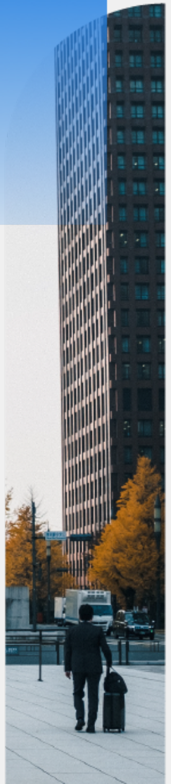
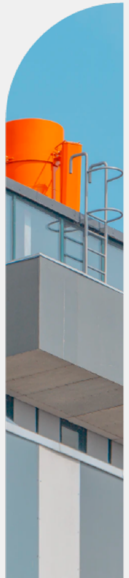


Fortinet FortiSIEM

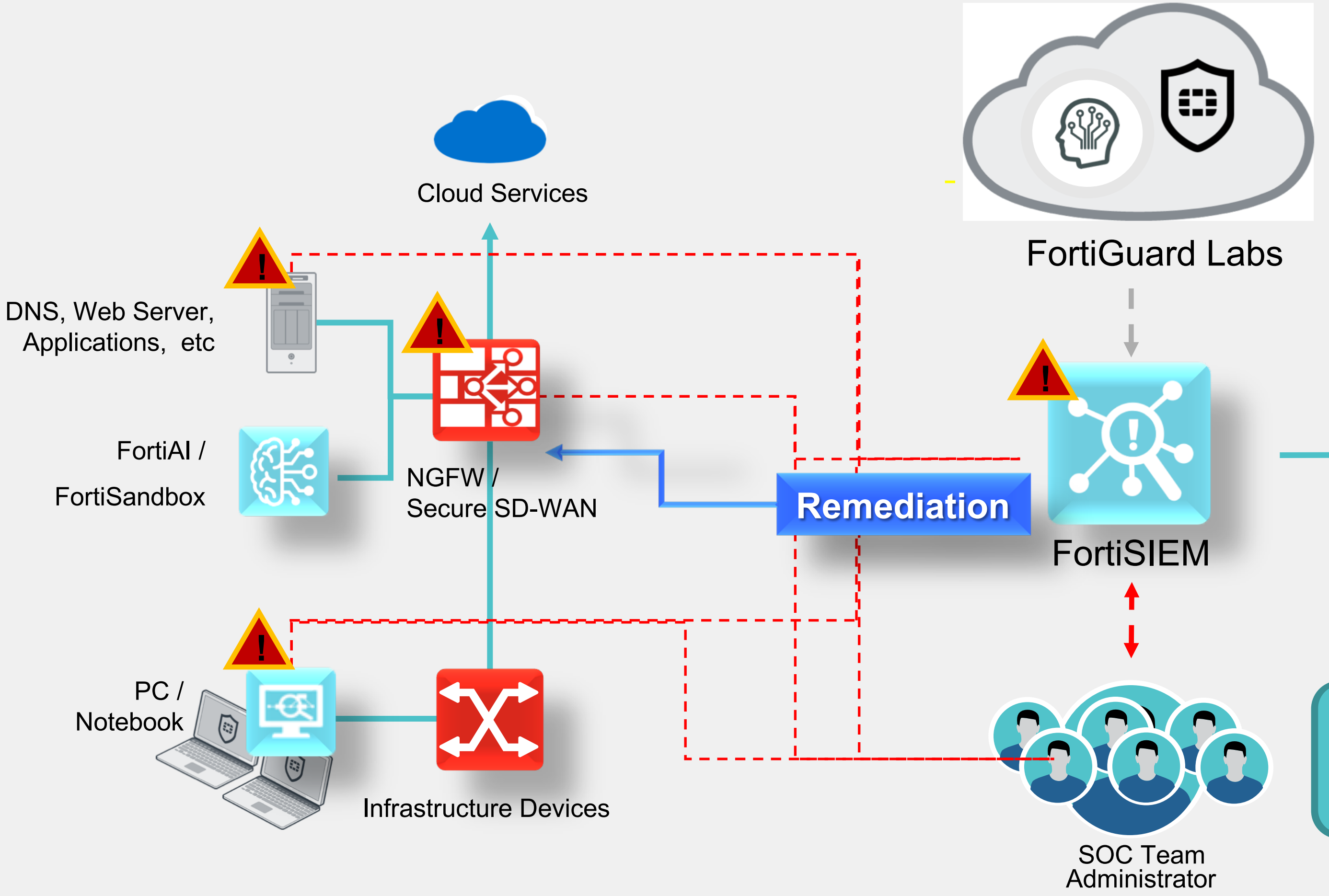
不是攻擊手法簡化了，而是「FortiSIEM」把事件一目瞭然了。
原來SIEM的使用也可以很簡單。

Jarvis Lee
ljarvis@fortinet.com



資安維運中心協作聯防再進化 (SOAR)

多來源、多品牌日誌關聯分析，資安事故回應自動化



- 日誌與記錄中央匯整
- 與各式情資整合分析
- 直覺式的查詢與報表
- AI 趨動關聯分析規則
- 中央監看儀表板與告警
- 工單系統管理與協作
- 資安事故回應自動化

優化的資安維運中心 (SOC)
更佳的資安可視性, 集中彙整日誌關聯分析,
中央資安事故告警與自動化回應處理

誰需要SIEM Support?

Security Information and Event Management

現今資安網維面臨的挑戰

不僅需要防護型資安解決方案，還需要建立早期預警系統

① 滿足法規針對資通安全防護及控制措施等相關要求

② 不同品牌產品與各自獨立的管理系統，資訊統整難

③ 每天太多日誌事件產生，缺乏好工具找出關鍵問題

④ 進階威脅與勒索病毒持續成長，如何發現潛在威脅

⑤ 建立資安事故反應標準作業流程與緩解動作自動化

資安 (SOC) 與網維 (NOC) 融合式分析

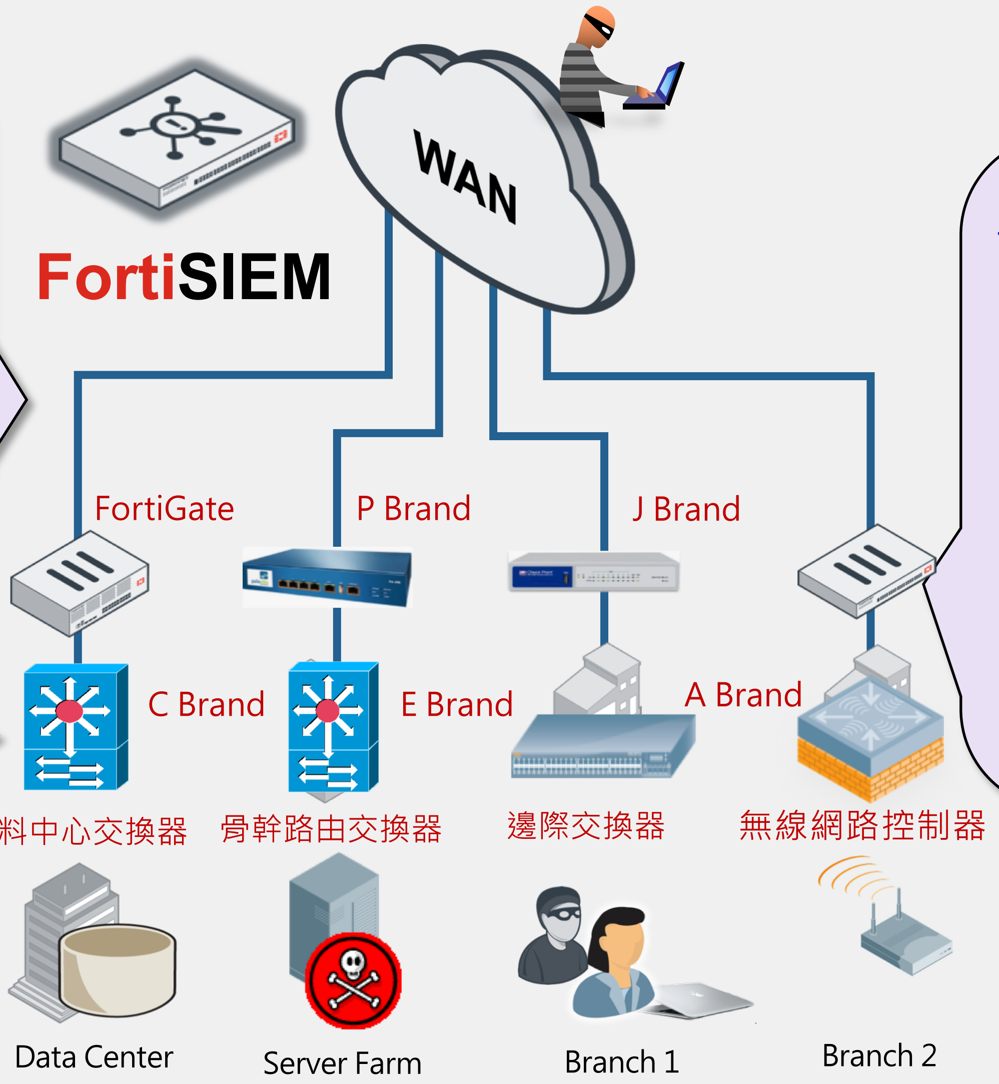
多源、多品牌日誌記錄關聯分析

SNMP、CLI、API, etc.

- CMDB 資產管理
- 設備健康狀態(Up/Down)
- 效能使用率(CPU/ Memory/Bandwidth)
- 儲存空間 (Storage)
- 異常效能分析

Syslog、WMI、API, etc.

- 系統事件(Event Log)
- 資安事件(Security Log)
- 流量記錄 (Traffic Log)
- 應用系統事件 (Application Layer)
- 異常行為、事件分析

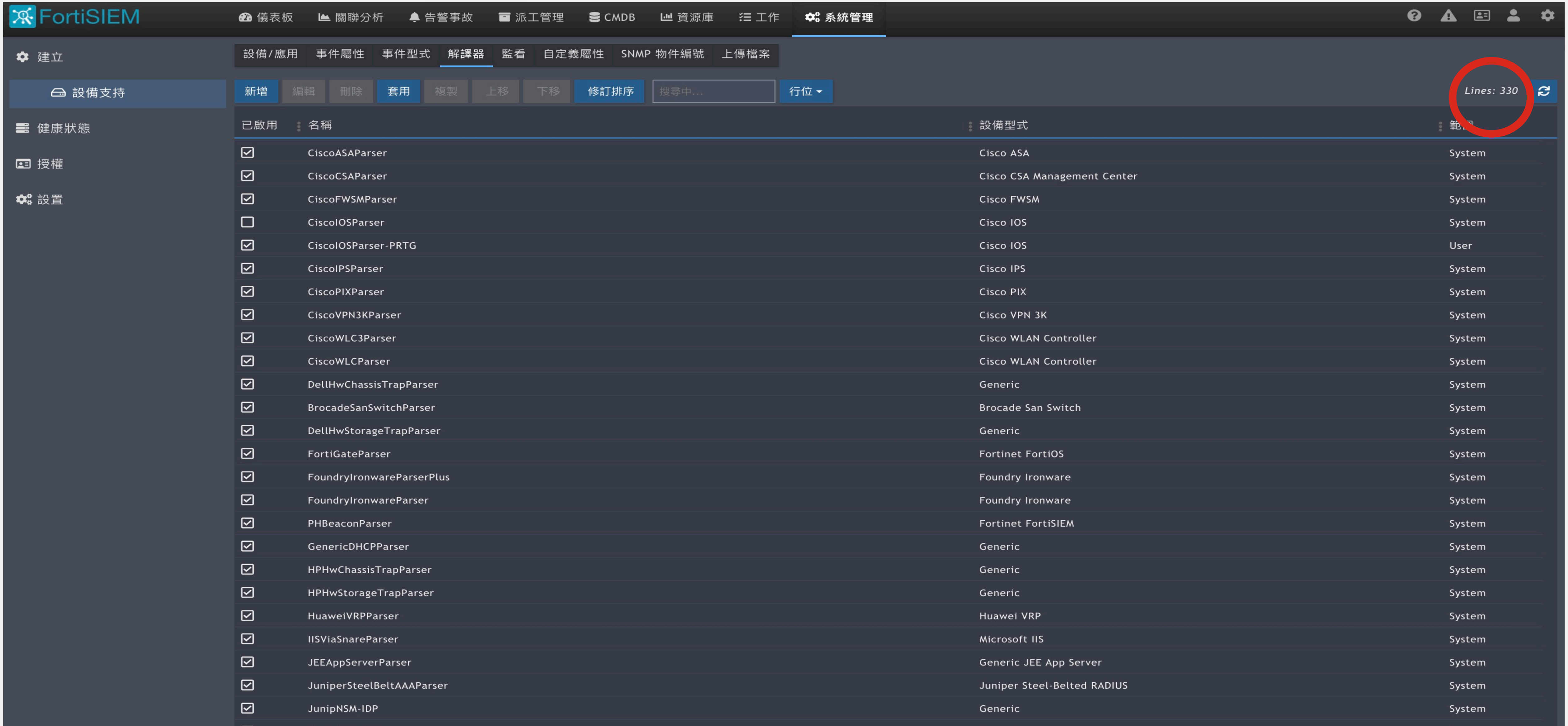


Flows

- NetFlow/Sflow /Jflow/IPFix
- 內外網路流量使用分析
- 通訊協定流量使用分析
- 點對點會談流量排行
- 網路 scan/DoS 威脅分析
- 異常行為、流量分析

內建多品牌Parsers

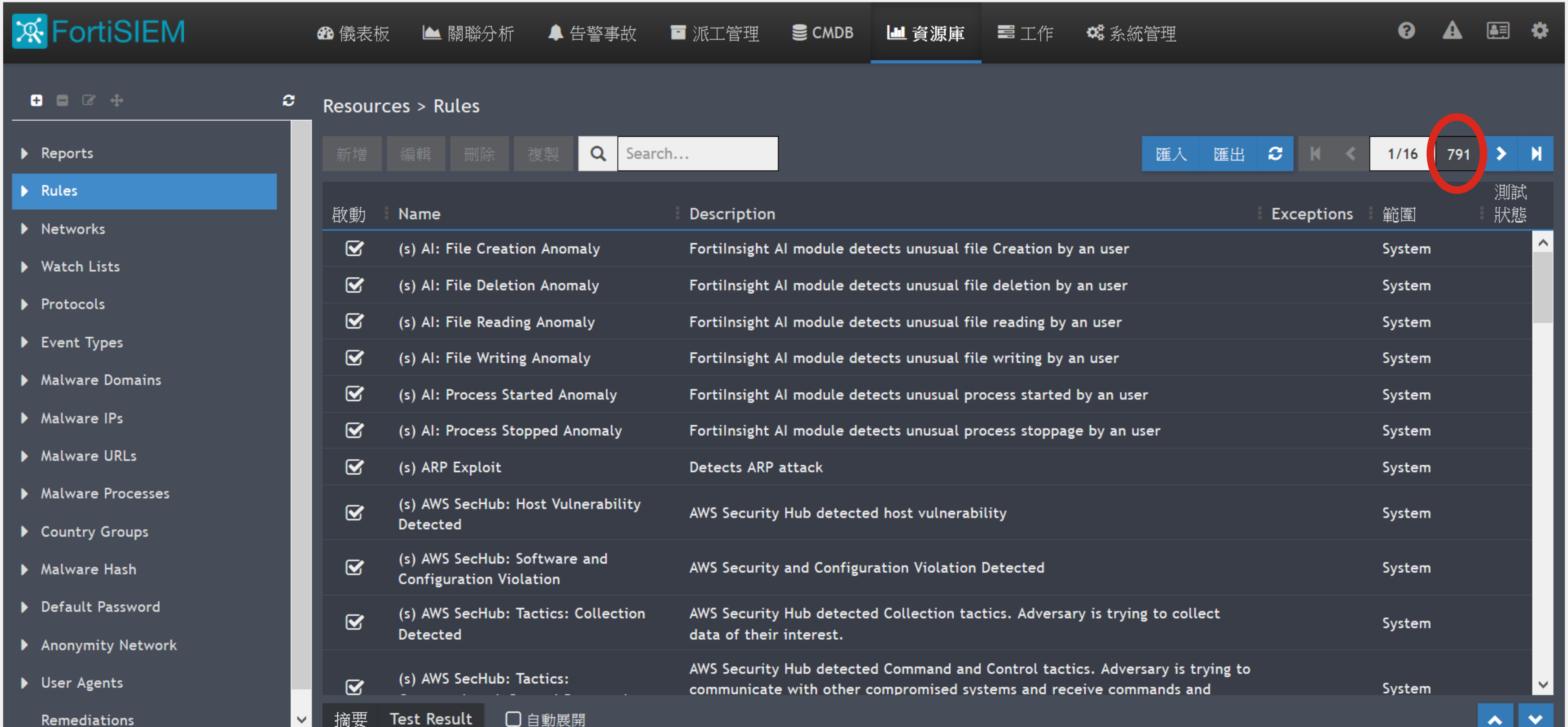
無需花費過多人力自定義正規劃



已啟用	名稱	設備型式	範圍
☑	CiscoASAParser	Cisco ASA	System
☑	CiscoCSAParser	Cisco CSA Management Center	System
☑	CiscoFWSMParser	Cisco FWSM	System
□	CiscoIOSParser	Cisco IOS	System
☑	CiscoIOSParser-PRTG	Cisco IOS	User
☑	CiscoIPSParser	Cisco IPS	System
☑	CiscoPIXParser	Cisco PIX	System
☑	CiscoVPN3KParser	Cisco VPN 3K	System
☑	CiscoWLC3Parser	Cisco WLAN Controller	System
☑	CiscoWLCParser	Cisco WLAN Controller	System
☑	DellHwChassisTrapParser	Generic	System
☑	BrocadeSanSwitchParser	Brocade San Switch	System
☑	DellHwStorageTrapParser	Generic	System
☑	FortiGateParser	Fortinet FortiOS	System
☑	FoundryIronwareParserPlus	Foundry Ironware	System
☑	FoundryIronwareParser	Foundry Ironware	System
☑	PHBeaconParser	Fortinet FortiSIEM	System
☑	GenericDHCPParser	Generic	System
☑	HPHwChassisTrapParser	Generic	System
☑	HPHwStorageTrapParser	Generic	System
☑	HuaweiVRPParser	Huawei VRP	System
☑	IISViaSnareParser	Microsoft IIS	System
☑	JEEAppServerParser	Generic JEE App Server	System
☑	JuniperSteelBeltAAAParser	Juniper Steel-Belted RADIUS	System
☑	JunipNSM-IDP	Generic	System

豐富的內建告警事故規則

豐富的內建關聯性資安規則，無須煩惱如何定義

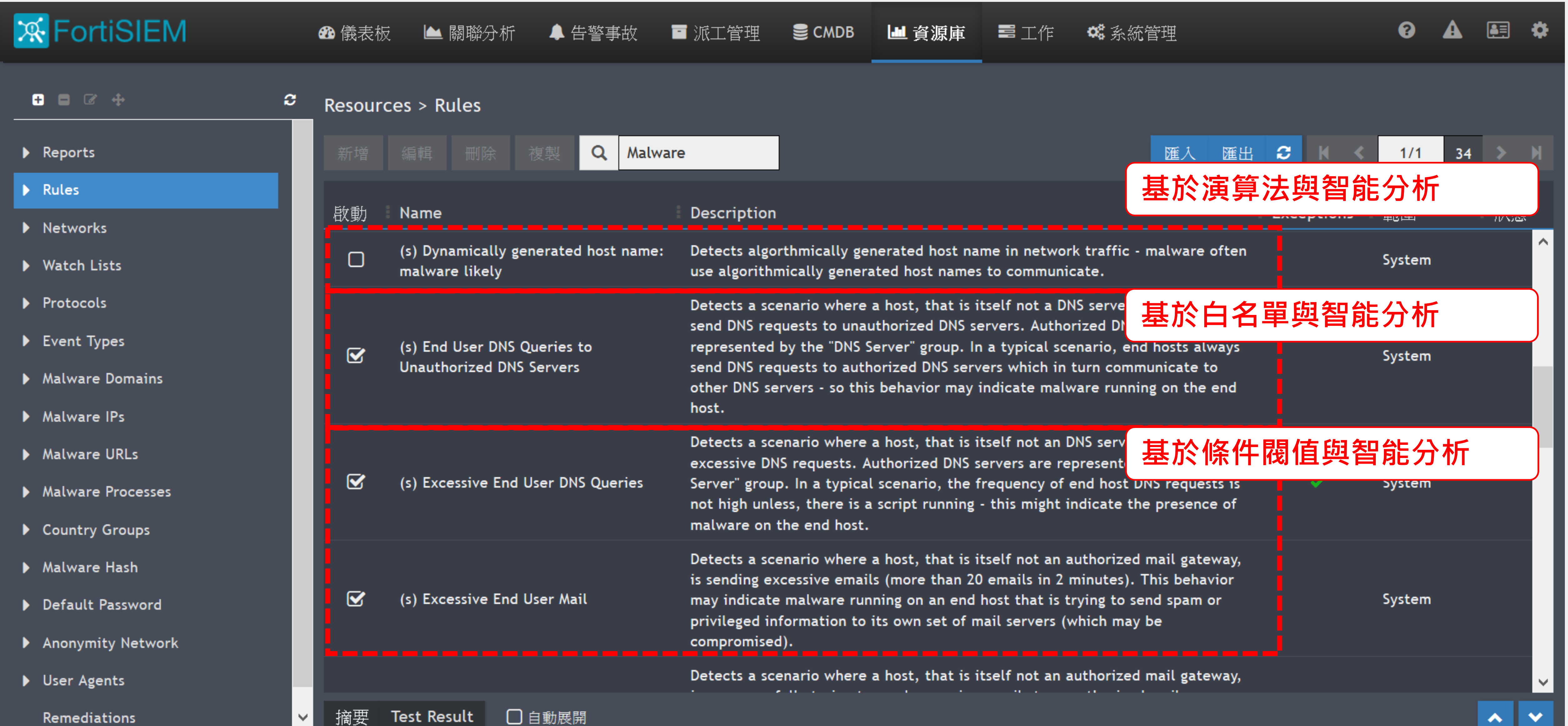


Resources > Rules

啟動	Name	Description	Exceptions	範圍	測試狀態
☑	(s) AI: File Creation Anomaly	FortiInsight AI module detects unusual file Creation by an user		System	
☑	(s) AI: File Deletion Anomaly	FortiInsight AI module detects unusual file deletion by an user		System	
☑	(s) AI: File Reading Anomaly	FortiInsight AI module detects unusual file reading by an user		System	
☑	(s) AI: File Writing Anomaly	FortiInsight AI module detects unusual file writing by an user		System	
☑	(s) AI: Process Started Anomaly	FortiInsight AI module detects unusual process started by an user		System	
☑	(s) AI: Process Stopped Anomaly	FortiInsight AI module detects unusual process stoppage by an user		System	
☑	(s) ARP Exploit	Detects ARP attack		System	
☑	(s) AWS SecHub: Host Vulnerability Detected	AWS Security Hub detected host vulnerability		System	
☑	(s) AWS SecHub: Software and Configuration Violation	AWS Security and Configuration Violation Detected		System	
☑	(s) AWS SecHub: Tactics: Collection Detected	AWS Security Hub detected Collection tactics. Adversary is trying to collect data of their interest.		System	
☑	(s) AWS SecHub: Tactics:	AWS Security Hub detected Command and Control tactics. Adversary is trying to communicate with other compromised systems and receive commands and		System	

智能分析 (AI)，機器學習 (ML) 分析異常行為

AI / ML 告警事故規則



Resources > Rules

Malware

啟動	Name	Description	範圍
☐	(s) Dynamically generated host name: malware likely	Detects algorthmically generated host name in network traffic - malware often use algorithmically generated host names to communicate.	System
☑	(s) End User DNS Queries to Unauthorized DNS Servers	Detects a scenario where a host, that is itself not a DNS serve send DNS requests to unauthorized DNS servers. Authorized D represented by the "DNS Server" group. In a typical scenario, end hosts always send DNS requests to authorized DNS servers which in turn communicate to other DNS servers - so this behavior may indicate malware running on the end host.	System
☑	(s) Excessive End User DNS Queries	Detects a scenario where a host, that is itself not an DNS serv excessive DNS requests. Authorized DNS servers are represent Server" group. In a typical scenario, the frequency of end host DNS requests is not high unless, there is a script running - this might indicate the presence of malware on the end host.	System
☑	(s) Excessive End User Mail	Detects a scenario where a host, that is itself not an authorized mail gateway, is sending excessive emails (more than 20 emails in 2 minutes). This behavior may indicate malware running on an end host that is trying to send spam or privileged information to its own set of mail servers (which may be compromised).	System
		Detects a scenario where a host, that is itself not an authorized mail gateway,	

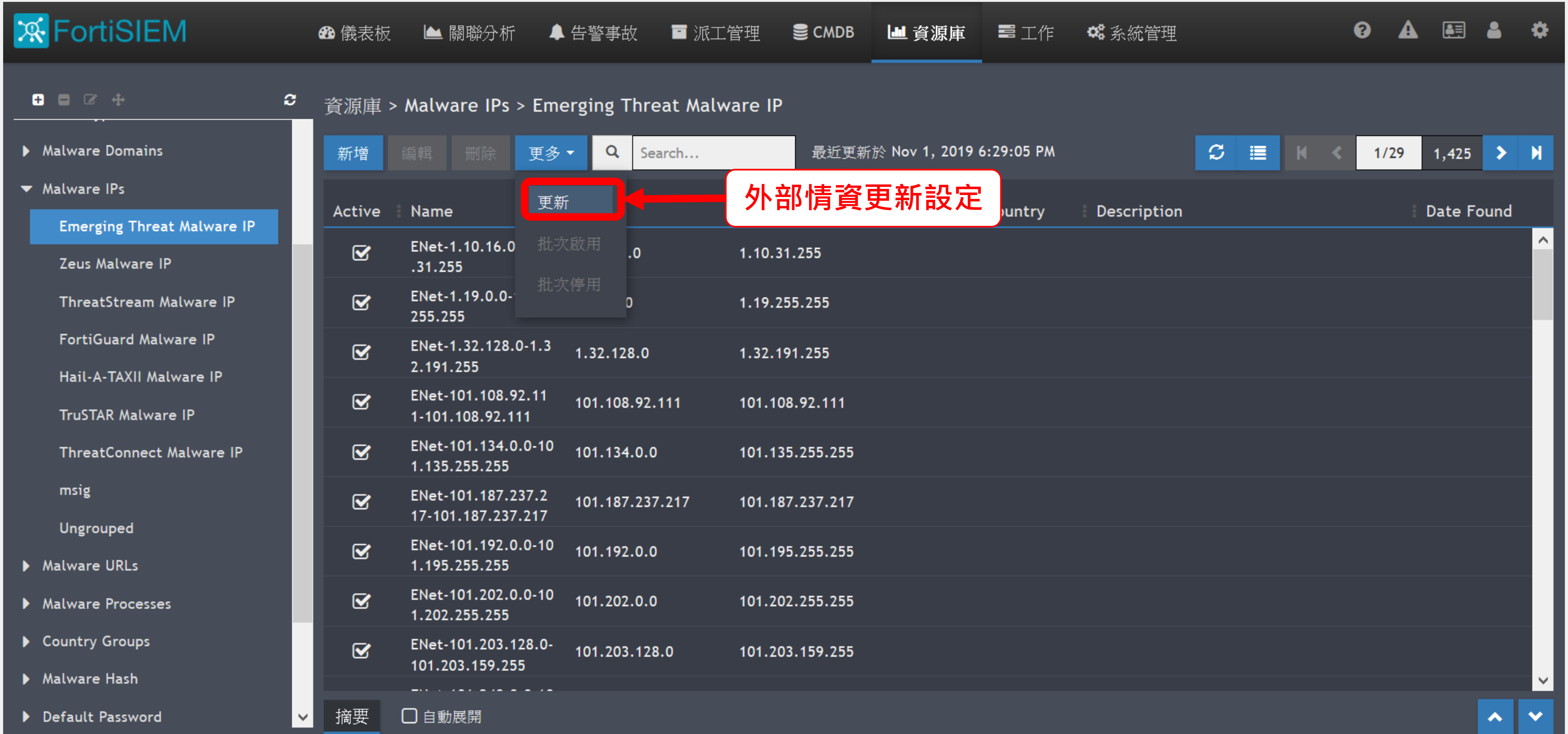
基於演算法與智能分析

基於白名單與智能分析

基於條件閥值與智能分析

整合及自動外部情資更新 (內建或自行設定)

網域、IP地址、URL網址、程式及程式雜湊的情資交換與分析告警



資源庫 > Malware IPs > Emerging Threat Malware IP

最近更新於 Nov 1, 2019 6:29:05 PM

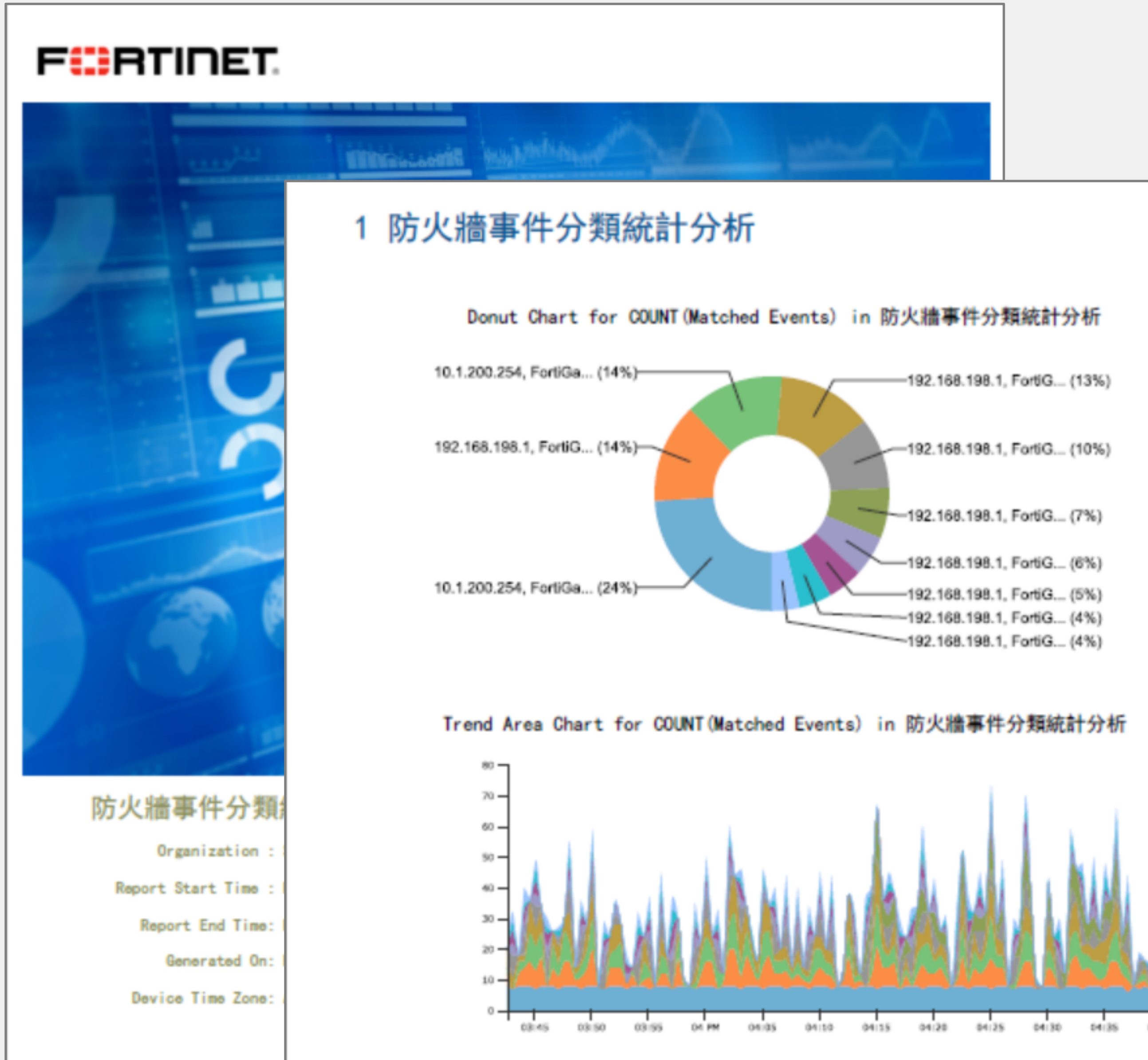
外部情資更新設定

Active	Name			untry	Description	Date Found
☑	ENet-1.10.16.0 .31.255	.0	1.10.31.255			
☑	ENet-1.19.0.0- 255.255	0	1.19.255.255			
☑	ENet-1.32.128.0-1.32.191.255	1.32.128.0	1.32.191.255			
☑	ENet-101.108.92.111-101.108.92.111	101.108.92.111	101.108.92.111			
☑	ENet-101.134.0.0-101.135.255.255	101.134.0.0	101.135.255.255			
☑	ENet-101.187.237.217-101.187.237.217	101.187.237.217	101.187.237.217			
☑	ENet-101.192.0.0-101.195.255.255	101.192.0.0	101.195.255.255			
☑	ENet-101.202.0.0-101.202.255.255	101.202.0.0	101.202.255.255			
☑	ENet-101.203.128.0-101.203.159.255	101.203.128.0	101.203.159.255			

豐富的內建合規性報表

提供彈性的報表客製化能力

- 數以千計的內建報表樣板可供選擇
- 合規性報表 (Compliance Reports)
  - PCI – HIPAA – FERPA
  - SOX, NERC, COBIT, ITIL,
  - ISO, GLBA, GPG13
  - SANS Critical Controls
- 報表客製化建構器
  - 2,000+ 可客製化欄位
  - 封面客製化能力
  - 支持多段落報表格式
  - 豐富可視性圖表，可穿插文字與附件



防火牆事件分類

Organization :

Report Start Time :

Report End Time:

Generated On:

Device Time Zone:

1 防火牆事件分類統計分析

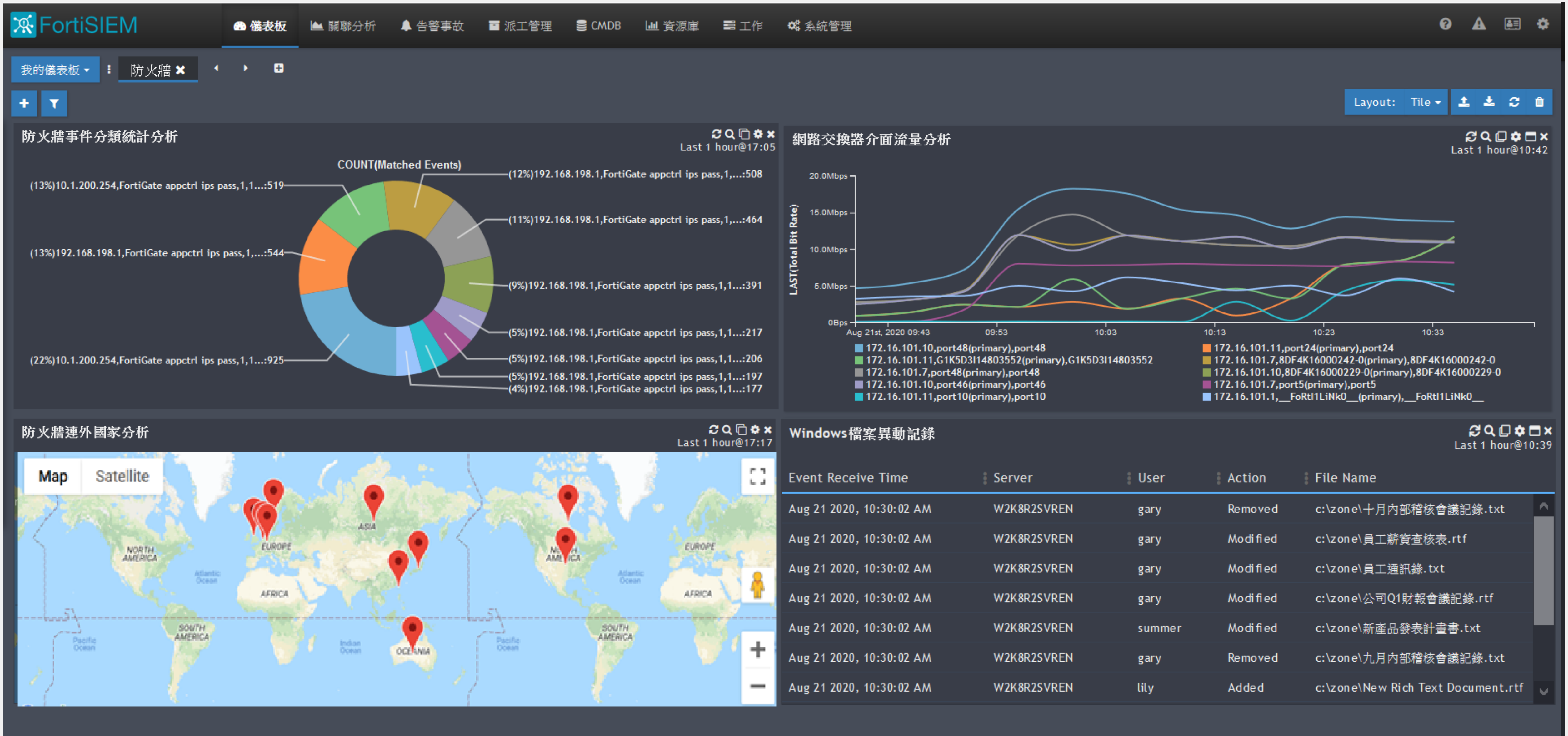
Donut Chart for COUNT(Matched Events) in 防火牆事件分類統計分析

Trend Area Chart for COUNT(Matched Events) in 防火牆事件分類統計分析

FORTINET
10.1.200.254, FortiGa... (14%)
192.168.198.1, FortiG... (14%)
10.1.200.254, FortiGa... (24%)
192.168.198.1, FortiG... (13%)
192.168.198.1, FortiG... (10%)
192.168.198.1, FortiG... (7%)
192.168.198.1, FortiG... (6%)
192.168.198.1, FortiG... (5%)
192.168.198.1, FortiG... (4%)
192.168.198.1, FortiG... (4%)
80
70
60
50
40
30
20
10
0

關聯分析結果可輕鬆轉成各式監看儀表板

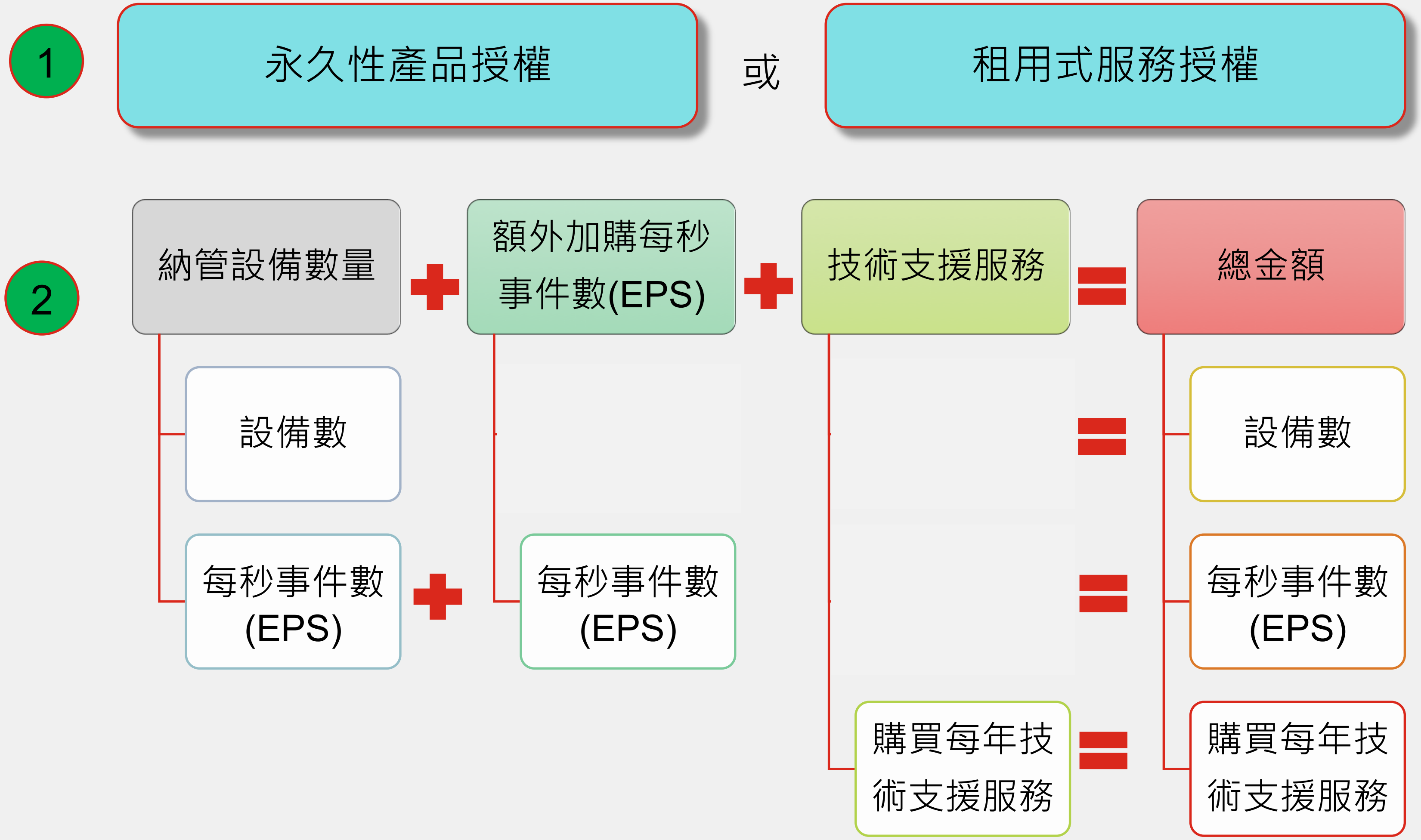
任何關聯分析結果都可變成您的儀表板


FortiSIEM
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
我的儀表板
防火牆
Layout: Tile
防火牆事件分類統計分析
Last 1 hour@17:05
COUNT(Matched Events)
(13%)10.1.200.254,FortiGate appctrl ips pass,1,1...:519
(13%)192.168.198.1,FortiGate appctrl ips pass,1,...:544
(22%)10.1.200.254,FortiGate appctrl ips pass,1,1...:925
(12%)192.168.198.1,FortiGate appctrl ips pass,1,...:508
(11%)192.168.198.1,FortiGate appctrl ips pass,1,...:464
(9%)192.168.198.1,FortiGate appctrl ips pass,1,1...:391
(5%)192.168.198.1,FortiGate appctrl ips pass,1,1...:217
(5%)192.168.198.1,FortiGate appctrl ips pass,1,1...:206
(5%)192.168.198.1,FortiGate appctrl ips pass,1,1...:197
(4%)192.168.198.1,FortiGate appctrl ips pass,1,1...:177
網路交換器介面流量分析
Last 1 hour@10:42
LAST(Total Bit Rate)
20.0Mbps
15.0Mbps
10.0Mbps
5.0Mbps
0Bps
Aug 21st, 2020 09:43
09:53
10:03
10:13
10:23
10:33
172.16.101.10,port48(primary),port48
172.16.101.11,G1K5D3I14803552(primary),G1K5D3I14803552
172.16.101.7,port48(primary),port48
172.16.101.10,port46(primary),port46
172.16.101.11,port10(primary),port10
172.16.101.11,port24(primary),port24
172.16.101.7,8DF4K16000242-0(primary),8DF4K16000242-0
172.16.101.10,8DF4K16000229-0(primary),8DF4K16000229-0
172.16.101.7,port5(primary),port5
172.16.101.1,__FoRtI1LiNk0__(primary),__FoRtI1LiNk0__
防火牆連外國家分析
Last 1 hour@17:17
Map
Satellite
NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
Atlantic Ocean
Pacific Ocean
Indian Ocean
Windows檔案異動記錄
Last 1 hour@10:39

Event Receive Time	Server	User	Action	File Name
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	gary	Removed	c:\zone\十月內部稽核會議記錄.txt
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	gary	Modified	c:\zone\員工薪資查核表.rtf
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	gary	Modified	c:\zone\員工通訊錄.txt
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	gary	Modified	c:\zone\公司Q1財報會議記錄.rtf
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	summer	Modified	c:\zone\新產品發表計畫書.txt
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	gary	Removed	c:\zone\九月內部稽核會議記錄.txt
Aug 21 2020, 10:30:02 AM	W2K8R2SVREN	lily	Added	c:\zone\New Rich Text Document.rtf

簡單的軟體授權計算

無隱藏成本，所有功能全開



1 永久性產品授權 或 租用式服務授權

2 納管設備數量 ＋ 額外加購每秒事件數(EPS) ＋ 技術支援服務 ＝ 總金額

設備數 ＝ 設備數

每秒事件數 (EPS) ＋ 每秒事件數 (EPS) ＝ 每秒事件數 (EPS)

購買每年技術支援服務 ＝ 購買每年技術支援服務

3

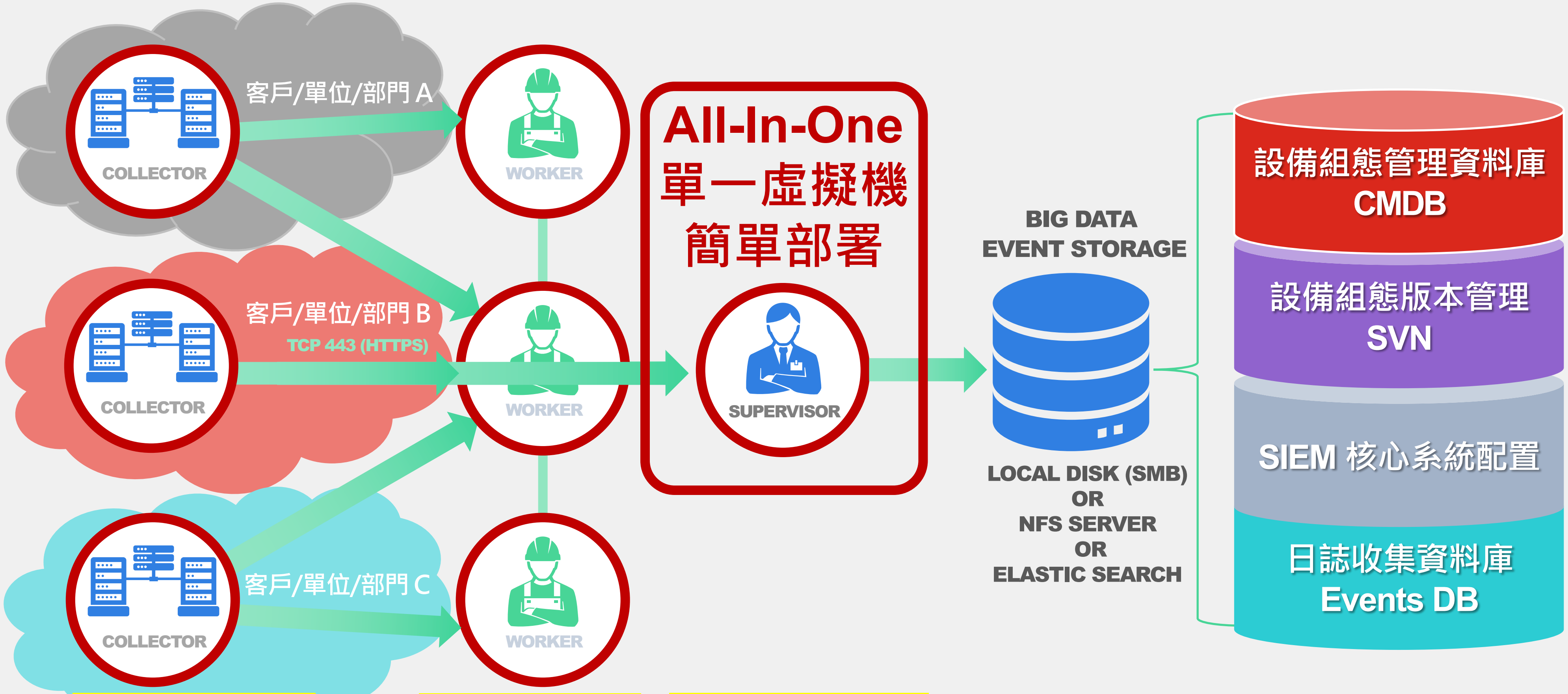
可選購外加服務

- Windows 代理程式授權
- FortiGuard IOC 專業情資訂閱服務
- 專業安裝與客製化服務
- 教育訓練

*EPS: Events per Second

可快速擴容的高彈性架構

支援彈性管理授權與多租戶架構部署 (Multitenant Architecture)



All-In-One
單一虛擬機
簡單部署

設備組態管理資料庫
CMDB

設備組態版本管理
SVN

SIEM 核心系統配置

日誌收集資料庫
Events DB

分散部署
+ 收集器
(Collectors)
虛擬機

效能強化
+ 協作器
(Workers)
虛擬機

系統核心
(Supervisor)
虛擬機

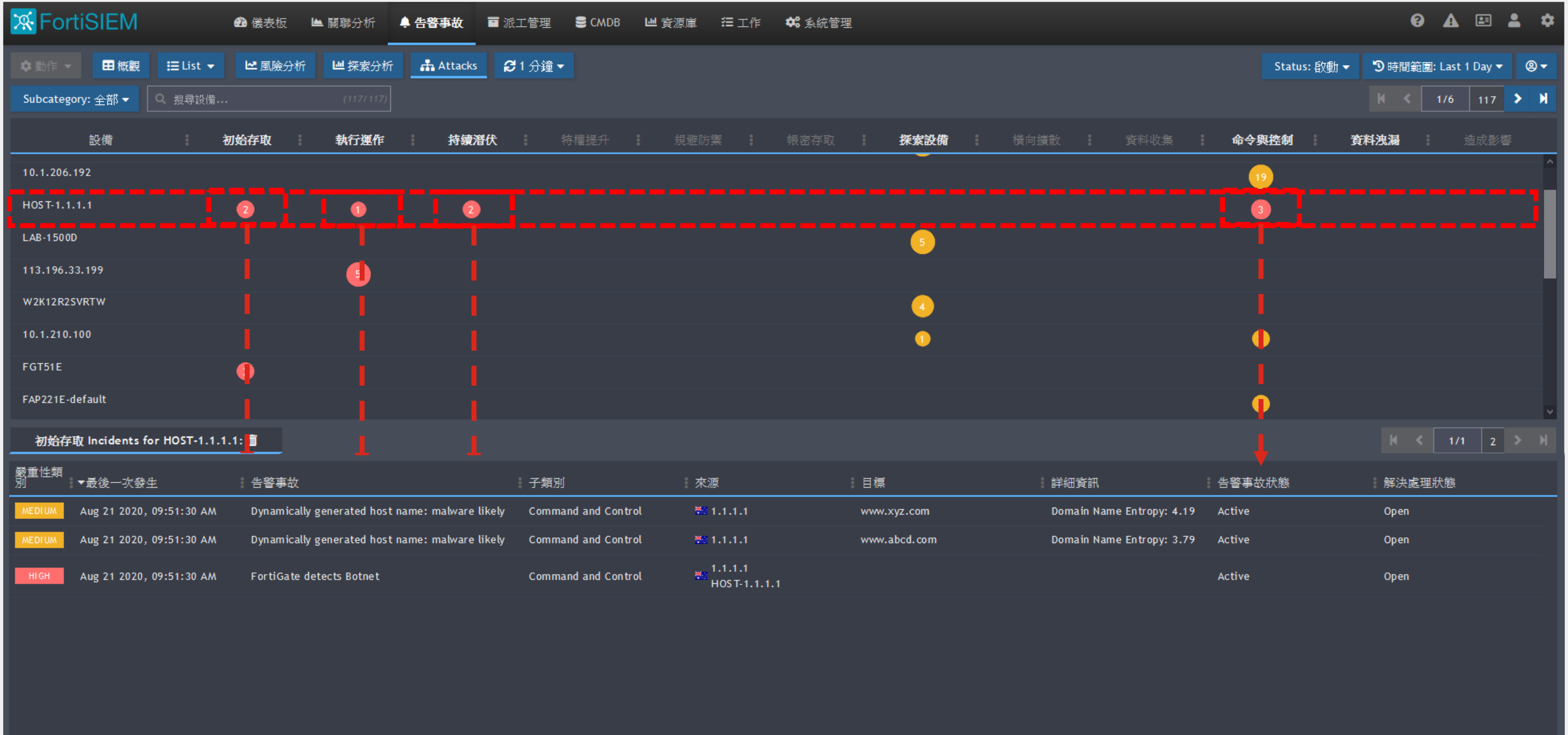
擴大資料儲存節點
(Storage) 或 NFS
虛擬機

MITRE ATT

道高一尺，魔高一丈，資安防護是一場永不休止的戰爭

MITRE ATT&CK 資安對抗策略、手段分類圖

快速了解觸發告警主機在資安攻擊鏈所處的狀態



設備	初始存取	執行運作	持續潛伏	特權提升	規避防禦	帳密存取	探索設備	橫向擴散	資料收集	命令與控制	資料洩漏	造成影響
10.1.206.192										19		
HOST-1.1.1.1	2	1	2							3		
LAB-1500D							5					
113.196.33.199		5										
W2K12R2SVRTW							4					
10.1.210.100							1			[illegible]		
FGT51E	[illegible]											
FAP221E-default										[illegible]		

初始存取 Incidents for HOST-1.1.1.1:

1/1 2

嚴重性類別	▾最後一次發生	告警事故	子類別	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
MEDIUM	Aug 21 2020, 09:51:30 AM	Dynamically generated host name: malware likely	Command and Control	1.1.1.1	www.xyz.com	Domain Name Entropy: 4.19	Active	Open
MEDIUM	Aug 21 2020, 09:51:30 AM	Dynamically generated host name: malware likely	Command and Control	1.1.1.1	www.abcd.com	Domain Name Entropy: 3.79	Active	Open
HIGH	Aug 21 2020, 09:51:30 AM	FortiGate detects Botnet	Command and Control	1.1.1.1 HOST-1.1.1.1			Active	Open

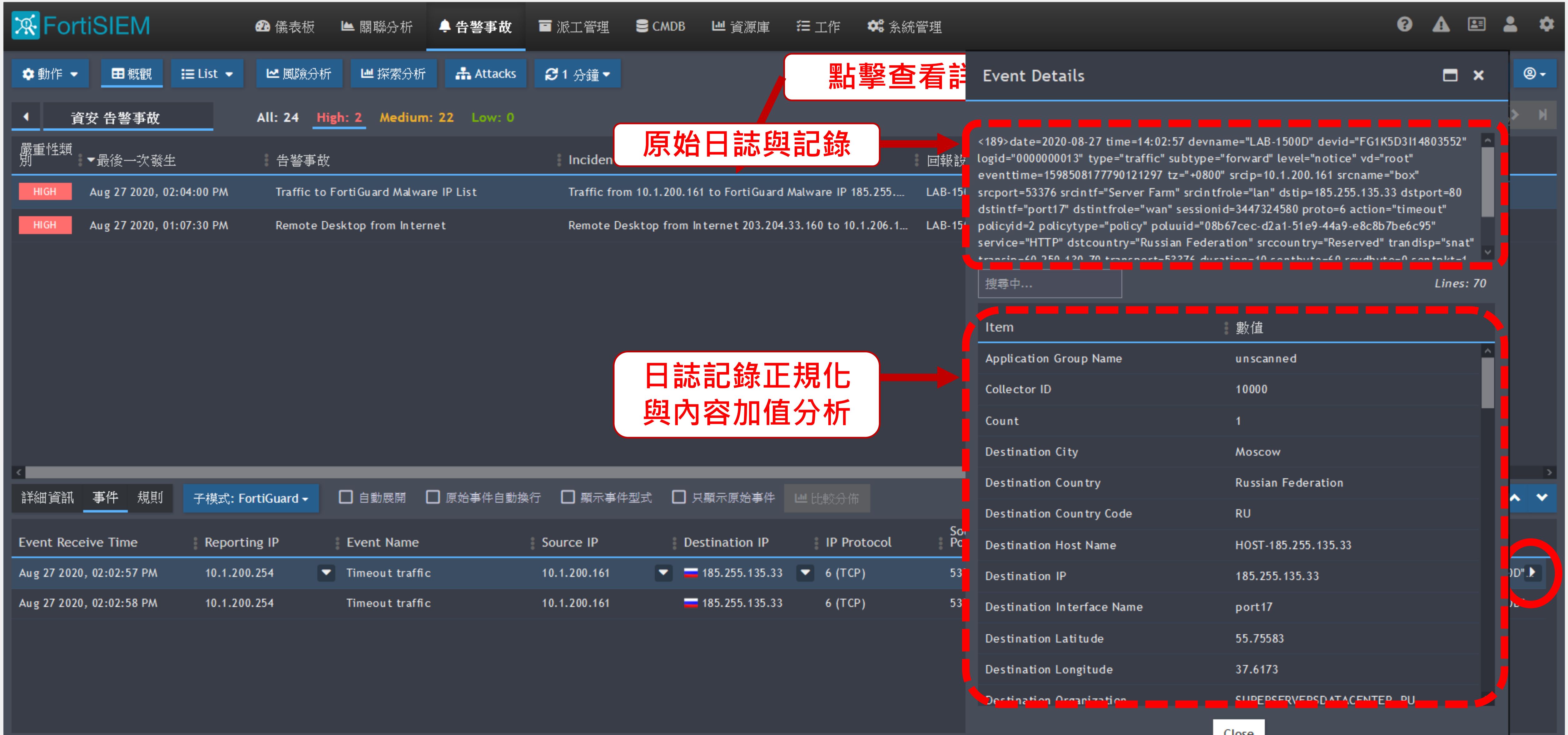
簡單建立標準化事故協作回應流程與自動化 (SOAR)

優化資安維運中心 (SOC)

中央資安事故告警與自動化回應處理

簡單建立標準化事故協作回應流程與自動化 (SOAR)

詳細檢視、追蹤告警事故



點擊查看詳

原始日誌與記錄

日誌記錄正規化
與內容加值分析

All: 24 High: 2 Medium: 22 Low: 0

嚴重性類別	最後一次發生	告警事故	Inciden	回報設
HIGH	Aug 27 2020, 02:04:00 PM	Traffic to FortiGuard Malware IP List	Traffic from 10.1.200.161 to FortiGuard Malware IP 185.255....	LAB-15
HIGH	Aug 27 2020, 01:07:30 PM	Remote Desktop from Internet	Remote Desktop from Internet 203.204.33.160 to 10.1.206.1...	LAB-15

Event Receive Time	Reporting IP	Event Name	Source IP	Destination IP	IP Protocol	So Po
Aug 27 2020, 02:02:57 PM	10.1.200.254	Timeout traffic	10.1.200.161	185.255.135.33	6 (TCP)	53
Aug 27 2020, 02:02:58 PM	10.1.200.254	Timeout traffic	10.1.200.161	185.255.135.33	6 (TCP)	53

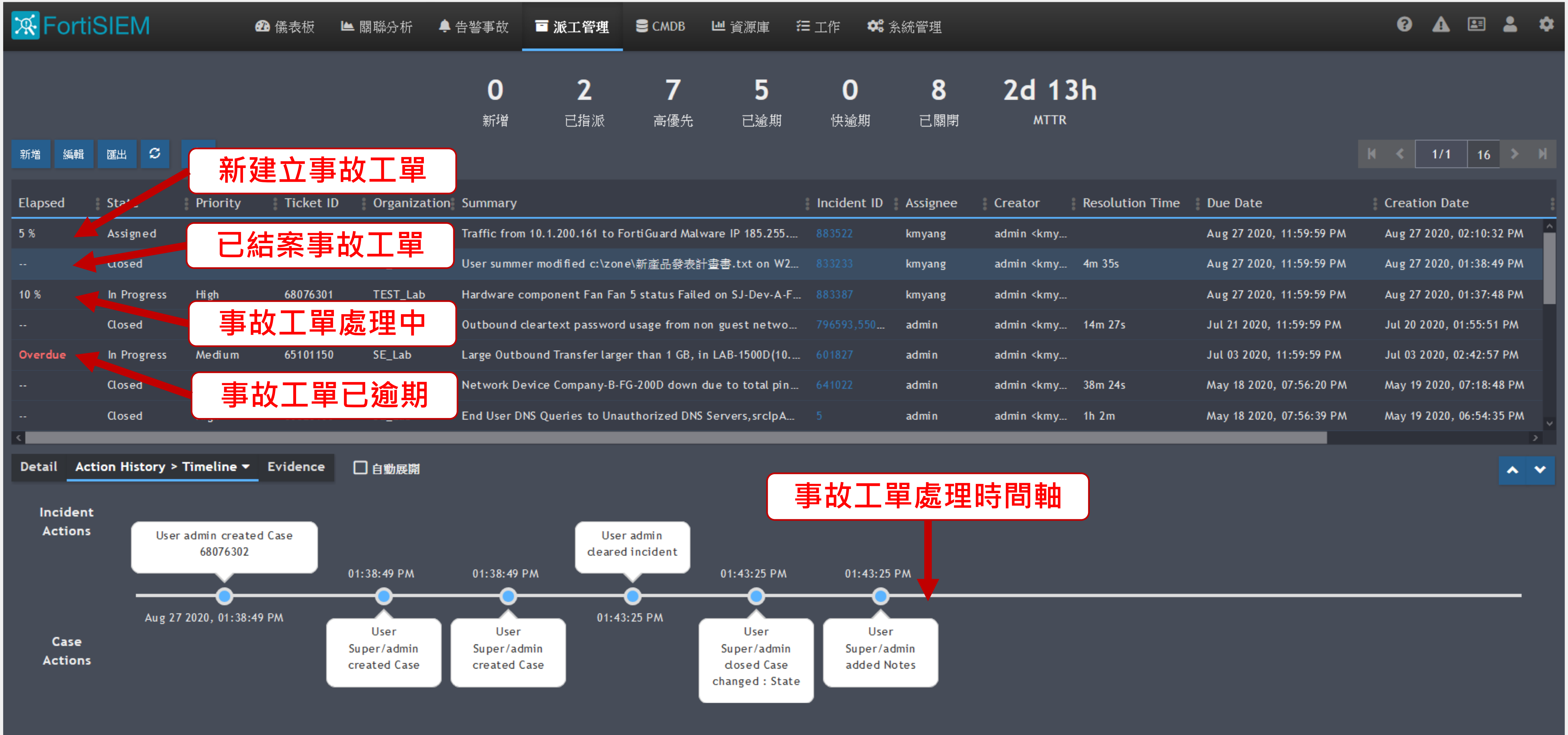
```
<189>date=2020-08-27 time=14:02:57 devname="LAB-1500D" devid="FG1K5D3I14803552"
logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root"
eventtime=1598508177790121297 tz="+0800" srcip=10.1.200.161 srcname="box"
srcport=53376 srcintf="Server Farm" srcintfrole="lan" dstip=185.255.135.33 dstport=80
dstintf="port17" dstintfrole="wan" sessionid=3447324580 proto=6 action="timeout"
policyid=2 policytype="policy" poluuid="08b67cec-d2a1-51e9-44a9-e8c8b7be6c95"
service="HTTP" dstcountry="Russian Federation" srccountry="Reserved" trandisp="snat"
transip=60.250.130.70 transport=53376 duration=10 sentbyte=60 rcvdbyte=0 sentpkt=1
```

Lines: 70

Item	數值
Application Group Name	unscanned
Collector ID	10000
Count	1
Destination City	Moscow
Destination Country	Russian Federation
Destination Country Code	RU
Destination Host Name	HOST-185.255.135.33
Destination IP	185.255.135.33
Destination Interface Name	port17
Destination Latitude	55.75583
Destination Longitude	37.6173
Destination Organization	SUPERSERVERSDATACENTER, RU

簡單建立標準化事故協作回應流程與自動化 (SOAR)

內建派工管理系統，告警事故即時反應並進行追蹤



0	2	7	5	0	8	2d 13h
新增	已指派	高優先	已逾期	快逾期	已關閉	MTTR

新建立事故工單

已結案事故工單

事故工單處理中

事故工單已逾期

Elapsed	Sta	Priority	Ticket ID	Organization	Summary	Incident ID	Assignee	Creator	Resolution Time	Due Date	Creation Date
5 %	Assigned				Traffic from 10.1.200.161 to FortiGuard Malware IP 185.255....	883522	kmyang	admin <kmy...		Aug 27 2020, 11:59:59 PM	Aug 27 2020, 02:10:32 PM
--	Closed				User summer modified c:\zone\新產品發表計畫書.txt on W2...	833233	kmyang	admin <kmy...	4m 35s	Aug 27 2020, 11:59:59 PM	Aug 27 2020, 01:38:49 PM
10 %	In Progress	High	68076301	TEST_Lab	Hardware component Fan Fan 5 status Failed on SJ-Dev-A-F...	883387	kmyang	admin <kmy...		Aug 27 2020, 11:59:59 PM	Aug 27 2020, 01:37:48 PM
--	Closed				Outbound cleartext password usage from non guest netwo...	796593,550...	admin	admin <kmy...	14m 27s	Jul 21 2020, 11:59:59 PM	Jul 20 2020, 01:55:51 PM
Overdue	In Progress	Medium	65101150	SE_Lab	Large Outbound Transfer larger than 1 GB, in LAB-1500D(10....	601827	admin	admin <kmy...		Jul 03 2020, 11:59:59 PM	Jul 03 2020, 02:42:57 PM
--	Closed				Network Device Company-B-FG-200D down due to total pin...	641022	admin	admin <kmy...	38m 24s	May 18 2020, 07:56:20 PM	May 19 2020, 07:18:48 PM
--	Closed				End User DNS Queries to Unauthorized DNS Servers,srcIpA...	5	admin	admin <kmy...	1h 2m	May 18 2020, 07:56:39 PM	May 19 2020, 06:54:35 PM

事故工單處理時間軸

User admin created Case 68076302 — Aug 27 2020, 01:38:49 PM

01:38:49 PM — User Super/admin created Case

01:38:49 PM — User Super/admin created Case

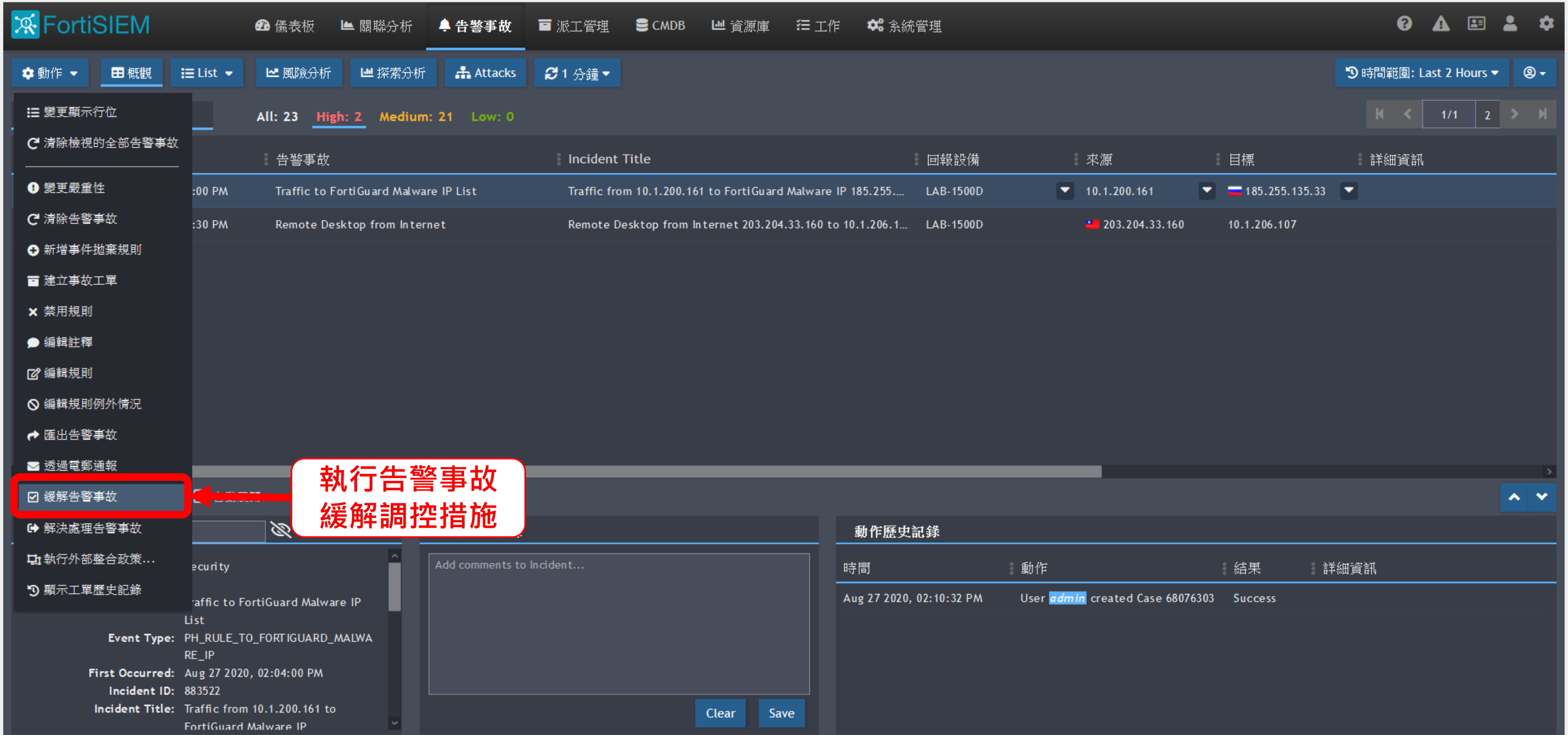
User admin cleared incident — 01:43:25 PM

01:43:25 PM — User Super/admin closed Case changed : State

01:43:25 PM — User Super/admin added Notes

簡單建立標準化事故協作回應流程與自動化 (SOAR)

迅速反應執行緩解調控措施



	告警事故	Incident Title	回報設備	來源	目標	詳細資訊
:00 PM	Traffic to FortiGuard Malware IP List	Traffic from 10.1.200.161 to FortiGuard Malware IP 185.255....	LAB-1500D	10.1.200.161	185.255.135.33	
:30 PM	Remote Desktop from Internet	Remote Desktop from Internet 203.204.33.160 to 10.1.206.1...	LAB-1500D	203.204.33.160	10.1.206.107	

ecurity

affic to FortiGuard Malware IP List

Event Type: PH_RULE_TO_FORTIGUARD_MALWARE_IP

First Occurred: Aug 27 2020, 02:04:00 PM

Incident ID: 883522

Incident Title: Traffic from 10.1.200.161 to FortiGuard Malware IP

Add comments to Incident...

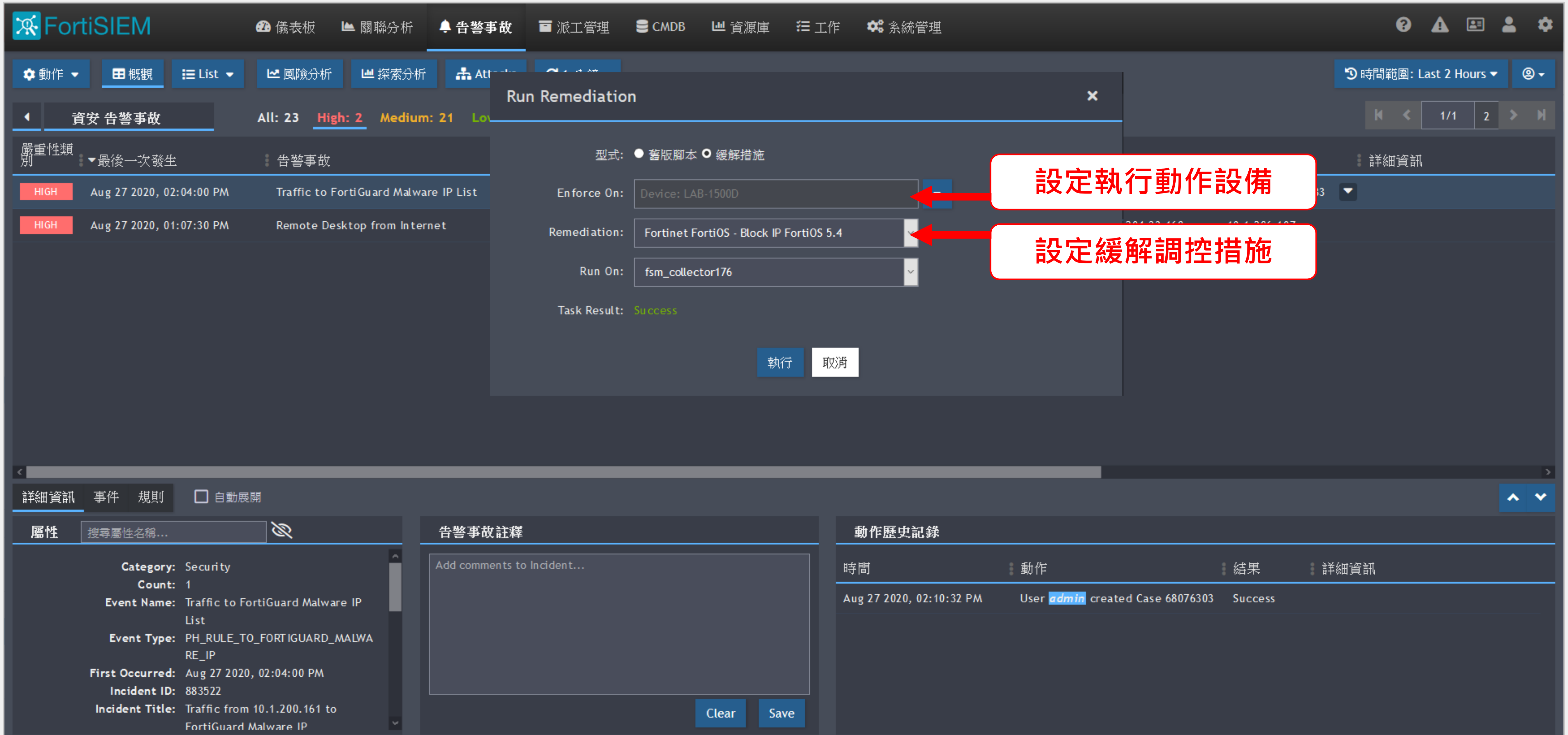
動作歷史記錄

時間	動作	結果	詳細資訊
Aug 27 2020, 02:10:32 PM	User admin created Case 68076303	Success	

執行告警事故
緩解調控措施

簡單建立標準化事故協作回應流程與自動化 (SOAR)

迅速反應執行緩解調控措施



Run Remediation

型式: ○ 舊版腳本 ● 緩解措施

Enforce On: Device: LAB-1500D

Remediation: Fortinet FortiOS - Block IP FortiOS 5.4

Run On: fsm_collector176

Task Result: Success

設定執行動作設備

設定緩解調控措施

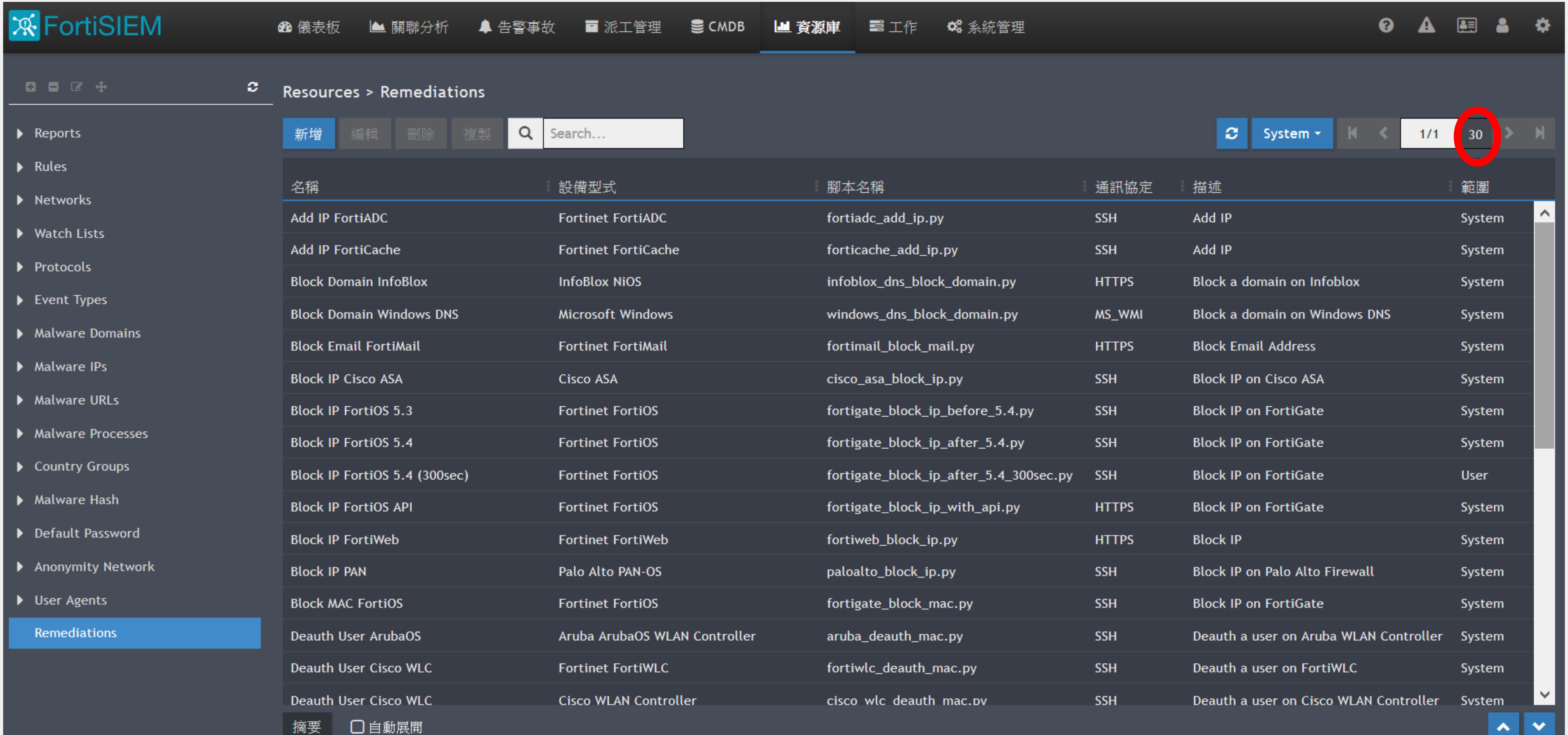
嚴重性類別	最後一次發生	告警事故
HIGH	Aug 27 2020, 02:04:00 PM	Traffic to FortiGuard Malware IP List
HIGH	Aug 27 2020, 01:07:30 PM	Remote Desktop from Internet

Category: Security
Count: 1
Event Name: Traffic to FortiGuard Malware IP List
Event Type: PH_RULE_TO_FORTIGUARD_MALWARE_IP
First Occurred: Aug 27 2020, 02:04:00 PM
Incident ID: 883522
Incident Title: Traffic from 10.1.200.161 to FortiGuard Malware IP

時間	動作	結果	詳細資訊
Aug 27 2020, 02:10:32 PM	User admin created Case 68076303	Success	

簡單建立標準化事故協作回應流程與自動化 (SOAR)

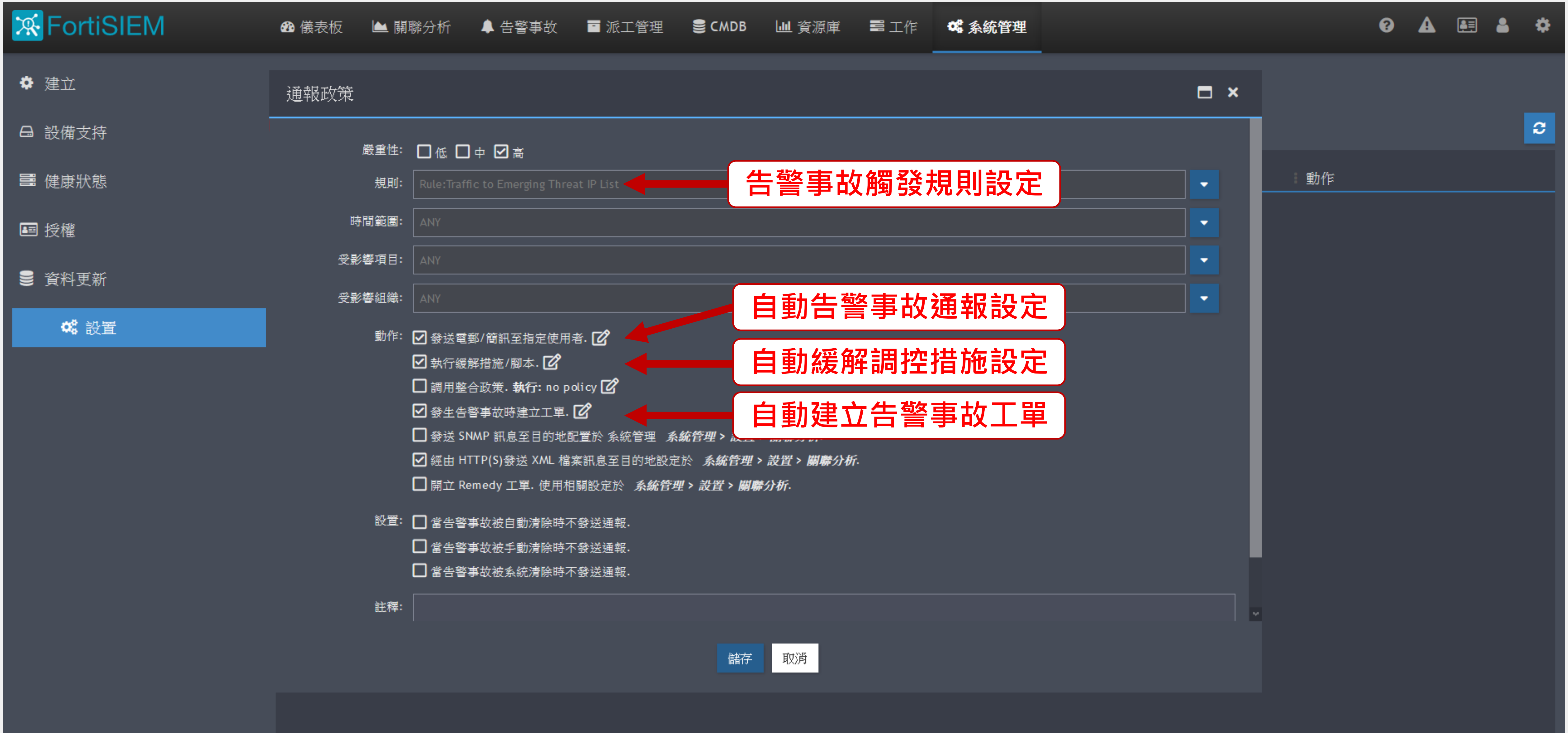
內建緩解調控措施腳本，可與多品牌設備協作聯防



名稱	設備型式	腳本名稱	通訊協定	描述	範圍
Add IP FortiADC	Fortinet FortiADC	fortiadc_add_ip.py	SSH	Add IP	System
Add IP FortiCache	Fortinet FortiCache	forticache_add_ip.py	SSH	Add IP	System
Block Domain InfoBlox	InfoBlox NiOS	infoblox_dns_block_domain.py	HTTPS	Block a domain on Infoblox	System
Block Domain Windows DNS	Microsoft Windows	windows_dns_block_domain.py	MS_WMI	Block a domain on Windows DNS	System
Block Email FortiMail	Fortinet FortiMail	fortimail_block_mail.py	HTTPS	Block Email Address	System
Block IP Cisco ASA	Cisco ASA	cisco_asa_block_ip.py	SSH	Block IP on Cisco ASA	System
Block IP FortiOS 5.3	Fortinet FortiOS	fortigate_block_ip_before_5.4.py	SSH	Block IP on FortiGate	System
Block IP FortiOS 5.4	Fortinet FortiOS	fortigate_block_ip_after_5.4.py	SSH	Block IP on FortiGate	System
Block IP FortiOS 5.4 (300sec)	Fortinet FortiOS	fortigate_block_ip_after_5.4_300sec.py	SSH	Block IP on FortiGate	User
Block IP FortiOS API	Fortinet FortiOS	fortigate_block_ip_with_api.py	HTTPS	Block IP on FortiGate	System
Block IP FortiWeb	Fortinet FortiWeb	fortiweb_block_ip.py	HTTPS	Block IP	System
Block IP PAN	Palo Alto PAN-OS	paloalto_block_ip.py	SSH	Block IP on Palo Alto Firewall	System
Block MAC FortiOS	Fortinet FortiOS	fortigate_block_mac.py	SSH	Block IP on FortiGate	System
Deauth User ArubaOS	Aruba ArubaOS WLAN Controller	aruba_deauth_mac.py	SSH	Deauth a user on Aruba WLAN Controller	System
Deauth User Cisco WLC	Fortinet FortiWLC	fortiwlc_deauth_mac.py	SSH	Deauth a user on FortiWLC	System
Deauth User Cisco WLC	Cisco WLAN Controller	cisco_wlc_deauth_mac.py	SSH	Deauth a user on Cisco WLAN Controller	System

簡單建立標準化事故協作回應流程與自動化 (SOAR)

全面自動化的告警事故反應流程



告警事故觸發規則設定

自動告警事故通報設定

自動緩解調控措施設定

自動建立告警事故工單

通報政策

嚴重性: □ 低 □ 中 ☑ 高

規則: Rule:Traffic to Emerging Threat IP List

時間範圍: ANY

受影響項目: ANY

受影響組織: ANY

動作:
- ☑ 發送電郵/簡訊至指定使用者.
- ☑ 執行緩解措施/腳本.
- □ 調用整合政策. **執行:** no policy
- ☑ 發生告警事故時建立工單.
- □ 發送 SNMP 訊息至目的地配置於 系統管理 ***系統管理 >***
- ☑ 經由 HTTP(S)發送 XML 檔案訊息至目的地設定於 ***系統管理 > 設置 > 關聯分析.***
- □ 開立 Remedy 工單. 使用相關設定於 ***系統管理 > 設置 > 關聯分析.***

設置:
- □ 當告警事故被自動清除時不發送通報.
- □ 當告警事故被手動清除時不發送通報.
- □ 當告警事故被系統清除時不發送通報.

註釋:

FortiSIEM 重要特點與價值

1.資安 (SOC) 與網維 (NOC) 融合式分析

2.自動探索，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.內建派工管理系統，標準化維運流程

Question

- FortiSIEM 擁有哪些特色？(複選題)

  - 1.資安 (SOC) 與網維 (NOC) 融合式分 /自動探索，組態與效能管理 (CMDB) / 可快速擴容的高彈性架構
  - 2.直覺式事件關聯分析，簡單易用 /智能分析 (AI)，機器學習 (ML) /自動更新情資，分析告警與聯防
  - 3.內建工單處理系統，標準化維運流程 / 支援中文化介面

Question

- 下列哪些是FortiSIEM可以做到的？(複選題)

  - 1.滿足法規針對資通安全防護及控制措施等相關要求

  - 2.不同品牌產品的事件，分散收集、集中儲存管理

  - 3.有效並且快速發現潛在威脅 / 建立資安事故反應標準作業流程與緩解動作自動化

FortiSIEM

FORTINET®