



FORTINET[®]

新世代 SIEM 平台 – FortiSIEM AI 驅動的安全營運

Kevin Yang

kmyang@fortinet.com



現今資安與網維面臨的挑戰

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



What is FortiSIEM

新一代 SIEM 管理平台，提供網路及用戶異常行為智能分析

Skilled Personnel

日誌、記錄的收集

壓縮減量，加密傳輸

分散收集，集中彙整儲存

正規化 / 內容增值 / 關聯分析

進階資料搜尋及鑑識能力

即時告警 / 事故反應

資料保留，稽核備查

手動 / 排程定期產生報表

資安 (SOC) 與網維 (NOC) 融合式分析

自動探索，組態與效能管理 (CMDB)

可快速擴容的高彈性架構

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

內建派工管理系統，標準化維運流程

傳統 SIEM 基本功能

新一代 SIEM 平台

更好的可視性 (**Visibility**) 與擴容性 (**Scalability**)

降低維運管理複雜度 (**Less Complexity**)



資安 (SOC) 與網維 (NOC) 融合式分析

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



資安 (SOC) 與網維 (NOC) 融合式分析

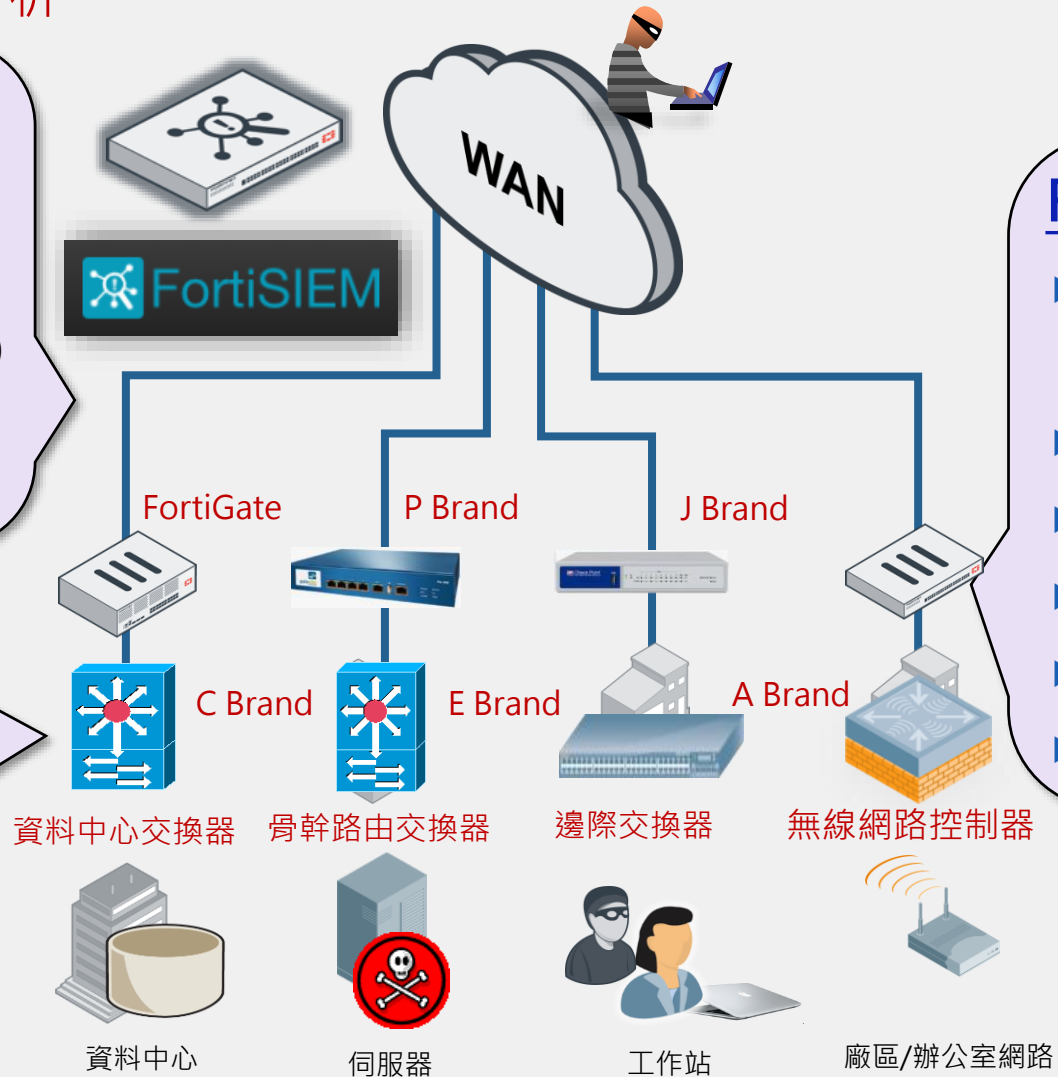
多源、多品牌日誌記錄統整與關聯分析

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

自動身分識別與連網位置關聯分析

快速查找人員與設備，何時、何地以及如何連網

The screenshot shows the FortiSIEM interface with the 'Identity & Location' module selected. The table displays network activity logs with columns for IP Address, MAC Address, User, Host Name, Domain, VLAN ID, Connected to, First Seen, and Last Seen. Red boxes highlight these columns, and red arrows point from callout boxes to specific data points. The callout boxes contain the following text:

- 來自 DHCP 日誌 (From DHCP log)
- 來自 AD 登入日誌 (From AD login log)
- 來自 L2 交換器自動探索記錄 (From L2 switch auto-discovery log)
- 來自所有相關日誌或記錄 (From all related logs or records)

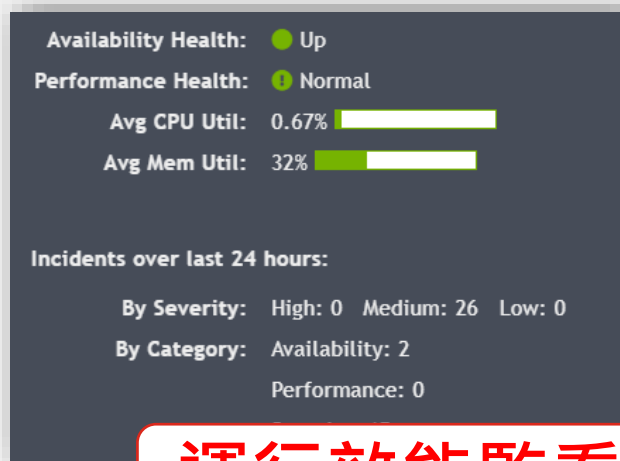
IP Address	MAC Address	User	Host Name	Domain	VLAN ID	Connected to	First Seen	Last Seen
192.168.26.120	00:26:b9:1f:3b:76	sara.tanner (Domain)	stanner-laptop	ACCELOPS			Jun 24, 2021 1:58:41 AM	Jul 9, 2021 1:55:11 AM
192.168.64.187	00:0c:29:9d:d4:c6	svc_monitor (Domain)	lab03-ws14SCw8-2	ACCELOPS	22	ph-network-3560_1 192.168.19.1 (GigabitEthernet0/14)	Jun 24, 2021 1:23:52 AM	Jul 9, 2021 1:56:08 AM
192.168.20.116	00:0c:29:4e:e1:e8	svc_monitor (Domain)	lab03-ws14SCw8	ACCELOPS	30	SJ-Main-Cat6500 192.168.20.1 (GigabitEthernet1/36)	Jun 24, 2021 1:23:52 AM	Jul 9, 2021 1:56:18 AM
192.168.26.102	00:23:5a:3e:62:69	ANONYMOUS (Domain)	lab02-ws07SCw8-LAPTOP	NT			Jul 9, 2021 1:04:07 AM	Jul 9, 2021 1:54:42 AM
192.168.26.109	00:24:d6:4c:f0:d0	greg.allan (Domain)	greg.allan-LAPTOP	ACCELOPS			Jul 9, 2021 1:00:53 AM	Jul 9, 2021 1:55:20 AM
192.168.64.195	00:0c:29:1e:a1:d8		sdavis-desktop		3	SJ-Main-Cat6500 192.168.20.1 (GigabitEthernet0/11)	Jul 9, 2021 2:00:01 AM	Jul 9, 2021 2:00:01 AM
62.210.247.100		don.freeman (VPN)				192.168.19.65	Jul 9, 2021 2:00:02 AM	Jul 9, 2021 2:00:02 AM
192.168.26.109	00:24:d6:4c:f0:d0		kpeterson-laptop				Jul 9, 2021 2:00:02 AM	Jul 9, 2021 2:00:02 AM

自動探索，設備組態管理資料庫 (CMDB)

學習了解您的網路環境並建立基準線



設備識別分類



運行效能監看

摘要 屬性 監看 軟體 硬體 組態配置

Diff... 刪除 Export

Rev	Date	Type/File Name
40	Jul 08 2021, 07:11:30 PM	startup-config
39	Jul 08 2021, 01:03:54 PM	startup-config

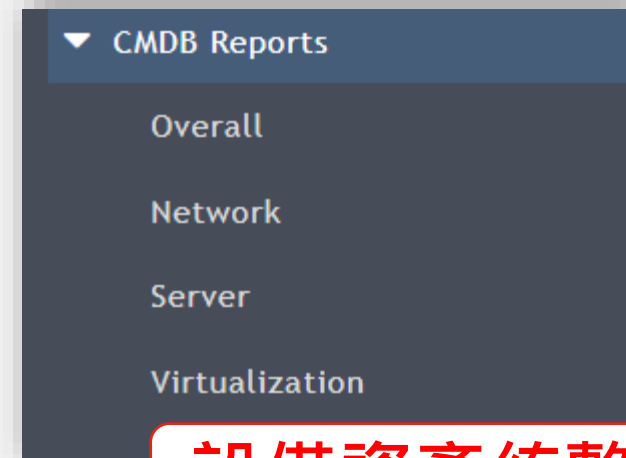
組態配置監看



應用導向管理



威脅情資比對



設備資產統整



自動探索，設備組態管理資料庫 (CMDB)

詳細檢視設備資訊、資安態勢、效能狀況、組態異動比對

The screenshot displays the FortiSIEM interface with a 'Configuration Diff' window open. The window compares configurations for two devices, likely 'CoreFW' and 'FGT51E'. The diff shows several configuration changes, with some highlighted in yellow to indicate differences.

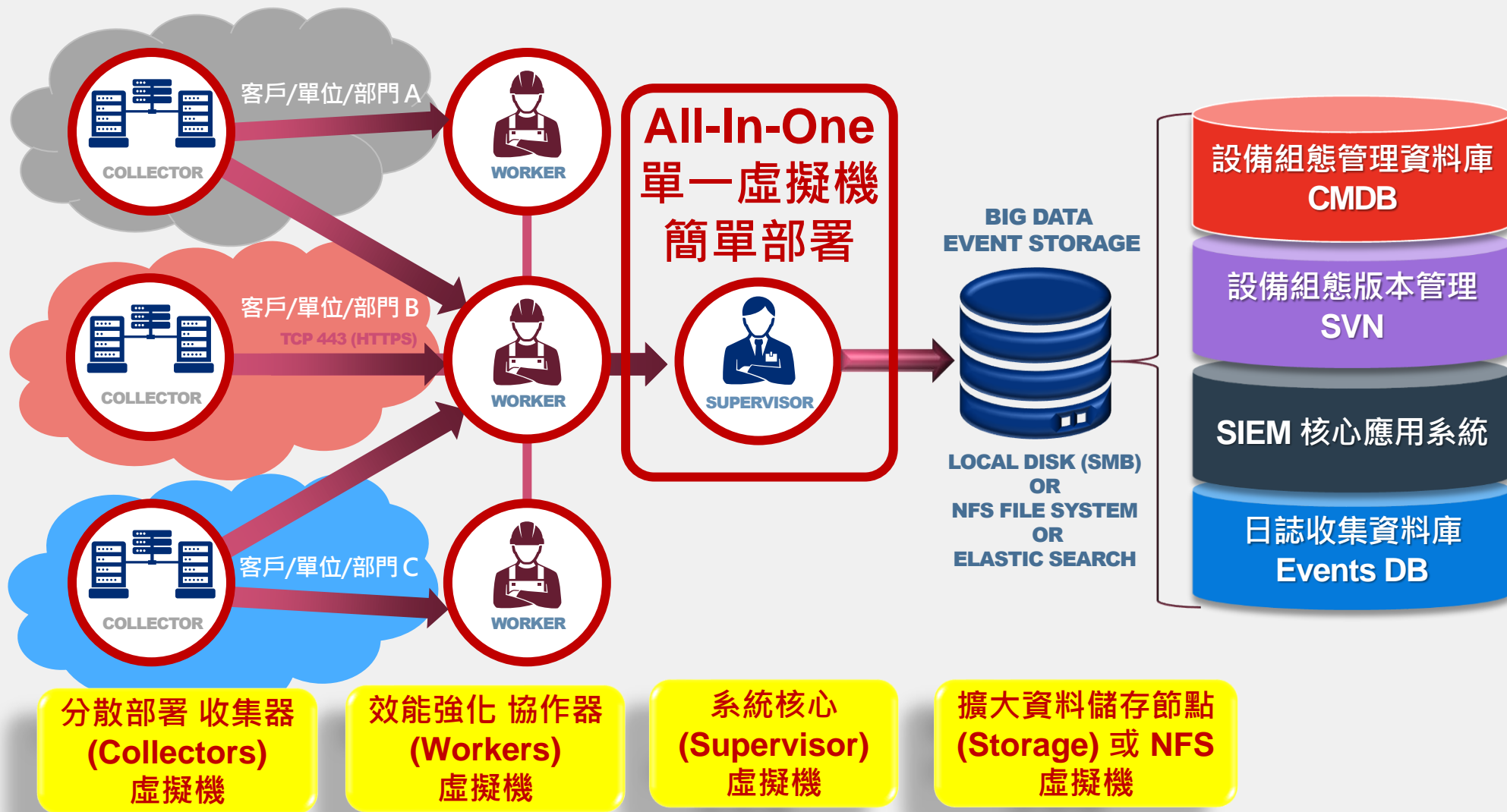
Line	Device 1 Configuration	Device 2 Configuration
60589	set poe-pre-standard-detection enable	set poe-pre-standard-detection enable
60590	set poe-capable 1	set poe-capable 1
60591	set vlan "Josh"	set vlan "vsw.FortiLink"
60592	set allowed-vlans-all disable	set allowed-vlans-all enable
60593	set allowed-vlans "qtn.FortiLink"	
60594	set untagged-vlans "qtn.FortiLink"	set untagged-vlans "qtn.FortiLink"
60595	set type physical	set type physical
60596	set dhcp-snooping untrusted	set dhcp-snooping untrusted
60597	set dhcp-snoop-option82-trust disable	set dhcp-snoop-option82-trust disable
60598	set arp-inspection-trust untrusted	set arp-inspection-trust untrusted
60599	set igmp-snooping enable	set igmp-snooping enable
60600	set igmps-flood-reports disable	set igmps-flood-reports disable
60601	set igmps-flood-traffic disable	set igmps-flood-traffic disable
60602	set stp-state enabled	set stp-state enabled
60603	set stp-root-guard disabled	set stp-root-guard disabled
60604	set stp-bpdu-guard disabled	set stp-bpdu-guard disabled
60605	set edge-port enable	set edge-port enable
60606	set discard-mode none	set discard-mode none
60607	set packet-sampler disabled	set packet-sampler disabled
60608	set sflow-counter-interval 0	set sflow-counter-interval 0

Navigation buttons at the bottom of the diff window: Top, Bottom, Previous, Next, Close.

The background interface shows a sidebar with device categories like 'Network Device', 'Firewall', 'Router Switch', etc., and a main panel displaying a list of configuration revisions (Rev, Date, Type/File Name) and a detailed configuration view.

可快速擴容的高彈性架構

支援彈性分層管理權限與多租戶架構部署 (Multitenant Architecture)



直覺式的事件關聯分析簡單易用

以人為本的操作邏輯，過濾及顯示繁雜事件，減輕人員負擔

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

動作 [1] 搜尋

Reporting IP IN Devices: Firewall AND (Event Type CONTAIN FortiGate-auth OR Event Typi 執行

過濾條件

- 事件關鍵字
- 事件屬性

括號	屬性	運算符	數值	括號	下一步	列位
+ -	Reporting IP	IN	Devices: Firewall	+ -	AND	+ -
+ - (Event Type	CONTAIN	FortiGate-auth	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-webfilter	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-event	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-antivirus	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-ips	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-dlp	+ -)	AND	+ -

載入 儲存 清除全部

15m 1h 1d 7d 30d

顯示

時間範圍

- 即時發生
- 相對時間 最近的 1 Hour
- 絕對時間

定義想關聯分析甚麼?

定義資料搜尋時間範圍?

直覺式的事件關聯分析簡單易用

以人為本的操作邏輯，過濾及顯示繁雜事件，減輕人員負擔

The screenshot displays the FortiSIEM interface for configuring event correlation analysis. The top navigation bar includes icons for Dashboard (儀表板), Correlation Analysis (關聯分析), Alerts (告警事故), Ticket Management (派工管理), CMDB, Resource Library (資源庫), Work (工作), and System Management (系統管理). The main search bar contains the query: "Reporting IP IN Devices: Firewall AND (Event Type CONTAIN FortiGate-auth OR Event Typ".

A red callout box with the text "定義如何顯示分析結果?" (Define how to display analysis results?) points to the "群組條件與顯示欄位" (Group conditions and display fields) table. This table allows users to select attributes, set their order, choose how they are displayed, and manage their column positions.

屬性	次序	顯示為	列位	移動
Reporting IP	▼		+ -	↑ ↓
Event Type	▼		+ -	↑ ↓
Event Name	▼		+ -	↑ ↓
Event Severity	▼		+ -	↑ ↓
Source IP	▼		+ -	↑ ↓
Destination IP	▼		+ -	↑ ↓
COUNT(Matched Events)	▼		+ -	↑ ↓

Below this table is the "顯示條件" (Display conditions) section, which includes a table for defining logical conditions:

括號	屬性	運算符	數值	括號	下一步	列位
+ -	▼	▼		+ -	AND ▼	+ -

At the bottom right, there are buttons for "套用並執行" (Apply and execute), "套用" (Apply), and "取消" (Cancel).

直覺式的事件關聯分析簡單易用

以人為本的操作邏輯，過濾及顯示繁雜事件，減輕人員負擔



關聯分析結果可產生各式報表

手動或排程自動產生報表

1 防火牆事件分類分析

防火牆事件分類圖

10.1.200.254, FortiGa... (23%):15k

10.1.200.254, FortiGate-event-dns-query, I

10.1.200.254, FortiGate-event-dns-query, I

10.1.200.254, FortiGate-event-dns-query, I

10.1.200.254, FortiGate-event-dns-ftgd-cat

防火牆事件分類趨勢圖

Organization : Demo_Lab
Report Start Time : Jul 19 2021, 10:16:57 PM CST
Report End Time : Jul 19 2021, 11:16:56 PM CST
Generated On : Jul 19 2021, 11:32:46 PM CST
Device Time Zone : Asia/Taipei

10.1.200.254, FortiGate-event-dns-ftgd-cat-allow, FortiGate event dns ftgd cat allow, 3, 10.1.206.192, 8.8.8.8

10.1.200.254, FortiGate-event-dns-ftgd-cat-allow, FortiGate event dns ftgd cat allow, 3, 10.1.206.192, 168.95.1.1

10.1.200.254, FortiGate-event-dns-query, FortiGate event dns query, 1, 10.1.206.192, 8.8.8.8

10.1.200.254, FortiGate-event-dns-query, FortiGate event dns query, 1, 10.1.206.192, 168.95.1.1

10.1.200.254, FortiGate-event-dns-query, FortiGate event dns query, 1, 10.1.206.100, 8.8.8.8

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, SOX, HIPAA, FISMA
 - NERC, COBIT, ITIL, NIST
 - ISO, GLBA, GPG13, CIS
 - SANS Critical Controls
- OT 設備相關報表
- 報表客製化建構器
 - 3,000+ 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

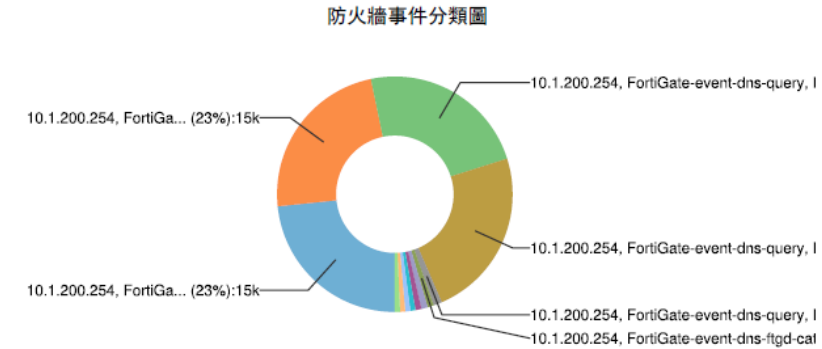
FORTINET



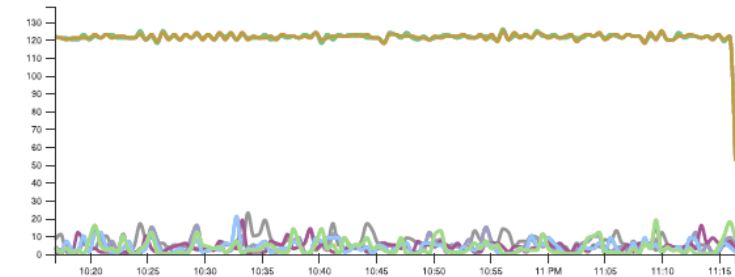
防火牆事件分類分析報告

Organization : Demo_Lab
Report Start Time : Jul 19 2021, 10:16:57
Report End Time : Jul 19 2021, 11:16:56
Generated On: Jul 19 2021, 11:32:46
Device Time Zone: Asia/Taipei

1 防火牆事件分類分析



防火牆事件分類趨勢圖



關聯分析結果可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



關聯分析結果可產生規則，觸發告警事故

輕鬆監看及告警您關心的事件

The screenshot displays the FortiSIEM interface in '編輯子模式' (Edit Sub-mode). The main window is titled 'Filter_1' and is used for configuring correlation rules. It features a table for '過濾條件' (Filter Conditions) and a '彙總' (Summary) section.

過濾條件 (Filter Conditions):

括號	屬性	運算符	數值	括號	下一步	列位
+ -	Reporting IP	IN	Devices: Firewall	+ -	AND	+ -
+ - (Event Type	CONTAIN	FortiGate-auth	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-webfilter	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-event	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-antivirus	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-ips	+ -	OR	+ -
+ -	Event Type	CONTAIN	FortiGate-dlp	+ -)	AND	+ -

彙總 (Summary):

括號	屬性	運算符	數值	下一步	列位
+ -	COUNT(Matched Events)	>=	1		+ -

群組分類依 (Group Classification):

屬性	列位	移動
Reporting IP	+ -	↑ ↓
Event Type	+ -	↑ ↓

Annotations in the image:

- A red callout box with the text '自動帶入關聯分析條件' (Automatically import correlation analysis conditions) points to the '數值' (Value) column of the filter conditions table.
- A red callout box with the text '定義關聯規則觸發閾值' (Define correlation rule trigger threshold) points to the '數值' (Value) field in the summary section, which is set to '1'.

At the bottom of the interface, there are buttons for '儲存' (Save), '儲存為報告' (Save as Report), '執行查詢' (Execute Query), and '取消' (Cancel).

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 with the 'Resources > Rules' page. A search bar contains 'sudden'. A table of rules is displayed, with a red dashed box highlighting five rules. A red callout box contains the text '基於機器學習 (ML) 基準線與異常行為智能分析'.

已啟用	Severity	Name	Description	Impact	Scope
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase in Disk I/O	hosts - over a 30 minute interval, either the read or write volume is more than 3 standard deviations away from the mean over that same time period and the read/write volume is at least 1 Mbps	Impact	Endpoint Denial of Service: OS Exhaustion Flood (T1499.001)
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase In DNS Requests From A Specific Host	Detects sudden increase in DNS requests from a specific source IP - over a 15 minute period, a particular source IP is doing excessive DNS requests. Excessive DNS requests is defined as at least 100 requests and current count is 3 standard deviations away from mean for the current hour. Excessive Destination names is defined as 50 distinct name resolutions and current count is more than 3 standard deviations away from the mean for the current hour	Command And Control	Dynamic Resolution: Fast Flux DNS (T1568.001)
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase in Failed Logons To A Host	Detects a sudden 50% increase of failed logons to a specific host over a 30 minute window	Initial Access, Persistence, Privilege Escalation, Defense Evasion	Valid Accounts: Local Accounts (T1078.003)
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase In Firewall Connections	Detects sudden increase in permitted firewall connections. Over a 30 minute window, the current firewall connections is more than 3 standard deviations away from the mean.	Impact	Network Denial of Service: Direct Network Flood (T1498.001)
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Sudden Increase In Firewall Denied Inbound Traffic To A Specific TCP/UDP port	Detects anomalous denied inbound traffic profile on a specific TCP/UDP port - over a 30 minute window, both the total number of denials and the number of unique source IP addresses are at least 3 standard deviations away from the	Impact	Network Denial of Service: Direct Network Flood (T1498.001)

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 with the 'Resources > Rules' page. The search bar contains 'malware'. Four rules are listed, each with a red dashed box highlighting its description and a red callout box with a white background and red border. The callout boxes contain the following text:

- 基於演算法與智能分析 (Based on algorithm and intelligent analysis)
- 基於黑白名單與智能分析 (Based on black and white list and intelligent analysis)
- 基於條件閾值與智能分析 (Based on condition threshold and intelligent analysis)

已啟用	Severity	Name	Description	Control	Scope
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Dynamically generated host name: malware likely	Detects algorithmically generated host name in network traffic - malware often use algorithmically generated host names to communicate.	Command And Control	Dynamic Resolution: Domain Generation Algorithms (T1568.002) System
<input checked="" type="checkbox"/>	8 - MEDIUM	(s) End User DNS Queries to Unauthorized DNS Servers	Detects a scenario where a host, that is itself not a DNS server, is trying to send DNS requests to unauthorized DNS servers. Authorized DNS servers are 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.	Command And Control	Dynamic Resolution: Fast Flux DNS (T1568.001) System
<input checked="" type="checkbox"/>	6 - MEDIUM	(s) Excessive End User DNS Queries	Detects a scenario where a host, that is itself not a DNS server, is sending excessive DNS requests. Authorized DNS servers are represented by the "DNS 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.	Control	(T1568.001) System
<input checked="" type="checkbox"/>	8 - MEDIUM	(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).	Collection	Email Collection: Local Email Collection (T1114.001) System

At the bottom of the interface, there are tabs for '摘要' (Summary) and '測試結果' (Test Results), and a checkbox for '自動展開' (Auto-expand).

MITRE ATT&CK 資安對抗策略、手段告警圖

關聯規則對應 MITRE ATT&CK 新資安框架的覆蓋程度

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

動作 告警總覽 List 風險分析 探索分析 UEBA MITRE ATT&CK® Rule Coverage

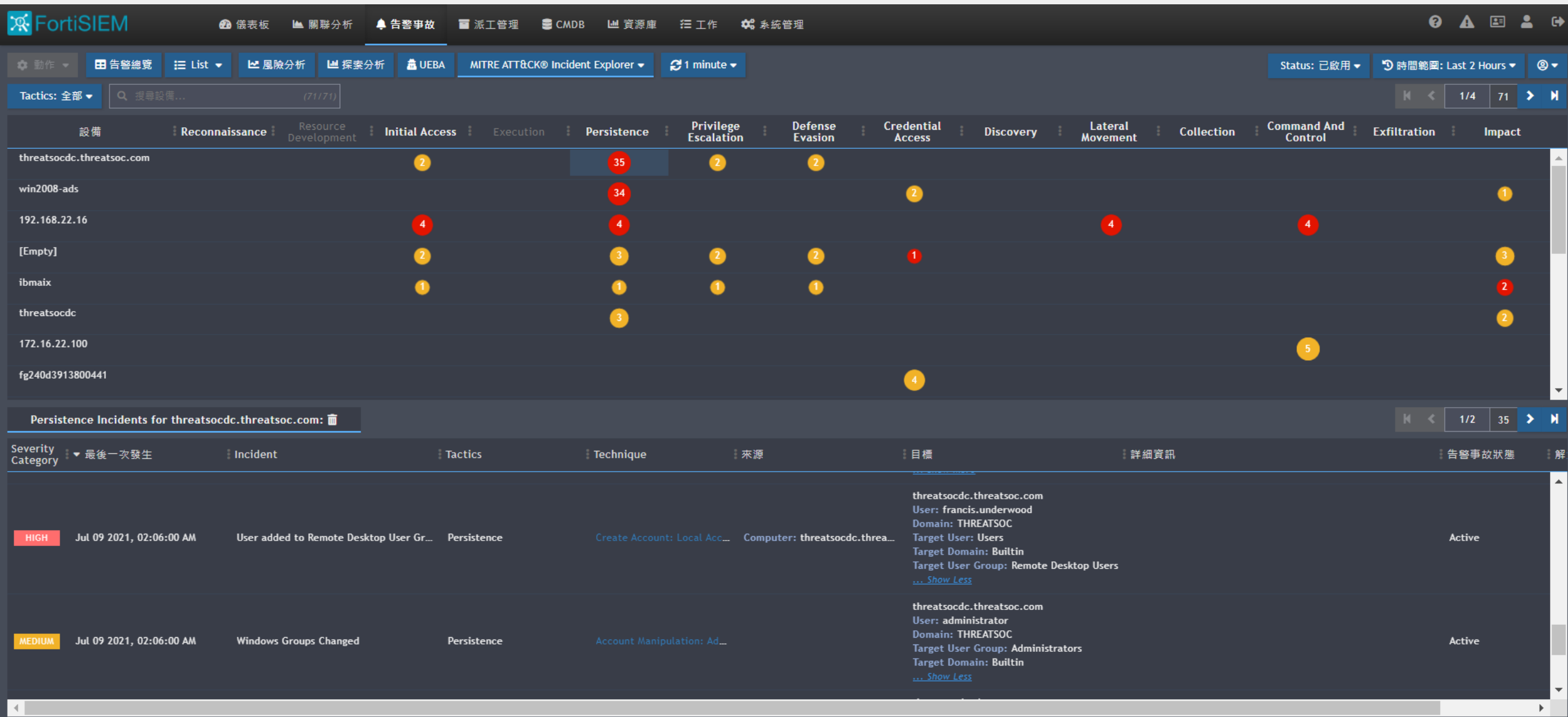
Search technique... (205/205) Show All

954 規則 - 76% Coverage

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
12 10 Tech 32 Sub-Tech	0 6 Tech 26 Sub-Tech	42 9 Tech 16 Sub-Tech	113 10 Tech 25 Sub-Tech	152 18 Tech 84 Sub-Tech	131 12 Tech 79 Sub-Tech	290 37 Tech 124 Sub-Tech	121 14 Tech 41 Sub-Tech	63 25 Tech 32 Sub-Tech	37 9 Tech 18 Sub-Tech	38 17 Tech 28 Sub-Tech	57 16 Tech 30 Sub-Tech	35 9 Tech 12 Sub-Tech	202 13 Tech 21 Sub-Tech
Search Closed Sources	Compromise Infrastructure	Valid Accounts [23]	Software Deployment Tools	Office Application Startup [1]	Boot or Logon Initialization Scripts [2]	Masquerading [31]	Unsecured Credentials [8]	Software Discovery [2]	Remote Service Session Hijacking [2]	Data Staged [5]	Application Layer Protocol [9]	Exfiltration Over Physical Medium [1]	Endpoint Denial of Service [103]
Phishing for Information [1]	Acquire Infrastructure	External Remote Services [4]	System Services [7]	Boot or Logon Initialization Scripts [2]	Access Token Manipulation [4]	Subvert Trust Controls	Steal or Forge Kerberos Tickets [6]	System Owner/User Discovery [5]	Software Deployment Tools	Man in the Browser	Encrypted Channel	Exfiltration Over Web Service [2]	Network Denial of Service [29]
Search Open Technical Databases	Obtain Capabilities	Replication Through Removable Media [1]	User Execution [16]	Browser Extensions	Abuse Elevation Control Mechanism [16]	Obfuscated Files or Information [14]	Steal Web Session Cookie	Virtualization/Sandbox Evasion	Use Alternate Authentication Material [7]	Data from Removable Media [3]	Protocol Tunneling [4]	Automated Exfiltration [1]	Disk Wipe
Active Scanning [11]	Develop Capabilities	Phishing [7]	Scheduled Task/Job [12]	Create Account [13]	Scheduled Task/Job [12]	Use Alternate Authentication Material [7]	Man-in-the-Middle [7]	Network Share Discovery [2]	Exploitation of Remote Services [4]	Man-in-the-Middle [7]	Non-Standard Port [2]	Exfiltration Over Alternative Protocol [9]	Resource Hijacking
Search Victim-Owned Websites	Compromise Accounts	Hardware Additions [1]	Inter-Process Communication [2]	Scheduled Task/Job [12]	Process Injection [13]	Abuse Elevation Control Mechanism [16]	Network Sniffing [5]	System Network Connections Discovery [2]	Lateral Tool Transfer	Data from Network Shared Drive [1]	Communication Through Removable Media	Exfiltration Over Other Network Medium	Firmware Corruption
Gather Victim Host Information [1]	Establish Accounts	Supply Chain Compromise [1]	Windows Management Instrumentation [11]	Traffic Signaling	Exploitation for Privilege Escalation [4]	Modify Authentication Process	Modify Authentication Process	Password Policy Discovery [2]	Remote Services [23]	Data from Configuration Repository [1]	Non-Application Layer Protocol [4]	Data Transfer Size Limits	Inhibit System Recovery [4]
Search Open Websites/Domains		Trusted Relationship [1]	Exploitation for Client Execution [4]	BITS Jobs [2]	Group Policy Modification [2]	Process Injection [13]	Steal Application Access Token [3]	Cloud Service Dashboard	Replication Through Removable Media [1]	Data from Cloud Storage Object [1]	Traffic Signaling	Transfer Data to Cloud Account [1]	Service Stop [22]
Gather Victim Org Information		Drive-by Compromise [1]	Native API [1]	Compromise Client Software Binary [1]	Valid Accounts [23]	Hide Artifacts [5]	Credentials from Password Stores [1]	Network Sniffing [5]	Internal Spearphishing	Data from Local System [2]	Proxy [9]	Scheduled Transfer	Defacement [1]
Gather Victim Network Information [7]		Exploit Public-Facing Application [1]	Command and Scripting Interceptor [7]	Valid Accounts [23]	Hijack Execution Flow [17]	Impair Defenses [49]	Forced Authentication	Account Discovery [11]	Taint Shared Content	Input Capture [1]	Data Obfuscation [2]	Exfiltration Over C2 Channel [21]	Data Encrypted for Impact [2]

MITRE ATT&CK 資安對抗策略、手段告警圖

觸發告警主機在資安攻擊鏈所處的狀態



整合並自動更新外部情資 (FortiGuard 或第三方情資)

網域、IP 地址、URL 網址、程序及雜湊碼的情資交換與分析告警

The screenshot displays the FortiSIEM interface for managing Malware IPs. The left sidebar shows a tree view with categories like Malware Domains, Malware IPs, Malware URLs, etc. The main area is titled '資源庫 > Malware IPs > Emerging Threat Malware IP'. At the top of this area, there are buttons for '新增' (Add), '編輯' (Edit), '刪除' (Delete), and '更多' (More). A search bar and a refresh button are also present. The '更多' dropdown menu is open, showing options: '更新' (Update), '批次啟用' (Batch Enable), and '批次禁用' (Batch Disable). A red box highlights the '更新' button, with a red arrow pointing to it from a callout box containing the text '外部情資更新設定' (External Intelligence Update Settings). Below the menu, a table lists various IP addresses with checkboxes in the 'Active' column. The table has columns for 'Active', 'Low IP', 'Description', and 'Date Found'. The bottom of the interface includes a '摘要' (Summary) button and a checkbox for '自動展開' (Auto Expand).

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

資源庫 > Malware IPs > Emerging Threat Malware IP

新增 編輯 刪除 更多 搜尋... 最後更新於 Jul 8, 2021 9:11:01 PM

更新 批次啟用 批次禁用

外部情資更新設定

Active	Low IP	Description	Date Found
<input checked="" type="checkbox"/>	101.134.0.0		
<input checked="" type="checkbox"/>	101.192.0.0		
<input checked="" type="checkbox"/>	101.203.128.0		
<input checked="" type="checkbox"/>	101.248.0.0		
<input checked="" type="checkbox"/>	101.42.0.0		
<input checked="" type="checkbox"/>	102.196.96.0		
<input checked="" type="checkbox"/>	102.211.224.0		
<input checked="" type="checkbox"/>	102.212.224.0		
<input checked="" type="checkbox"/>	102.228.0.0		
<input checked="" type="checkbox"/>	102.232.0.0		
<input checked="" type="checkbox"/>	102.240.0.0		
<input checked="" type="checkbox"/>	103.100.168.0		
<input checked="" type="checkbox"/>	103.101.104.229		
<input checked="" type="checkbox"/>	103.12.160.164		

摘要 自動展開

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

The screenshot displays the FortiSIEM interface with the following components:

- Top Navigation:** 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.
- Event Details Panel:**
 - Event Details (Title)
 - Raw Log and Record (原始日誌與記錄) - Points to the raw log text.
 - Normalized Log Record and Content Value Analysis (日誌記錄正規化與內容加值分析) - Points to the structured log data table.
- Main Event List:**

Severity Category	最後一次發生	Incident	Tactics	T	來源
HIGH	Jul 12 2021, 09:25:00 PM	Traffic to FortiGuard Malware IP List	Exfiltration	Exfiltration Over ...	LAB-1500D 10.1.200.181
HIGH	Jul 12 2021, 09:16:30 PM	High Severity Inbound Permitted IP...			LAB-1500D 194.165.1
HIGH	Jul 12 2021, 09:10:00 PM	High Severity Inbound Permitted IP...			FG240D3913800441 114.36.65
HIGH	Jul 12 2021, 09:01:30 PM	Concurrent VPN Authentications To...	Credential Acc...		
HIGH	Jul 12 2021, 09:01:30 PM	Concurrent VPN Authentications To...	Credential Acc...		
- Log Summary Table:**

Event Receive Time	Reporting IP	Event Name	Source IP	Destination IP	IP Protocol	Source TCP/Port
Jul 12 2021, 09:23:57 PM	10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	52738
Jul 12 2021, 09:23:57 PM	10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	58705
Jul 12 2021, 09:23:57 PM	10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	51704
- Log Details Table:**

Item	數值
Application Group Name	unscanned
Collector ID	10000
Count	1
Destination City	Kazan
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	55.83043
Destination Longitude	49.06608
Destination Organization	FIRSTBYTE-AS RU

簡單建立標準化事故協作回應流程與自動化 (SOAR)

開立工單、派工協作處理

The screenshot displays the FortiSIEM SOAR interface. At the top, there are navigation tabs: 儀表板 (Dashboard), 關聯分析 (Correlation Analysis), 告警事故 (Alerts/Incidents), 派工管理 (Incident Management), CMDB, 資源庫 (Resource Library), 工作 (Work), and 系統管理 (System Management). Below these are summary statistics: 0 新增 (New), 0 已指派 (Assigned), 2 高優先 (High Priority), 1 已逾期 (Overdue), 0 快逾期 (Near Overdue), 1 已關閉 (Closed), and 5m MTTR (Mean Time to Resolve).

The main table lists incidents with columns for Elapsed, State, Priority, Ticket ID, Organization, Summary, Incident ID, Assignee, Creator, Resolution Time, Due Date, and Creation Date. Red callout boxes highlight specific rows: '事故工單已逾期' (Overdue incident ticket), '事故工單處理中' (Incident ticket being processed), '新建立事故工單' (Newly created incident ticket), and '已結案事故工單' (Closed incident ticket).

Below the table, the 'Action History > Timeline' section shows a detailed view of an incident. It includes a '告警事故動作' (Alert Incident Action) and a '案件動作' (Case Action) timeline. A red callout box labeled '事故工單處理時間軸' (Incident ticket processing timeline) points to this section. The timeline shows the following actions:

- 09:37:22 PM: User admin created Case 53403753
- 09:37:22 PM: User Super/admin created Case
- 09:53:40 PM: User Super/admin changed : State
- 09:53:40 PM: User Super/admin added Notes

Elapsed	State	Priority	Ticket ID	Organization	Summary	Incident ID	Assignee	Creator	Resolution Time	Due Date	Creation Date
Overdue	In Progress				CASE Email test		admin	admin <km...		Jul 09 2021, 11:59:59 PM	Jun 30 2021, 11:07:05
25 %	In Progress	Medium	53403750	Test_Lab	Sudden location change for susan.davis at City Walnut Cre...	3511	jim	admin <km...		Jul 12 2021, 11:59:59 PM	Jul 12 2021, 09:10:06
2 %	In Progress				High Severity Inbound Permitted IPS Exploit FortiGate-ips-...	90	jenny	admin <km...		Jul 13 2021, 11:59:59 PM	Jul 12 2021, 09:10:31
1 %	In Progress				Traffic from 10.1.200.181 to FortiGuard Malware IP 185.25...	4641	kevin	admin <km...		Jul 13 2021, 11:59:59 PM	Jul 12 2021, 09:37:22
--	Closed	High	53403752	Test_Lab	VNC from Internet 185.56.80.120 to 192.168.22.16, in FG2...	4532	bob	admin <km...	5m 58s	N/A	Jul 12 2021, 09:13:18

簡單建立標準化事故協作回應流程與自動化 (SOAR)

迅速反應，執行聯防緩解調控措施

The screenshot displays the FortiSIEM interface. At the top, there are navigation tabs: 儀表板 (Dashboard), 關聯分析 (Correlation Analysis), 告警事故 (Alerts), 派工管理 (Task Management), CMDB, 資源庫 (Resource Library), 工作 (Work), and 系統管理 (System Management). Below these, a secondary navigation bar includes 動作 (Action), 告警總覽 (Alert Overview), List, 風險分析 (Risk Analysis), 探索分析 (Discovery Analysis), UEBA, MITRE ATT&CK®, and a refresh button for 1 minute. A time range filter is set to 'Last 2 Hours'. The main area shows a list of alerts with columns for 告警事故 (Alert), 戰術 (Tactics), 技術 (Techniques), 回報設備 (Reporting Device), 來源 (Source), 目標 (Destination), and 詳細資訊 (Details). A summary bar indicates 'All: 180', 'High: 17', 'Medium: 157', and 'Low: 6'. A left sidebar contains various management options, with '緩解告警事故' (Mitigate Alerts) highlighted in a red box. A red callout box with white text points to this option, containing the text '執行告警事故 緩解調控措施' (Execute alert mitigation measures). Below the alert list, there are checkboxes for '自動換行' (Wrap), '顯示事件型式' (Show event type), '只顯示原始事件' (Show only original events), and '比較分佈' (Compare distribution). A detailed table at the bottom shows reporting IP, source IP, destination IP, IP protocol, source TCP/UDP port, destination TCP/UDP port, and original event records.

告警事故	戰術	技術	回報設備	來源	目標	詳細資訊	告警事故狀態	解決處理狀態
5:30 PM Traffic to FortiGuard Malware IP List	Exfiltration	Exfiltration Over ...	LAB-1500D	10.1.200.181	185.255.135.33		Active	Open
1:30 PM Sudden User Location Change			fsm-super172	Source City: P... Source State: ... Source Countr...	User: don.freeman Destination City: Ho... Destination State: T...	Duration: 1s	Active	Open
1:00 PM Sudden User Location Change			fsm-super172	Source City: H... Source State: ... Source Countr...	User: don.freeman Destination City: Lo... Destination State: E...	Duration: 59m 58s	Active	Open
1:00 PM Sudden User Location Change			fsm-super172	Source City: Lon... Source State: En... Source Country: ...	User: don.freeman Destination City: Pa... Destination State: IL...	Duration: 1s	Active	Open

Reporting IP	Source IP	Destination IP	IP Protocol	Source TCP/UDP Port	Destination TCP/UDP Port	原始事件記錄	
10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	61511	80 (HTTP)	<189>date=2021-07-12 time=23:55:41 devname="LAB-1500...
10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	51505	80 (HTTP)	<189>date=2021-07-12 time=23:55:41 devname="LAB-1500...
Jul 12 2021, 11:55:42 PM	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	50323	80 (HTTP)	<189>date=2021-07-12 time=23:55:41 devname="LAB-1500...

簡單建立標準化事故協作回應流程與自動化 (SOAR)

迅速反應，執行聯防緩解調控措施

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 (300sec)

Run On: fsm-collector176

執行 取消

設定執行動作設備

設定緩解調控措施

Event Receive Time	Reporting IP	事件名稱	Source IP	Destination IP	IP Protocol	Source TCP/UDP Port	Destination TCP/UDP Port	原始事件記錄
Jul 12 2021, 11:55:42 PM	10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	61511	80 (HTTP)	<189>date=2021-07-12 time=23:55:41 devname="LAB-1500...
Jul 12 2021, 11:55:42 PM	10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	51505	80 (HTTP)	<189>date=2021-07-12 time=23:55:41 devname="LAB-1500...
Jul 12 2021, 11:55:42 PM	10.1.200.254	Timeout traffic	10.1.200.181	185.255.135.33	6 (TCP)	50323	80 (HTTP)	<189>date=2021-07-12 time=23:55:41 devname="LAB-1500...

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

The screenshot displays the FortiSIEM interface, specifically the 'Resources > Remediations' section. The interface includes a top navigation bar with various icons and a search bar. A left sidebar lists navigation categories such as Reports, Rules, Networks, Watch Lists, Protocols, Event Types, Malware Domains, Malware IPs, Malware URLs, Malware Processes, Country Groups, Malware Hash, Default Password, Anonymity Network, and User Agents. The main content area shows a table of remediation scripts with columns for Name, Device Type, Script Name, Protocol, Description, and Scope. The table is currently displaying 14 entries, with pagination controls showing 1/1 and 36 items. At the bottom, there are controls for '摘要' (Summary) and '自動展開' (Auto-expand).

名稱	設備型式	腳本名稱	通訊協定	描述	範圍
Block IP FortiOS 5.4 (300sec)	Fortinet FortiOS	fortigate_block_ip_after.4_2021_06_23_16_05_12.py	SSH	Block IP on FortiGate	User
Block IP FortiOS 5.4 (put in Address Group)	Fortinet FortiOS	fortigate_block_ip_after.4_2021_06_23_16_06_36.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 IP (Source) FortiOS 5.4	Fortinet FortiOS	fortigate_block_ip_after.4_2021_06_23_16_02_37.py	SSH	Block IP on FortiGate	User
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	Cisco WLAN Controller	cisco_wlc_deauth_mac.py	SSH	Deauth a user on Cisco WLAN Controller	System
Deauth User Cisco WLC	Fortinet FortiWLC	fortiwlc_deauth_mac.py	SSH	Deauth a user on FortiWLC	System
Deauth User Linux	Generic Linux	linux_deauth_user.py	SSH	Deauth user	System
Delete File By Checksum Linux	Generic Linux	linux_delete_file_with_hash.py	SSH	Delete a file with specific checksum	System
Delete File By Checksum Windows	Microsoft Windows	windows_delete_file_with_hash.py	MS_WMI	Delete a file with specific checksum	System
Delete File By Type Linux	Generic Linux	linux_delete_file_type.py	SSH	Delete files with specific type	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

The screenshot shows the FortiSIEM SOAR configuration interface. The left sidebar contains navigation options: 建立 (Build), 設備支持 (Device Support), 健康狀態 (Health Status), 授權 (Authorization), and 設置 (Settings). The main area is titled '通報政策' (Notification Policy) and includes a '新增' (Add) button circled in red. The configuration fields are as follows:

- 嚴重性 (Severity): 低 中 高
- 規則 (Rule): Rule: Traffic to FortiGuard Malware IP List (Annotated with '告警事故觸發規則設定')
- 時間範圍 (Time Range): ANY
- 受影響項目 (Affected Item): ANY
- 受影響組織 (Affected Organization): ANY
- 動作 (Actions):
 - 發送電郵/簡訊至指定使用者. (Annotated with '自動告警事故通報設定')
 - 執行緩解措施/腳本. (Annotated with '自動緩解調控措施設定')
 - 調用整合政策. 執行: no policy
 - 發生告警事故時建立工單. (Annotated with '自動建立告警事故工單')
 - 發送 SNMP 訊息至目的地配置於 系統管理 > 設置 > 關聯分析.
 - 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 (Settings):
 - 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 (Remarks):

At the bottom, there are '儲存' (Save) and '取消' (Cancel) buttons.

FortiSIEM 重要特點與價值

AI 驅動的安全營運

- 新世代的 FortiSIEM，不再只是單純的安全資訊與事件管理 (SIEM)
- 還可進一步做為企業安全/網維管理的優化工具
- 彈性的資安/網路監看儀表板提供更好的可視性
- 針對進階持續性威脅或勒索病毒的攻擊，導入 AI / ML 智能分析，對應 MITRE 資安新框架，提供先期預警能力
- 內建派工管理系統，可連動跨品牌設備，滿足自動化協作聯防的需要



FORTINET®