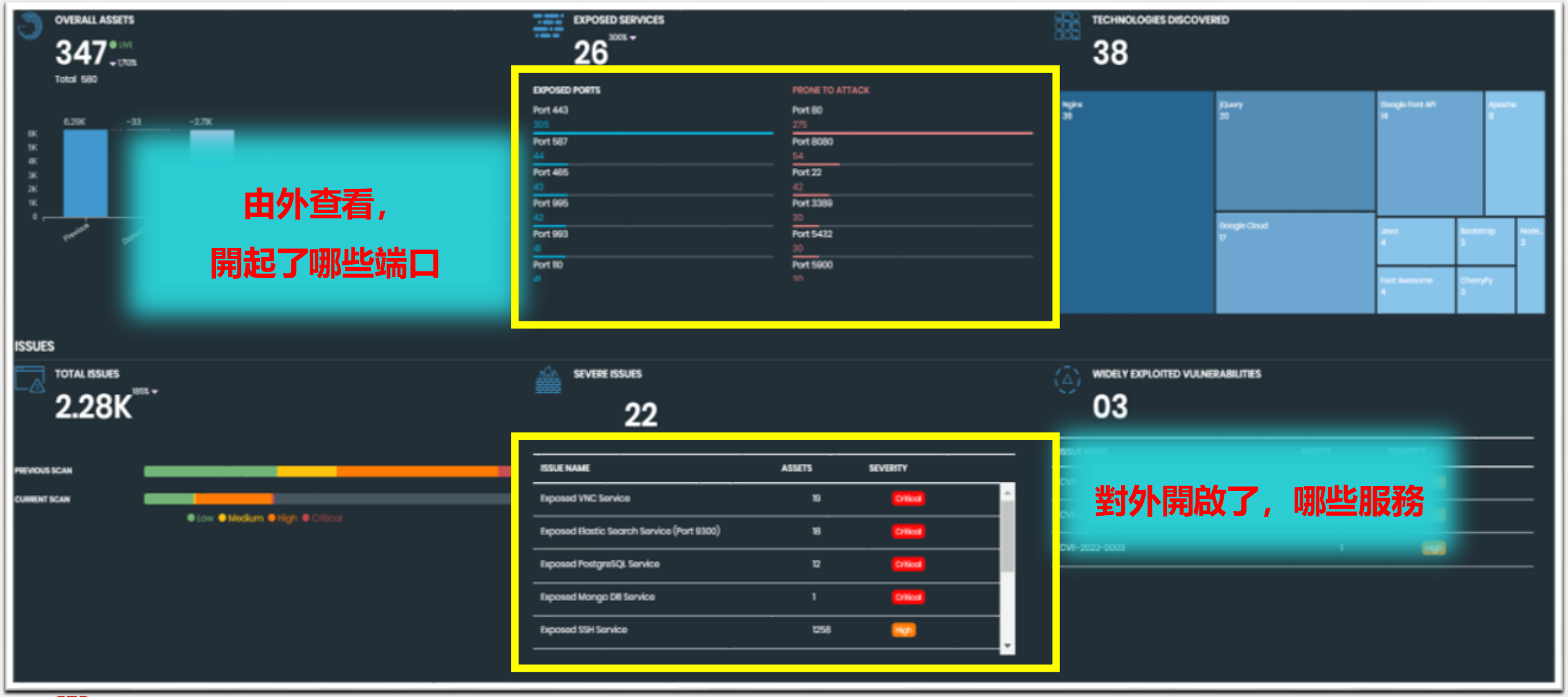
外部攻擊面管理 (EASM) 提供組織及其子公司從**外部視角的檢測**，識別暴露已知和未知企業資產及相關漏洞，藉以幫助確定修復最關鍵問題的優先級。 EASM 將幫助識別可能被惡意行為者利用的服務、憑證、公有雲服務設定錯誤和第三方合作夥伴軟體程式漏洞等。



© Fortinet Inc. All Rights Reserved.

在駭客找到你的問題前，先進行修補！

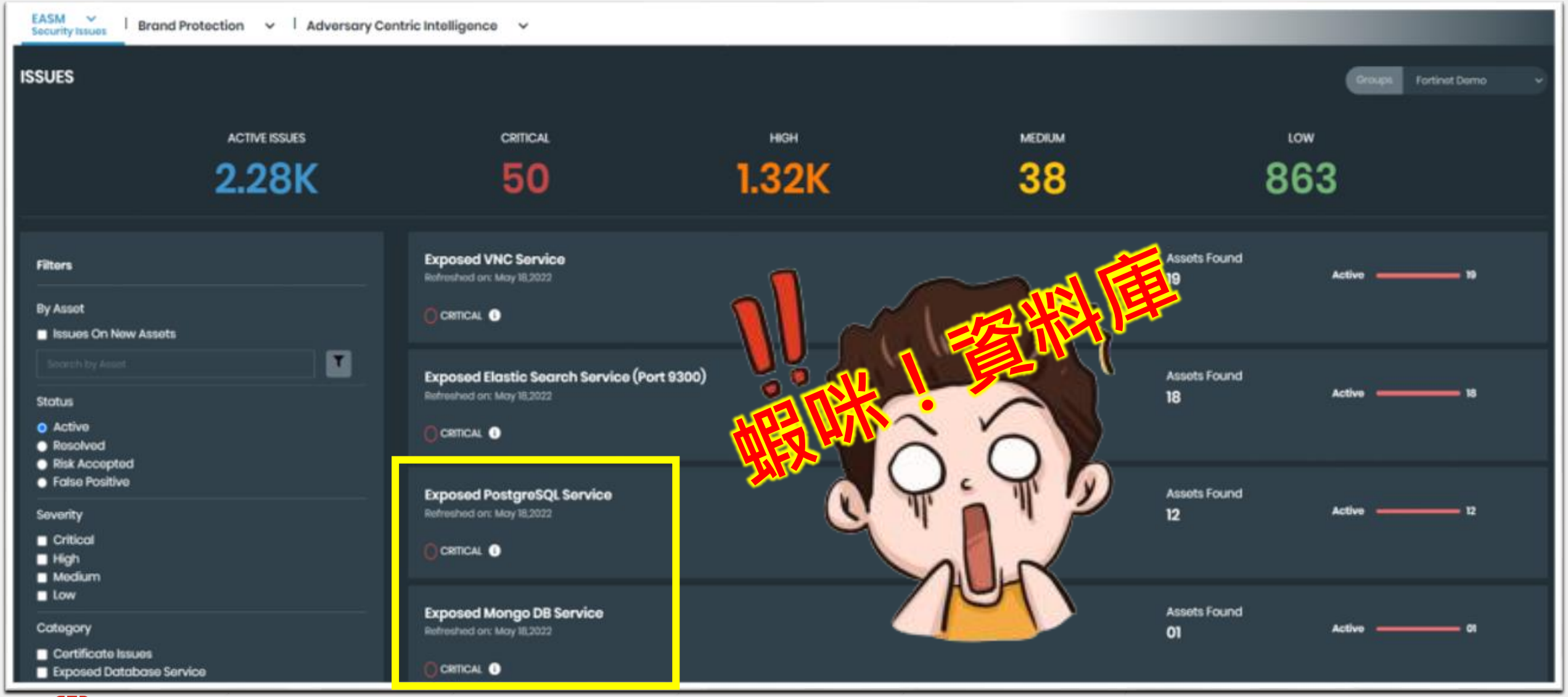
從外部幫您進行檢測，找出曝露在外的資產、服務、資安問題以及弱點！



© Fortinet Inc. All Rights Reserved.

駭客攻擊前都會來探測一下，那它們能看到什麼就很重要

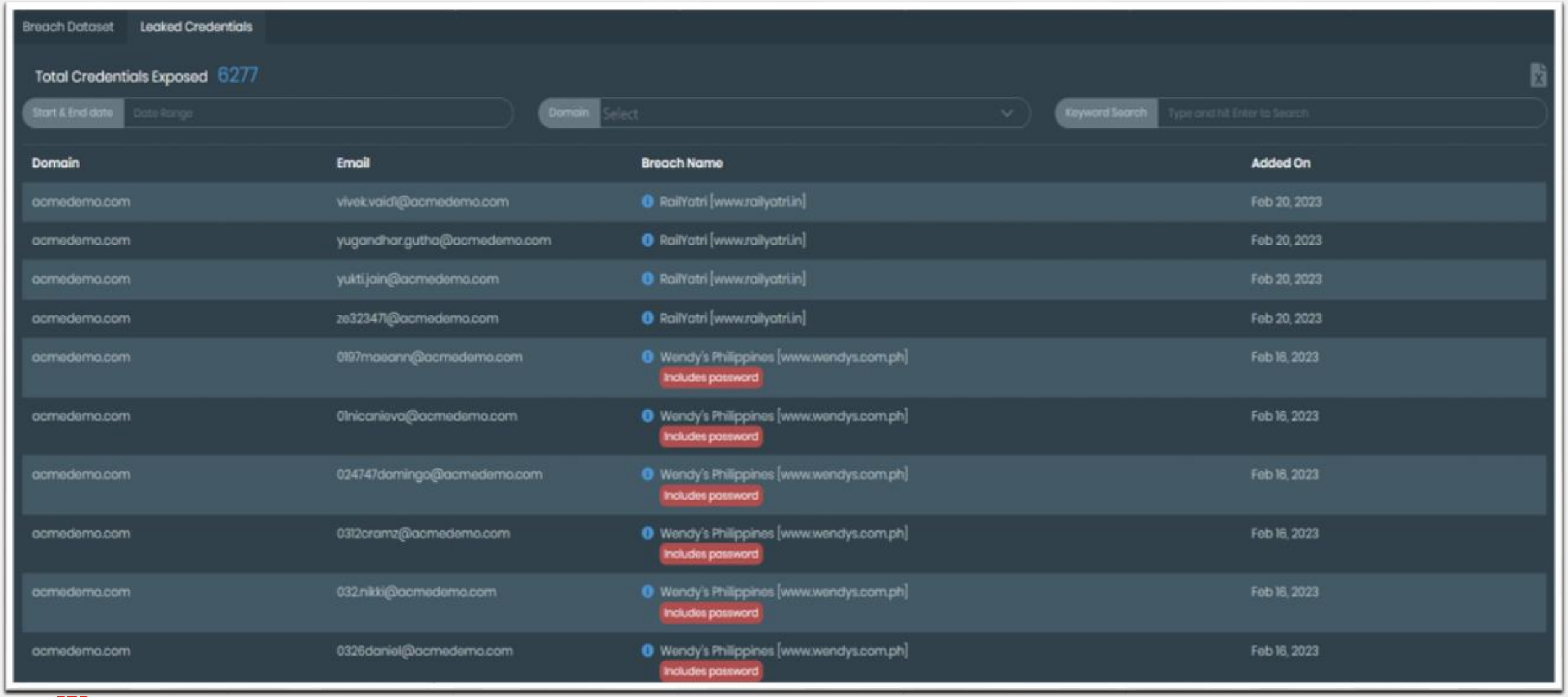
這些都是從外部任意來源可以看到的問題，要在駭客利用前更快的去處理!



© Fortinet Inc. All Rights Reserved.

有無使用者帳密外洩？！

駭侵事件很多，很多竊取的資料都公布在Internet上，我們要注意有沒有跟我們使用者相關的部份!



© Fortinet Inc. All Rights Reserved.

FortiRecon - 數位風險保護服務 (DRPS)

Brand Protection (BP)

品牌保護

使用專有演算法，檢測網路釣魚攻擊、域名仿冒、網頁置換、可疑的應用程序、帳密洩露和攻擊者使用社交媒體及品牌假冒。

通過及早檢測並採取行動(例如下架網站或應用程序)，幫助組織**保護品牌價值和聲譽**。



© Fortinet Inc. All Rights Reserved.

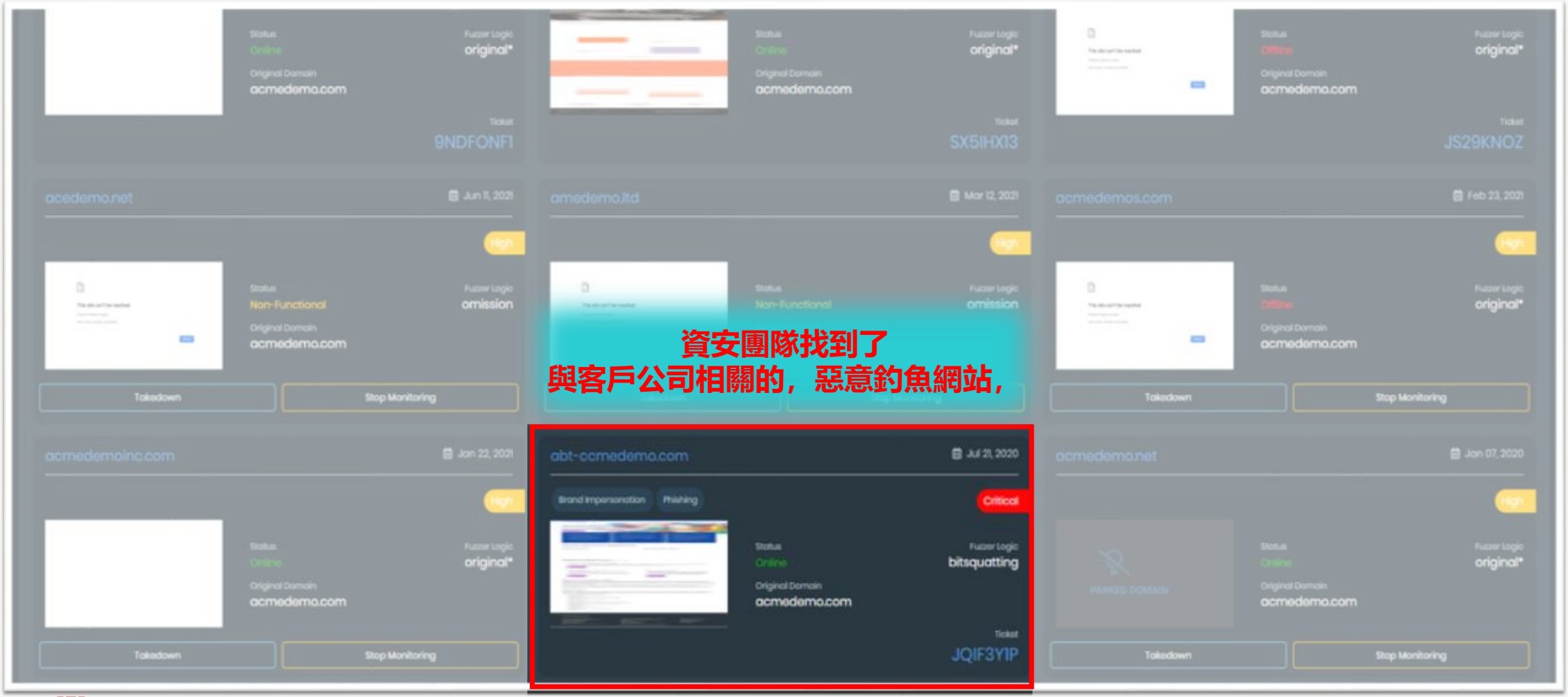
社群媒體 – 有跟公司名稱相關帳號的的活動?

FB, IG 上面有沒有人打著公司的名號在進行可疑的活動?



© Fortinet Inc. All Rights Reserved.

釣魚網站 – 冒用內容進行釣魚的網站

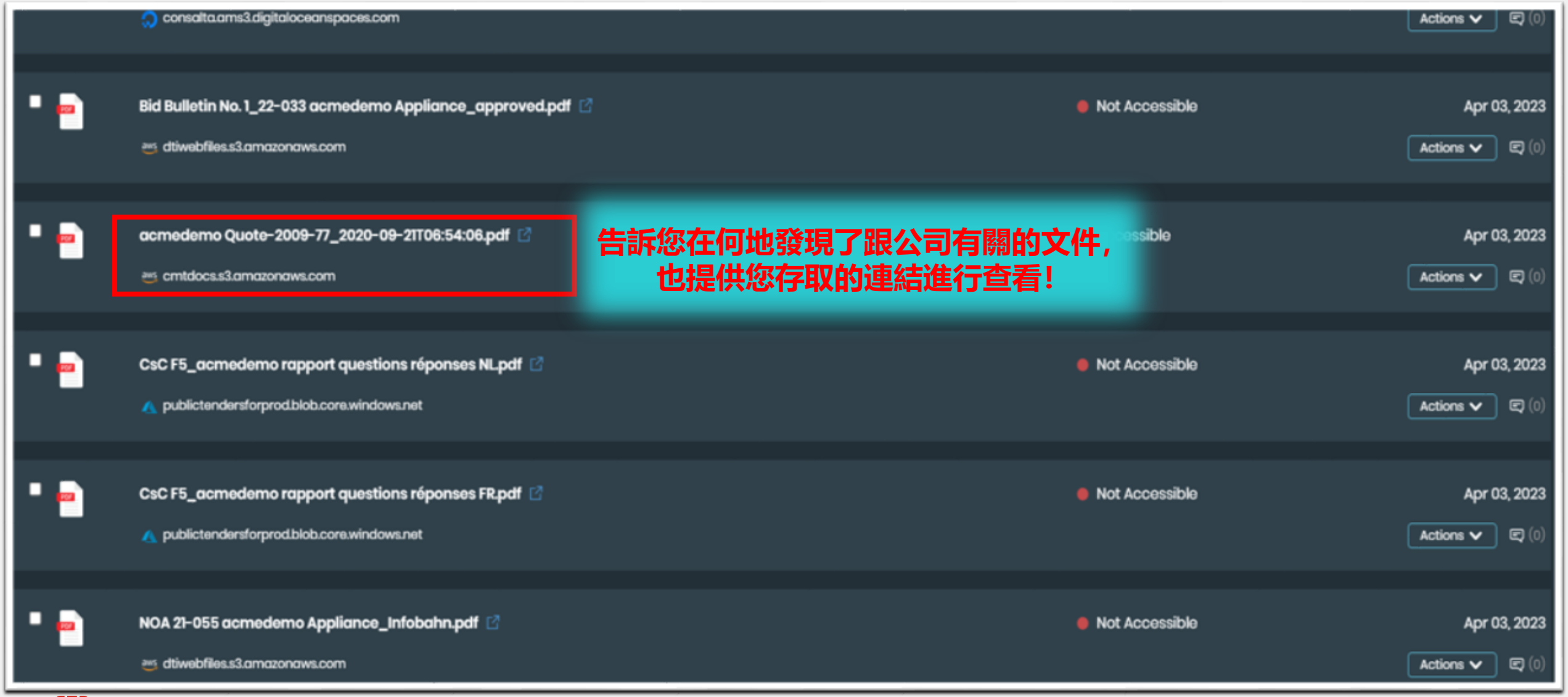


資安團隊找到了
與客戶公司相關的，惡意釣魚網站，

© Fortinet Inc. All Rights Reserved.

公開存取的雲端存儲空間有沒有公司相關的文件?

由於權限設定的問題，往往會有員工將文件放在雲端存儲但是忘了鎖定存取權限



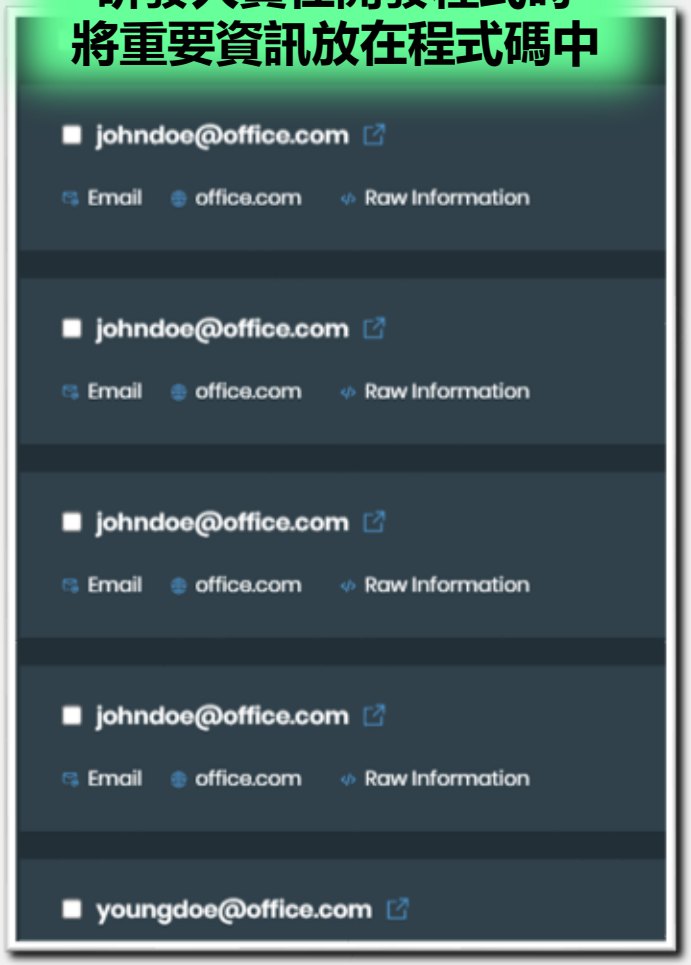
告訴您在何地發現了跟公司有關的文件，
也提供您存取的連結進行查看！

© Fortinet Inc. All Rights Reserved.

雲端程式碼倉庫有沒有洩漏了重要資訊?

檢測開發的程式碼倉庫中，是否有的相關重要資訊

研發人員在開發程式時
將重要資訊放在程式碼中





© Fortinet Inc. All Rights Reserved.

FortiRecon - 數位風險保護服務 (DRPS)

Adversary Centric Intelligence (ACI)

敵情中心

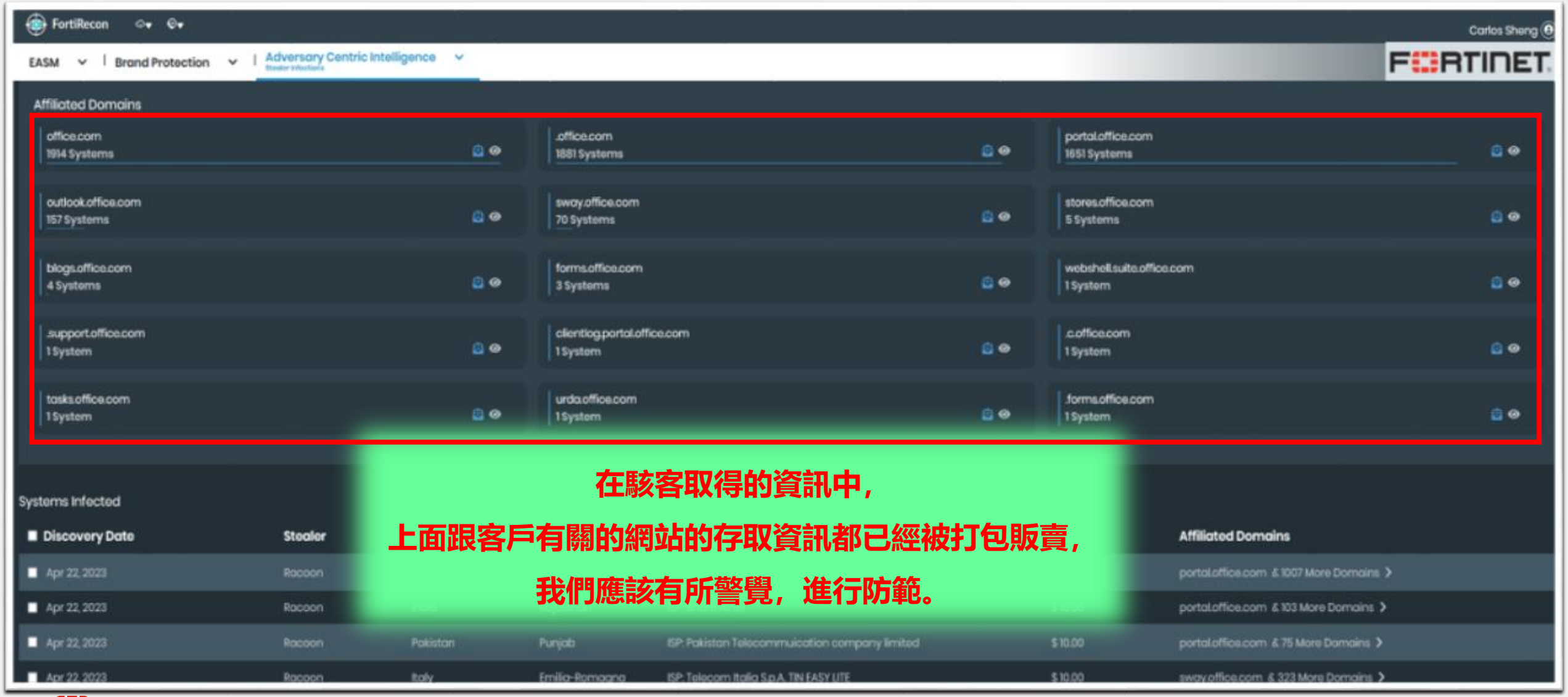
為組織提供來自對手的即時性威脅的內容，使他們能夠更快地響應事件，更好地了解攻擊者並保護他們的資產。

全面涵蓋來自主要和新興威脅的**暗網、開源和技術威脅指標**。



在暗網交易的內容比我們想像中的更多更頻繁

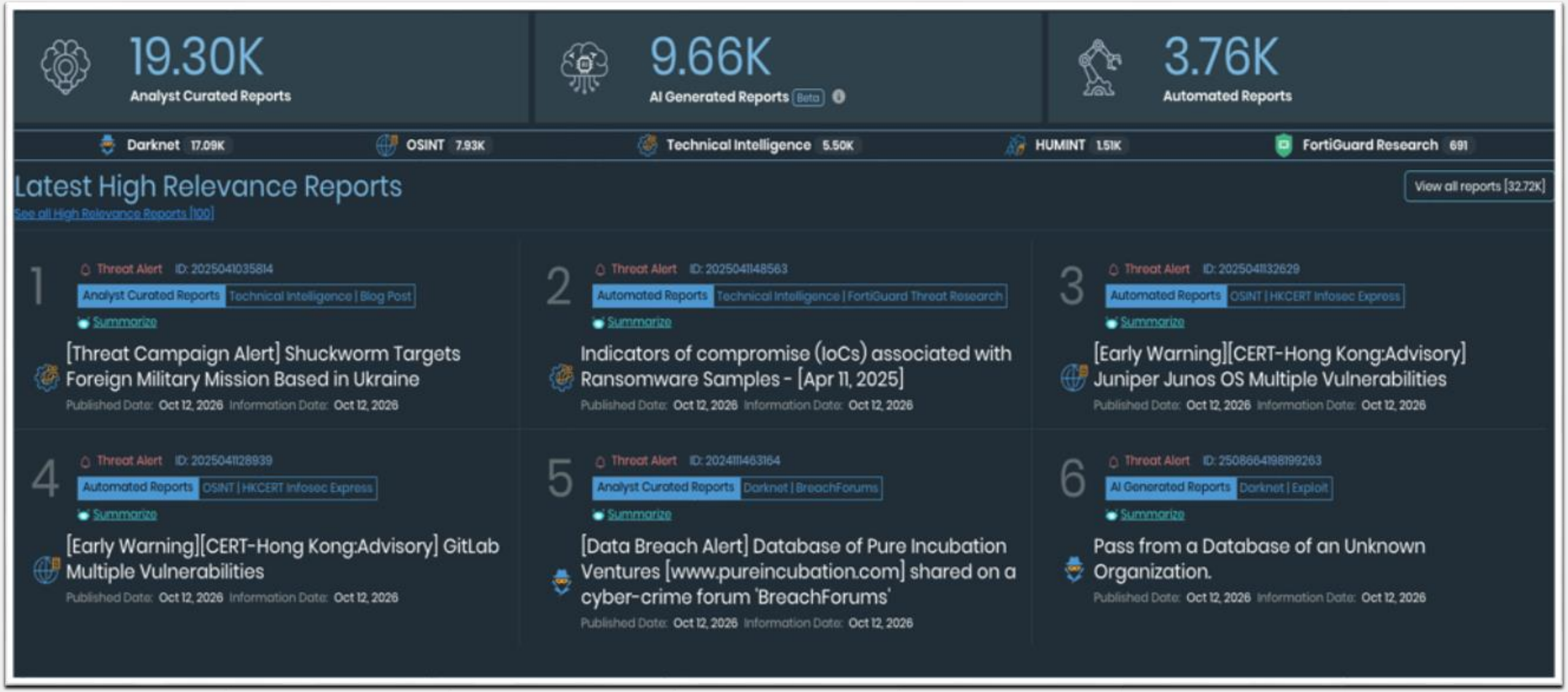
駭客透過惡意程式取得的資訊，往往在暗網中進行交易，其中有沒有跟我們有關的?



© Fortinet Inc. All Rights Reserved.

團隊監控暗網，發現有相關事件即時通報

駭客往往會在暗網中活動，及時的情報通知，才能有更早的防護!



© Fortinet Inc. All Rights Reserved.

BBC

NEWS 中文

主頁 | 觀看

國際 | 中國 | 香港 | 台灣 | 英國 | 財經

OpenAI智能體入侵澳洲政府網站竊取資料 官方兩月後才發覺



新聞

您現在位置：首頁 > 新聞

全球最大AI模型庫Hugging Face遭自主AI代理人攻擊 內部資料與憑證外洩

2026 / 07 / 21 - 編輯部



資料來源：https://www.bbc.com/ , https://www.informationsecurity.com.tw/

© Fortinet Inc. All Rights Reserved.

為什麼需要自動化(SOAR)？問題總是在睡覺時發生



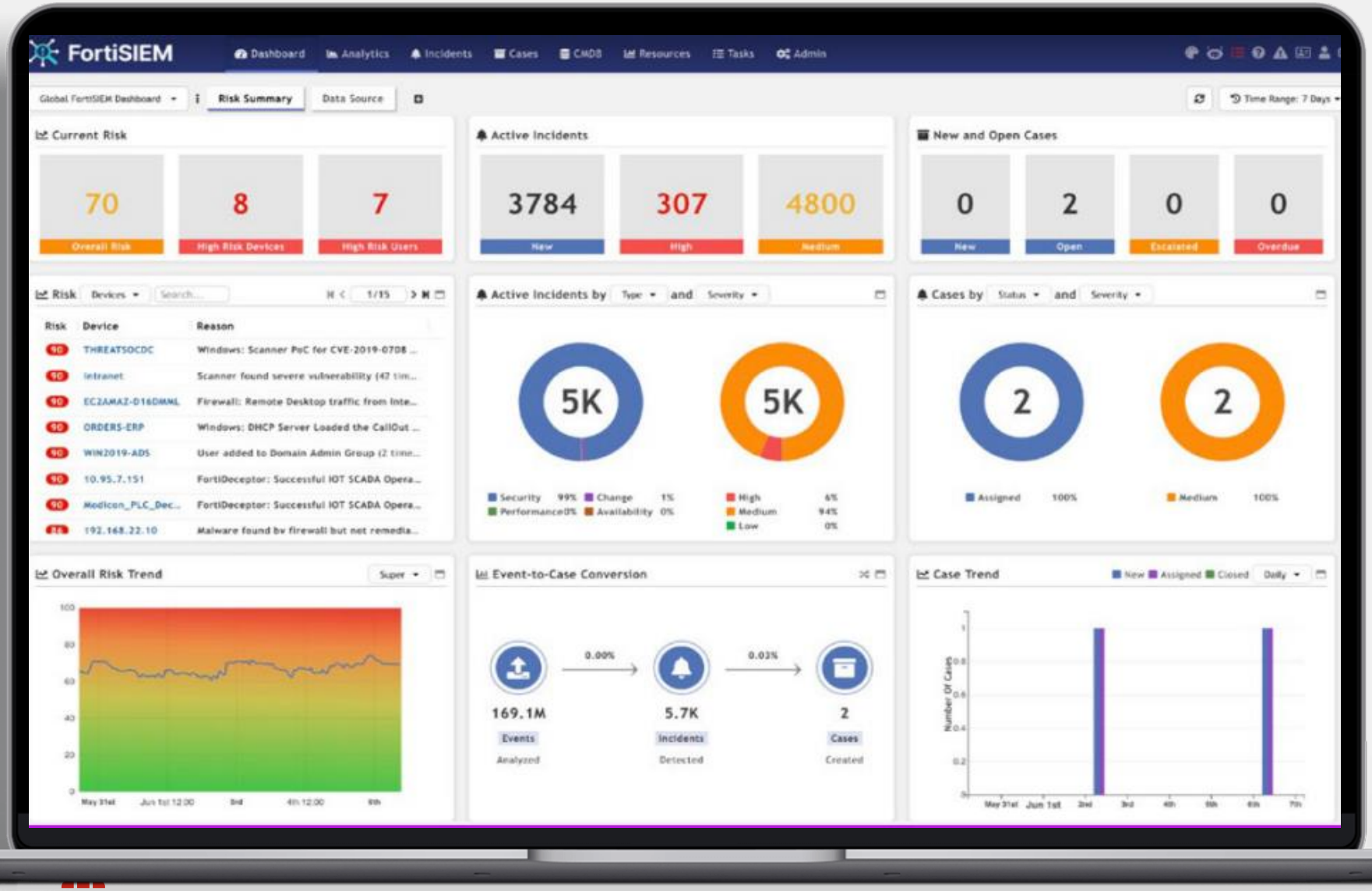


Image from https://www.parentingheadline.com/article/13288/%E9%9C%B2%E7%87%9F%E6%84%8F%E5%A4%96-%E5%B8%B3%E7%AF%B7%E5%85%A7%E9%96%8B%E6%9A%96%E7%88%90-%E4%B8%80%E5%AE%B6%E4%B8%89%E5%8F%A3-%E4%B8%80%E6%B0%A7%E5%8C%96%E7%A2%B3%E4%B8%AD%E6%AF%92-%E5%B9%B8%E7%8D%B2%E6%95%91

© Fortinet Inc. All Rights Reserved.

FortiSIEM - 安全資訊與事件管理平台

敏銳的眼睛與大腦，串聯萬物 無所遁形



可協同運作或獨立運行，
為企業級 SOC 提供核心動力

企業級威脅偵測
(Enterprise Threat Detection)

支援多供應商設備的事件收集、行為威脅偵測，以及全方位的 SIEM 核心功能。

事件管理
(Incident Management)

具備專為分析師優化的豐富功能與自動化流程，能自動排定優先權並即時回應攻擊者。

資安維運職能與管理
(SecOps Functions and Management)

涵蓋漏洞與合規性管理、威脅情資與威脅獵捕、維運管理... 等多項功能。

無處不在的自動化流程
(Automation Everywhere)

包含 SIEM 內建的 light-SOAR 自動化功能，可快速執行常見的威脅阻斷。

© Fortinet Inc. All Rights Reserved.

FortiSOAR – 進階協作與自動化回應平台

靈活的雙手與流程骨幹，打造全面自動化編排與回應



跨廠牌生態系整合

超過 700+ 種多廠牌產品的整合與解決方案套件與數千多個自動化動作。不限於 Fortinet 產品，能完美串聯企業現有的第三方資安工具、IT 系統與服務台

動態劇本與案件管理

提供可視化拖拉式劇本編輯器，輕鬆將繁瑣的調查流程標準化。結合全功能案件管理面板，自動關聯警報、留存鑑識軌跡，大幅提升一線分析師的處理效率。

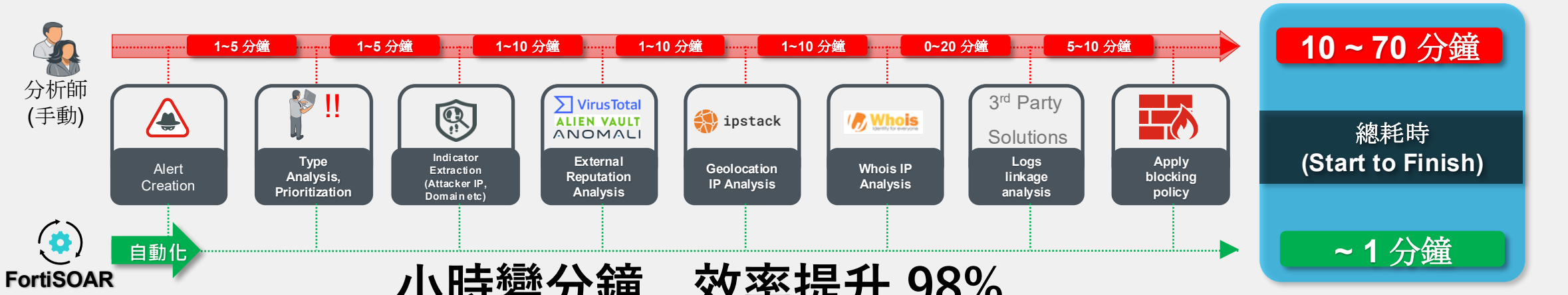
企業級自動化編排

具備完整、強大的重度 SOAR能力。支援多租戶架構、高可用性（HA）與自定義角色權限控制（RBAC），完美對應大型企業與 MSSP 託管服務商的複雜運維需求。

© Fortinet Inc. All Rights Reserved.

FortiSOAR – 進階協作與自動化回應平台

大幅縮短複雜事件回應處理時間



小時變分鐘，效率提升 98%



© Fortinet Inc. All Rights Reserved.

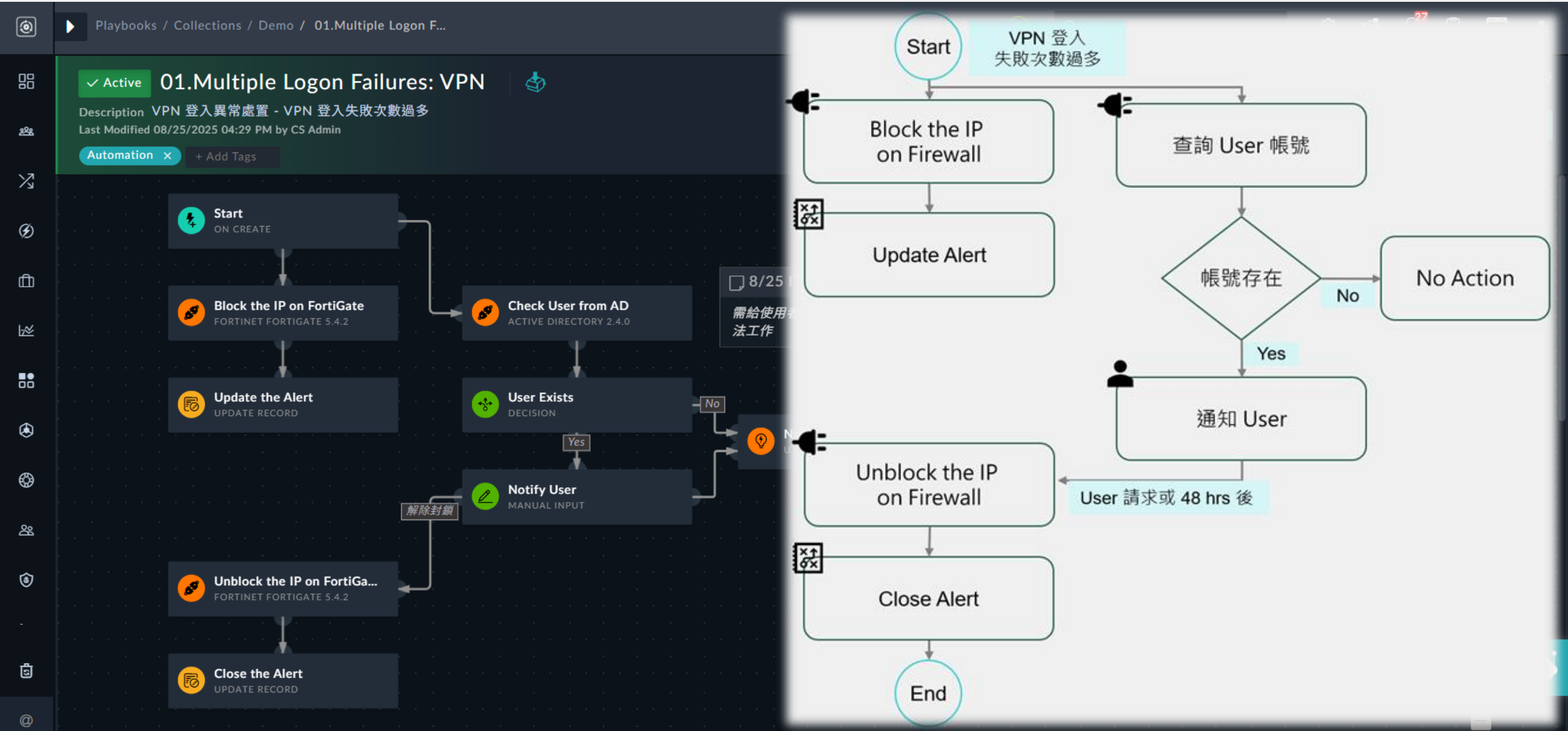
FortiSIEM 與 FortiSOAR 的協奏曲

VPN 異常登入與自助解鎖： 偵測異常與協調封鎖、驗證與解鎖

© Fortinet Inc. All Rights Reserved.

模擬場景 — VPN 登入異常處置

FortiSOAR Playbook – 封鎖流程暨使用者自助「快速解鎖流程」實作



模擬場景 — VPN 登入異常處置

IP 封鎖通知電郵: 含使用者自助「快速解鎖流程」

From	To	Subject	Received
<secops@fortilab.cc> size=2677	<eve.dropper@fortilab.cc>	[FortiSOAR] VPN 登入失敗次數過多, 已封鎖 IP - 175.27.168.51	Thursday, 11 Sep 2025 11:06:08 AM

Received Thursday, 11 Sep 2025 11:06:08 AM
From <secops@fortilab.cc> size=2677
To <eve.dropper@fortilab.cc>
Subject **[FortiSOAR] VPN 登入失敗次數過多, 已封鎖 IP - 175.27.168.51**

HTML | Plain Text | Source — Download

Hi,

IP: **175.27.168.51** 已被封鎖
原因: VPN 登入失敗次數過多

若是您的 IP, 並希望解除此 IP 封鎖, 請使用以下連結進行解除封鎖請求：

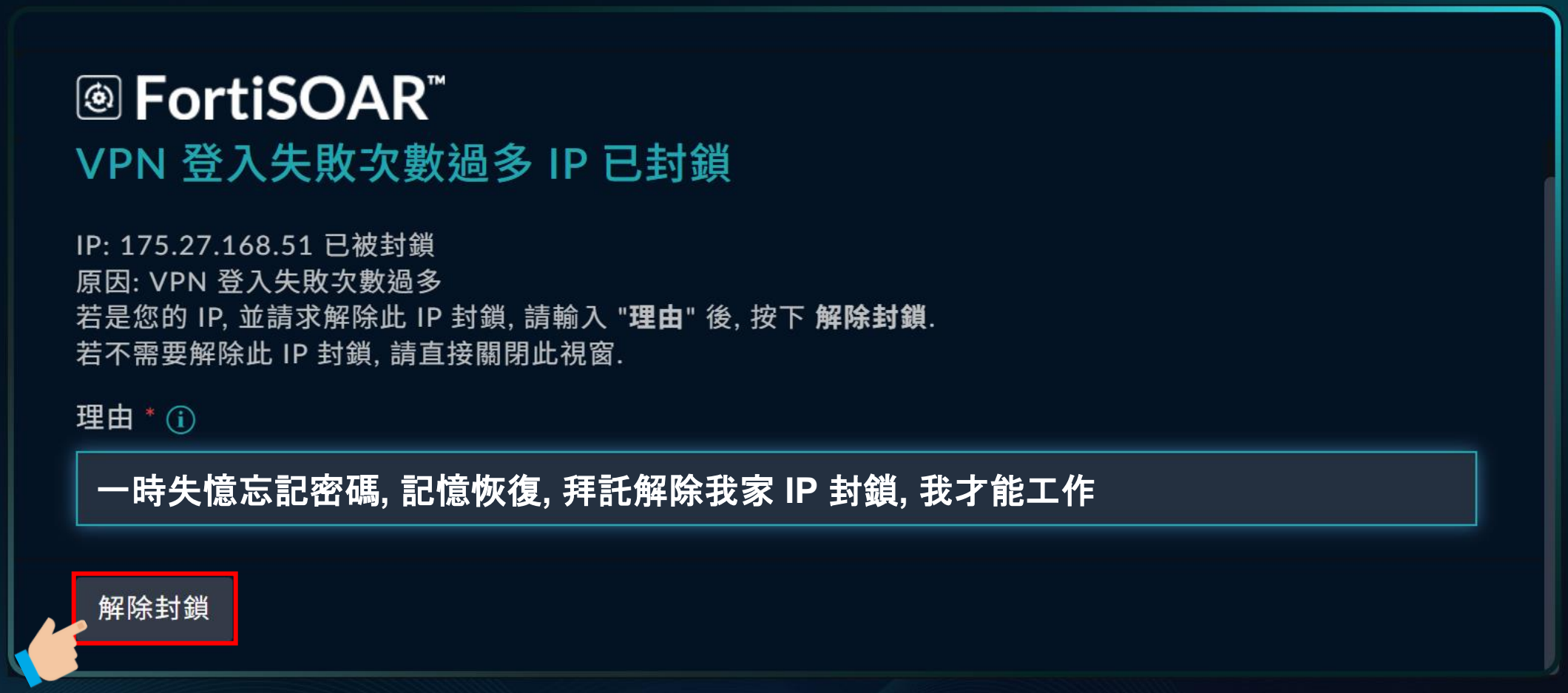
開啟請求表單

FortiSOAR Admin.

© Fortinet Inc. All Rights Reserved.

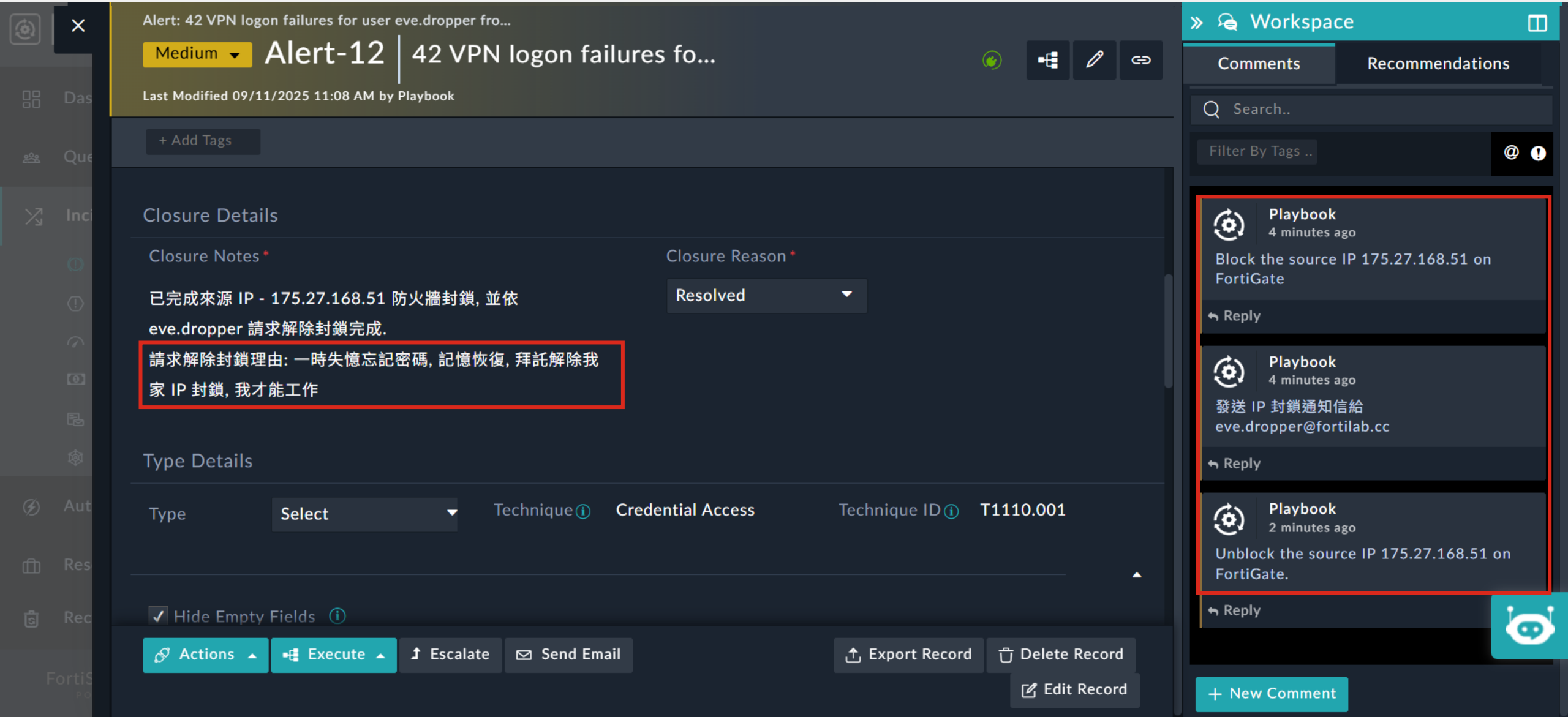
模擬場景 — VPN 登入異常處置

解除 IP 封鎖 – 使用者自助「快速解鎖流程」申請表單



模擬場景 — VPN 登入異常處置

FortiSOAR – IT 可於事後查詢告警與所有自動化處理流程細節



Fortinet 深研 AI 數十載，極致淬鍊







第六代

機器學習引擎演進

感知人工智慧

了解輸入

- 參見
- 解讀
- 想想看

>300 頂尖資深 AI 工程師

生成式人工智慧

產生輸出

- 總結
- 分析
- 建造

>500 全球專利與專利技術

代理型人工智慧

採取行動

- 計畫
- 決定
- 執行

>100 AI 與 ML 原生創新功能

>30 全方位搭載 AI 之產品

© Fortinet Inc. All Rights Reserved.

Fortinet AI 原生資安聯防架構

全面治理

Shadow AI Lockdown

FortiOS
FortiGate
FortiDLP
FortiSASE
FortiWeb
FortiClient
FortiNDR
FortiAuthenticator

極致防護

LLM Security

FortiAIGate
FortiWeb

AI Factory

FortiGate
FortiWeb
FortiDLP
FortiAnalyzer
FortiCNAPP
FortiSIEM
FortiAIGate
FortiPAM

Autonomous Threat Detection

FortiData
FortiMail
FortiSandbox
FortiNDR
FortiEDR
FortiRecon
FortiWeb
FortiAIOps
FortiGuard

高效維運

Agentic Framework

FortiManager
FortiAnalyzer
FortiDLP
FortiSASE
FortiSOAR
FortiNDR
FortiWeb
FortiPAM

FortiAI 已嵌入與整合 在安全織網平台中

© Fortinet Inc. All Rights Reserved.



FORTINET

AI 不會因為資安而停止
資安也不能等AI全面上線後才開始。