



FORTINET[®]

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）

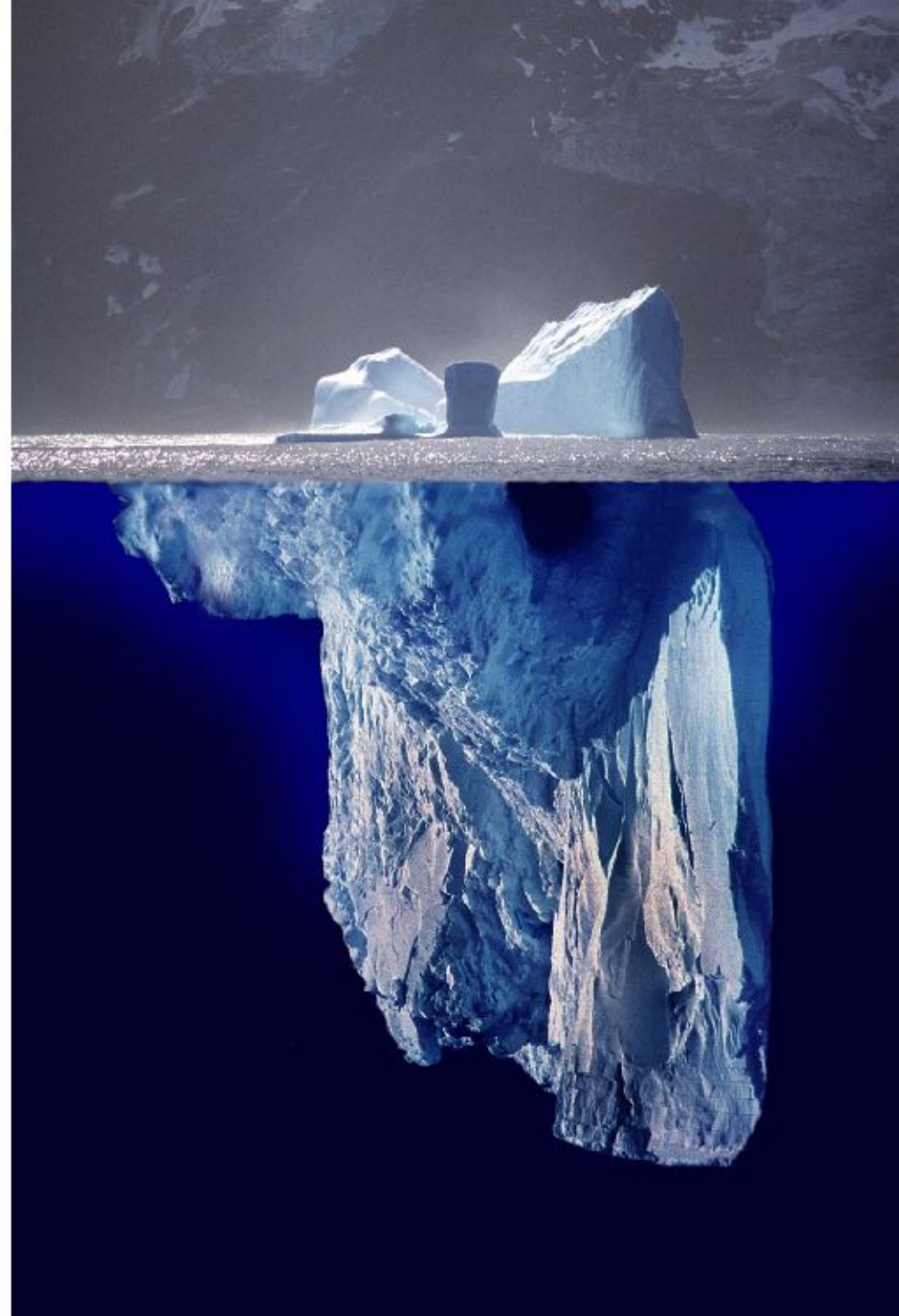
傳駭客勒索14億 廣達證實遭攻擊不影響營運



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

2



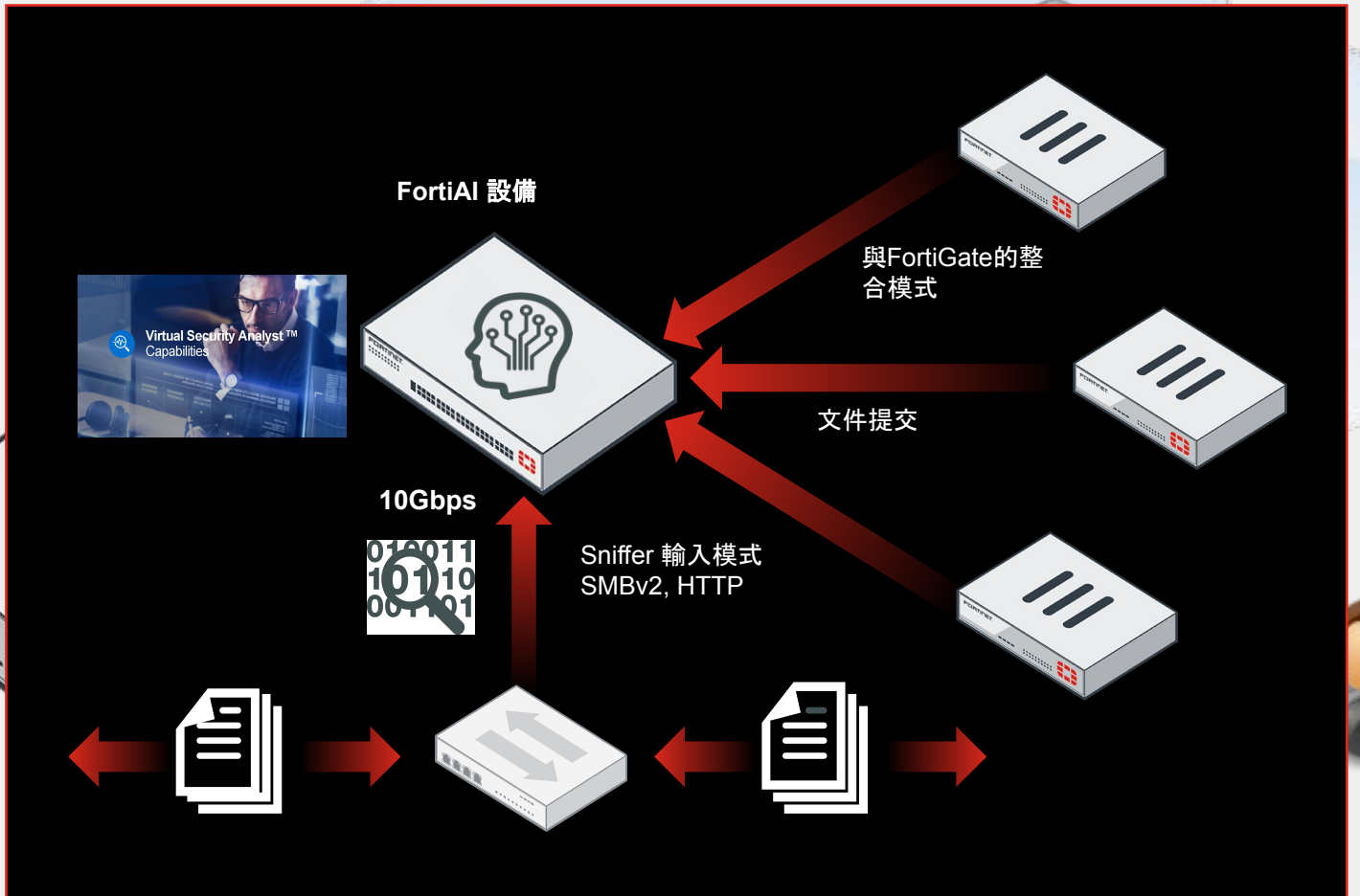
3



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



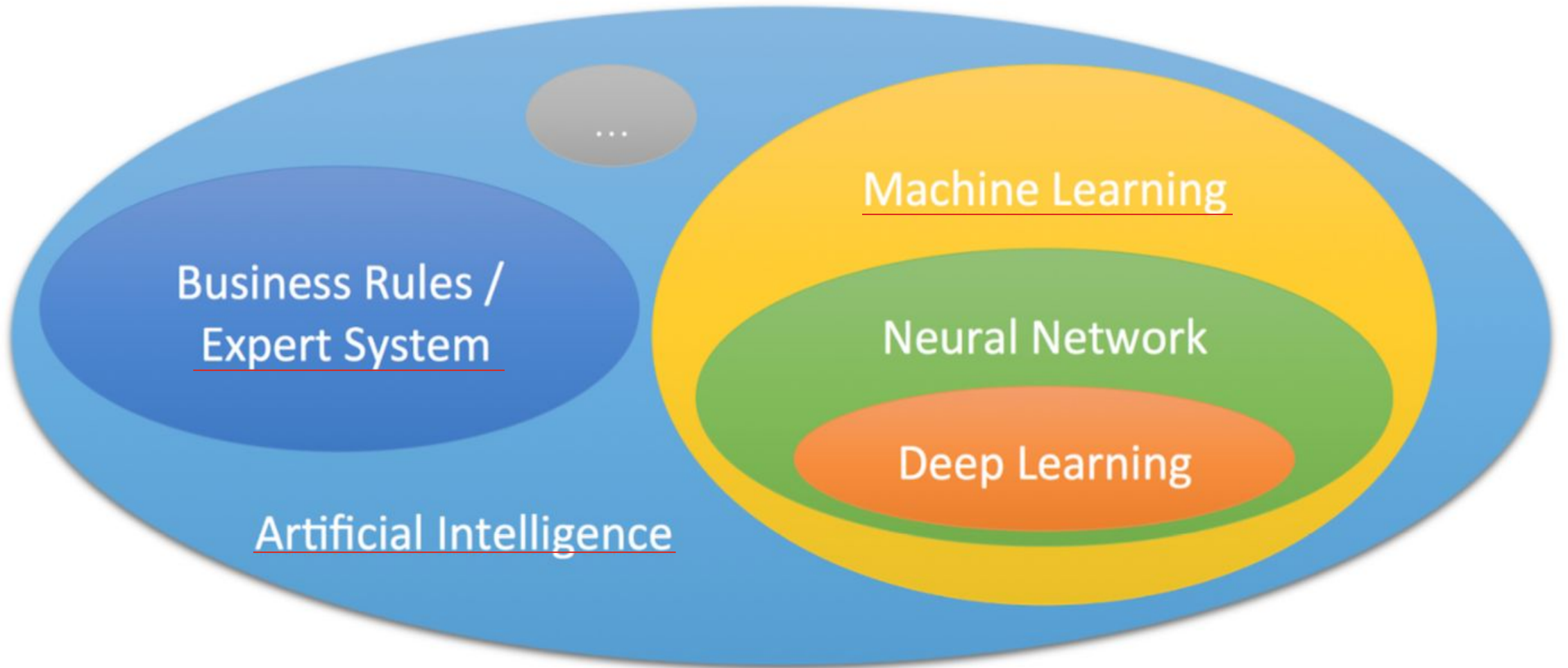


淺談【人工智慧】及【機器學習】



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



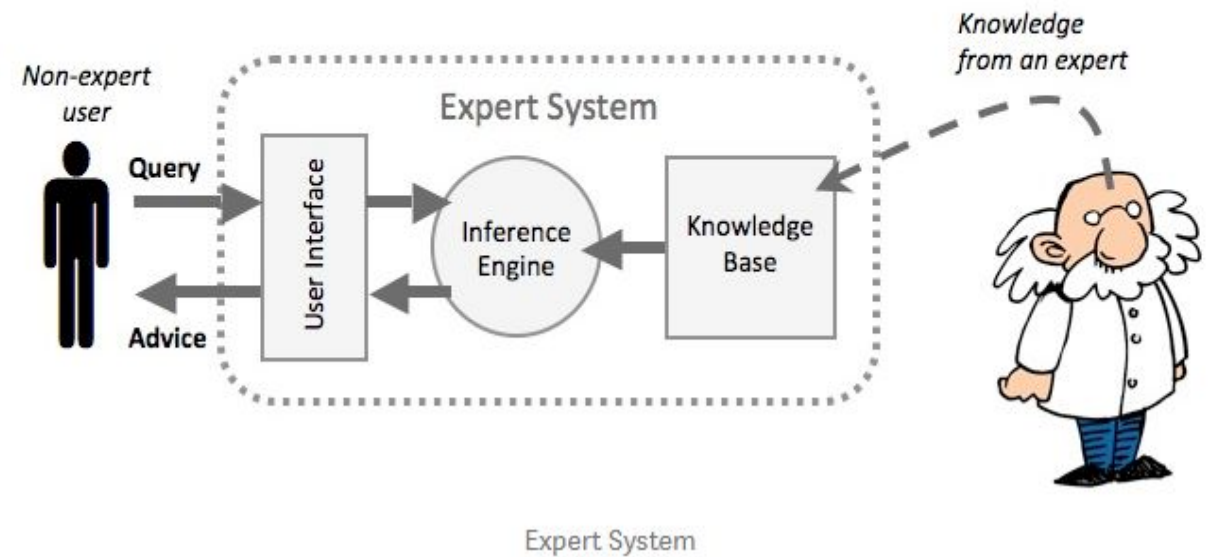
專家系統 — 人工給定的經驗法則

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)

Expert Systems



Machine Learning – 自我演繹, 自我調整

機器學習的盲點和優勢

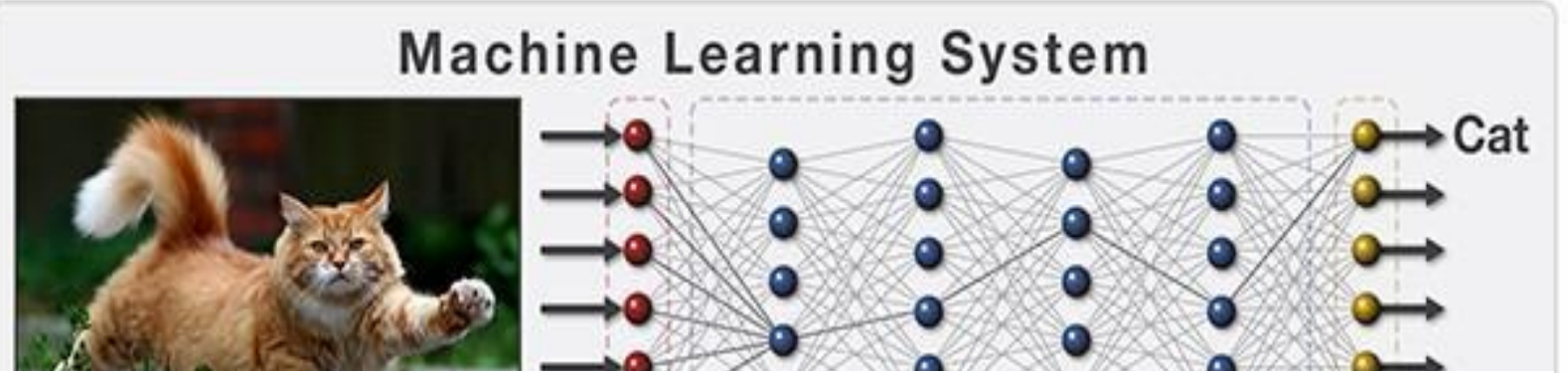
老虎



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

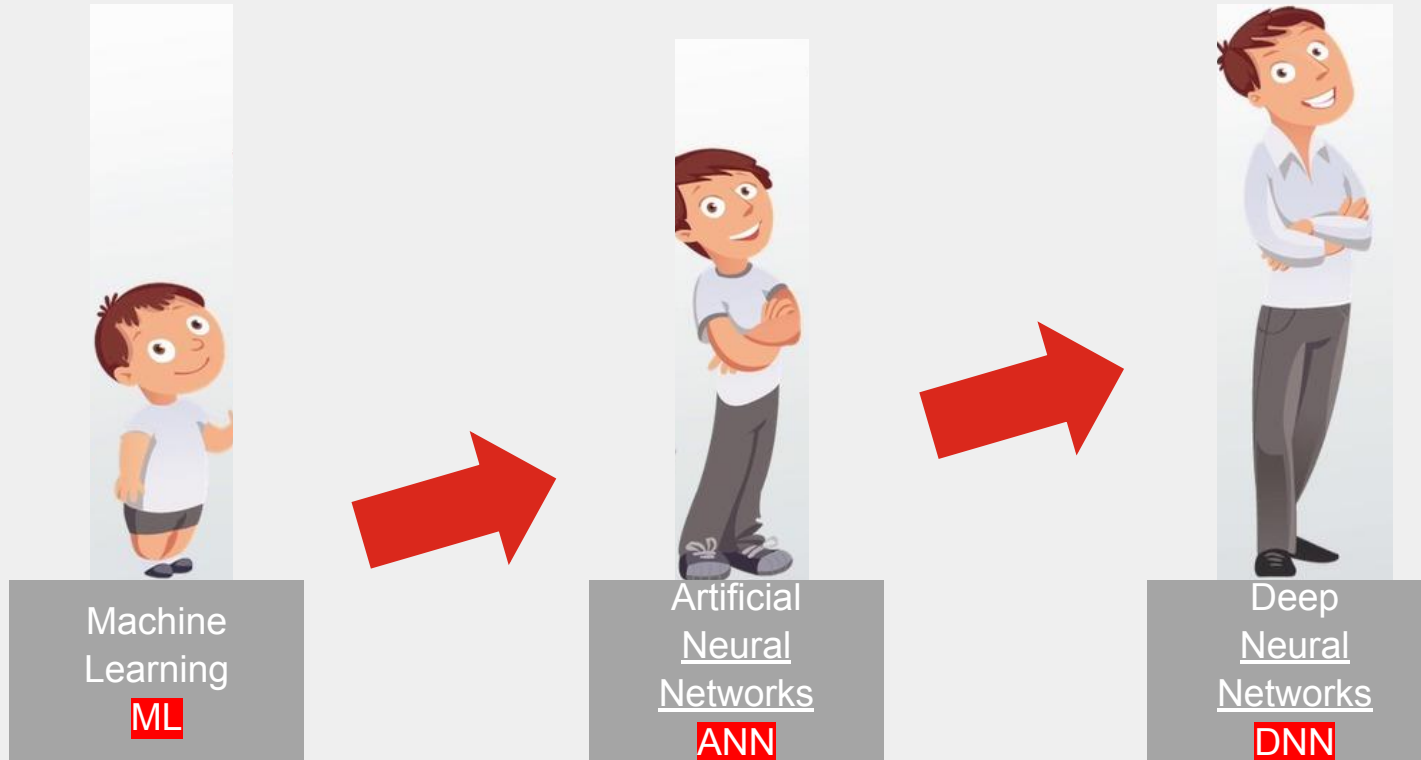


盲人摸象的啟發

AI: 學習機器的成熟度

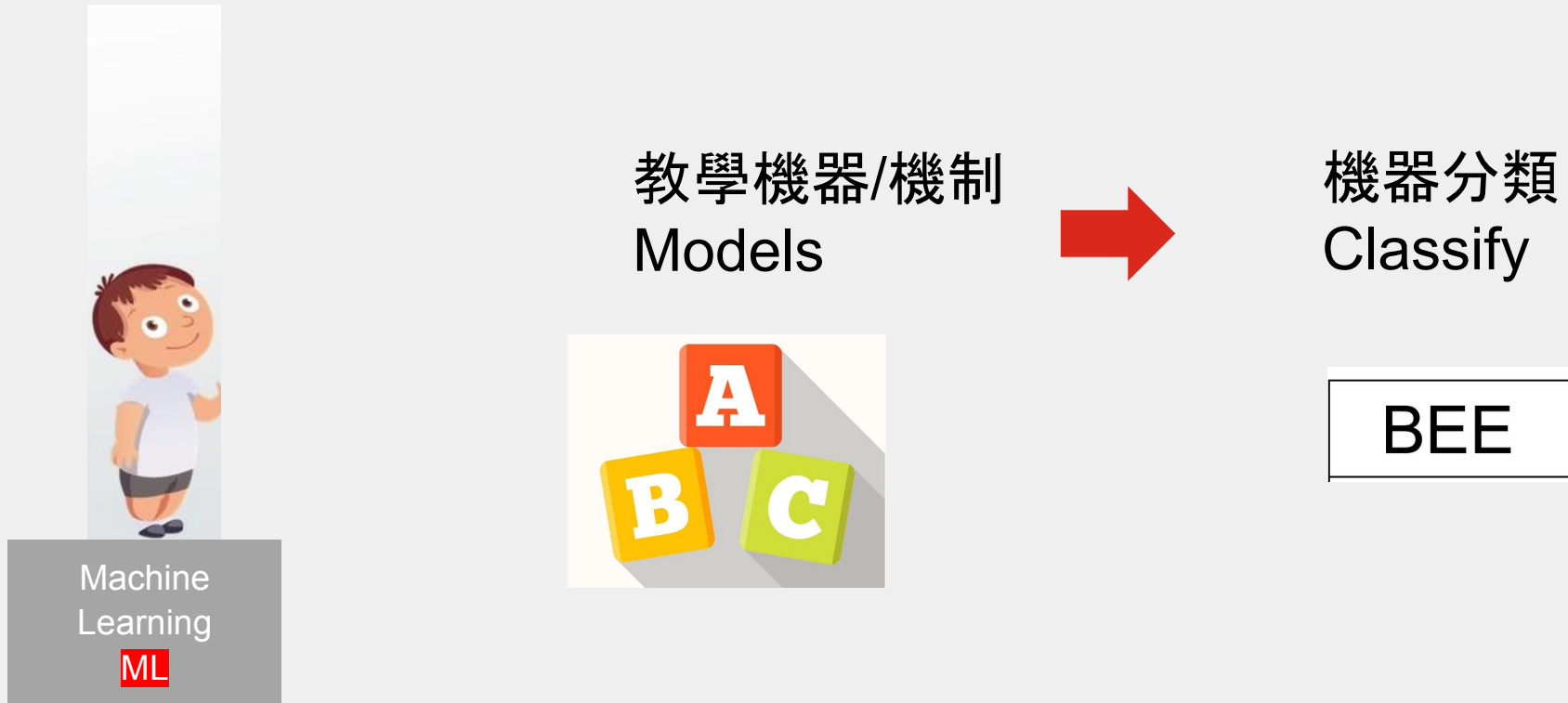
學習機器的種類大大影響學習能力

MODELS



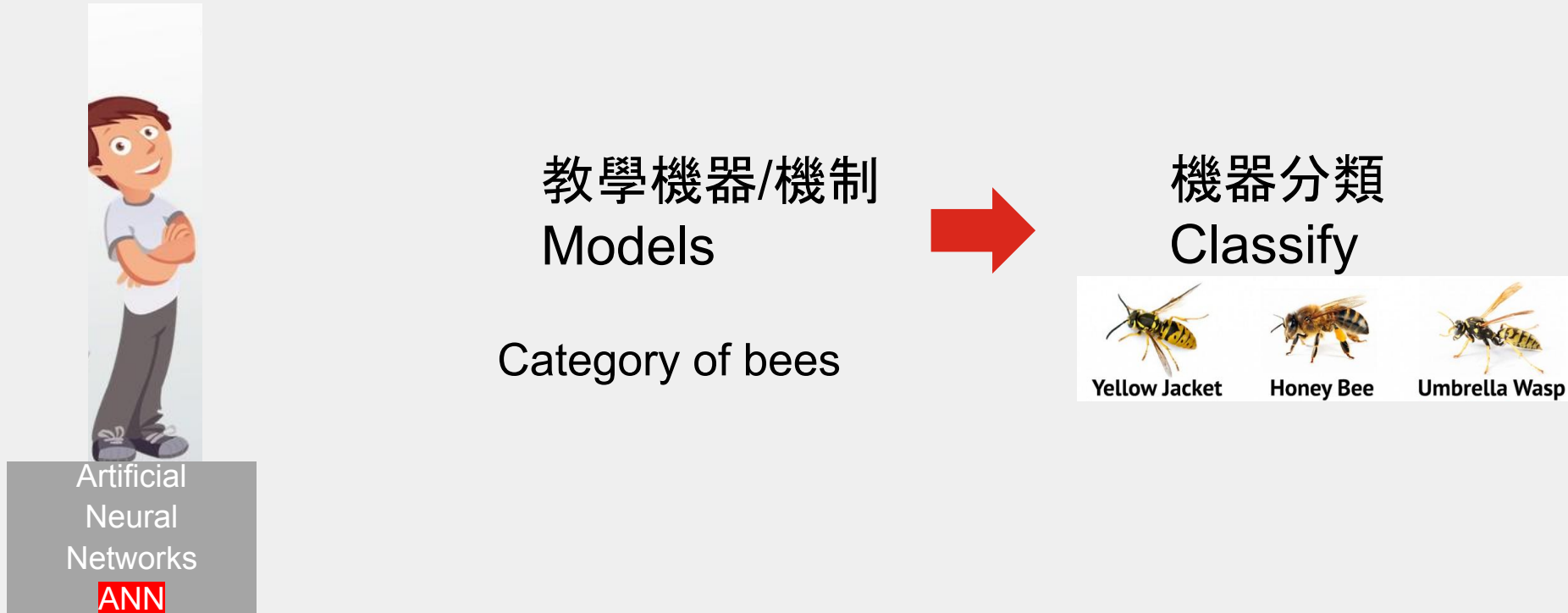
AI: Machine Learning

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



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。



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



教學機器/機制
Models

ANN #1

蜜蜂分類



Yellow Jacket

Honey Bee

Umbrella Wasp

ANN #2

時辰:
9am vs 9pm



ANN #3

鄉村 vs 都市

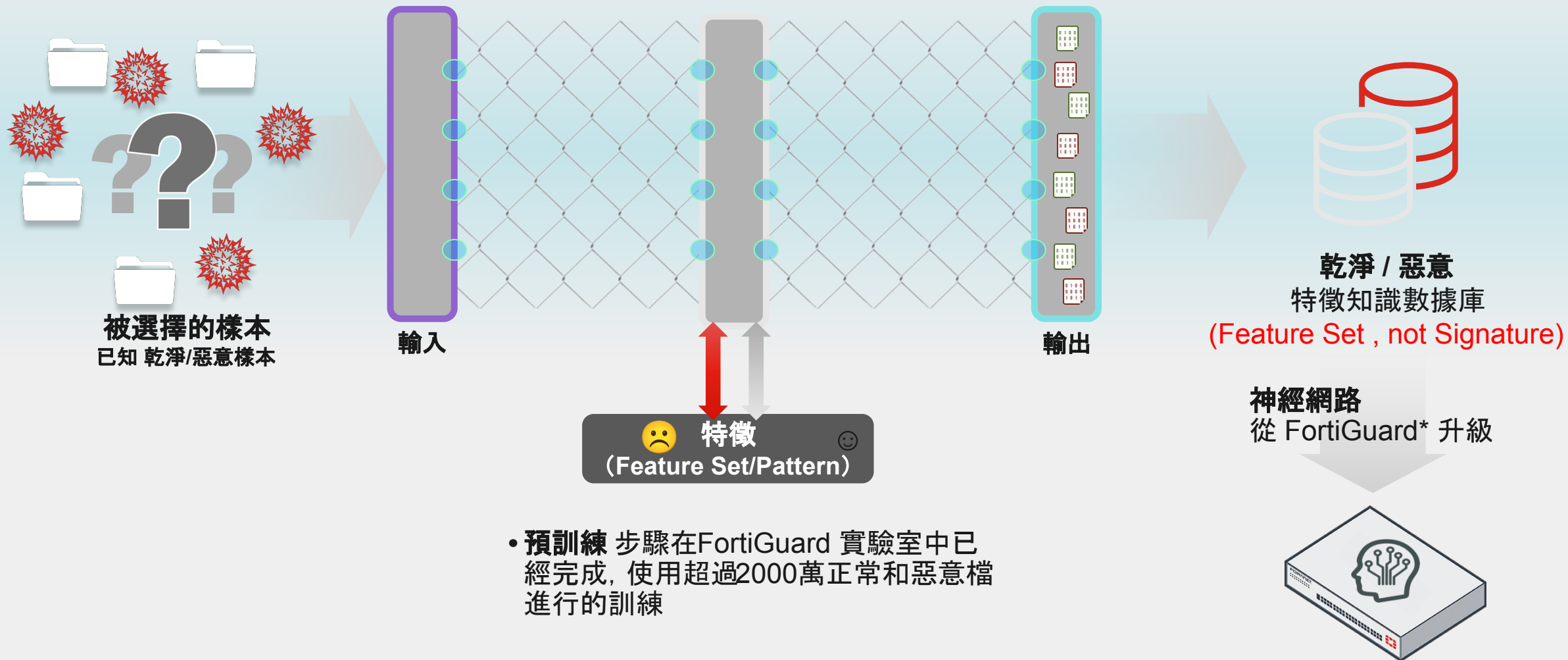


機器解譯



蜜蜂
在早上10:00,
在田野間,
停留在花上採蜜

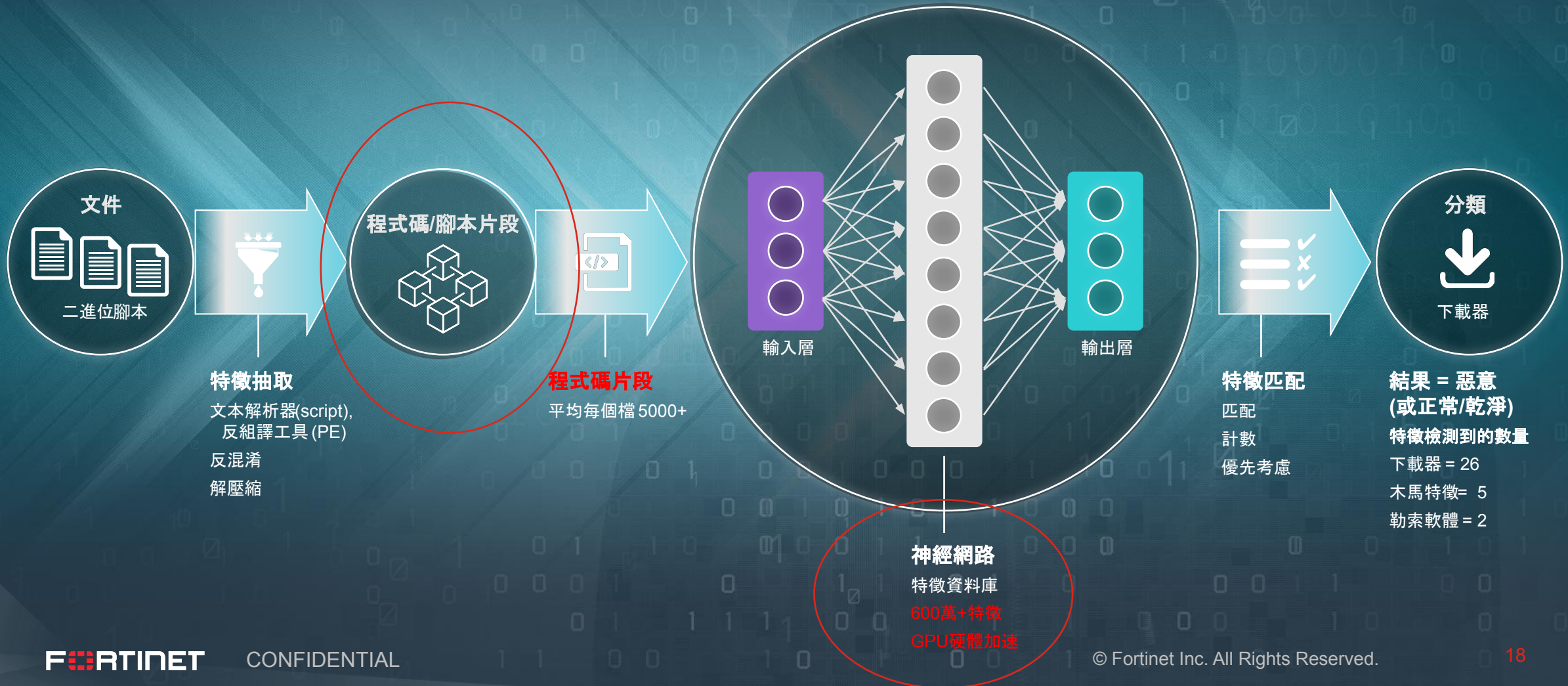
FortiAI 出廠前預訓練



- 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 workflow (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™ (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)



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-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

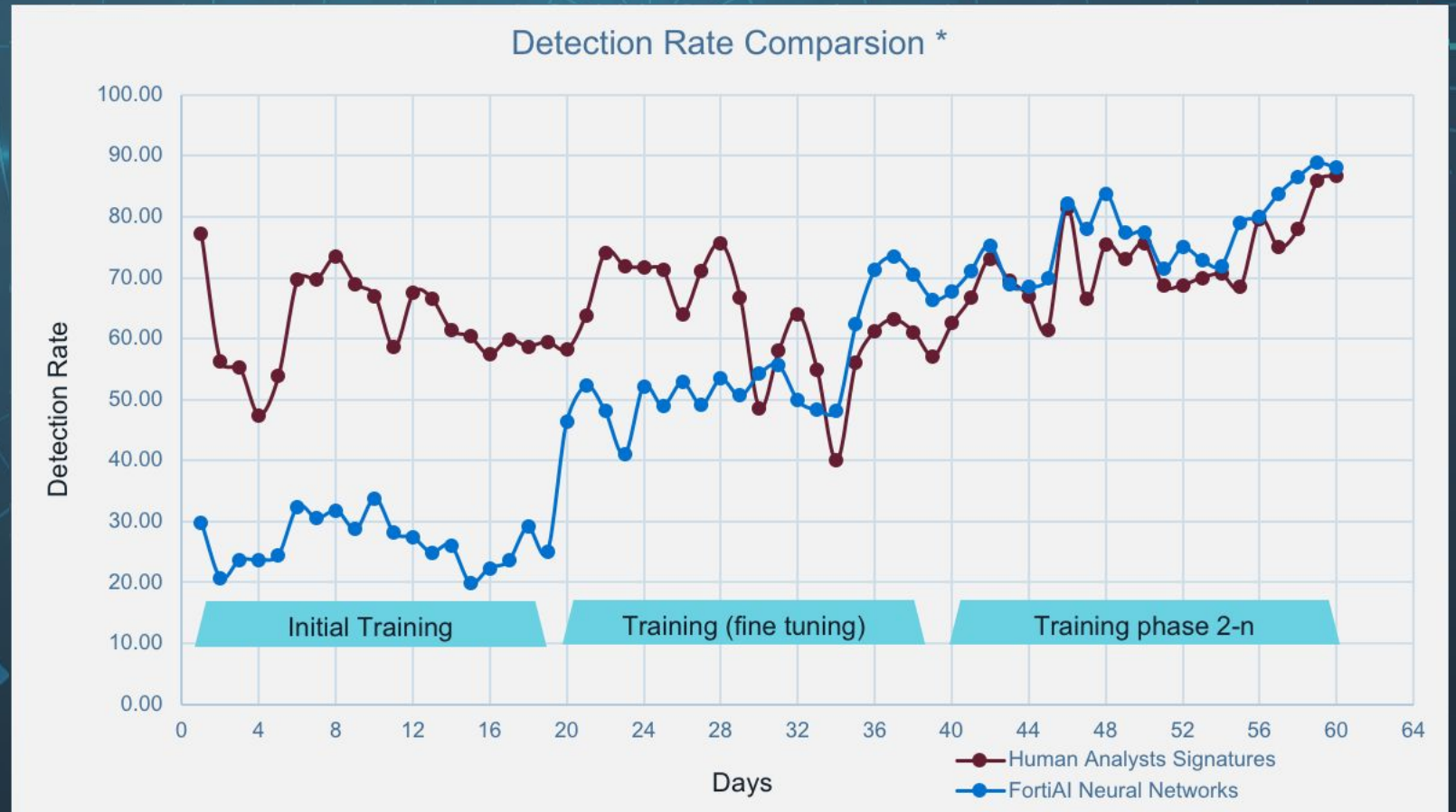
● FortiGuard 升級

ANN 升級

與最新威脅保持同步

● 未來學習

在客戶現場完成





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

The screenshot displays the FortiAI Attack Scenario interface. On the left, a sidebar lists various attack scenarios with their respective counts and severity levels. The main area is divided into two sections: 'Worm Activity' and 'Attack Timeline'.

Worm Activity Section:

根據攻擊場景進行分類 / 檢測出的類別

Host IP	Attack Name	Identified date
172.17.45.105	Generic	Mar 27, 2019 8:16:57 AM
172.16.92.175	Generic	Mar 24, 2019 12:39:57 PM
172.16.92.175	Generic	Mar 22, 2019 11:32:46 AM
172.16.92.175	Generic	Mar 21, 2019 10:45:17 PM
172.17.45.105	Generic	Mar 21, 2019 6:44:32 PM
10.10.10.56	Generic	Feb 12, 2019 11:13:41 PM
10.10.10.51	Generic	Jan 10, 2019 5:40:51 AM
10.10.10.53	Generic	Jan 6, 2019 12:43:00 AM
10.10.10.57	Generic	Jan 5, 2019 1:24:56 AM
10.10.10.52	Generic	Jan 4, 2019 1:52:27 PM
10.10.10.53	Generic	

受感染 IP : 172.16.92.175

Attack Timeline Section:

Downloader (通過 HTML), Dropper (2 秒後), 檢測到 Worm (3 秒後)
Note: 實際中可能是幾天或幾周

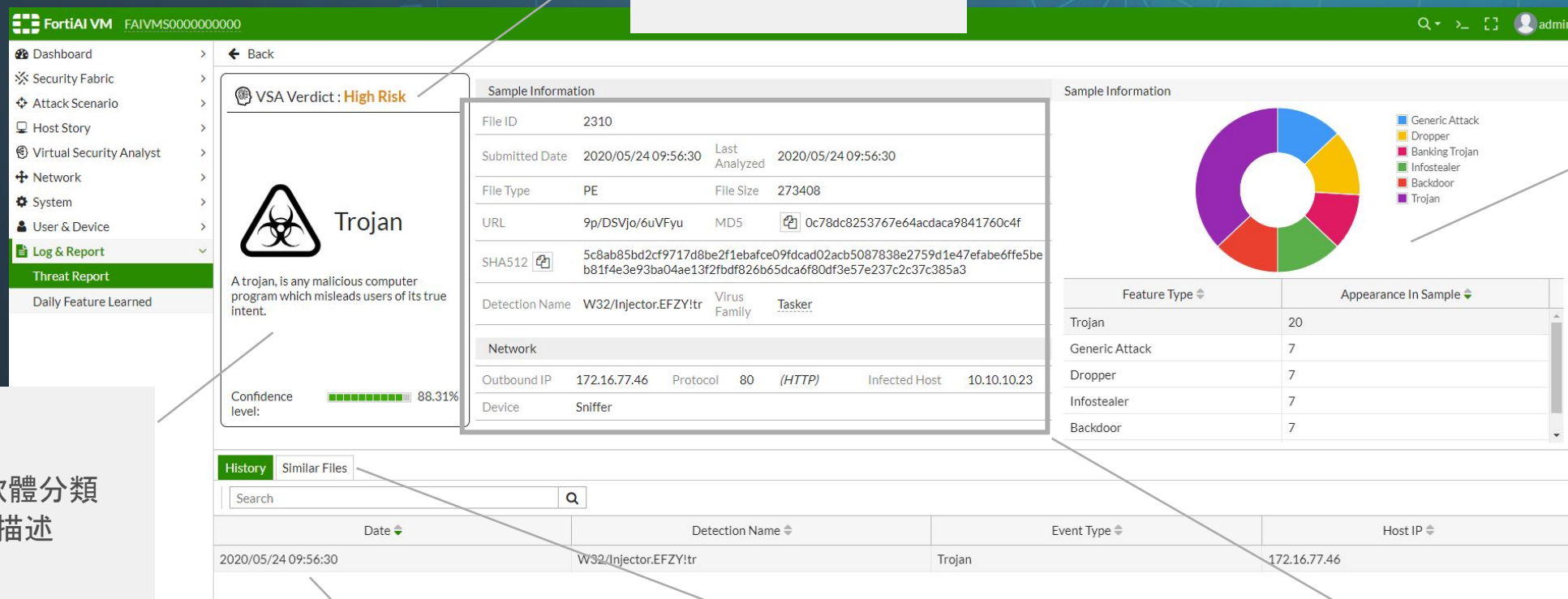
Worm傳播到 172.17.45.105

The Attack Timeline shows a sequence of events: 1. JS/Shadraem.Altr.dldr (HTML, Downloader, Shadraem) at 00:00:00. 2. W32/EncPk.AC0ltr (PE, Downloader, Small) at 00:00:02. 3. W32/Adurk.A@mm (PE, Worm, Ardurk) at 00:00:03. 4. Worm Activity (172.17.45.105 - 2019-03-21 22:32:46) at 00:00:19.



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

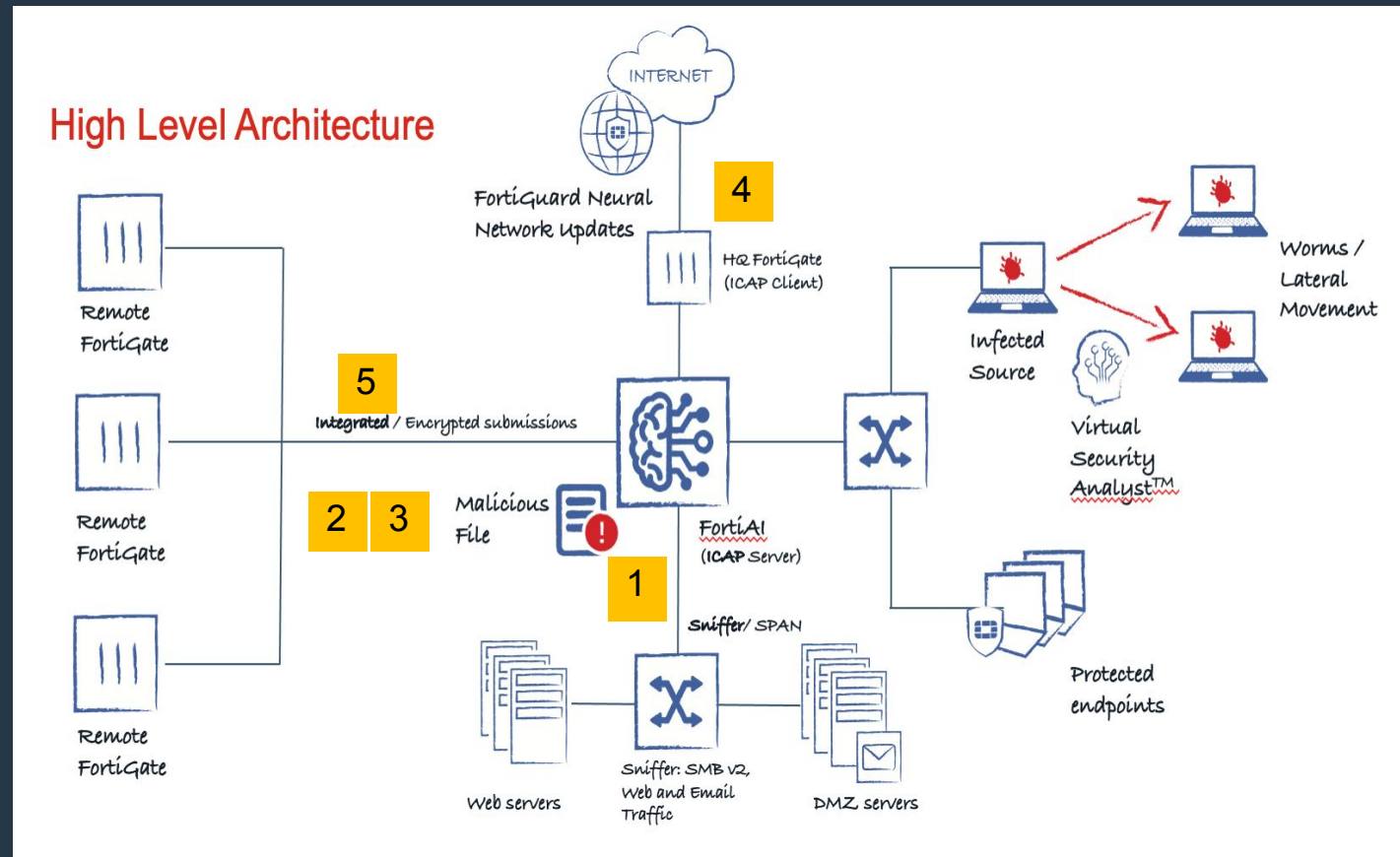
- 無需安裝/配備端點軟體 (Agent)，不需要 Internet 連線
- Syslog 結合 FAZ, 或是 FortiSIEM (結合SOC做資安事件回應)
- 多種模式 (10G 線速探勘流量)

偵測模式

- 1. Sniffer (HTTP, Mail, FTP & SMB)
- 2. 人工匯入
- 3. API 自動匯入

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

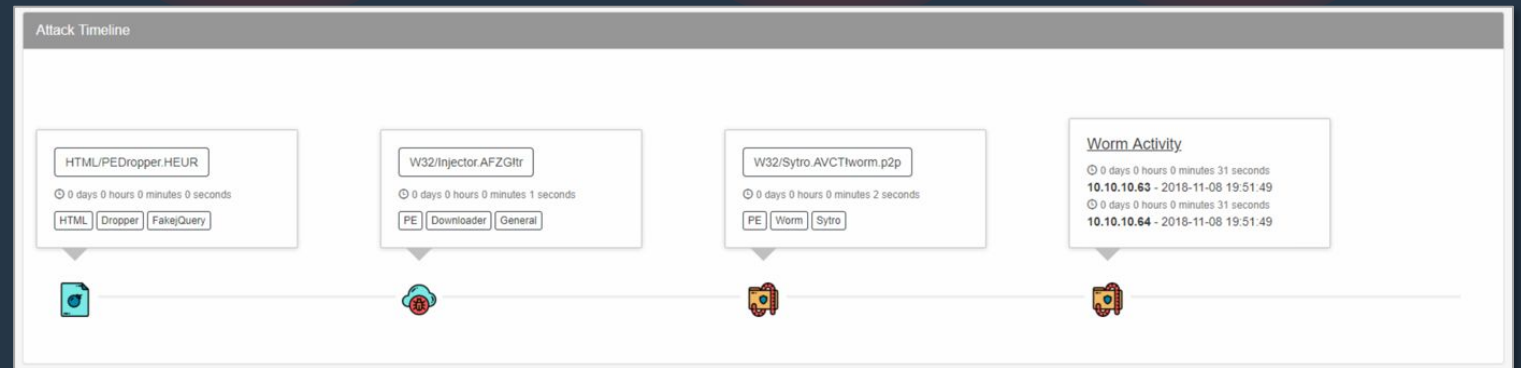
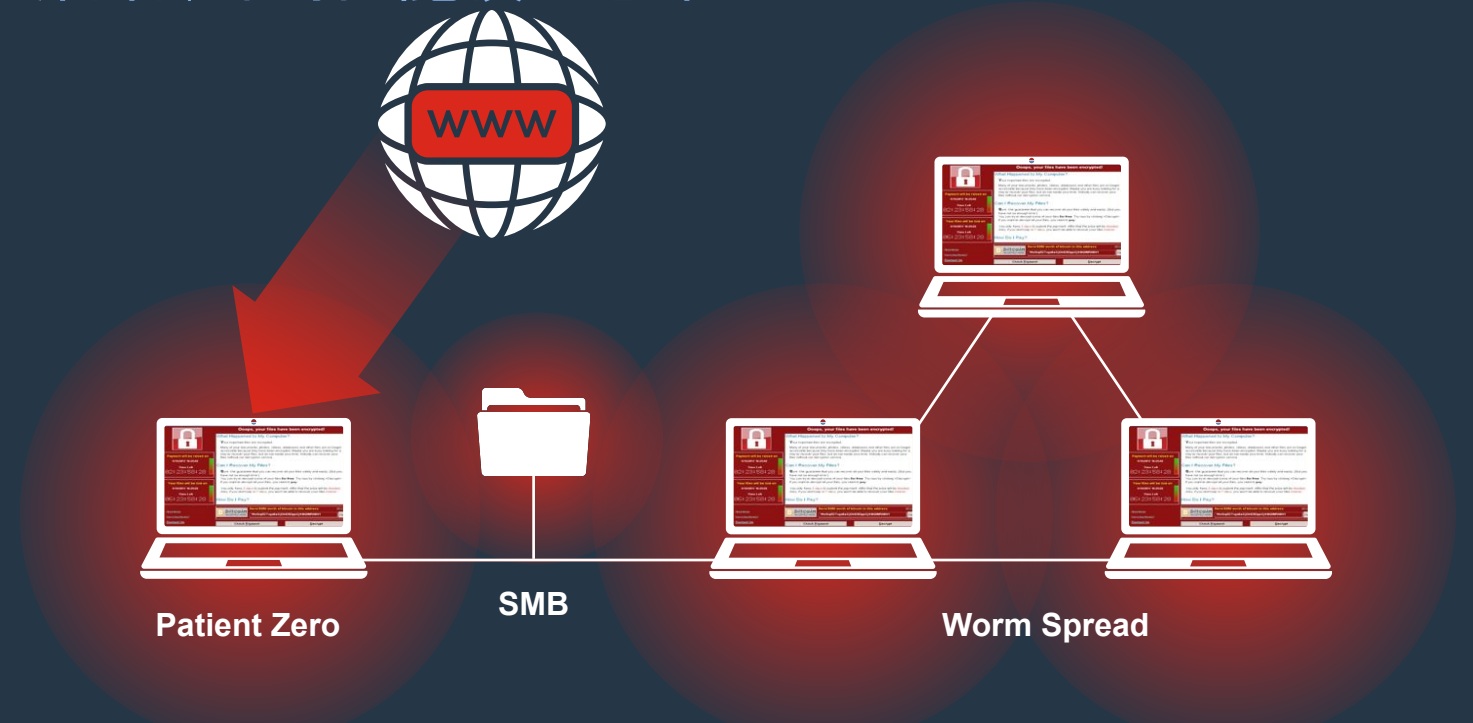


FortiAI Virtual Security Analyst™ –

如何在第一時間找到第零號受害者;即時阻絕橫向感染

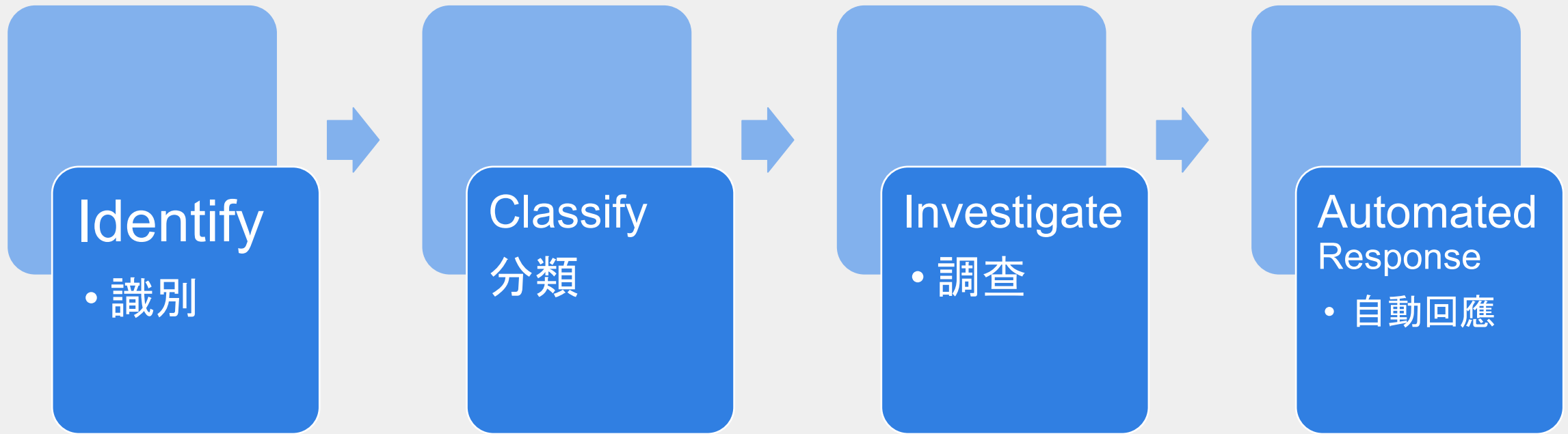
找到“Patient Zero” 攻擊場境實例解析

- 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

The screenshot displays the FortiAI 3500F interface with a table of threat detection results. A green box highlights the 'Sniffer 模式' (Sniffer Mode) in the table. Below the table, an 'Attack Timeline at Host 10.10.10.57' shows three events: a Downloader (JS/Crypt.BBES!tr), another Downloader (W32/Waski.A!tr), and a Worm (W32/Palevo.BWC!worm.p2p).

Discovery Date	Infected Host IP	Device	VDOM	Malware Family
2020/06/23 13:53:06	10.10.10.23	Sniffer	Sniffer	PornoAsset
2020/06/23 17:17:31	10.10.10.27	Sniffer	Sniffer	PornoAsset
2020/06/23 13:04:20	10.10.10.57	Sniffer	Sniffer	Ruledor
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:10	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:15	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:32	10.10.10.23	Sniffer	Sniffer	Small

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

Identify 次秒內識別威脅





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

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

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。

The screenshot displays the FortiAI VM interface. On the left is a navigation menu with categories like Dashboard, Security Fabric, Attack Scenario, Fileless, Industroyer, Wiper, Ransomware, Worm Activity, Data Leak, Exploit, Botnet, Backdoor, Banking Trojan, Rootkit, Scenario Heuristic, DoS, Generic Trojan, Sophisticated, Application, and Cryptojacking. The main area shows an 'Attack Scenario Summary' table with columns for Time, IP, and Threat Type. A red callout box points to a specific entry in the table. Below the table is an 'Attack Timeline at Host 10.10.10.57' showing a sequence of events: a Downloader (JS/Crypt.BBES!tr) at 10:10:10.4, another Downloader (W32/Waski.A!tr) at 10:10:10.5, and a Worm (W32/Palevo.BWC!worm.p2p) at 10:10:10.6. Each event includes a duration and associated tags like HTML, Downloader, Benjamin, PE, Dinwod, Worm, and Ruledor.

Time	IP	Threat Type	Family
2020/06/23 13:53:06	10.10.10.23	Sniffer	PornoAsset
2020/06/23 17:17:31	10.10.10.27	Sniffer	PornoAsset
2020/06/23 13:04:20	10.10.10.57	Sniffer	Ruledor
2020/06/23 13:36:30	10.10.10.23	Sniffer	Small
2020/06/23 13:36:30	10.10.10.23	Sniffer	Small
2020/06/23 13:37:10	10.10.10.23	Sniffer	Small
2020/06/23 13:37:15	10.10.10.23	Sniffer	Small
2020/06/23 13:37:32	10.10.10.23	Sniffer	Small





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

Discovery Date	Infected Host IP	Device	VDOM	Malware Family
2020/06/23 13:53:06	10.10.10.23	Sniffer	Sniffer	PornoAsset
2020/06/23 17:17:31	10.10.10.27	Sniffer	Sniffer	PornoAsset
2020/06/23 13:04:20	10.10.10.57	Sniffer	Sniffer	Ruleдор
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:36:30	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:10	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:15	10.10.10.23	Sniffer	Sniffer	Small
2020/06/23 13:37:32	10.10.10.23	Sniffer	Sniffer	Small

Attack Timeline at Host 10.10.10.4

Investigate threats in "Kill Chain" format

- JS/Crypt.BBES!tr (HTML, Downloader, Benjamin) - 0 days 0 hours 0 minutes 0 seconds
- W32/Waski.A!tr (PE, Downloader, Dinwod) - 0 days 0 hours 0 minutes 1 seconds
- W32/Palevo.BWC!worm.p2p (PE, Worm, Ruleдор) - 0 days 0 hours 0 minutes 3 seconds

Identify patient-zero





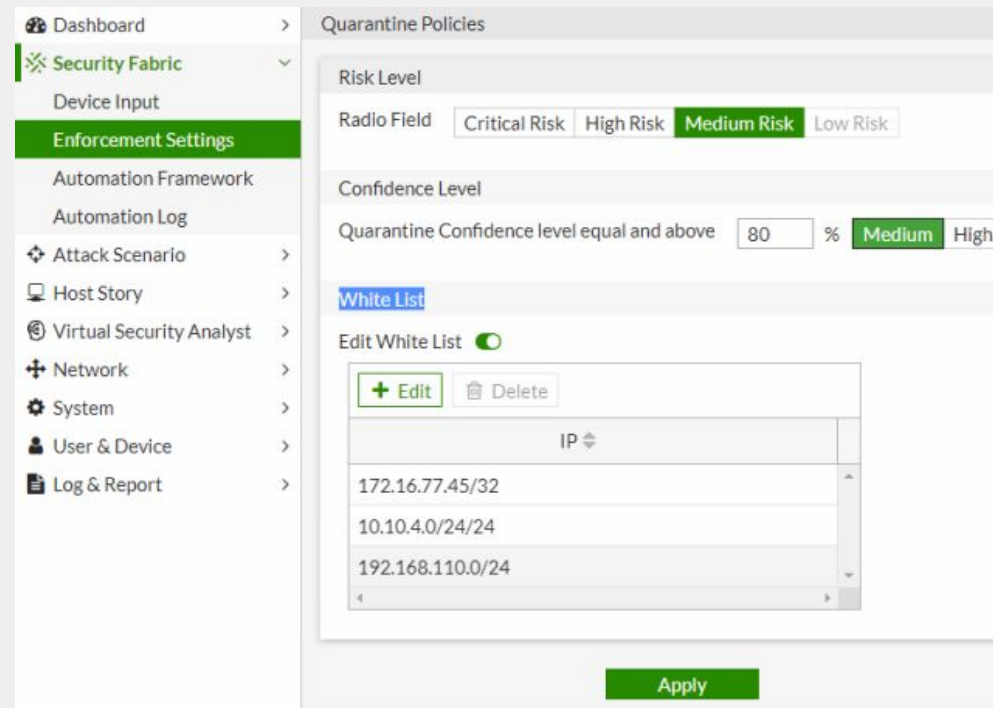
Virtual Security Analyst™ 運用類神經網路深度學習 (DNN) 進行 identifies (識別), classifies (分類), and investigates (調查) 精巧資安威脅 可完成次秒級的檢測和即時**自動反應**即時阻殺

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 VM FAIVMS0000000000 admin

Dashboard > Security Fabric > Attack Scenario > Attack Scenario Summary

Industroyer (5) Wiper (1) Fileless (9) **Worm Activity (44)** Ransomware (872) Rootkit (1) Botnet (6) Backdoor (62) Banking Trojan (20) Exploit (70) Data Leak (28) Generic Trojan (730) DoS (8) Scenario Heuristic (5) Sophisticated (3) Phishing (1) SEP (4) Web Shell (15) Application (22) Cryptojacking (174)

Host Story > Virtual Security Analyst >

Information View **Investigator View** Generate Report

MITRE ATT&CK

Detected Techniques

Risk Level	Count
Critical Risk	1
High Risk	3
Medium Risk	7
Low Risk	3

Detected Categories

Category	Count
Execution	2
Persistence	1
Privilege Escalation	1
Defense Evasion	10

入侵初期
執行
持續
提權
防禦躲避
憑證存取
發現
橫向移動
收集
C&C
滲透

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Command and Scripting Interpreter 1	Boot or Logon Autostart Execution 1 <small>Obsolete</small>	Process Injection 1	Indicator Removal on Host 2 <small>Obsolete</small>							
	Native API 1			Masquerading 2							
				Modify Registry 6							

Mitre ATT&CK Detail

Severity	FilePath	MD5
Technique : T1106 Native API 1		
20 ■■■■ low	%SYSTEMROOT%\System32\wbem\WmiPrivSE.exe	203c3380a744ca5b9b1a9caeb57f7d57



FortiAI 系列

專利

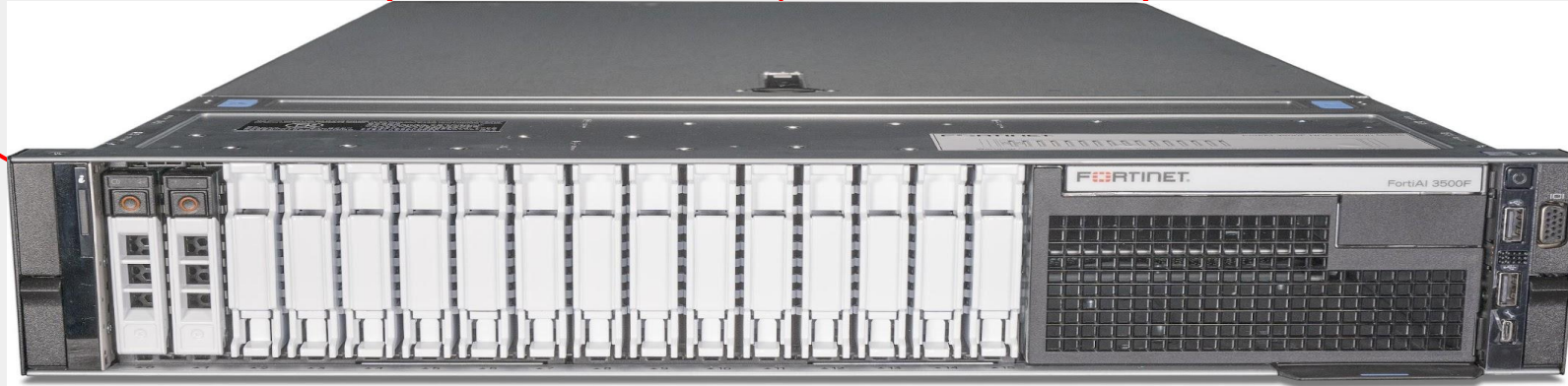
Self-Learning Model

8+
years
Mature AI

<100 ms
Sub-second Investigation

6+ million
malware
features

10G
Network
Throughput



FortiAI-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®