



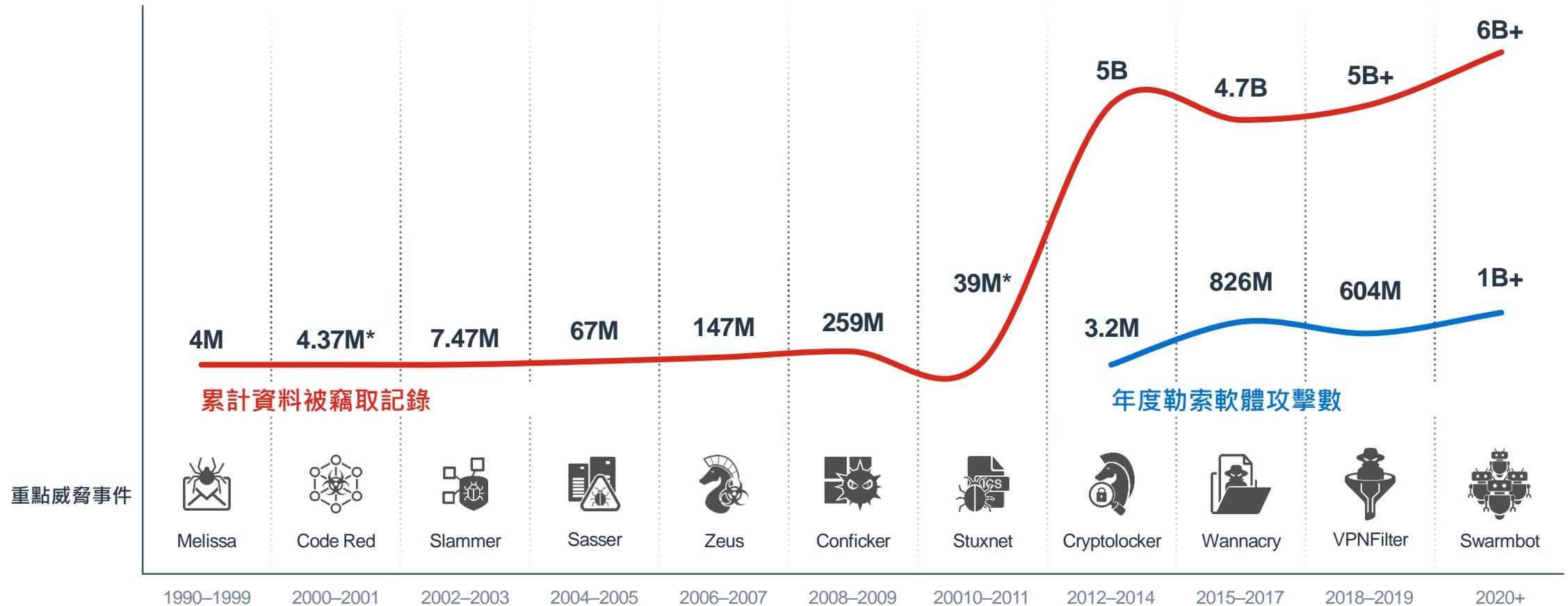
# MITRE ATT&CK 與FortiSIEM的完美演出

Marty 張益盛

[mchang@fortinet.com](mailto:mchang@fortinet.com)

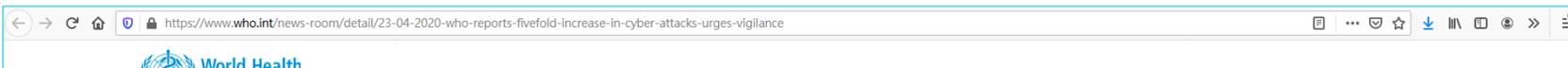
# 進階持續威脅 (Advanced Persistent Threats) 持續在發生

進階持續威脅仍然極度依賴社交工程



\*Many undisclosed | Record Stolen Reference—Breach Level Index | Ransomware stats—Statista

# 全球衛生機構電子郵件帳密遭外洩



Home Health Topics Countries Newsroom Emergencies

Home / Newsroom / Detail / WHO reports fivefold increase in cyber attacks, urges vigilance

## WHO reports fivefold increase in cyber attacks, urges vigilance

自由時報

Liberty Times Net

即時 熱門 政治 社會 生活 健康 國際 地方 蒐奇 影  
汽車 時尚 體育 3C 評論 玩咖 食譜 地產 專區 T

### 週刊爆疾管署遭駭 69人電郵帳密被竊



https://www.cdc.gov.tw/Bulletin/Detail/86s-TTbLXU4toqaOqZR1BA?typeid=9



關於CDC 傳染病與防疫專題 預防接種

首頁 新聞稿

### 有關駭客入侵竊取公務信箱帳密一事，經查非直接從疾管署系統中外洩

發布日期：2020  
有關媒體報導疾管署電子郵件帳密遭國際駭客入侵一事，疾管署今(29)日表示，於今(2020)年4月23日接獲國家資通安全會報技術服務中心通報竊取電子郵件帳密資料外洩事件計68筆，隨即進行清查，結果發現其中65筆資料為2018年、2019年曾經通報之歷史資料(2018年56筆、2019年9筆)，3年首次出現；目前已針對這些外洩的電子郵件帳密予以停用。

https://www.washingtonpost.com/technology/2020/04/21/nearly-25000-email-addresses-passwords-allegedly-nih-who-gates-foundation-are-dumped-online/



Get 1 year for \$29 Gift

Sections

Technology

## Nearly 25,000 email addresses and passwords allegedly from NIH, WHO, Gates Foundation and others are dumped online

Who posted them is unknown, but



Attachment Tools [redacted] Purchase Order ...

File Message Attachments Tell me what you want to do...  
Open Quick Print Send Save Save All Remove Copy Show Message  
Print To As Attachments Attachment Selection Message  
Actions

[redacted] - Purchase Order  
This message was sent with High importance.

PO - 01CTKT\_0001483.z  
247 KB

Dear Sir/Madam,

This is our second mail, we are sending base the on the above subject yet no feedback from your ends. pls confirm you received this mail.

we still await your reply. Hope you are fine and your company is still in office and running despite the issue regarding the COVID-19, all over the world, Please stay safe.

Your product has been highly rated and recommended by our customers and that got our interest.

Please find our order for your processing and send us back order acknowledgement along with your invoice with bank details.

# 仁寶傳出遭勒索軟體攻擊，該公司予以否認，並認為疑似是駭客入侵造成網路異常

筆電代工大廠仁寶電腦今天早上傳出疑似遭到勒索軟體攻擊，傍晚該公司表示並非如此，僅是有可能因駭客攻擊而出現網路異常，事故是發生於辦公自動化系統 (OA) 的環境

文/周峻佑 | 2020-11-09 發表

讚 6.3 萬 按讚加入iThome粉絲團 讚 290 分享



HP SPECTRE DELL XPS AMAZON AVS



今年國內多家科技製造廠遭到勒索軟體攻擊，一旦有關的消息出現，便會引發關注。根據民視新聞報導，今天早上仁寶電腦出現電腦大當機的情況，並指出有員工一早開機看到中毒的畫面，疑似是遭到勒索軟體攻擊。針對這樣的情況，我們自上午11時30分開始，透過多種管道聯繫仁寶，也檢視股市公開資訊觀測站，但截稿之前沒有相關公告。直到大約

新聞

# 日本電玩開發商卡普空疑遭勒索軟體攻擊，被盜走1TB資料

ZDNet及Bleeping Computer報導指稱，Ragnar Locker駭客近期同時攻擊這家知名電玩開發商，以及義大利知名釀酒公司Campari

文/林妍濤 | 2020-11-06 發表

讚 6.3 萬 按讚加入iThome粉絲團 讚 143 分享



**MICRO FOCUS**

Mini RPA + AI  
 限時一年 特價每個 Seat User  
 NT\$80,000

黑箱白箱、行動 App、  
 應用程式弱掃

基本掃描一年 NT\$ 1 萬起

知名電玩開發商卡普空 (Capcom) 日本及海外公司網路發生駭客入侵事件，可能遭勒索軟體Ragnar Locker攻擊，並竊走近1TB的資料。

卡普空為知名電玩製作公司，其作品包括快打旋風、惡靈古堡、惡魔獵人、魔物獵人、洛克人等。該公司本周一公布網路安全事件，公司部份郵件伺服器、檔案伺服器系統遭到未授權第三方人士存取，同時也造

AWS re:Invent  
 NOV. 30 - DEC. 18, 2020

史上首次免  
 全球最大且最

11/30-12/1

iThome  
 說這

iThome  
 11 小時前

不同於國際間由賽如wn2Own、2018年自創天... 舉辦，當地隊伍... 競賽中表現最



# 中油、台塑、力成 連遭勒索病毒攻擊

## 中油、台塑、力成 連遭勒索病毒攻擊

2020-05-06 05:30



## 中油遭勒索病毒攻擊 調查局解析惡意程式追駭客



即時 新聞 影音 專題 特企 圖輯 名家 直播 活動 旅遊 遊戲 銀行家

## 接二連三受駭！力成科技湖口3廠區遭攻擊 生產線一度中斷

2020/05/06 08:59:00 新聞台

追蹤三立:

三立新聞 / 綜合報導

繼中油公司、台塑集團傳出遭到「勒索病毒」攻擊，半導體業的記憶體封測廠「力成」也遭勒索病毒一度受到影響。力成表示，4日下午湖口3個廠區遭到攻擊，不過緊急處理後，目前已經逐漸恢復。

10-%E3%80%8C%E5%8B%92%E7%B4%A2%E7%97%85%E6%AF%92%E3%



## 中油遭勒索軟體攻擊隔天，台塑集團也出現電腦病毒攻擊，全面停機 清查後於傍晚6點恢復運作

繼中油之後，台塑集團也被駭客攻擊了嗎？台塑集團證實今天（5月5日）上午發現電腦病毒，決定全面清查，確認其他電腦沒有問題才逐步開放使用。再者，他們也表示旗下的台亞加油站沒有受到波及。

文/周峻佑 | 2020-05-05 發表 讚 6.1萬 按讚加入iThome粉絲團 讚 289 分享

關於我們 活動優惠 產品與服務 投資人關係 公司治理

VMware EVOLVE™ ONLINE  
VMware 週三線上講堂  
企業營運不中斷  
解決方案系列  
立即報名

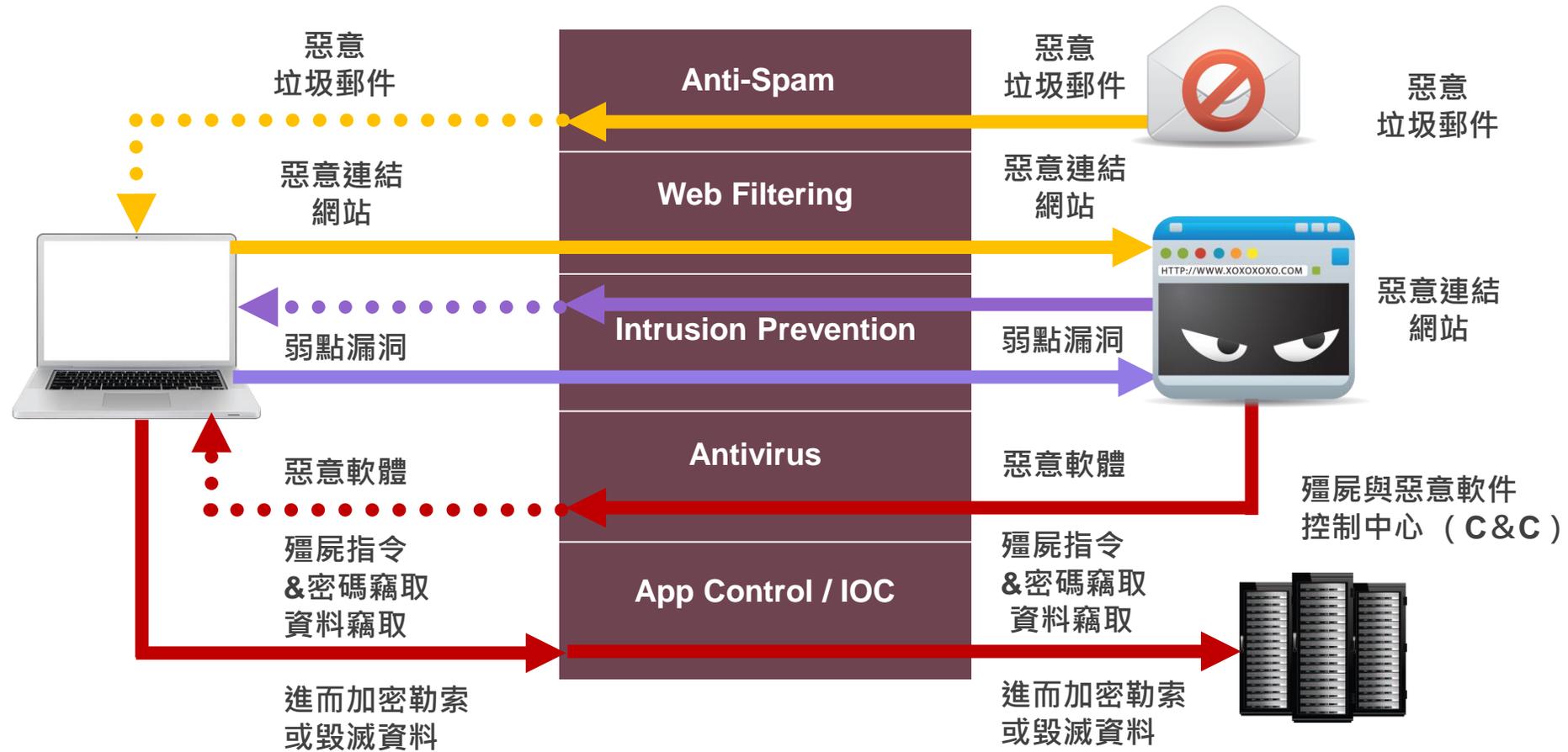
# 國內重要企業遭勒索軟體攻擊事件調查說明



# 六點防勒索!!

1. 檢視網路防護機制，對外網路服務因需求開啟或關閉、重要主機(RDP)應該限制存取來源。
2. 時常檢查VPN有無異常登入行為或電腦安裝了遠端連線等軟體時,不定時監控異常的連線。
3. 隨時監控具備有軟體派送功能的系統，如網域/(AD)伺服器、防毒軟體、資產管理系統，尤其注意AD伺服器的群組原則是  
否遭受到異動、工作排程異常遭新增等。
4. 隨時更新防毒軟體病毒碼，留意防毒軟體發出之告警。
5. 加強監控網域中特權帳號，應限定帳號使用範圍與登入主機。
6. 建立備份機制，並離線保存。

# 進階持續威脅 (Advanced Persistent Threats) 基本步驟



# 如何描述發生的資安事故與討論可能的防禦措施？

需要一個通用的資安框架來進行溝通

## 攻擊分析 資安框架

### Lockheed Martin® Cyber Kill Chain

- What** – 將資安入侵活動的各階段建立模型
- Why** – 了解對手並找出流程、技術和人員方面的弱點
- How** – 對應 ATP 資安解決方案與防禦手段
- Who** – 方便相關人員溝通與經驗分享

一般常被使用討論的資安框架

### MITRE ATT&CK® Framework

- What** – 描述對手採取的 TTP (戰術, 技巧與程序)
- Why** – 了解對手用於攻擊所使用的技術細節
- How** – 對應 ATP 資安解決方案與做法來阻止對手戰術實施
- Who** – 資安團隊細部戰術討論 (i.e. 事前監看預防, 事故反應, 事後追蹤分析與回饋)

# Lockheed Martin® Cyber Kill Chain (資安攻擊鍊)



Reconnaissance  
偵察目標

武器配置  
Weaponization



Delivery  
交付武器

## 第一階段 計畫與準備

對手感興趣/有價的目標  
你的弱點可能已經暴露

攻擊者已將你的組織作為攻擊目標，並經由多方資訊收集來了解您重要的資產和弱點。

弱點利用  
Exploitation



Installation  
安裝執行

## 第二階段 入侵與執行

你的重要資訊已經被發現  
你的特權帳號已經被利用

攻擊者已經可以訪問你的網路，並取得管理員帳號。攻擊者會安裝加密和隱匿惡意軟體，準備將重要資訊上傳至外部伺服器。

命令與控制  
Command & Control



Action on Objectives  
對目標採取行動

## 第三階段 控制與破壞

你的重要資訊已經遭到竊取、加密或破壞

攻擊者悄悄地將你的重要資訊傳送到外部伺服器、加密勒索、發動破壞，刪除他們在網路上訪問的任何痕跡。

# MITRE ATT&CK® (對手戰術、技術與通識新資安框架)

需要一個更細緻的模型來描述攻擊者的戰術、技術與手段

高階層模型  
(Lockheed Martin® Cyber Kill Chain)

中階層模型  
(MITRE ATT&CK®)

低層次概念  
(已知漏洞、弱點情資資料庫與模型)

- 將高階模型中未能有效說明攻擊者做出的每個動作，與各個動作之間的相互關聯性、行動順序，如何來達成戰術目標，進一步做更具描述性的分類，並對其可能採用的技術與實行手法作說明。
- 對於低層次的漏洞、惡意程式等情資，除了常規的漏洞掃描，快速補丁和 IOC 之外，賦予其運用情境，並著重於行為模式技術分析。

# MITRE ATT&CK® 的技術分類與施行細節

## ATT&CK Matrix for Enterprise

戰術  
TACTICS

技術  
TECHNIQUE

施行細節  
PROCEDURE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP							Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface							Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hard-Drive Additions								Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM							Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
										Exfiltration	

### Exploit Public-Facing Application

The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL<sup>[1]</sup>), standard services (like SMB<sup>[2]</sup> or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services.<sup>[3]</sup> Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

If an application is hosted on cloud-based infrastructure, then exploiting it may lead to compromise of the underlying instance. This can allow an adversary a path to access the cloud APIs or to take advantage of weak identity and access management policies.

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.<sup>[4][5]</sup>

# 以勒索軟體攻擊事件為例來對應 MITRE ATT&CK<sup>®</sup>

- 初始存取 (Initial Access)：事件相關源頭入侵手法，調查局雖並未揭露細節。但透過社群工程、釣魚電郵與附件 (T1192/T1193)、VPN 遠端連線 (T1133)、對外應用服務網頁 (T1190) 或是用戶使用受感染的可移除式裝置 (T1091) 都是常見的手法。
- 執行運作(Execution) / 持續潛伏 (Persistence)：數月前就透過員工個人電腦、網頁及DB伺服器入侵公司內部網路並開始刺探及潛伏。如透過 PowerShell 下載執行惡意程式 (T1086)。
- 規避防禦 (Defense Evasion)：使用 Windows 作業系統標準群組原則 ( GPO ) (T1484) 裡的工作排程執行惡意程式 `lc.tmp` (T1064)。其他還包括程式碼遮罩 (T1027)。
- 特權提升 (Privilege Escalation) / 帳密存取 (Credential Access)：竊取到特權帳號後便侵入網域控制伺服器 (T1078)。
- 探索設備 (Discovery) / 橫向擴散 (Lateral Movement)：利用凌晨時段竄改群組原則 ( GPO ) 裡的工作排程，待員工上班後就會立即套用。(T1037)
- 命令與控制 (Command and Control)：發現駭客亦留有後門程式連往境外中繼站，向美國境內 VPS 主機服務商「[petaexpress.com](http://petaexpress.com)」租用雲端主機。常用手法包括自定義的 C2 協定 (T1094) ) 或透過其他標準協定 (T1071)。
- 資料收集 (Collection) / 資料外洩 (Exfiltration)：寄送勒索郵件，表示企業須支付一台電腦3千美元的贖金，否則就要公布自公司竊取的內部資料。如本地電腦系統上的重要資料 (T1005)。
- 造成影響 (Impact)：執行駭客預埋在內部伺服器中的勒索軟體下載至記憶體中執行，若檔案加密成即會顯示勒索訊息及聯絡電子信箱功能 (T1486)。

# 以勒索軟體攻擊事件為例來對應 MITRE ATT&CK<sup>®</sup>

入侵初期	執行	持續潛伏	權限提升	防禦逃脫	憑證存取	發現	橫向移動	收集	命令與控制	滲出	衝擊
Replication Through Removable Media (T1091)	PowerShell (T1086)		Valid Accounts (T1078)	Obfuscated Files or Information (T1027)			Logon Scripts (T1037)		Standard Application Layer Protocol (T1071)	Data from Local System (T1005)	Data Encrypted for Impact (T1486)
External Remote Services (T1133)				Scripting (T1064)					Custom Command and Control Protocol (T1094)		
Exploit Public-Facing Application (T1190)				Group Policy Modification (T1484)							
Spearphishing Link (T1192)											
Spearphishing Attachment (T1193)											

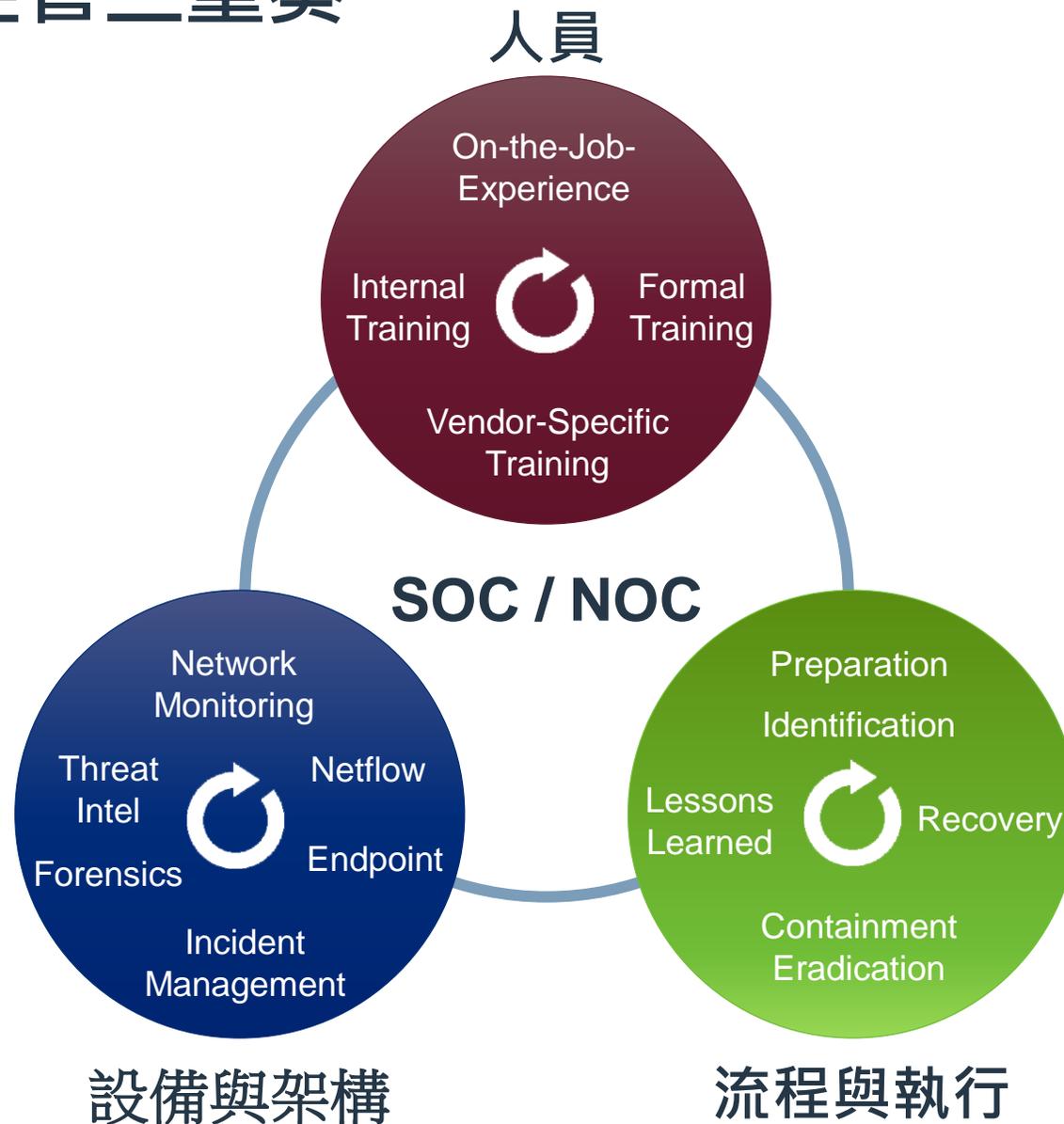
# 進階威脅防護產品解決方案與 MITRE ATT&CK<sup>®</sup> 對應

入侵初期	執行	持續潛伏	權限提升	防禦逃脫	憑證存取
<b>NGFW / ISFW, VPN, 2FA, Secure LAN / WLAN, Secure Email GW, Web App FW, Secure Web GW / Isolator, EPP / EDR</b> <b>AV, IPS, WF</b> (phishing, attachment, removable media, app exploit, drive-bys)	<b>Sandbox, Honeypot, EPP / EDR</b> <b>AV</b> (PowerShell, scripting)	<b>Sandbox, Honeypot, EPP / EDR</b> (create account, bypass user account controls)	<b>Sandbox, Honeypot, EPP / EDR</b> <b>IPS</b> (process injection, launch daemons, brute force)	<b>Sandbox, Honeypot, EPP / EDR</b> <b>AV, IPS, WF</b> (disable security tools, del / hidden files / folders)	<b>NGFW / ISFW, VPN, 2FA, Web App FW</b> <b>IPS,</b> Credential Stuffing (account manipulation, brute force)
<b>Security Operation Monitoring, Network Operation Monitoring, SIEM, NTA, IOC, Threat Intelligent DB</b>					

發現	橫向移動	收集	命令與控制	滲出	衝擊
<b>NGFW / ISFW, Sandbox, Honeypot, EPP / EDR</b> <b>AV, IPS</b> (IP / Port scans, discovery)	<b>NGFW / ISFW, Sandbox, Honeypot, EPP / EDR</b> <b>AV, IPS</b> (remote services, file copy, logon scripts, SSH hijacking)	<b>EPP / EDR, Secure Email GW</b> <b>DLP</b> (removable media, email, screen / video capture)	<b>NGFW, Sandbox, Honeypot, EPP / EDR</b> <b>IP / Domain / URL Filtering, AppCtrl</b> (connection proxy, remote access tools)	<b>NGFW, Sandbox, Honeypot, EPP / EDR</b> <b>DLP, IP / Domain / URL Filtering, AppCtrl</b> (data transfer, network / physical)	<b>DDOS prevention</b> <b>EDR</b> (data encryption / destruction, DDOS)

**Security Operation Monitoring, Network Operation Monitoring, SIEM, NTA, IOC, Threat Intelligent DB**

# 資安維運控管三重奏



# FortiSIEM 資安事件管理平台

提早告警預防-AI自動學習

進階資安事件與網路威脅鑑識分析

# What is a SIEM?

**SIEM** = **S**ecurity **I**nformation & **E**vent **M**anagement

**SIM**

(Security Information Management)

(歷史性記錄分析)

收集並儲存網路設備安全“日誌”與相關資訊，觀察趨勢，分析事件發生的原因。

+

**SEM**

(Security Event Management)

(即時性事件分析)

著重於通過自動化工具即時識別網路安全“事件”進行關聯性分析並採取應對行動。

# 業界唯一的資安 (SOC) 與網維 (NOC) 融合式分析

## 資安 SOC 分析

Log Ingestion, Parsing and Storage

File Integrity Monitoring

Patented Log Analytics

Incident Management, Ticketing and Response

Dynamic Identity and Location Report

External Threat Feed Intelligence Integration

Reporting and Compliance – Built in/Custom

Rule and Statistical Anomaly Based Reporting

## 網維 NOC 分析

Real-Time Infrastructure Discovery CMDB

Network and Interface Utilization

CPU, Memory, Disk Performance Monitoring

Availability Monitoring

Storage Monitoring

Change monitoring – config., installed software

Infrastructure and User Application Monitoring

Synthetic Transaction Monitoring

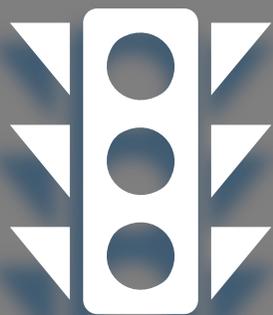
**Cross Correlated in Real-Time**

# 提升資訊安全層級



## Scalable, Multi-Tenant Architecture

企業營運服務監測



監測與回應



合規報表



**CMDB: Discovery and Inventory**

# FortiSIEM 設備組態資產管理

伺服器與網通設備效能監控設備  
網通設備設定自動備份

# 設備組態與資產管理 (CMDB)

收到 syslog、flows 之後，系統會自動將來源設備加入 CMDB

The screenshot displays the FortiSIEM CMDB interface. At the top, there is a navigation bar with icons for Dashboard, Correlation Analysis, Alerts, Task Management, CMDB, Resource Library, Work, and System Management. Below this, a summary row shows counts for various device types: Routers (2), Firewalls (7), Windows (6), Unix (2), ESX (0), AWS (0), and Azure (0).

The main content area is titled "CMDB > Devices" and includes a search bar and a table of devices. The table has columns for Name, IP, Device Type, Status, Last Discovered, Method, Agent Policy, and Agent Status. The device "HP-Core-SW2" is highlighted.

名稱	IP	設備型式	狀態	已探索	方法	代理程式政策	代理狀態
HLEMRSVR2	10.2.0.217	Microsoft Windows Server ...	Approved	Jun 18 2020, 03:16:23 PM	AGENT	windows	R
HP-Core-SW	192.168.64.253	HP 3Com Switch	Approved	Jul 09 2020, 02:45:08 PM	SNMP, PING		
<b>HP-Core-SW2</b>	<b>192.168.64.254</b>	<b>HP 3Com Switch</b>	<b>Approved</b>	<b>Jul 09 2020, 02:41:44 PM</b>	<b>SNMP, PING</b>		
Kaspersky-Manager	10.2.0.110	Kaspersky Security Center	Approved	Jun 18 2020, 03:26:48 PM	LOG		
MDA	10.2.0.121	Microsoft Windows Server ...	Approved	Jun 18 2020, 04:31:43 PM	AGENT	windows	R
MRI-FW	10.2.71.253	Fortinet FortiOS	Approved	Jun 19 2020, 05:15:03 PM	LOG		

Below the table, there are tabs for Summary, Attributes, Monitoring, Software, Hardware, Configuration, Relationships, and Archives. The "Summary" tab is active, showing details for "HP-Core-SW2":

- 名稱: HP-Core-SW2
- Access IP: 192.168.64.254
- 設備型式: HP 3Com Switch
- Version: 7.1.045
- 型號: 5900AF-48XGT4QSFPPlus
- Importance: 重要的

On the right side of the summary, there is a "Health Overview" section:

- Availability Health: Up
- Performance Health: Normal
- Incidents(last 24 hrs):
  - By Severity: High: 0 Medium: 9 Low: 0
  - By Category: Availability: 0

# 設備組態與資產管理 (CMDB)

配置不同設備的認證訊息 (SNMP、HTTPS、SSH、API 等等)

儀表板 關聯分析 告警事故 派工管理 CMDB 資源庫 工作 系統管理

儲存設備 收集器 認證資訊 探索設備 導入事件 監看效能 STM 保養維護時程 Windows 代理程式 Linux 代理程式

### 步驟 1: 輸入認證資訊

新增 編輯 刪除 複製 搜尋中

名稱
Firewall-HTTPS
Firewall-SNMP
Firewall-SSH
snmp-generic

### 步驟 2: 輸入 IP 地址區段與認證資訊關聯

新增 編輯 刪除 測試 搜尋

名稱 / IP / IP 範圍
192.168.64.254
10.2.71.230
10.2.96.220

### 存取方式定義

Name: Firewall-HTTPS

Device Type: Fortinet FortiOS

Access Protocol: HTTPS

Port: 443

URI: /login

Password config: Manual

User Name: admin

Password: .....

資訊名稱
-generic
-generic
-generic

# 設備組態與資產管理 (CMDB)

## 日誌與效能資訊收集驗證

名稱	IP	設備型式	狀態	已探索	方法	代理程式政策	代理程式狀態	監看狀態	事件狀態
Citrix-WAF	192.168.71.253	Citrix NetScaler	Approved	Jun 19 2020, 10:01:16 AM	LOG				Normal
FG200B3912612260	10.2.6.203	Fortinet FortiOS	Approved	Jun 19 2020, 05:14:27 PM	LOG				Normal
FW-DMZ-EXT_140D	10.2.96.210	Fortinet FortiOS	Approved	Jun 18 2020, 01:45:37 PM	LOG				Normal
FW-Internet_500D	10.2.96.220	Fortinet FortiOS	Approved	Jun 18 2020, 01:45:14 PM	LOG				Normal
FW-Internet_501E	10.2.71.230	Fortinet FortiOS	Approved	Jun 18 2020, 11:02:03 AM	LOG				Critical
FW-Wifi_1000D	192.168.64.251	Fortinet FortiOS	Approved	Jun 18 2020, 02:42:40 PM	LOG				Normal
HL-FW	10.2.71.241	Fortinet FortiOS	Approved	Jun 18 2020, 11:01:33 AM	LOG				Normal
MRI-FW	10.2.71.253	Fortinet FortiOS	Approved	Jun 19 2020, 05:15:03 PM	LOG				Normal
FortiSIEM-Super	10.2.71.222	Fortinet FortiSIEM	Approved	Jun 10 2020, 12:17:14 PM	LOG				Critical
FortiSIEM-Collector	10.2.71.221	Generic Unix	Approved	Jun 10 2020, 03:44:02 PM	LOG				Critical
HP-Core-SW	192.168.64.253	HP 3Com Switch	Approved	Jul 09 2020, 02:45:08 PM	SNMP, PING				Normal
HP-Core-SW2	192.168.64.254	HP 3Com Switch	Approved	Jul 09 2020, 02:41:44 PM	SNMP, PING			Normal	Normal
Kaspersky-Manager	10.2.0.110	Kaspersky Security Center	Approved	Jun 18 2020, 03:26:48 PM	LOG				Normal

摘要 屬性 監看 軟體 硬體 組態配置 關聯性 檔案  自動展開

### 事件接收狀態

指標	最後回報成功	狀態
NetFlow	1m 58s ago	Normal

### 監看狀態

指標	最後回報成功	狀態
Net Intf Stat (HS)(SN...	1m 32s ago	Normal
Hardware Status(SNMP...		N/A

# 設備組態與資產管理 (CMDB)

## 設備效能監看

The screenshot displays the FortiSIEM CMDB interface for monitoring the health of a device named HP-Core-SW2. The interface includes a sidebar with navigation options like '建立', '設備支持', '健康狀態', '授權', and '設置'. The main content area shows the device's health status, performance metrics, and a table of top interface utilizations.

**健康狀態 for HP-Core-SW2**

Availability Status: ● Up

Performance Status: ● Normal

Uptime: Uptime % (30 d):

Events Per Second (Avg): 1.52

Ping Round Trip: 1 ms

告警事故 (Last 24 hrs): High: 0 Medium: 9 Low: 0

**Top 10 Interface Utilization**

名稱	1h		5h		12h		1d		7d	
	接收用量	發送用量	接收 Bps	發送速率(Bps)	接收用量	發送用量	接收 Bps	發送速率(Bps)	接收用量	發送速率(Bps)
Ten-GigabitEthernet3/0/10	6.08%	0.92%	61Mbps	9Mbps						
Ten-GigabitEthernet3/0/14	1.85%	1.89%	18Mbps	19Mbps						
Ten-GigabitEthernet3/0/33	1.65%	0.02%	165Mbps	2Mbps						
Ten-GigabitEthernet1/0/14	1.45%	0.10%	145Mbps	10Mbps						
Ten-GigabitEthernet2/0/12	1.24%	0.98%	12Mbps	10Mbps						
Ten-GigabitEthernet2/0/32	1.24%	0.26%	124Mbps	26Mbps						
Ten-GigabitEthernet3/0/44	1.14%	0.13%	114Mbps	13Mbps						
Ten-GigabitEthernet1/0/38	0.85%	0.42%	85Mbps	42Mbps						

# FortiSIEM 支援眾多廠牌設備





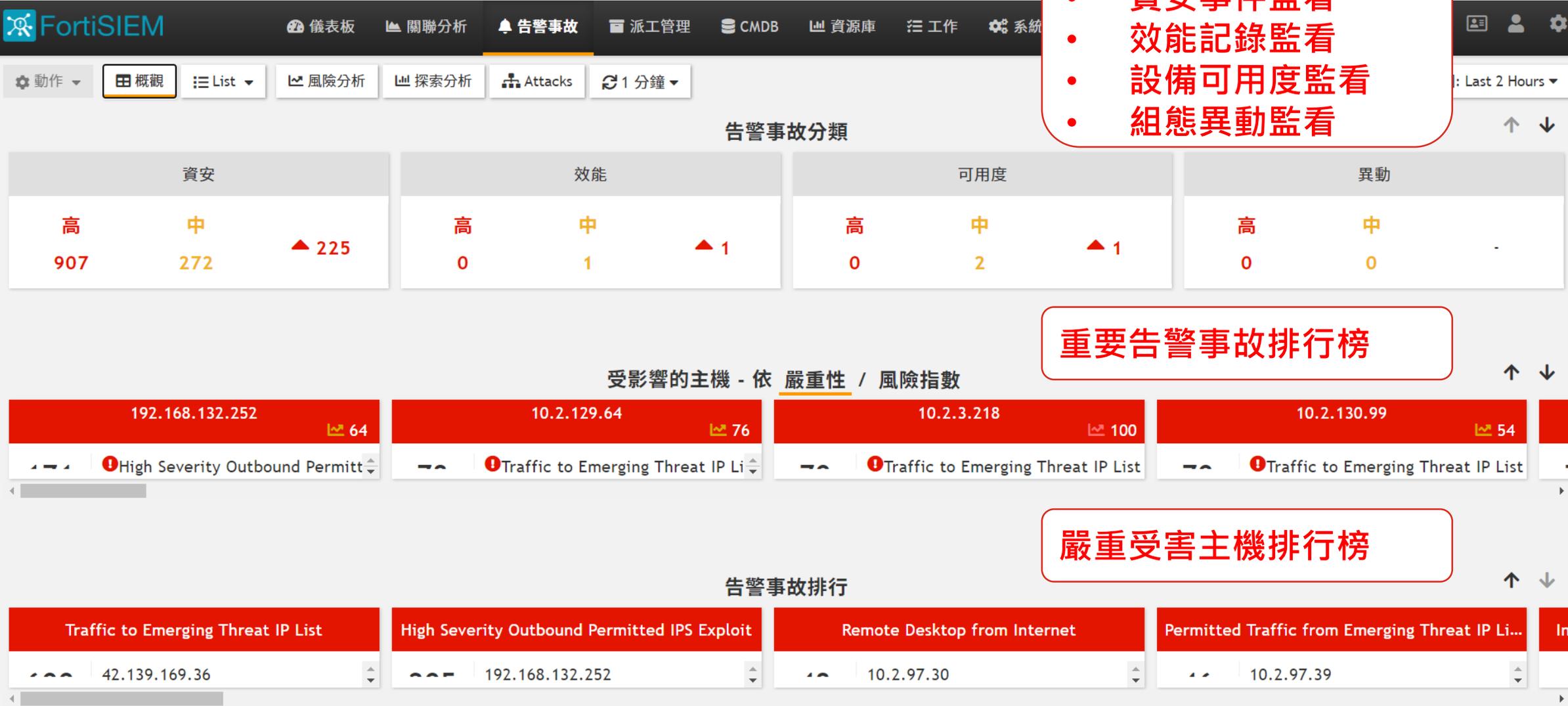
- 即時的分析 (patented)
  - » UEBA: Baselining and Machine Learning
  - » IoC Service: FortiGuard and Fabric Ready Partner Feeds
- 資安威脅消除腳本
- 動態支援新的設備及支援多樣化的紀錄格式
  - 不需要專業技能以及長時間的學習曲線

# 資安事件/警示與智能解析

所有告警事故分類及優先處理順序一目了然

## 告警事故分類

- 資安事件監看
- 效能記錄監看
- 設備可用度監看
- 組態異動監看



## 重要告警事故排行榜

## 嚴重受害主機排行榜

# 導入智能分析 (AI) , 機器學習 (ML) 分析異常行為

豐富的內建 AI / ML 告警事故規則

The screenshot shows the FortiSIEM interface for configuring rules. The left sidebar lists various categories like Reports, Rules, Networks, etc. The main area displays a table of rules with columns for 'Name' and 'Description'. A search filter 'Malware' is applied. Three red dashed boxes highlight specific rules, each with a callout box:

- 基於演算法與智能分析**: Points to the rule '(s) Dynamically generated host name: malware likely'.
- 基於白名單與智能分析**: Points to the rule '(s) End User DNS Queries to Unauthorized DNS Servers'.
- 基於條件閾值與智能分析**: Points to the rule '(s) Excessive End User DNS Queries'.

Other visible rules include '(s) Excessive End User Mail' and '(s) Excessive End User Mail to Unauthorized Mail Gateways'. The interface includes navigation buttons like '新增', '編輯', '刪除', '複製', 'Test', and 'Malware' search. At the bottom, there are tabs for '摘要' and '測試結果', and a checkbox for '自動展開'.

# 資安事件/警示與智能解析

偵測到短時間來自不同地區但同個 VPN 帳號的連線

The screenshot displays the FortiSIEM interface. At the top, there are navigation tabs: DASHBOARD, ANALYTICS, INCIDENTS (selected), CASES, CMDB, RESOURCES, TASKS, and ADMIN. Below the navigation is a toolbar with options like Action, Overview, List by Incident (selected), Risk, Explorer, Attacks, and a refresh button set to 1 minute. A search bar is also present. The main content area shows a grid of incident cards under the heading 'Top Impacted Incidents'. One card, 'Concurrent VPN Authent...', is highlighted. Below this, a specific incident is detailed: 'Incidents for Concurrent VPN Authentications To Same Account From Different Cities'. This incident is shown in a table with columns for Severity, Last Occurred, Incident, Reporting, Source, Target, Detail, and Incident Status. Two rows are visible, both with a 'HIGH' severity and 'Active' status. The first row shows an event at 09:08:30 AM for user 'hlids004'. The second row shows an event at 00:17:00 AM for user '20007'. Below the incident list, there are tabs for Details, Events, and Rule. The 'Events' tab is active, showing a table of event logs. The table has columns for Event Receive Time, Event Name, Source IP, Source Country, Source City, User, Reporting Device, Reporting IP, and Raw Event Log. Two rows are highlighted with red boxes. The first row shows an event at 09:02:43 AM from source IP 125.227.172.68 in Taipei City, Taiwan, for user 'hlids004'. The second row shows an event at 09:07:33 AM from source IP 110.25.88.161 in Zhushan Township, Taiwan, for user 'hlids004'. Red callout boxes with arrows point to the 'Source City' column for these two rows, containing the text '台北市' (Taipei City) and '竹山鎮' (Zhushan Township) respectively.

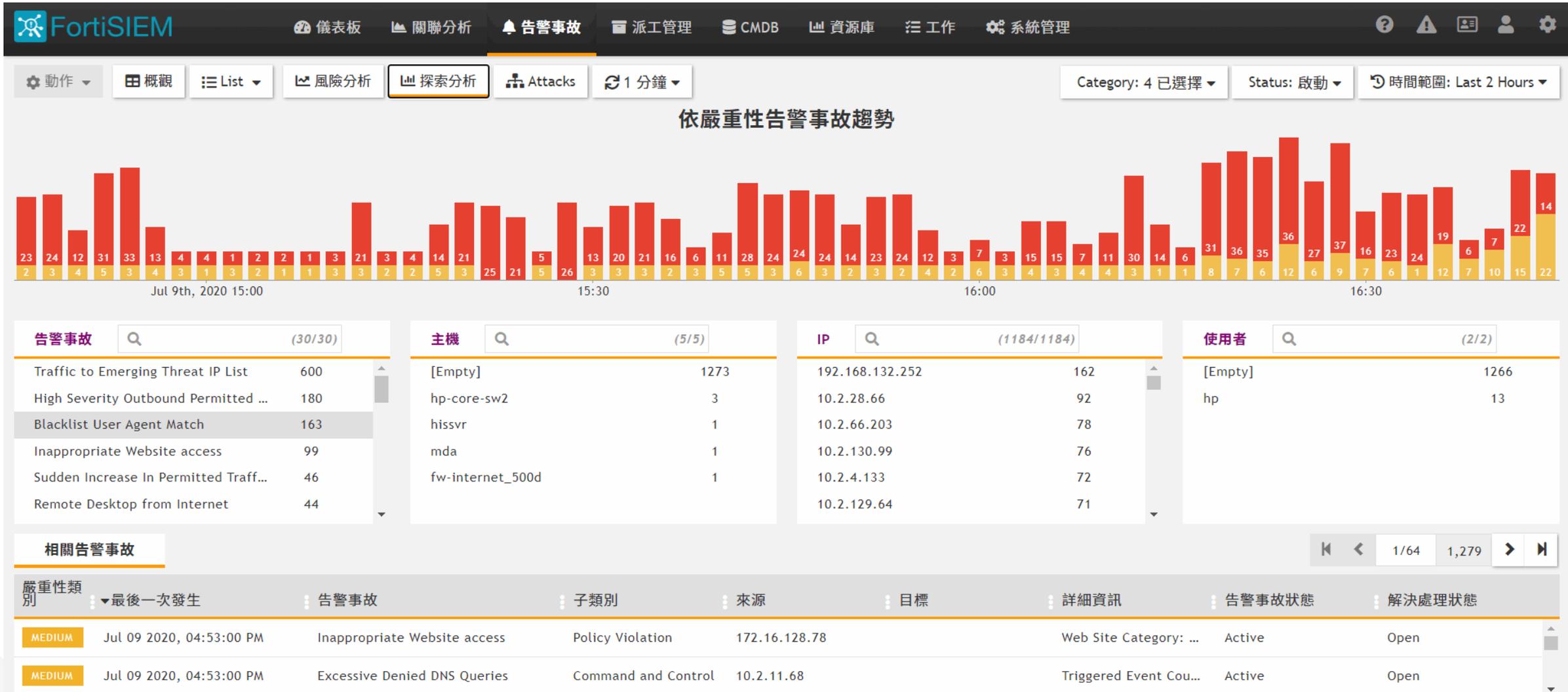
Severity Category	Last Occurred	Incident	Reporting	Source	Target	Detail	Incident Status
HIGH	Jul 17 2020, 09:08:30 AM	Concurrent VPN Authenticatio...	FW-DMZ-EXT_140D		User: hlids004		Active
HIGH	Jul 17 2020, 00:17:00 AM	Concurrent VPN Authenticatio...	FW-DMZ-EXT_140D		User: 20007		Active

Event Receive Time	Event Name	Source IP	Source Country	Source City	User	Reporting Device	Reporting IP	Raw Event Log
Jul 17 2020, 09:02:43 AM	FortiGate ssl vpn user tunnel ...	125.227.172.68	Taiwan	Taipei City	hlids004	FW-DMZ-EXT_140D	10.2.96.210	<190>date=2020-07-17 time=09
Jul 17 2020, 09:07:33 AM	FortiGate ssl vpn user tunnel ...	110.25.88.161	Taiwan	Zhushan Township	hlids004	FW-DMZ-EXT_140D	10.2.96.210	<190>date=2020-07-17 time=09

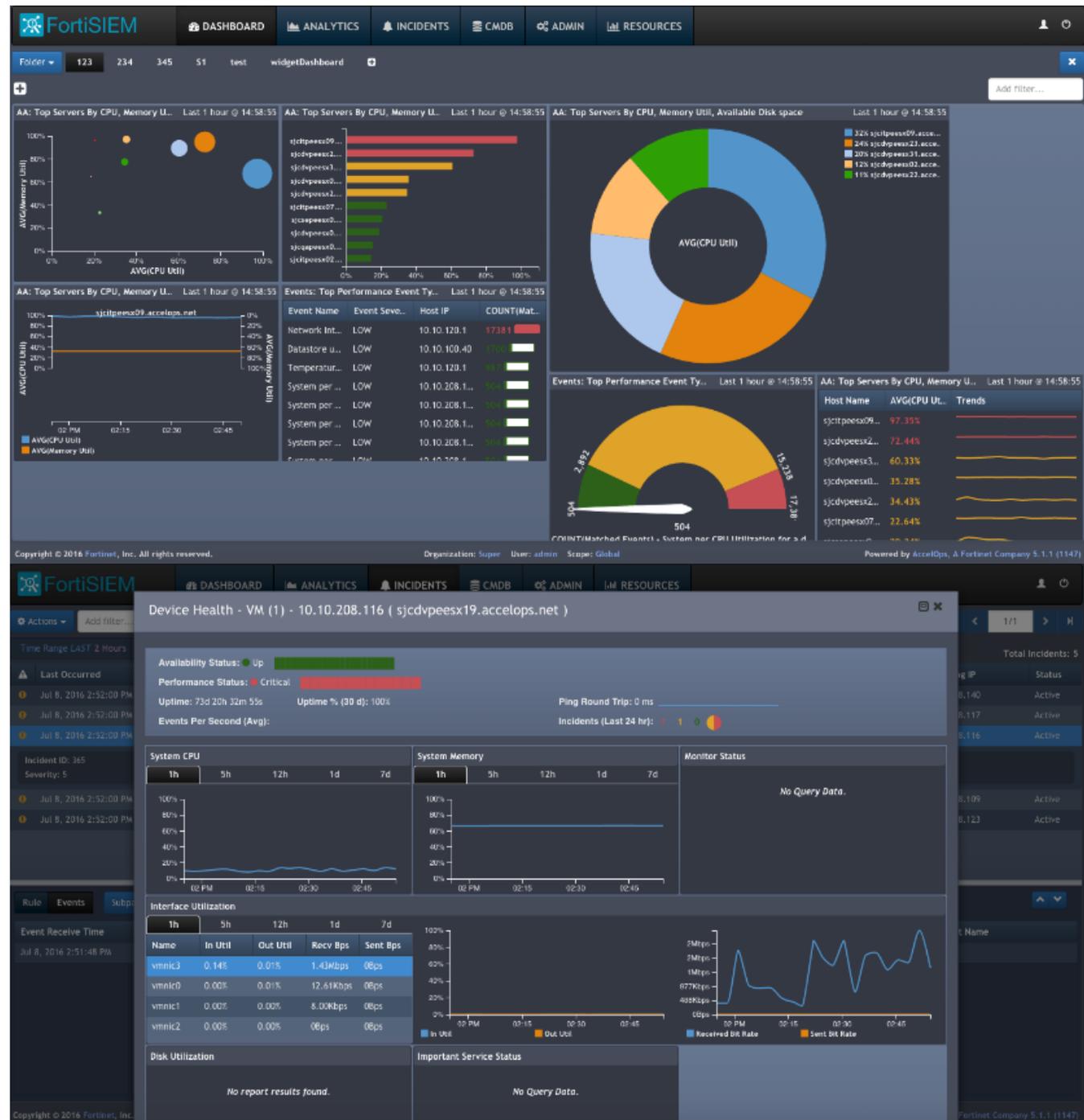
# 資安事件/警示與智能解析 (事件快速探索分析/整合檢視)

可根據告警種類、使用者、IP及主機名稱快速篩選事件



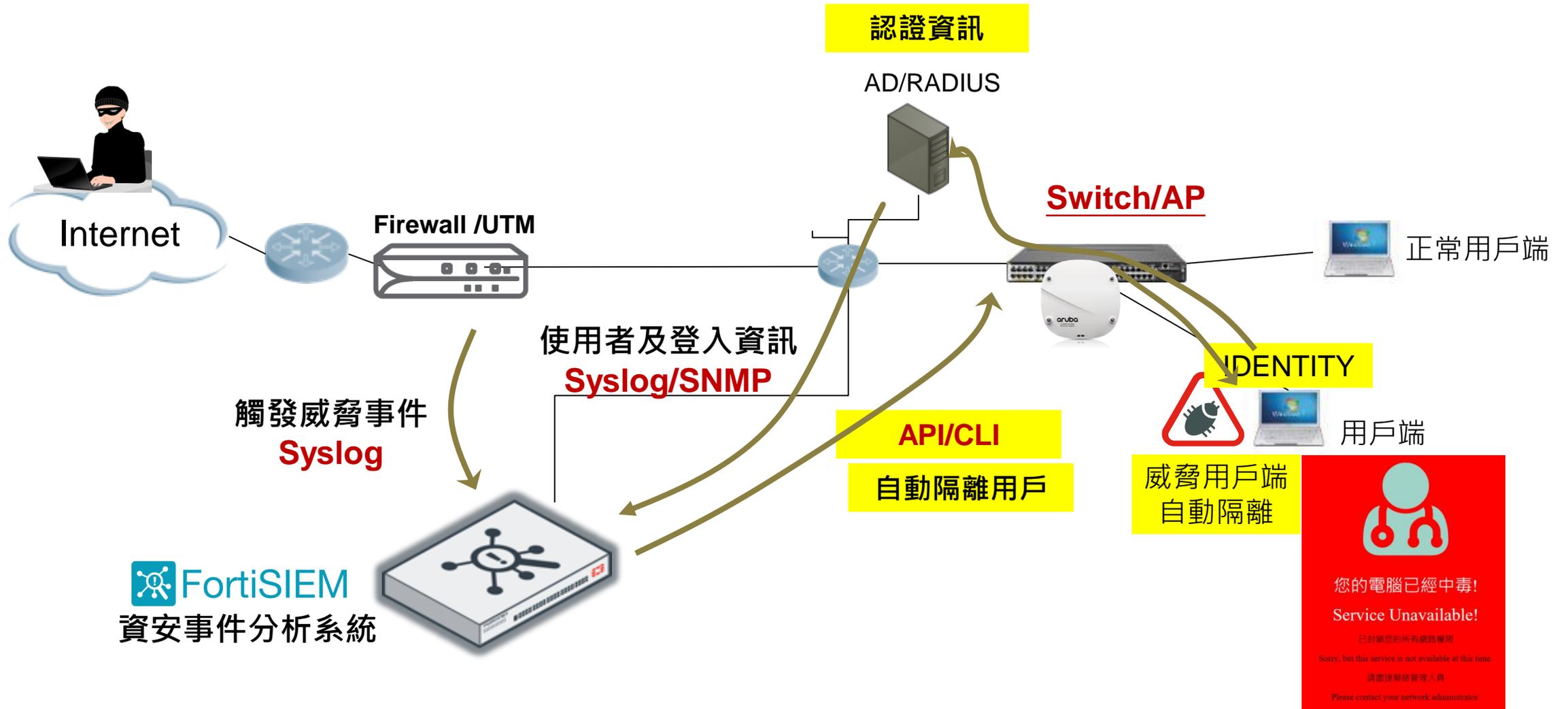
# 內建合規性報表 (可客製化)

- 數以百計的內建報表可供選擇
- 合規性報表 (Compliance Reports)
  - PCI – HIPAA – FERPA
  - SOX, NERC, COBIT, ITIL,
  - ISO, GLBA, GPG13
  - SANS Critical Controls
- 2,000+ 可客製化欄位



# 資安事件/警示，處理協作與回應自動化 (SOAR)

FortiSIEM 資安聯防協作自動回應處理示意圖



# FortiSIEM 重要特點與價值

1. 資安與網維融合式分析, 結合MITRE ATT&CK分類
2. 自動探索, 網路設備組態與效能管理 (CMDB)
3. 可快速擴容的高彈性架構
4. 直覺式事件關聯分析, 簡單易用
5. 智能分析 (AI), 機器學習 (ML)
6. 自動更新情資, 分析告警與聯防



7. 內建工單處理系統, 標準化維運流程

8. 支援繁體中文操作介面