

駭客攻擊永不停歇



iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 臺灣資安大會 搜尋

宏碁傳出疑似遭到勒索軟體REvil攻擊，駭客索討5千萬美元贖金

臺灣電腦龍頭宏碁傳出遭勒索軟體組織REvil攻擊，而駭客不只要支付天價贖金，更值得留意的是，攻擊者入侵該公司的管道，很有可能就是Exchange的重大漏洞ProxyLogon

文/ 周敏怡 | 2021-03-20 發表

Happy Blog Auction (new) Blog words Search

Acer Inc. **acer**

Acer Inc. - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xitai, New Taipei City. Its products include desktop PCs, laptop PCs, tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 4th-largest PC vendor by unit sales as of January 2021.

Category	Product Name	Price	Availability
Desktop	Acer Aspire 5	NT\$12,990	In Stock
Laptop	Acer Swift 3	NT\$10,990	In Stock
Tablet	Acer Iconia One	NT\$4,990	In Stock
Server	Acer Aspire Server	NT\$15,990	In Stock
Storage	Acer Aspire Storage	NT\$8,990	In Stock
VR	Acer Aspire VR	NT\$19,990	In Stock
Display	Acer Aspire Display	NT\$12,990	In Stock
Smartphone	Acer Aspire Smartphone	NT\$10,990	In Stock
Peripherals	Acer Aspire Peripherals	NT\$5,990	In Stock
Gaming PC	Acer Aspire Gaming PC	NT\$18,990	In Stock
Accessories	Acer Aspire Accessories	NT\$3,990	In Stock

圖片來源: Bleeping Computer

又有臺灣的科技公司傳出疑似遭到勒索軟體攻擊了！根據資安新聞網站Bleeping Computer的報導，勒索軟體駭客組織REvil宣稱，他們攻擊電腦大廠宏碁，並公布疑似內有竊得資料的螢幕截圖，駭客向宏碁勒索5千萬美元贖金，約相當於新臺幣14億元。這些圖片所透露的外洩內容，包含了財務報表、帳戶餘額，以及與銀行之間往來的相關文件。

針對這項傳聞，Bleeping Computer也取得宏碁的說法。該公司指出，類似他們這種公司經常受到網路攻擊，宏碁已經向多個國家相關的執法單位與資料保護部門，通報近期察覺到的異常情形。而對於進一步的細節，該公司表示尚有正在進行的調查，但基於安全考量，暫時無法透露細節。

anuba atmosphere 21 掌握網路、安全、智慧監控與自動化的創新技術 立即報名

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 科技防疫情報站 搜尋

廣達傳遭勒索軟體REvil攻擊，歹徒要脅蘋果購回外洩產品資料

根據BleepingComputer取得的資訊，REvil背後的駭客組織宣稱入侵廣達並取得大量機密，包括廣達替蘋果代工的Mac電腦等產品資料，藉此向這二家大廠勒索高額贖金

文/ 林妍潔 | 2021-04-21 發表

情境示意圖，圖片來源 / 蘋果

蘋果在今天凌晨的Spring Loaded大會上，公布iPad Pro、iMac等新品

Intel 英特爾® OpenVINO™ 工具套件 英特爾合作夥伴與您分享 OpenVINO™ 如何應用於 AI 解決方案

iThome Security 說這專真蹟 4.3萬個讚

iThome Security 4分鐘 臺灣物聯網智慧再成焦點，今年6月CISA才警告該公司的SDK存在CVE-2021-32934漏洞，最近FreeEye與CISA又揭露另一漏洞CVE-2021-28372

資安問題的源頭？



資安的源頭可以是多方面的，以下是一些常見的資安源頭：

1. 人為因素：人為因素是資安問題的主要源頭之一。這包括員工的疏忽、錯誤或惡意行為，例如弱密碼使用、不當的資訊分享、社交工程攻擊等。人為因素需要透過教育、訓練和資訊安全政策來加以管理和防範。





資安需要架構端點防護產品的原因有以下幾點：

1.端點是最容易受到攻擊的地方：

端點，例如個人電腦、筆記型電腦、智慧手機等，是組織內部網路中最容易受到攻擊的地方。攻擊者通常會針對端點進行入侵、惡意程式傳播和資料竊取等活動。因此，**保護端點是資安的關鍵**。

2.端點是重要資料存儲和處理的地方：

端點通常存儲和處理組織的重要資料，包括機密文件、客戶資料、財務記錄等。如果端點受到入侵或受到惡意程式的感染，這些資料可能會遭到竊取、破壞或勒索。因此，**保護端點資料的安全至關重要**。

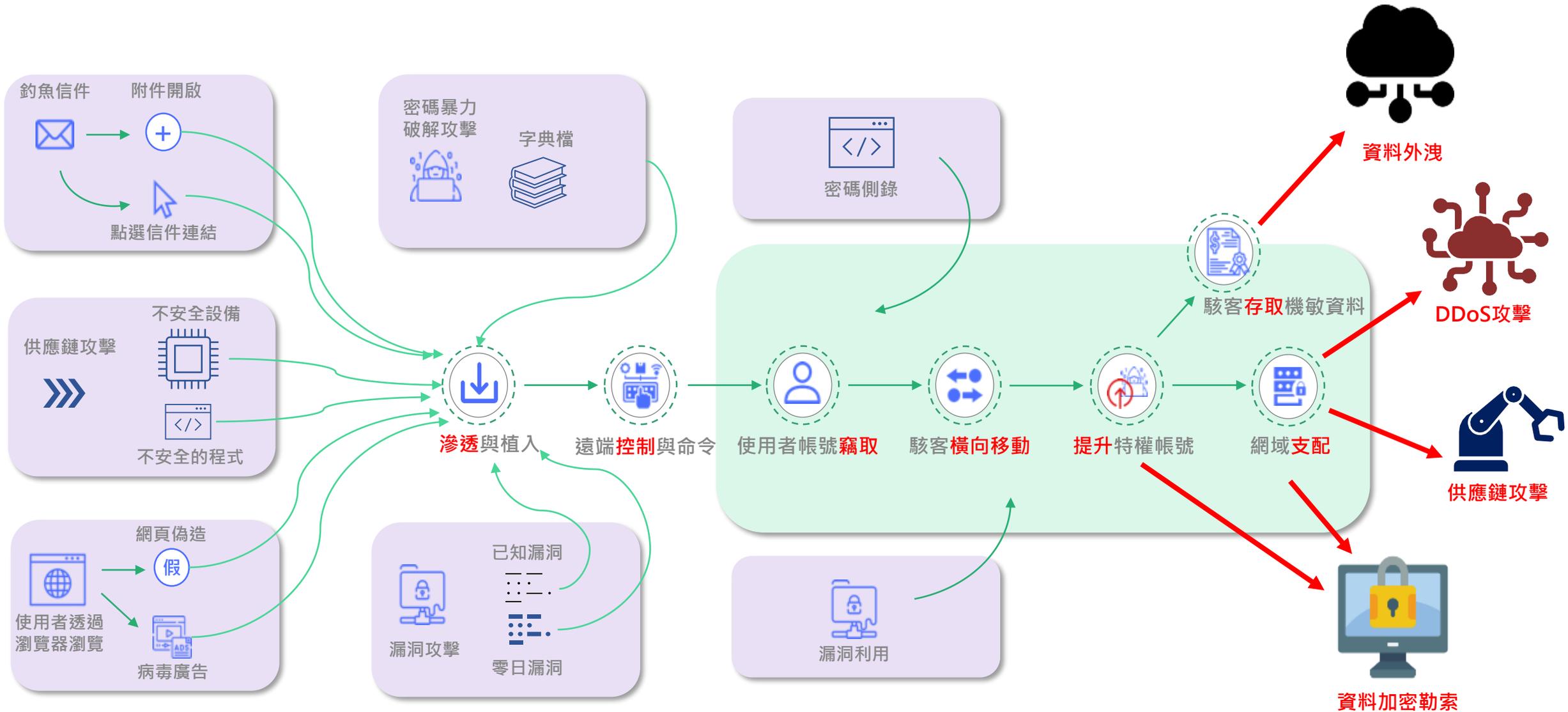
3.端點是內部網路的入口點：

攻擊者通常透過端點進入內部網路，並進一步擴大攻擊範圍。一旦攻擊者控制了端點，他們可以進一步探索網路、竊取憑證、發起橫向移動等活動。因此，**保護端點可以阻止攻擊者進入網路並限制攻擊擴散**。

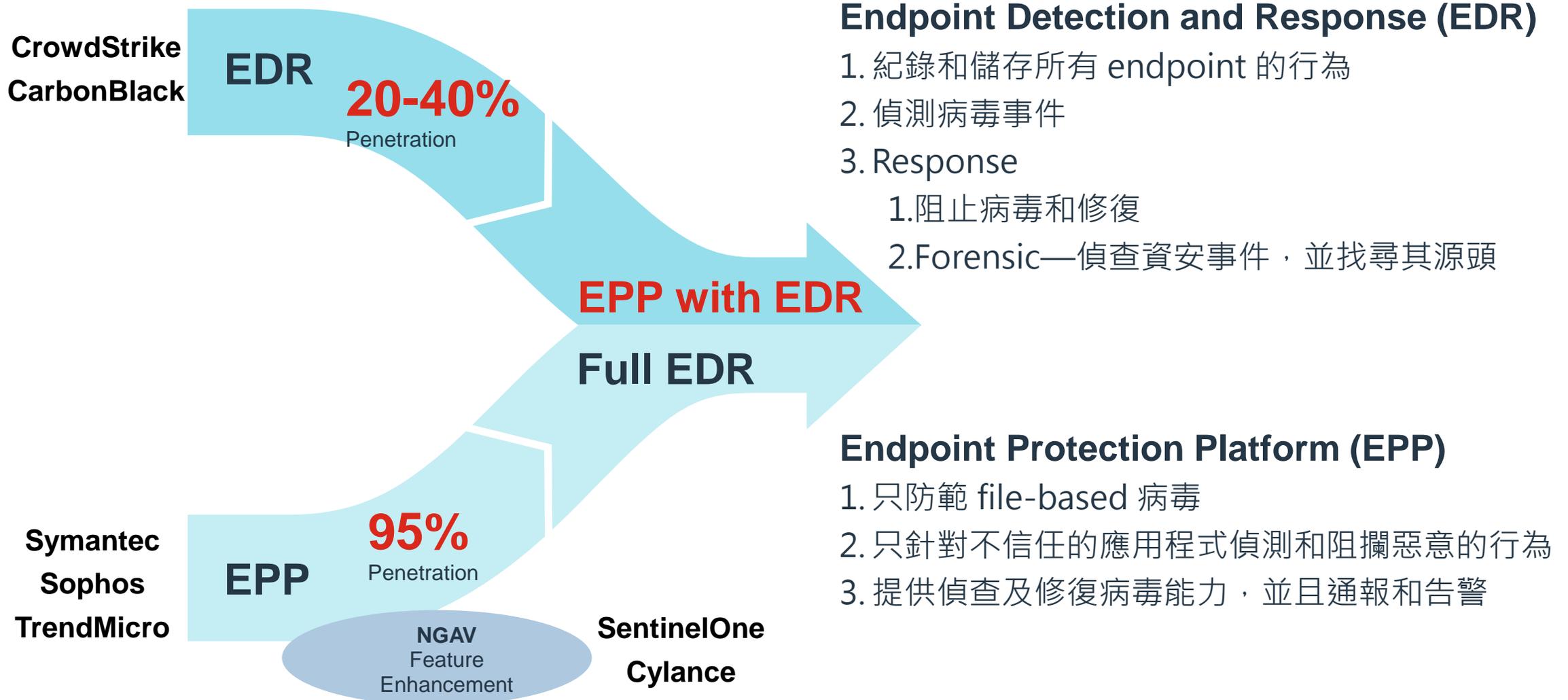
4.威脅環境不斷演變：

資安威脅不斷變化和進化，攻擊手法越來越複雜。傳統的防護措施，例如防火牆和入侵檢測系統，無法完全應對新興的威脅。**端點防護產品，例如EDR，通常具有更進階的威脅檢測和防禦能力**，可以更好地應對進階威脅和新興的攻擊手法。

防不勝防的駭客攻擊手法



端點防護的發展 - 特徵值比對 VS 行為模式分析



端點防護需要的是：事前防範&事後保護

- 事前防範 = EPP(防毒軟體)
資安工具,惡意軟體的過濾

防毒軟體

防毒引擎 (AV)

端點防火牆

應用程式控管 (伺服器)

網頁過濾

通訊埠與設備控管

弱點與補釘管理

- 事後保護 = EDR (偵測與回應)

記錄使用者的行為軌跡,偵測與回應異常行為

EDR 偵測與回應防護

行為模型建立

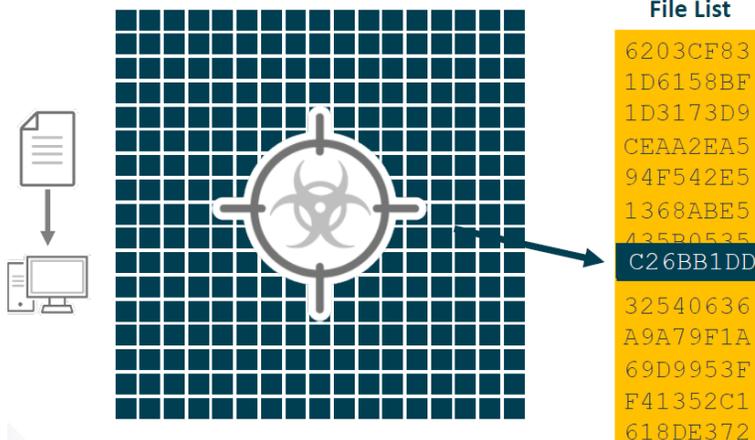
惡意軟體遏制功能

使用者行為軌跡紀錄,提供日後稽核

系統回復機制

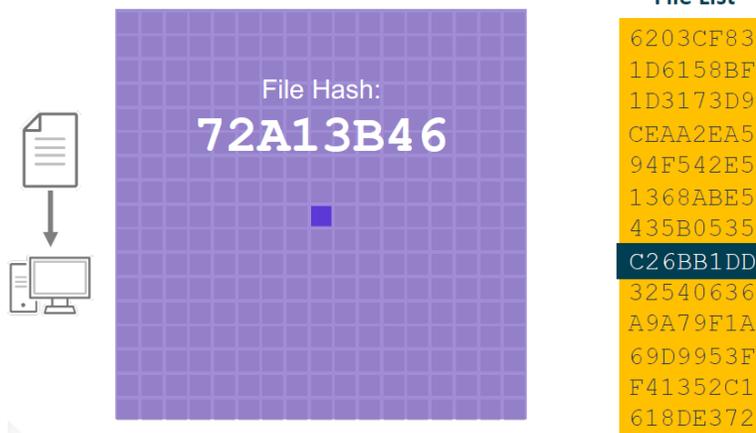
未知的威脅透過 AI 智能分析

Early 90s: Signatures



Fast and accurate...
...as long as the malware doesn't change.

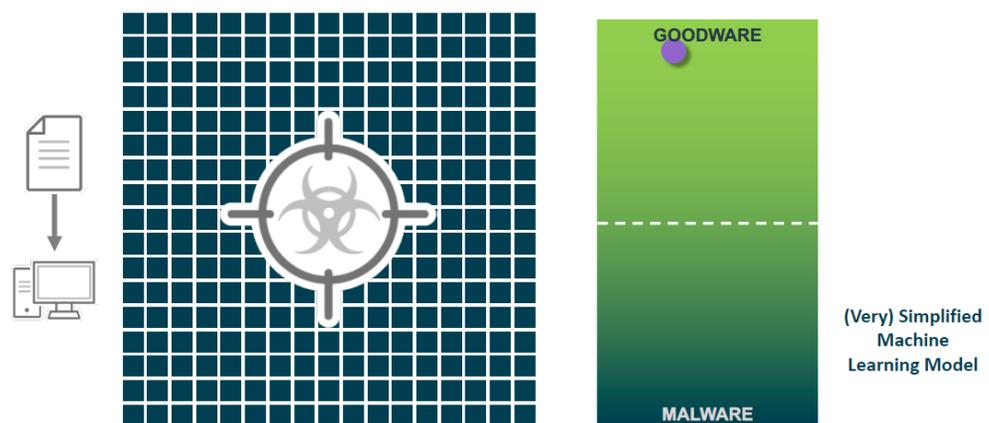
Late 90s: Signature Evasion



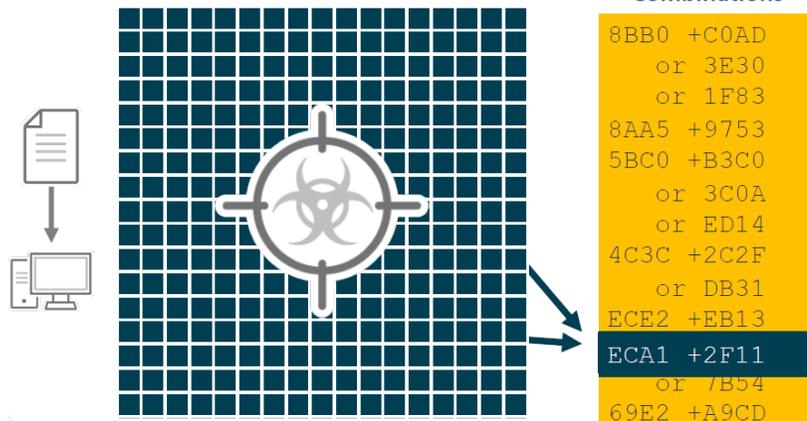
If just one byte changed, a file hash wouldn't match anymore

Simplified for clarity

Last Decade: Rise of Machine Learning

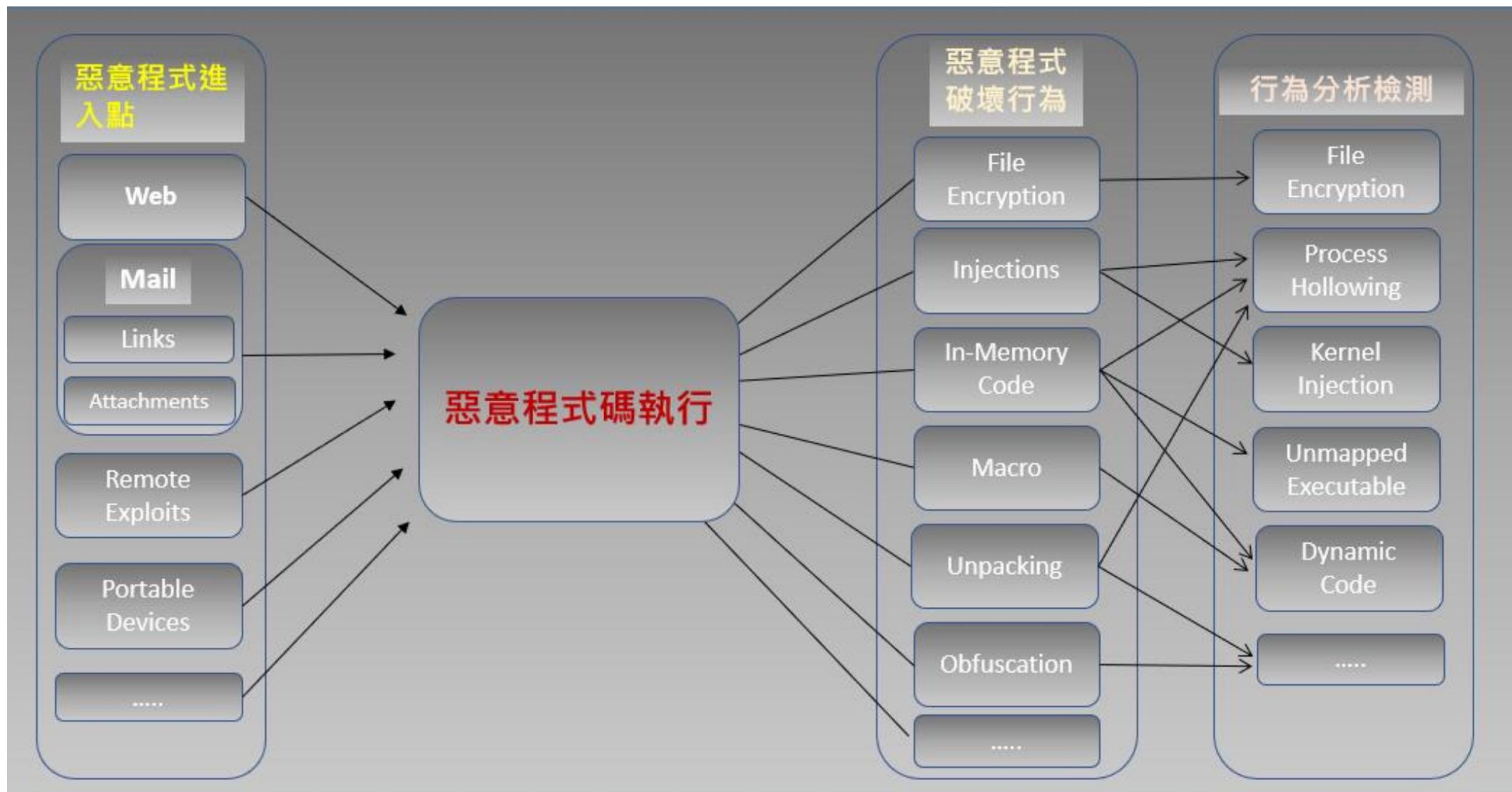


Variant Protection



Variant Protection helps spot entire malware families

惡意行為偵測與阻斷



端點資安事件觸發流程與分析



- Malicious
- Suspicious
- Inconclusive
- PUP



資安事件觸發後的處置

ensilofordev | DASHBOARD | EVENT VIEWER 196 | FORENSICS | COMMUNICATION CONTROL 1240 | SECURITY SETTINGS | INVENTORY 1 | ADMINISTRATION 696 | Protect

AUTOMATED INCIDENT RESPONSE - PLAYBOOKS

Clone Playbook | Set Mode | Assign Collector Group | Delete

NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
Default Playbook <small>FORTINET</small>					
NOTIFICATIONS (sent in protection and simulation modes)					
Send mail notification	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Send syslog notification	Syslog must be defined under Admin settings				
Open ticket	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
INVESTIGATION					
Isolate device with Collector	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolate device with NAC	A NAC connector must be defined under Admin settings				
Move device to the High Security Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
REMEDiation					
Terminate process	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clean persistent data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Block address on Firewall	A firewall must be defined under Admin settings				

ASSIGNED COLLECTOR GROUPS

- Unassign Group
- High Security Collector Group (0 collectors included)
- Beta 4.1.0 (4 collectors included)
- Cloud (2 collectors included)
- Default Collector Group (8 collectors included)
- edrtest (1 collector included)
- emulation (0 collectors included)
- emulation_a (0 collectors included)
- Eugene-emulator (0 collectors included)
- Linux collectors (2 collectors included)
- lior (1 collector included)
- lior Testing (0 collectors included)
- lior333 (1 collector included)
- Nastya (0 collectors included)
- oti (0 collectors included)
- philip (1 collector included)
- PT (0 collectors included)
- ResearchTeam (1 collector included)
- shanitest (0 collectors included)

主動式威脅捕獵 –

深度端點行為記錄與追蹤 藉以強化資安鑑識能力

The screenshot displays the Fortinet Threat Hunting Settings interface. The top navigation bar includes 'DEMO', 'DASHBOARD', 'EVENT VIEWER 1', 'FORENSICS', 'COMMUNICATION CONTROL 66', 'SECURITY SETTINGS', 'INVENTORY', 'ADMINISTRATION 30', 'Protection', and 'roy'. The 'SECURITY SETTINGS' dropdown menu is open, showing 'Security Policies', 'Playbooks', 'Threat Hunting Settings', 'Exception Manager', and 'Exclusion Manager'. The main content area is titled 'THREAT HUNTING SETTINGS' and features three inventory profiles on the left: 'Inventory Profile (default)', 'Standard Collection Profile', and 'Comprehensive Profile'. The central section, 'Events Collection And Storage', is highlighted with a red box and contains the following settings:

- Inventory** (Enabled):
 - File Detected
- Process** (Enabled):
 - Process Termination
 - Process Creation
 - Process Start
 - Thread Created
 - Executable Loaded
- File** (Enabled):
 - File Create
 - File Write
 - File Read
 - File Rename
 - File Delete
 - File Permission Change
 - File Owner Change
- Network** (Enabled):
 - Socket Connect
 - Socket Bind
 - Socket Listen
 - Socket Close
 - Socket Accept
- Registry** (Disabled)
- Event Log** (Enabled)

主動式威脅捕獵 — 快速搜尋與定位關鍵記錄

The screenshot displays the Fortinet Threat Hunting dashboard. At the top, navigation tabs include DASHBOARD, EVENT VIEWER (197), FORENSICS, COMMUNICATION CONTROL (1240), SECURITY SETTINGS, INVENTORY (1), and ADMINISTRATION (696). The main section is titled "Threat Hunting" and features a search bar with a Lucene-like syntax prompt. Below the search bar, a summary table is shown with columns for Behavior, Type, Device Name, Target Process, Protocol, Remote IP, Remote Port, Target Process Signed, and Signed By. A red box highlights the "Behavior" column, which lists "credential access" (3052) and "discovery" (855). Below the summary table, there are tabs for "All EDR Events (2.16M)", "Process (771.6K)", "File (1.37M)", "Network (21.2K)", "Registry", and "Event Log (1.5K)". The main event log table has columns for Category, Time, OS, Device Name, Type, Behavior, Process And Attributes, and Target. A red box highlights a specific event: a "File Read" operation on "LIOR-NewPC" by "chrome.exe" with target "f_005f5b". To the right, a sidebar provides detailed information for the selected "File Read" event, including a "Summary" tab, status "Disconnected", internal IP, up time, and a list of attributes such as Path, Executing user, Product, SHA1, and Command line.

Behavior	Type	Device Name	Target Process ...	Protocol	Remote IP	Remote Port	Target Process Signed	Signed By
credential access (3052)	File Read (2161981)	lior-newpc (2161981)	chrome.exe (33395)	tcp (21152)	3.222.249.36 (21152)	636 (21152)	Signed (33075)	engineering (32196)
discovery (855)	Executable Loaded (735967)	ensw-lap153 (350083)	proxy/host.exe (3927)	udp (2885)	8.241.17.254 (1)	993 (1)	Unsigned (320)	empty (320)
	File Write (259258)	ensw-lap149 (97660)	teams.exe (2398)		10.0.0.30 (1)	5000 (1)		information technology (78)
	File Create (136152)	ensw-lap119 (37322)	svchost.exe (1715)		10.0.0.138 (1)	5353 (1)		acrobat dc (75)
	File Delete (105581)	einat-pc (10816)	backgroundtaskhost.exe (1509)		10.51.102.170 (1)	10443 (1)		

Category	Time	OS	Device Name	Type	Behavior	Process And Attributes	Target	Event Attributes
🌐	2020-Sep-16...	Windows	ENSW-LAP119	Socket Conn...		chrome.exe	2001:4860:4...	Source PID: 13284, Local Address: 0:0:0:0:0:0:64983, Remote Address: 2001:4860:4860:0:...
📄	2020-Sep-16...	Windows	LIOR-NewPC	File Read		chrome.exe	f_000474	Source PID: 53584, Path: Users\lior\AppData\...
📄	2020-Sep-16...	Windows	ENSW-LAP119	File Read		SelfElectController.exe	downloader...	Source PID: 8696, Path: ProgramData\LAN...
📄	2020-Sep-16...	Windows	LIOR-NewPC	File Read		chrome.exe	f_005f5b	Source PID: 53584, Path: Users\lior\AppData\...
🌐	2020-Sep-16...	Windows	LIOR-NewPC	Socket Close		chrome.exe	0:0:0:0:0:0:...	Source PID: 53584, Local Address: 10.51.121.49/56718, Remote Address: 0:0:0:0:0:0:0/0

File Read

Summary → chrome.exe 2020-Sep-16, 13:05:13 TC

Status: ● Disconnected Internal IP: 10.51.121.49, 192.168.116.1...

LIOR-NewPC Up time: 3d, 3h, 49min, 38sec

chrome.exe PID-53584

Path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Executing user: ENSILO\lior

Product: Google Chrome

SHA1: 943A2D62A7AB288B239DC690AEAF75A67155C642

Command line: --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1632.5379426322936354670,3234879161765688624,131072 --

安全聯防提升整體防禦能力

設定要進行自動聯防的Playbook

資安事件觸發聯防動作

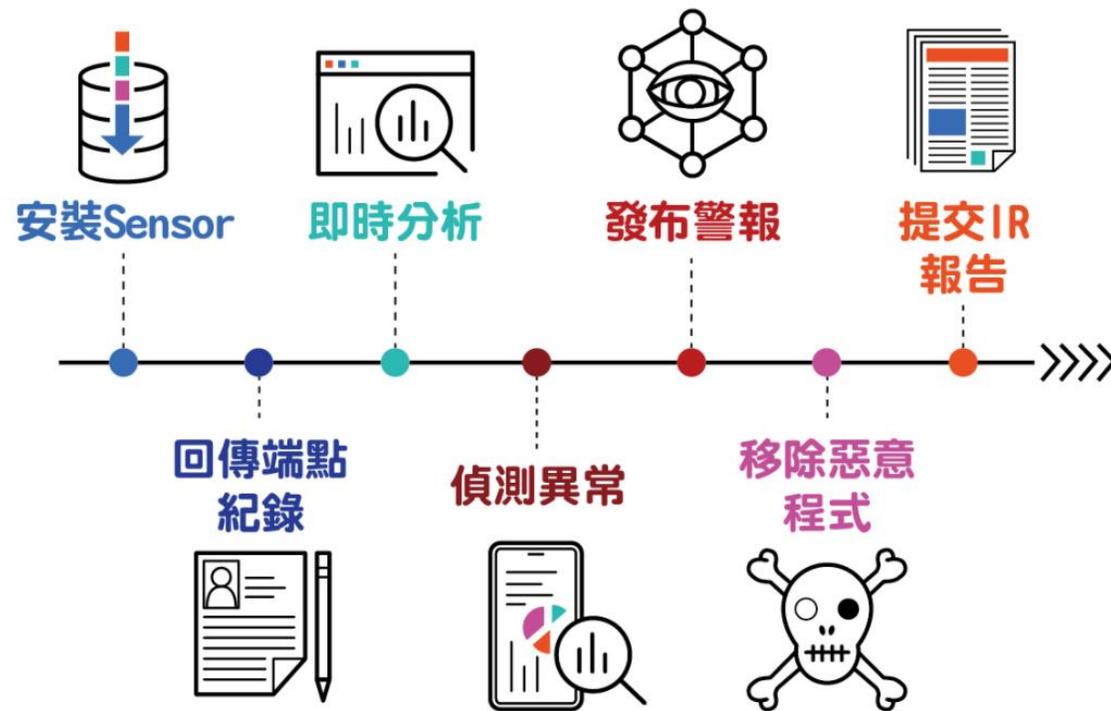
在FortiGate上加入惡意IP進行阻擋

The screenshot displays the FortiGate Security Fabric interface. At the top, navigation tabs include DASHBOARD, EVENT VIEWER (2), FORENSICS, COMMUNICATION CONTROL (38), SECURITY SETTINGS, INVENTORY (1), and ADMINISTRATION (37). The main area shows a table of events with columns for Name, Details, Interface, Fabric Sync, Type, and Ref. A dropdown menu is open for the 'Demo_Malicious_IP' event, showing details such as Address (FortiEDR_185.199.109.133), Type (IP Range), IP Range (185.199.109.133 - 185.199.109.133), Interface (any), Fabric Sync (Disabled), and Comments (FortiEDR Event ID - 335899). Below the table, a flowchart illustrates a playbook with steps: 1 Create (Process explorer.exe), 2 Create (Process cmd.exe), 3 Connect (Suspicious Application), and a final step (Connection 185.199.109.133). A red box highlights the 'Process powershell.exe' step in the flowchart and the 'Connection 185.199.109.133' step. At the bottom, a list of firewalls includes 'All Firewalls' and 'FG-60E_SSL'.

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 - 239.0.0.0		undefined	Multicast A...	0
all_hosts	224.0.0.1 - 224.0.0.1		undefined	Multicast A...	0
all_routers	224.0.0.2 - 224.0.0.2		undefined	Multicast A...	0
Address Group 5					
Demo_Malicious_IP	FortiEDR_7 FortiEDR_9 FortiEDR_5 FortiEDR_185.199.109.133		Disable	Address Gr...	1

端點安全防護基本需求

- 偵測到惡意程式自動刪除，管理者不需要任何其他額外的動作
- 偵測到惡意程式後，有個便捷的管理平台可以確認警報內容跟處理
- 除偵測到惡意程式並自動處理外，還能對應警訊額外收集資料，讓管理者可以分析攻擊的完整資訊

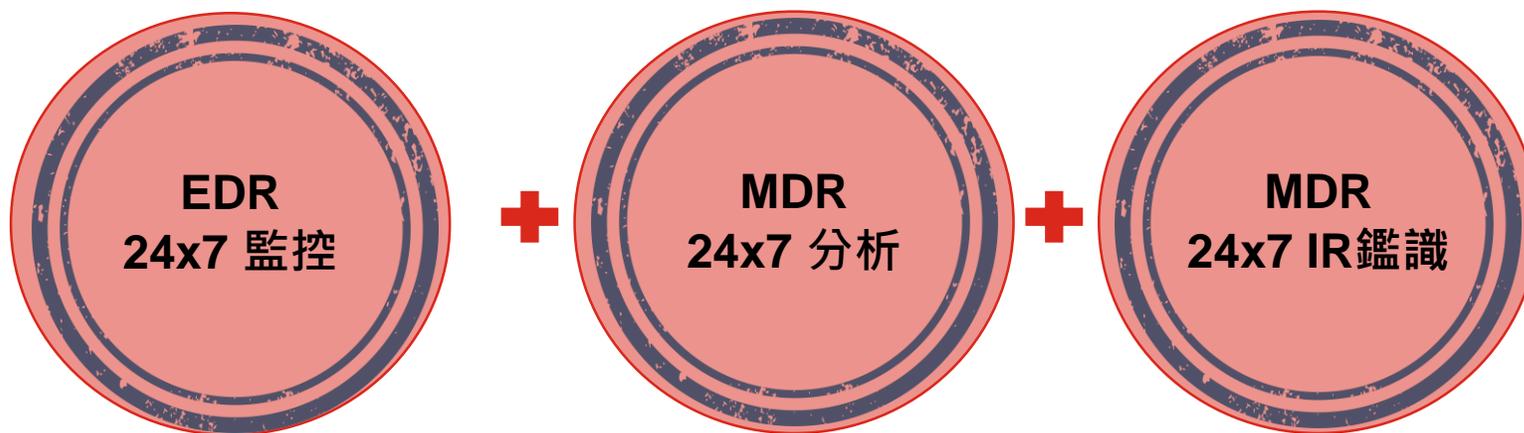


各種端點防護功能差異

EPP 端點防護	EDR Endpoint Detection & Response	MDR Managed Detection & Response	XDR eXtended Detection & Response
防毒引擎 AV / Signature / Pattern Hash / IoC / 情資	端點未知型異常行為偵測	異常未知型行為偵測	異常未知型行為偵測
端點防火牆	惡意程式行為遏制功能	惡意程式行為遏制功能	惡意程式行為遏制功能
應用程式控管 (伺服器)	異常行為軌跡紀錄 提供日後稽核	異常行為軌跡紀錄 提供日後稽核	異常行為軌跡紀錄 提供日後稽核
網頁過濾	系統回復機制	系統回復機制	系統回復機制
通訊埠與設備控管		協同專家政策調整	異質平台資安設備 跨端點與網路資安設備即時分析
弱點與補丁管理		協同專家即時監控	資安事件軌跡跨端點與網路設備 聚合，能更精準/即時IR
		資安事件處理報告	

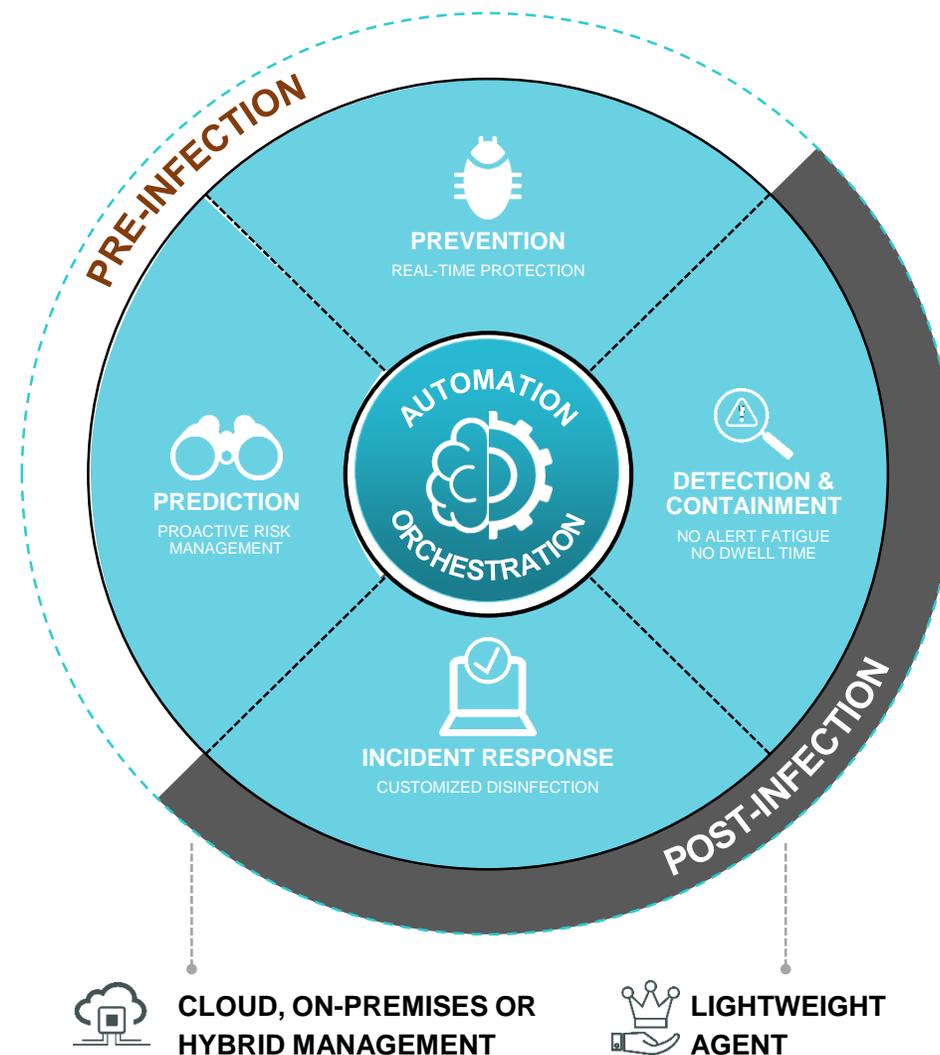
為何需要 MDR ?

- 要分析：EDR產品的保存端點的各種活動資料，需要有人分析才有效益
- 要專業：當EDR發出可疑行為分析警報時，可以有專業技術團隊協助
- 要即時：可以即時透過遠端方式處理威脅，無須等到事後處理
- 要完整：可以提供專業的事件分析報告，完整分析資安事件發生的過程
- 要可控：由專業資安技術團隊提供深入分析，可以減少企業在資安的支出

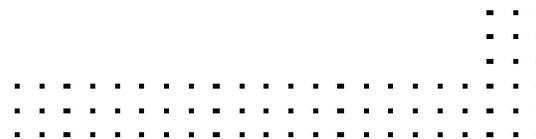


採用進階端點防護的幾個參考建議

- ✓ 是否具備針對未知攻擊手法（如零日攻擊）的檢測與防護能力，經過第三方驗證？
- ✓ 防護時效性（是7x24不間斷的即時防護VS傳統排程式掃描）？
- ✓ 端點使用者體驗（作業系統支援度與效能影響）與部署方式的選擇（雲端或落地）？
- ✓ 自動化回應能力以及與現有資安防護體系的整合？
- ✓ 鑑識能力（能記錄那些端點行為軌跡）與專業服務（MDR：本地還是國外遠端服務）？



資安網維管理平台 SIEM



什麼是 SIEM ？

ChatGPT



SIEM 是安全信息與事件管理 (Security Information and Event Management) 的縮寫。SIEM 是一種安全管理解決方案，用於集中收集、分析和管理的來自不同資訊系統和設備的安全事件和日誌資料。

SIEM 與 SOC 差別？

SIEM

Security Information and Event Management

別名

譯名：安全資訊與事件管理

比較 ▸ SOAR：Security Orchestration, Automation, and Response

定義

一種資安**解決方案/產品**，用來集中各種資安產品所蒐集到的Log，進而整合事件告警、關聯分析、產出數據報表，甚至是採取自動化腳本回應等，以輔助資安人員更有效率地建立整體環境可視性並即時排除問題。

SOC

Security Operation Center

別名

譯名：資安監控中心、資訊安全作業維運中心、資安中心

定義

在組織中，將所有資訊系統的安全性事件集中監控管理的**團隊**，通常會有一個資安戰情室，由資安人員5X8或24X7偵測、回應威脅。現有「服務產品化」的趨勢，有些人容易將SOC和SIEM的功能混稱。

現今資安網路維運所面臨的挑戰

不僅需要防護型資安解決方案，還需要建立早期預警系統

- ① 滿足
- ② 不同
- ③ 每天
- ④ 進階
- ⑤ 建立



SIEM 平台主要功能

1.安全事件**收集**：

SIEM 通過收集來自各種資訊系統（如防火牆、入侵檢測系統、網絡設備等）和應用程序的事件和日誌數據，建立一個**集中化的數據庫**。

2.安全事件**分析**：

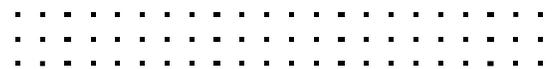
SIEM 對收集到的事件和日誌進行分析，**檢測潛在的安全威脅、異常行為和攻擊模式**。這包括實時事件監測、日誌分析、漏洞掃描等技術。

3.安全事件**管理**：

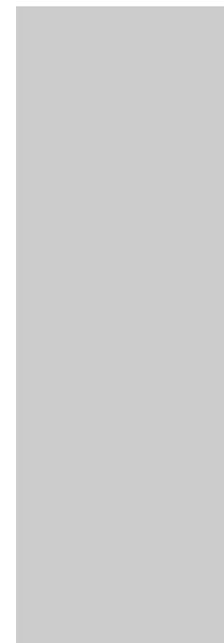
SIEM 提供對安全事件的管理功能，例如**警報生成、事件追蹤、優先級分類、工作流程管理**等。這有助於組織快速響應和處理安全事件。

4.合規性**報告**：

SIEM 可以生成合規性報告，幫助組織**滿足法規和合規要求**。它可以監測和記錄安全事件，並生成符合特定合規標準（如PCI DSS、HIPAA等）的報告。



一、收集



SIEM的基本功 – 任何類型的LOG收集

資安日誌與系統資訊

NGFW / IPS / VPN

EPP/EDR

Web Application

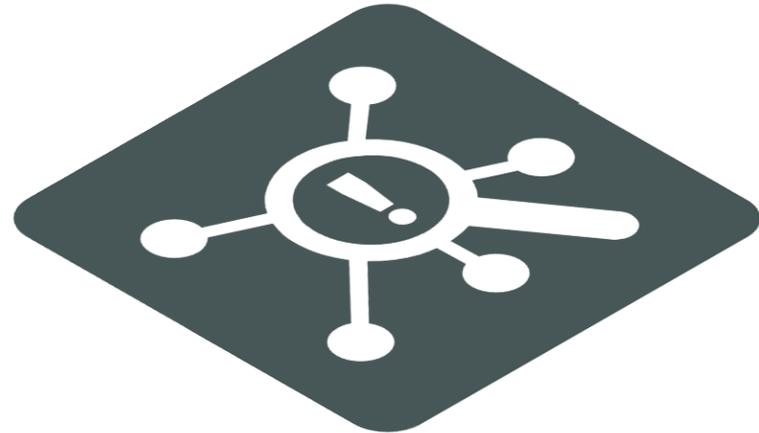
Email System

AAA Server

Database

Traffic / Flows

Router / Switch / WLAN, etc.



基本功要札實 – 品牌的支援度



基本功有彈性 – 內建 Parser 系統

無需花費過多人力自定義 或
需要原廠額外收費客製

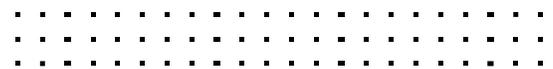
“Teddy” , “183” , “76” , “20.2” , “單身” , “靦腆害羞”

姓名	Teddy
身高	183
體重	76
BMI	20.2
感情狀況	單身
個性	靦腆害羞

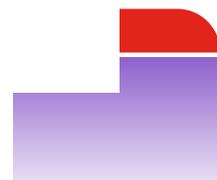
原始日誌與記錄

日誌記錄正規化
與內容加值分析

The screenshot shows a window titled "Event Details" with a search bar and a list of log entries. A red dashed box highlights the raw log data, which is a JSON-like string containing various fields such as date, time, devname, devid, logid, type, subtype, level, vd, root, eventtime, tz, srcip, srcname, srcport, srcintf, srcintfrole, dstip, dstport, dstintf, dstintfrole, sessionid, proto, action, policyid, policytype, poluid, dstcountry, srccountry, transp, transpport, duration, contrib, and contribrole. Below the log data, a table with two columns, "Item" and "數值", displays normalized and analyzed data. The table includes fields like Application Group Name (unscanned), Collector ID (10000), Count (1), Destination City (Moscow), Destination Country (Russian Federation), Destination Country Code (RU), Destination Host Name (HOST-185.255.135.33), Destination IP (185.255.135.33), Destination Interface Name (port17), Destination Latitude (55.75583), Destination Longitude (37.6173), and Destination Organization (SUPERSERVERSDATACENTER RU).



二、分析

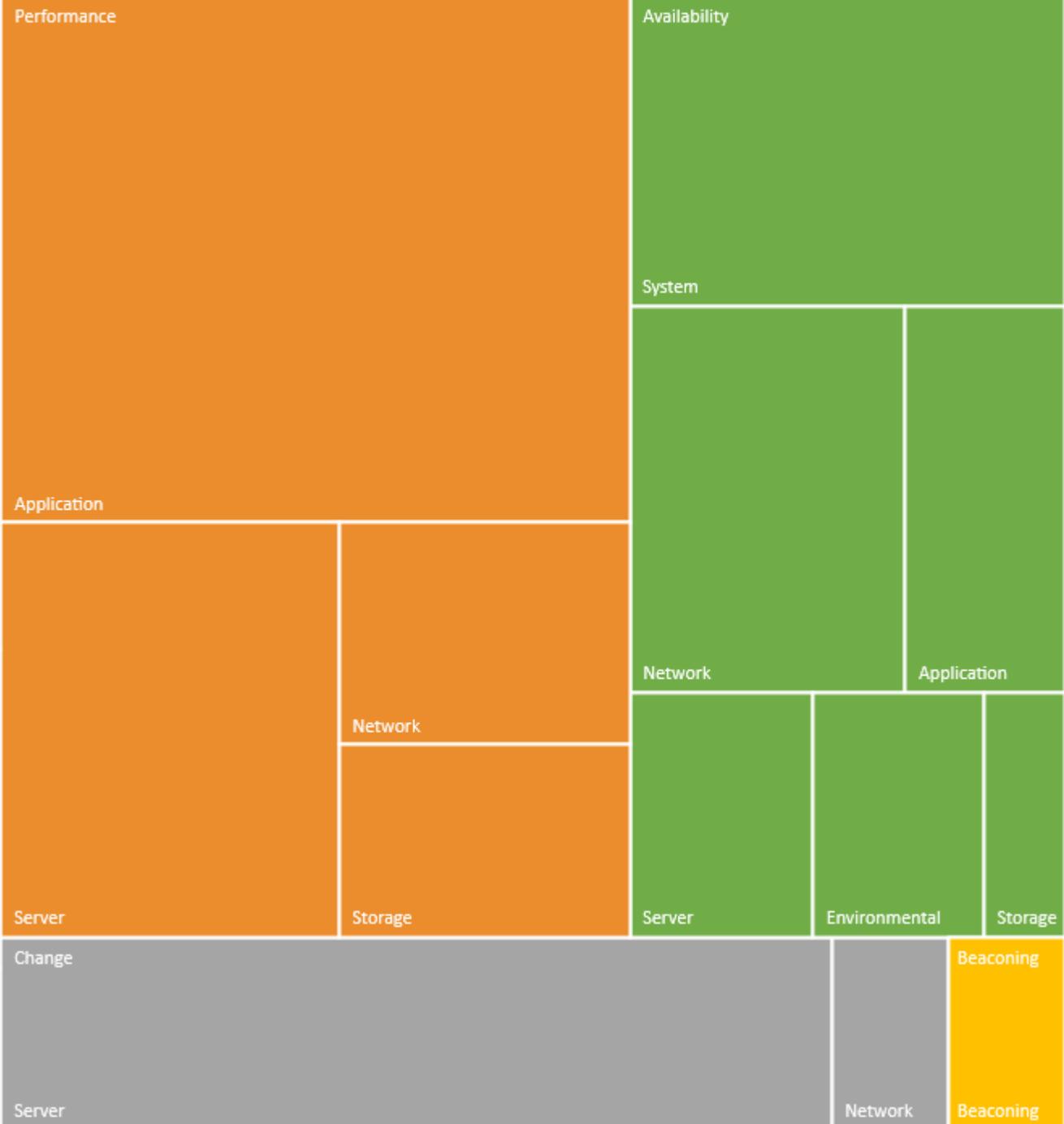


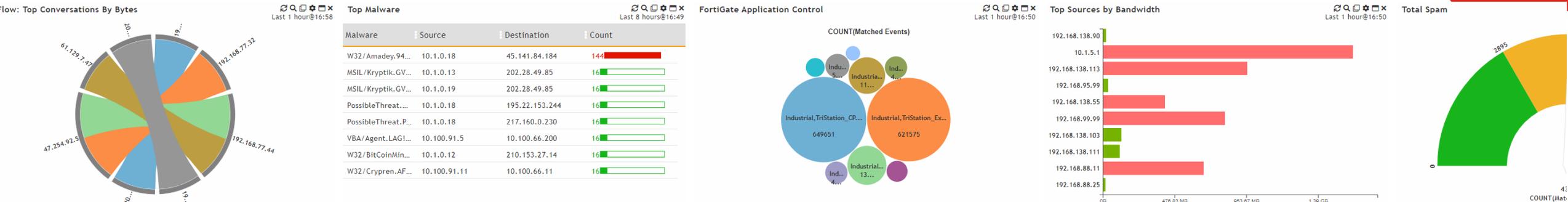
智能分析 (AI) 與 機器學習 (ML) 關聯規則

智能關聯分析規則，一般橫跨四大領域：

- 資安 (Security)
- 效能 (Performance)
- 可用度 (Availability)
- 異動 (Change)

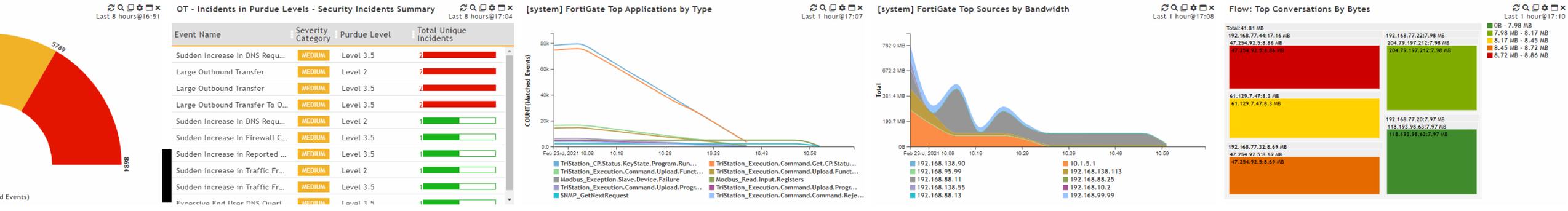
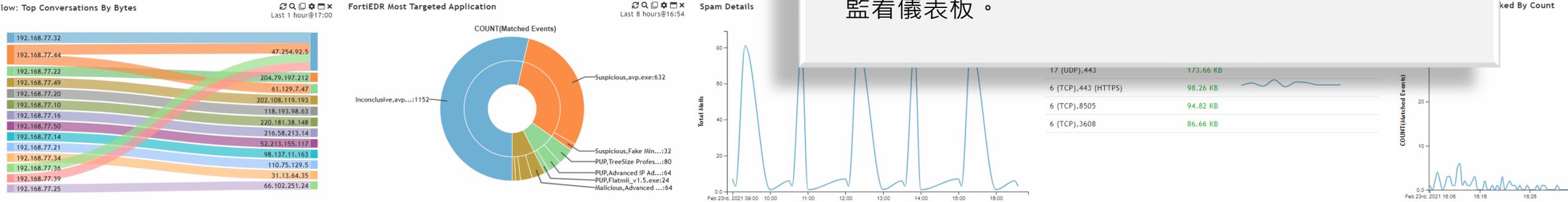
可自行定義修改關聯分析規則來
滿足各種監看告警需求





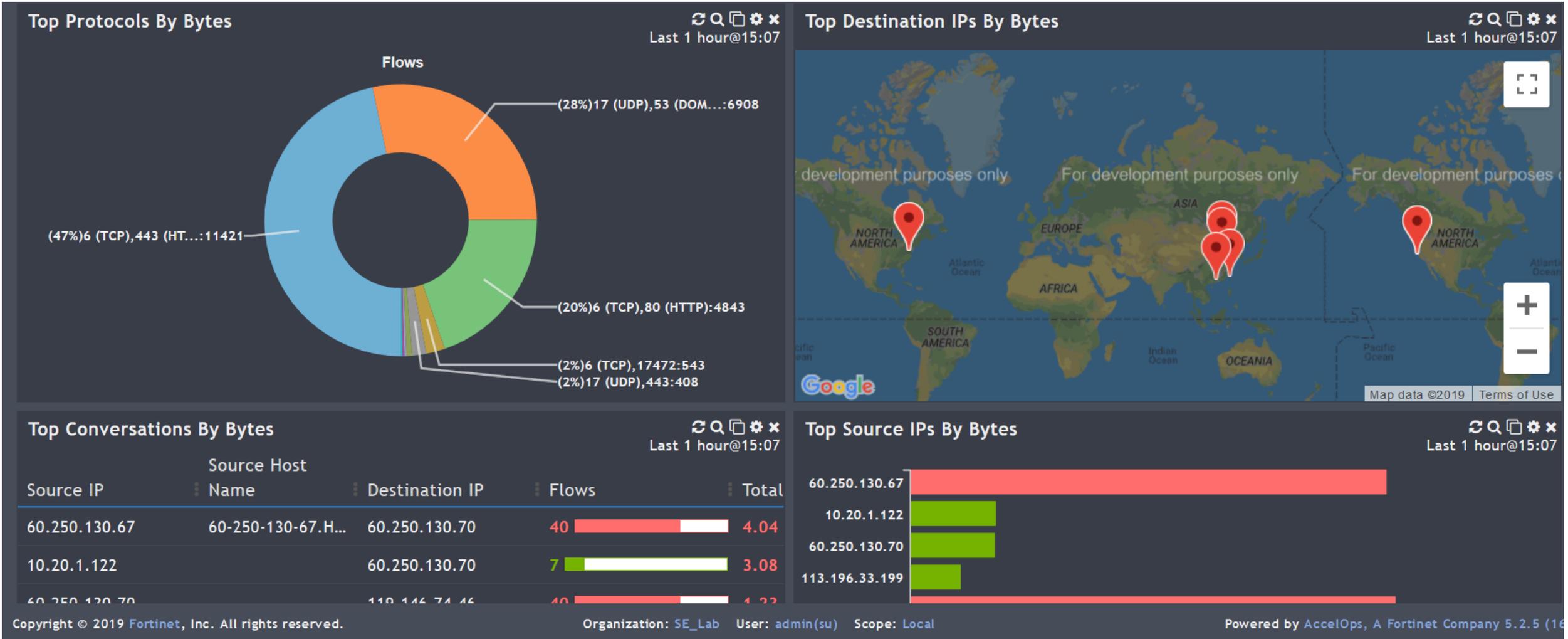
任何分析結果轉成儀表板顯示

SIEM 提供眾多預設的儀表板方便您監看資安與效能資訊，亦可將任何關聯分析儲存樣板轉變成自定義的監看儀表板。



融合式分析第一步

- 支持防火牆與 NetFlow / SFlow / JFlow / IPFix 流量記錄分析統計



身分識別與連網位置關聯分析

- 快速查找人員與設備，何時、何地以及如何連網

The screenshot shows the 'Identity & Location' dashboard with a table of network activity. Red boxes highlight specific columns: IP Address, MAC Address, User, Host Name, Domain, VLAN ID, Connected to, First Seen, and Last Seen. Red arrows point from text boxes below to these columns, indicating data sources: '來自 DHCP 日誌' (from DHCP logs) for IP and MAC; '來自 AD 登入日誌' (from AD login logs) for User; '來自 L2 交換器自動探索記錄' (from L2 switch auto-discovery records) for Host Name, Domain, and VLAN ID; and '來自所有相關日誌或記錄' (from all related logs or records) for First Seen and Last Seen.

IP Address	MAC Address	User	Host Name	Domain	VLAN ID	Connected to	First Seen	Last Seen	Organization
10.10.1.120	98:E0:D9:8B:E3:23		JaniedeAir-2			OA-600D.fortinet.com .tw 192.168.1.254	Dec 26, 2018 2:24:48 PM	Jan 9, 2019 8:19:06 PM	SE_Lab
10.1.206.151	90:6C:AC:29:FE:28		FG800D3915800145				Dec 19, 2018 3:57:48 PM	Jan 9, 2019 8:19:36 PM	SE_Lab
10.1.200.242	00:50:56:ba:47:86	kevin (Domain)	WIN7B.fortinet.com.tw	FORTINET	1	ERS3510GT 10.1.210.35 (Ifc4 (Slot: 1 Port: 4))	Dec 17, 2018 12:28:19 AM	Jan 9, 2019 8:34:30 PM	Super/Local
10.1.206.1	:A0:D9:1C						Dec 5, PM	3:03	SE_Lab
10.1.206.1	:18:D6:9F						Dec 5, PM	3:25	SE_Lab
10.30.1.107	d4:6d:6d:2e:05:68		LAPTOP-4PIG5MCO			OA-600D.fortinet.com .tw 192.168.1.254	Jan 3, 2019 2:52:46 PM	Jan 3, 2019 2:52:46 PM	SE_Lab
10.30.1.105	f0:18:98:50:ff:48		zhangheeMacBook			OA-600D.fortinet.com .tw 192.168.1.254	Jan 3, 2019 3:02:24 PM	Jan 3, 2019 3:02:24 PM	SE_Lab
10.30.1.105	F0:18:98:50:FF:48		zhangheeMacBook			OA-600D.fortinet.com .tw 192.168.1.254	Jan 7, 2019 5:12:21 PM	Jan 7, 2019 5:12:53 PM	SE_Lab
42.74.77.177		marty (VPN)		10.1.200.254			Jan 4, 2019 2:08:50 PM	Jan 4, 2019 2:08:50 PM	SE_Lab
10.30.1.102	34:36:3b:cd:f1:4a		Spencerteki-MBP			OA-600D.fortinet.com .tw 192.168.1.254	Jan 3, 2019 1:49:23 PM	Jan 3, 2019 2:44:01 PM	SE_Lab

智能分析 (AI) 異常行為

啟動	Name	Description	Exceptions	範圍
<input checked="" type="checkbox"/>	(s) AI: File Creation Anomaly	FortiInsight AI module detects unusual file Creation by an user		System
<input checked="" type="checkbox"/>	(s) AI: File Deletion Anomaly	FortiInsight AI module detects unusual file deletion by an user		System
<input checked="" type="checkbox"/>	(s) AI: File Reading Anomaly	FortiInsight AI module detects unusual file reading by an user		System
<input checked="" type="checkbox"/>	(s) AI: File Writing Anomaly	FortiInsight AI module detects unusual file writing by an user		System
<input checked="" type="checkbox"/>	(s) AI: Process Started Anomaly	FortiInsight AI module detects unusual process started by an user		System
<input checked="" type="checkbox"/>	(s) AI: Process Stopped Anomaly	FortiInsight AI module detects unusual process stoppage by an user		System
<input checked="" type="checkbox"/>	(s) ARP Exploit	Detects ARP attack		System
<input checked="" type="checkbox"/>	(s) AWS SecHub: Host Vulnerability Detected	AWS Security Hub detected host vulnerability		System
<input checked="" type="checkbox"/>	(s) AWS SecHub: Software and Configuration Violation	AWS Security and Configuration Violation Detected		System
<input checked="" type="checkbox"/>	(s) AWS SecHub: Tactics: Collection Detected	AWS Security Hub detected Collection tactics. Adversary is trying to collect data of their interest.		System
<input checked="" type="checkbox"/>	(s) AWS SecHub: Tactics:	AWS Security Hub detected Command and Control tactics. Adversary is trying to communicate with other compromised systems and receive commands and		System

機器學習 (ML) 分析異常行為

啟動	Name	Description	Exceptions	範圍
<input checked="" type="checkbox"/>	(s) Sudden Decrease in Reported Events From A Host	Detects that a reporting device is suddenly reporting less events. The current average over the one hour time window is less than 3 times the standard deviation and also 50% less than the statistical mean		System
<input checked="" type="checkbox"/>	(s) Sudden Increase In DNS Requests From A Specific Host	Detects sudden increase in DNS requests from a specific source IP - over a 15 minute period, a particular source IP is doing excessive DNS requests. Excessive DNS requests is defined as at least 100 requests and current count is 3 standard deviations away from mean for the current hour. Excessive Destination names is defined as 50 distinct name resolutions and current count is more than 3 standard deviations away from the mean for the current hour		System
<input checked="" type="checkbox"/>	(s) Sudden Increase In Firewall Connections	Detects sudden increase in permitted firewall connections in a 30 minute window, the current firewall connections is more than 3 standard deviations away from the mean.		System
<input checked="" type="checkbox"/>	(s) Sudden Increase In Firewall Denied Inbound Traffic To A Specific TCP/UDP port	Detects anomalous denied inbound traffic profile on a specific TCP/UDP port - over a 30 minute window, both the total number of denies and the number of unique source IP addresses are at least 3 standard deviations away from the mean for the current hour		System
<input checked="" type="checkbox"/>	(s) Sudden Increase In Firewall Denied Outbound Traffic To A Specific TCP/UDP port	Detects anomalous denied outbound traffic profile on a specific TCP/UDP port - over a 30 minute window, both the total number of denies or the number of unique destination IP addresses are at least 3 standard deviations away from the mean for the current hour		System

基於機器學習 (ML) 基準線
與異常行為智能分析

進階的智能分析機制

啟動	Name	Description	Exceptions	範圍
<input checked="" type="checkbox"/>	(s) Sudden Increase in STM Response Times	Detects a sudden 50% increase of Synthetic transaction monitoring response Times over a 30 minute time window		System
<input checked="" type="checkbox"/>	(s) Sudden Increase in Server Process Count	Detects that a server is suddenly running 25% more processes than the average		System
<input checked="" type="checkbox"/>	(s) Sudden Increase in Successful Logons To A Host	Detects a sudden 50% increase of successful logons to a host over a 30 minute window		System
<input checked="" type="checkbox"/>	(s) Sudden Increase in System Memory Usage	Detects a sudden increase in system memory usage - over a 30 minute interval, either the physical or virtual memory is 25% more than the statistical average over that same time period and the current physical memory usage is at least 50%		System
<input checked="" type="checkbox"/>	(s) Sudden Increase in User Login Volume	Detects daily user login volume anomaly against profile. This may indicate suspicious user behaviors.		System
<input checked="" type="checkbox"/>	(s) Sudden Increase in WMI Response Times	Detects a sudden 50% increase of WMI Response window		System
<input checked="" type="checkbox"/>	(s) Sudden User Location Change	Detects location change for a user unfeasible in the period of time. This may indicate a stolen credential.		System
<input checked="" type="checkbox"/>	(s) Sudden User Login Pattern Change	Detects daily user login distribution anomaly against profile. This may indicate suspicious user behaviors.		System

基於經緯度智能分析

進階的智能分析機制

啟動	Name	Description	Exceptions	範圍
<input type="checkbox"/>	(s) Dynamically generated host name: malware likely	Detects algorithmically generated host name in network traffic - malware often use algorithmically generated host names to communicate.		System
<input checked="" type="checkbox"/>	(s) End User DNS Queries to Unauthorized DNS Servers	Detects a scenario where a host, that is itself not a DNS server, is trying to send DNS requests to unauthorized DNS servers. Authorized DNS servers are represented by the "DNS Server" group. In a typical scenario, end hosts always send DNS requests to authorized DNS servers which in turn communicate to other DNS servers - so this behavior may indicate malware running on the host.		System
<input checked="" type="checkbox"/>	(s) Excessive End User DNS Queries	Detects a scenario where a host, that is itself not an DNS server, is sending excessive DNS requests. Authorized DNS servers are represented by the "DNS Server" group. In a typical scenario, the frequency of end host DNS requests is not high unless, there is a script running - this might indicate the presence of malware on the end host.	✓	System
<input checked="" type="checkbox"/>	(s) Excessive End User Mail	Detects a scenario where a host, that is itself not an authorized mail gateway, is sending excessive emails (more than 20 emails in 2 minutes). This behavior may indicate malware running on an end host that is trying to send spam or privileged information to its own set of mail servers (which may be compromised).		System
		Detects a scenario where a host, that is itself not an authorized mail gateway,		

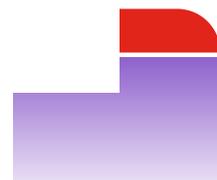
基於演算法智能分析

基於白名單智能分析

基於條件閾值智能分析



三、管理



簡單建立標準化 SOC / NOC 日常維運流程

- 詳細檢視、追蹤告警事故

The screenshot displays the FortiSIEM interface with a top navigation bar containing '儀表板', '關聯分析', '告警事故', '派工管理', 'CMDB', '資源庫', and '工作'. Below this is a secondary navigation bar with '動作', '概觀', '清單', '風險', '探索者', and a refresh button. The main content area shows '資安 Incidents' with a summary: 'HIGH: 3', 'MEDIUM: 221', and 'LOW: 0'. A table lists recent incidents with columns for '最近一次發生', 'Incident', '報告', '來源', and '目標'. A red callout box labeled '原始日誌與記錄' points to the 'Incident' column. Below the incident table, there are tabs for 'Details', '事件 Events', and '規則'. The '事件 Events' tab is active, showing a table with columns for 'Event Name', 'Source IP', 'Destination IP', 'IP Protocol', 'Source TCP/UDP Port', and 'Destination TCP'. A red callout box labeled '日誌記錄正規化與內容增值分析' points to this table. On the right side, an 'Event Details' window is open, displaying raw event data in XML format and a list of normalized items with their counts. A red dashed box highlights the raw event data and the normalized items list. The raw event data includes fields like 'date', 'time', 'devname', 'devid', 'logid', 'type', 'subtype', 'level', 'vd', 'eventtime', 'tz', 'srcip', 'srcname', 'srcport', 'srcintf', 'srcintfrole', 'dstip', 'dstport', 'dstintf', 'dstintfrole', 'wan', 'poluuid', 'action', 'policyid', 'policytype', 'service', 'dstcountry', 'srccountry', 'trandisp', 'transip', and 'transport'. The normalized items list includes 'Collector ID', 'Count', 'Destination City', 'Destination Country', 'Destination Host Name', 'Destination IP', 'Destination Interface Name', 'Destination Latitude', 'Destination Longitude', and 'Destination Organization'.

原始日誌與記錄

日誌記錄正規化與內容增值分析

最近一次發生	Incident	報告	來源	目標
Nov 01 2019, 06:44:30 PM	Traffic to Emerging Threat IP ...	LAB-1500D	10.1.210.100	159.151.129.61
Nov 01 2019, 06:01:00 PM	Outbound cleartext password ...	LAB-1500D	10.1.206.150	210.59.230.27
Nov 01 2019, 05:54:30 PM	Outbound cleartext password ...	OA-600D.fortinet.com.tw	10.10.1.105	208.91.113.85

Item	數值
Collector ID	10000
Count	1
Destination City	Nanterre
Destination Country	France
Destination Host Name	HOST-159.151.129.61
Destination IP	159.151.129.61
Destination Interface Name	port18
Destination Latitude	48.892
Destination Longitude	2.2067
Destination Organization	Saint-Gobain Systeme d'Information

簡單建立標準化 SOC / NOC 日常維運流程

- 內建工單系統，告警事故即時反應並進行追蹤

The screenshot displays the FortiSIEM interface for incident management. At the top, there are navigation tabs: 儀表板 (Dashboard), 關聯分析 (Correlation Analysis), 告警事故 (Alerts/Incidents), 派工管理 (Ticket Management), CMDB, 資源庫 (Resource Library), 工作 (Work), and 系統管理 (System Management). Below the navigation, a summary bar shows: 0 New, 1 Assigned, 2 High, 1 Overdue, and 1 Late. A table lists incident tickets with columns: Elapsed, State, Priority, Ticket ID, Summary, Assignee, Creator, and Creation Date. Three red callout boxes highlight specific tickets: '事故工單逾期' (Overdue Incident Ticket) points to a ticket with state 'Reopened' and priority 'Medium'; '事故工單處理中' (Incident Ticket Being Processed) points to a ticket with state 'In Progress' and priority 'High'; '新建立事故工單' (Newly Created Incident Ticket) points to a ticket with state 'Assigned' and priority 'High'. Below the table, there are two panels: '詳情' (Details) on the left and 'Action History' on the right. The '詳情' panel shows Incident ID: 225314, 組織: SE_Lab, Due Date: Nov 01 2019, 07:40:11 PM, and Escalation Policy: escalate to supervisor. The 'Action History' panel shows a sequence of actions: Super/admin at 07:40:05 PM, Due date changed to Fri Nov 01 19:40:11 CST 2019, system/SYSTEM(su) at 07:40:02 PM, and two email notifications sent according to the escalation policy at 19:40:02 CST 2019.

Elapsed	State	Priority	Ticket ID	Summary	Assignee	Creator	Creation Date
Overdue	Reopened	Medium	5650352	Brute Force Login Success, in Company-...	Unicomp	admin <kmyang@fortinet.com>	Oct 25 2019, 08:58:38 PM
90 %	In Progress	High	5650354	Outbound cleartext password usage det...	kmyang	admin <kmyang@fortinet.com>	Nov 01 2019, 07:39:02 PM
0 %	Assigned	High	5650353	Traffic to Emerging Threat IP List, in LA...	kmyang	admin <kmyang@fortinet.com>	Nov 01 2019, 07:37:13 PM

事故工單逾期

事故工單處理中

新建立事故工單

詳情

Incident ID: 225314

組織: SE_Lab

Due Date: Nov 01 2019, 07:40:11 PM

Escalation Policy: escalate to supervisor

Action History

Super/admin Nov 01 2019, 07:40:05 PM

Due date changed to Fri Nov 01 19:40:11 CST 2019

system/SYSTEM(su) Nov 01 2019, 07:40:02 PM

Email sent according to policy: escalate to supervisor

Email sent at time: Fri Nov 01 19:40:02 CST 2019

簡單建立標準化 SOC / NOC 日常維運流程

- 迅速反應執行緩解調控措施

The screenshot displays the FortiSIEM interface. At the top, there are navigation tabs: 儀表板 (Dashboard), 關聯分析 (Correlation Analysis), 告警事故 (Alerts/Incidents), 派工管理 (Ticket Management), CMDB, 資源庫 (Resource Library), 工作 (Work), and 系統管理 (System Management). Below these are secondary tabs: 動作 (Actions), 概觀 (Overview), 清單 (List), 風險 (Risk), 探索者 (Explorer), and 1 分鐘 (1 Minute). On the right, there are filters for 選擇行位 (Select Row) and Time Range: Last 2 Hours.

A summary bar shows incident counts: HIGH: 5, MEDIUM: 226, and LOW: 0. Below this is a table of incidents with columns: Incident, 報告 (Report), 來源 (Source), 目標 (Target), 詳情 (Details), 告警事故狀態 (Alert Status), and 解決方式 (Resolution Method).

Incident	報告	來源	目標	詳情	告警事故狀態	解決方式
Outbound cleartext password ...	LAB-1500D	10.1.206.150	210.59.230.27 Destination TCP/UDP Port: 110	IP Protocol: 6	Active	Open
Permitted Traffic from Emergi...	LAB-1500D	80.82.77.139	60.250.130.72		Active	Open
Traffic to Emerging Threat IP ...	LAB-1500D	10.1.210.100	159.151.129.61		Active	Open

Below the table, there are filter options: 子模式: Shadowserver, 自動展開 (checked), 原始事件自動換行 (unchecked), 顯示事件型式 (unchecked), and Show Raw Event Only (unchecked).

A red box highlights the 'Remediate Incident' option in the left-hand '動作' (Actions) menu. A red callout box with white text points to this option, containing the text: 執行告警事故 緩解調控措施 (Execute Alert Incident Mitigation Measures).

簡單建立標準化 SOC / NOC 日常維運流程

- 迅速反應執行緩解調控措施

The screenshot displays the FortiSIEM interface with a 'Run Remediation' modal window open. The modal contains the following configuration:

- Enforce On:** Device:LAB-1500D
- Remediation:** Fortinet FortiOS - Block IP FortiOS API (30)
- Run On:** fsm_collector176

Red callouts with arrows indicate the configuration steps:

- 設定執行動作設備 (Set execution action device) - points to the 'Enforce On' field.
- 設定緩解調控措施 (Set mitigation measure) - points to the 'Remediation' dropdown.

The background interface shows incident details for 'Outbound cleartext password' and a table of events:

Event Receive Time	Reporting IP	Event Name	Source IP	Destination IP	IP Protocol	Source TCP/UDP Port	Destination TCP/UDP P	Raw Event Log
Nov 01 2019, 06:43:17 PM	10.1.200.254	Timeout traffic	10.1.210.100	159.151.129.61	6 (TCP)	59954	80 (HTTP)	<189>date=2019-11-01 time=18:43:17 devn:
Nov 01 2019, 06:43:17 PM	10.1.200.254	Timeout traffic	10.1.210.100	159.151.129.61	6 (TCP)	59953	80 (HTTP)	<189>date=2019-11-01 time=18:43:16 devn:

簡單建立標準化 SOC / NOC 日常維運流程

- 內建緩解調控措施腳本，可與多品牌設備協作聯防

The screenshot displays the FortiSIEM interface, specifically the 'Resources > Remediations' section. The page features a navigation menu on the left with categories like Reports, Rules, Networks, Watch Lists, Protocols, Event Types, Malware Domains, Malware IPs, Malware URLs, Malware Processes, Country Groups, Malware Hash, Default Password, Anonymity Network, and User Agents. The 'Remediations' category is currently selected.

At the top of the Remediations section, there are buttons for '新增' (Add), '編輯' (Edit), '刪除' (Delete), and '複製' (Copy), along with a search bar labeled 'Search...'. On the right side, there are navigation controls including a refresh button, a dropdown menu set to 'System', and pagination controls showing '1/1' and '30', with the number '30' circled in red.

The main content is a table listing various remediation scripts. The table has the following columns: 名稱 (Name), 設備型式 (Device Type), 腳本名稱 (Script Name), 通訊協定 (Protocol), 描述 (Description), and 範圍 (Scope).

名稱	設備型式	腳本名稱	通訊協定	描述	範圍
Add IP FortiADC	Fortinet FortiADC	fortiadc_add_ip.py	SSH	Add IP	System
Add IP FortiCache	Fortinet FortiCache	forticache_add_ip.py	SSH	Add IP	System
Block Domain InfoBlox	InfoBlox NiOS	infoblox_dns_block_domain.py	HTTPS	Block a domain on Infoblox	System
Block Domain Windows DNS	Microsoft Windows	windows_dns_block_domain.py	MS_WMI	Block a domain on Windows DNS	System
Block Email FortiMail	Fortinet FortiMail	fortimail_block_mail.py	HTTPS	Block Email Address	System
Block IP Cisco ASA	Cisco ASA	cisco_asa_block_ip.py	SSH	Block IP on Cisco ASA	System
Block IP FortiOS 5.3	Fortinet FortiOS	fortigate_block_ip_before_5.4.py	SSH	Block IP on FortiGate	System
Block IP FortiOS 5.4	Fortinet FortiOS	fortigate_block_ip_after_5.4.py	SSH	Block IP on FortiGate	System
Block IP FortiOS 5.4 (300sec)	Fortinet FortiOS	fortigate_block_ip_after_5.4_300sec.py	SSH	Block IP on FortiGate	User
Block IP FortiOS API	Fortinet FortiOS	fortigate_block_ip_with_api.py	HTTPS	Block IP on FortiGate	System
Block IP FortiWeb	Fortinet FortiWeb	fortiweb_block_ip.py	HTTPS	Block IP	System
Block IP PAN	Palo Alto PAN-OS	paloalto_block_ip.py	SSH	Block IP on Palo Alto Firewall	System
Block MAC FortiOS	Fortinet FortiOS	fortigate_block_mac.py	SSH	Block IP on FortiGate	System
Deauth User ArubaOS	Aruba ArubaOS WLAN Controller	aruba_deauth_mac.py	SSH	Deauth a user on Aruba WLAN Controller	System
Deauth User Cisco WLC	Fortinet FortiWLC	fortiwlc_deauth_mac.py	SSH	Deauth a user on FortiWLC	System
Deauth User Cisco WLC	Cisco WLAN Controller	cisco_wlc_deauth_mac.py	SSH	Deauth a user on Cisco WLAN Controller	System

At the bottom of the page, there are buttons for '摘要' (Summary) and '自動展開' (Auto-expand), along with up and down arrow icons.

簡單建立標準化 SOC / NOC 日常維運流程

- 全面自動化的告警事故反應流程

The screenshot shows the FortiSIEM interface with the 'Notification Policy' configuration window open. The interface includes a top navigation bar with icons for Dashboard, Correlation Analysis, Alerts, Ticket Management, CMDB, Resource Library, Work, and System Management. A left sidebar contains menu items for Build, Device Support, Health Status, Authorization, and Data Update, with a 'Settings' button highlighted. The 'Notification Policy' window has the following configuration:

- Severity: Low Medium High
- Rules: Rule: Traffic to Emerging Threat IP List
- Time Range: ANY
- Affected Items: DevGroup: Firewall
- Affected Orgs: DevGroup: Firewall
- Action:
 - Send Email/SMS to the target users.
 - Run Remediation/Script.
 - Invoke an Integration Policy. Run: no policy
 - Create Ticket when an incident is created.
 - Send SNMP message to the destination set in Admin > Settings > Analytics.
 - Send XML file over HTTP(S) to the destination set in Admin > Settings > Analytics.
 - Open Remedy ticket using the configuration set in Admin > Settings > Analytics.
- Settings:
 - Do not notify when an incident is cleared automatically.
 - Do not notify when an incident is cleared manually.
 - Do not notify when an incident is cleared by system.

At the bottom of the window are '儲存' (Save) and '取消' (Cancel) buttons. Three red callout boxes with arrows point to specific settings:

- 自動告警事故通報設定 (Automatic alert incident notification setting) points to the 'Send Email/SMS to the target users' checkbox.
- 自動緩解調控措施設定 (Automatic mitigation control measure setting) points to the 'Run Remediation/Script' checkbox.
- 自動建立告警事故工單 (Automatic creation of alert incident tickets) points to the 'Create Ticket when an incident is created' checkbox.

設備自動探索與組態管理資料庫

學習了解監控的網路環境並建立維運基準線



設備識別分類



運行效能監看

A screenshot of a configuration management interface. It shows a table with columns 'Rev', 'Date', and 'Type/File Name'. The table contains three rows of data for 'startup-config' files. Above the table are buttons for 'Diff...', '刪除', and 'Export'. At the top, there are tabs for '摘要', '屬性', '監看', '軟體', '硬體', and '組態配置'.

Rev	Date	Type/File Name
33	Feb 13 2022, 01:15:42 AM	startup-config
32	Feb 12 2022, 11:06:37 PM	startup-config
31	Dec 07 2021, 11:29:14 AM	startup-config
30	Dev	

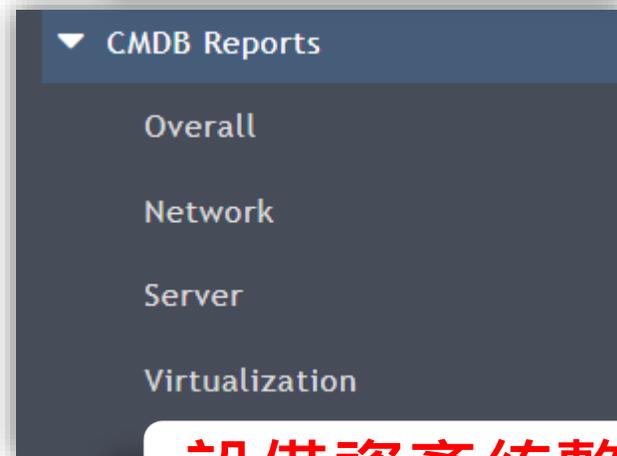
組態配置監看



應用導向管理



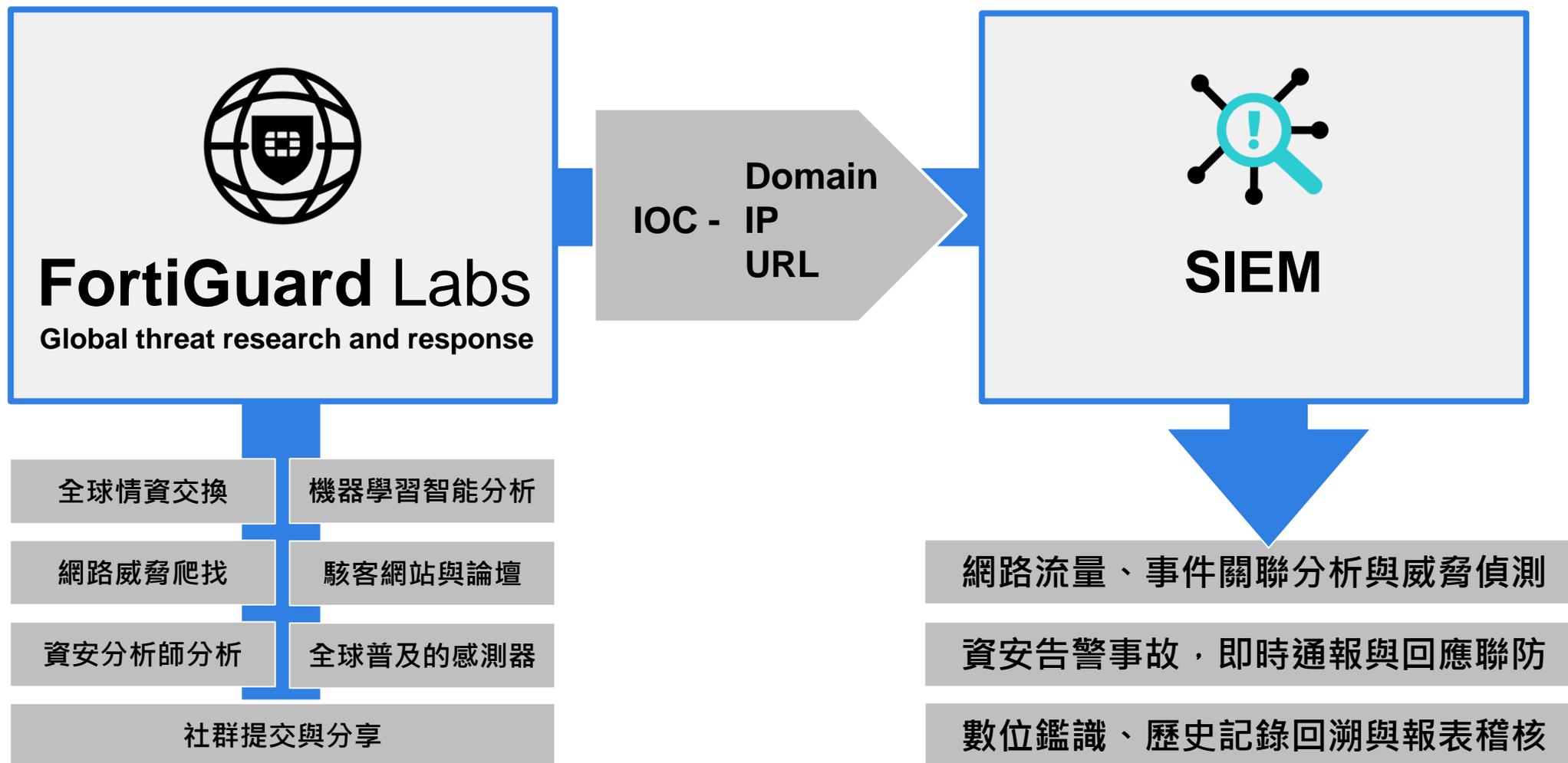
威脅情資整合

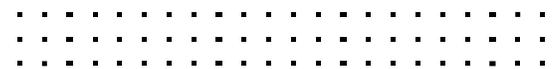


設備資產統整

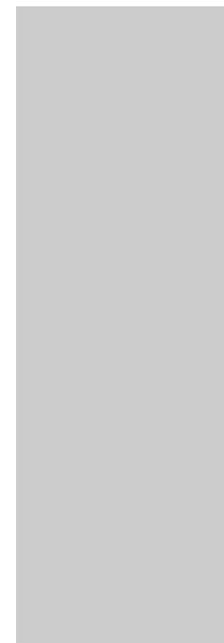
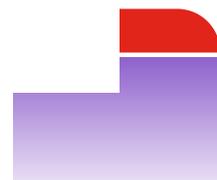
自動更新情資，分析、告警與聯防

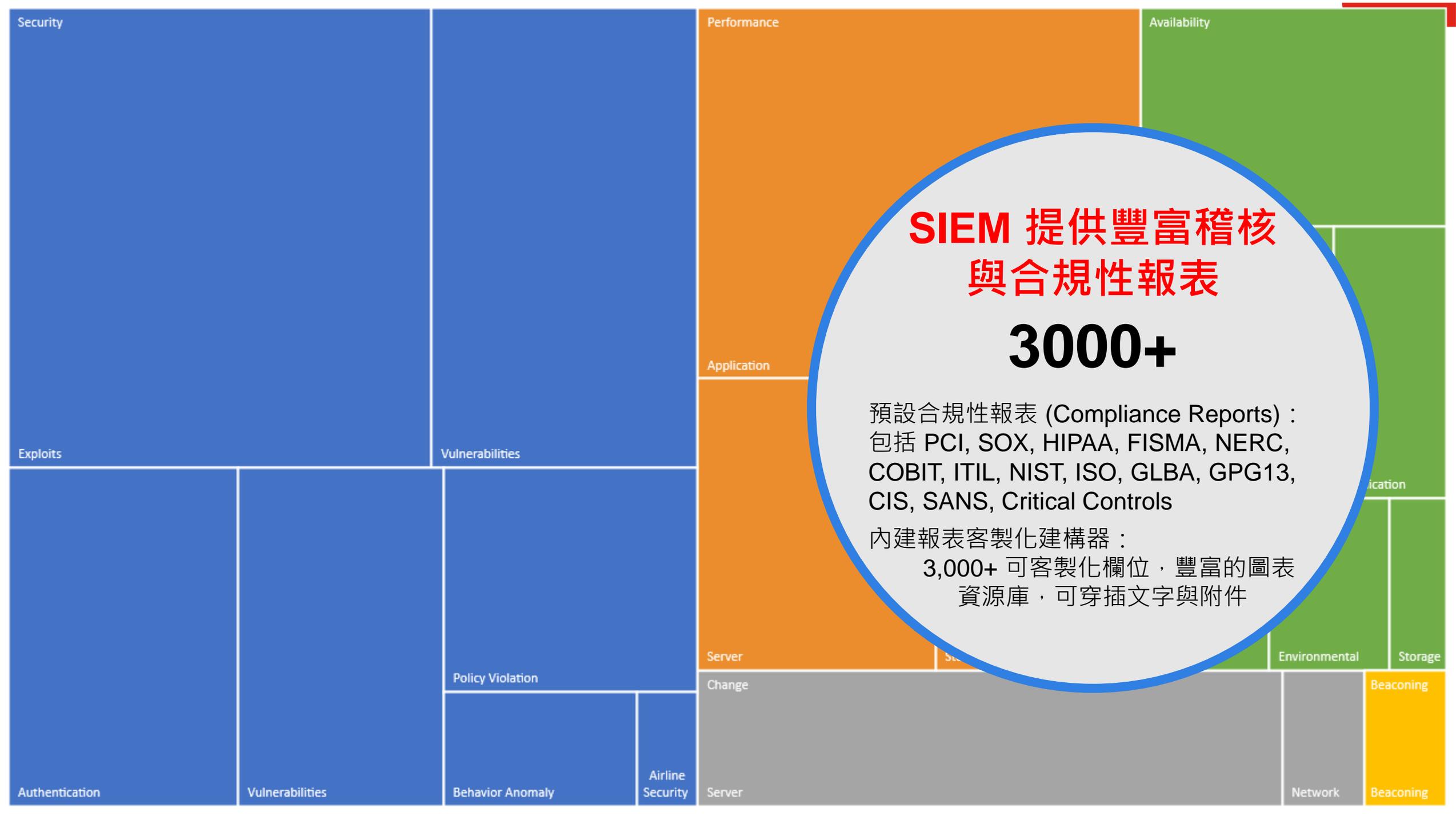
整合並自動更新外部情資 (FortiGuard、第三方情資或用戶自行定義)





四、報告





SIEM 提供豐富稽核 與合規性報表

3000+

預設合規性報表 (Compliance Reports) :
包括 PCI, SOX, HIPAA, FISMA, NERC,
COBIT, ITIL, NIST, ISO, GLBA, GPG13,
CIS, SANS, Critical Controls

內建報表客製化建構器 :
3,000+ 可客製化欄位，豐富的圖表
資源庫，可穿插文字與附件

SIEM 與 SOC 差別？

SIEM

Security Information and Event Management

別名

譯名：安全資訊與事件管理

比較 ▸ SOAR：Security Orchestration, Automation, and Response

定義

一種資安**解決方案/產品**，用來集中各種資安產品所蒐集到的Log，進而整合事件告警、關聯分析、產出數據報表，甚至是採取自動化腳本回應等，以輔助資安人員更有效率地建立整體環境可視性並即時排除問題。

SOC

Security Operation Center

別名

譯名：資安監控中心、資訊安全作業維運中心、資安中心

定義

在組織中，將所有資訊系統的安全性事件集中監控管理的**團隊**，通常會有一個資安戰情室，由資安人員5X8或24X7偵測、回應威脅。現有「服務產品化」的趨勢，有些人容易將SOC和SIEM的功能混稱。

市場



在台灣市場，有一些常見的 SIEM 品牌和解決方案供應商。以下是其中一些較知名的品牌：

1. **IBM QRadar**：IBM QRadar 是一個集成的安全情報與事件管理解決方案，提供實時事件監控、安全事件分析和合規性報告等功能。
2. **Splunk Enterprise Security**：Splunk Enterprise Security 是一個基於日誌分析和大數據技術的 SIEM 平台，提供實時威脅檢測、事件分析和威脅情報集成等功能。
3. **McAfee Enterprise Security Manager**：McAfee Enterprise Security Manager (ESM) 是一個綜合的安全事件和日誌管理解決方案，用於監測、分析和回應安全事件。
4. **Fortinet FortiSIEM**：Fortinet FortiSIEM 提供實時的事件監測和分析，並結合了入侵檢測和預防系統 (IDPS) 功能，用於威脅檢測和響應。
5. **LogRhythm**：LogRhythm 是一個綜合的 SIEM 平台，結合了日誌管理、事件監測、威脅情報和合規性管理等功能，用於實時安全監控和威脅檢測。



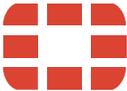
FortiSIEM



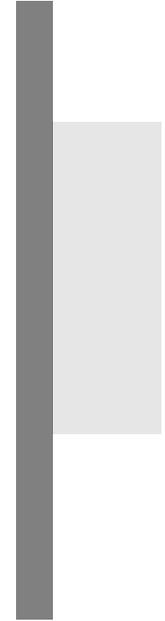
Microsoft Sentinel

Ar

IB

F**RTINET**®

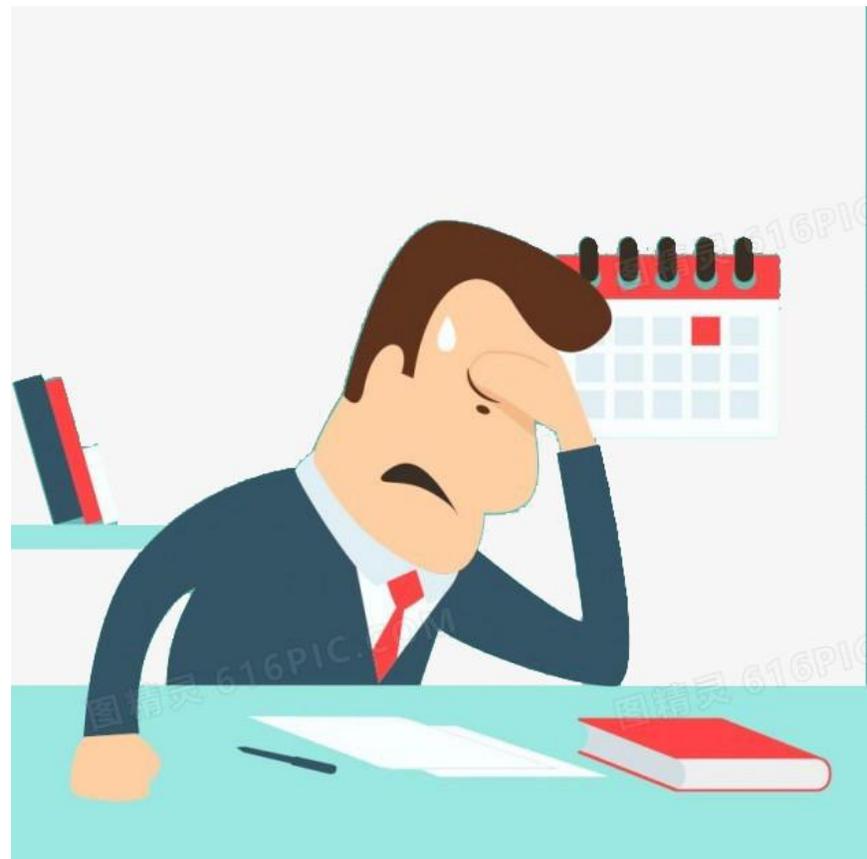
Configuration Manager



Configuration Manager

客戶需求期望

- 客戶需求:
 - 希望有方案可以幫忙做到稽核設備的設定檔。
 - 異動紀錄、差異比對、更動告警。
- 稽核設備：
 - Palo Alto、Fortinet、F5、Cisco Switch.



Configuration Manager

FortiSIEM 如何做到 – 異動紀錄

The screenshot displays the FortiSIEM Configuration Manager interface. The top navigation bar includes Dashboard, Analytics, Incidents, Cases, CMDB, Resources, Tasks, and Admin. The main dashboard shows counts for various device types: Routers (0), Firewalls (2), Windows (0), Unix (0), ESX (0), AWS (0), and Azure (0). The breadcrumb path is CMDB > Devices > Network Device > Firewall. The left sidebar lists device categories, with Firewall selected. The main content area shows a table of firewall configurations with columns for Name, IP, Device Type, Status, Discovered, Method, Parser Name, and Agent. Two entries are listed, both with a status of Pending. Below the table, the Configuration tab is active, showing a table of configuration revisions. A red box highlights the configuration history table, which includes columns for Revision, Date, and Type/File Name. The configuration details for the selected revision (Rev #1) are displayed on the right, showing a list of configuration commands.

CMDB > Devices > Network Device > Firewall

Name	IP	Device Type	Status	Discovered	Method	Parser Name	Agent
FGVM02TM21008567	10.1.225.202	Fortinet FortiOS	Pending	Mar 28 2022, 09:13:45 PM	SSH, SNMP, PING		
FGVM02TM21008571	10.1.225.201	Fortinet FortiOS	Pending	Mar 28 2022, 09:13:45 PM	SSH, SNMP, PING		

Summary Properties Monitor Software Hardware Configuration Relationships File Auto expand

Rev	Date	Type/File Name
2	Mar 28 2022, 09:35:27 PM	startup-config
1	Mar 28 2022, 09:14:00 PM	startup-config

Rev #1 - Mar 28, 2022 9:14 PM - startup-config

```
discoverTime 1648473225
#config-version=FGVM64-7.0.5-FW-build0304-220208:opmode=1:vdom=0:user=fortisiem
#buildno=0304
#global_vdom=1
config system global
set admin-concurrent enable
set admin-console-timeout 0
set admin-forticloud-sso-login disable
set admin-hsts-max-age 15552000
```

Configuration Manager

FortiSIEM 如何做到 – 異動紀錄

The screenshot displays the FortiSIEM Configuration Manager interface. At the top, a navigation bar includes links for DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, TASKS, and ADMIN. Below this, a summary row shows counts for various device types: Routers (4), Firewalls (11), Windows (0), Unix (3), ESX (0), AWS (0), and Azure (0).

The main content area is titled "CMDB > Devices > Network Device > Load Balancer". It features a table with columns for Name, IP, Device Type, Status, Method, Organization, Agent Policy, and Agent Status. Two entries are listed:

Name	IP	Device Type	Status	Method	Organization	Agent Policy	Agent Status
TPEC-S08-Trade-A-LTM.yuanta.com	10.216.6.151	F5 Big-IPOS	Pending	LOG	Super		
tsb-fortisiem.com	10.1.200.158	F5 Big-IPOS	Pending	SSH, SNMP, PING	Super		

Below the table, a "Configuration" tab is selected, showing a table of configuration revisions. A red box highlights the first revision:

Rev	Date	Type/F
1	Apr 22 2022, 03:03:53 PM	custom

To the right of the revision table, the configuration details for "Rev #1 - Apr 22, 2022 3:03 PM - custom-config" are displayed as a JSON object:

```
discoverTime 1650611021
y
auth password-policy {}
auth remote-role {}
auth remote-user {}
auth source {}
auth user admin {
description "Admin User"
encrypted-password
$6$5b0PFekf$qA8O2qpDdvLQ1fw4cynQ/mw/ifyMbiKh9PL3zYHdBWbZCiWIH8uaAln3LVRn8T2GWTktl0Ha
```

At the bottom of the interface, a footer contains the copyright notice "Copyright © 2022 Fortinet, Inc. All rights reserved.", the user information "Organization: Super User: admin Scope: Global", and the version "FortiSIEM 6.4.1 (1415)".

Configuration Manager

FortiSIEM 如何做到 – 差異比對

Configuration Diff

30748	edit 7	30748	edit 7
30749	set status enable	30749	set status enable
30750	set name "	30750	set name "
30751	set uuid a006b000-ae75-51ec-bdc7-6bb9e439e9dd	30751	set uuid a006b000-ae75-51ec-bdc7-6bb9e439e9dd
30752	set srcintf "port2"	30752	set srcintf "port2"
30753	set dstintf "port1"	30753	set dstintf "port1"
30754	set action deny	30754	set action deny
30755	set ztna-status enable	30755	set ztna-status enable
30756	set srcaddr "all"	30756	set srcaddr "all"
30757	set dstaddr "all"	30757	set dstaddr "all"
30758	set ztna-ems-tag "FCTEMS0000113945_123"	30758	set ztna-ems-tag "FCTEMS0000113945_123"
30759	set internet-service disable	30759	set internet-service disable
30760	set internet-service-src disable	30760	set internet-service-src disable
30761	unset reputation-minimum	30761	unset reputation-minimum
30762	set rtp-nat disable	30762	set rtp-nat disable
30763	set schedule "always"	30763	set schedule "always"
30764	set schedule-timeout disable	30764	set schedule-timeout disable
30765	set service "ALL_ICMP"	30765	set service "ALL_ICMP" "ALL_UDP"
30766	set tos-mask 0x00	30766	set tos-mask 0x00
30767	set anti-replay enable	30767	set anti-replay enable

Top

Bottom

Previous

Next

Close

Configuration Manager

FortiSIEM 如何做到 – 更動告警

The screenshot displays the FortiSIEM Configuration Manager interface. At the top, there is a navigation bar with tabs for DASHBOARD, ANALYTICS, INCIDENTS, CASES, CMDB, RESOURCES, TASKS, and ADMIN. Below this, a left sidebar shows a mailbox view with folders like '收件匣', 'Google', and '已加上旗標'. The main content area is divided into three columns: a list of incidents, a detailed view of a selected incident, and a reporting device summary.

Incident List:

- sunphone2103@gmail.com 下午10:27
fortigate config change firewall policy
詳細資料: Source IP: 10.1.225.14 User: jarvis [firewallpolicychange] <190>date=2022-03-28 time=22:26:12 d...
- sunphone2103@gmail.com 下午10:27**
fortigate config change firewall policy
詳細資料: Source IP: 10.1.225.14 User: jarvis [firewallpolicychange] <190>date=2022-03-28 time=22:26:09 d...
- STUDIO M' 台灣 下午9:04
用剛烤好的麵包喚醒一日朝氣 – 早晨餐桌的麵包盤精選 | STUDIO...
早晨餐桌的麵包盤精選 用剛烤好的麵包喚醒一日朝氣 每日早上能為...

Selected Incident Details:

sunphone2103@gmail.com 下午10:27
fortigate config change firewall policy
收件人: 李尚峰、副本: 李尚峰

詳細資料:
Source IP: 10.1.225.14
User: jarvis
[firewallpolicychange]
<190>date=2022-03-28 time=22:26:09 devname="FGVM02TM21008567" devid="FGVM02TM21008567" eventtime=1648477569568686247 tz="+0800" logid="0100044547" type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configured" user="jarvis" ui="GUI(10.1.225.14)" action="Edit" cfgtid=8781980 cfgpath="firewall.policy" cfgobj="3" cfgattr="service[ALL->ALL_ICMP ALL_TCP ALL_UDP HTTP HTTPS]" msg="Edit firewall.policy 3"

Reporting Device Summary:

Reporting Device: FGVM02TM21008567

☆ sunphone2103@gmail.com 下午10:27
fortigate config change firewall policy
收件人: 李尚峰、副本: 李尚峰

詳細資料:
Source IP: 10.1.225.14
User: jarvis
[firewallpolicychange]
<190>date=2022-03-28 time=22:26:12 devname="FGVM02TM21008567" devid="FGVM02TM21008567" eventtime=1648477572874856803 tz="+0800" logid="0100044545" type="event" subtype="system" level="information" vd="root" logdesc="Object configured" user="jarvis" ui="GUI(10.1.225.14)" action="Delete" cfgtid=8781981 cfgpath="firewall.policy" cfgobj="4" msg="Delete firewall.policy 4"

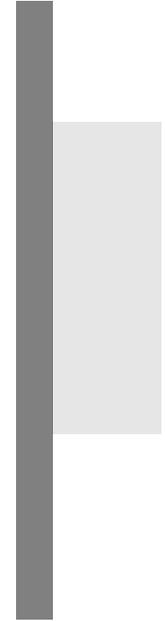
Detects that the configuration of a network device (router or firewall) has changed. This is achieved via logging in and keeping track of the last change

Defense Evasion

Disable or Modify System Firewall (T1562.004)

System

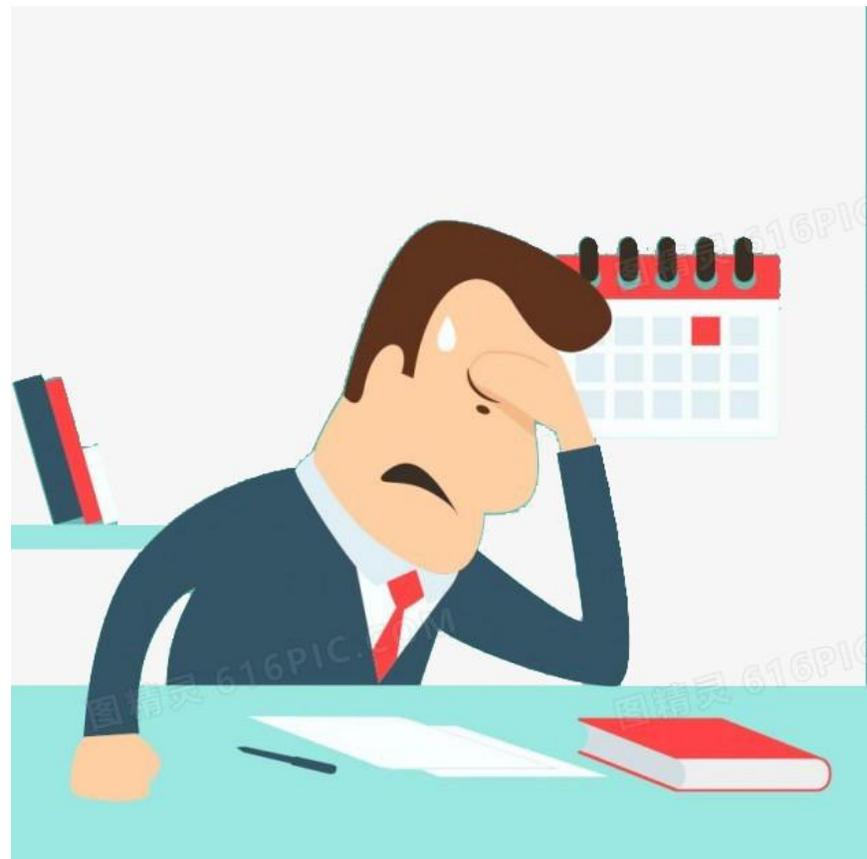
FortiSIEM Rule



FortiSIEM Rule

情境說明

- 客戶內部有幾個帳號很常因為太多次登入失敗而被AD封鎖。
- 詢問使用者，使用者表示那段時間沒在使用.....
- 想找到來源IP封鎖解決此問題。



FortiSIEM Rule

Win-Security-4740

- 使用者被AD封鎖Windows會產生4740這筆資訊。
- 4740的內容包含：只會有使用者帳號，不會有來源IP。
- 所以管理者無法知道是透過哪個IP來連線。

FortiSIEM Rule

Win-Security-4625

- 使用者登入失敗Windows會產生4625這筆資訊。
- 4625的內容包含：使用者帳號 / 來源IP。

FortiSIEM Rule

關聯性

- 透過FortiSIEM Rule 關聯性，將4625 以及 4740作相關的對應。
- 舉例：五分鐘內 登入失敗五次 就會被AD封鎖。
- 我們可以在FortiSIEM上定義一個Rule，當五分鐘內發生五次4625之後(相同帳號)。後續出現的4740只要與前面五次的4625帳號相同就跳出告警。並且顯示出4625的來源IP以及4740的使用者帳號。
- 這樣管理者就可以收到告警 **誰** 透過 **什麼IP**，登入失敗太多次**被AD封鎖**。

FortiSIEM Rule

關聯性

Add New Rule

Step 1: General >

Step 2: Define Condition >

Step 3: Define Action

Condition: If this Pattern occurs within any second time window

Generate Incident for: Windows Account Lock SourceIP



Incident Attributes:

Event Attribute		Subpattern		Filter Attribute	Row	
<input type="text" value="Source IP"/>	=	<input type="text" value="4625"/>	▼	<input type="text" value="Source IP"/>	<input type="button" value="⊕"/>	<input type="button" value="⊖"/>
<input type="text" value="User"/>	=	<input type="text" value="4740"/>	▼	<input type="text" value="User"/>	<input type="button" value="⊕"/>	<input type="button" value="⊖"/>

Save

Cancel