次世代端點安全解決方案
FortiEDR / XDR

Carlos Sheng
shengc@fortinet.com

資安的挑戰

在大量的遠端工作者出現後變得更加複雜

缺乏可視性

63%

的企業無法監控外網的端點，超過一半無法確認端點的合規狀況

威脅現況

進階的威脅
勒索病毒攻擊
營運的中斷

缺乏專業人員

告警疲勞
資安分析師過勞

Notes/Sources:
Gartner: Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017

對於Ransomware的焦慮

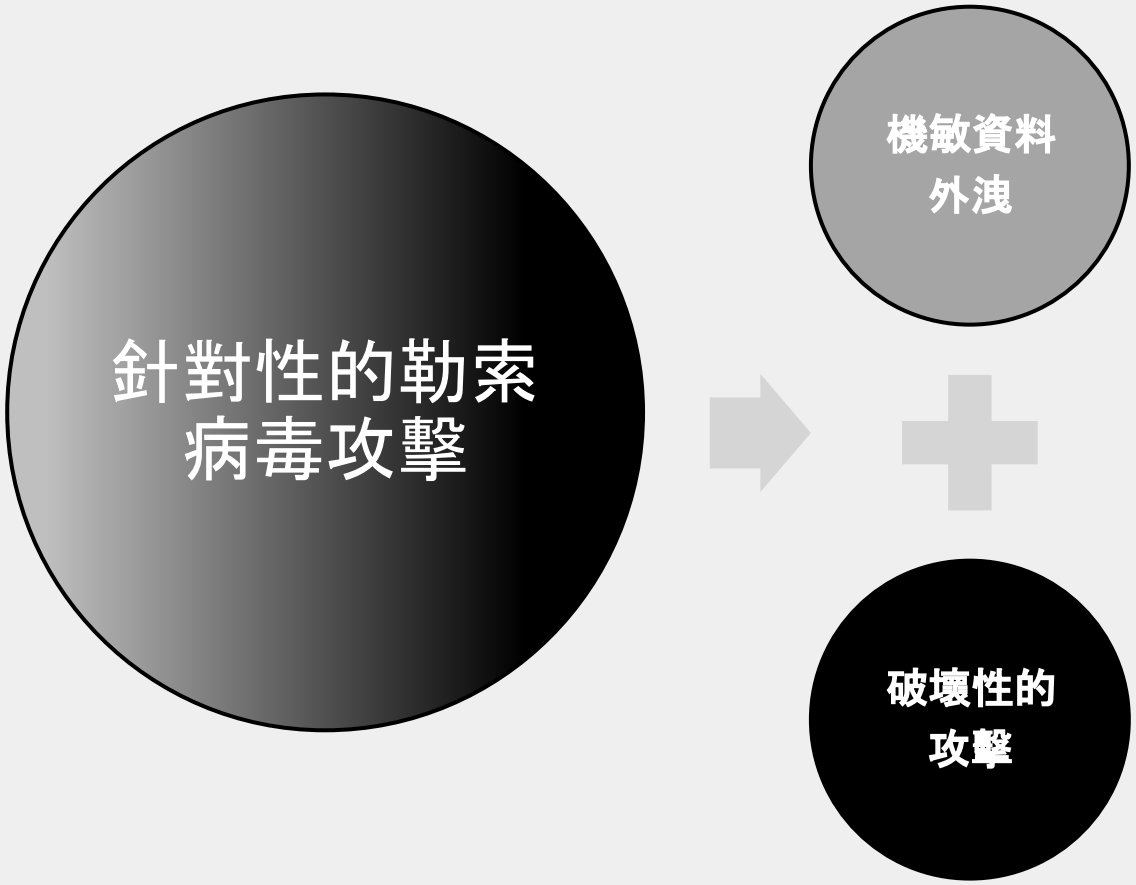
Ransomware攻擊大流行的高峰

16 Days

修復勒索病毒攻擊事件平均需要多少時間

Downtime costs 5-10x

營運中斷的成本是實際勒索金額的



Source: Verizon 2020 data breach investigation report

端點防護加上偵測與回應(EPP + EDR)

對於企業的價值

01 強化安全現狀	通過在廣泛的端點與工作平台上擴展可視性與增強安全能力以盡可能的防止攻擊事件
02 保持營運不中斷	確保韌性！通過早期偵測、快速回應與恢復以最大限度的降低攻擊事件帶來的衝擊。
03 簡化安全營運	借助資安服務和自動化與整合提升SOC成熟度以應對資安技能短缺的挑戰

端點防護的發展 ---- 特徵值比對 VS 行為模式分析

早期EDR廠商

EDR

20-40%
Penetration

Endpoint Detection and Response (EDR)

1. 分析所有 endpoint 的行為
2. 偵測惡意行為
3. 回應
    1. 阻擋—中斷惡意行為和進行修復動作
    2. 鑑識—偵查資安事件, 並找尋其源頭

EPP with EDR

Full EDR

Fortinet整合兩種防護機制

傳統EPP廠商

EP
P

95%
Penetratio
n

Endpoint Protection Platform (EPP)

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

端點安全:FortiEDR提供進階的端點全面防護

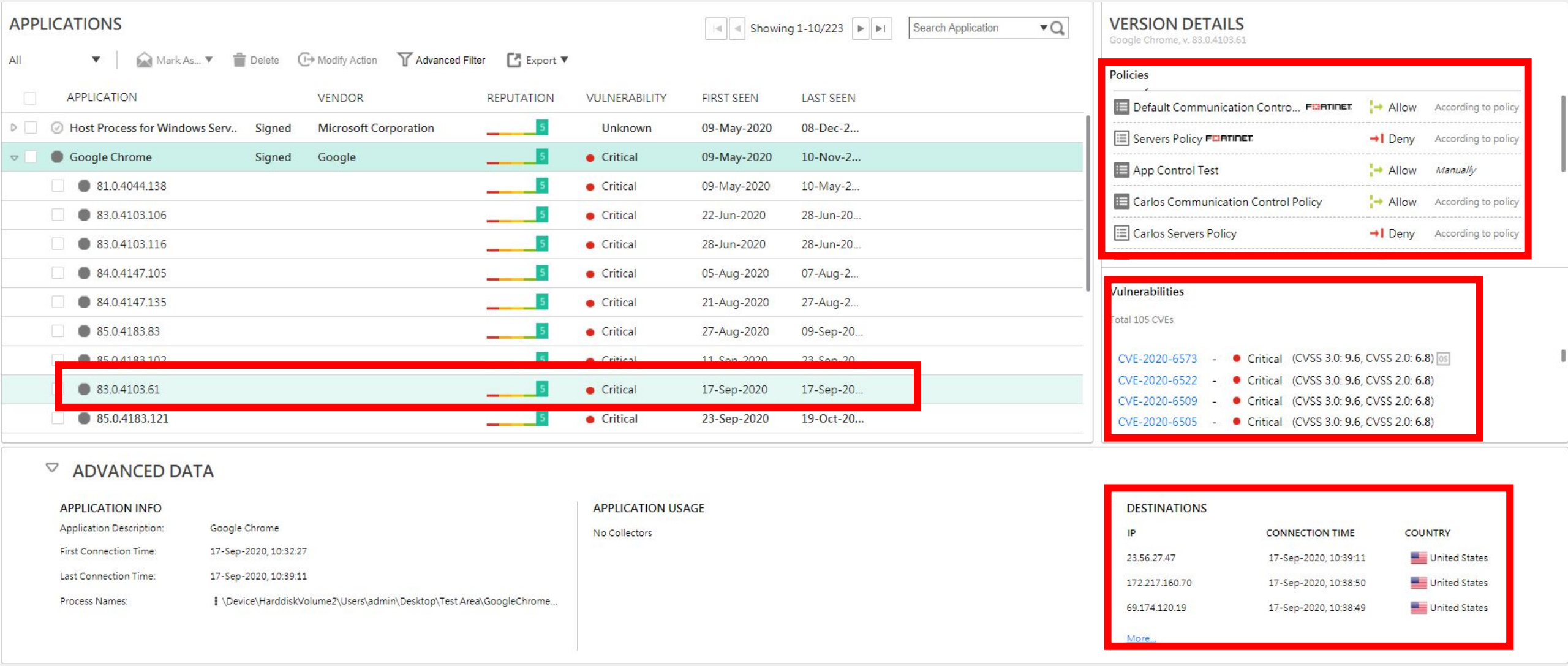
事前/安全可視性

事中/自我保護

事後/快速修復

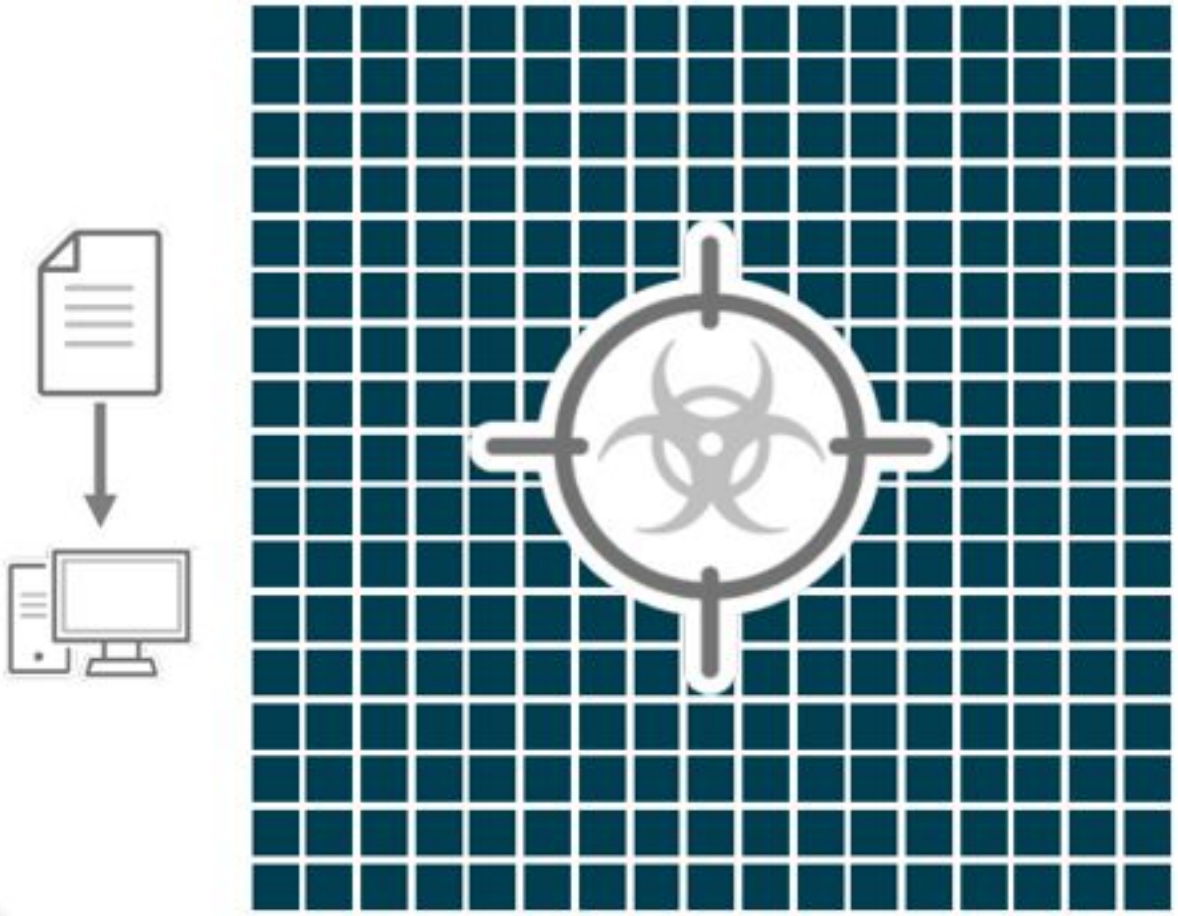
預 測	防 護	偵 測	回 應
減少攻擊面的暴露	檔案類型的病毒 機器學習不依靠特徵碼 預防惡意程式的攻擊	針對端點上程式行為的 行為模式的偵測	快速回應資安事件 遏制惡意事件 回復機制 MDR 服務 [可選擇]
避免危害的發生 • 找出非法的設備與IoT設備的威脅 • 虛擬補丁功能	• 避免惡意程式執行的保護	*自動解除資安危脅* • 避免勒索病毒的迫害 • 持續不斷的檢測 • 營運不中斷	• 自動化通知與回應 • 依風險定義自動回應 • 記憶體快照功能,提供日後鑑識與調查 • 防火牆自動聯防

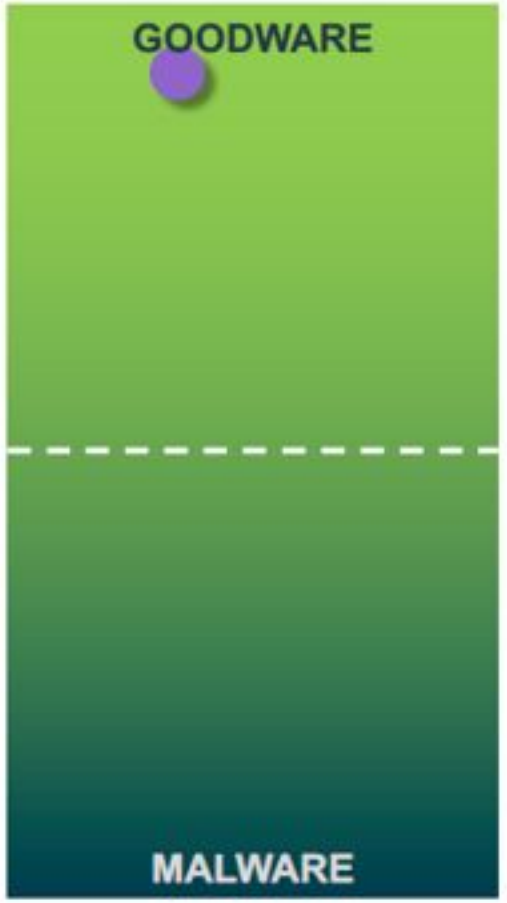
減少攻擊面-應用程式通訊控管



惡意程式防護方式的演進與攻防

Last Decade: Rise of Machine Learning





引進機器學習防護

(Very) Simplified Machine Learning Model

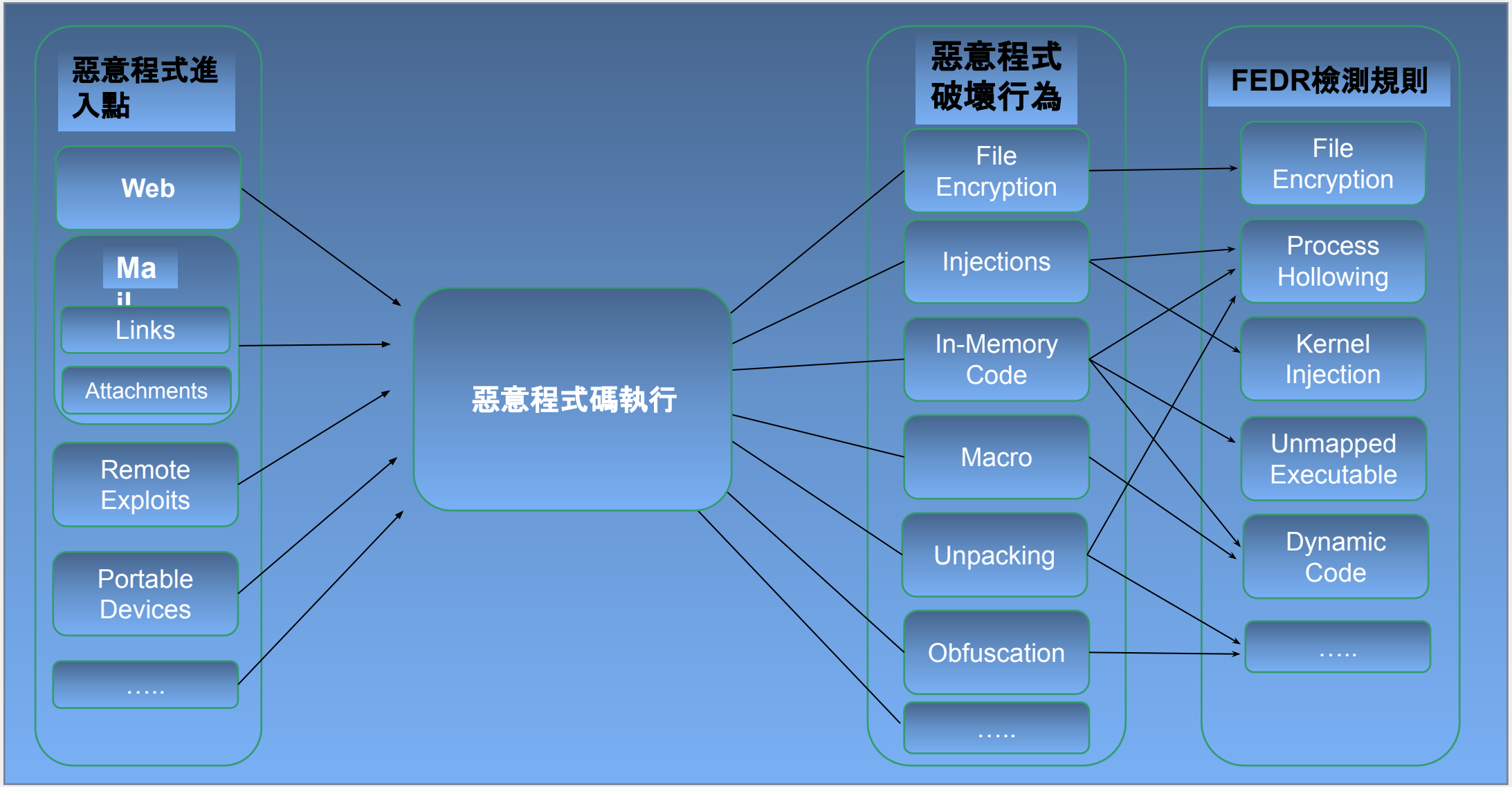
主動防護 – NGAV Technology

- **基於機器學習的防惡意程式執行保護引擎**
- 在AV-TEST測試報告中取得100%偵測率
- 透過雲端AI服務不斷的加強
- **不使用特徵碼**
- 基於作業系統核心

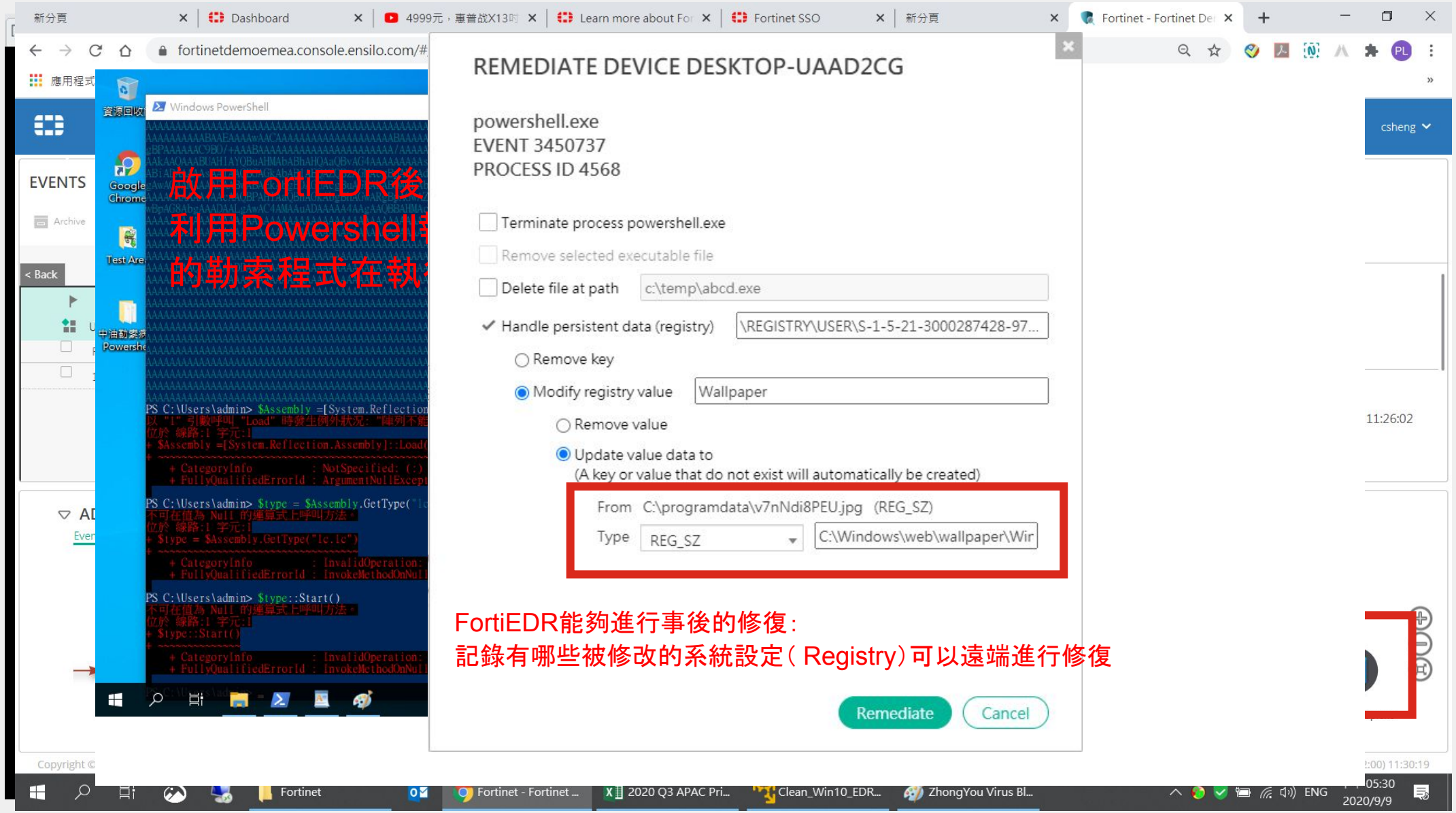
AV-TEST
The Independent IT-Security Institute

Test-Category			
BLOCKING OF "REAL WORLD" ATTACKS			
Ensilo	100.00% (129 / 129) blocked	0 (0.00%) partial blocked not blocked	
DETECTION OF PREVALENT MALWARE (STATIC AND DYNAMIC)			
Ensilo	100.00% (2835 / 2835) detected	0 (0.00%) not detected	
FALSE POSITIVE TESTING (STATIC SET OF FILES)			
Ensilo	99.99% (376553 / 376558) detected but ignored not detected	5 (0.01%) detected	

惡意行為主動防護- 端點異常行為檢測



示例：FortiEDR的惡意行為阻擋與修復功能



FortiEDR 安全織網的整合

3rd Party Firewall
- Palo Alto, Check Point

3rd Party Identity
- Active Directory

3rd party Mail security
- ProofPoint

3rd party SIEM
- Splunk App

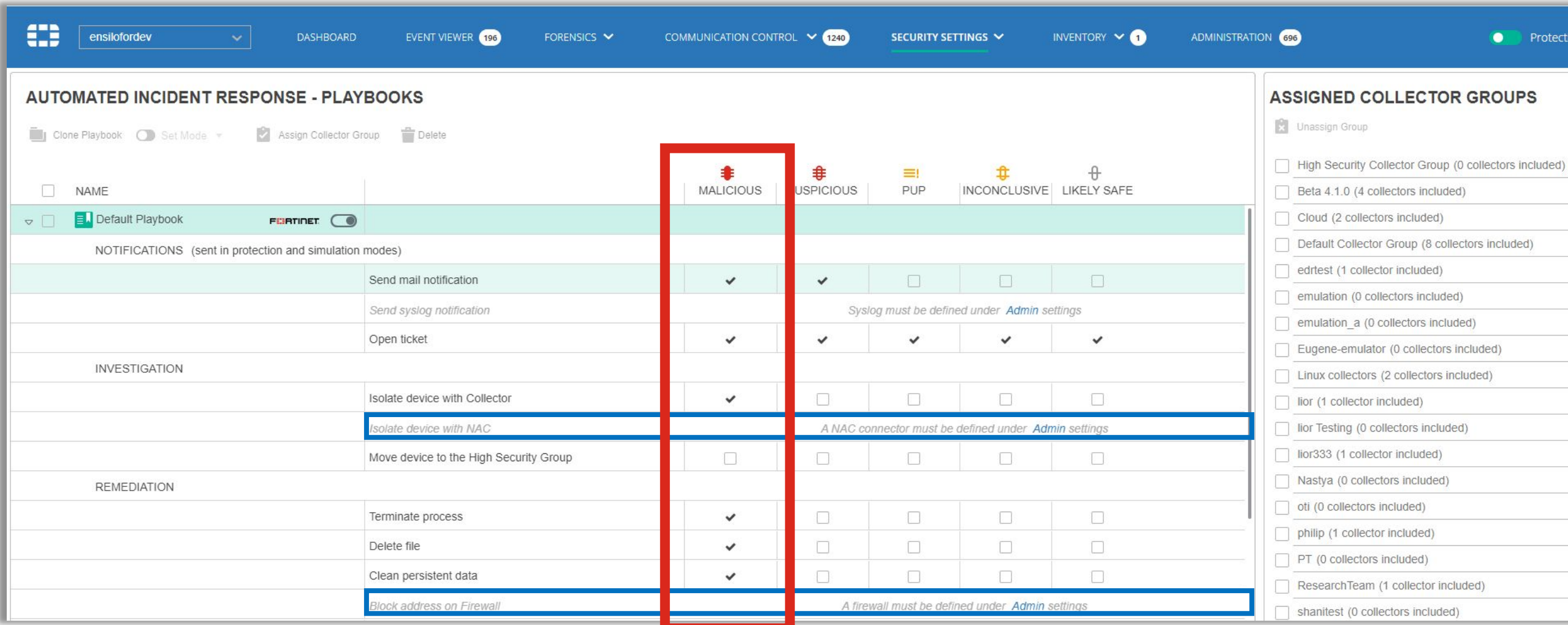
示例：FortiEDR與FortiGate的聯防功能

設定要進行自動聯防的Playbook

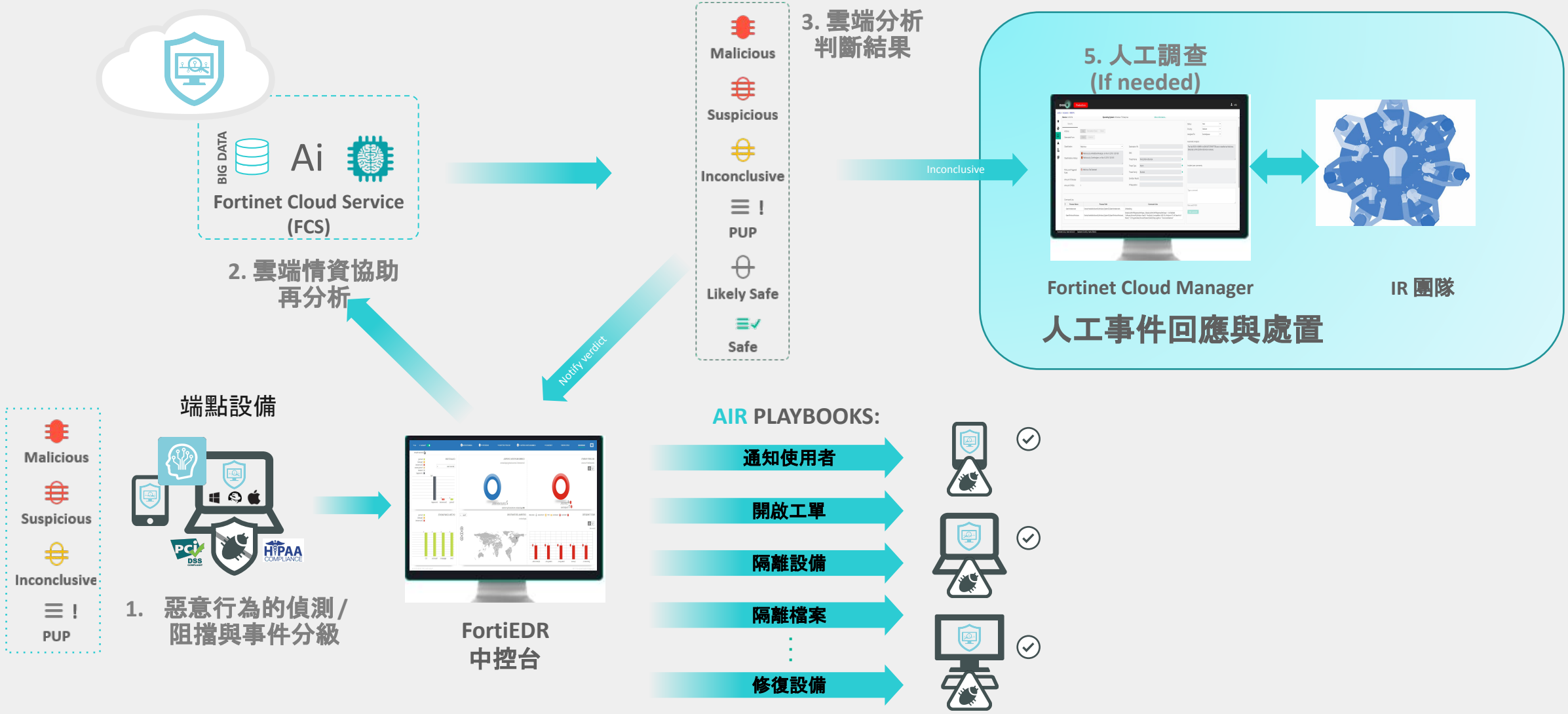
資安事件觸發聯防動作

在FortiGate上加入惡意IP進行阻擋

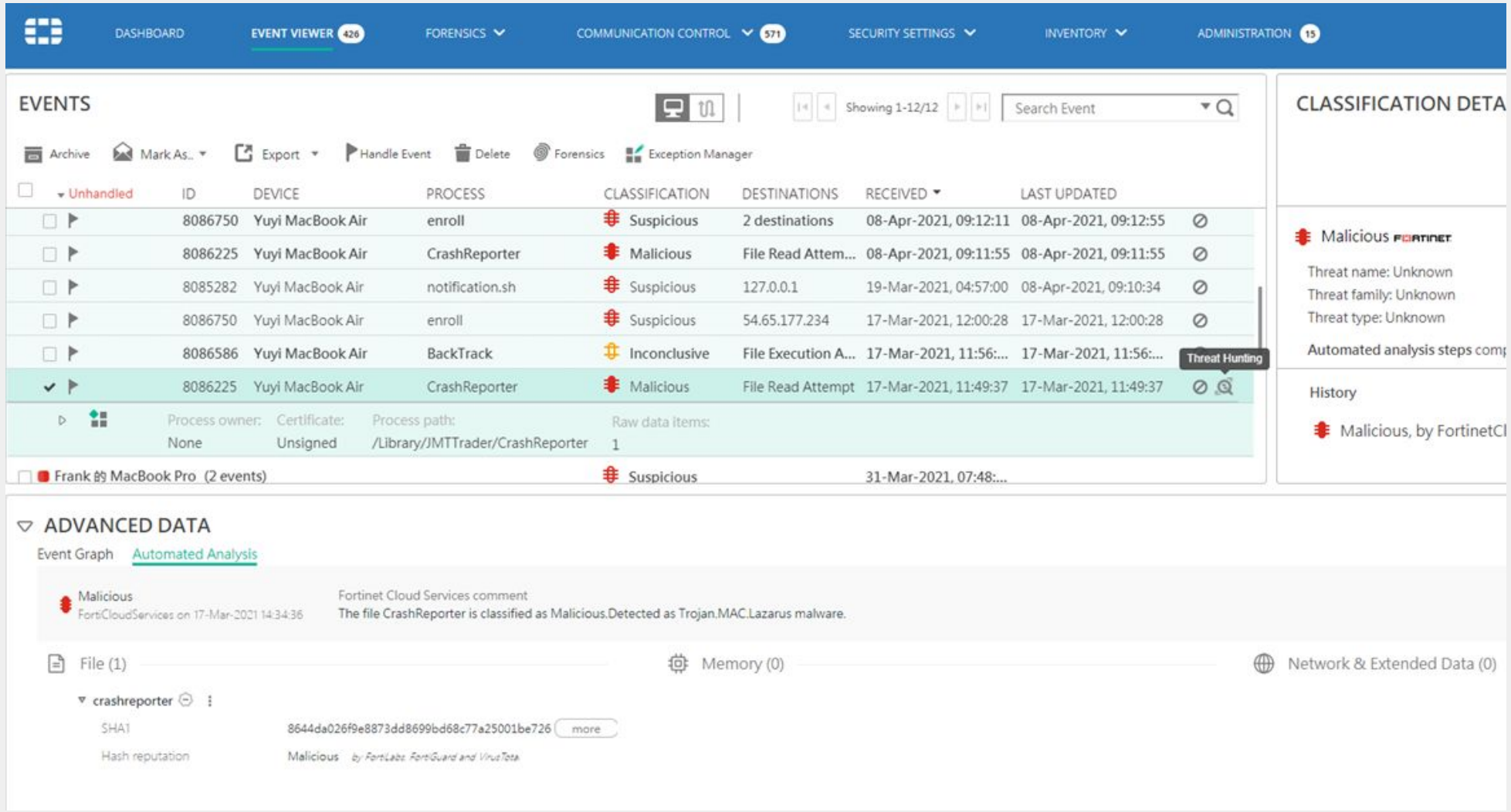
資安事件自動回應 —> Playbook設定,多樣的處理方式



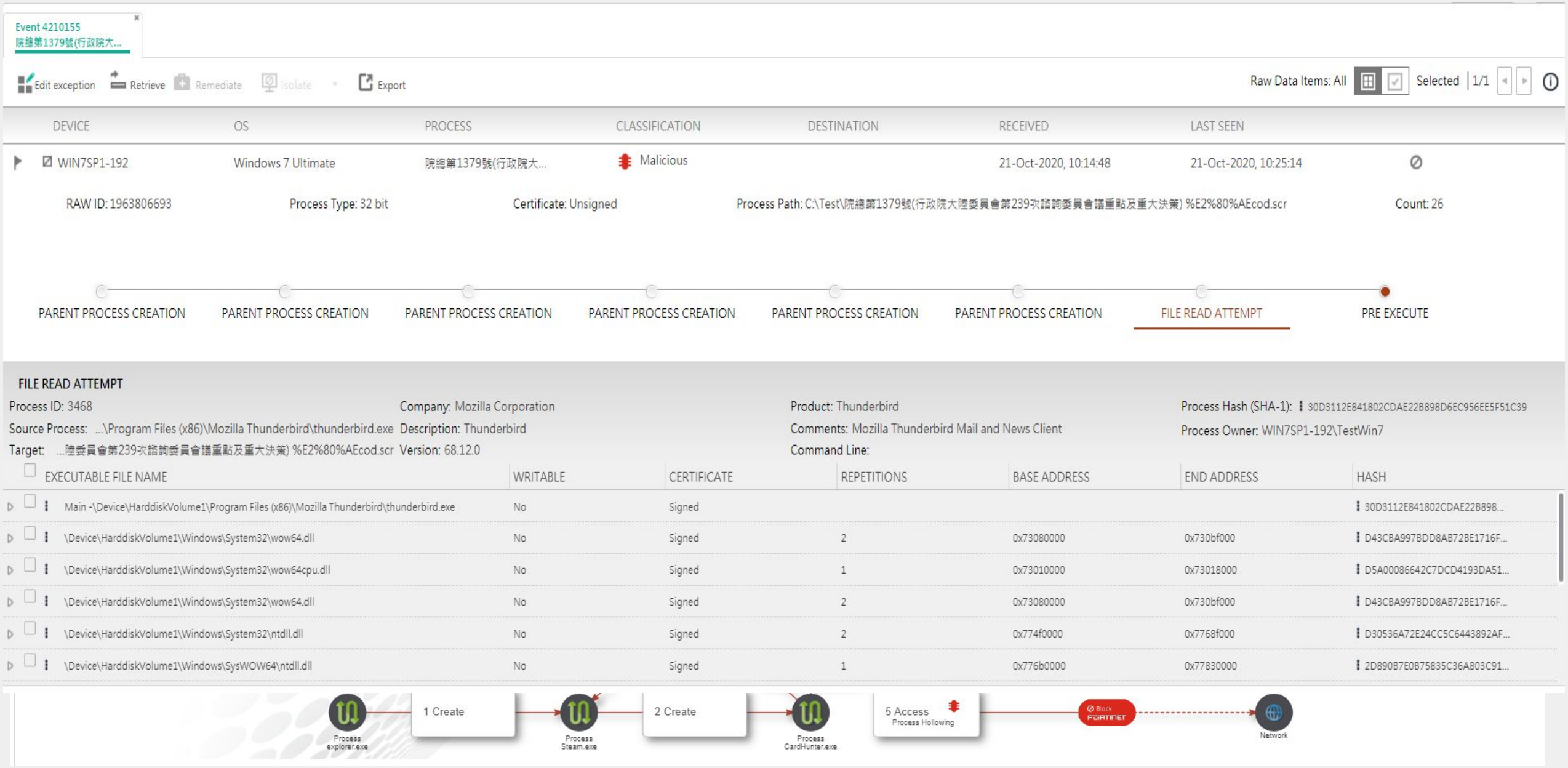
FortiEDR 資安事件處理運作流程



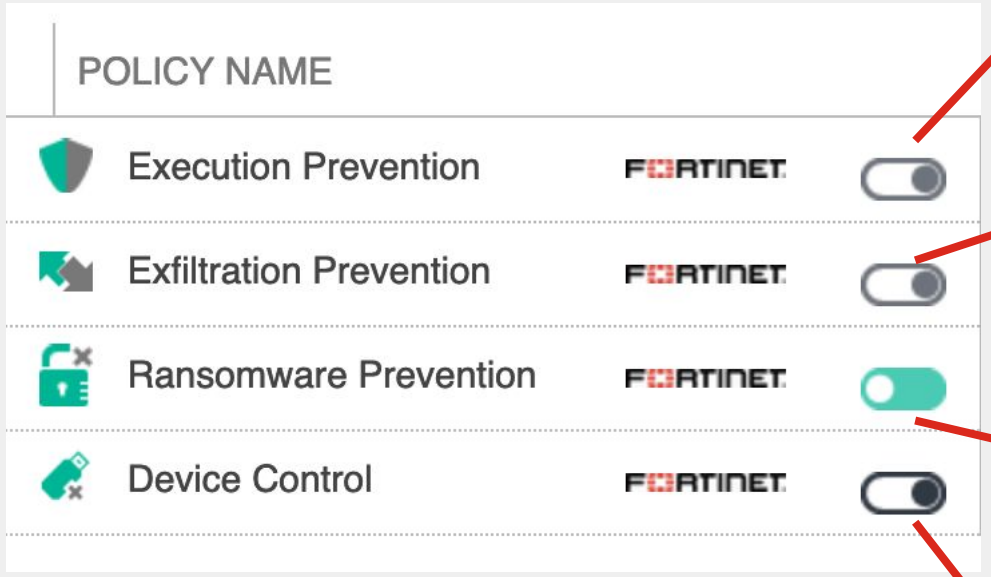
資安事件的分類檢視與資訊分析



資安事件進階鑑識


Event 4210155
院總第1379號(行政院大...
Edit exception
Retrieve
Remediate
Isolate
Export
Raw Data Items: All
Selected 1/1
DEVICE
OS
PROCESS
CLASSIFICATION
DESTINATION
RECEIVED
LAST SEEN
WIN7SP1-192
Windows 7 Ultimate
院總第1379號(行政院大...
Malicious
21-Oct-2020, 10:14:48
21-Oct-2020, 10:25:14
RAW ID: 1963806693
Process Type: 32 bit
Certificate: Unsigned
Process Path: C:\Test\院總第1379號(行政院大陸委員會第239次諮詢委員會議重點及重大決策) %E2%80%AEcod.scr
Count: 26
PARENT PROCESS CREATION
PARENT PROCESS CREATION
PARENT PROCESS CREATION
PARENT PROCESS CREATION
PARENT PROCESS CREATION
PARENT PROCESS CREATION
FILE READ ATTEMPT
PRE EXECUTE
FILE READ ATTEMPT
Process ID: 3468
Source Process: ...\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
Target: ...陸委員會第239次諮詢委員會議重點及重大決策) %E2%80%AEcod.scr
Company: Mozilla Corporation
Description: Thunderbird
Version: 68.12.0
Product: Thunderbird
Comments: Mozilla Thunderbird Mail and News Client
Command Line:
Process Hash (SHA-1): 30D3112E841802CDAE22B898D6EC956EE5F51C39
Process Owner: WIN7SP1-192\TestWin7
EXECUTABLE FILE NAME
WRITABLE
CERTIFICATE
REPETITIONS
BASE ADDRESS
END ADDRESS
HASH
Main -\Device\HarddiskVolume1\Program Files (x86)\Mozilla Thunderbird\thunderbird.exe
No
Signed
30D3112E841802CDAE22B898...
\Device\HarddiskVolume1\Windows\System32\wow64.dll
No
Signed
2
0x73080000
0x730bf000
D43CBA9978DD8AB72BE1716F...
\Device\HarddiskVolume1\Windows\System32\wow64cpu.dll
No
Signed
1
0x73010000
0x73018000
D5A00086642C7DCD4193DA51...
\Device\HarddiskVolume1\Windows\System32\wow64.dll
No
Signed
2
0x73080000
0x730bf000
D43CBA9978DD8AB72BE1716F...
\Device\HarddiskVolume1\Windows\System32\ntdll.dll
No
Signed
2
0x774f0000
0x7768f000
D30536A72E24CC5C6443892AF...
\Device\HarddiskVolume1\Windows\SysWOW64\ntdll.dll
No
Signed
1
0x776b0000
0x77830000
2D890B7E0B75835C36A803C91...
Process explorer.exe
1 Create
Process Steam.exe
2 Create
Process CardHunter.exe
5 Access
Process Hollowing
Block
FORTINET
Network

多種資安政策的設定與套用



Malicious File Detected	Block
Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block
Sandbox Analysis - File was sent to the sandbox for analysis	Log

Access to critical system information	Block
Bruteforce Attempt Detected	Log
Debugged Process - Connection from a Debugged Process	Log

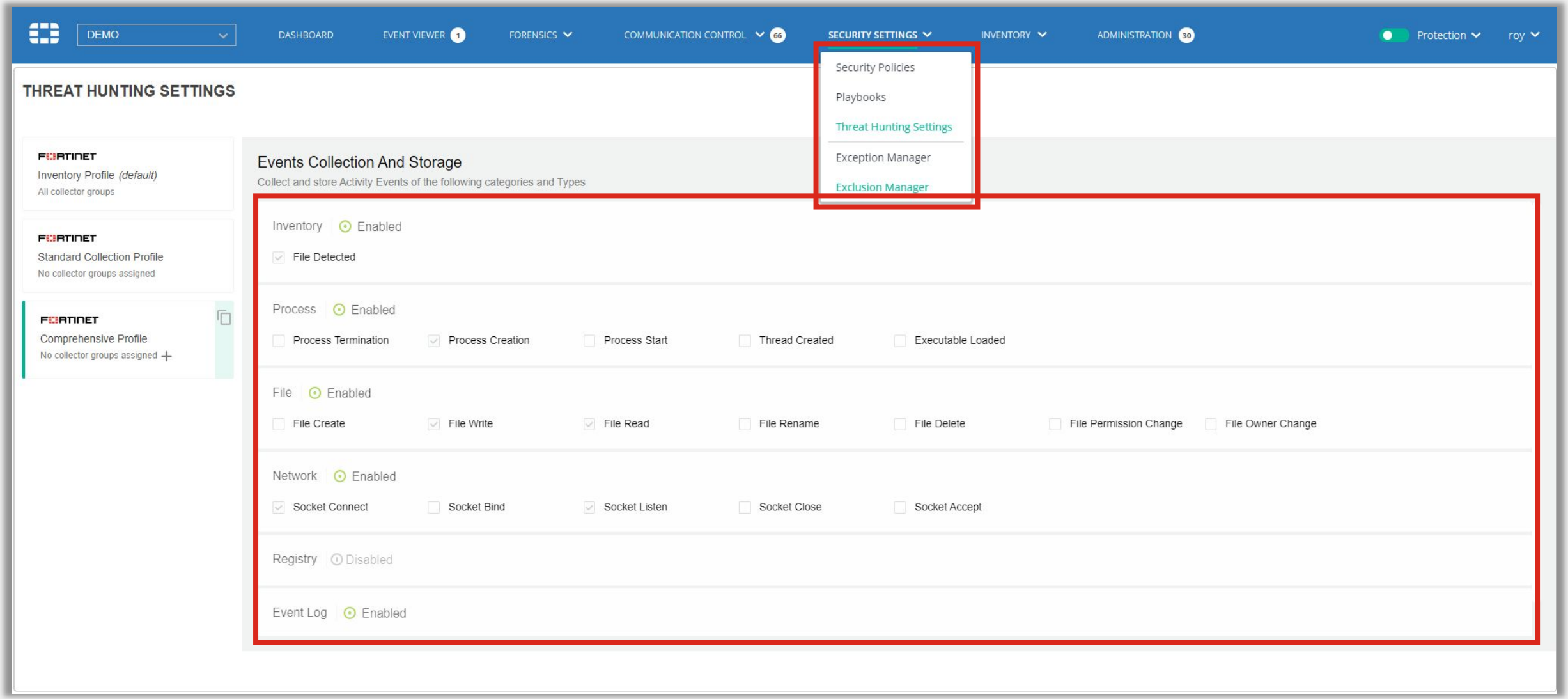
Process Hollowing - Process Code Was Replaced

Process Hollowing is a technique used by malware to masquerade as a legitimate process by stripping the original process from its code and replacing it with malicious payload. Attackers find this technique very efficient as the process will appear to be valid, and even signed, when examined.

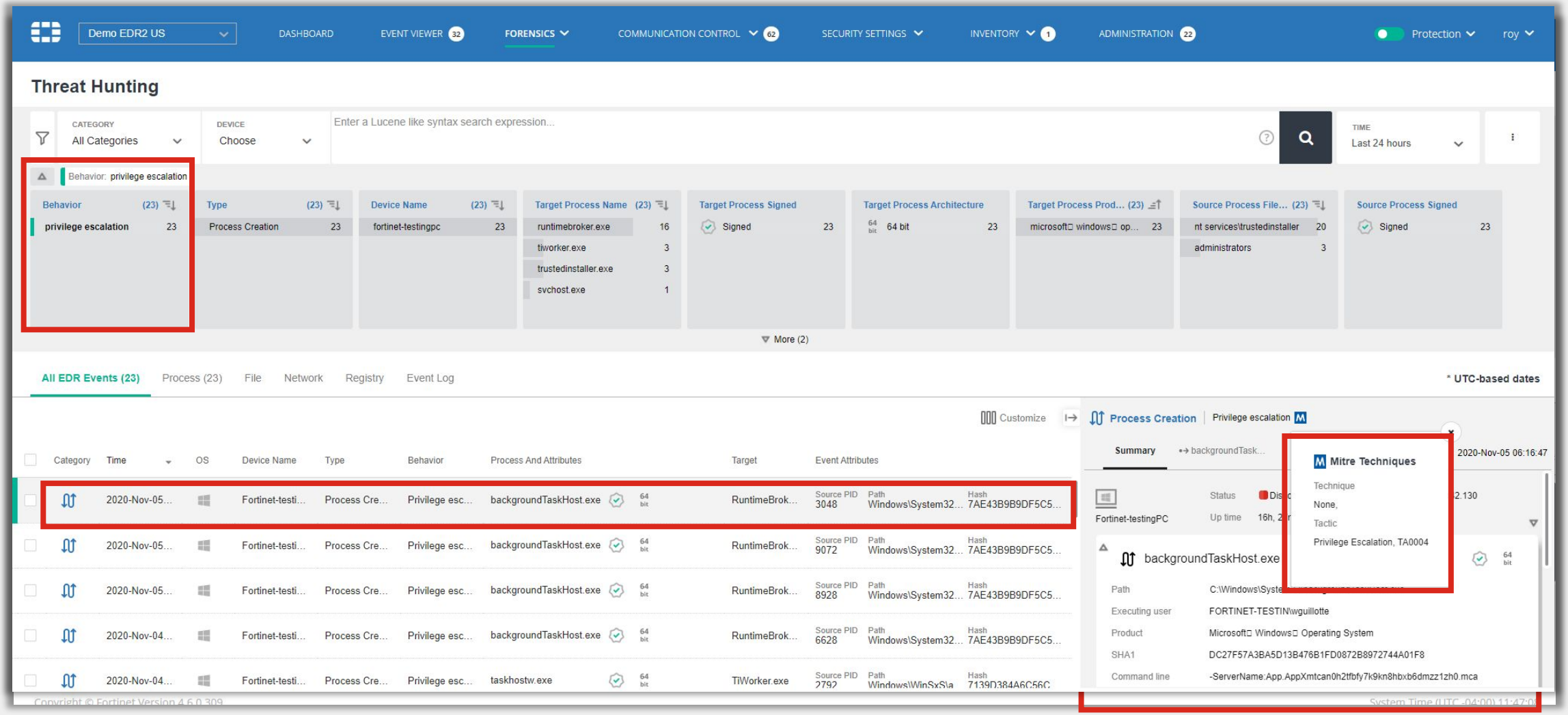
MITRE Techniques:
T1186 - Process Doppelganging
T1093 - Process Hollowing

Retrieve the executable file of the parent process from the targeted device according to its Path by using the Forensic Tab. In addition, retrieve a full executable file memory of the process for deeper analysis.

FortiEDR強大的威脅捕獵功能 – 記錄多種系統行為



FortiEDR強大的威脅捕獵功能 – 基於行為類型與MITRE分類



FortiEDR 的優勢

防　護　效　能

- **即時的保護**
  - 自動化達成事前防範與事後保護
  - 不再遭受弱點與勒索病毒的危害
  - 離線防護機制
- **自動化偵測與回應**
  - 行為模式偵測
  - 系統化與自動化的資安事件回應處理
  - 營運不中斷
- **資安事件調查與分析,威脅軌跡紀錄**
  - 記憶體快照功能,幫助調查非檔案類型攻擊—例如勒索軟體
  - 資安鑑識 – 資安事件攻擊軌跡與記錄分析
- **減少潛在的攻擊來源**
  - 找出可疑IoT設備
  - 基於應用程式風險等級的虛擬補釘技術

運　作　效　能

- **輕量化的端點程式避免造成效能衝擊**
  - 約60-120 MB的記憶體使用
  - 平均系統使用率不超過 1% CPU
- **加速資安事件的處理時間**
  - 災難的處理與回復無須離線
  - 可進行系統回復操作
  - 針對惡意程式進行處理, 免除系統重灌的困擾
- **廣泛的作業系統支援**
  - Windows, Mac, Linux
  - Legacy OS – Windows XP, Windows 7, Windows 2003, and VDI
- **彈性的系統建置選擇**
  - 雲端, 本地,混合模式
  - 可在Air Gap狀態下運作

FortiXDR - AI驅動的資安營運

1. 取得跨資安設備多樣的資訊

2. 透過雲端大腦多樣化檢測流程強化事件關聯分析能力

3. 自動化的事件回應處理機制

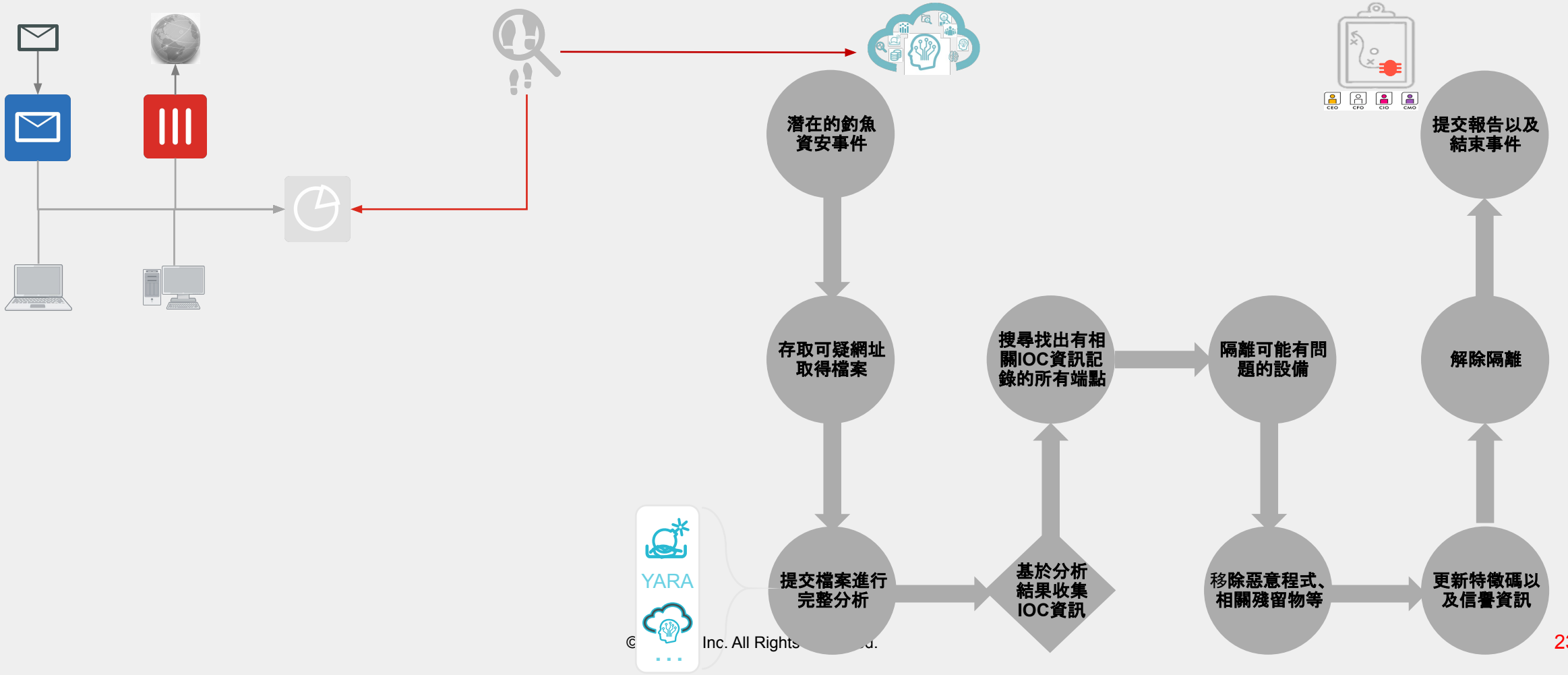
FortiXDR示例：SpearPhishing事件的偵測，調查與回應

多個資安設備記錄了可疑的URL

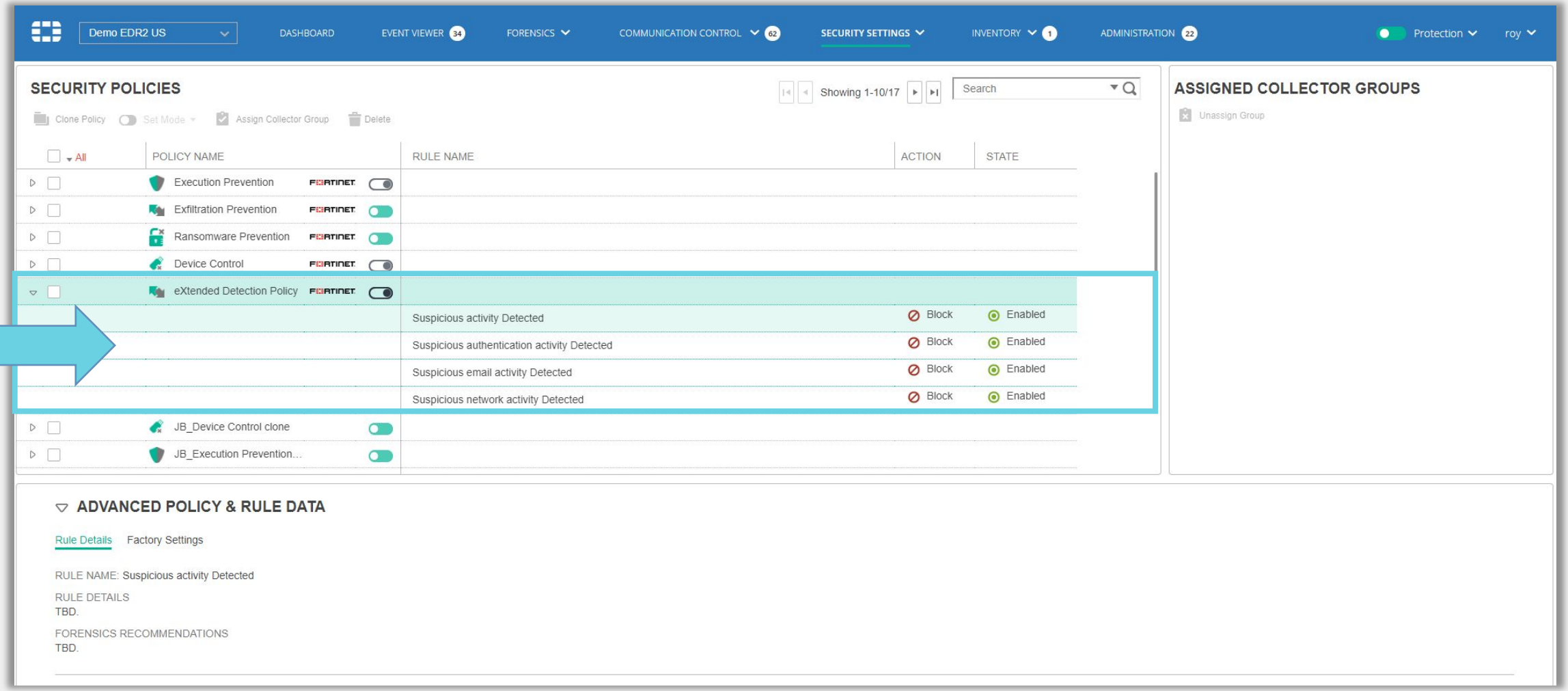
Stage 2: 分析引擎指出可能有資安事件發生

Stage 3: AI決策引擎啟動調查

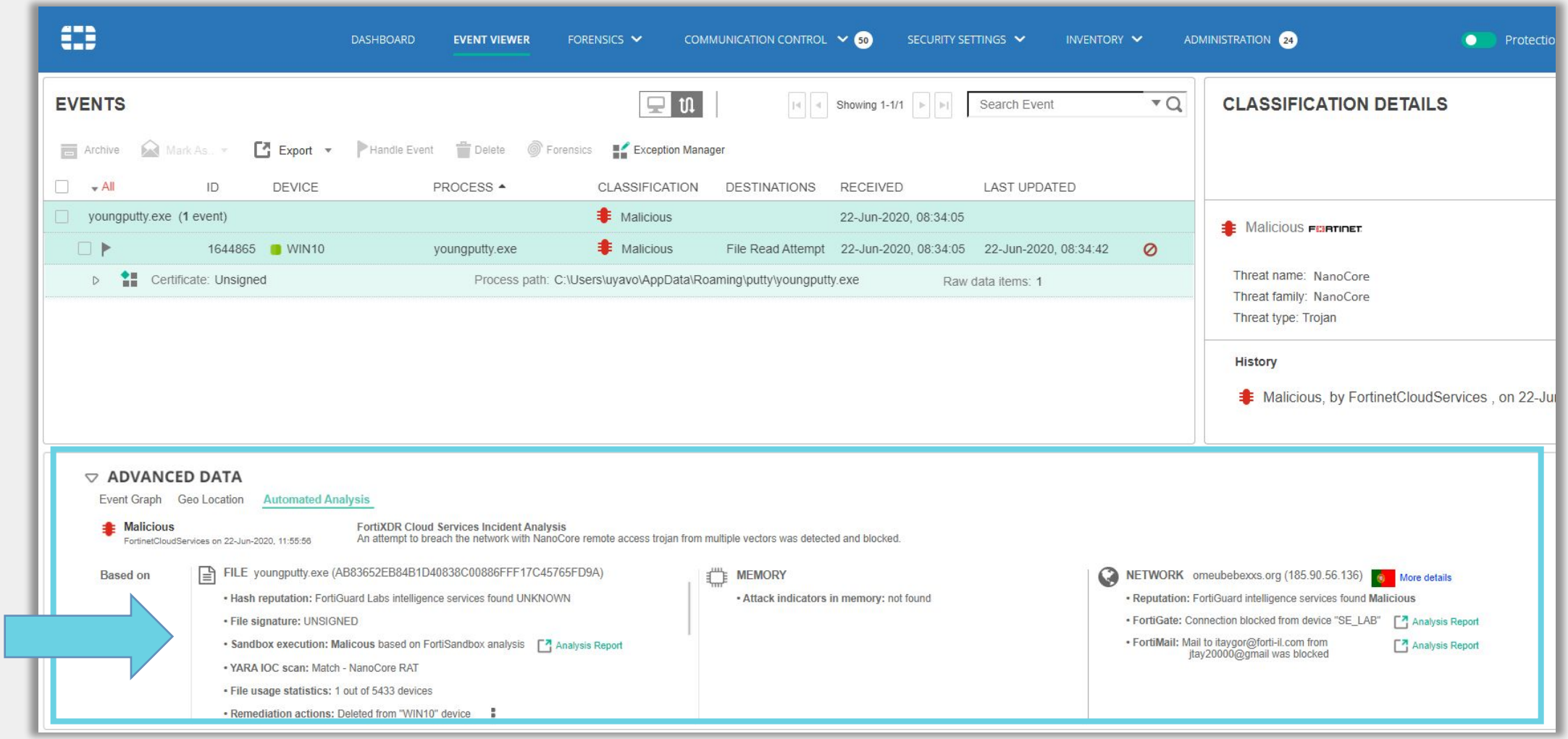
Stage 4: 透過回應框架進行統整修復



Fortinet XDR資安政策的設定



FortiEDR資安事件檢視- XDR Enabled View



Fortinet多樣化的端點防護解決方案與安全服務

- **事前防範 = EPP(端點防護)**

  多種資安功能、惡意程式的過濾

- **事後保護 = EDR/MDR/XDR (偵測與回應)**

  記錄使用者的行為軌跡,偵測異常行為與回應修復

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	


FORTINET