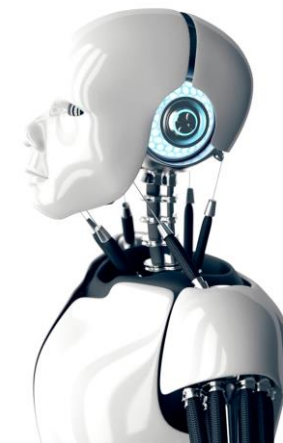





FORTINET[®]

透過 **AI SecOps** 讓資安防護「看的到、找得到、管的到」

李尚峰 Jarvis
ljarvis@fortinet.com



Fortinet 四大主軸資安解方：降低複雜性、提高營運效率、優化用戶體驗



Secure Networking

橫跨網路與資安有效整合
涵蓋有線、無線、端點與
新世代防火牆



Security Operation (SecOps)

透過 AI-Powered 的高度
自動化，帶來更有效率的
維運管理



Universal SASE

為來自各地工作的使用者
提供一致的安全管控，達
成最佳的使用者體驗



ASIC Appliance



Virtual



Cloud Native



As-a Service



Container



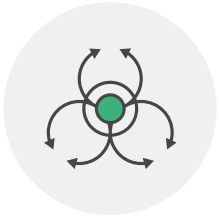
Secure Operational Technology

實現融合 IT/OT 生態系統的安全性。提供以 OT 為中心的功能和產品，
將 Security Fabric 功能擴展到工廠、車間、遠端位置和船舶中的 OT 網路



威脅情勢比起以往更複雜

魚叉式網路釣魚和深度偽造



更有針對性、更自動化、更多管道

N-day 漏洞



新漏洞在前7天內就會被網路犯罪分子廣泛利用（在大多數情況下，修補週期仍然是每30天一次）

網路實體攻擊



2023 年上半年針對網路實體資產的攻擊呈上升趨勢，

活躍的威脅行為者



2023年1月-6月有30%的APT族群被檢測為活躍

勒索病毒



勒索軟體感染時間從 5 天縮短至 5 小時

雲端風險



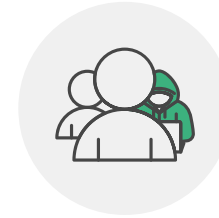
69% 的公司使用兩個或更多雲

供應鏈攻擊



12% 的資料外洩源自於軟體供應鏈攻擊

內部風險



內部風險事件較去年同期成長 +32%

保護並不完美 – SecOps 必須專注於**威脅偵測、調查和回應**

AI 驅動的安全營運 (Fortinet SecOps)

導入 AI 與機器學習，結合大數據情資分析，對抗新型態與未知的資安威脅

基於網路資訊流 Network-Based



Sandbox



NDR



Mail

基於日誌與記錄 Log-Based



Analyzer



SIEM



SOAR

Key Use Cases

- Fabric 可見度
- Fabric 分析
- Fabric 自動化

Key Use Cases

- 多供應商可見度
- 進階關聯分析
- 事件管理

Key Use Cases

- 多供應商自動化
- 流程編排
- 管理威脅情報

基於端點行為模式 Endpoint-Based



EDR



Deceptor



FortiGuard Lab.

基於資安情資服務 TIS-Based



FortiRecon

Digital Risk Protection Service (DRPS)



2023 威脅態勢分析 (依地區)

NOT FOR MEDIA RELEASE

台灣依然是資安威脅高度關注的地區

Powered by FortiGuard Labs



Total Threats Detected

970.31bn



Exploit Techniques Detected

111.78bn



Malware Distribution Detected

913.13M



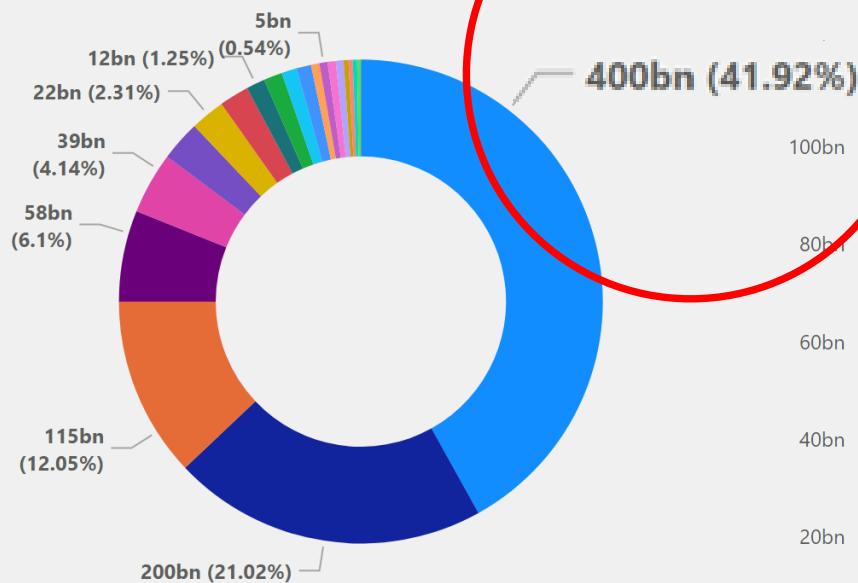
Botnet Activity Detected

2.79bn

Malicious Activity Distribution by Country

Country Name

- Taiwan
- Indonesia
- Thailand
- Japan
- India
- Korea
- China
- United Arab Emirates
- Australia
- Kuwait
- Malaysia
- Hong Kong
- Viet Nam
- Saudi Arabia
- Qatar

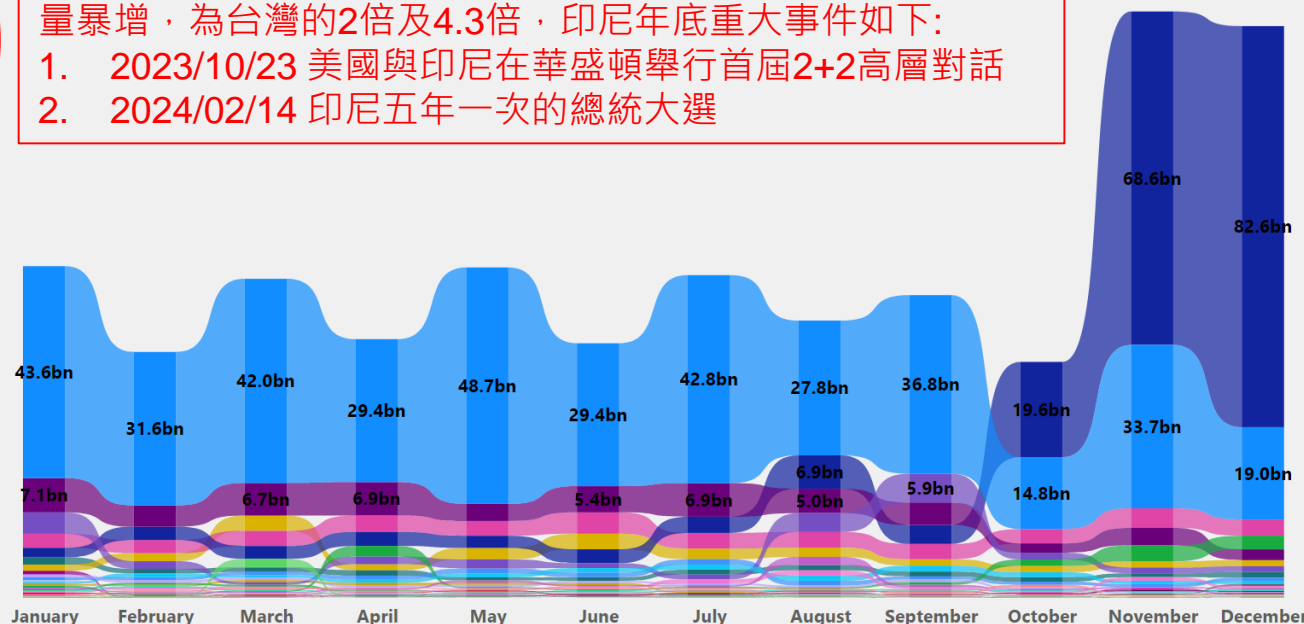


Behavioral Trend Analysis by Country



台灣總年度被攻擊次數還是第一，印尼最後兩個月被攻擊數量暴增，為台灣的2倍及4.3倍，印尼年底重大事件如下：

- 2023/10/23 美國與印尼在華盛頓舉行首屆2+2高層對話
- 2024/02/14 印尼五年一次的總統大選



2023 TAIWAN 威脅態勢分析

NOT FOR MEDIA RELEASE

勒索病毒下半年暴增 2.88 倍

Powered by FortiGuard Labs



Total Threats Detected

399.7bn

每秒鐘1.4萬次攻擊



Exploit Techniques Detected

6.12bn



Malware Distribution Detected

167.08M



Botnet Activity Detected

219.52M

Malicious Activity by Quarter



Growth Year over Year

7.43%

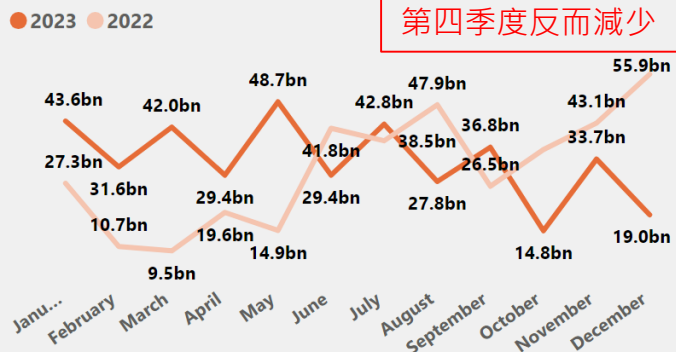
Cyber Kill Chain Model

Crime as a Service
DarkWeb

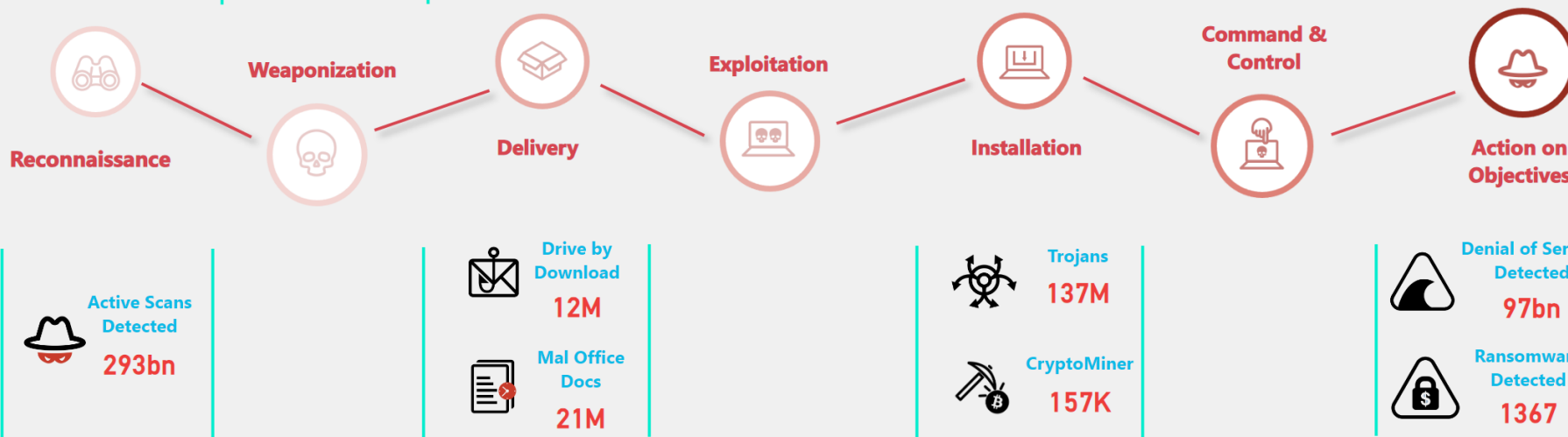
DoublePulsar
1bn
Web Vuls
142M

Andromeda
2M
IoT- MIRAI
30M

Behavioral Trend Analysis by Month



第四季度反而減少



上半年8M · 增加13M · 下半年增加1.6倍

上半年352 · 增加1015 · 下半年增加2.88倍



TLP: GREEN

© Fortinet Inc.

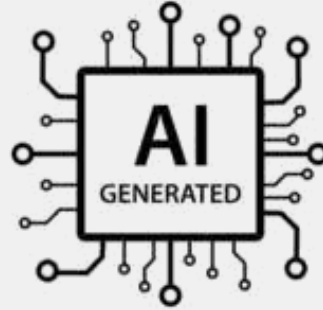
人工智能應用與資訊安全領域發展

保護人工智慧的資安

(Cybersecurity for AI)

保護人工智慧系統與服務開發、訓練、使用過程中的資訊安全，做為**可信賴人工智慧**的基礎。

人工智慧



- ✓ 人工智慧場域可信賴
- ✓ 人工智慧系統安全性
- ✓ 人工智慧的人類基本價值保護
- ✓ 人工智慧對抗性攻擊
- ✓ 訓練資料及輸出保護

強化

強化

攻擊

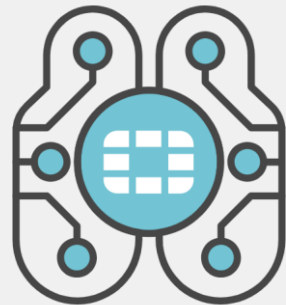
防護

使用人工智慧強化資安

(AI for Cybersecurity)

在資訊安全各領域中運用人工智慧，落實強度更高的控管，以達到更高的資安成熟度。

- ✓ 威脅偵測
- ✓ 異常行為分析
- ✓ 主動式防火牆
- ✓ 智慧鑑識
- ✓ 惡意程式分析



資安防護

攻擊

對抗

人工智慧驅動的攻擊

(AI against Cybersecurity)

同樣的，駭客也會運用人工智慧技術來強化犯罪的效率，或者嘗試使用更新穎的犯罪手法。

- ✓ 系統弱點分析
- ✓ 社交工程攻擊
- ✓ 假消息
- ✓ Deep Fake 詐騙
- ✓ AI 強化的DDOS攻擊

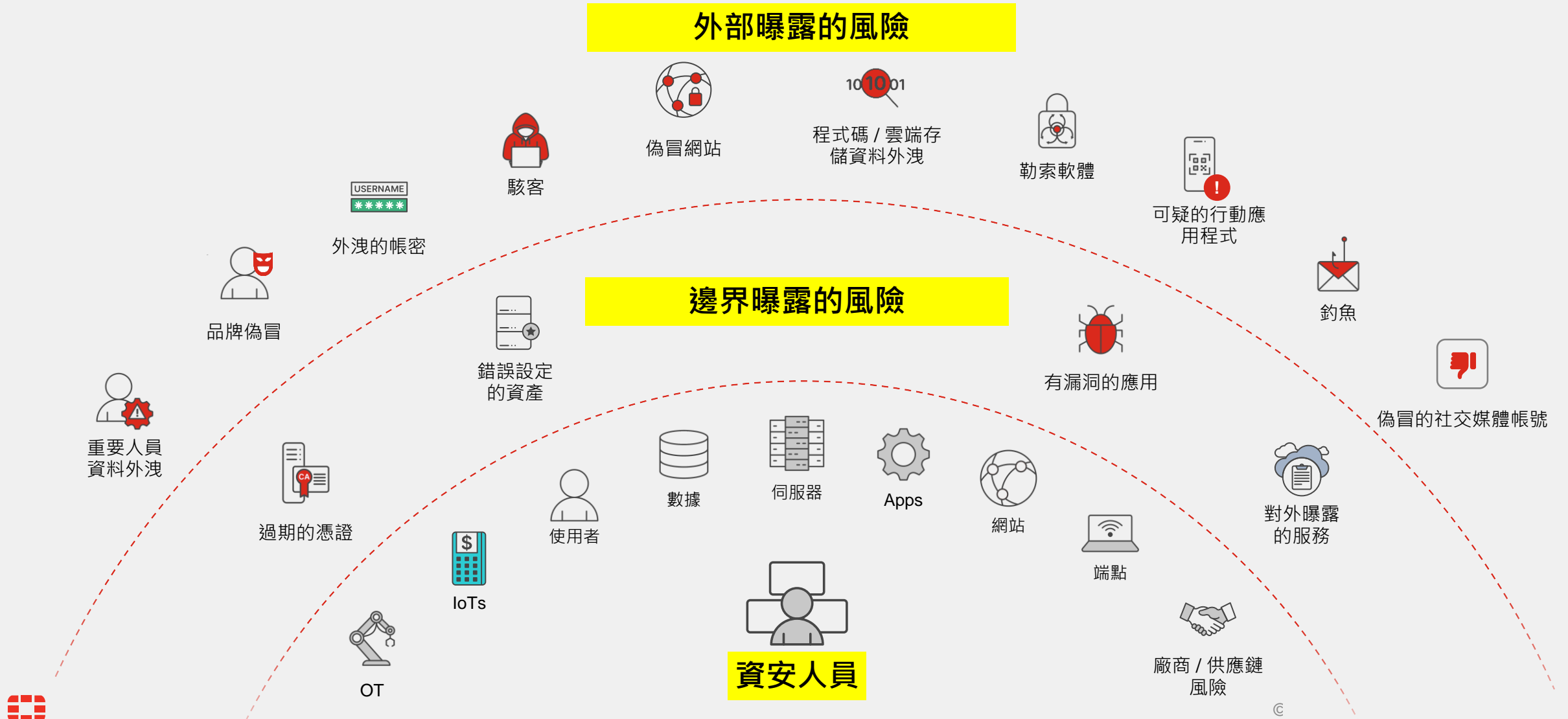


攻擊威脅



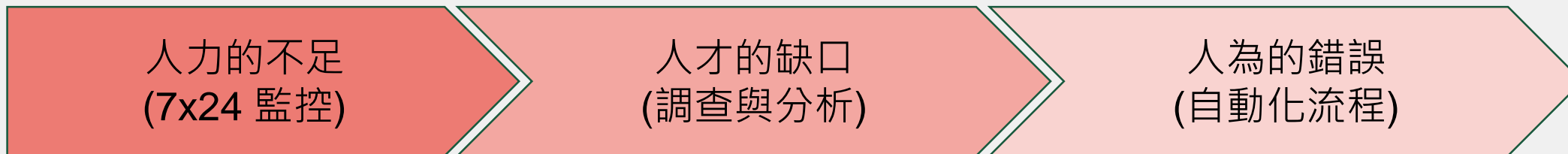
持續增加的數位風險，讓資安人員陷入瓶頸

1. 告警疲勞：過多的告警資訊無法負荷放棄解讀 2. 資安過勞：頻繁的登入多種設備影響調查效率

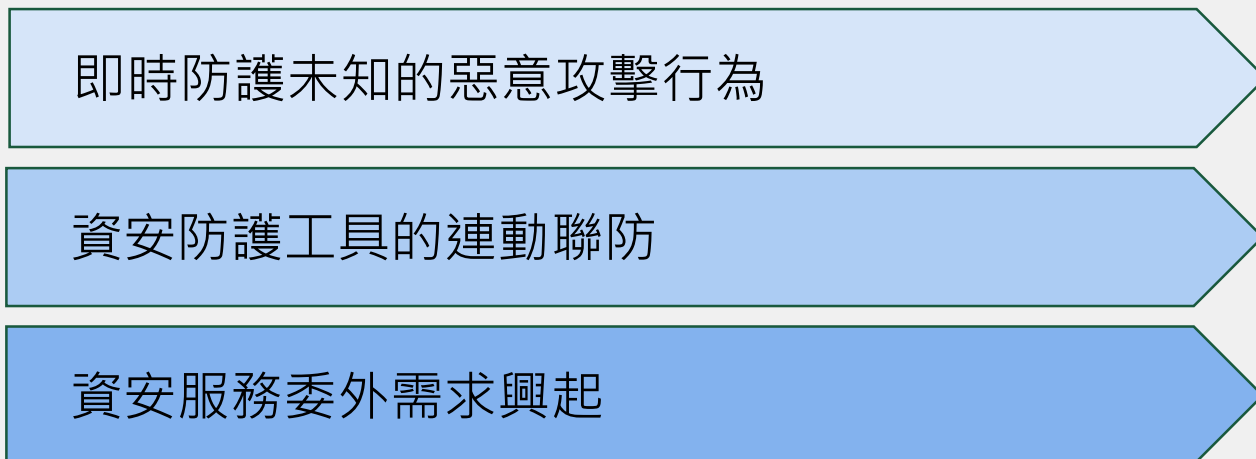


防護駭客攻擊的重點

- 善用整合人工智慧，機器學習及大數據情資的工具，解決資安防護的瓶頸，打造「看的到、找得到、管的到」的資安防護



- 新世代資安防護要點





故事的開始...



客戶架構圖 (既有)



寄件者: 9. [redacted]@chi. [redacted].com
<97 [redacted]@cl. [redacted].com>
寄件 信箱: 2024年 [redacted] 6日 05
收件者: C. [redacted]@chi. [redacted].com
mc [redacted].com>
主旨: 我強烈建議您檢查這封電子郵件中的資訊。

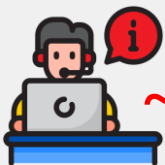
問候，
抱歉，但我必須先說壞消息。

幾個月前，我獲得了對您與作業系統關聯的帳戶的存取權限，因此也獲得了您用於網路瀏覽的所有裝置的存取權限。然後我就可以輕鬆地在您的所有裝置上安裝特殊軟體來追蹤您的每次按鍵和滑鼠移動。

此後，訪問您的個人電子郵件 9. [redacted]@chi. [redacted].com 不再是問題。

我不是天才，也不是優秀的駭客。你只是完全不關心數位衛生和網路安全。你似乎完全不知道

他牌 SOC
委外監控服務

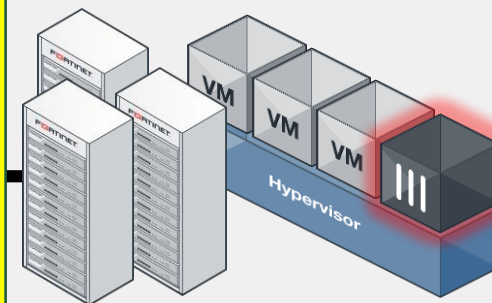


~ 無安全

面對駭客入侵， 資安防護整合的要求：

1. 駭客進來
我能知道嗎？(看的到)
2. 駭客行為
我能找到嗎？(找的到)
3. 駭客破壞
我能擋住嗎？(管的到)

流量 ~



資安防護常見的情境

- A牌 防火牆 > 設定有問題嗎？
- B牌 防火牆 > log 沒看到異常ㄚ？
- C牌 IPS > 告警那麼多！如何收斂？
- D牌 WAF > log 如何解讀？
- E牌 網路分析 > 告警那麼多！沒看！
- G牌 防毒系統 > 沒有告警ㄚ？
- H牌 EDR > 開了好多白名單，有關係嗎？
- SOC 委外監控報表 > 例行傳簽歸檔，沒看！

• 每樣產品我都只會一點，根本不熟～

問題在哪裡？搞得我好亂啊 !!!



攻擊者入侵網路後，駐留時間越長，組織蒙受的損失越多

威脅檢測到回復的平均時間



52%

受訪組織稱，相較於兩年前，目前組織 **SecOps** (安全營運) 更具挑戰性，涉及各類威脅、攻擊面、攻擊數量/複雜性¹

美國證券交易委員會 (SEC) 新規範

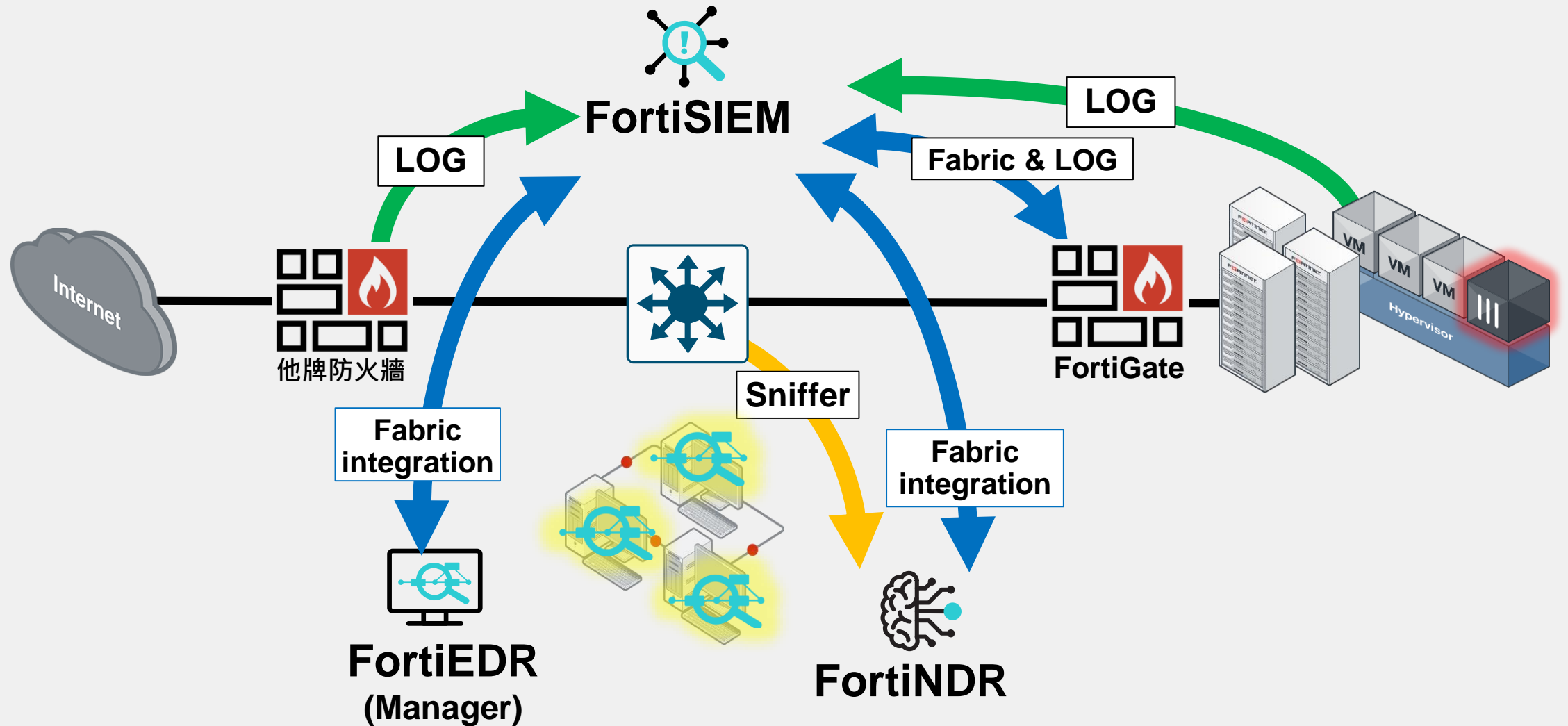
4 天

內部需披露重大網路安全事件

\$940 萬

平均入侵損失

客戶架構圖 (Fortinet SecOps 調查分析)



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

FortiSIEM 儀表板 關聯分析 告警事故 派工管理 CMDB 資源庫 工作 系統管理

動作 告警總覽 List 風險分析

Tactics: 全部 搜尋設備... (10/10)

Status: 已啟用 時間範圍: Last 2 Hours

1/1 10

設備	Reconnaissance	Resource Development	Initial Access	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad				12	5	11	3		1	2	3	7
laba	1		2	6	2	1	4	3	1	1		
FDC-Decoy-WIN7	1						1	4				
WIN10-LoCo	1						1	4				
211.141.78.56			1		1			1		1		
195.211.29.229											3	
www.abcd.z2.dca1.com										1		
www.xyz.z1.dca0.com										1		
221.229.172.66												

Initial Access Incidents

嚴重性類別	最後一次	事件描述	MITRE ATT&CK 技術	源 IP	目標 IP	狀態	處理狀態
MEDIUM	Jul 02 2023, 03:21:30 PM	Windows: Failed Logins with Different Accounts ...	Persistence, Privilege Escalation, Defense Evasion, Initial Access	211.141.78.56	192.168.68.74	Active	Open
HIGH	Jul 02 2023, 03:21:00 PM	VNC from Internet	Persistence, Lateral Movement, Command And Control, Initial Access	211.141.78.56	192.168.68.74	Active	Open

初始存取
FortiGate/FortiNDR
發現 VNC 遠端桌面連線
至受駭者電腦

VNC from Internet

211.141.78.56 192.168.68.74



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

The screenshot displays the FortiSIEM interface with a MITRE ATT&CK matrix and a detailed incident log. A callout box highlights a specific event: "執行運作 FortiEDR 偵測到利用 Powershell 執行的異常行為並建立後門" (Execution operation: FortiEDR detected abnormal behavior using Powershell and established a backdoor). The matrix shows various attack techniques across different hosts, with a '6' in the 'Defense Evasion' column for the 'laba' host. The incident log below shows a 'HIGH' severity event titled 'Backdoor Found' with the message 'FortiEDR-Security-Malicious-Logged'. A callout box provides details for the event: 'User: admin' and 'Process Name: powershell.exe'. A red arrow points to the 'net1.exe' process in the log.

設備	Reconnaissance	Resource Development	Initial Access	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1	12	5	11	3		1	2	3	7
laba	1		2	6	2	1	4	3	1	1		
FDC-Decoy-WIN7	1						1	4				
WIN10-LoCo	1						1	4				
211.141.78.56			1		1			1		1		
195.211.29.229											3	
www.abcd.z2.dca1.com										1		
www.xyz.z1.dca0.com										1		
221.229.172.66												

嚴重性類別	最後一次發生	技術	告警事故狀態	解決處理狀態
HIGH	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Active	Open
MEDIUM	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Active	Open
MEDIUM	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Active	Open
MEDIUM	Jul 02 2023, 03:21:00 PM	FortiEDR-Security-Malicious-Logged	Active	Open

執行運作
FortiEDR 偵測到利用 Powershell 執行的異常行為並建立後門

Backdoor Found
FortiEDR-Security-Malicious-Logged

User: admin Process Name: powershell.exe



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

The screenshot displays the FortiSIEM interface with the MITRE ATT&CK framework active. A callout box highlights the 'Discovery' technique, specifically 'FortiDeceptor 部署的誘餌 (Decoy) 發現 Port Scan 行為'. Below, a table shows a 'Discovery Incidents for FortiDeceptor Port Scan' with details for a scan on 192.168.210.10 targeting 192.168.210.101.

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Command And Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3				7
laba	1		2	6	2	1	4	3		1		
FDC-Decoy-WIN7	1								1	4		
WIN10-LoCo	1								1	4		
211.141.78.56			1		1				1		1	
195.211.29.229											3	
www.abcd.z2.dca1.com										1		
www.xyz.z1.dca0.com										1		
221.229.172.66												

嚴重性類別	最後一次發生	技術	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
MEDIUM	Jul 02 2023, 04:23:30 PM	FortiDeceptor Port Scan	Discovery,Reconnaissance	System Service Discovery, System Network Connections Discovery, ...	192.168.210.10 192.168.210.101	Active	Open



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

The screenshot displays the FortiSIEM interface with the MITRE ATT&CK Incident Explorer view. A callout box highlights the 'Initial Access' phase, specifically 'FortiDeceptor 部署的誘餌 (Decoy) 發現 RCE 漏洞利用 (MS RDP T120)'. Below this, a table shows incident details for 'FortiDeceptor IPS Attack'.

Severity	Time	Event Name	Category	Technique	Source IP	Destination IP	Port	Description	Status	Action
MEDIUM	Jul 02 2023, 05:12:00 PM	FortiDeceptor IPS Attack - ...	Lateral Movement	Exploitation of Remote Services	192.168.210.10	192.168.210.101	3389	remote_access: MS.Windows.RDP.Channel.MS_T120.Remote.Code.Execution...	Active	Open
MEDIUM	Jul 02 2023, 05:12:00 PM	FortiDeceptor IPS Attack - ...	Lateral Movement	Exploitation of Remote Services	192.168.210.10	192.168.210.101	445	remote_access: MS.Windows.RDP.Channel.MS_T120.Remote.Code.Execution...	Active	Open
MEDIUM	Jul 02 2023, 05:12:00 PM	FortiDeceptor IPS Attack - ...	Lateral Movement	Exploitation of Remote Services	192.168.210.10	192.168.210.101	135	remote_access: MS.Windows.RDP.Channel.MS_T120.Remote.Code.Execution...	Active	Open

橫向移動
FortiDeceptor 部署的誘餌 (Decoy) 發現 RCE 漏洞利用 (MS RDP T120)

FortiDeceptor IPS Attack - ...

192.168.210.10
192.168.210.101
Destination TCP/UDP ...: 3389

FortiDeceptor IPS Attack - ...

remote_access: MS.Windows.RDP.Channel.MS_T120.Remote.Code.Execution...

Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 **MITRE ATT&CK 資安框架**，顯示主機在資安攻擊鏈所處的狀態

帳密存取
FortiSIEM 從伺服器日誌偵測到暴力密碼破解
取得伺服器存取權限

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3			1	2	3	7
laba	1		2	6	2	1	4	3	1	1		1		
FDC-Decoy-WIN7	1								1	4				
WIN10-LoCo	1								1	4				
211.141.78.56			1		1					1		1		
195.211.29.229													3	
www.abcd.z2.dca1.com												1		
www.xyz.z1.dca0.com												1		

嚴重性類別	事件描述	MITRE ATT&CK	IP	主機名	用戶名	狀態	操作
MEDIUM	Brute Force Host Login Success	Credential Access	192.168.68.74	W2K12R2-AD	Administrator	Active	Open
HIGH	Brute Force Host Login Success	Credential Access	192.168.68.74	W2K12R2-AD	Administrator	Active	Open



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

持續潛伏
FortiSIEM 從伺服器日誌偵測到網域伺服器被建立後門帳號

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3			1	2	3	7
laba	1		2	6	2	1	4	3	1	1		1		
FDC-Decoy-WIN7	1								1	4				
WIN10-LoCo	1								1	4				
211.141.78.56			1		1					1		1		
195.211.29.229													3	
www.abcd.z2.dca1.com												1		
www.xyz.z1.dca0.com												1		
???.???.???.???														

Windows User Created

嚴重性類別	最後一次發生	戰術	技術	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
MEDIUM	Jul 02 2023, 03:23:00 PM	Windows User Created	Persistence	Create Account: Local Account	W2K12R2-AD	User: administrator Target User: Administrator ... Show More	Active	Open
MEDIUM	Jul 02 2023, 03:23:00 PM	Windows User Account Enabled	Persistence	Account Manipulation: Additional Clo...	W2K12R2-AD	User: administrator Target User: Administrator ... Show More	Active	Open



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 MITRE ATT&CK 資安框架，顯示主機在資安攻擊鏈所處的狀態

The screenshot displays the FortiSIEM interface. At the top, there are navigation tabs for '告警總覽', '風險分析', '探索分析', and 'UEBA'. A callout box highlights a '特權提升' (Privilege Escalation) event: 'FortiSIEM 從伺服器日誌偵測到後門帳號被加入到管理者群組'.

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3			1	2	3	7
laba	1		2	6	2	1	4	3	1	1		1		
FDC-Decoy-WIN7	1								1	4				
WIN10-LoCo	1								1	4				
211.141.78.56			1		1					1		1		
195.211.29.229													3	
www.abcd.z2.dca1.com												1		
www.xyz.z1.dca0.com												1		

Below the matrix, a 'Privilege Escalation' event is detailed:

嚴重性類別	時間	事件描述	技術	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
MEDIUM	Jul 02 2023, 04:25:00 PM	Windows: User Added to Local Administrators	Persistence, Privilege Escalation, Defense Evasion...	Valid Accounts: Local Accounts	W2K12R2-AD User: administrator Target User: Administrator	Object Name: CN=Administrators User: Administrator CN=Builtin DC=se	Active	Open
MEDIUM	Jul 02 2023, 04:24:00 PM	Group Policy Object Modified	Privilege Escalation, Defense Evasion	Domain Policy Modification: Gr...	W2K12R2-AD User: Administrator Domain: SE_Lab	Object Name: CN=Administrators User: Administrator CN=Builtin DC=se	Active	Open



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 **MITRE ATT&CK 資安框架**，顯示主機在資安攻擊鏈所處的狀態

The screenshot displays the FortiSIEM interface with the MITRE ATT&CK framework. A callout box highlights that logs from a server are compressed and packaged. Below, a table shows the attack chain for various assets, and an alert details a file creation event on W2K12R2-AD.

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3			1	2	3	7
laba	1		2	6	2	1	4	3	1	1		1		
FDC-Decoy-WIN7	1								1	4				
WIN10-LoCo	1								1	4				
211.141.78.56			1		1					1		1		
195.211.29.229													3	
www.abcd.z2.dca1.com												1		
www.xyz.z1.dca0.com												1		

資料收集
FortiSIEM 從伺服器日誌偵測到伺服器的檔案被壓縮打包

Agent FIM: Windows File or Directory Created
W2K12R2-AD
User: Administrator
File Name: c:\Windows\Temp\87b1-87f599f04a15.gzip

MEDIUM Jul 02 2023, 05:12:30 PM Agent FIM: Windows File or Directory Created Impact,Collection Data Staged: Local Data Staging, Data Manipulation... W2K12R2-AD User: Administrator File Name: c:\Windows\Temp\87b1-87f599f04a15.gzip Active Open



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 **MITRE ATT&CK 資安框架**，顯示主機在資安攻擊鏈所處的狀態

命令與控制
FortiSIEM 偵測到利用 DGA 演算法的異常網域名稱連線需求

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3			1	2	3	7
laba	1		2	6	2	1	4	3	1	1		1		
FDC-Decoy-WIN7	1								1	4				
WIN10-LoCo	1								1	4				
211.141.78.56			1		1					1		1		
195.211.29.229													3	
www.abcd.z2.dca1.com												1		
www.xyz.z1.dca0.com												1		

Dynamically generated host name: malware likely

嚴重性類別	時間	描述	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
MEDIUM	Jul 02 2023, 05:12:30 PM	Dynamically generated host name: malware likely	Command And Control	Dynamic Resolution: Domain Generation Algorithms	192.168.100.100 www.xyz.z1.dca0.com Domain Name Entropy: 3.69	Active	Open
MEDIUM	Jul 02 2023, 05:12:30 PM	Dynamically generated host name: malware likely	Command And Control	Dynamic Resolution: Domain Generation Algorithms	192.168.100.100 www.abcd.z2.dca1.com Domain Name Entropy: 5.21	Active	Open

Dynamic Resolution: Domain Generation Algorithms 192.168.100.100 www.abcd.z2.dca1.com



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 **MITRE ATT&CK 資安框架**，顯示主機在資安攻擊鏈所處的狀態

資料洩漏
FortiSIEM 從流量智能分析與 IOC 黑名單，偵測到對 C2 網站外傳資料

設備	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
w2k12r2-ad			1		12	5	11	3			1	2	3	7
laba	1		2	6	2	1	4	3	1	1		1		
FDC-Decoy-WIN7	1								1	4				
WIN10-LoCo	1								1	4				
211.141.78.56			1		1							1		
195.211.29.229													3	
www.abcd.z2.dca1.com														
www.xyz.z1.dca0.com														
221.229.172.66														

Traffic to FortiGuard Malware IP List
Large Outbound Transfer

195.211.29.229

Sent Bytes64: 4.91 GB

Sent Bytes64: 4.91 GB

嚴重性類別	最後一次發生	告警事故	戰術	技術	IP	IP	狀態	狀態
HIGH	Jul 02 2023, 05:12:30 PM	Traffic to FortiGuard Malware IP List	Exfiltration	Exfiltration Over C2 Channel	192.168.100.100	195.211.29.229	Active	Open
MEDIUM	Jul 02 2023, 05:12:30 PM	Large Outbound Transfer	Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Sy...	192.168.100.100	195.211.29.229	Sent Bytes64: 4.91 GB	Active
MEDIUM	Jul 02 2023, 05:12:30 PM	Large Outbound Transfer To Outside My Country	Exfiltration	Exfiltration Over Alternative Protocol: Exfiltration Over Sy...	192.168.100.100	195.211.29.229	Sent Bytes64: 4.91 GB	Active



Fortinet SecOps 導入，撥雲見日 (事件看的到、找得到、管的到)

AI/ML 關聯分析產生告警，對應 **MITRE ATT&CK 資安框架**，顯示主機在資安攻擊鏈所處的狀態

造成影响
FortiSIEM 從伺服器
日誌偵測到伺服器檔
案被刪除

The screenshot displays the FortiSIEM interface with the MITRE ATT&CK framework. The framework categories and their counts are as follows:

Category	Count
Reconnaissance	1
Resource Development	0
Initial Access	1
Execution	6
Persistence	2
Privilege Escalation	1
Defense Evasion	4
Credential Access	3
Discovery	1
Lateral Movement	1
Collection	1
Command And Control	1
Exfiltration	3
Impact	7

Below the framework, a table lists specific incidents:

Host	MITRE ATT&CK Category	Count
w2k12r2-ad	Initial Access	1
w2k12r2-ad	Persistence	12
w2k12r2-ad	Privilege Escalation	5
w2k12r2-ad	Defense Evasion	11
w2k12r2-ad	Credential Access	3
w2k12r2-ad	Discovery	1
w2k12r2-ad	Lateral Movement	1
w2k12r2-ad	Collection	1
w2k12r2-ad	Command And Control	2
w2k12r2-ad	Exfiltration	3
w2k12r2-ad	Impact	7
laba	Reconnaissance	1
laba	Initial Access	2
laba	Execution	6
laba	Persistence	2
laba	Privilege Escalation	1
laba	Defense Evasion	4
laba	Credential Access	3
laba	Discovery	1
laba	Lateral Movement	1
laba	Command And Control	1
FDC-Decoy-WIN7	Reconnaissance	1
FDC-Decoy-WIN7	Discovery	1
FDC-Decoy-WIN7	Lateral Movement	4
WIN10-LoCo	Reconnaissance	1
211.141.78.56	Initial Access	1
211.141.78.56	Persistence	1
195.211.29.229	Impact	1
www.abcd.z2.dca1.com	Impact	1
www.xyz.z1.dca0.com	Impact	1
221.229.172.66	Impact	1

Incident details for 'Agent FIM: Windows File or Directory Deleted' are shown below:

Host	User	File Name	Process Name
W2K12R2-AD	Administrator	c:\OA\新產品發表計畫書.txt	
W2K12R2-AD	Administrator	c:\OA\員工薪資查核表.rtf	C:\Program Files\Windows NT\Acc...
W2K12R2-AD	Administrator	c:\OA\公司Q1財報會議記錄.rtf	C:\Program Files\Windows NT\Acc...

The incident list at the bottom shows three entries for 'Agent FIM: Windows File or Directory Deleted' with a severity of MEDIUM, occurring on Jul 02 2023, 05:12:30 PM. The details for each entry are:

- Host: W2K12R2-AD, User: Administrator, File Name: c:\OA\新產品發表計畫書.txt
- Host: W2K12R2-AD, User: Administrator, File Name: c:\OA\員工薪資查核表.rtf, Process Name: C:\Program Files\Windows NT\Acc...
- Host: W2K12R2-AD, User: Administrator, File Name: c:\OA\公司Q1財報會議記錄.rtf, Process Name: C:\Program Files\Windows NT\Acc...



FortiAI 能為我們做些甚麼？



提升洞察力

建構整個維運環境的知識庫，從網路、用戶、傳輸數據的應用以及資安態勢



協助決策制定

依據洞察後狀態推薦管理者接續的行動制定，以上是基於維運環境的分析並執行最佳實踐執行



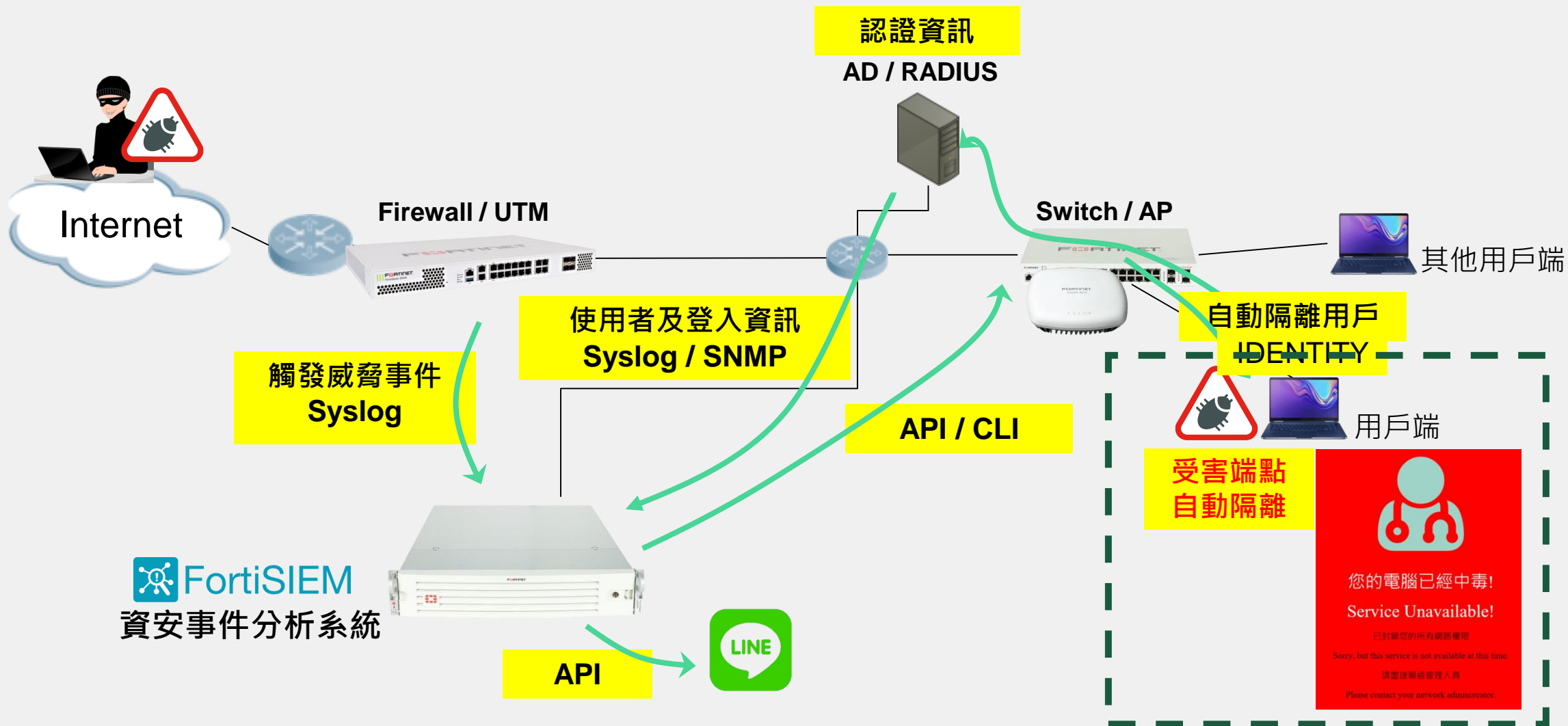
自動化腳本執行

通過管理者同意後的自動化腳本來執行決策後的推薦行動



Fortinet SecOps 協作聯防與回應自動化 (SOAR)

FortiSIEM 資安聯防協作自動回應處理示意圖 -- 發現受駭端點自動隔離並且通報



AI For 日常智能維運 (整合 OpenAI)

與生成式 AI 整合 AI for Operation



AI for 日常智能維運

- ✓ 整合 OpenAI (ChatGPT in FortiSIEM)
- ✓ 互動式問答, 分析師日常維運輕鬆尋求 AI 助理協助
- ✓ 查詢會遮蓋敏感資料, 保護重要資訊不外洩

FortiSIEM 結合生成式 AI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？



顯示事件型式 自動換行 執行 Playbook 運行連接器

◀ 50 2/3 132 ▶

Event Receive Time	Reporting IP	Event Type	Event Name	User	Source IP	Raw Event Log
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-ips-signature-32587	FortiGate-ips-signature-325...	user5	168.10.199.186	<185>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-Generic	Generic FortiGate Event	user	178.10.199.186	<188>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-webfilter-url-firewal...	The URL belongs to a denie...	user3	168.10.199.186	<188>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	user4	171.10.199.186	<190>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-auth-successful	FortiGate Authentication su...	user	1.1.1.1	<189>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	user5	170.10.199.186	<190>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	user5	174.10.199.186	<190>date=2024-02-16 time=20:08:27 devname="CoreFW" d...

FortiSIEM 結合生成式 AI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？

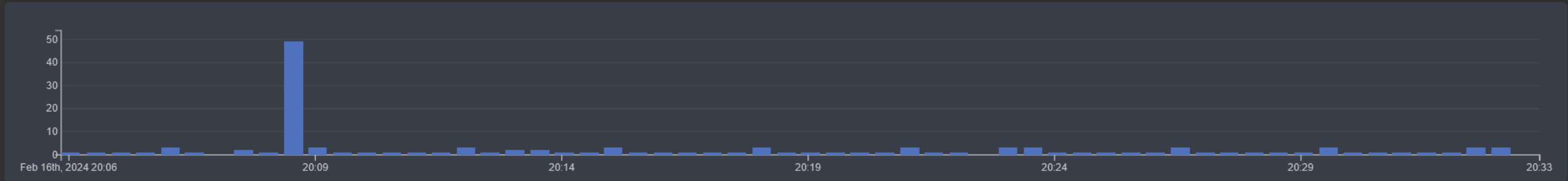
FortiSIEM 儀表板 關聯分析 告警事件 派工管理 CMDB 資源庫 工作 系統管理

Search Machine Learning Investigation

動作 [1] 歷史性事件於 10.200.250.254

Reporting IP = 10.200.250.254 AND User IS NOT NULL 執行 Table 15m 1h 1d 7d 30d

歷史性事件於 10.200.250.254 - Last 30 Minutes*



顯示事件型式 自動換行 執行 Playbook 運行連接器 2/3 132

Event Receive Time	Reporting IP	Event Type	Event Name	User	Source IP	Raw Event Log
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-ips-signature-32587	FortiGate-ips-signature-325...	user5	168.10.199.186	<185>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-Generic	Generic FortiGate Event	user	178.10.199.186	<188>date=2024-02-16 time=20:08:27 devr Show Detail
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-webfilter-url-firewal...	The URL belongs to a denie...	user3	168.10.199.186	<188>date=2024-02-16 time=20:08:27 devr Fortinet Advisor
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	user4	171.10.199.186	<190>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-auth-successful	FortiGate Authentication su...	user	1.1.1.1	<189>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	user5	170.10.199.186	<190>date=2024-02-16 time=20:08:27 devname="CoreFW" d...
Feb 16, 2024, 08:08:28 PM	10.200.250.254	FortiGate-appctrl-ips-pass	FortiGate appctrl ips pass	user5	174.10.199.186	<190>date=2024-02-16 time=20:08:27 devname="CoreFW" d...

FortiSIEM 結合生成式 AI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？

The image shows a screenshot of the FortiSIEM web interface. A 'Fortinet Advisor' chat window is open in the foreground. The chat window contains a disclaimer and instructions for using the AI assistant. A blue arrow points from the chat window to the background interface, and a white arrow points from the chat window to the text below.

Fortinet Advisor Feb 16 2024, 07:55:23 PM

Any information submitted to Fortinet Advisor may be submitted to OpenAI. Fortinet does not verify or correct the responses received from OpenAI and has no responsibility for them. You must exercise discretion and independently verify any information or recommendations you receive from OpenAI before relying on them.

Make sure you have entered ChatGPT Key in Settings > Analytics > ML / AI > Fortinet Advisor.

To start, select one of the pre-selected questions or type in your own question. Fortinet Advisor can answer generic questions about FortiSIEM installation and operations, create a report, analyze a log or an incident and provide recommendations.

Hello, May I help you ?

問問題前先確定有 ChatGPT 帳號在 FortiAI 內

Type in your question and hit enter or click send. Press UP key to show all pre-selected questions.

Background Interface Details:

- FortiSIEM Logo and Navigation: 儀表板, 關聯分析, 告警事件, 派工管理, CMDB, 資源庫, 工作, 系統管理
- Search and Filter: Search, Machine Learning, Inves, [1] 歷史性事件於 10.200.250.254
- Reporting IP: Reporting IP = 10.200.250.254 AND User IS
- Chart: Bar chart showing event counts over time (Feb 16th, 2024 20:06 to 20:09).
- Table: Table with columns 'Event Receive Time' and 'Reporting IP'. All entries show '10.200.250.254'.
- Execution: 執行, Table, 15m, 1h, 1d, 7d, 30d, 圖表為: COUNT(Matched Events)
- Log: Log entries showing 'e=2024-02-16 time=20:08:27 devname="CoreFW" d...'

FortiSIEM 結合生成式 AI 對告警的 IPS 攻擊事件提供建議

請分析以下 IPS 事件日誌，並告訴我如何處理？

The screenshot displays the FortiSIEM interface with a 'Fortinet Advisor' chat window open. The chat window contains the following text:

Fortinet Advisor Feb 16 2024, 08:36:25 PM

這是一個高嚴重性的入侵防護事件，攻擊的類型是"test_attack"，攻擊來自美國的IP地址，攻擊目標是位於保留區的IP地址。根據政策設定，系統已經檢測到並對此攻擊進行了警報。建議您立即採取措施來應對此攻擊，例如加強防火牆規則、封鎖攻擊源IP地址或尋求進一步的安全專業支援。

Below the chat window, a table of event logs is visible:

Event Receive Time	Reporting IP
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254
Feb 16, 2024, 08:08:28 PM	10.200.250.254

At the bottom of the chat window, there is a prompt: "Type in your question and hit enter or click send. Press UP key to show all pre-selected questions."

FortiSIEM 結合生成式 AI 對告警的 IPS 攻擊事件提供建議

Fortinet Advisor 查詢時會遮蓋敏感資料，保護機敏資訊不外洩

The screenshot displays the FortiSIEM interface. At the top, there is a navigation bar with various icons and labels: 儀表板, 關聯分析, 告警事件, 派工管理, CMDB, 資源庫, 工作, 系統管理. Below this, there are tabs for Search, Machine Learning, and Investigation. A search bar contains the query: System Event Category = 2 AND Event Type = PH_AUDIT_GENAI_USER_QUERY. The results are displayed as a bar chart titled "FortiSIEM ChatGPT Queries - Last 1 Hour*" and a table below it. The table has columns for Event Receive Time, Query Data, Token Count, Price, and Raw Event Log. A red line highlights the first row of the table, and a yellow hand icon points to the Raw Event Log column.

Event Receive Time	Query Data	Token Count	Price	Raw Event Log
Feb 16, 2024, 08:36:24 PM	{請分析以下日誌，用台語告訴...	4,544	0.01	<14>Feb 16 20:36:24 fsm-super172 phGenerativeAI: [PH_AUDIT_GENAI_USER_QUERY]:[eventSeve...
Feb 16, 2024, 08:30:28 PM	{請分析以下日誌，用台語告訴...	6,206	0.02	<14>Feb 16 20:30:28 fsm-super172 phGenerativeAI: [PH_AUDIT_GENAI_USER_QUERY]:[eventSeve...
Feb 16, 2024, 08:20:00 PM	{請分析以下日誌，用台語告訴...	4,789	0.01	<14>Feb 16 20:20:00 fsm-super172 phGenerativeAI: [PH_AUDIT_GENAI_USER_QUERY]:[eventSeve...
Feb 16, 2024, 08:18:29 PM	{請分析以下日誌，並告訴我如...	4,055	0.01	<14>Feb 16 20:18:29 fsm-super172 phGenerativeAI: [PH_AUDIT_GENAI_USER_QUERY]:[eventSeve...
Feb 16, 2024, 08:16:45 PM	{請分析以下日誌，並告訴我如...	4,008	0.01	<14>Feb 16 20:16:45 fsm-super172 phGenerativeAI: [PH_AUDIT_GENAI_USER_QUERY]:[eventSeve...
Feb 16, 2024, 07:58:02 PM	{請分析以下日誌，並告訴我如...	10,893	0.03	<14>Feb 16 19:58:02 fsm-super172 phGenerativeAI: [PH_AUDIT_GENAI_USER_QUERY]:[eventSeve...

FortiSIEM 結合生成式 AI 對告警的 IPS 攻擊事件提供建議

Fortinet Advisor 查詢時會遮蓋敏感資料，保護機敏資訊不外洩



Action ▾ 對比原始 log 資料 Feb 16 2024, 08:36:16 PM You

請分析以下日誌，用台語告訴我如何處理? "<185>date=2024-02-16 time=20:08:27 devname="CoreFW" devid="FG5H1E5818902695" eventtime=1708085307691569100 tz="+0800" logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" vd="root" severity="high" srcip="168.10.199.186" srccountry="United States" dstip="224.141.85.77" dstcountry="Reserved" srcintf="port9" srcintf-role="undefined" dstintf="ASE_FGVM" dstintfrole="undefined" sessionid="50000" action="detected" proto=6 service="HTTP" vrf=32 policyid=0 attack="test_attack" srcport="50000" dstport="80" hostname="host2" direction="N/A" attackid=32587 profile="sensor" ref="http://www.fortinet.com/ids/VID32587" user="user5" group="group1" incidentserialno=0 crscore=30 craction=8192 crlevel="high""

自動換行 執行 Playbook 運行連接器

Event Receive Time	Query Data	Token Count	Price
Feb 16, 2024, 08:36:24 PM	{請分析以下日誌，用台語告訴...	4,544	0.01
Feb 16, 2024, 08:30:28 PM	{請分析以下日誌，用台語告訴...	6,206	0.02
Feb 16, 2024, 08:20:00 PM	{請分析以下日誌，用台語告訴...	4,789	0.01
Feb 16, 2024, 08:18:29 PM	{請分析以下日誌，並告訴我如...	4,055	0.01
Feb 16, 2024, 08:16:45 PM	{請分析以下日誌，並告訴我如...	4,008	0.01
Feb 16, 2024, 07:58:02 PM	{請分析以下日誌，並告訴我如...	10,893	0.03

Event Details FortiAI 查詢送出去的資料

原始訊息

```
type=utm subtype=ips eventtype=signature level=alert vd=FSM_123209513FSM_0913619091 severity="high" srcip=FSM_7653FSM_091361909113589 srccountry="United States" dstip=FSM_2442984846 dstcountry="Reserved" srcintf=FSM_1FSM_091361909137742315 srcintfrole="undefined" dstintf=FSM_3853131513 dstintfrole="undefined" sessionid=5FSM_0913619091FSM_0913619091FSM_0913619091FSM_0913619091 action="detected" proto=6 service="HTTP" vrf=32 policyid=FSM_0913619091 attack="test_attack" srcport=FSM_0913619091FSM_0913619091FSM_0913619091FSM_0913619091 dstport=8FSM_0913619091 hostname=FSM_8332FSM_0913619091FSM_09136190911685 direction="N/A" attackid=32587 profile=FSM_278738685FSM_0913619091 ref="FSM_6787FSM_0913619091FSM_09136190913617" user=FSM_FSM_091361909177554FSM_0913619091678 group="FSM_75FSM_0913619091FSM_09136190912529FSM_09136190914" incidentserialno=FSM_0913619091 crscore=FSM_0913619091 craction=8192 crlevel="high"}
```

Event Attributes

搜尋中...

FortiAI 查詢時會遮蓋敏感資料，保護機敏資訊不外洩

Lines: 26

Display	Filter	Item	數值
<input type="checkbox"/>	<input type="checkbox"/>	Collector ID	1
<input type="checkbox"/>	<input type="checkbox"/>	Count	1
<input type="checkbox"/>	<input type="checkbox"/>	Device Time	Feb 16, 2024, 08:36:24 PM
<input type="checkbox"/>	<input type="checkbox"/>	Event ID	621637486311086352
<input type="checkbox"/>	<input type="checkbox"/>	Event Name	FortiSIEM sent Generative AI Query to ChatGPT
<input type="checkbox"/>	<input type="checkbox"/>	Event Parse Status	1
<input type="checkbox"/>	<input type="checkbox"/>	Event Parser Name	PHGenAIParser
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Event Receive Time	Feb 16, 2024, 08:36:24 PM
<input type="checkbox"/>	<input type="checkbox"/>	Event Rule Trigger	1

Fortinet SecOps Fabric 加速事件調查和回復時間

威脅檢測與抑制時間從 21 天縮短至不到 1 小時

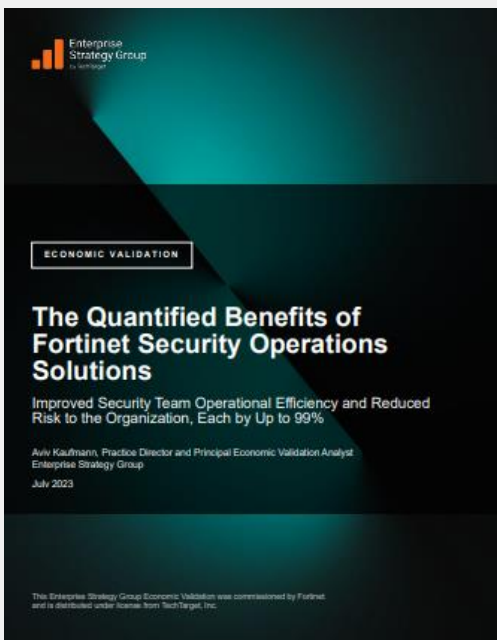
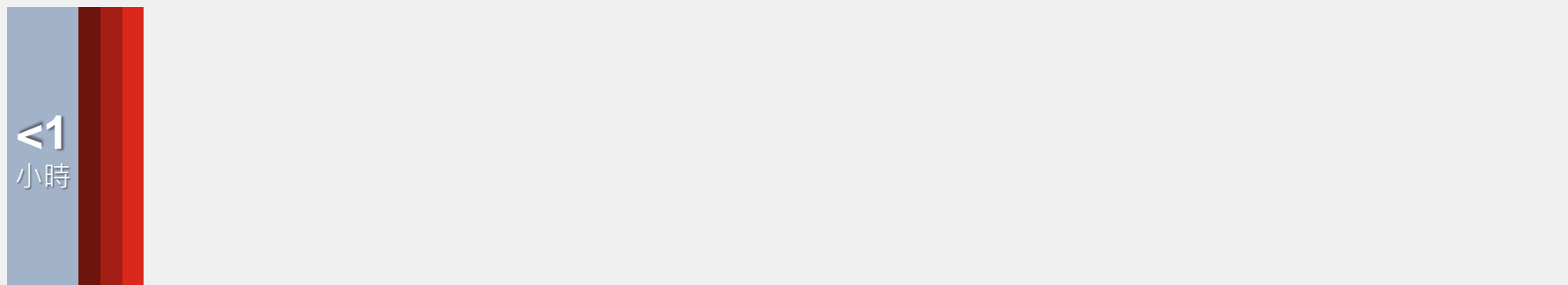
導入前

Fortinet SecOps 安全營運平臺



導入後

Fortinet SecOps 安全營運平臺



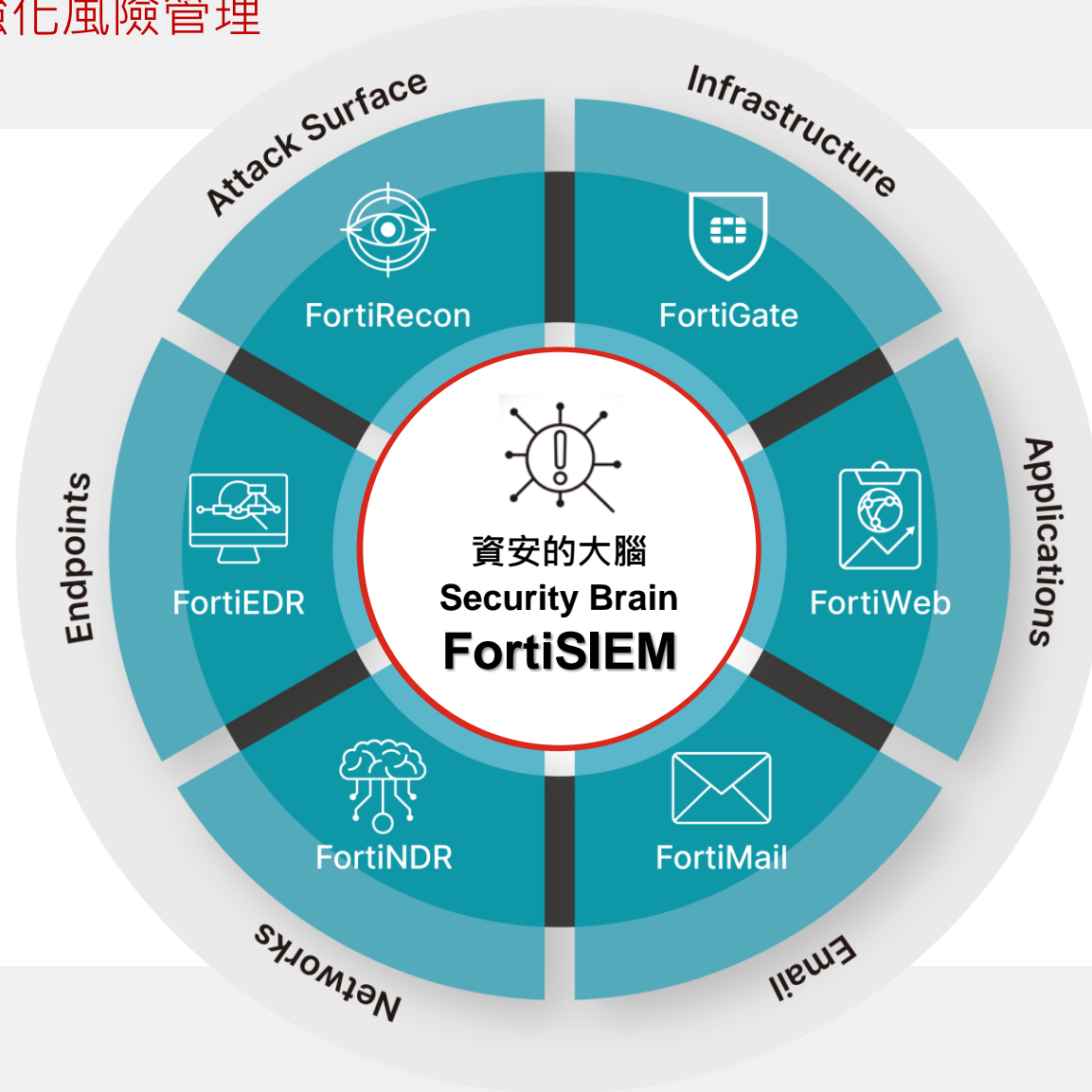
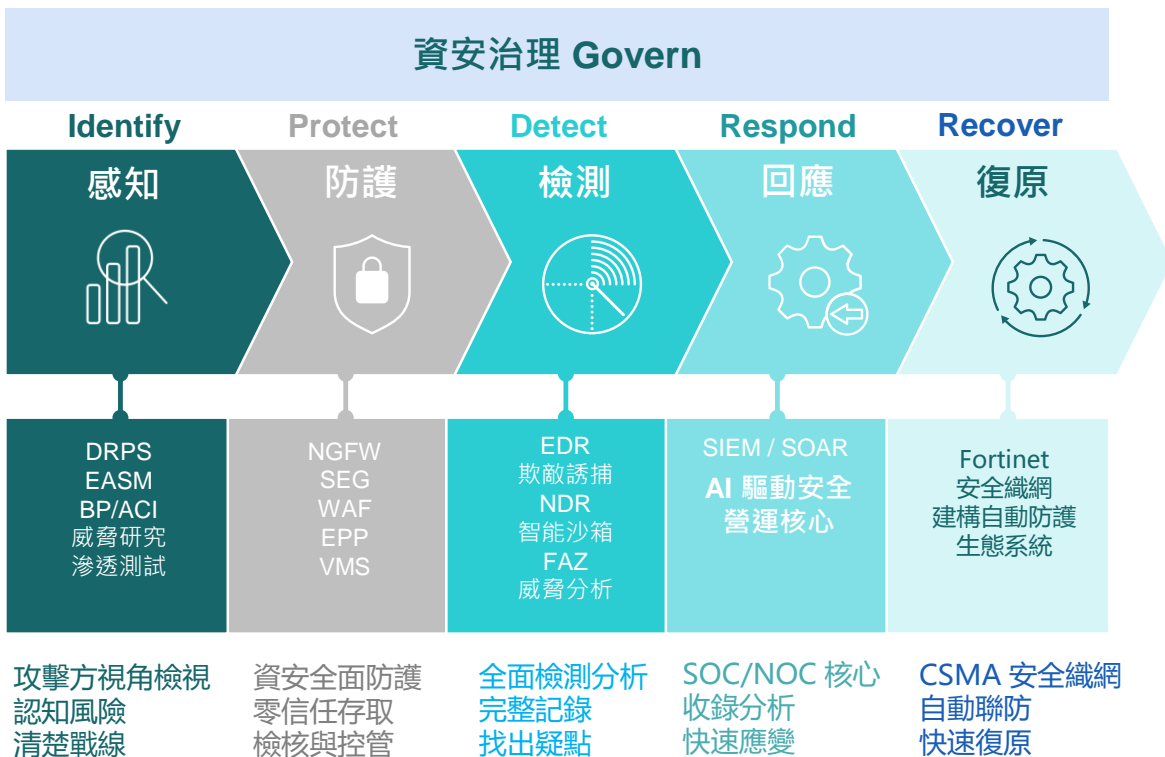


AI 驅動的安全營運解決方案加速威脅檢測與回應

Fortinet SecOps Fabric 滿足 NIST 資安框架規範，強化風險管理

NIST (美國國家標準技術研究院)

NIST Cybersecurity Framework 資安框架



Fortinet SecOps 三個基礎

1

FortiSIEM

統一管理可視性, 情資平台,
關聯分析, 早期預警, **自動化聯防**

2

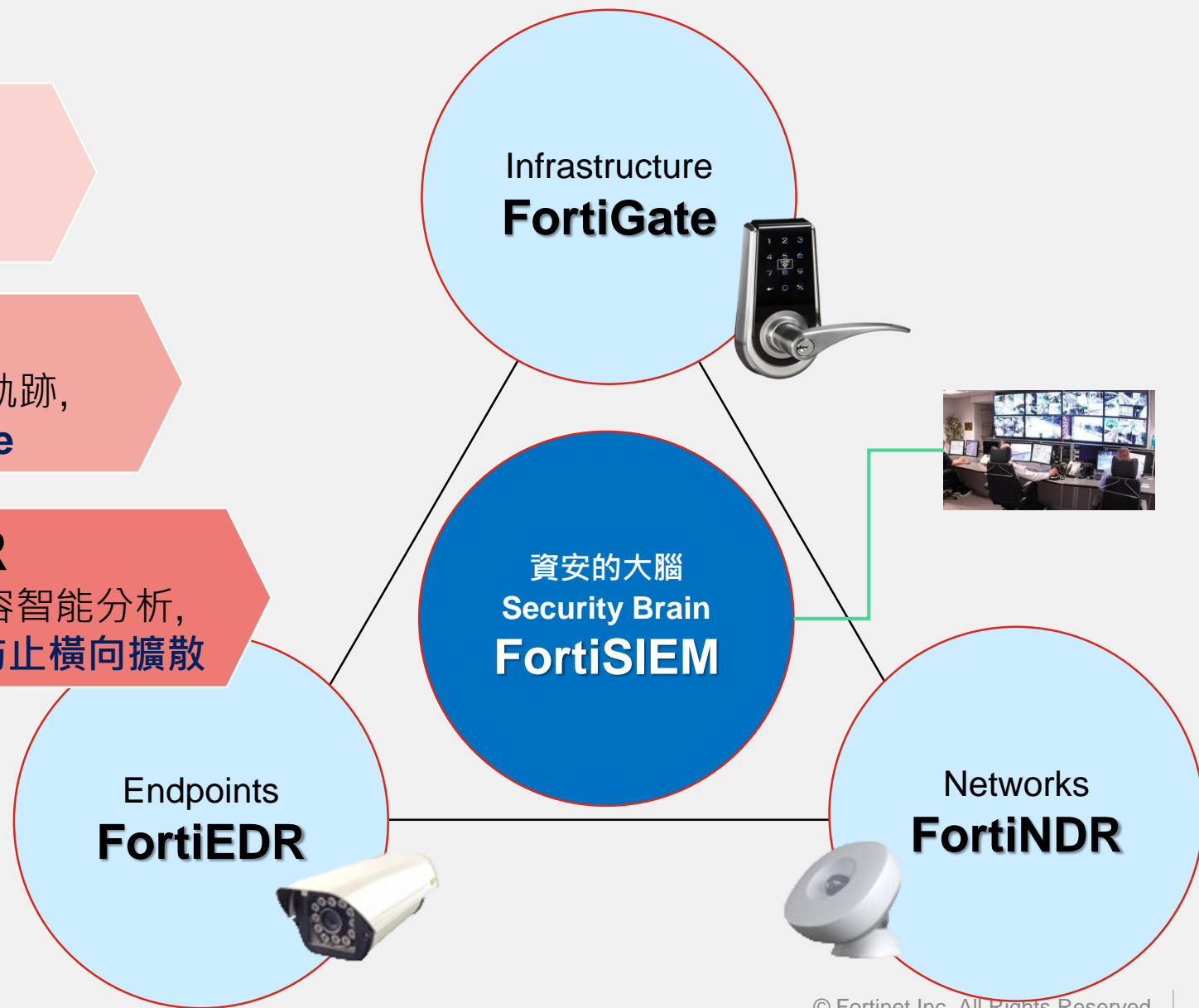
FortiEDR

記錄, 偵測, 調查端點行為軌跡,
及時阻擋 **Ransomware**

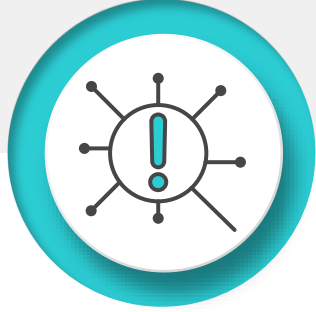
3

FortiNDR

AI 監控偵測, 流量&內容智能分析,
次秒級偵測 **Malware**, 防止橫向擴散

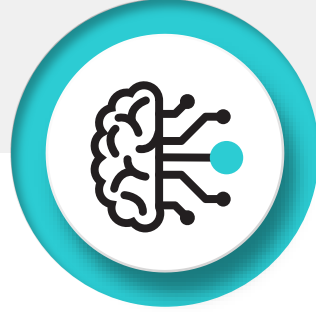


Fortinet SecOps 三個基礎產品功能重點



FortiSIEM SOC & NOC

- 資安與網維融合式分析
- 自動探索，組態與效能管理 (CMDB)
- 可快速擴容的高彈性架構
- 直覺式事件關聯分析，簡單易用
- 智能分析 (AI)，機器學習 (ML)
- 自動情資更新、分析、告警與聯防
- IOC 情資
- 事件處理及設備聯防
- 內建派工管理系統
- 標準化維運流程
- AI for 日常維運



FortiNDR 網路資安

- ANN 神經網路分析
- ML 流量異常偵測
- FortiGuard 威脅情資
- 異常連線行為的分析、偵測與追蹤
- 7x24 虛擬資安分析師
- 協作與自動化回應
- 橫跨 OT / IT 網路環境
- 降低營運成本
- 次秒級找出網路環境中的 Malware



FortiEDR 端點資安

- 7x24 NGAV
- USB 設備管控
- 應用程式連網控管
- 惡意行為、外洩及橫向移動防護
- 勒索軟體防護
- FCS 威脅情資
- 自動回應腳本
- 軌跡紀錄與威脅獵捕
- 與 FortiGate 整合，連動聯防

FortiNDR – 底層揭秘

ML-ANN 專利 # U.S. Serial No. 16/053,479 (US11574051B2)

– 使用專利的人工神經網路 (ANN) 來偵測和判決網路異常以及惡意軟體

– 單層神經網路

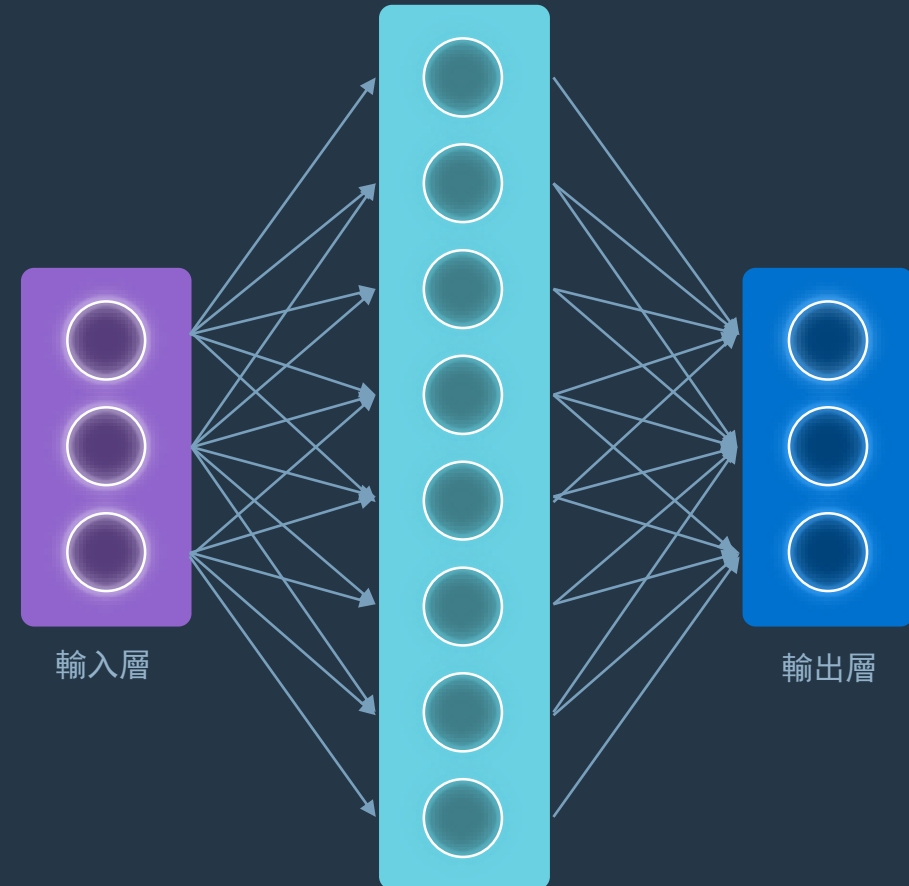
- 預訓練：2,000萬+ 乾淨和惡意文件不斷匯入
- 培養數十億計的乾淨和惡意特征識別

– 每個節點 (中間的圓圈) 代表一個“分析師”
600 萬個節點等於擁有 600 萬個資安分析師的能力

- 工作職能 - 以確定它們是否匹配單個惡意軟體特徵
- 當前 特徵資料庫 由如下元件組成:
 - PE 特徵 (可移植可執行) & 非 PE 特徵
 - 一些技術手段，如檔案分析，註冊表值，堆疊狀態，執行流程等等

– 不需要“執行”檔案檢核 (和沙箱技術相比)

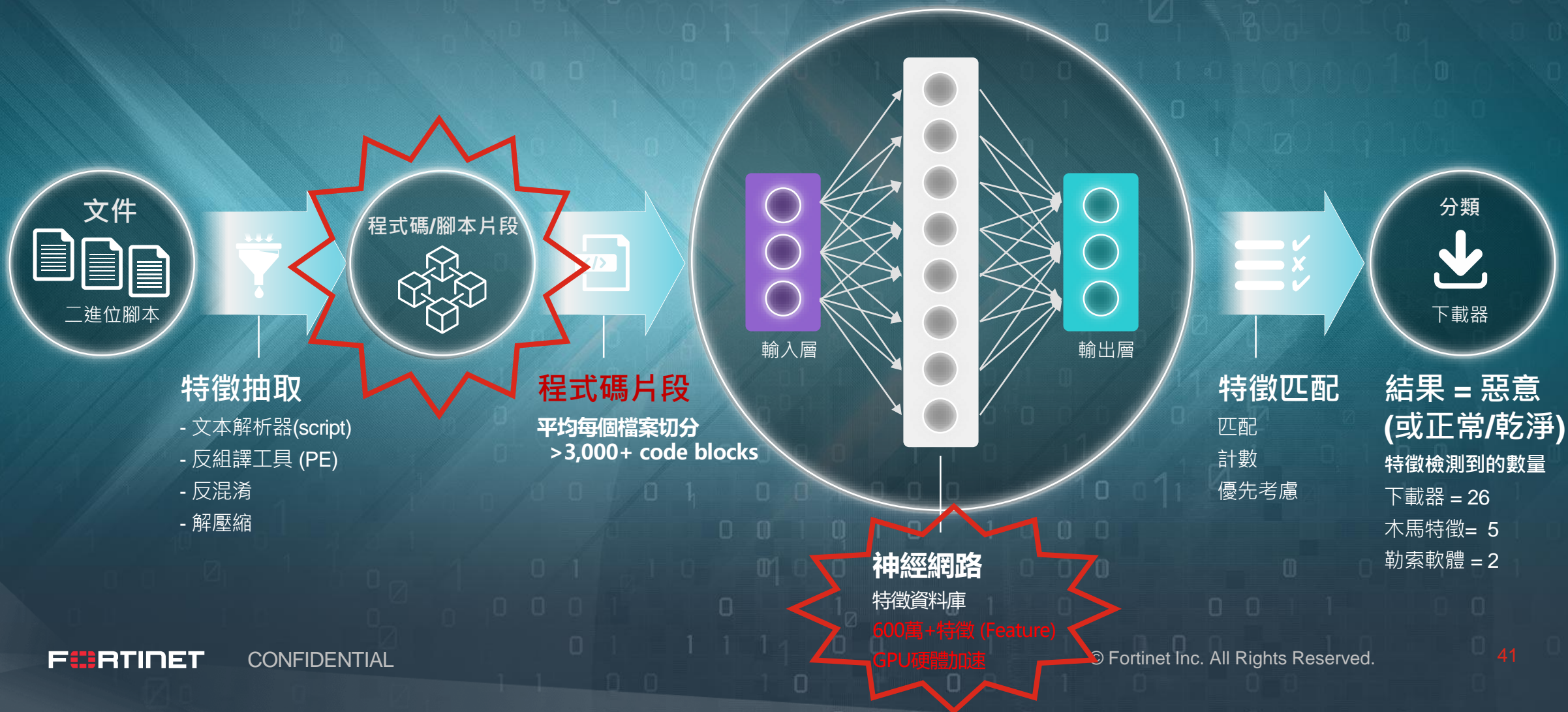
– 機器學習 (ML) 流量模式動態分析



人工神經網路
(ANN)
600萬+ 節點

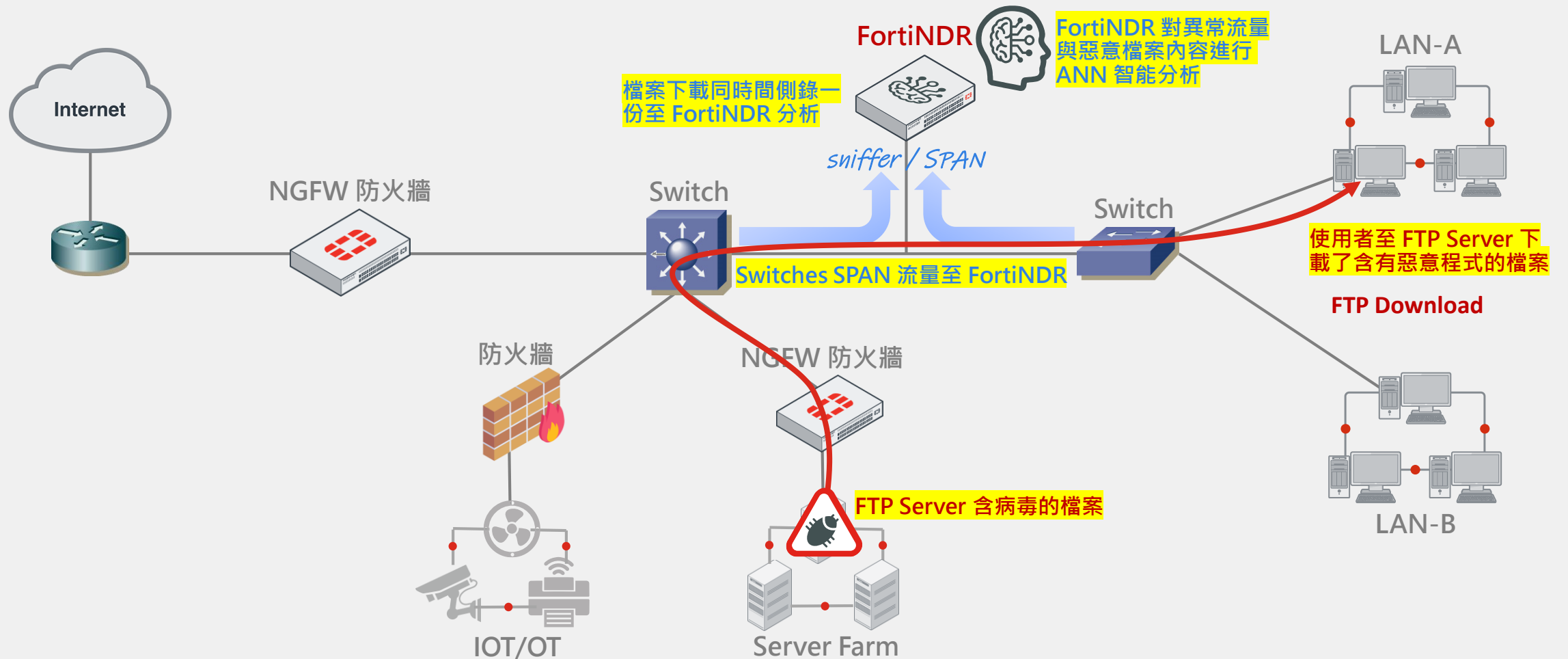
FortiNDR 的過人之處 – METADATA 剖析(流量內容智能分析)

惡意軟體檢測 workflow (執行檔 / 無檔案式腳本語言 JS · Powershell)



FortiNDR Sniffer Mode, Malware Detection

流量監聽偵測模式 (FTP Traffic)



FortiNDR Sniffer Mode, Malware Detection

流量監聽偵測模式 (FTP Traffic)



Sample 6

VSA Verdict: **Critical Risk**

Ransomware

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Confidence level: High 95.5%

Sample Information

Submitted Date	2022/11/26 19:21:30	Last Analyzed	2022/11/26 19:21:55
File Type	PE	File Size	5064980(4.8 MB)

SHA1: A9992CE4E5188EAC75E7B14262C88EA548C8D9CD

Detection Name	W32/Filecoder_WannaCryptor.D!tr.ransom	Virus Family	WannaCryptor
Source Device			
Device Type	Sniffer		
Network			
Attacker	10.0.0.2: 49913 (Private port)	Victim	10.2.2.1: 445 (Microsoft-DS)

Information View + Add to Allow List Generate Report

Feature Composition

- Ransomware: 310
- CoinMiner: 23

333 Detection(s)

Feature Type	Appearance In Sample
Ransomware	310
CoinMiner	23

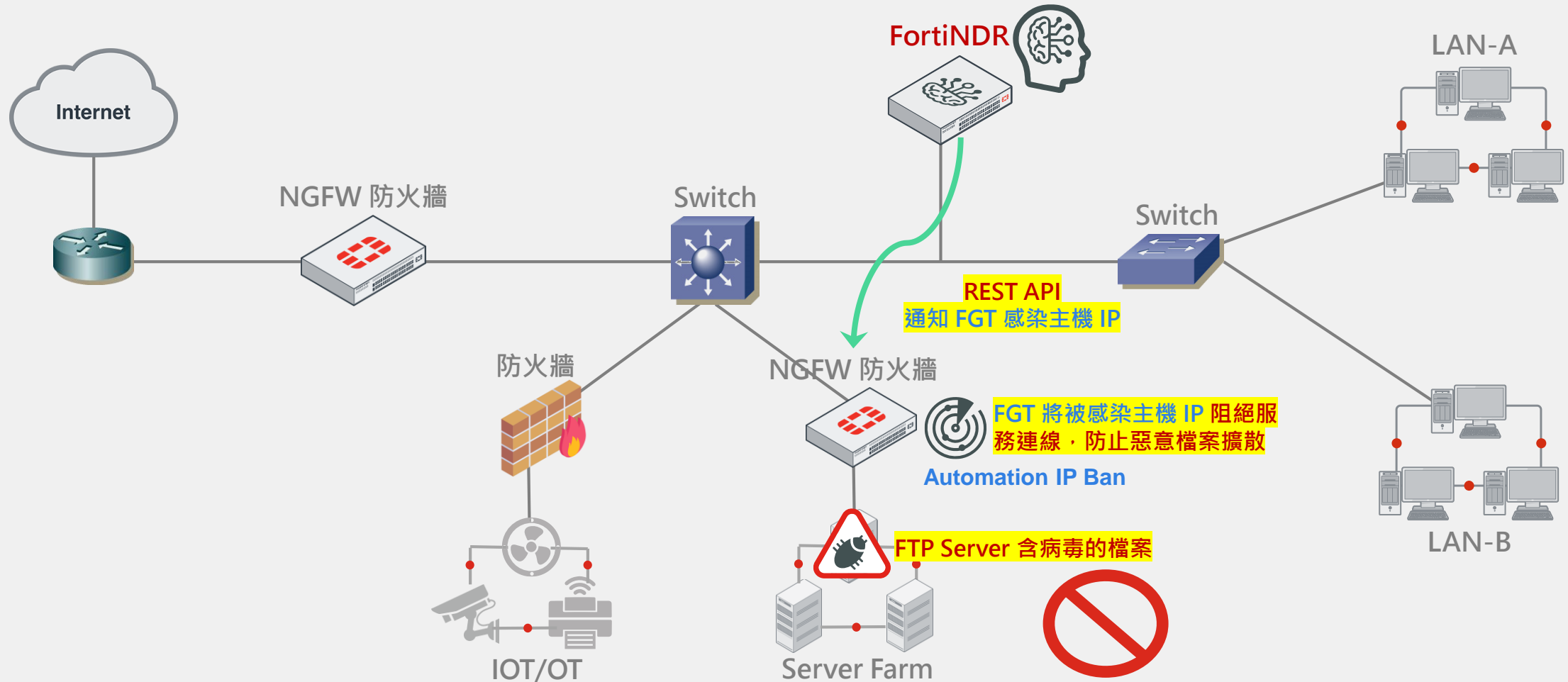
History

Date	MD5	File Type	Detection Name	Device Type	VDOM	Attacker	Victim	Confidence	Risk
2022/11/26 19:21:30	28B86C773E378F5CC06AB3FFC1ADAC1B	PE	W32/Filecoder_WannaCryptor.D!tr.ransom	Sniffer		10.0.0.2	10.2.2.1	95.5	Critical

次秒級快速判定傳輸內容符合 Ransomware 家族中的 WannaCryptor 病毒特徵，並具有95.5%的可信度(極低誤判率)

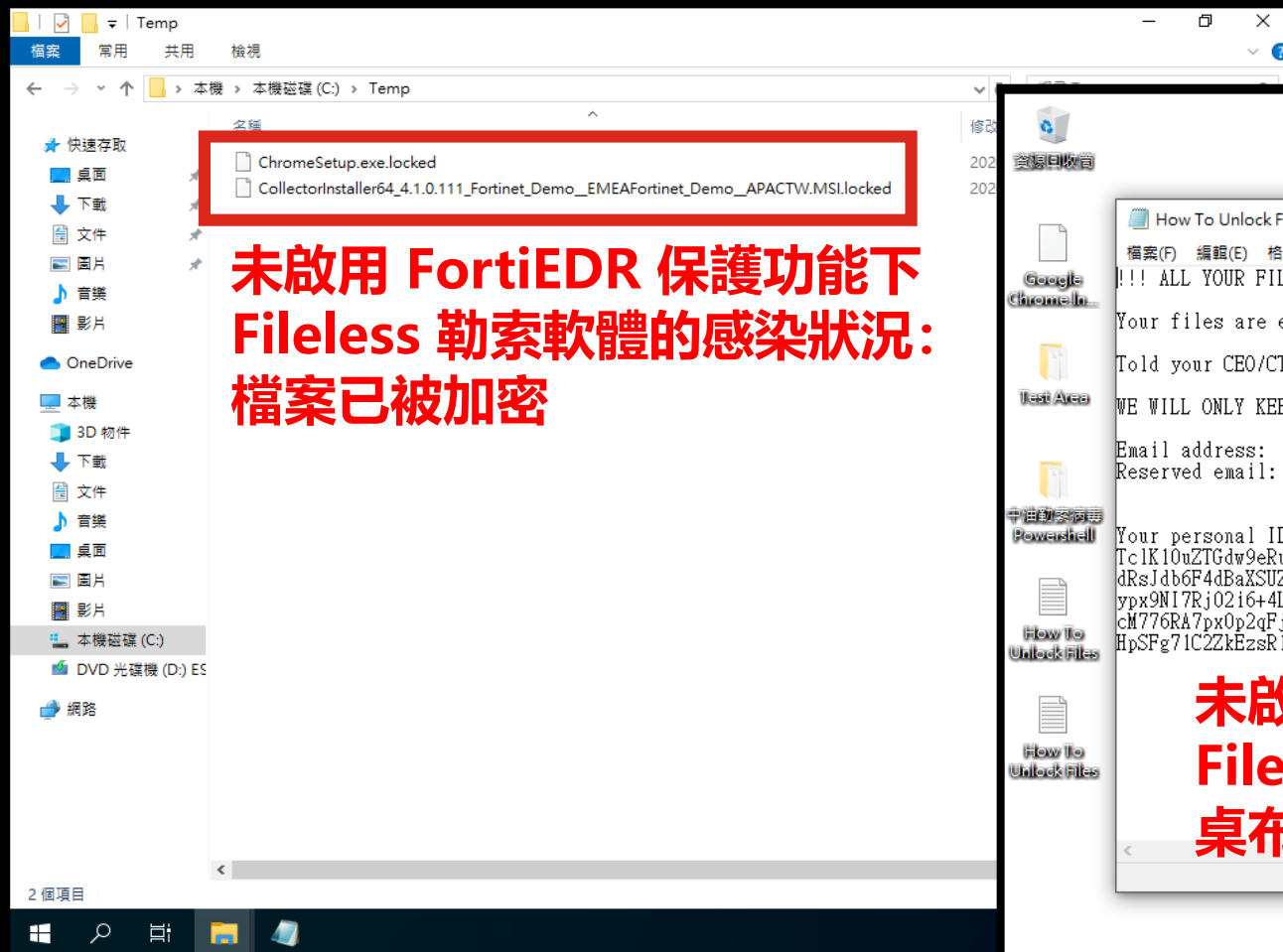
FortiNDR Sniffer Mode, Malware Detection

流量監聽偵測模式 (FTP Traffic) + 線上即時阻斷模式 (整合 NGFW)

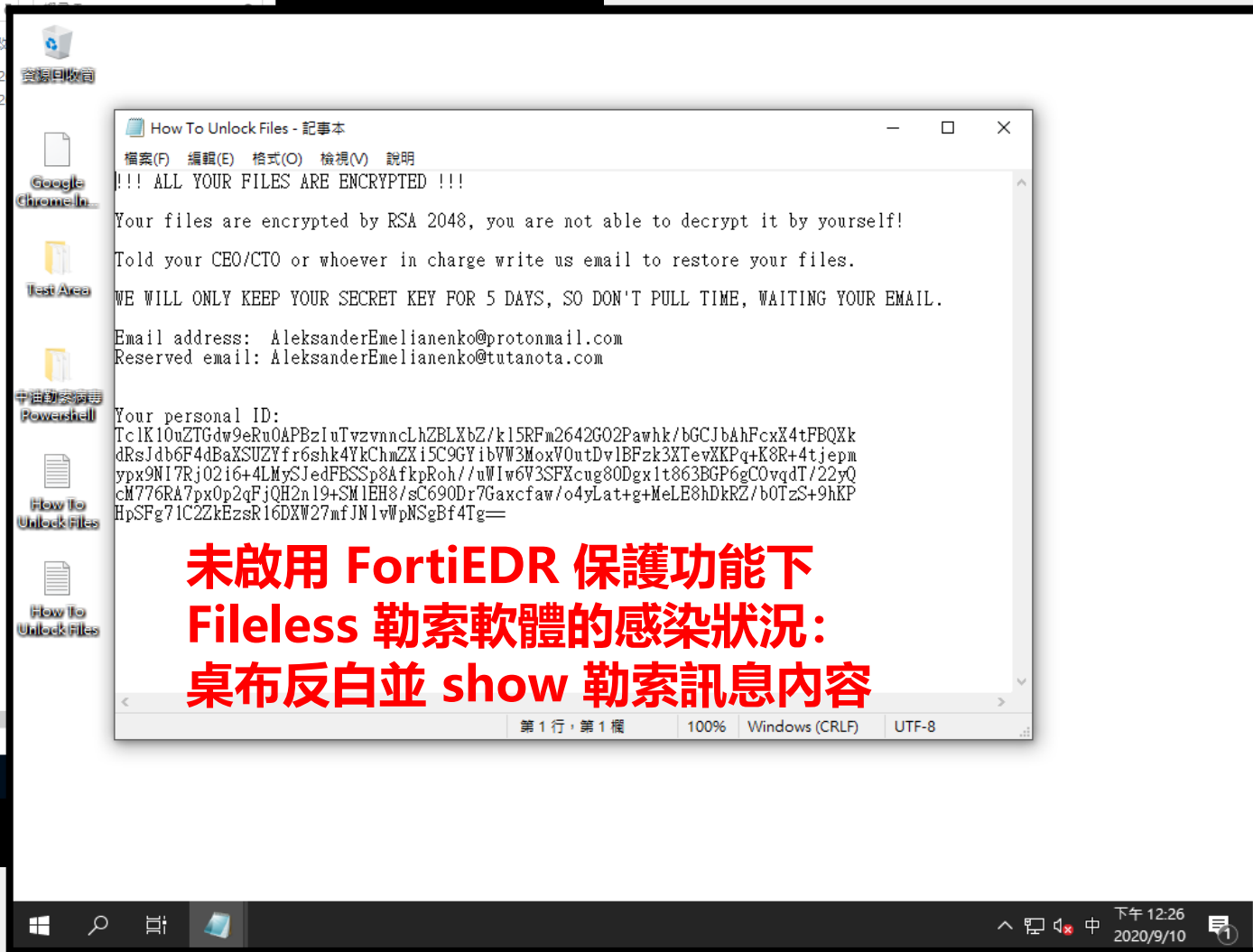


FortiEDR 即時防護功能

VM_Clean_Win10



**未啟用 FortiEDR 保護功能下
Fileless 勒索軟體的感染狀況：
檔案已被加密**



**未啟用 FortiEDR 保護功能下
Fileless 勒索軟體的感染狀況：
桌布反白並 show 勒索訊息內容**



FortiEDR 即時防護功能

The screenshot displays a Windows desktop environment. A Windows PowerShell terminal window is open, showing the execution of a PowerShell command to load an assembly. The terminal output shows several error messages, including 'ArgumentNullException' and 'InvalidOperationException'. A red text overlay is positioned over the terminal, stating: '- 啟用 FortiEDR 後', '- 潛藏的 Fileless 勒索軟體利用合法的 Powershell', and '- Powershell 在執行階段就被 FortiEDR 主動阻擋'. In the bottom right corner, a Fortinet notification dialog box is visible, titled 'Blocked process powershell.exe (PID 9060)'. The dialog box contains the text: 'Contact your system administrator if a trusted application is blocked. 如果被信任的應用程式被攔阻，請聯絡您的系統管理員。' and a 'Got It' button.

- 啟用 FortiEDR 後
- 潛藏的 Fileless 勒索軟體利用合法的 Powershell
- Powershell 在執行階段就被 FortiEDR 主動阻擋

Blocked process powershell.exe (PID 9060)
Contact your system administrator if a trusted application is blocked.
如果被信任的應用程式被攔阻，請聯絡您的系統管理員。

Got It



FortiEDR 即時防護功能

The screenshot displays the Fortinet console interface. The top navigation bar includes 'DASHBOARD', 'EVENT VIEWER 24', 'FORENSICS', 'COMMUNICATION CONTROL 137', 'SECURITY SETTINGS', 'INVENTORY 1', and 'ADMINISTRATION 33'. The 'EVENT VIEWER' section shows a table of events. A red box highlights a specific event:

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	ACTION
3424973	DESKTOP-UAAD2CG	powershell.exe	Suspicious	File Write Access	09-Sep-2020, 11:25:53	09-Sep-2020, 11:26:03	[Block]

The 'CLASSIFICATION DETAILS' panel on the right shows 'Suspicious' by Fortinet, with threat name, family, and type all listed as 'Unknown'. The 'History' section shows the event was triggered by FortinetCloudServices on 09-Sep-2020, 11:26:02.

Below the event viewer, the 'ADVANCED DATA' section shows a process flow diagram. It starts with 'Process userinit.exe' (circled in red), followed by '5 Create', then 'Process explorer.exe' (circled in red), then '6 Create', then 'Process powershell.exe' (circled in red), then '7 Write File Encryptor', and finally 'Block FE:ATINET' (circled in red). A red arrow points from the 'Block FE:ATINET' step back to the event viewer table. The final step in the flow is 'ChromeSetup.exe'.

Red text annotations are present:

- 系統啟動程序(userinit)帶起 explorer 執行
- 瀏覽器(explorer.exe)帶起 Powershell 執行
- 已啟用 FortiEDR 保護功能下
- 當惡意軟體呼叫合法程式 (如: Powershell)
- 檔案加密程序立即被 FortiEDR 攔截阻擋

Copyright © Fortinet Version 4.2.0.83. System Time (UTC +02:00) 11:30:19. The taskbar at the bottom shows various open applications and system icons.



資安聯防提升整體防禦能力

在 FortiEDR 中控台上設定要參與聯動防護的 FortiGate 防火牆

The screenshot displays the FortiEDR Administration console interface. The top navigation bar includes 'Default', 'DASHBOARD', 'EVENT VIEWER 145', 'FORENSICS', 'COMMUNICATION CONTROL 53', 'SECURITY SETTINGS', 'INVENTORY', 'ADMINISTRATION', 'Protection', and 'admin'. The left sidebar lists various management sections: LICENSING, ORGANIZATIONS, USERS, DISTRIBUTION LISTS, EXPORT SETTINGS, TOOLS, SYSTEM EVENTS, and IP SETS. The main content area is titled 'CONNECTORS' and shows a list of connectors, with 'Firewall : FG-60E_SSL' selected. Below this, the configuration details are shown, including 'Firewall Enabled' (checked) and 'On-premise Core' (fedr-core: 60.250.130.70:555). The 'Details' section is highlighted with a red box and contains the following fields: Name (FG-60E_SSL), Type (FortiGate), Host (60.250.130.70), Port (20443), and API Key (masked). The 'Actions' section is also highlighted with a red box and contains the following fields: Block address on Firewall (checked) and Address group (FEDR_Blocking). Below the 'Actions' section, there is a red box containing the text: '將連線的惡意網站 IP 放入防火牆 阻擋黑名單'. At the bottom of the configuration area, there are 'Save', 'Cancel', and 'Delete' buttons. The text '透過 API 聯動 FortiGate 防火牆' is displayed at the bottom of the configuration area.

透過 API 聯動 FortiGate 防火牆

資安聯防提升整體防禦能力

資安事件觸發後自動啟動聯防動作

The screenshot displays the Fortinet Security Manager interface. The top navigation bar includes Dashboard, Event Viewer (2), Forensics, Communication Control (38), Security Settings, Inventory (1), and Administration (37). The main area is divided into 'EVENTS' and 'CLASSIFICATION DETAILS'.

EVENTS Table:

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
powershell.exe (1 event)						
335899	WIN7SP1-192	SQBFAFgAIAAoAE4AZQ...	Malicious	185.199.109.133	29-Mar-2021, 19:48:54	29-Mar-2021, 19:48:54
User: WIN7SP1-192\TestWin7 Certificate: Signed Process path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Raw data items: 1						
ed01ebfbc9eb5bbea545af4d01bf5f10716618404... (1 event)						
cloudnet.exe (1 event)						
5.exe (1 event)						

CLASSIFICATION DETAILS:

- Malicious **FORTINET**
- Threat name: Unknown
- Threat family: Unknown
- Threat type: Unknown

History:

- Malicious, by FortinetCloudServices, on 29-Mar-2021, 19:49:17
 - IP 185.199.109.133 was added to malicious IP addresses on firewall FortiGate FG-SE_Lab

ADVANCED DATA - Event Graph:

The event graph shows a sequence of actions: 1. Create (Process explorer.exe) → 2. Create (Process cmd.exe) → 3. Connect (Process powershell.exe) → Block (Suspicious Application) → Connection (185.199.109.133). Red annotations describe the steps: '瀏覽器帶起 Cmd 程序' (Browser starts Cmd process), 'Cmd 呼叫 Powershell' (Cmd calls Powershell), and 'Powershell 嘗試連線惡意網站 IP_185.199.109.133' (Powershell attempts to connect to malicious website IP).

FEDR 自動通知 FGT 將該惡意網站 IP 放入阻擋黑名單



資安聯防提升整體防禦能力

在 FortiGate 防火牆上自動將連線的惡意網站 IP 放入防火牆阻擋黑名單

Name	Details	Interface	Fabric Sync	Type	Ref.
Bonjour	224.0.0.251 - 224.0.0.251		undefined	Multicast A...	0
EIGRP	224.0.0.10 - 224.0.0.10		undefined	Multicast A...	0
OSPF	224.0.0.5 - 224.0.0.5		undefined	Multicast A...	0
all	224.0.0.0 - 239.255.255.255		undefined	Multicast A...	0
all_hosts	224.0.0.1 - 224.0.0.255		undefined	Multicast A...	0
all_routers	224.0.0.2 - 224.0.0.255		undefined	Multicast A...	0
Address Group 5					
Demo_Malicious_IP	<ul style="list-style-type: none">FortiEDR_7FortiEDR_9FortiEDR_5FortiEDR_185.199.109.133		Disable	Address Gr...	1

Address FortiEDR_185.199.109.133

Type IP Range

IP Range 185.199.109.133 - 185.199.109.133

Interface any

Fabric Sync Disabled

Comments **FortiEDR Event ID - 335899**

References 1

Edit

✓ 有裝 FortiEDR 的電腦保護了自己

✓ 沒裝 FortiEDR 的電腦或 IOT/OT 設備受到了防火牆自動聯防機制的保護



導入 SecOps 評估的重點

人

AI & ML + 大數據情資分析

統一可視性

有效的管理

快速的偵測

自動化回應

整合性聯防

全球的情資

彈性的部署

別讓人力去對抗新型態資安威脅

資安威脅正 AI 武裝化，犯罪即服務 (Crime as a Service) 易得，**資安防護沒有最好的架構，只有更符合需求的架構**



讓機器去處理過

透過 AI-驅動的安

人力放在核心業務上

責任框架下的資安人才需求



FORTINET®