7×24 全年無休的虛擬資安分師
— FortiAI

劉　乙 / 北亞區技術總監

Agenda

1. 被忽視的企業資安死角
2. 淺談「人工智慧」及「機器學習」
3. 虛擬資安分析師的能力
4. FortiAI 特點及功能畫面

資訊產業資安事件頻傳

我們在此學到了什麼？

來源：中央社

鴻海證實美洲廠區受勒索病毒攻擊 傳金額達10億台幣

最新更新：2020/12/09 21:53

鴻海8日證實，美洲廠區近日遭受網路勒索病毒攻擊，受影響廠區網路逐漸恢復正常，對集團整體營運影響不大。（示意圖 / 圖取自Pixabay圖庫）

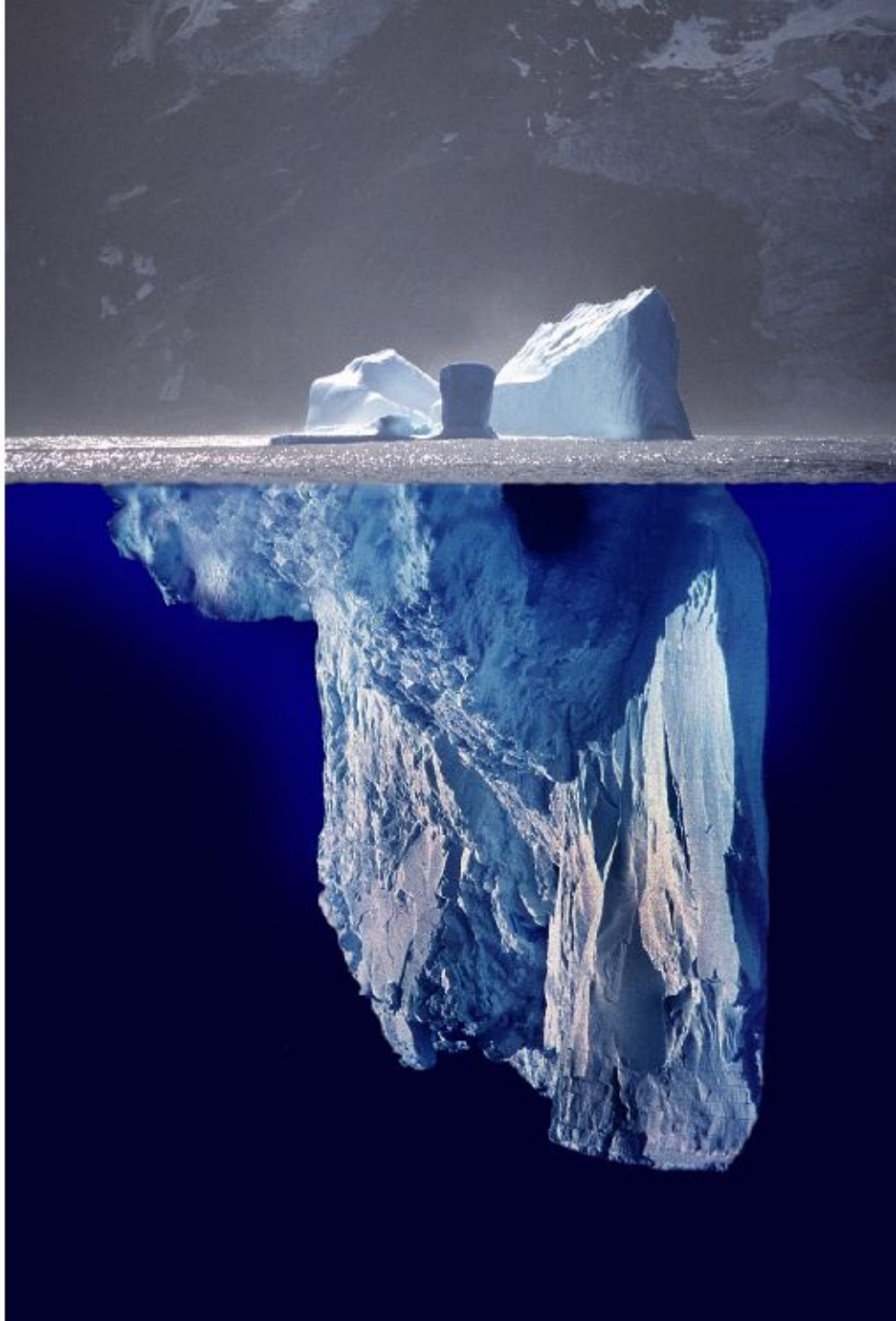
傳駭客勒索14億 廣達證實遭攻擊不影響營運

廣達21日證實，少部分伺服器遭網路攻擊，已與外部技術專家合作處理，公司日常營運未受影響。（圖取自廣達電腦網頁quantatw.com）

Visibility（可視性）

知己知彼，百戰不殆

冰山一角？



企業永遠面臨資安的三大難題？

1. 缺人

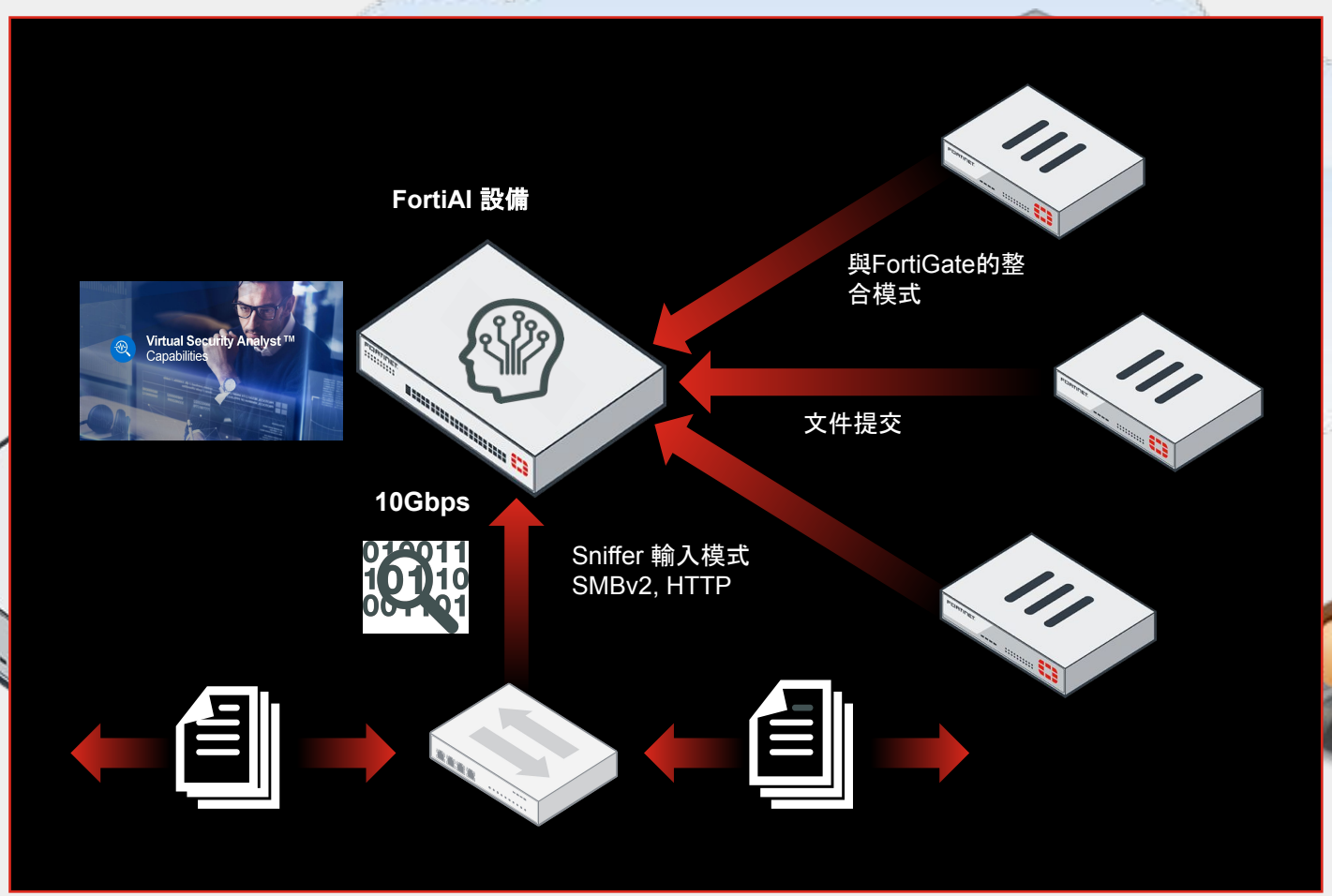
2

3.

自動化的神兵利器，7x24 全年無休健檢未知威脅？

全球第一個將 FortiGuard 雲端智慧，完整釋放到地端

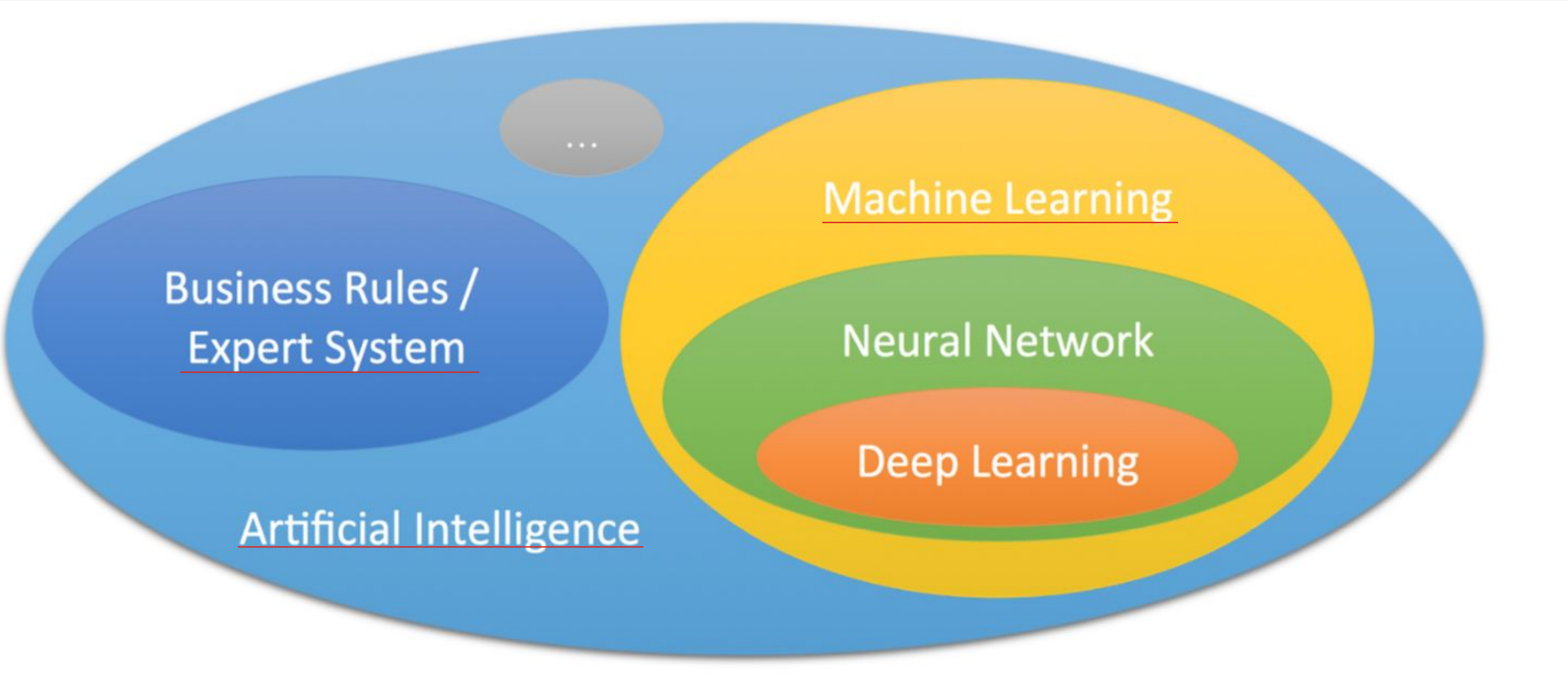
- Fortinet AI 黑科技
- 無需安裝任何端點軟體(agent)
- 自動學習分析網路流量/文件
- 惡意軟體，惡意威脅無所遁形



淺談【人工智慧】及【機器學習】

AI, Expert System, Machine Learning and Deep Learning

人工智慧, 專家系統, 機器學習 , 深度學習



什麼是教育, 什麼是學習？

與其說是科學, 它更像是一門藝術 (結合生物, 心理, 教育, 數學, 電腦科技....)

1.講述法
2.分析法
3.觀察法
4.練習法
5.啟發法
6.問思教學法
14演繹法
15歸納法

© Fortinet Inc. All Rights Reserved.

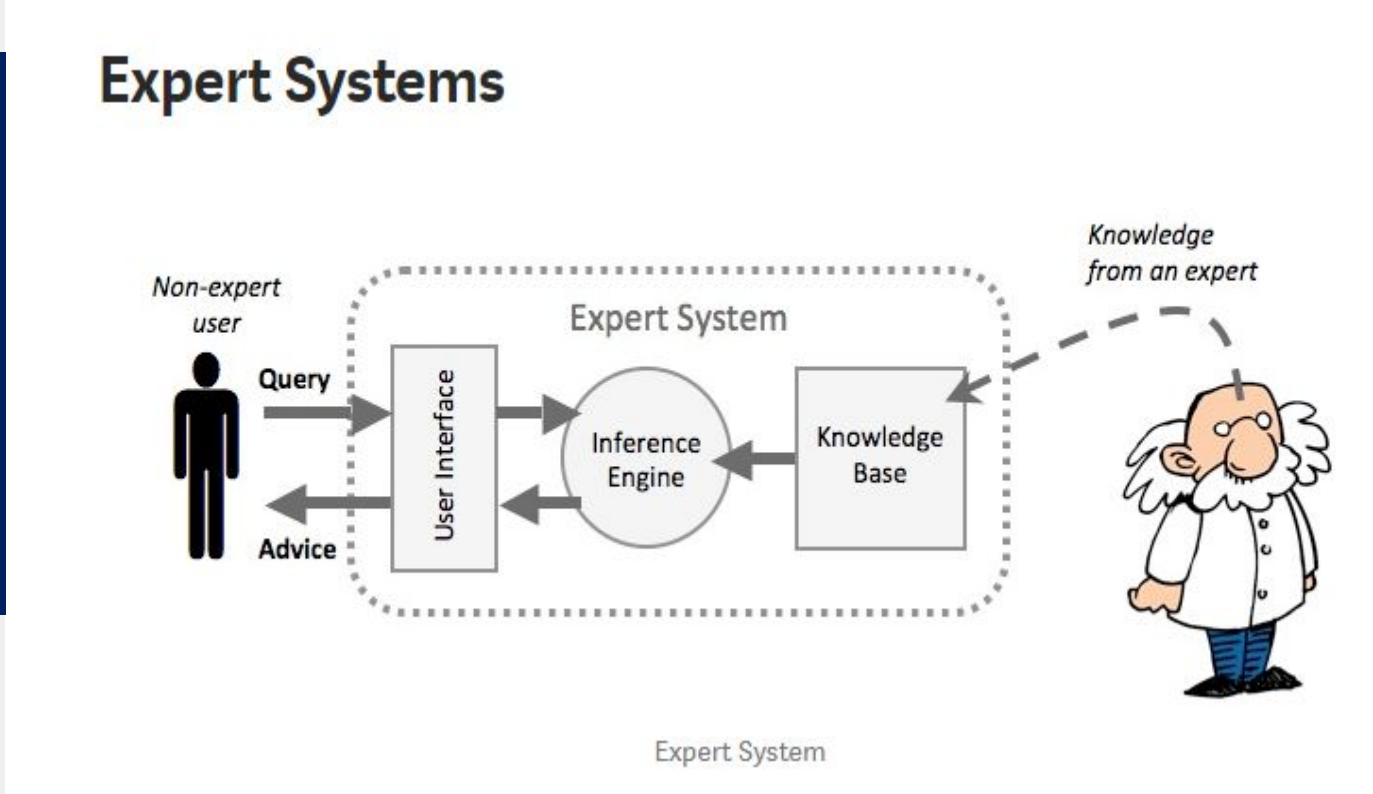
9

專家系統 — 人工給定的經驗法則

Virus Signatures 特徵碼 / 病毒碼

第一代傳統防護已知惡意軟體技術

- Hash
- Static Rule 靜態分析
  (CPRL --- if then)
- 病毒引擎 (人工智慧比對)



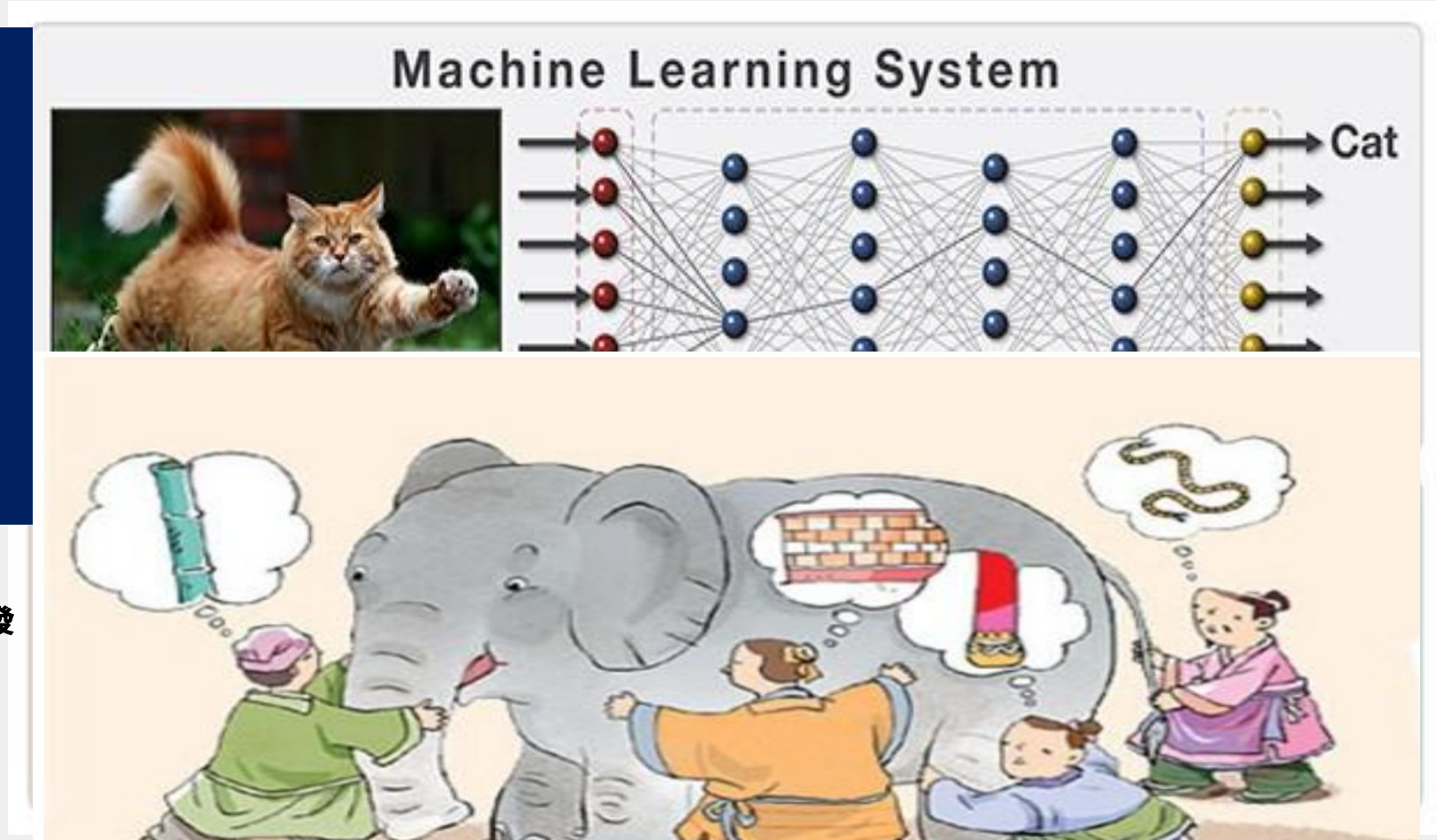
Machine Learning – 自我演繹, 自我調整

機器學習的盲點和優勢

成熟的機器學習機

第三代的防惡意軟體技術　FortiAI

- 不需要特徵值 (signature)
- 需要強大運算能力
- Sub-Second 檢測能力
- 虛擬的資安分析師

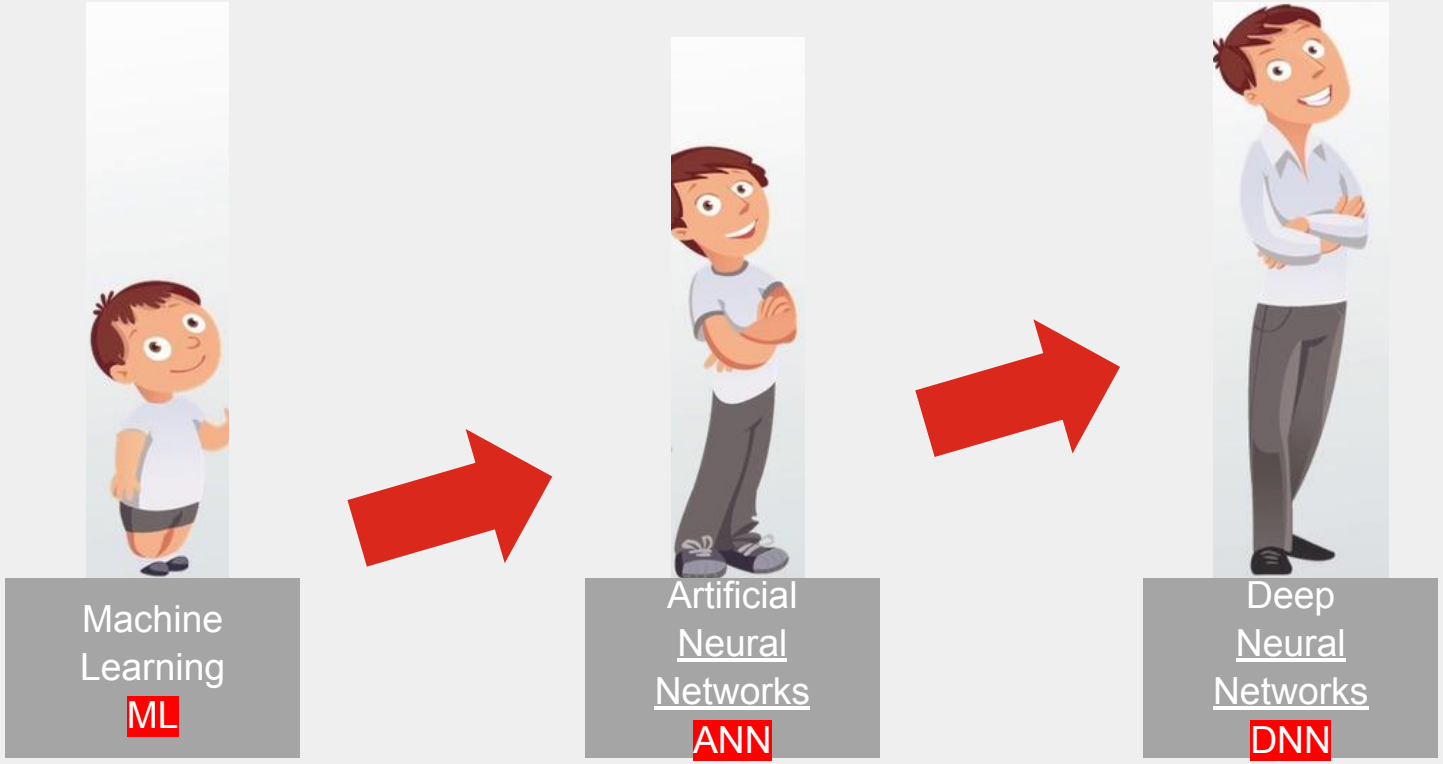


盲人摸象的啟發

AI: 學習機器的成熟度

學習機器的種類大大影響學習能力

MODELS



AI: Machine Learning

Machine Learning : 廣義的定義 -- 利用已知的資料透過一些運算方式訓練電腦，讓電腦可完成預測工作

教學機器/機制
Models

機器分類
Classify

BEE

AI: Artificial Neural Networks (ANN)

Artificial Neural Network : 它是一個由硬體和軟體組成的系統，仿造人腦神經元的運作制定而成。

Artificial Neural Networks ANN

教學機器/機制
Models

Category of bees

機器分類
Classify

AI: Deep Neural Networks (DNN)

Deep Neural Networks :是一種在輸入和輸出層之間具有兩層或更多維的類神經網路，用於針對複雜的非線性關係進行建模型。

Deep Neural Networks DNN

教學機器/機制 Models

ANN #1 蜜蜂分類

ANN #2 時辰:
9am vs 9pm

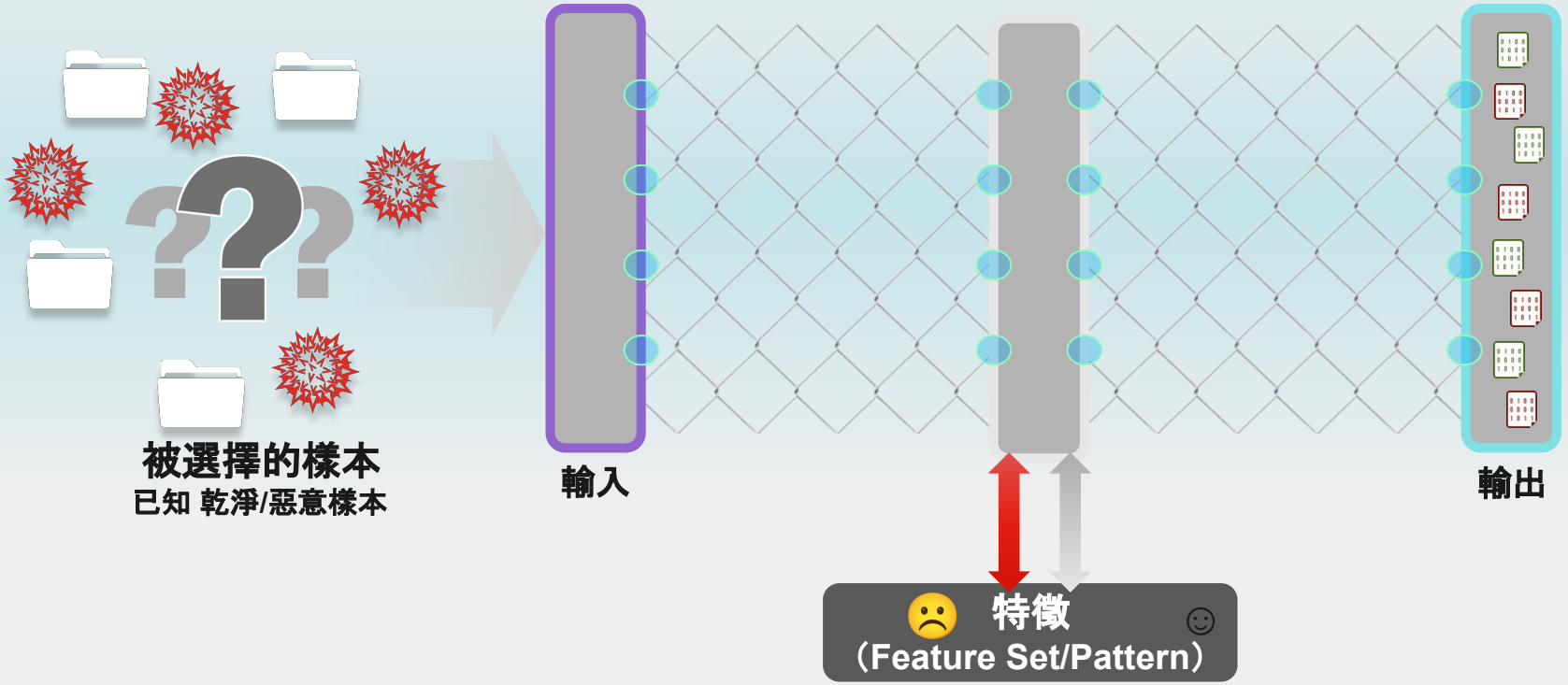
ANN #3 鄉村 vs 都市

教學機器/機制 Models

機器解譯

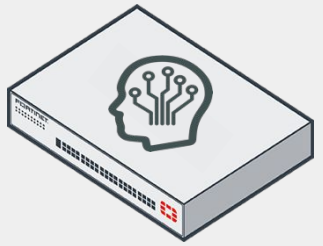
蜜蜂
在*早上10:00*,
在*田野間*,
停留在花上採蜜

FortiAI 出廠前預訓練



乾淨 / 惡意
特徵知識數據庫
(Feature Set , not Signature)

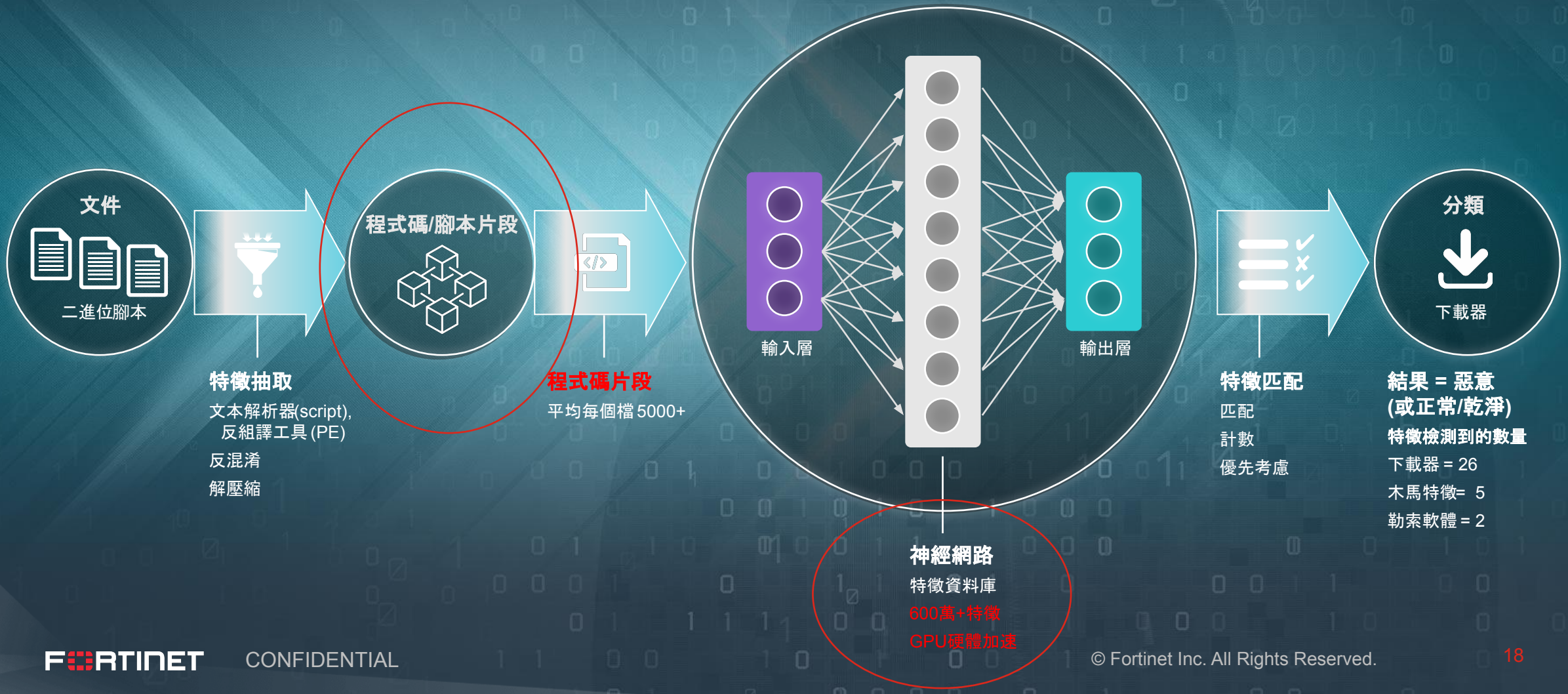
神經網路
從 FortiGuard* 升級



- **預訓練** 步驟在FortiGuard 實驗室中已經完成，使用超過2000萬正常和惡意檔進行的訓練
- 持續進行訓練和升級

FortiAI 線上機器學習和判決

惡意軟體檢測工作流（執行檔/無檔案式腳本語言 JS，Powershell)



Virtual Security Analyst ™
Capabilities

FortiAI 虛擬資安分析師TM (DNN)

虛擬安全分析師的惡意軟體分析能力

客戶專屬的惡意軟體分析師–
識別超過20種攻擊場景

- 例如 Ransomware, Dropper, PWS (Password Stealing Trojan), CoinMiner, Banking Trojan, Fileless attack etc
- 能夠為客戶回答如下問題:
  - 我受到了哪種惡意軟體的攻擊？(What)
  - 惡意軟體的目的是什麼？(How)
  - 為什麼是惡意的？(Why)
- 特徵在日誌中會被打上相應的‘標籤”(Tag)

Downloader	Redirector	Dropper	Ransomware	Worm
Password Stealer	RootKit	Banking Trojan	InfoStealer	Exploit
Clicker	Virus	Application	CoinMiner	DoS
BackDoor	WebShell	Search Engine Poisioning	Proxy	Trojan
Phishing	Fileless	Wiper	Industroyer	

7x24 全年無休，不斷精進的資安鑑識專家

提供更好的ROI選擇

人力成本 年薪 -- 60K-95K美元
5-6 年工作經驗

安全分析師的成本*
技能需求

- 惡意軟體研究經驗
- 入侵事件調查分析能力
- 即時更新時下最新的鑑識新知

思考一下

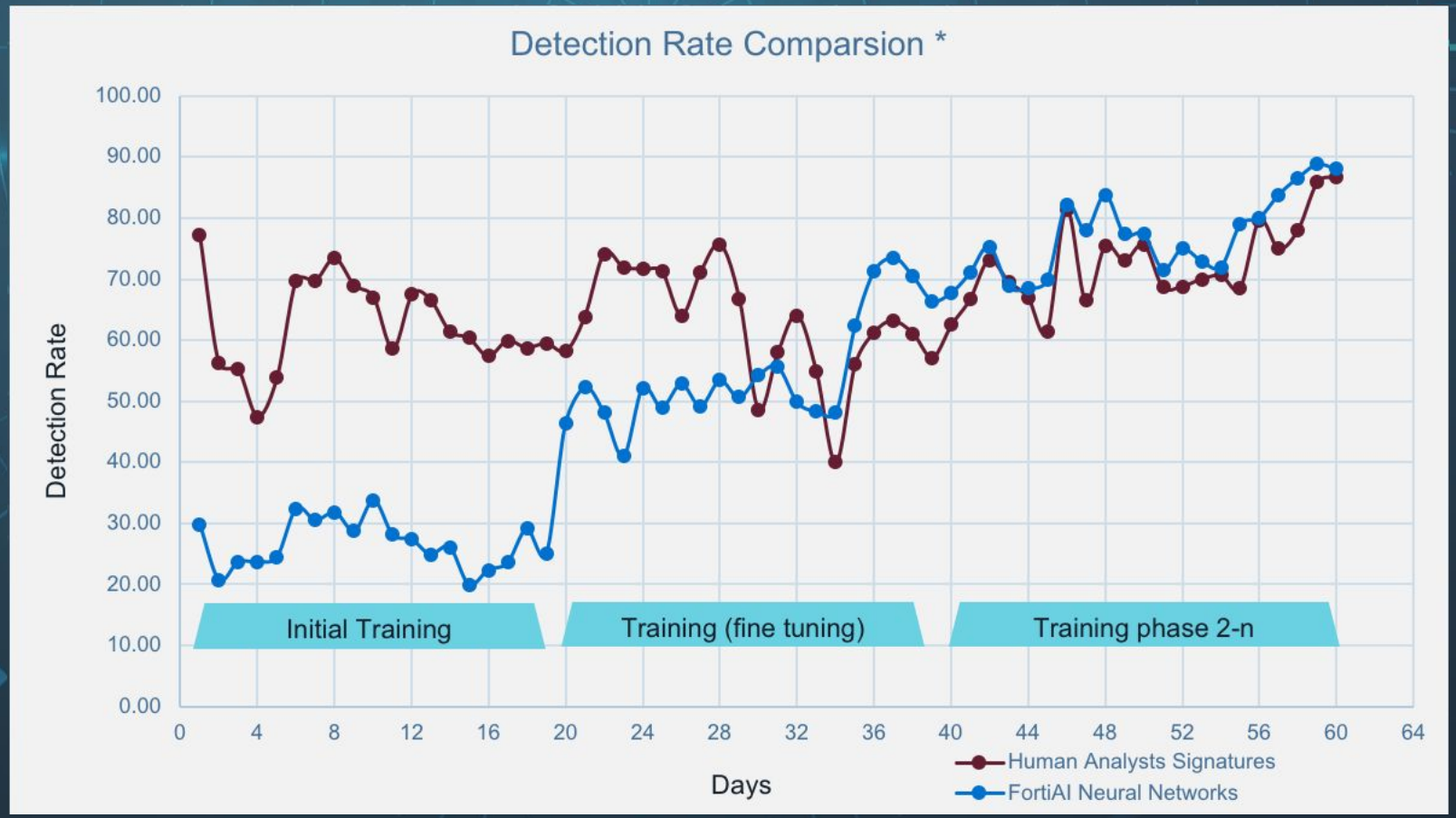
- 入侵的直接成本和間接產生的商譽損失
- 一種能夠分攤當前安全分析師繁重工作的方法，並且能夠降低人為失誤
- 人工結合AI分析師組合團隊帶來的可能

* Based on https://www.salary.com/research/salary/benchmark/information-security-analyst-ii-salary

持續訓練 – 人工 vs 機器

人工vs機器的檢出率隨著訓練週期產生變化

- **FortiAI 人工智慧神經網路**
  - 發貨前完成預訓練
- **訓練階段目標**
  - 最高檢出率
  - 最低誤報率
- **FortiGuard 升級**
  - ANN 升級
  - 與最新威脅保持同步
- **未來學習**
  - 在客戶現場完成

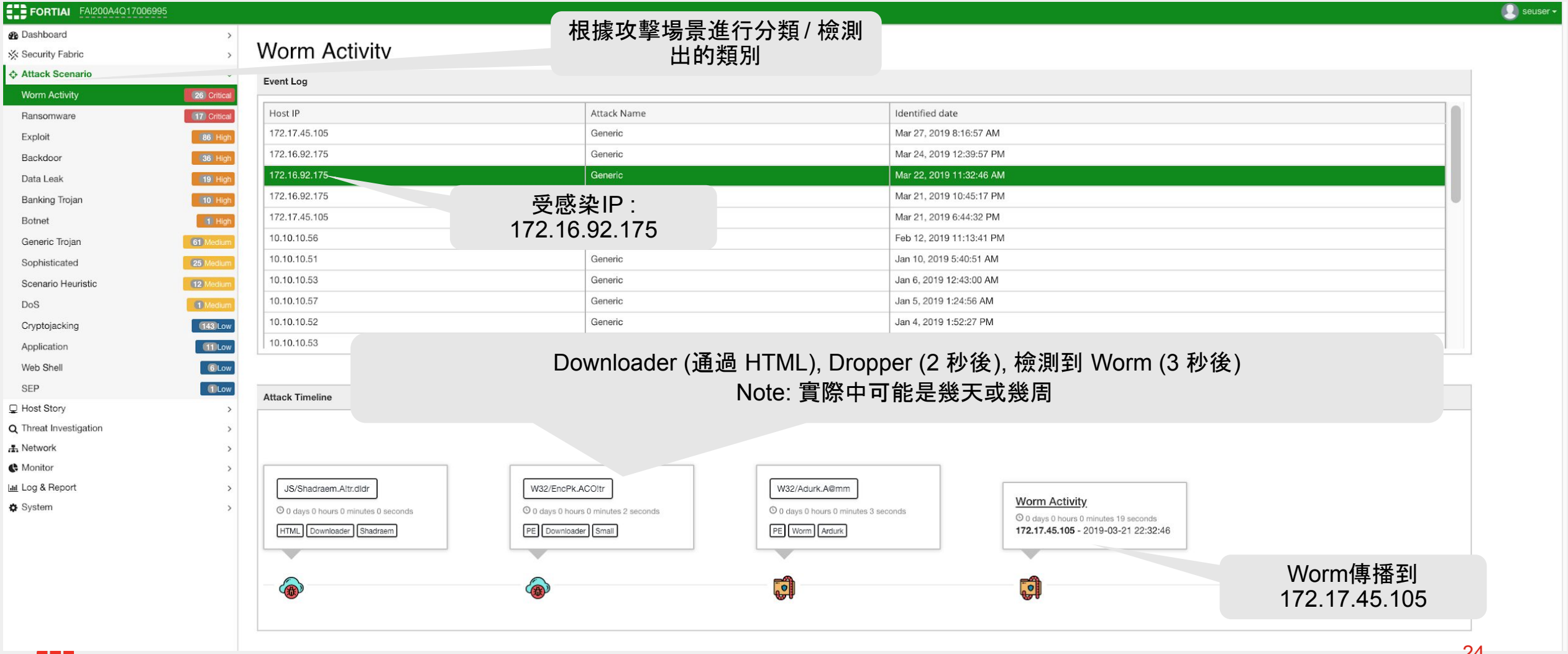


*Detection Rate on FortiGuard QA samples

FortiAI 的特點及功能畫面

FortiAI – 攻擊場景 AI 引擎 – GUI

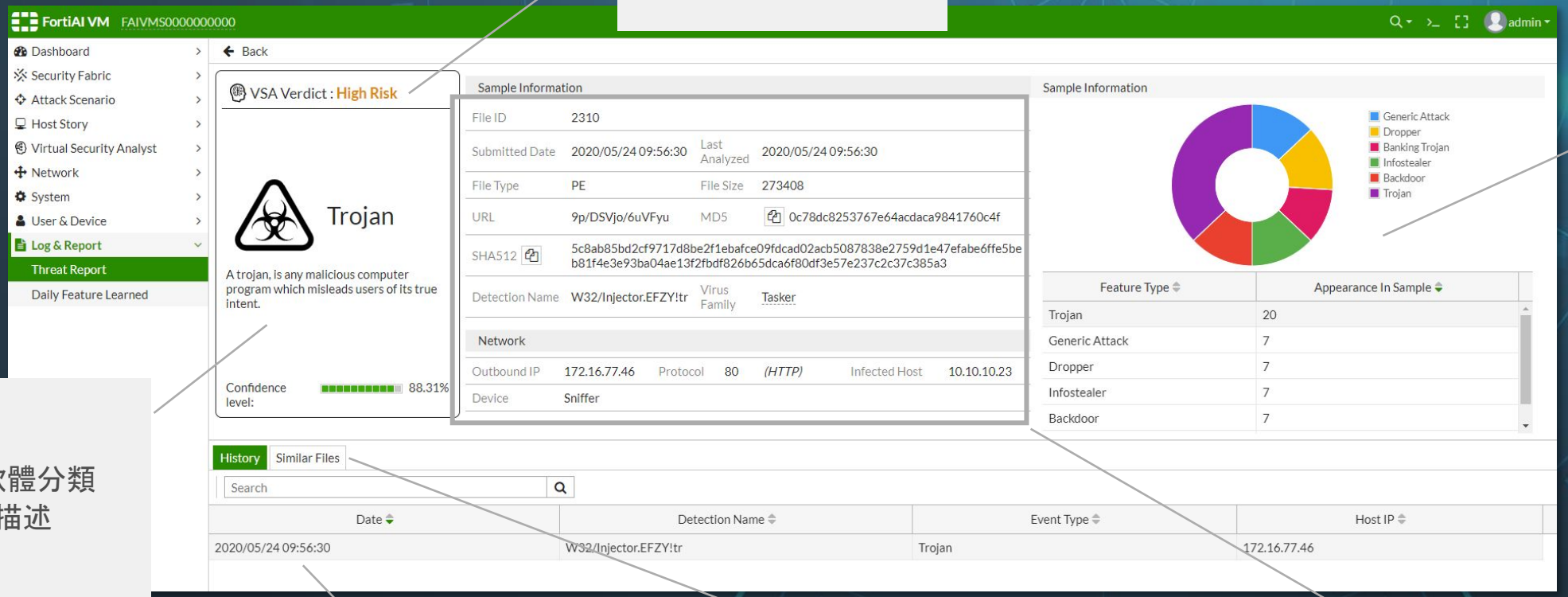
根據攻擊場景進行分類



24

FortiAI 一目瞭然的分析報表

判決和可信度



功能分解

惡意軟體分類與描述

出現在網路上的事件(歷史)

相似性分析引擎搜索

雜湊 / 類型 / 時間 / 病毒家族 / 來源

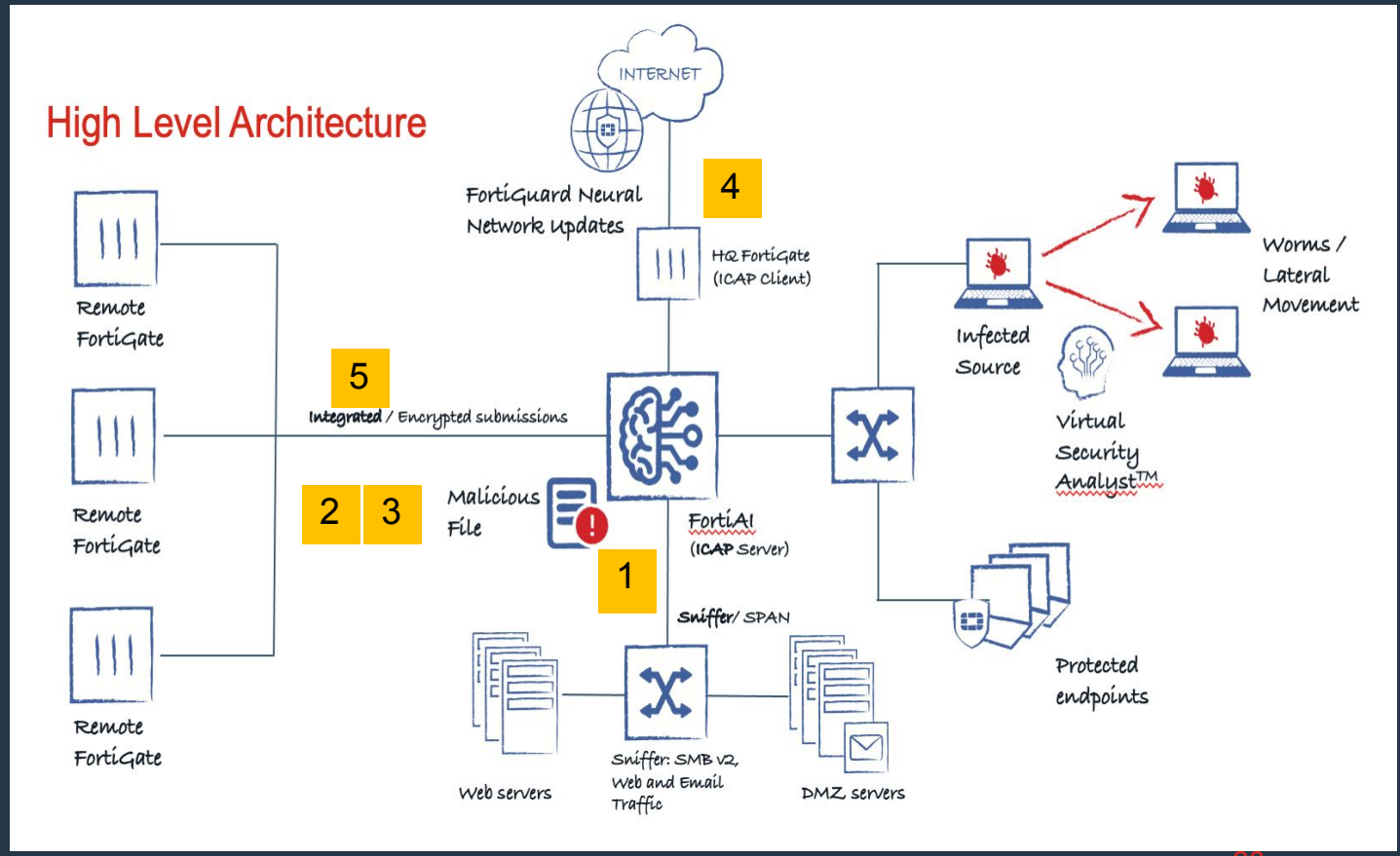
FortiAI 部署

佈署架構

- 無需 安裝/配備 端點軟體 (Agent)， 不需要 Internet 連線
- Syslog 結合 FAZ, 或是 FortiSIEM (結合SOC做資安事件回應)
- 多種模式 (10G 線速探勘流量)

偵測模式
  - 1. Sniffer (HTTP, Mail, FTP & SMB)
  - 2. 人工滙入
  - 3. API 自動滙入

線上即時阻斷模式
  - 4. ICAP Server (整合第三方Prxoy, WAF..)
  - 5. 透過 FortiGate 整合模式



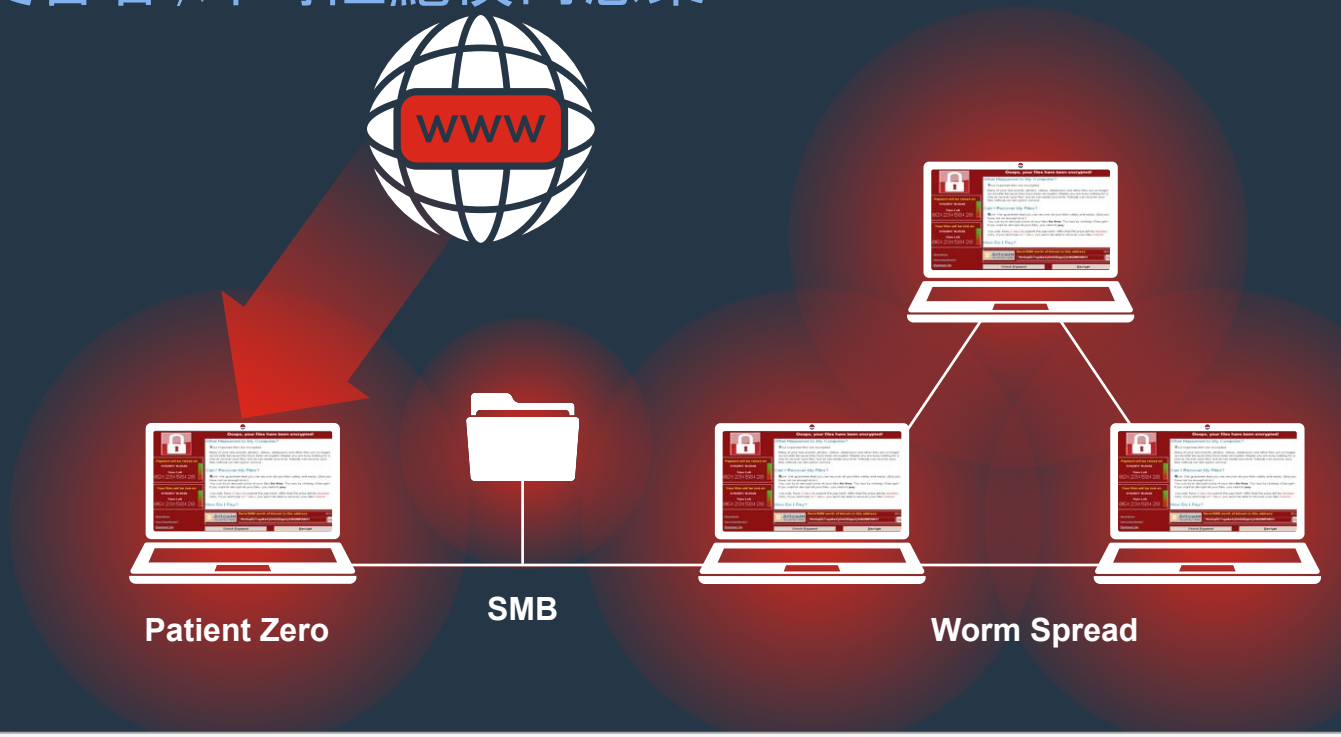
FortiAI Virtual Security Analyst ™ –

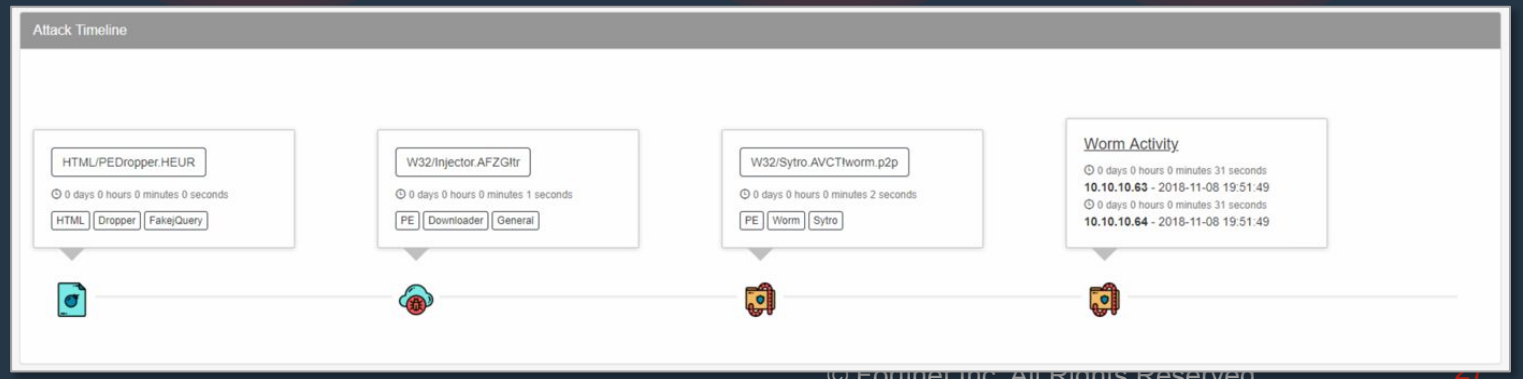
如何在第一時間找到第零號受害者;即時阻絕橫向感染

找到 “Patient Zero”

攻擊場境實例解析

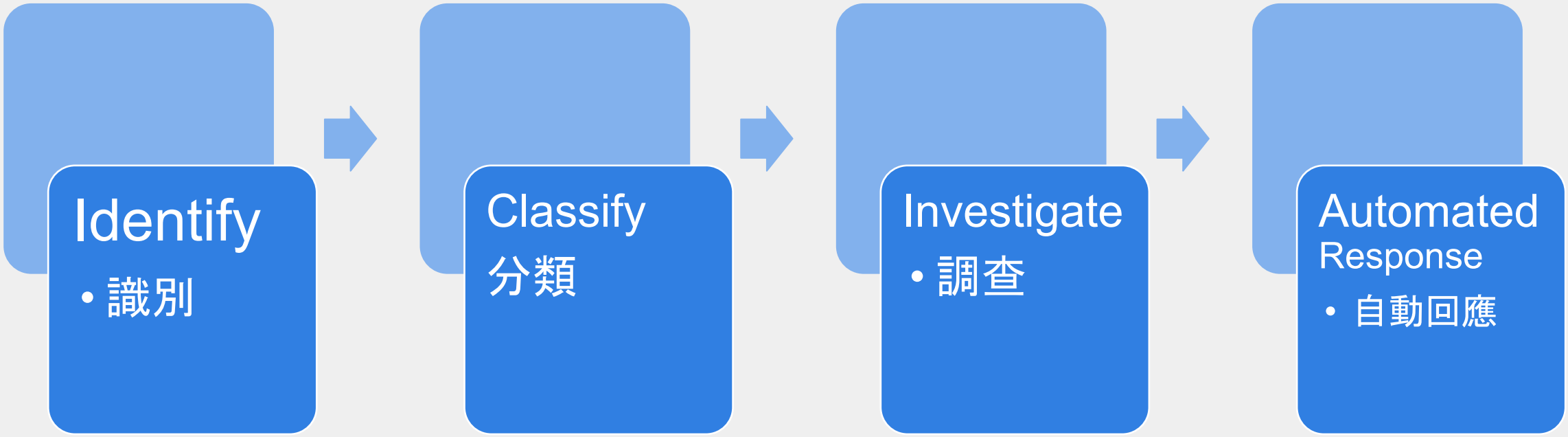
- 場景分析引擎, 即時做不同場景分類
- 次秒級的判讀和完整解析





完全地端，不需連網的次秒級資安威脅解決方案

自動完成 本地資安事件調查基本步驟

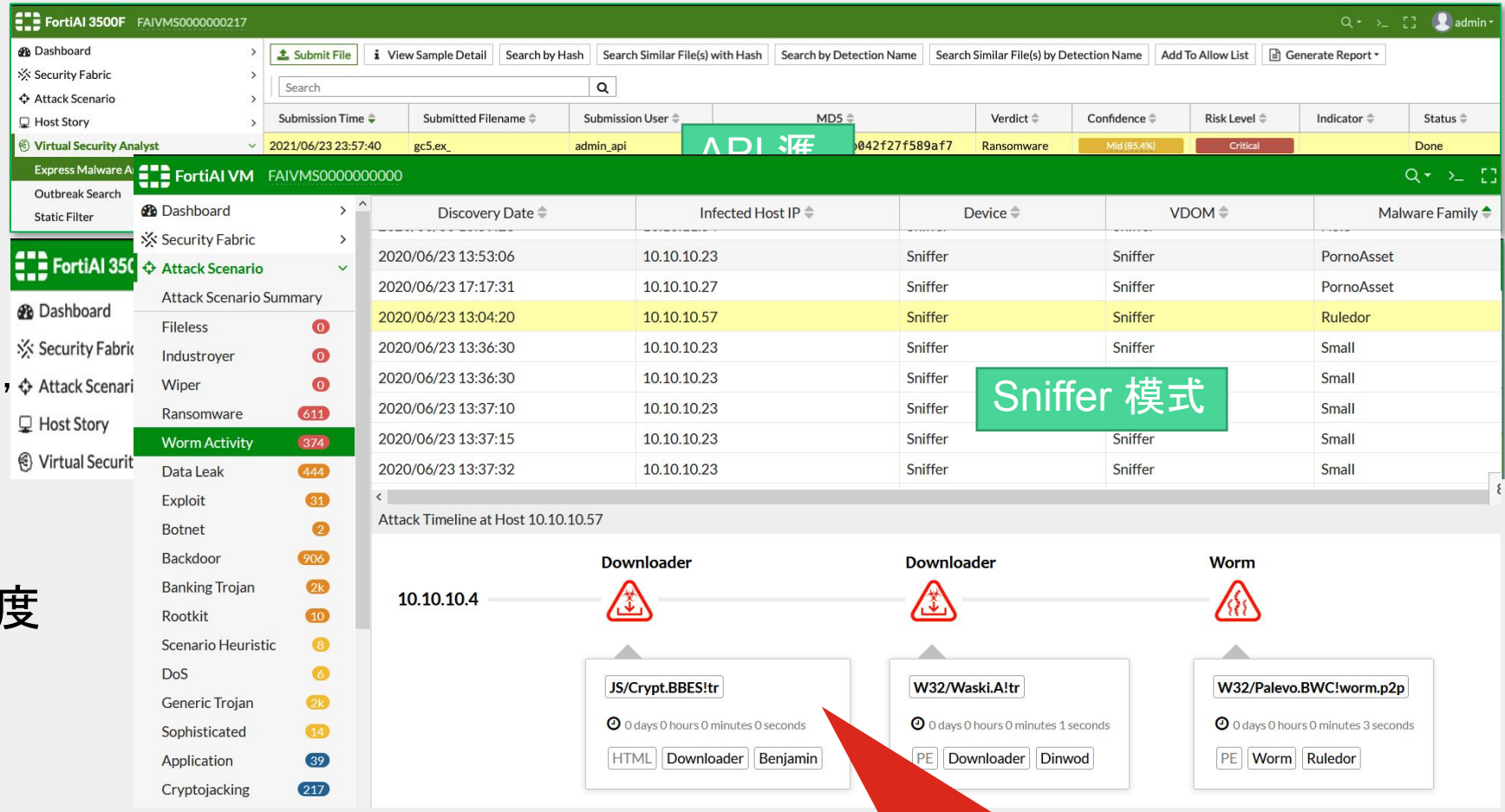


Virtual Security Analyst™ 運用類神經網路深度學習(DNN)進行 **identifies(識別)**, classifies(分類), and investigates(調查)精巧資安威脅 可完成次秒級的檢測和即時自動反應即時阻殺。

1

Identify(識別)
通過次秒級的檢測來破壞威脅，即時阻殺新的威脅。

解決
SecOps 正面臨威脅的數量，速度和複雜程度不斷提升



Virtual Security Analyst™ 運用類神經網路深度學習(DNN) 進行 identifies(識別), **classifies**(分類), and investigates(調查)精巧資安威脅 可完成次秒級的檢測和即時自動反應即時阻殺。

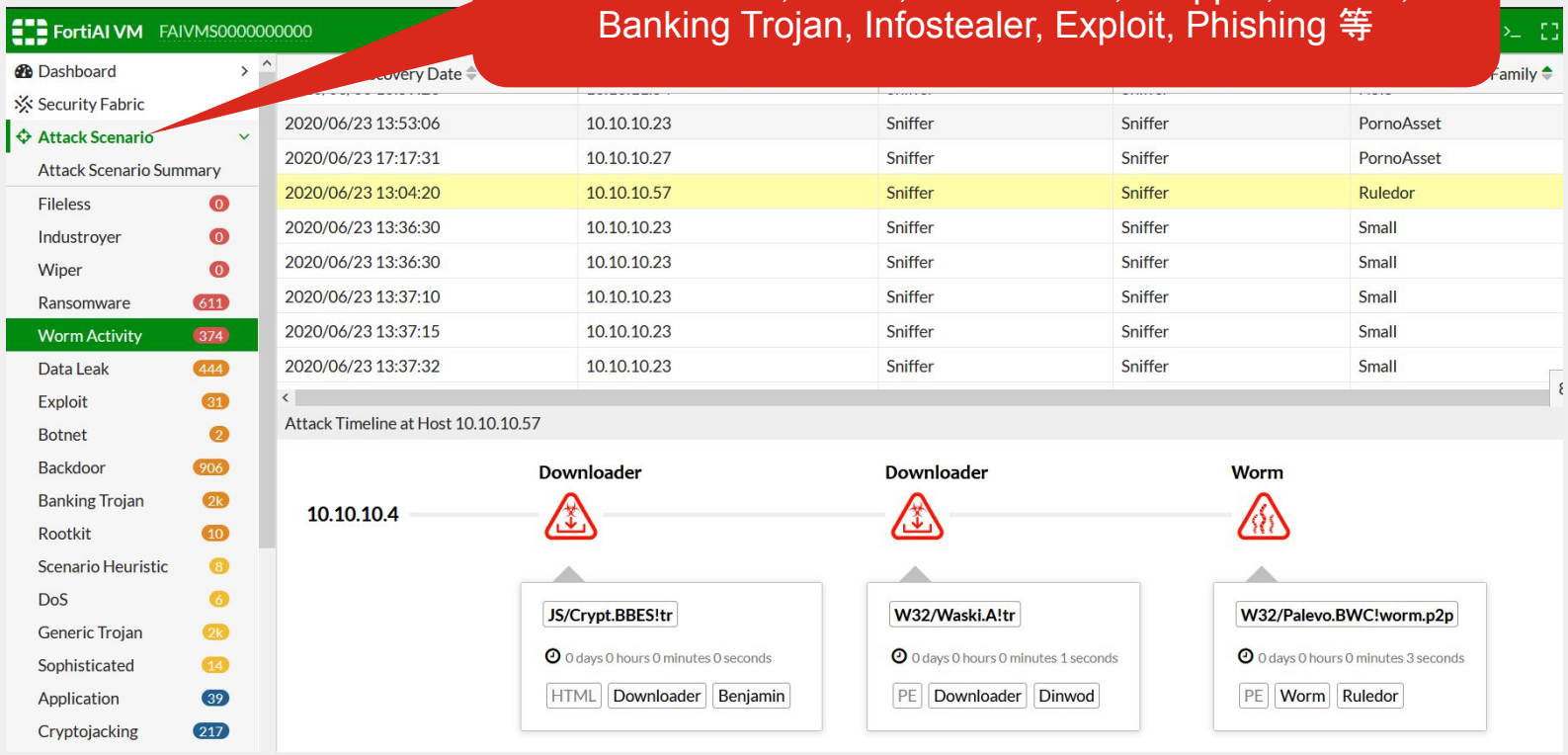
2 Classify（分類）

科學地分析IT和OT惡意軟體，以準確確定威脅的類型並減少誤報。

解決

偽裝惡意軟體會逃避安全控制並延長緩解措施。

Classify IT and OT threats: Industroyer, Wiper, Fileless, Ransomware, Worm, Downloader, Dropper, Rootkit, Banking Trojan, Infostealer, Exploit, Phishing 等



Virtual Security Analyst™ 運用類神經網路深度學習(DNN) 進行 **identifies(識別)**, classifies (分類), and investigates(調查)精巧資安威脅 可完成次秒級的檢測和即時自動反應即時阻殺

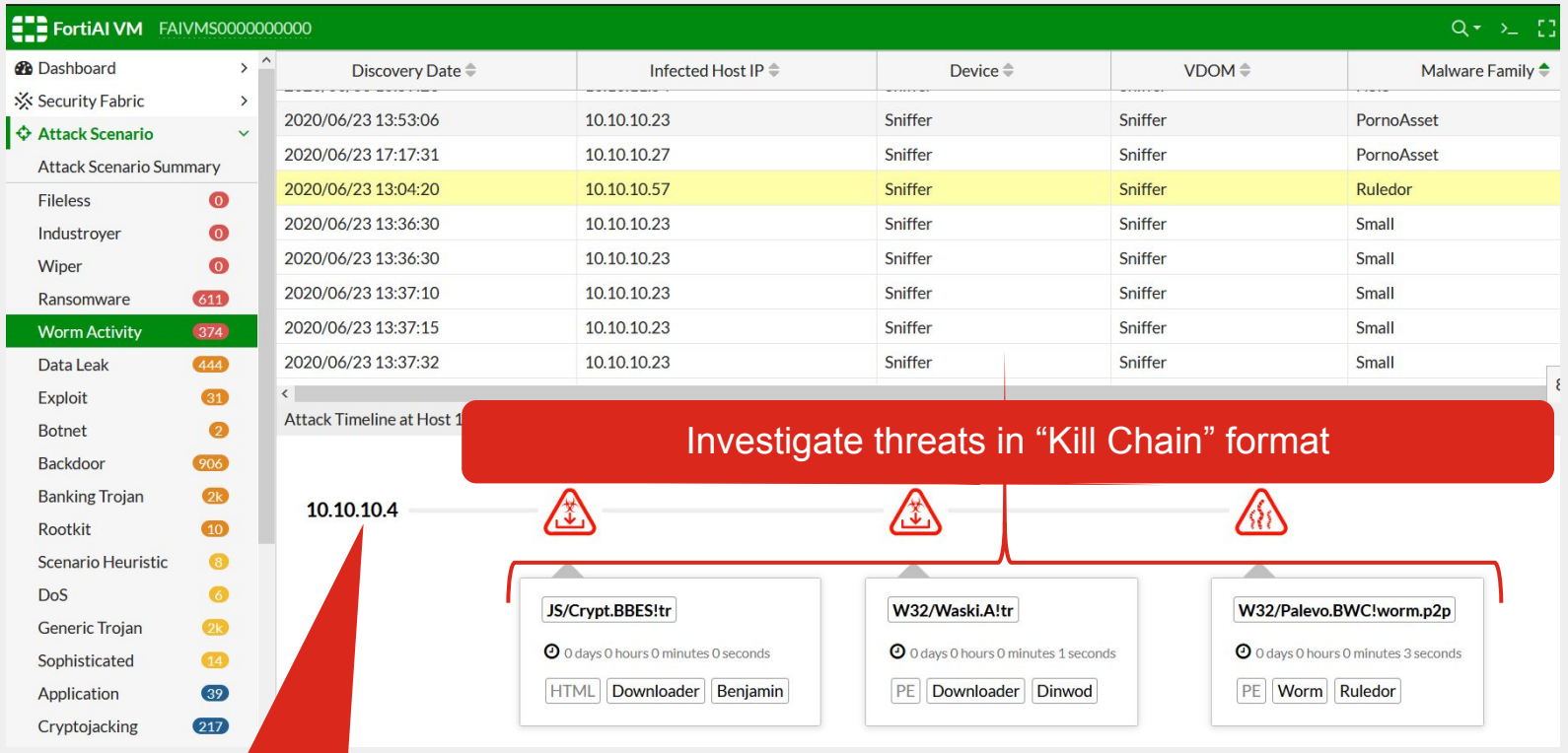
3

3 Investigate(調查)

通過分析整個威脅運動來加快調查速度，並實時識別零號患者和後續受害者.

解決

傳統緩慢的手動調查惡意軟體爆發/橫向傳播

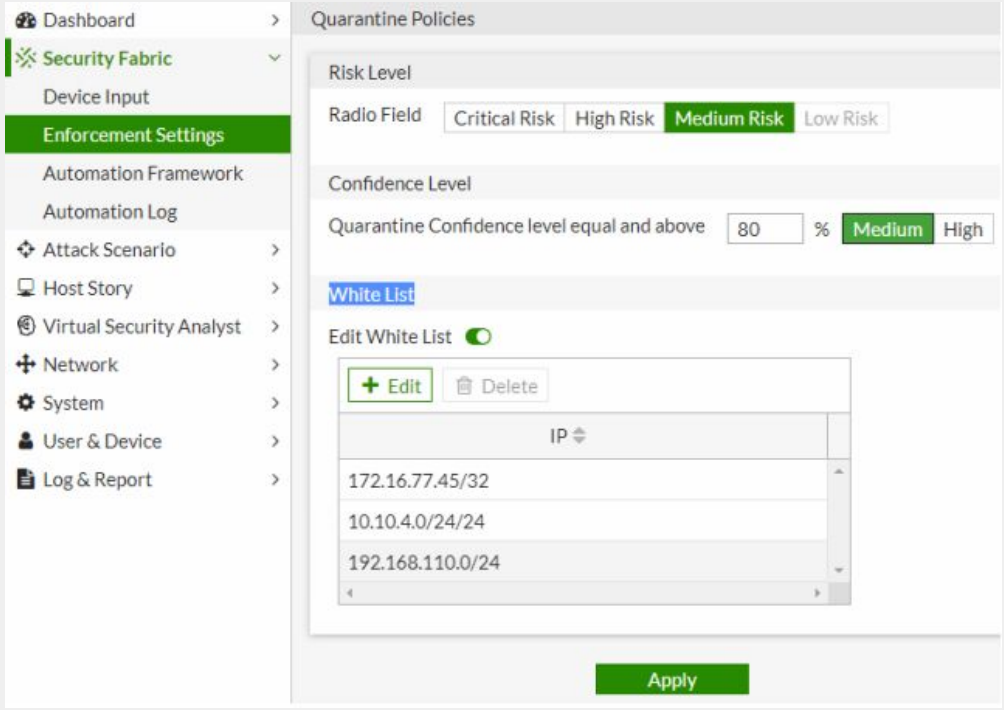


Virtual Security Analyst™ 運用類神經網路深度學習(DNN) 進行 identifies(識別), classifies (分類), and investigates(調查)精巧資安威脅 可完成次秒級的檢測和即時**自動反應**即時阻殺

4

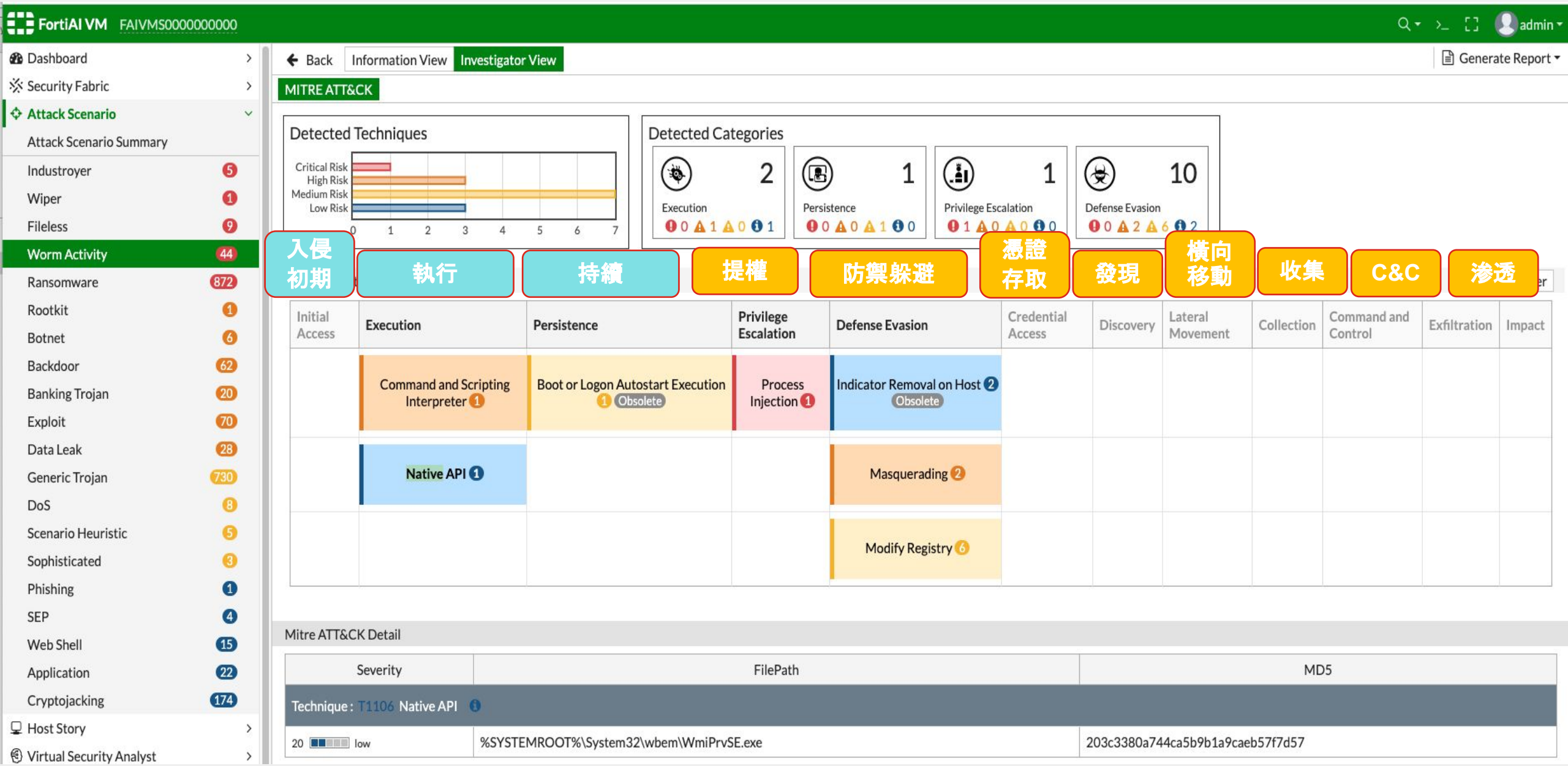
4 **Automated Response(自動反應)**
通過與FortiGate無縫整合，即時隔離網路中發現的這些威脅。

解決
結合 ICAP，FortiGate整合，SysLog
手動/自動緩解工作以應對持續的攻擊或爆發情況



FortiGate quarantine based on FortiAI risk & confidence levels

正視 Mitre ATT&CK 資安框架 – 了解網路活動



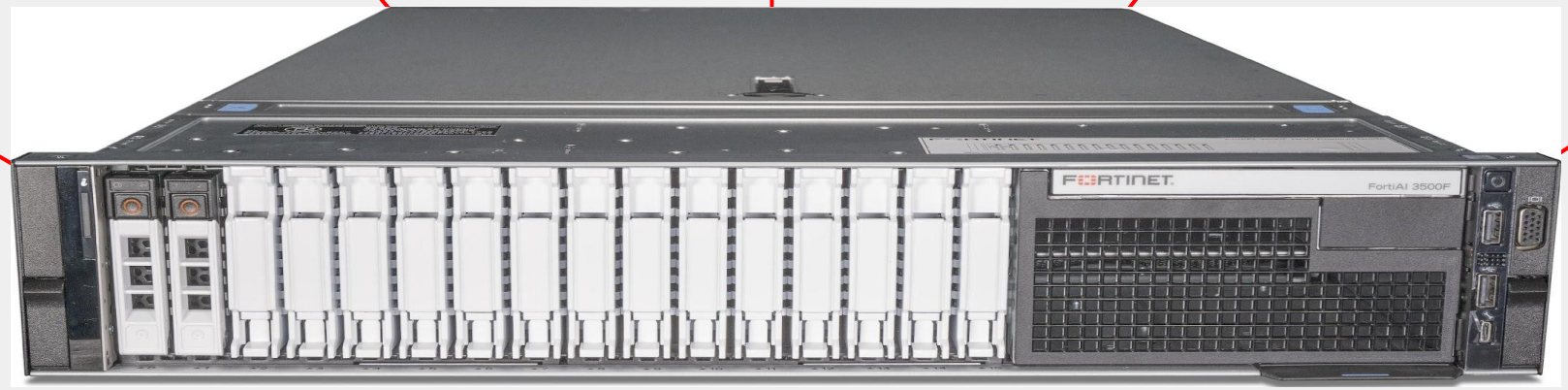
FortiAI 系列

專利
Self-Learning Model

8+
years
Mature AI

<100 ms
Sub-second Investigation

6+ million
malware
features



10G
Network
Throughput

	ForitAI-3500F	FortiAI-VM16	FortiAI-VM32
Appliance/ VM support	硬體式(2RU)	16vCPU(VM)/128GB ~ 256GB ESXi 6.7 U2+	32vCPU(VM)/128GB ~ 256GB ESXi 6.7 U2+
協定支援	HTTP, SMB,SMTP, POP3, IMAP, MAPI, and FTP	HTTP, SMB,SMTP, POP3, IMAP, MAPI, and FTP	HTTP, SMB,SMTP, POP3, IMAP, MAPI, and FTP
效能	100,000 檔案/小時 次秒級檢測	14,000 檔案/小時 次秒級檢測	22,000 檔案/小時 次秒級檢測
Interfaces	2 x 10GE RJ45 (10/100/1000), 1 x GE RJ45 , 1 x RJ45 Console	使用者自定義	使用者自定義
Storage Capacity	7.68 TB(2 x 3.84 TB HDD)	1TB to 8TB	1TB to 8TB


FORTINET