



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

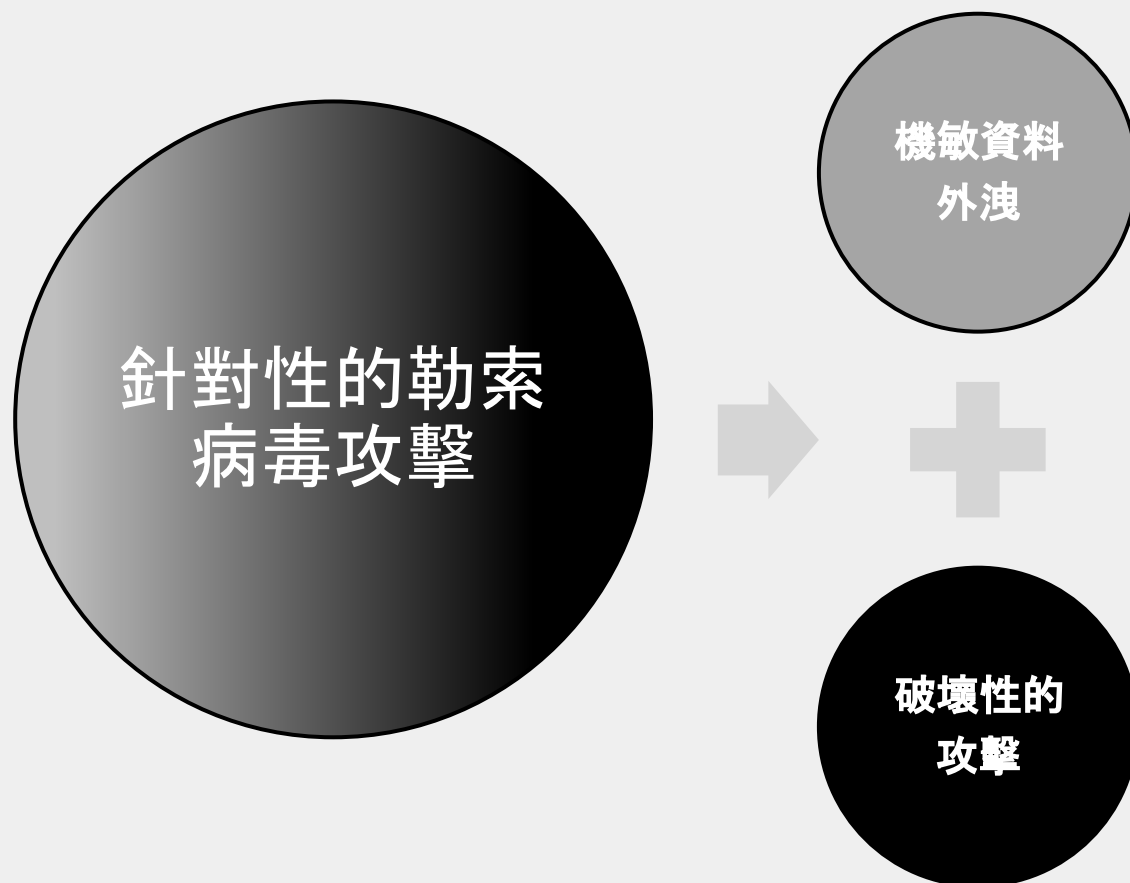
16 Days

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

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

Fortinet整合兩種防護機制

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

早期EDR廠商

EDR

20-40%

Penetration

EPP with EDR

Full EDR

傳統EPP廠商

EPP

95%

Penetration



端點安全: FortiEDR提供進階的端點全面防護

事前/安全可視性

事後/快速修復

事中/自我保護

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 <ul style="list-style-type: none">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 <ul style="list-style-type: none">避免惡意程式執行的保護	自動解除資安威脅 <ul style="list-style-type: none">避免勒索病毒的迫害持續不斷的檢測營運不中斷	<ul style="list-style-type: none">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

APPLICATIONS

Showing 1-10/223

Search Application

All | Mark As... | Delete | Modify Action | Advanced Filter | Export

APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN
Host Process for Windows Serv...	Signed Microsoft Corporation	5	Unknown	09-May-2020	08-Dec-2...
Google Chrome	Signed Google	5	Critical	09-May-2020	10-Nov-2...
81.0.4044.138		5	Critical	09-May-2020	10-May-2...
83.0.4103.106		5	Critical	22-Jun-2020	28-Jun-20...
83.0.4103.116		5	Critical	28-Jun-2020	28-Jun-20...
84.0.4147.105		5	Critical	05-Aug-2020	07-Aug-2...
84.0.4147.135		5	Critical	21-Aug-2020	27-Aug-2...
85.0.4183.83		5	Critical	27-Aug-2020	09-Sep-20...
85.0.4183.102		6	Critical	11-Sep-2020	23-Sep-20...
83.0.4103.61		5	Critical	17-Sep-2020	17-Sep-20...
85.0.4183.121		5	Critical	23-Sep-2020	19-Oct-20...

VERSION DETAILS

Google Chrome, v. 83.0.4103.61

Policies

Default Communication Contro...	FORTINET	Allow	According to policy
Servers Policy	FORTINET	Deny	According to policy
App Control Test		Allow	Manually
Carlos Communication Control Policy		Allow	According to policy
Carlos Servers Policy		Deny	According to policy

Vulnerabilities

Total 105 CVEs

CVE-2020-6573	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)
CVE-2020-6522	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)
CVE-2020-6509	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)
CVE-2020-6505	Critical	(CVSS 3.0: 9.6, CVSS 2.0: 6.8)

ADVANCED DATA

APPLICATION INFO

Application Description:	Google Chrome
First Connection Time:	17-Sep-2020, 10:32:27
Last Connection Time:	17-Sep-2020, 10:39:11
Process Names:	\\Device\HarddiskVolume2\Users\admin\Desktop\Test Area\GoogleChrome...

APPLICATION USAGE

No Collectors

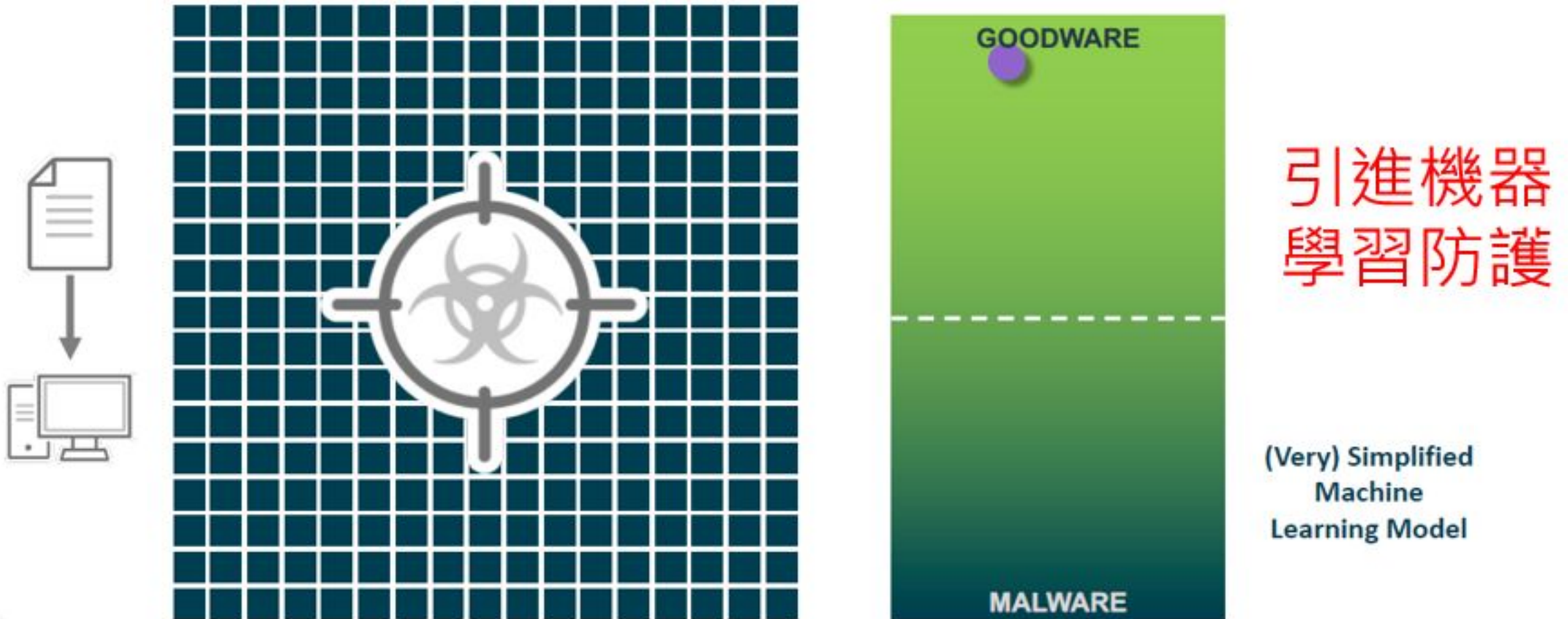
DESTINATIONS

IP	CONNECTION TIME	COUNTRY
23.56.27.47	17-Sep-2020, 10:39:11	United States
172.217.160.70	17-Sep-2020, 10:38:50	United States
69.174.120.19	17-Sep-2020, 10:38:49	United States



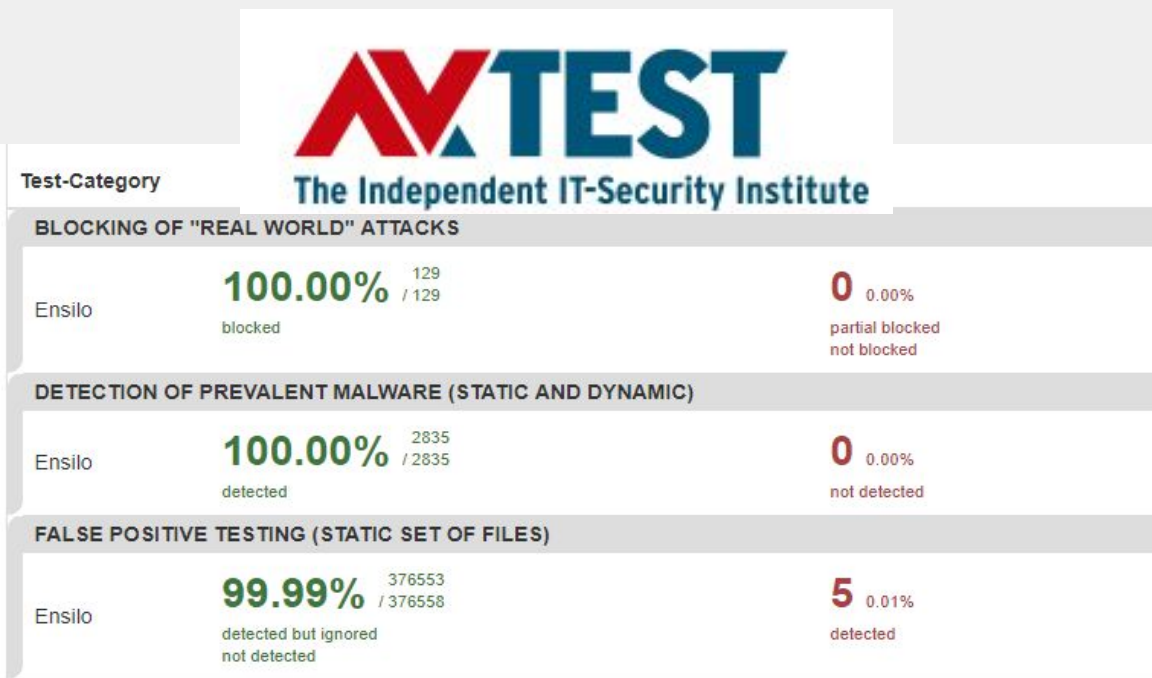
惡意程式防護方式的演進與攻防

Last Decade: Rise of Machine Learning

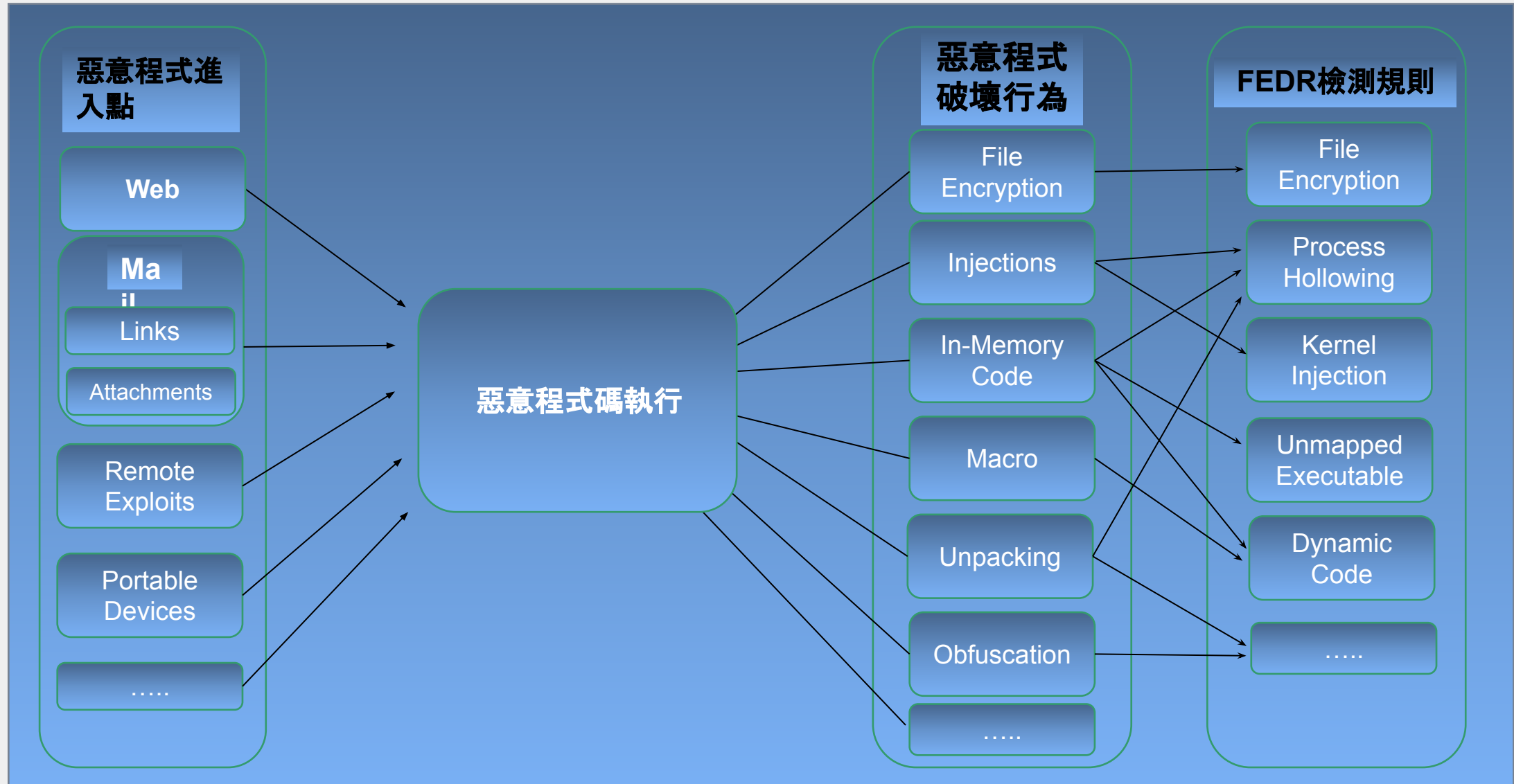


主動防護 – NGAV Technology

- 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



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

啟用FortiEDR後
利用Powershell
的勒索程式在執行

REMIEDIATE DEVICE DESKTOP-UAAD2CG

powershell.exe
EVENT 3450737
PROCESS ID 4568

- Terminate process powershell.exe
- Remove selected executable file
- Delete file at path
- Handle persistent data (registry)

 - Remove key
 - Modify registry value
 - Remove value
 - Update value data to
(A key or value that do not exist will automatically be created)

Type

Remediate Cancel

Copyright © 2020/9/9 11:30:19

FortiEDR能夠進行事後的修復：
記錄有哪些被修改的系統設定 (Registry) 可以遠端進行修復

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

The screenshot displays the FortiGate management interface. At the top, navigation tabs include DASHBOARD, EVENT VIEWER (selected), FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY, and ADMINISTRATION. The main content area is titled 'EVENTS' and shows a table of events. A modal window is open over the 'Demo_Malicious_IP' event, displaying 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 event table, a 'Playbook' configuration is visible, showing a sequence of 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 playbook. The bottom of the screen shows a status bar with 'All Firewalls' and 'FG-60E_SSL' checked.

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

在FortiGate上加入惡意IP進行阻擋

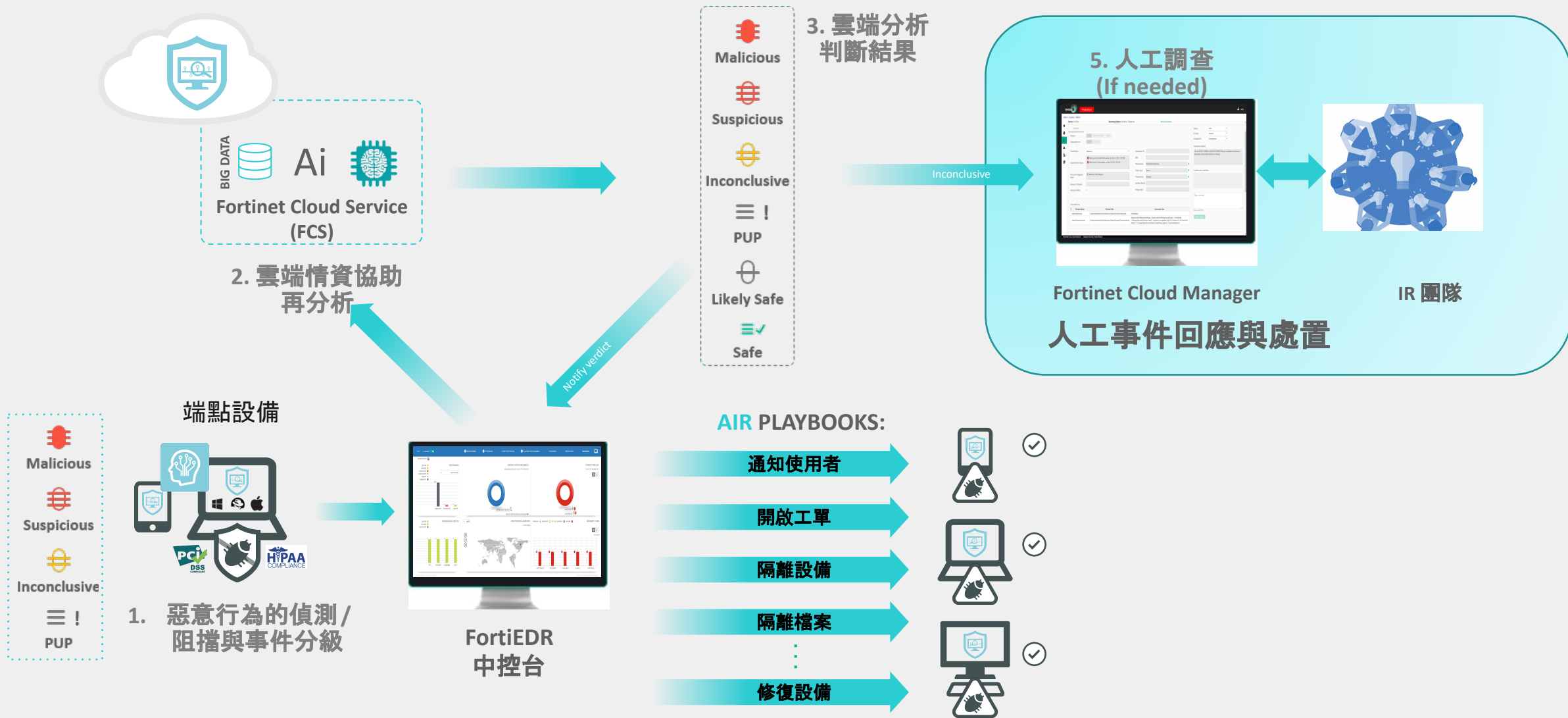
資安事件自動回應 → Playbook設定, 多樣的處理方式

The screenshot displays the 'AUTOMATED INCIDENT RESPONSE - PLAYBOOKS' configuration page in the Fortinet Security Manager. The interface includes a top navigation bar with various modules like Dashboard, Event Viewer, Forensics, Communication Control, Security Settings, Inventory, and Administration. The main content area shows a table of playbooks for the 'Default Playbook'. The table has columns for event categories: MALICIOUS, SUSPICIOUS, PUP, INCONCLUSIVE, and LIKELY SAFE. A red box highlights the MALICIOUS column. The table is organized into sections: NOTIFICATIONS, INVESTIGATION, and REMEDIATION. The 'Isolate device with NAC' and 'Block address on Firewall' rows are highlighted with blue boxes. On the right side, there is a sidebar for 'ASSIGNED COLLECTOR GROUPS' with a list of groups and their collector counts.

	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
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"/>
REMIEDIATION					
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				



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

The screenshot displays the Fortinet Security Fabric Event Viewer interface. The top navigation bar includes Dashboard, Event Viewer (426), Forensics, Communication Control (571), Security Settings, Inventory, and Administration (15). The main content area is divided into 'EVENTS' and 'CLASSIFICATION DATA'.

EVENTS

Showing 1-12/12 | Search Event

Archive | Mark As... | Export | Handle Event | Delete | Forensics | Exception Manager

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
8086750	Yuyi MacBook Air	enroll	Suspicious	2 destinations	08-Apr-2021, 09:12:11	08-Apr-2021, 09:12:55
8086225	Yuyi MacBook Air	CrashReporter	Malicious	File Read Attem...	08-Apr-2021, 09:11:55	08-Apr-2021, 09:11:55
8085282	Yuyi MacBook Air	notification.sh	Suspicious	127.0.0.1	19-Mar-2021, 04:57:00	08-Apr-2021, 09:10:34
8086750	Yuyi MacBook Air	enroll	Suspicious	54.65.177.234	17-Mar-2021, 12:00:28	17-Mar-2021, 12:00:28
8086586	Yuyi MacBook Air	BackTrack	Inconclusive	File Execution A...	17-Mar-2021, 11:56:...	17-Mar-2021, 11:56:...
8086225	Yuyi MacBook Air	CrashReporter	Malicious	File Read Attempt	17-Mar-2021, 11:49:37	17-Mar-2021, 11:49:37

Process owner: None | Certificate: Unsigned | Process path: /Library/JMTTrader/CrashReporter | Raw data items: 1

Frank 的 MacBook Pro (2 events) | Suspicious | 31-Mar-2021, 07:48:...

CLASSIFICATION DATA

Malicious **FORTINET**

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

Automated analysis steps completed

History

Malicious, by FortinetCloud

ADVANCED DATA

Event Graph | Automated Analysis

Malicious
FortiCloudServices on 17-Mar-2021 14:34:36
Fortinet Cloud Services comment
The file CrashReporter is classified as Malicious. Detected as Trojan.MAC.Lazarus malware.

File (1) | Memory (0) | Network & Extended Data (0)

crashreporter

SHA1: 8644da026f9e8873dd8699bd68c77a25001be726 (more)

Hash reputation: Malicious by FortiLab, FortiGuard and VirusTotal



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次諮詢委員會會議重點及重大決策)%E2%80%AEcod.scr Count: 26





FILE READ ATTEMPT

Process ID: 3468 Company: Mozilla Corporation Product: Thunderbird Process Hash (SHA-1): 30D3112E841802CDAE22B898D6EC956EE5F51C39
 Source Process: ...Program Files (x86)\Mozilla Thunderbird\thunderbird.exe Description: Thunderbird Comments: Mozilla Thunderbird Mail and News Client Process Owner: WIN7SP1-192\TestWin7
 Target: ...陸委員會第239次諮詢委員會會議重點及重大決策)%E2%80%AEcod.scr Version: 68.12.0 Command Line:

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...



多種資安政策的設定與套用

POLICY NAME			
	Execution Prevention	FORTINET	<input type="checkbox"/>
	Exfiltration Prevention	FORTINET	<input type="checkbox"/>
	Ransomware Prevention	FORTINET	<input checked="" type="checkbox"/>
	Device Control	FORTINET	<input type="checkbox"/>

Malicious File Detected	<input checked="" type="checkbox"/> Block
Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	<input checked="" type="checkbox"/> Block
Sandbox Analysis - File was sent to the sandbox for analysis	<input type="checkbox"/> Log
Access to critical system information	<input checked="" type="checkbox"/> Block
Bruteforce Attempt Detected	<input type="checkbox"/> Log
Debugged Process - Connection from a Debugged Process	<input type="checkbox"/> 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

The screenshot displays the FortiEDR Threat Hunting Settings interface. The top navigation bar includes sections for DASHBOARD, EVENT VIEWER (1), FORENSICS, COMMUNICATION CONTROL (66), SECURITY SETTINGS (dropdown), INVENTORY, and ADMINISTRATION (30). The SECURITY SETTINGS dropdown menu is open, showing options for Security Policies, Playbooks, Threat Hunting Settings (highlighted in green), 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 'Events Collection And Storage' section is highlighted with a red border 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)



FortiEDR強大的威脅捕獵功能 – 基於行為類型與MITRE分類

The screenshot displays the FortiEDR Threat Hunting interface. At the top, there's a navigation bar with tabs for Dashboard, Event Viewer (32), Forensics, Communication Control (62), Security Settings, Inventory (1), and Administration (22). The main section is titled "Threat Hunting" and includes a search bar with filters for Category (All Categories), Device (Choose), and a search expression field. A table shows a list of events, with "Behavior: privilege escalation" highlighted. Below this, a detailed view of a "Process Creation" event is shown, including fields for Type, Device Name, Target Process Name, Target Process Signed, Target Process Architecture, Target Process Product, Source Process File, and Source Process Signed. A "Process Creation" sidebar is open on the right, showing a "Summary" tab and a "Mitre Techniques" section. The "Mitre Techniques" section lists "Privilege Escalation, TA0004".

Behavior	Type	Device Name	Target Process Name	Target Process Signed	Target Process Architecture	Target Process Prod...	Source Process File...	Source Process Signed
privilege escalation (23)	Process Creation (23)	fortinet-testingpc (23)	runtimebroker.exe (16) tiworker.exe (3) trustedinstaller.exe (3) svchost.exe (1)	Signed (23)	64 bit 64 bit (23)	microsoft windows op... (23)	nt services\trustedinstaller (20) administrators (3)	Signed (23)

Category	Time	OS	Device Name	Type	Behavior	Process And Attributes	Target	Event Attributes
Process Creation	2020-Nov-05...	Windows	Fortinet-testi...	Process Cre...	Privilege esc...	backgroundTaskHost.exe	RuntimeBrok...	Source PID: 3048, Path: Windows\System32..., Hash: 7AE43B9B9DF5C5...
Process Creation	2020-Nov-05...	Windows	Fortinet-testi...	Process Cre...	Privilege esc...	backgroundTaskHost.exe	RuntimeBrok...	Source PID: 9072, Path: Windows\System32..., Hash: 7AE43B9B9DF5C5...
Process Creation	2020-Nov-05...	Windows	Fortinet-testi...	Process Cre...	Privilege esc...	backgroundTaskHost.exe	RuntimeBrok...	Source PID: 8928, Path: Windows\System32..., Hash: 7AE43B9B9DF5C5...
Process Creation	2020-Nov-04...	Windows	Fortinet-testi...	Process Cre...	Privilege esc...	backgroundTaskHost.exe	RuntimeBrok...	Source PID: 6628, Path: Windows\System32..., Hash: 7AE43B9B9DF5C5...
Process Creation	2020-Nov-04...	Windows	Fortinet-testi...	Process Cre...	Privilege esc...	taskhostw.exe	TiWorker.exe	Source PID: 2792, Path: Windows\WinSxSla, Hash: 7139D384A6C56C...



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

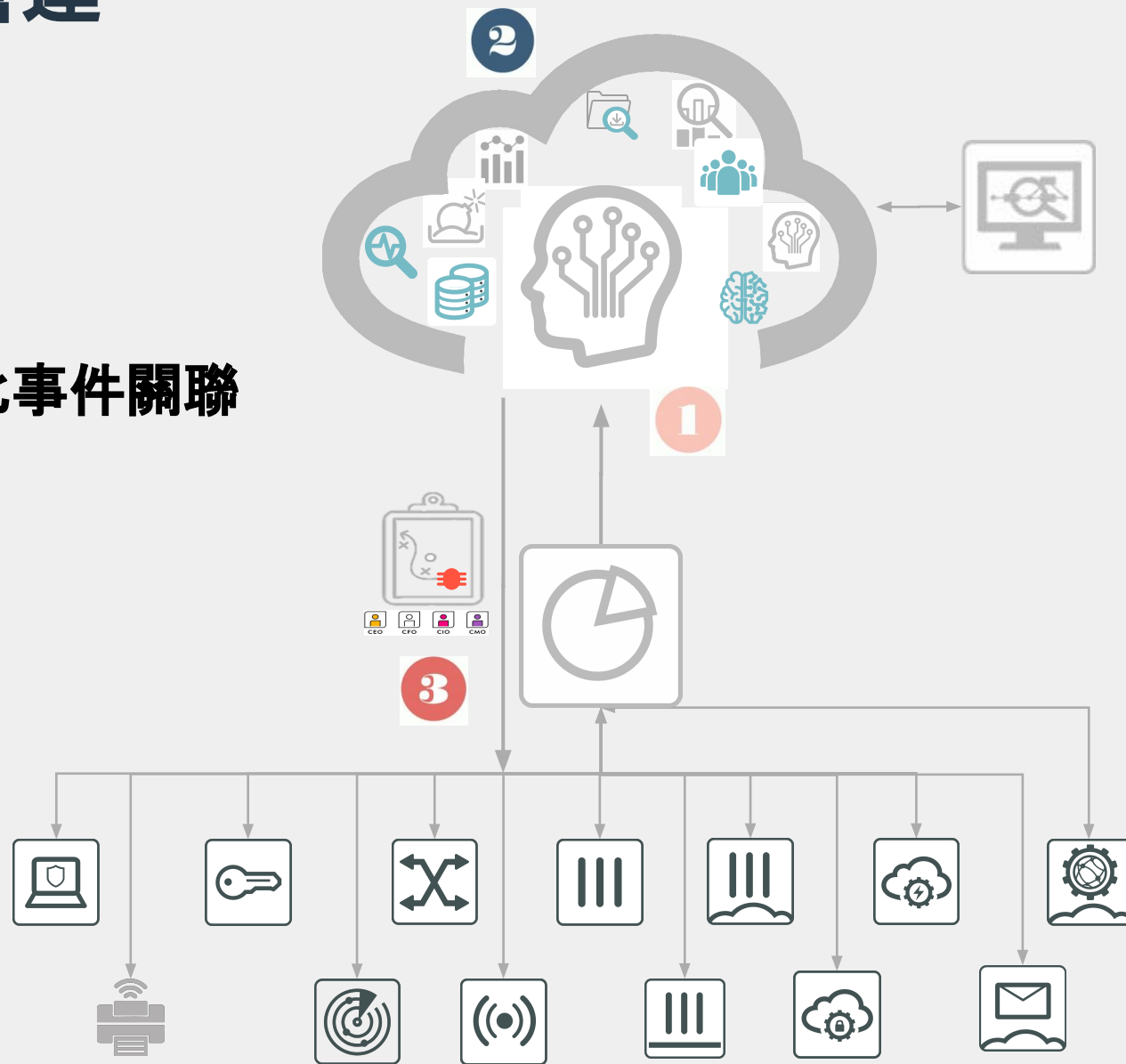
運作效能

- 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



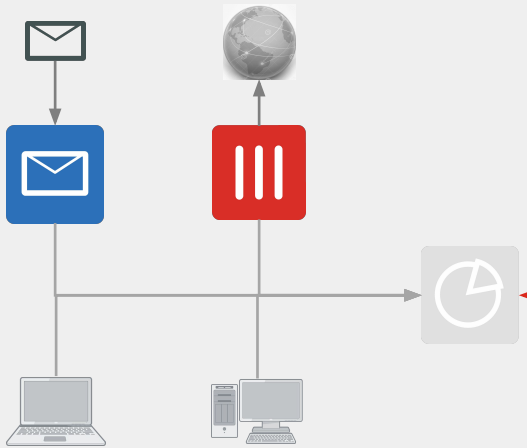
FortiXDR - AI驅動的資安營運

- 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



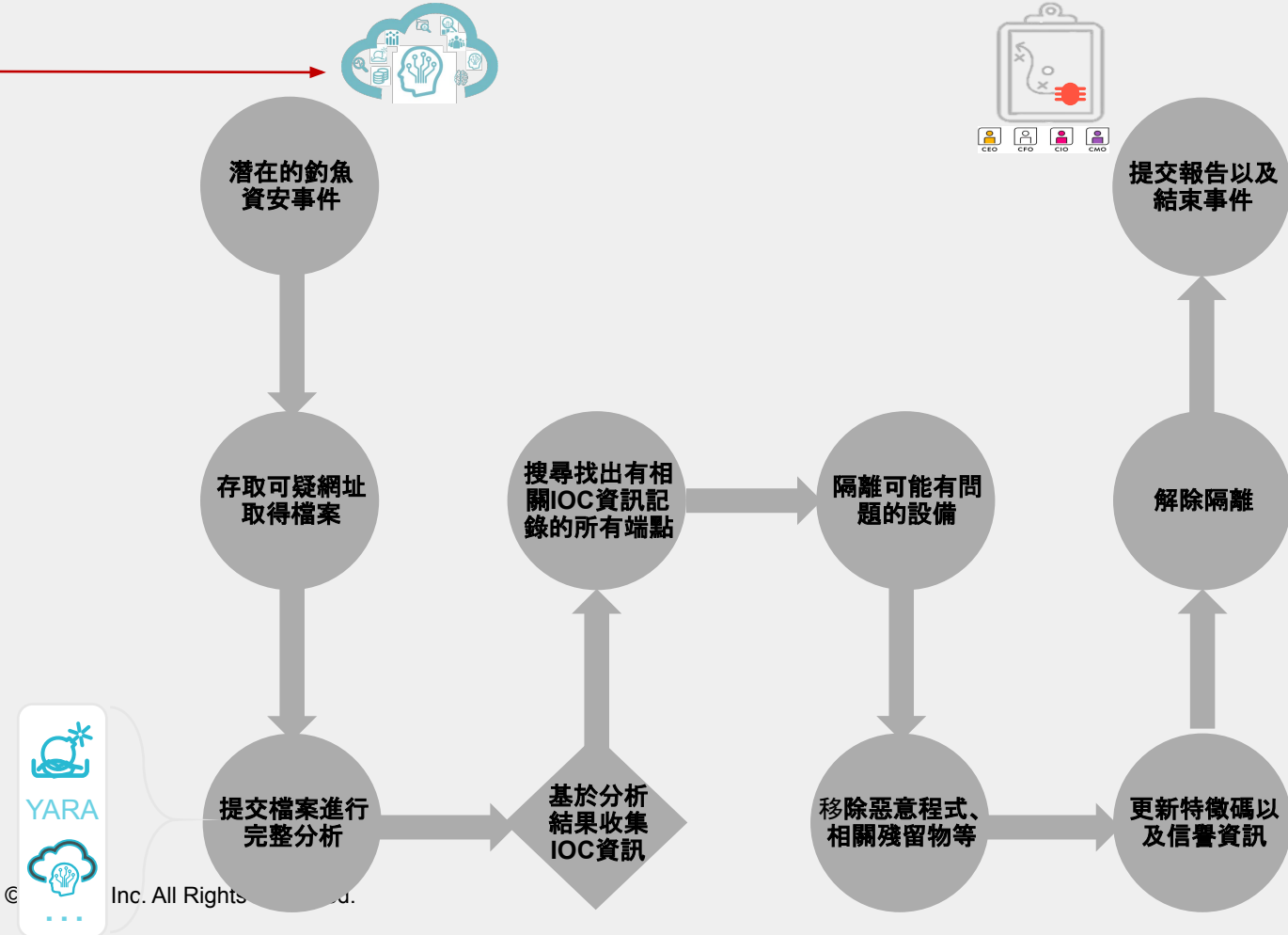
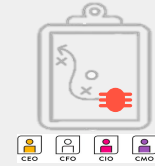
Stage 2: 分析引擎指出可能有資安事件發生



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

The screenshot displays the Fortinet Security Settings interface. The top navigation bar includes 'Demo EDR2 US', 'DASHBOARD', 'EVENT VIEWER 34', 'FORENSICS', 'COMMUNICATION CONTROL 62', 'SECURITY SETTINGS', 'INVENTORY 1', 'ADMINISTRATION 22', and a 'Protection' toggle. The main content area is titled 'SECURITY POLICIES' and features a table of policies. A blue arrow points to the 'eXtended Detection Policy' row. Below the table, the 'ADVANCED POLICY & RULE DATA' section is visible, showing details for the 'Suspicious activity Detected' rule.

	POLICY NAME	RULE NAME	ACTION	STATE
<input type="checkbox"/>	Execution Prevention			<input type="checkbox"/>
<input type="checkbox"/>	Exfiltration Prevention			<input checked="" type="checkbox"/>
<input type="checkbox"/>	Ransomware Prevention			<input checked="" type="checkbox"/>
<input type="checkbox"/>	Device Control			<input type="checkbox"/>
<input checked="" type="checkbox"/>	eXtended Detection Policy			<input type="checkbox"/>
		Suspicious activity Detected	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enabled
		Suspicious authentication activity Detected	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enabled
		Suspicious email activity Detected	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enabled
		Suspicious network activity Detected	<input checked="" type="checkbox"/> Block	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/>	JB_Device Control clone			<input checked="" type="checkbox"/>
<input type="checkbox"/>	JB_Execution Prevention...			<input checked="" type="checkbox"/>

ADVANCED POLICY & RULE DATA

[Rule Details](#) [Factory Settings](#)

RULE NAME: Suspicious activity Detected

RULE DETAILS
TBD.

FORENSICS RECOMMENDATIONS
TBD.



FortiEDR資安事件檢視- XDR Enabled View

The screenshot displays the FortiEDR XDR Enabled View interface. The top navigation bar includes 'DASHBOARD', 'EVENT VIEWER', 'FORENSICS', 'COMMUNICATION CONTROL', 'SECURITY SETTINGS', 'INVENTORY', and 'ADMINISTRATION'. The 'EVENTS' section shows a table with columns for ID, DEVICE, PROCESS, CLASSIFICATION, DESTINATIONS, RECEIVED, and LAST UPDATED. A single event is listed for 'youngputty.exe' with a classification of 'Malicious'. The 'CLASSIFICATION DETAILS' panel on the right shows the threat name 'NanoCore', threat family 'NanoCore', and threat type 'Trojan'. The 'ADVANCED DATA' section is highlighted with a blue box and a blue arrow pointing to the 'FILE' tab. This section includes an 'Automated Analysis' summary, a 'Based on' section with file details, and a 'NETWORK' section with connection details.

ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
youngputty.exe (1 event)			Malicious		22-Jun-2020, 08:34:05	
1644865	WIN10	youngputty.exe	Malicious	File Read Attempt	22-Jun-2020, 08:34:05	22-Jun-2020, 08:34:42

CLASSIFICATION DETAILS

Malicious **FORTINET**

Threat name: NanoCore
Threat family: NanoCore
Threat type: Trojan

History

Malicious, by FortinetCloudServices, on 22-Jun-2020

ADVANCED DATA

Event Graph Geo Location Automated Analysis

Malicious
FortinetCloudServices on 22-Jun-2020, 11:55:56
FortiXDR Cloud Services Incident Analysis
An attempt to breach the network with NanoCore remote access trojan from multiple vectors was detected and blocked.

Based on

- FILE youngputty.exe (AB83652EB84B1D40838C00886FFF17C45765FD9A)
 - Hash reputation: FortiGuard Labs intelligence services found UNKNOWN
 - File signature: UNSIGNED
 - Sandbox execution: Malicious based on FortiSandbox analysis [Analysis Report](#)
 - YARA IOC scan: Match - NanoCore RAT
 - File usage statistics: 1 out of 5433 devices
 - Remediation actions: Deleted from "WIN10" device

MEMORY

- Attack indicators in memory: not found

NETWORK omeubebexxs.org (185.90.56.136) [More details](#)

- Reputation: FortiGuard intelligence services found Malicious
- FortiGate: Connection blocked from device "SE_LAB" [Analysis Report](#)
- FortiMail: Mail to itaygor@forti-il.com from jlay20000@gmail was blocked [Analysis Report](#)



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®