FORTINET

SIEM與EDR的威脅防護戰略

Teddy 莊永杰

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
新聞
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，而駭客不只要求支付天價贖金，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/ 周峻佑 | 2021-03-20 發表
Happy Blog
Acer Inc.
acer
aruba
atmosphere21
掌握網路、安全、智慧監控與自動化的創新技術
立即報名
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。
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
新聞
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/ 林妍潼 | 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
iThome Security
臺廠物聯智慧再成焦點，今年6月CISA才警告該公司的SDK存在CVE-2021-32934漏洞，最近FireEye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**。

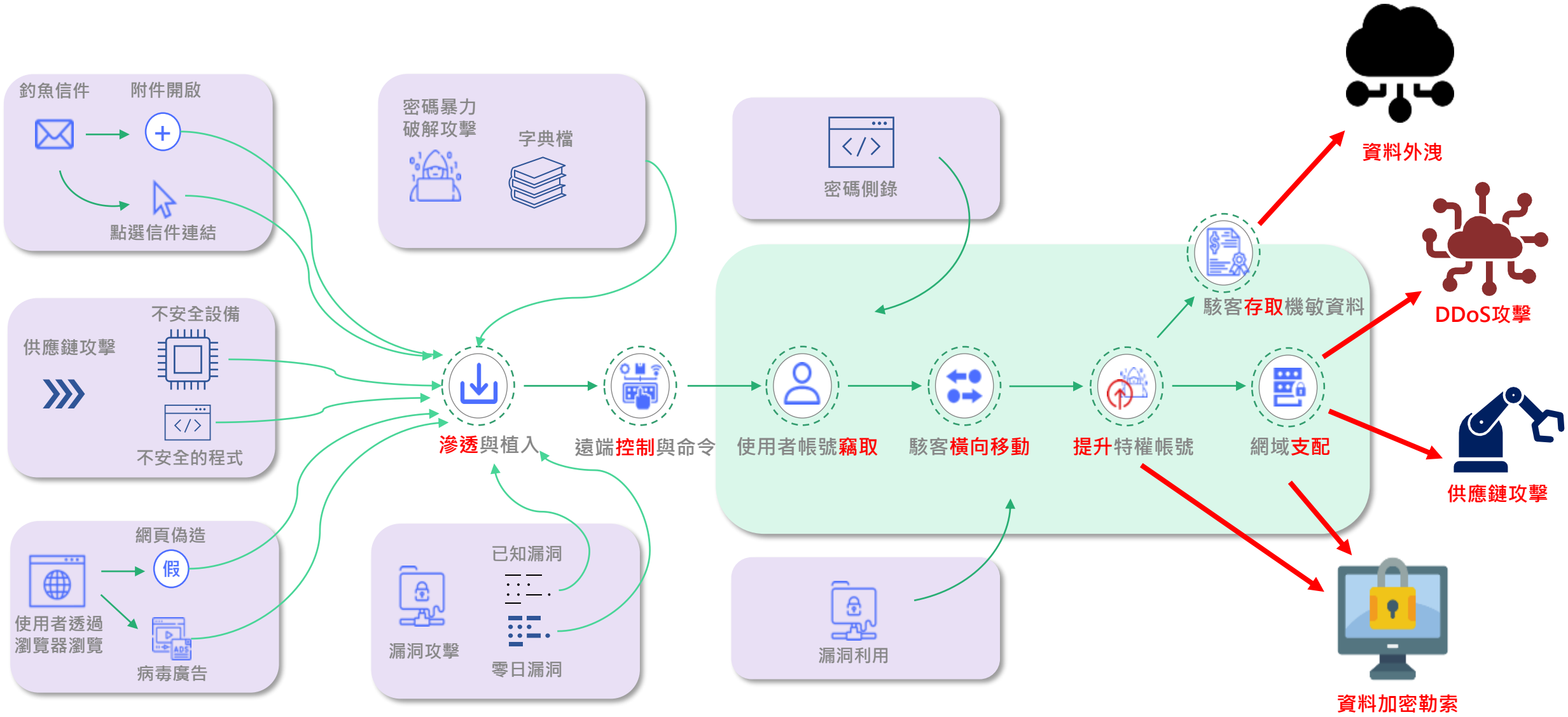
3.端點是內部網路的入口點：

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**。

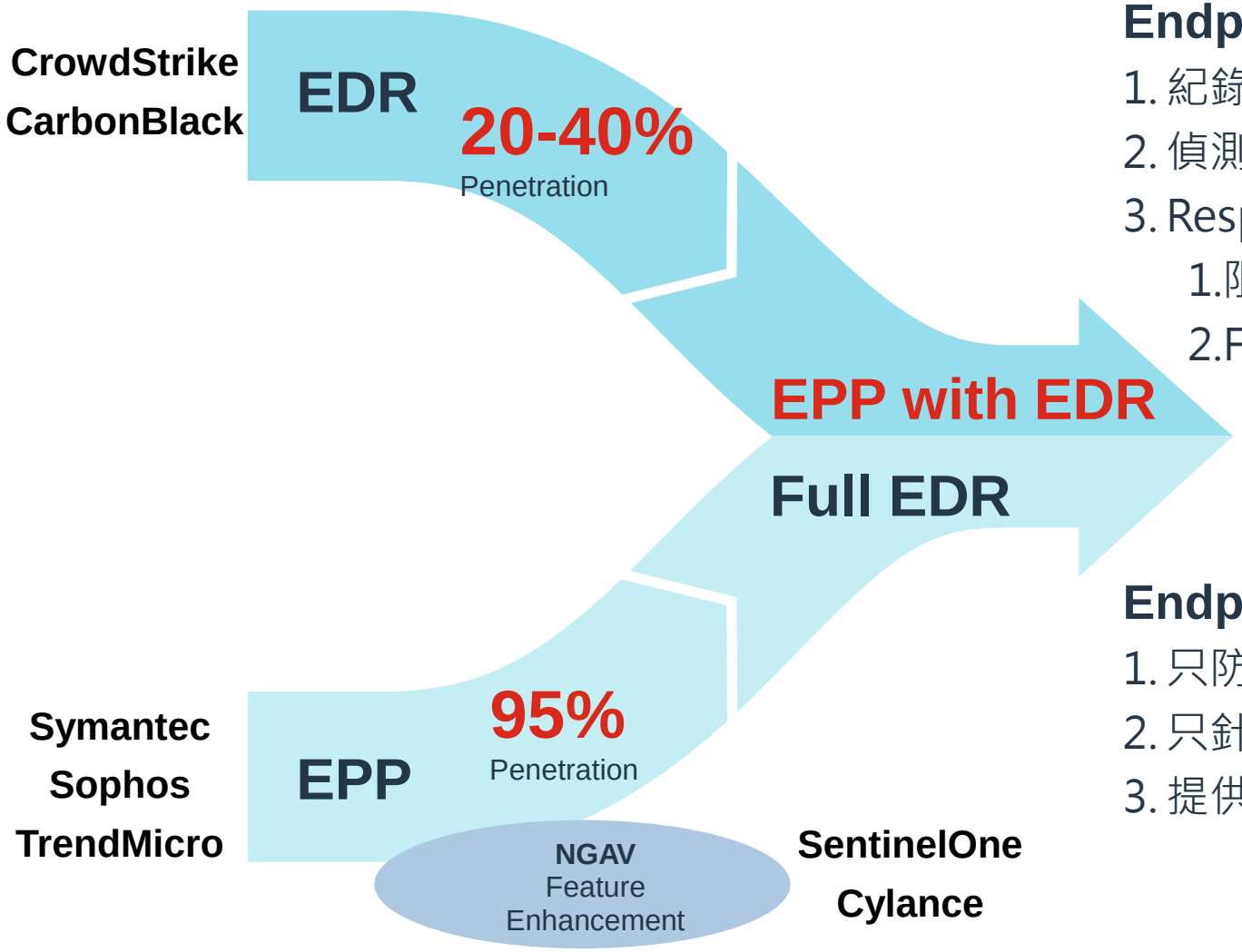
4.威脅環境不斷演變：

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



Endpoint Detection and Response (EDR)

1. 紀錄和儲存所有 endpoint 的行為
2. 偵測病毒事件
3. Response
    1.阻止病毒和修復
    2.Forensic—偵查資安事件，並找尋其源頭

Endpoint Protection Platform (EPP)

1. 只防範 file-based 病毒
2. 只針對不信任的應用程式偵測和阻攔惡意的行為
3. 提供偵查及修復病毒能力，並且通報和告警

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

- **事後保護 = EDR (偵測與回應)**

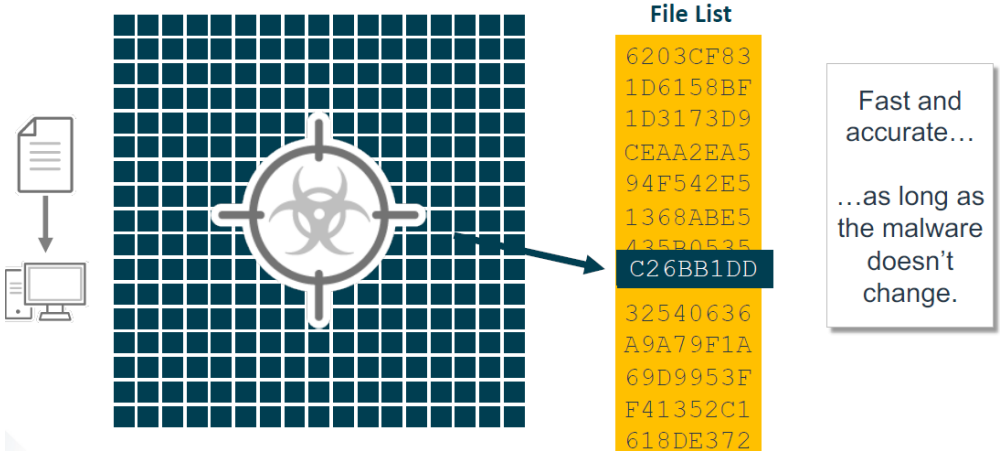
  記錄使用者的行為軌跡,偵測與回應異常行為

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

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

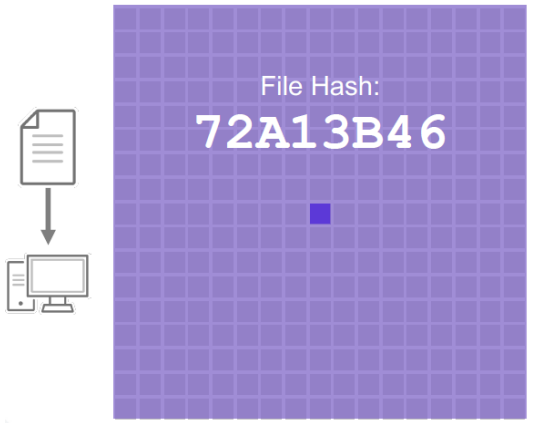
Early 90s: Signatures



Fast and accurate…

…as long as the malware doesn't change.

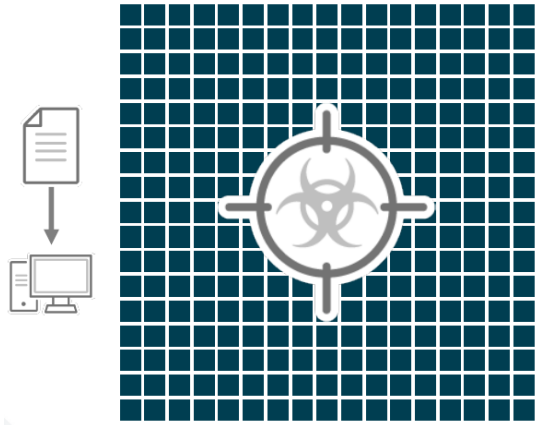
Late 90s: Signature Evasion

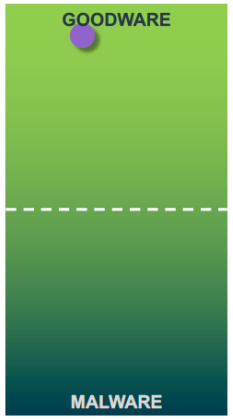


If just one byte changed, a file hash wouldn't match anymore

Simplified for clarity

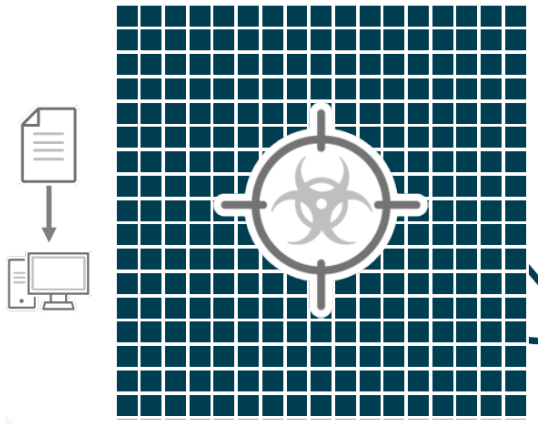
Last Decade: Rise of Machine Learning

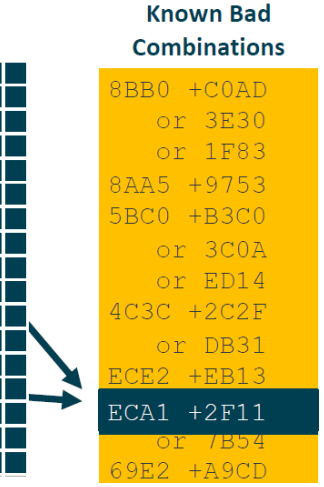




(Very) Simplified Machine Learning Model

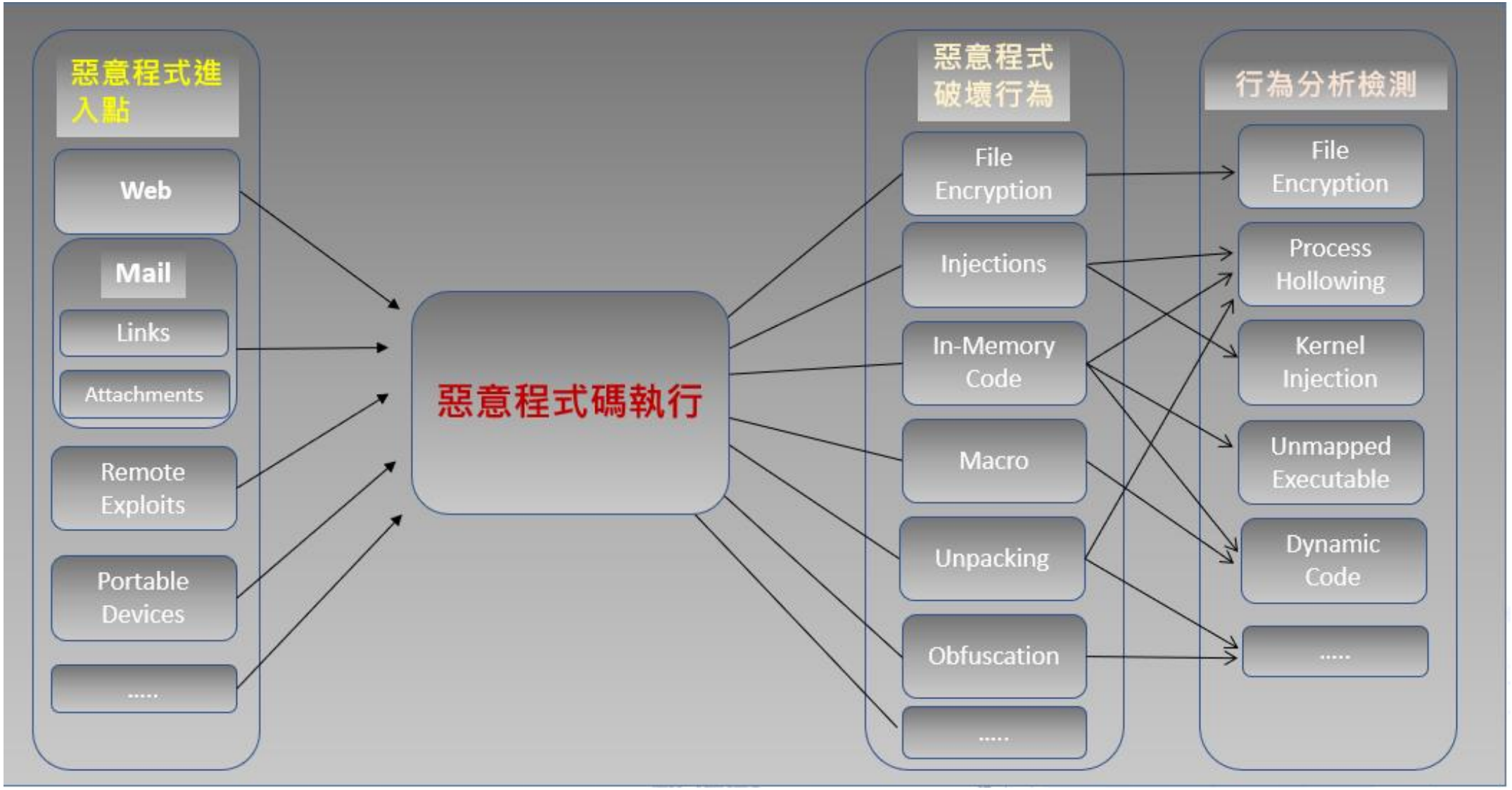
Variant Protection



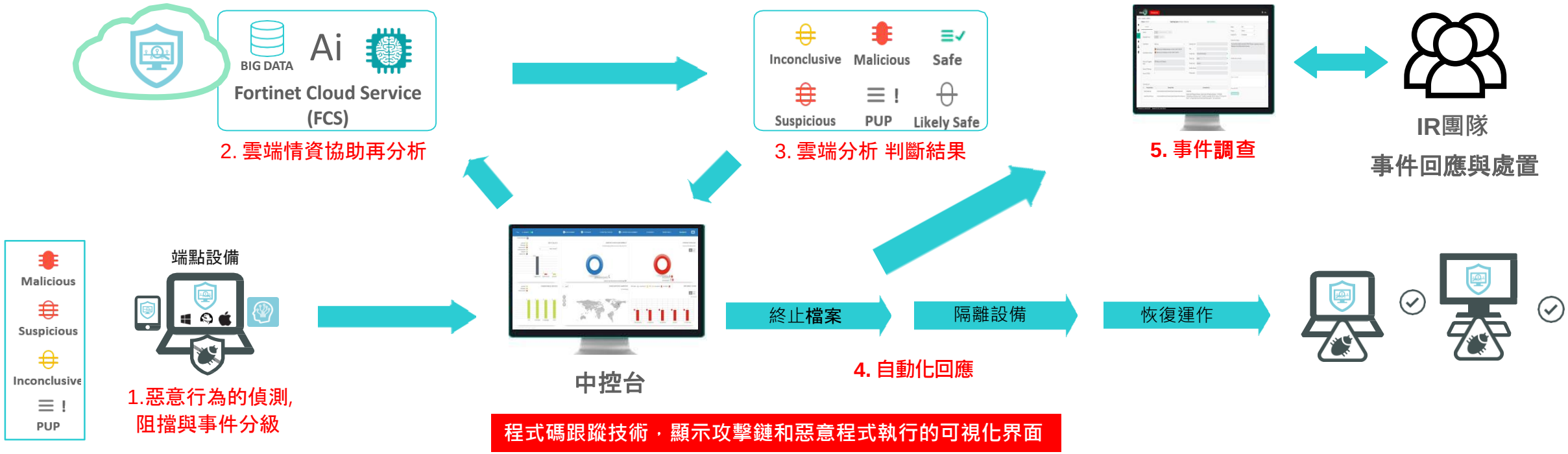


Variant Protection helps spot entire malware families

惡意行為偵測與阻斷

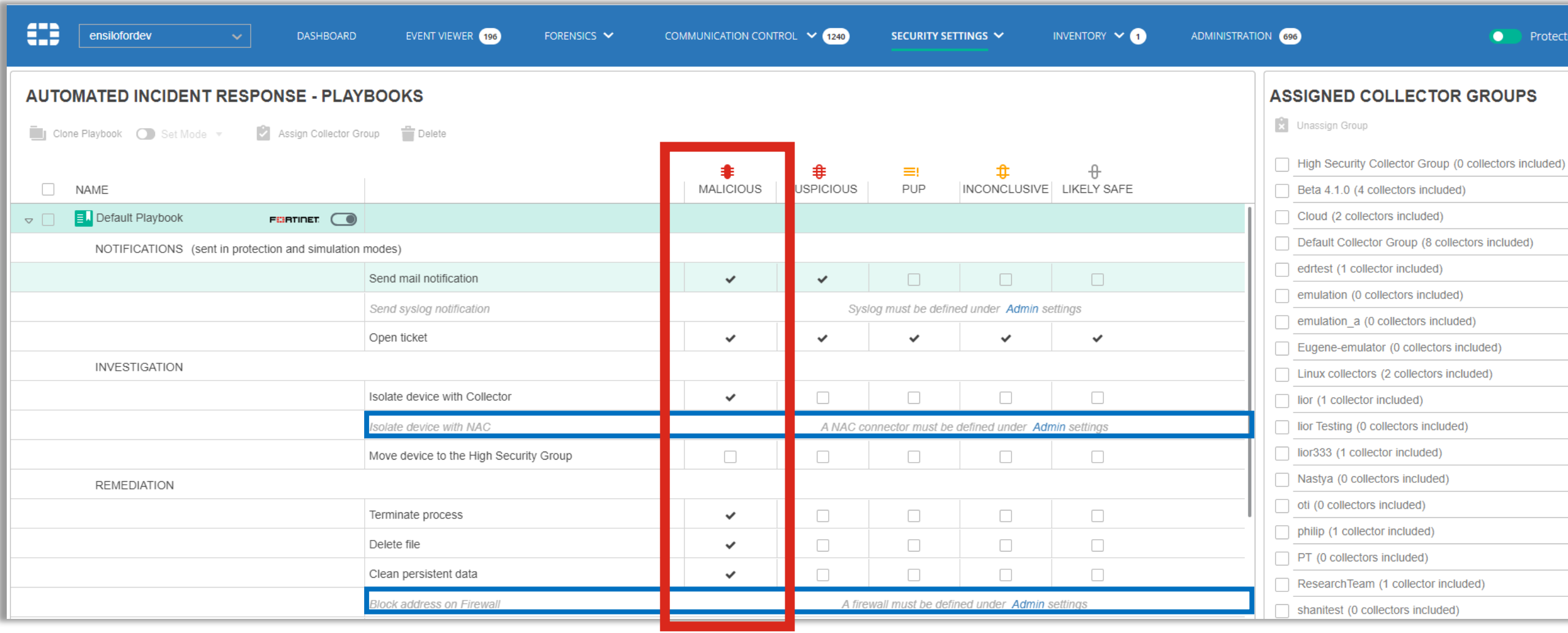

惡意程式進入點
Web
Mail
Links
Attachments
Remote Exploits
Portable Devices
.....
惡意程式碼執行
惡意程式破壞行為
File Encryption
Injections
In-Memory Code
Macro
Unpacking
Obfuscation
.....
行為分析檢測
File Encryption
Process Hollowing
Kernel Injection
Unmapped Executable
Dynamic Code
.....

端點資安事件觸發流程與分析

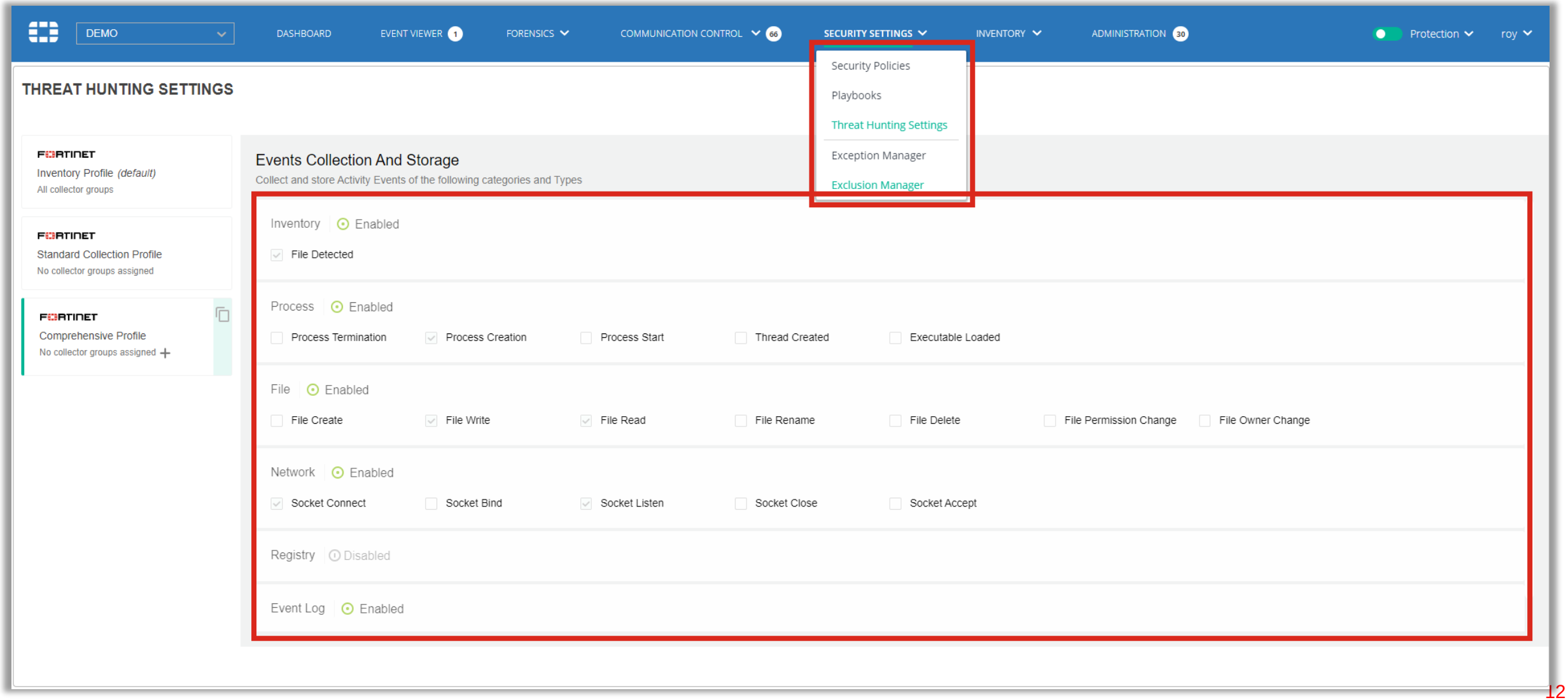


程式碼跟蹤技術，顯示攻擊鏈和惡意程式執行的可視化界面

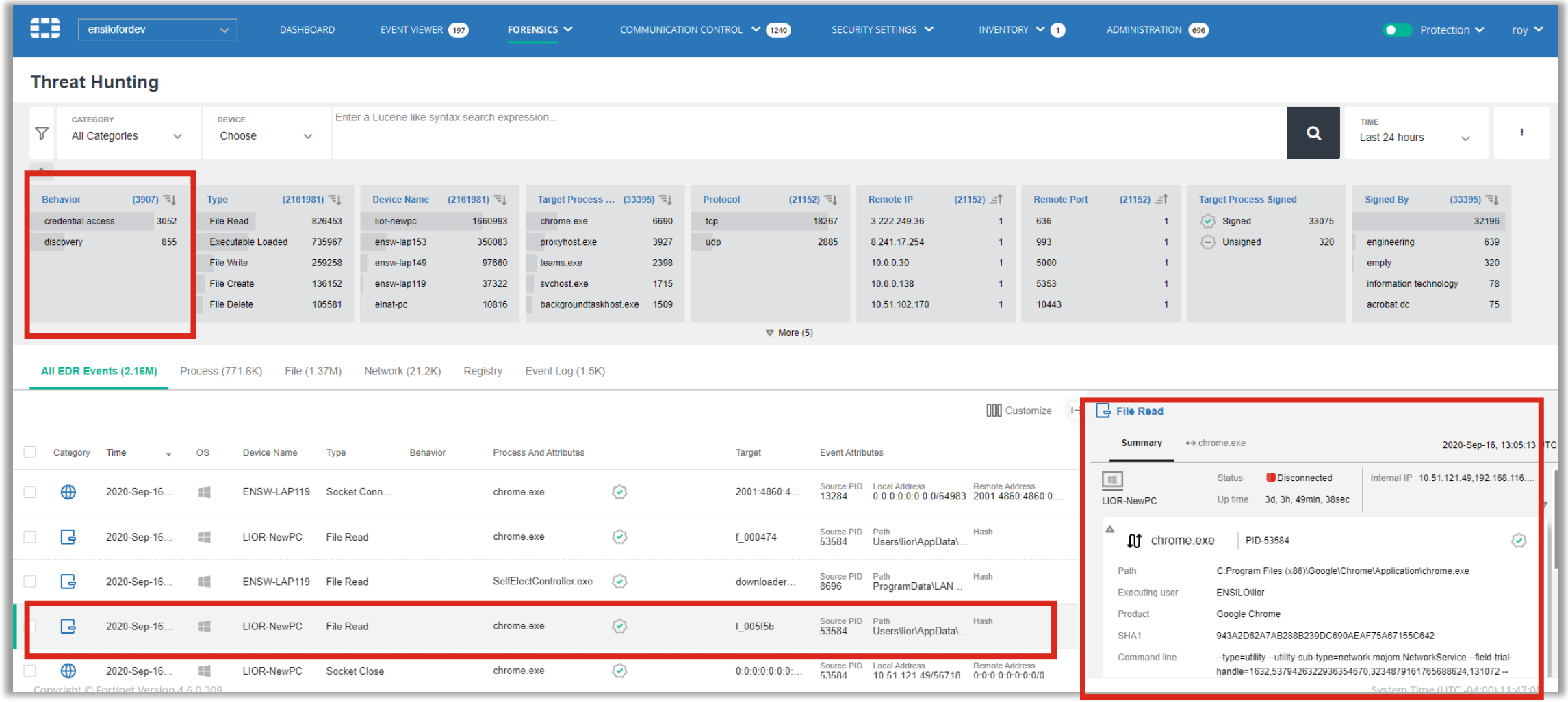
資安事件觸發後的處置


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
USPICIOUS
PUP
INCONCLUSIVE
LIKELY SAFE
Default Playbook
FORTINET
NOTIFICATIONS (sent in protection and simulation modes)
Send mail notification
Send syslog notification
Syslog must be defined under Admin settings
Open ticket
INVESTIGATION
Isolate device with Collector
Isolate device with NAC
A NAC connector must be defined under Admin settings
Move device to the High Security Group
REMEDIATION
Terminate process
Delete file
Clean persistent data
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



主動式威脅捕獵 — 快速搜尋與定位關鍵記錄



安全聯防提升整體防禦能力

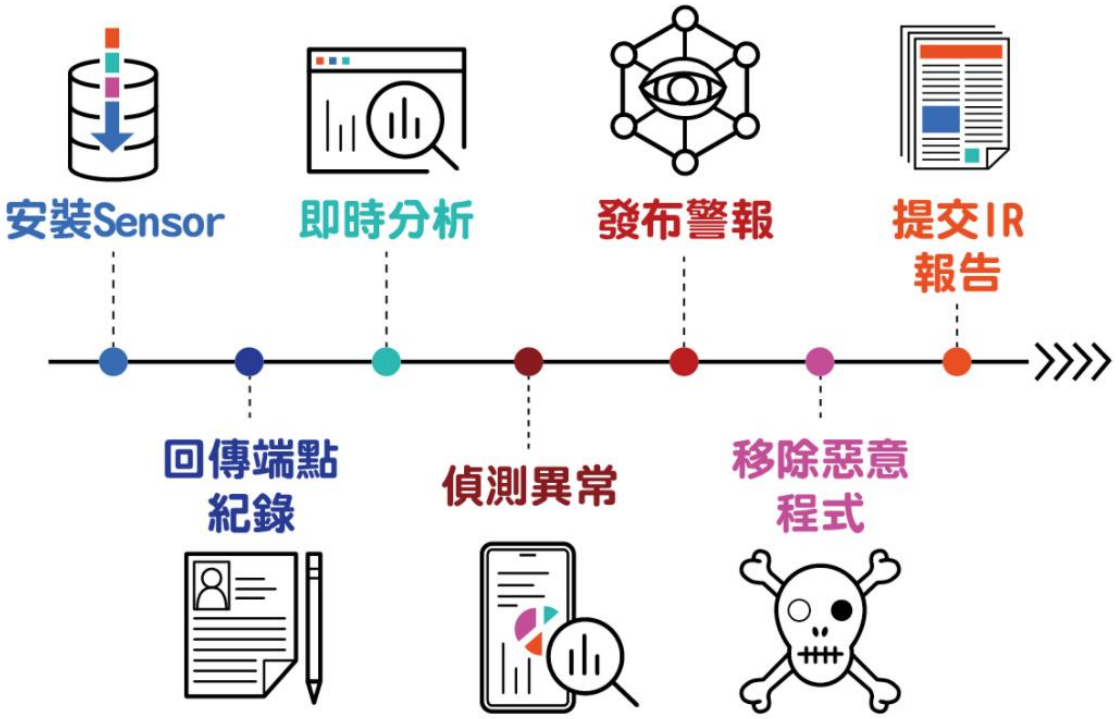
設定要進行自動聯防的Playbook

資安事件觸發聯防動作

在FortiGate上加入惡意IP進行阻擋

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

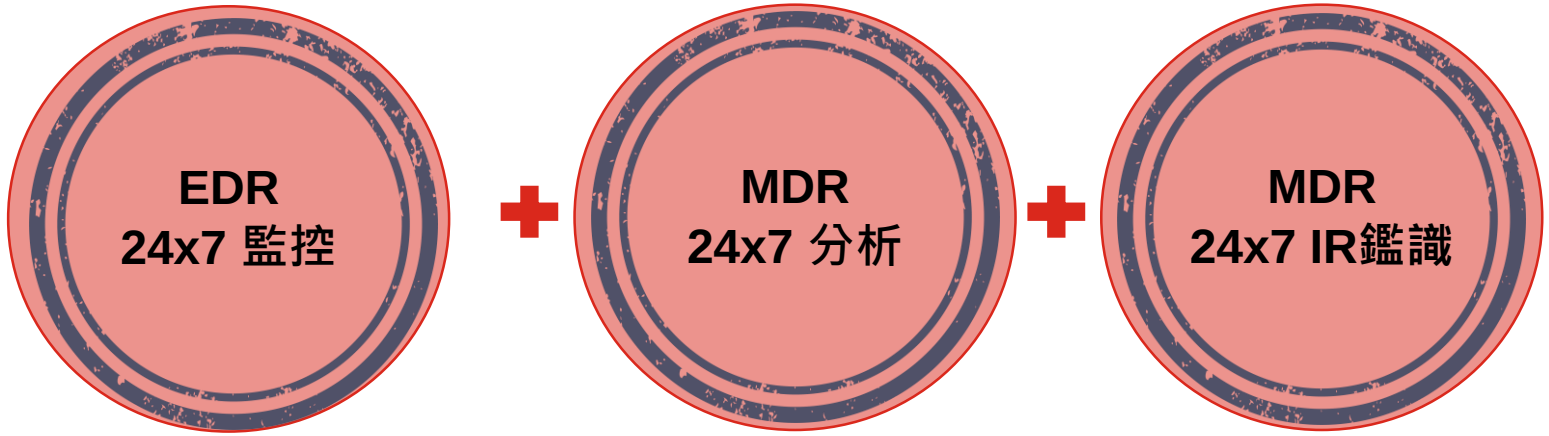


各種端點防護功能差異

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	

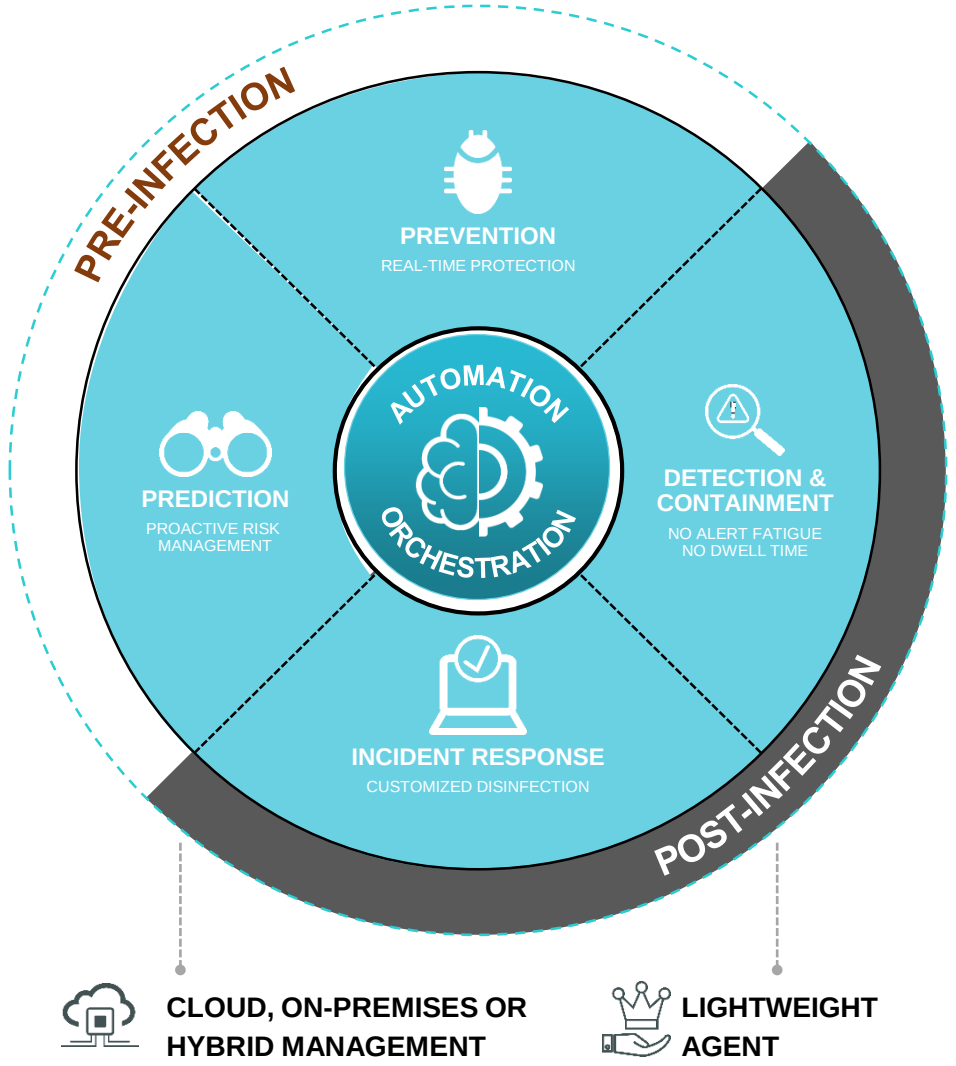
為何需要 MDR？

- 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傳統排程式掃瞄）？
- ✓ 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

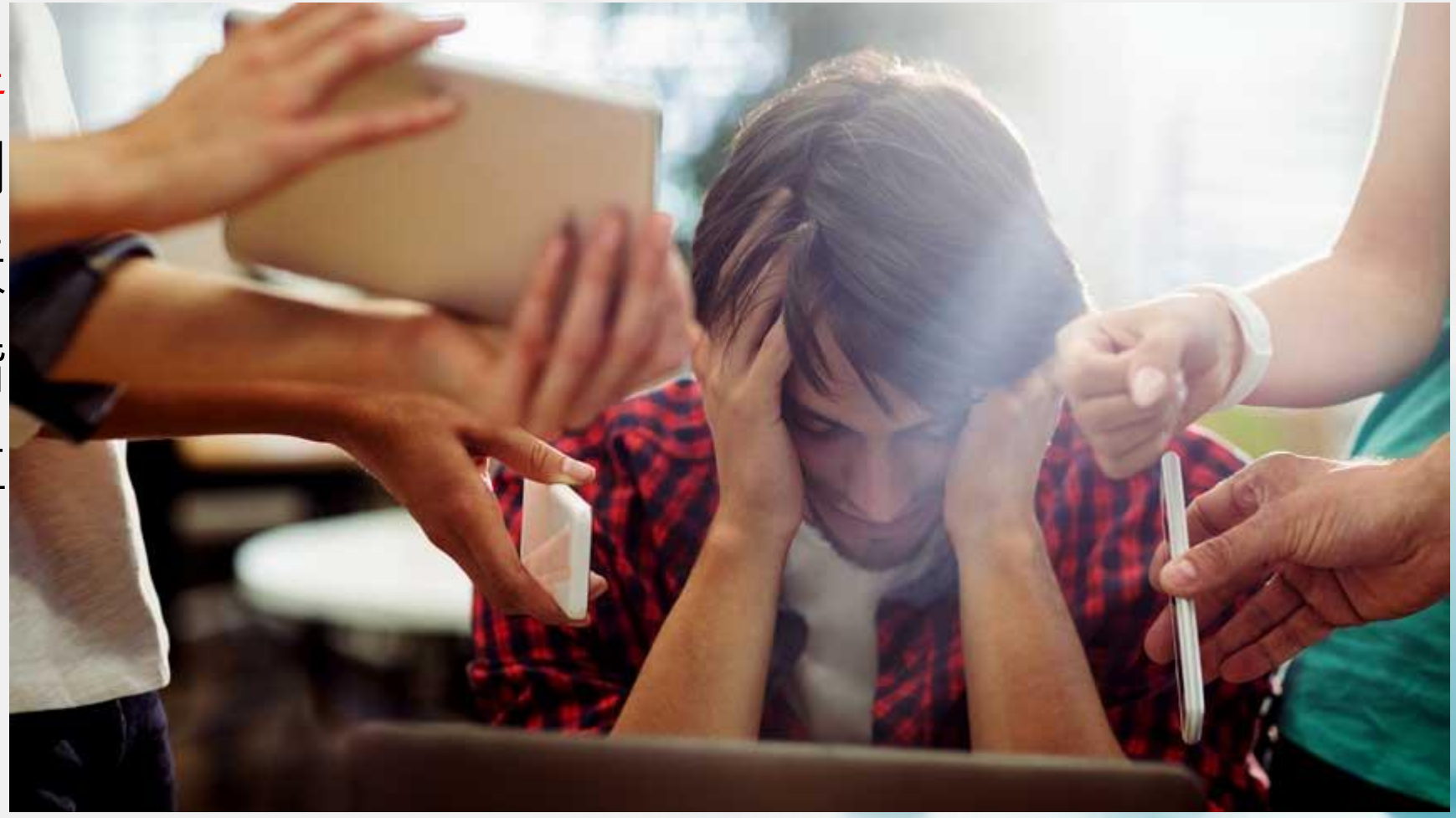
定義

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、事件追踪、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

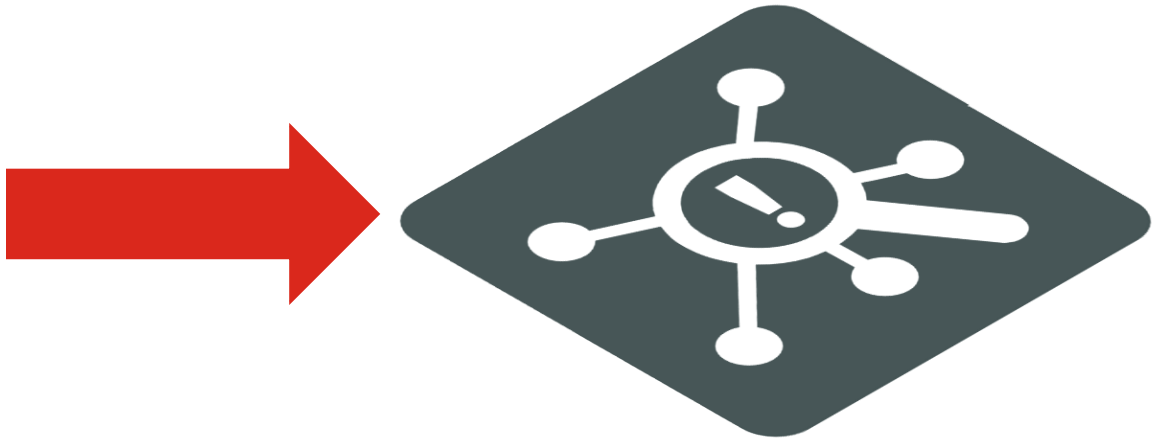
Email System

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

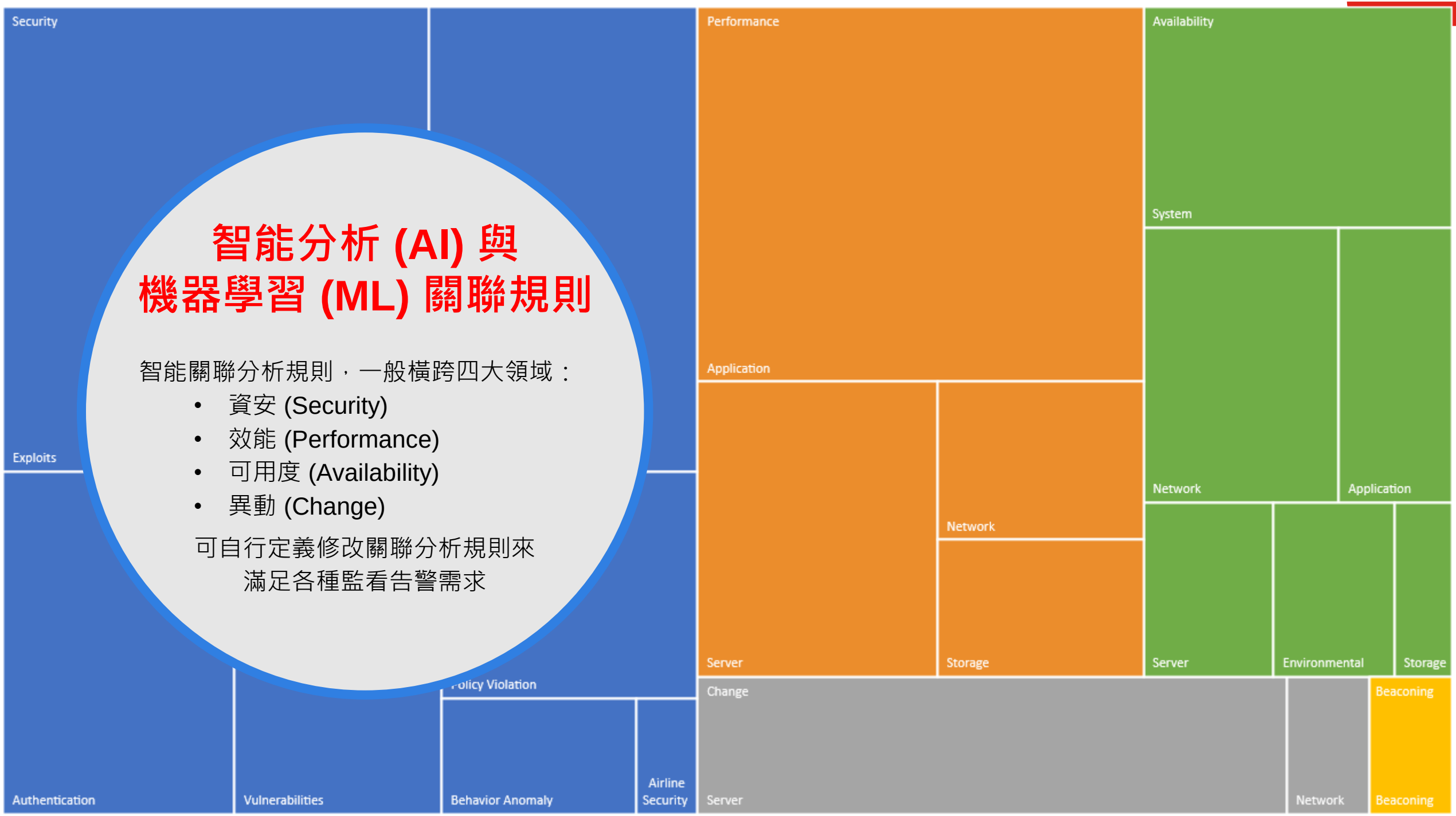
“Teddy”，“183”，“76”，“20.2”，“單身”，“靦腆害羞”

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

二、分析

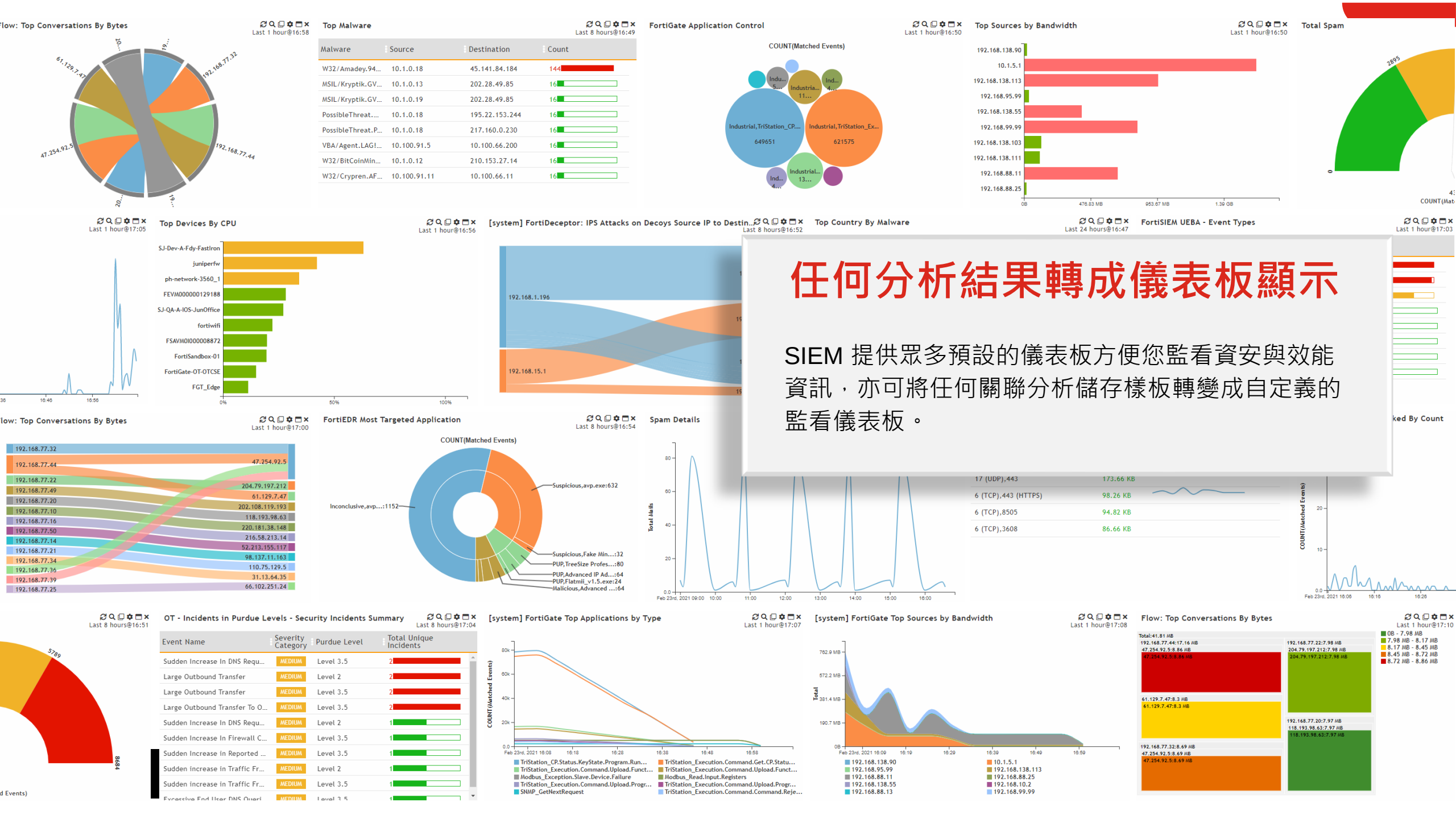


智能分析 (AI) 與 機器學習 (ML) 關聯規則

智能關聯分析規則，一般橫跨四大領域：

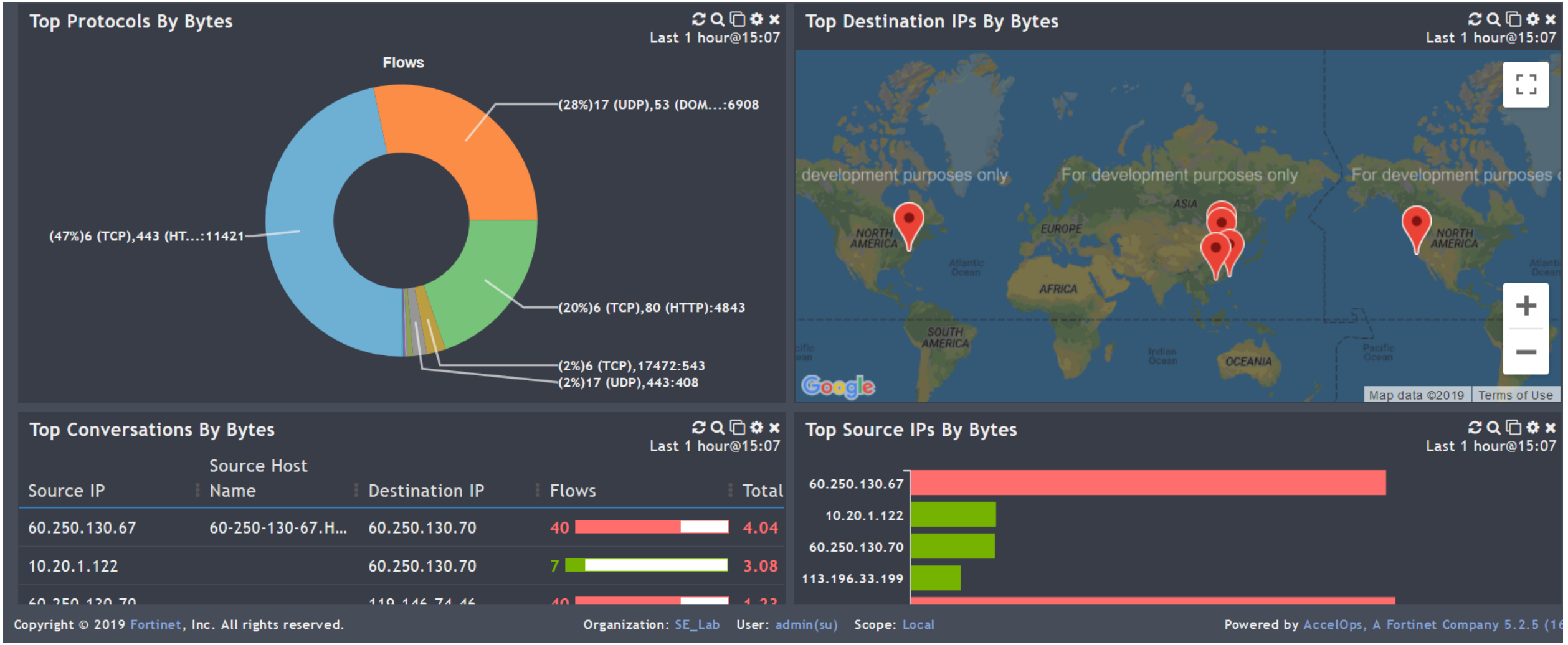
- 資安 (Security)
- 效能 (Performance)
- 可用度 (Availability)
- 異動 (Change)

可自行定義修改關聯分析規則來
滿足各種監看告警需求


Flow: Top Conversations By Bytes
Last 1 hour@16:58
Top Malware
Last 8 hours@16:49
Malware
Source
Destination
Count
W32/Amadey.94...
10.1.0.18
45.141.84.184
144
MSIL/Kryptik.GV...
10.1.0.13
202.28.49.85
16
MSIL/Kryptik.GV...
10.1.0.19
202.28.49.85
16
PossibleThreat....
10.1.0.18
195.22.153.244
16
PossibleThreat.P...
10.1.0.18
217.160.0.230
16
VBA/Agent.LAG!...
10.100.91.5
10.100.66.200
16
W32/BitCoinMin...
10.1.0.12
210.153.27.14
16
W32/Crypren.AF...
10.100.91.11
10.100.66.11
16
FortiGate Application Control
Last 1 hour@16:50
COUNT(Matched Events)
Industrial,TriStation_CP....
649651
Industrial,TriStation_Ex...
621575
Top Sources by Bandwidth
Last 1 hour@16:50
192.168.138.90
10.1.5.1
192.168.138.113
192.168.95.99
192.168.138.55
192.168.99.99
192.168.138.103
192.168.138.111
192.168.88.11
192.168.88.25
0B
476.83 MB
953.67 MB
1.39 GB
Total Spam
Last 1 hour@16:50
2895
0
Top Devices By CPU
Last 1 hour@16:56
SJ-Dev-A-Fdy-FastIron
juniperfw
ph-network-3560_1
FEVM000000129188
SJ-QA-A-IOS-JunOffice
fortiwifi
FSAVM0I000008872
FortiSandbox-01
FortiGate-OT-OTCSE
FGT_Edge
0%
50%
100%
[system] FortiDeceptor: IPS Attacks on Decoys Source IP to Destin...
Last 8 hours@16:52
192.168.1.196
192.168.15.1
Top Country By Malware
Last 24 hours@16:47
FortiSIEM UEBA - Event Types
Last 1 hour@17:03
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。
Flow: Top Conversations By Bytes
Last 1 hour@17:00
192.168.77.32
192.168.77.44
192.168.77.22
192.168.77.49
192.168.77.20
192.168.77.10
192.168.77.16
192.168.77.50
192.168.77.14
192.168.77.21
192.168.77.34
192.168.77.36
192.168.77.39
192.168.77.25
47.254.92.5
204.79.197.212
61.129.7.47
202.108.119.193
118.193.98.63
220.181.38.148
216.58.213.14
52.213.155.117
98.137.11.163
110.75.129.5
31.13.64.35
66.102.251.24
FortiEDR Most Targeted Application
Last 8 hours@16:54
COUNT(Matched Events)
Suspicious,avp.exe:632
Inconclusive,avp...:1152
Suspicious,Fake Min...:32
PUP,TreeSize Profes...:80
PUP,Advanced IP Ad...:64
PUP,Flatmii_v1.5.exe:24
Malicious,Advanced ...:64
Spam Details
Total Mails
17 (UDP),443
173.66 KB
6 (TCP),443 (HTTPS)
98.26 KB
6 (TCP),8505
94.82 KB
6 (TCP),3608
86.66 KB
COUNT(Matched Events)
Feb 23rd, 2021 16:06
OT - Incidents in Purdue Levels - Security Incidents Summary
Last 8 hours@17:04
Event Name
Severity Category
Purdue Level
Total Unique Incidents
Sudden Increase In DNS Requ...
MEDIUM
Level 3.5
Large Outbound Transfer
MEDIUM
Level 2
Large Outbound Transfer
MEDIUM
Level 3.5
Large Outbound Transfer To O...
MEDIUM
Level 3.5
Sudden Increase In DNS Requ...
MEDIUM
Level 2
Sudden Increase In Firewall C...
MEDIUM
Level 3.5
Sudden Increase in Reported ...
MEDIUM
Level 3.5
Sudden increase in Traffic Fr...
MEDIUM
Level 2
Sudden increase in Traffic Fr...
MEDIUM
Level 3.5
[system] FortiGate Top Applications by Type
Last 1 hour@17:07
COUNT(Matched Events)
TriStation_CP.Status.KeyState.Program.Run...
TriStation_Execution.Command.Upload.Funct...
Modbus_Exception.Slave.Device.Failure
TriStation_Execution.Command.Upload.Progr...
SNMP_GetNextRequest
TriStation_Execution.Command.Get.CP.Statu...
TriStation_Execution.Command.Upload.Funct...
Modbus_Read.Input.Registers
TriStation_Execution.Command.Upload.Progr...
TriStation_Execution.Command.Command.Reje...
[system] FortiGate Top Sources by Bandwidth
Last 1 hour@17:08
Total
192.168.138.90
192.168.95.99
192.168.88.11
192.168.138.55
192.168.88.13
10.1.5.1
192.168.138.113
192.168.88.25
192.168.10.2
192.168.99.99
Flow: Top Conversations By Bytes
Last 1 hour@17:10
0B - 7.98 MB
7.98 MB - 8.17 MB
8.17 MB - 8.45 MB
8.45 MB - 8.72 MB
8.72 MB - 8.86 MB

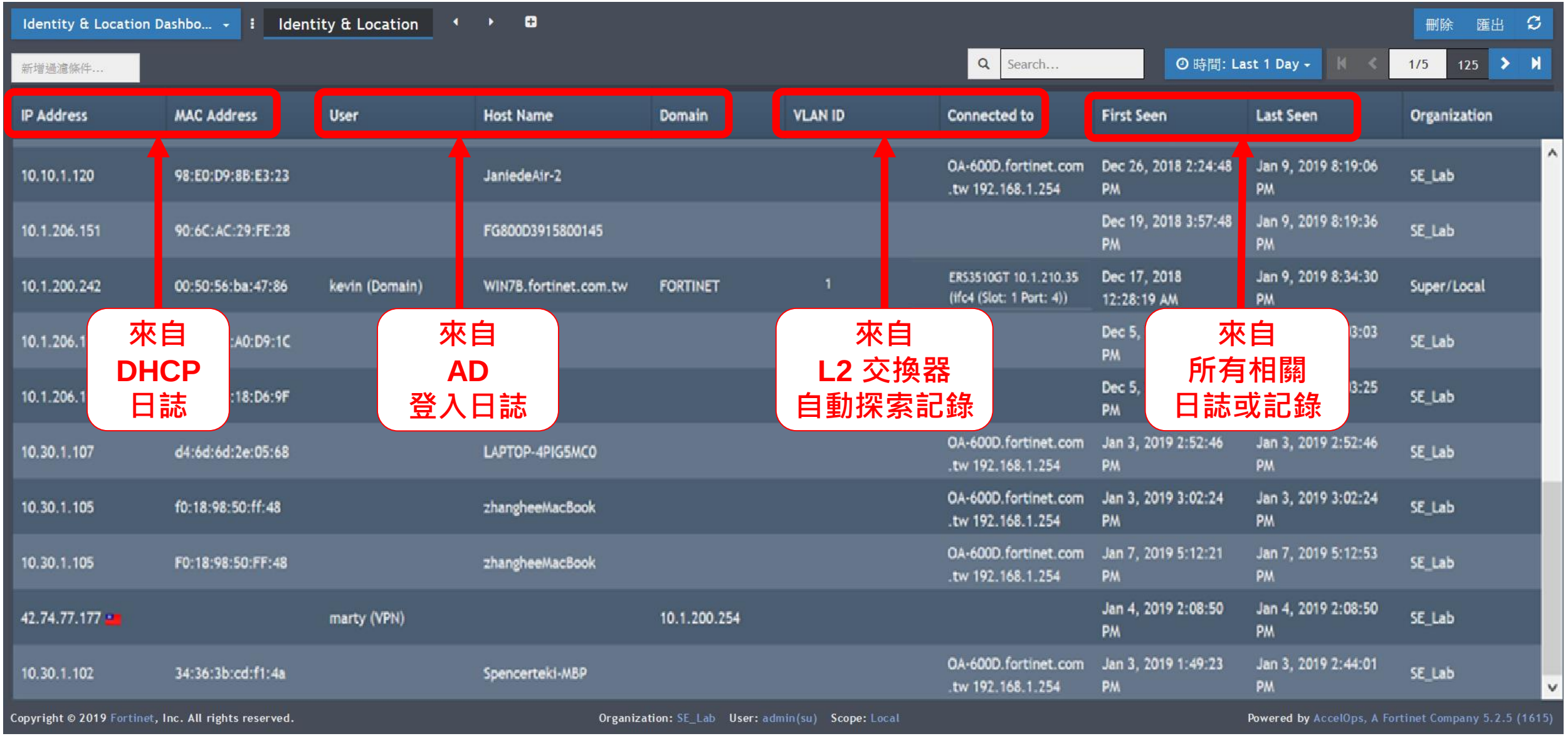
融合式分析第一步

- 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



智能分析 (AI) 異常行為

啟動	Name	Description	Exceptions	範圍
☑	(s) AI: File Creation Anomaly	FortiInsight AI module detects unusual file Creation by an user		System
☑	(s) AI: File Deletion Anomaly	FortiInsight AI module detects unusual file deletion by an user		System
☑	(s) AI: File Reading Anomaly	FortiInsight AI module detects unusual file reading by an user		System
☑	(s) AI: File Writing Anomaly	FortiInsight AI module detects unusual file writing by an user		System
☑	(s) AI: Process Started Anomaly	FortiInsight AI module detects unusual process started by an user		System
☑	(s) AI: Process Stopped Anomaly	FortiInsight AI module detects unusual process stoppage by an user		System
☑	(s) ARP Exploit	Detects ARP attack		System
☑	(s) AWS SecHub: Host Vulnerability Detected	AWS Security Hub detected host vulnerability		System
☑	(s) AWS SecHub: Software and Configuration Violation	AWS Security and Configuration Violation Detected		System
☑	(s) AWS SecHub: Tactics: Collection Detected	AWS Security Hub detected Collection tactics. Adversary is trying to collect data of their interest.		System
☑	(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
☑	(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
☑	(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
☑	(s) Sudden Increase In Firewall Connections	Detects sudden increase in permitted firewall conne window, the current firewall connections is more th away from the mean.		System
☑	(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
☑	(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
☑	(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
☑	(s) Sudden Increase in Server Process Count	Detects that a server is suddenly running 25% more processes than the average		System
☑	(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
☑	(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
☑	(s) Sudden Increase in User Login Volume	Detects daily user login volume anomaly against profile. This may indicate suspicious user behaviors.		System
☑	(s) Sudden Increase in WMI Response Times	Detects a sudden 50% increase of WMI Response window		System
☑	(s) Sudden User Location Change	Detects location change for a user unfeasible in the period of time. This may indicate a stolen credential.		System
☑	(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
☐	(s) Dynamically generated host name: malware likely	Detects algorithmically generated host name in network traffic - malware often use algorithmically generated host names to communicate.		tem
☑	(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 runnir host.		System
☑	(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
☑	(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

基於條件閥值智能分析

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

簡單建立標準化 SOC / NOC 日常維運流程

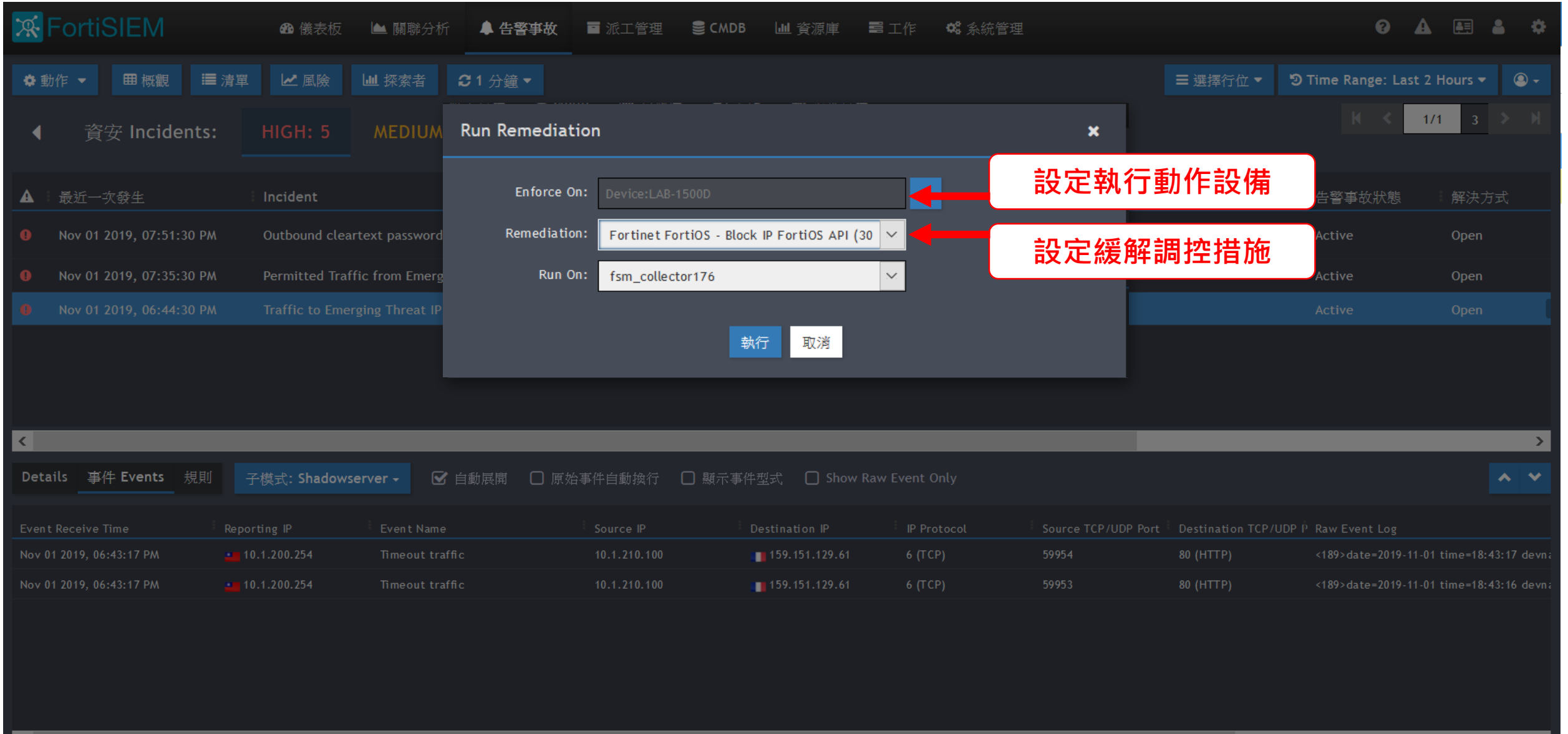
- 內建工單系統，告警事故即時反應並進行追蹤

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

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

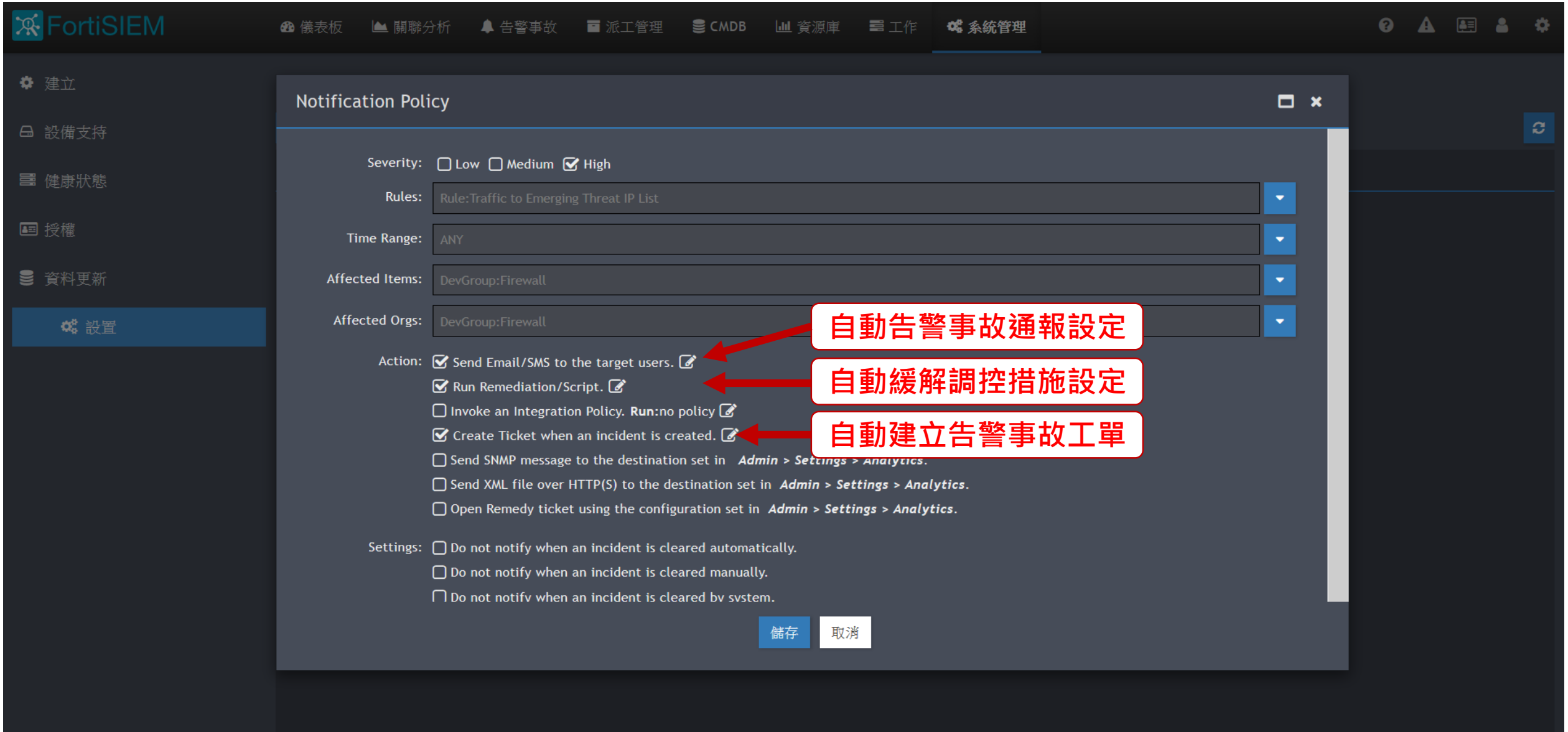


簡單建立標準化 SOC / NOC 日常維運流程

- 內建緩解調控措施腳本，可與多品牌設備協作聯防

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

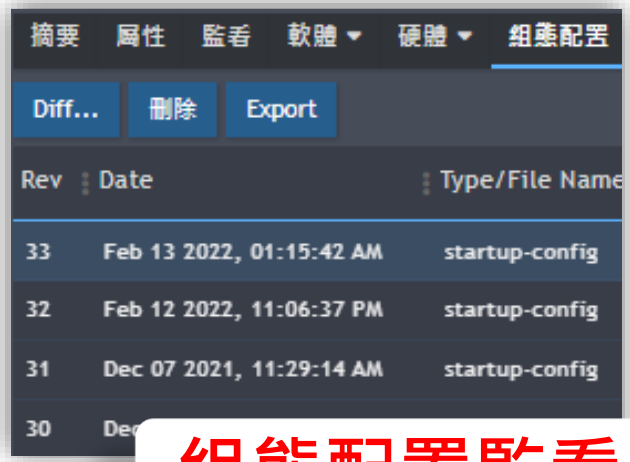


設備自動探索與組態管理資料庫

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



組態配置監看

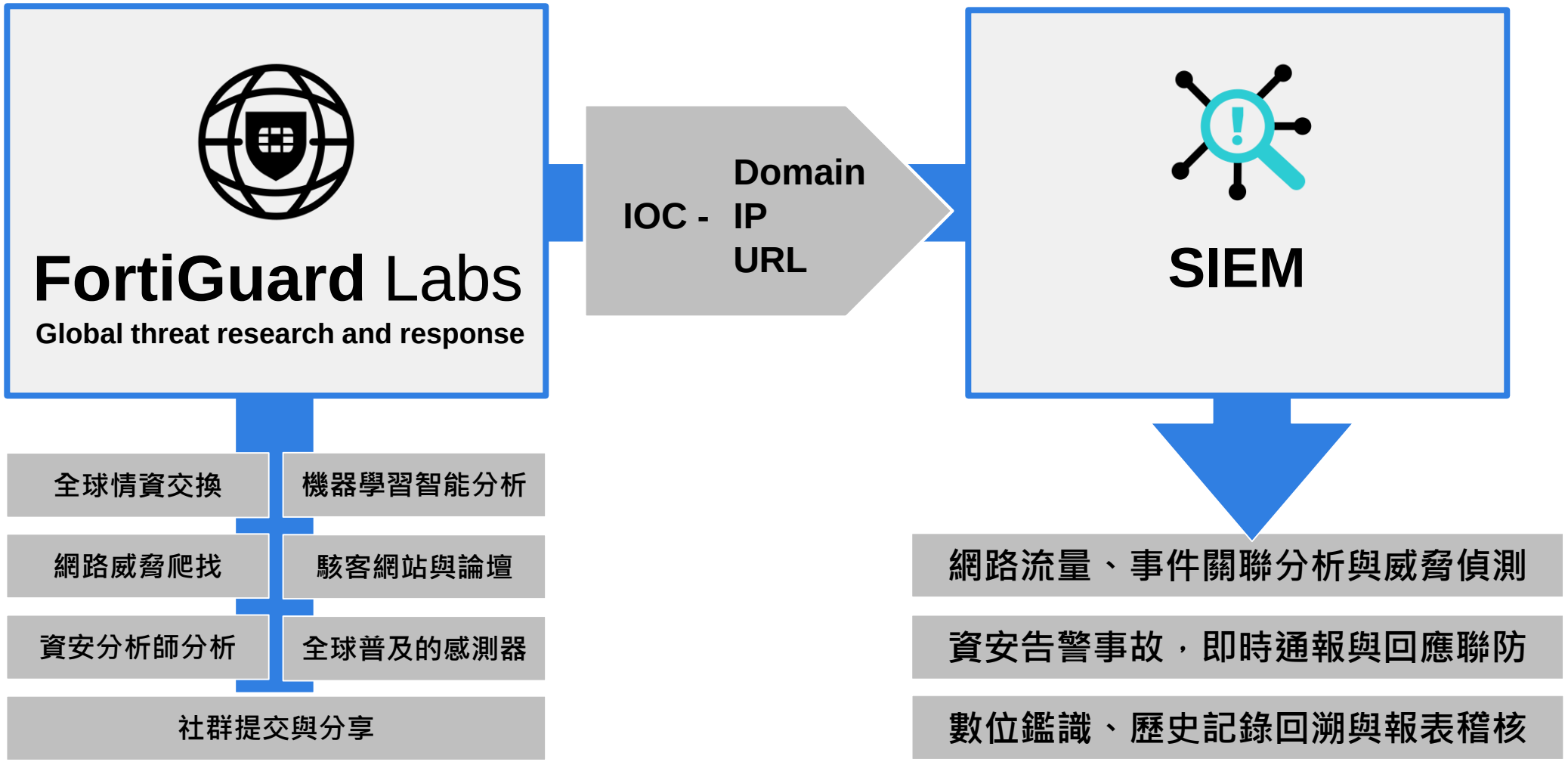
應用導向管理

威脅情資整合

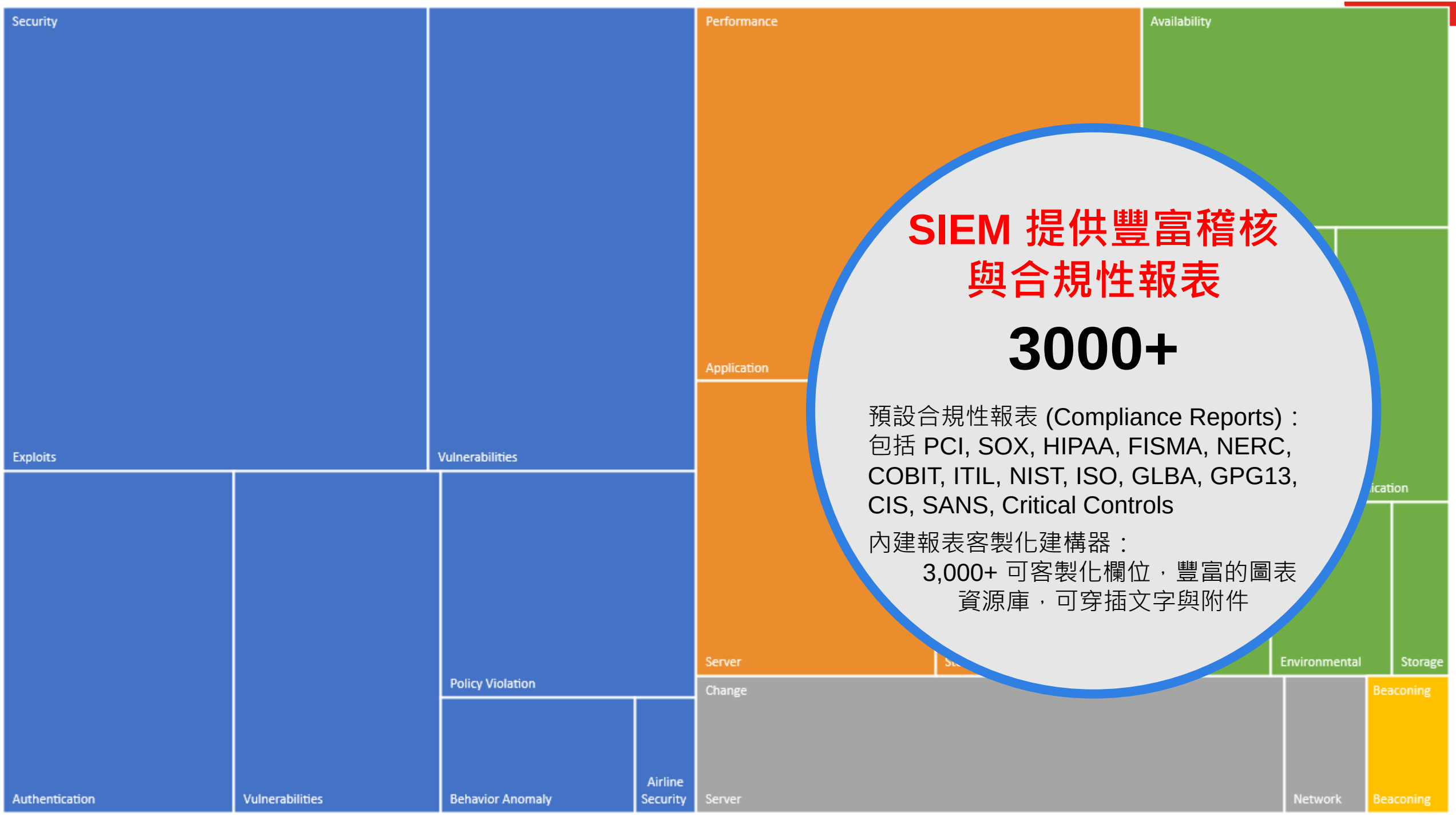
設備資產統整

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


Security
Exploits
Vulnerabilities
Authentication
Vulnerabilities
Policy Violation
Behavior Anomaly
Airline Security
Performance
Application
Server
Availability
Environmental
Storage
Change
Server
Network
Beaconing
Beaconing
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


FORTINET

Configuration Manager

Configuration Manager

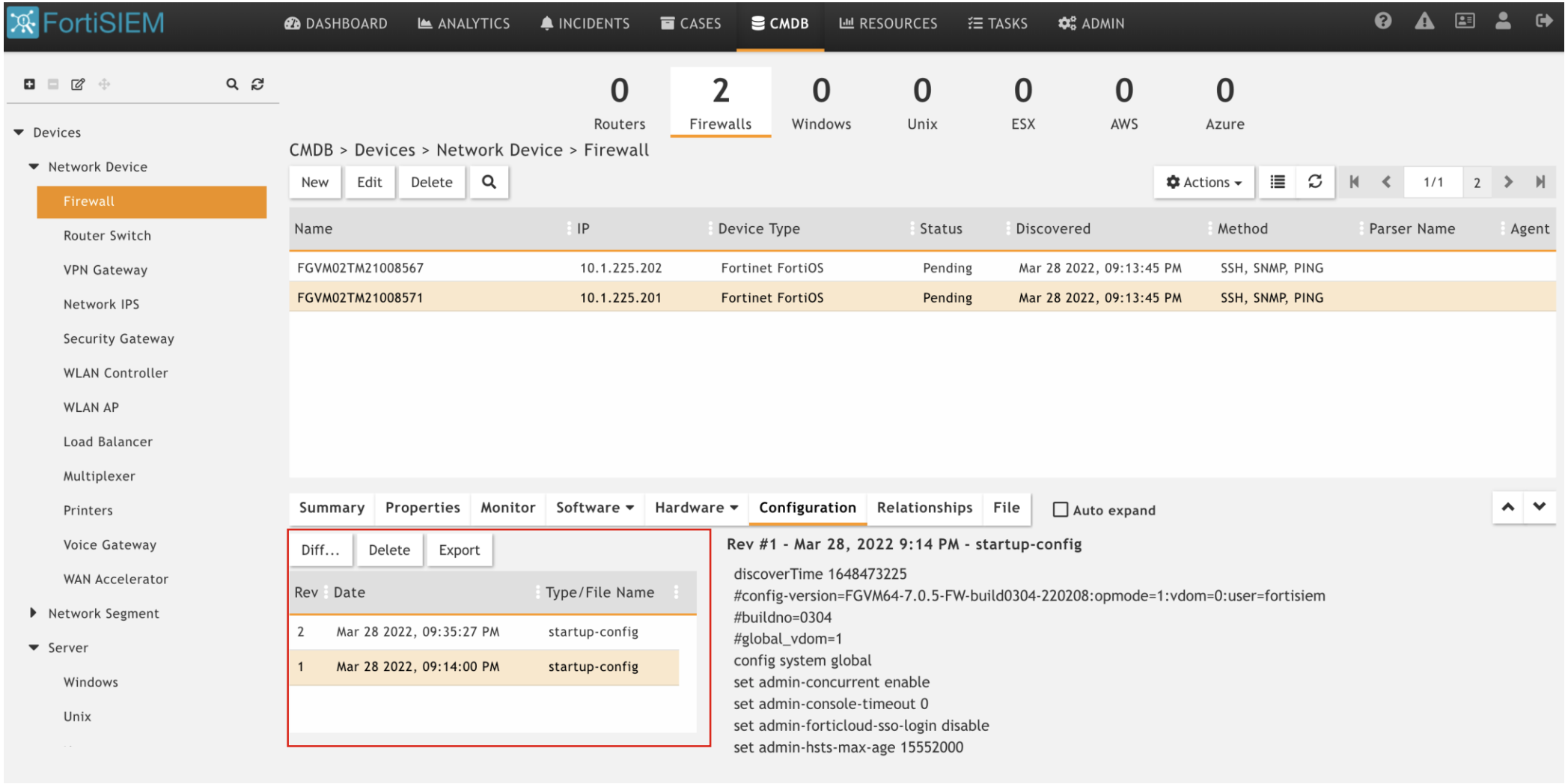
客戶需求期望

- 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.

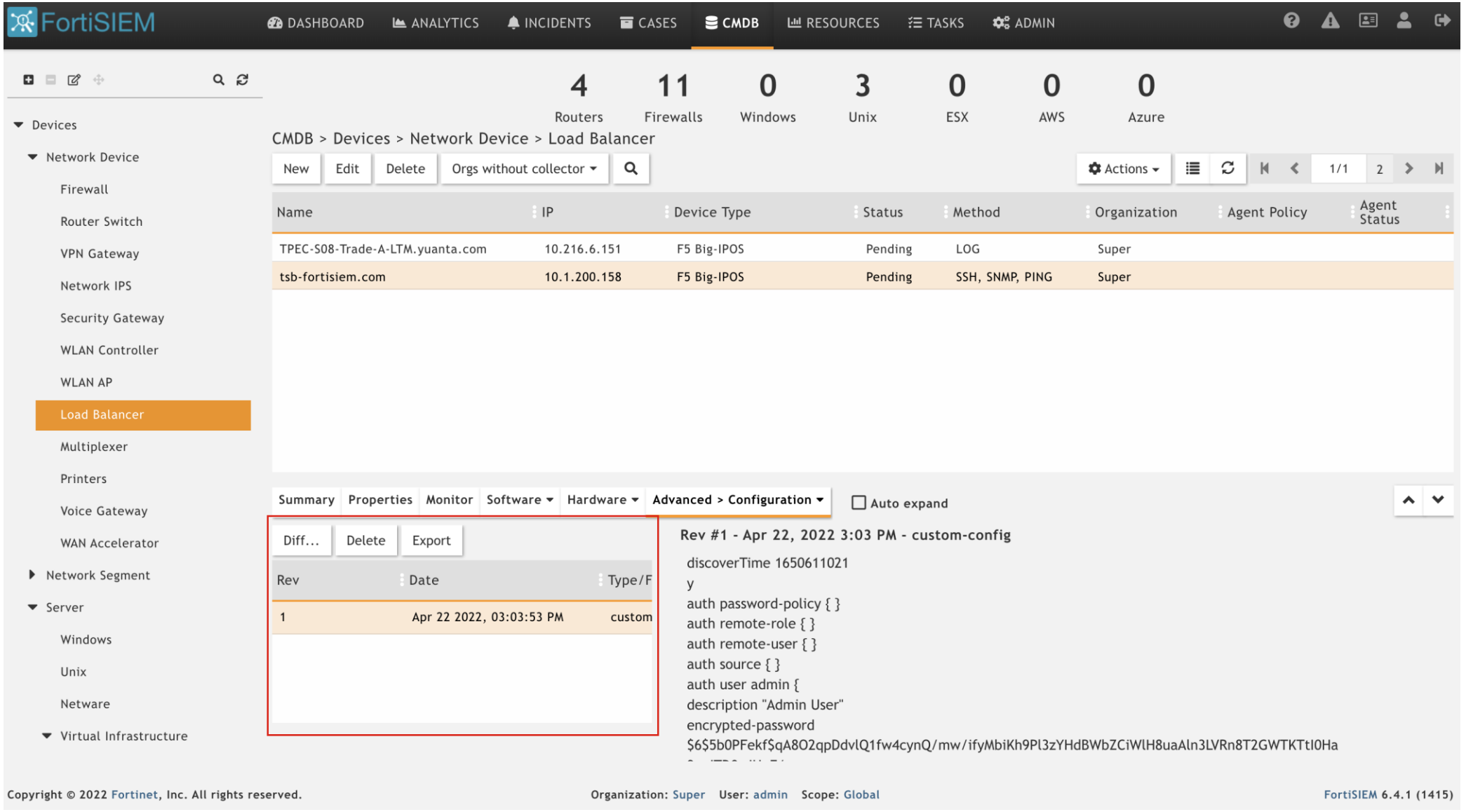
Configuration Manager

FortiSIEM 如何做到 – 異動紀錄



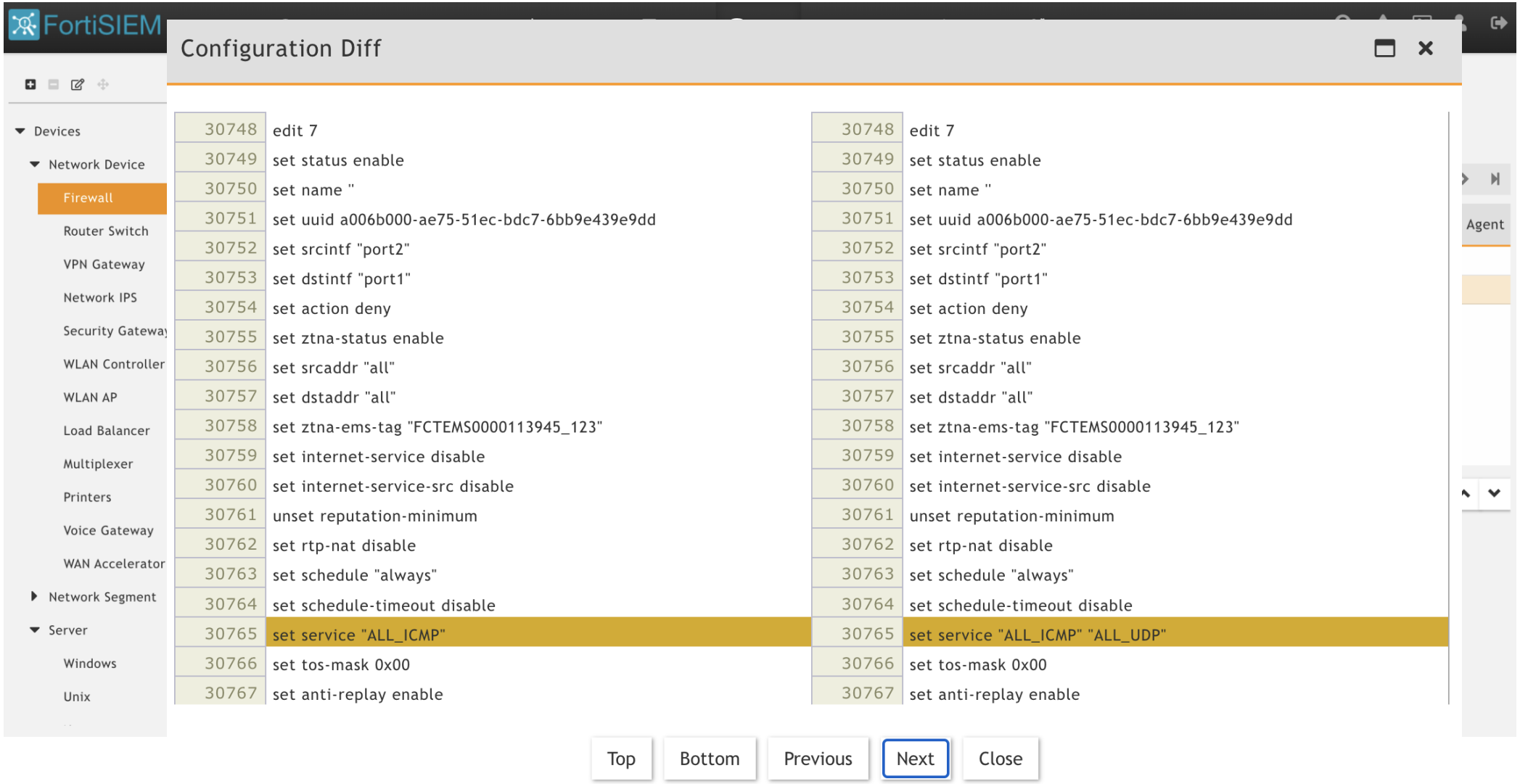
Configuration Manager

FortiSIEM 如何做到 – 異動紀錄



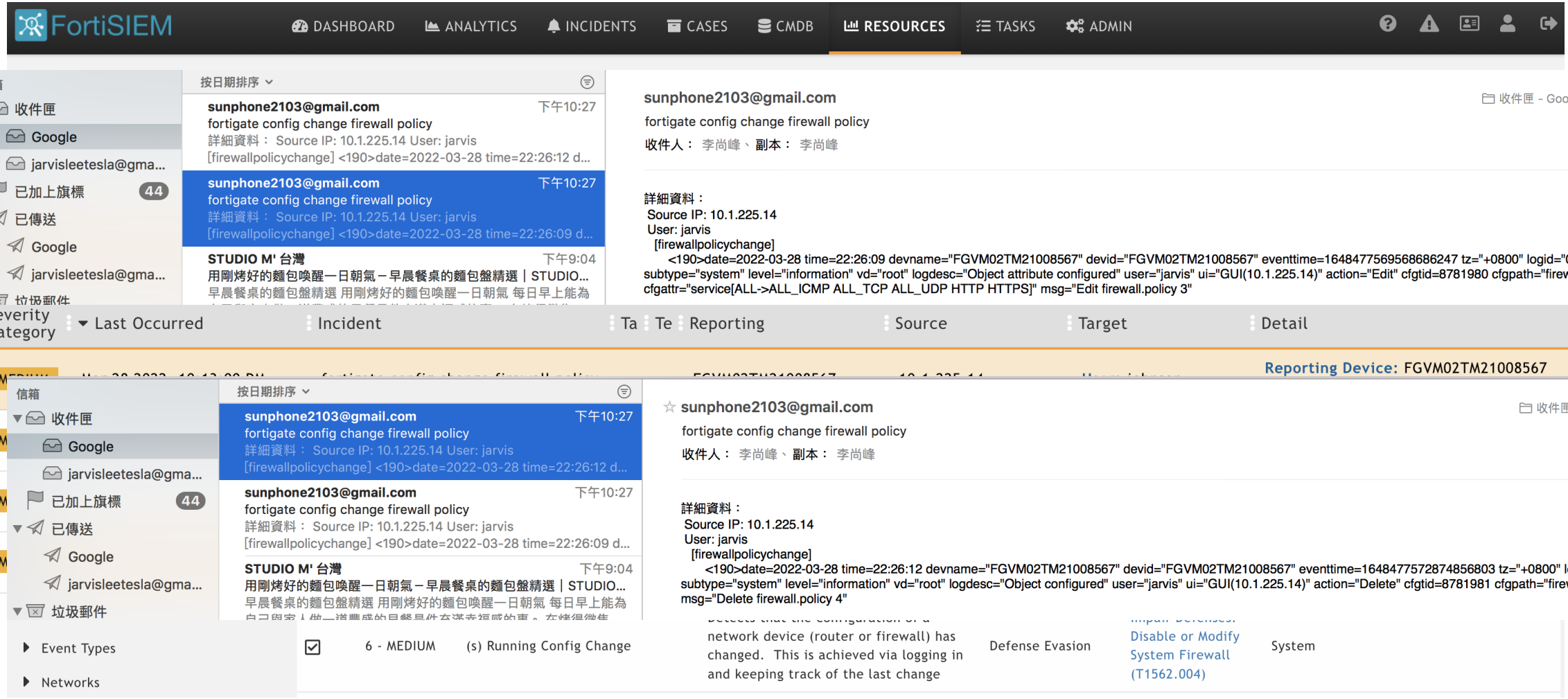
Configuration Manager

FortiSIEM 如何做到 – 差異比對



Configuration Manager

FortiSIEM 如何做到 – 更動告警



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 300 second time window

Generate Incident for: Windows Account Lock SourceIP

Incident Attributes:

Event Attribute		Subpattern	Filter Attribute	Row
Source IP	=	4625	Source IP	
User	=	4740	User	

Save Cancel