

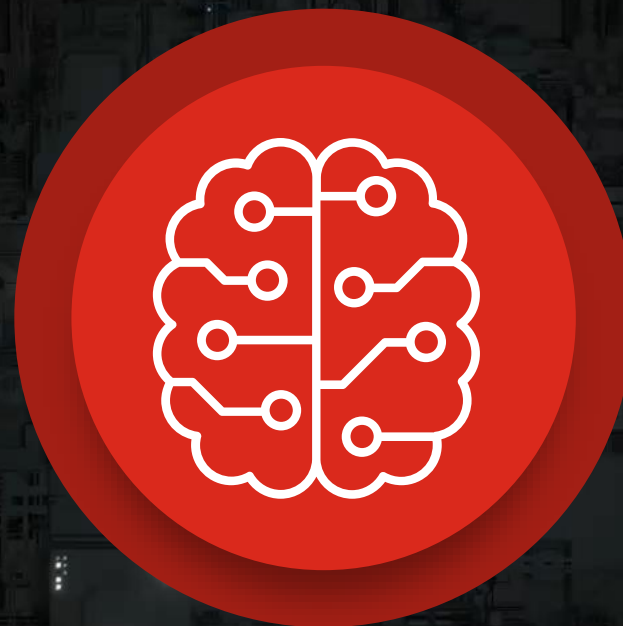
AI 驅動的安全運營

Why work harder when you can work smarter



李鵬 Paul Li

Fortinet 技術顧問

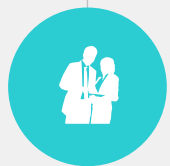


AI 人工智能 應用在網維營運 (NoC) 與資安營運中心 (SoC)



新一代生成式 AI 的安全助理

使用自然語言 (natural language) 和生成式 AI 來引導管理者，與管理者互動應答，啟動自動化作業流程，大幅簡化網維與分析師日常維運負載。



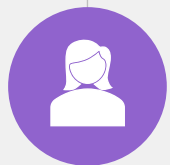
降低人為判斷失誤，決策有 AI 幫忙

借助 FortiAI，資安團隊可以做出更明智的判斷與決策，快速應對威脅，並在複雜任務上節省時間，提高了運營效率，提升了 IT 團隊的技能水平。



FortiAI 大型語言模型 LLM 安全架構

FortiAI 大語言模型 (LLM)，強化安全訓練，透過「內容過濾」「監控稽核」「存取控制」「提示固化」「機密確保」建構 LLM 安全架構，個資檢測，資料屏蔽，機敏資訊不外露。



AI 驅動的安全營運中心 Fortinet SecOps

FortiAI 已無縫整合到 FortiManager、FortiAnalyzer、FortiSIEM 和 FortiSOAR 的管理者日常維運中，協助優化分析師資安威脅調查並快速響應，即時緩解，SIEM 事件互動確認、SOAR 自動化流程劇本創建 ... 等。



✓ Security-First AI

✓ Platform Approach

✓ Use Case-Focused

✓ Automation-Driven



FortiAI 能為我們做些甚麼？



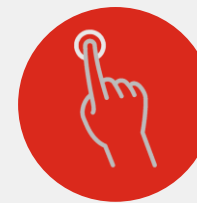
提升洞察力

建構整個維運環境的知識庫，從網路、用戶、傳輸數據的應用以及資安態勢



協助決策制定

依據洞察後狀態推薦管理者接續的行動制定，以上是基於維運環境的分析並依最佳實踐執行



自動化腳本執行

通過管理者同意後的自動化腳本來執行決策後的建議行動





FortiAI for FortiAnalyzer

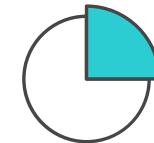


CONFIDENTIAL

Access Limited to Authorized Personnel

帶您認識全新的 SOC AI 安全助理

FortiAI 新一代生成式 AI 安全助理，為主動型安全運維而生



高效減輕 工作負擔

- 大幅降低安全運維團隊的工作壓力



直觀簡化 平台操作

- 透過自然語言互動應答，輕鬆上手



智能解析、 評估與建議

- 即時解析資安事件
- 自動生成事件摘要
- 精準評估潛在風險
- 提供專業修復建議



輕鬆創建 化繁為簡

- 事件查詢
- 報表產出
- SIEM 偵測規則
- 自動化腳本
- 安全織網設備聯防



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



FAZ-SOC

Last 4 Hours 2024-11-07 13:36:00 - 2024-11-07 17:36:00

1 High Severity Incidents 0 Outbreak Alerts 1 Compromised Host

What happened today in my network

Summarizing the latest event and alerts from Today...

FortiAI 摘要今天最新的事件與告警給您參考

What happened today in my network

What's new in FortiAnalyzer 7.6 What can I do with FortiAI

What happened today in my network

Monthly token usage 0.0%

0/1024

今天我們公司網路維運中有發生什麼事件嗎？



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



The image shows a laptop screen displaying the FortiAnalyzer SOC Dashboard on the left and the FortiAI chat interface on the right. The dashboard shows a sidebar with navigation options like Dashboards, Status, Email Metrics, SOC Dashboard, Device Manager, FortiView, Log View, Fabric View, Incidents & Events, FortiAI, Reports, and System Settings. The main content area displays an 'Event Summary for Today (今日事件摘要)' for the event group 'Default-Risky-Destination-Detection-By-Threat'. The summary includes event date (2024-11-07), summary (Multiple high-severity risky destinations detected), key details (Attack Type: Risky Destination Detection, Vulnerable Component: Network security, Severity: High, Target Information: Endpoint IP: 192.168.0.2 (client001), Endpoint Name: client001), and alert details (Handler: Default-Risky-Destination-Detection-By-Threat, Rule: Unspecified, Impact Explanation: Connection attempts to known risky destinations, Root Cause: Unspecified). The FortiAI chat interface on the right shows a conversation with the AI assistant, who has responded with the same event summary. A red box highlights the event details in the dashboard, and a red arrow points from this box to the chat interface. Below the dashboard, there is a text overlay in Chinese.

於 2024/11/07 資安事件中，過濾出內網中有嘗試連線至高風險標的物的情事發生。內網端點 IP = 192.168.0.2 / Client001



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



FAZ-SOC

Dashboards

Status

Email Metrics

SOC Dashboard

Device Manager

FortiView

Log View

Fabric View

Incidents & Events

FortiAI

Reports

System Settings

Last 4 Hours 2024-11-07 13:36:00 - 2024-11-07 17:36:00

1 High Severity Incidents

0 Outbreak Alerts

1 Compromised Host

Events Map

critical

high

medium

low

client001

endpoint 18 95%

Incident Category

Denial of Service (DoS)

1

Events and Incidents

Logs

Events

high

critical

FortiGate

FortiAI

Do we have an incident for client001

Getting incidents...

What's new in FortiAnalyzer 7.6

What can I do with FortiAI

Do we have an incident for client001

Monthly token usage 0.0%

0/1024

我們是否有針對端點 client001 的資安事件?



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



Incident Details for client001

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

FortiAI

Do we have an incident for client001?

Incident Details for client001

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

FortiAI

Do we have an incident for client001?

What's new in FortiAnalyzer 7.6

What can I do with FortiAI

Do we have an incident for client001?

Monthly token usage 0.0%

0/1024

FortiAI 檢視 client001 相關事件後：
發現 client001 有存取外部惡意網站 (Malicious Website) 的資安事件

我們是否有針對端點 client001 的資安事件?



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



FAZ-SOC Last 4 Hours 2024-11-07 13:36:00 - 2024-11-07 17:36:00

SOC Dashboard

- 1 High Severity Incidents
- 0 Outbreak Alerts
- 1 Compromised Host

Events Map

critical

high

medium

low

client001 endpoint 18 95%

Denial of Service (DoS) 1

Incident Details for client001

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

Events and Incidents

Logs

Events

high

critical

FortiGate

FortiAI

Do we have an incident for client001?

What's new in FortiAnalyzer 7.6 What can I do with FortiAI

Can you show me the web filter logs for srcip 192.168.0.2 for today?

Monthly token usage 0.0%

0/1024

請幫我列出 192.168.0.2 (client001) 今天的 web filter 上網事件清單



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，即時解析資安事件



The screenshot displays the FortiAI interface within the FortiAnalyzer SOC (FAZ-SOC) environment. The left sidebar shows navigation options like Dashboards, Device Manager, FortiView, Log View, Logs, Log Settings, Fabric View, Incidents & Events, FortiAI, Reports, and System Settings. The main area is divided into two panels. The left panel shows the 'Fortinet Logs' section with a table of logs for 'Security: Web Filter'. The right panel shows the 'Incident Details for client001' and a chat interface.

Table: Web Filter Logs

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host
1	2024-11-07 1	FGVM01TM24002		192.168.0.2	104.18.29.80	HTTPS	coin
2	2024-11-07 1	FGVM01TM24002		192.168.0.2	104.18.28.80	HTTPS	coin
3	2024-11-07 1	FGVM01TM24002		192.168.0.2	208.94.116.24	HTTP	malv
4	2024-11-07 1	FGVM01TM24002		192.168.0.2	208.94.116.24	HTTP	malv

Incident Details for client001

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

Chat Interface:

Do we have an incident for client001

Can you show me the web filter logs for srcip 192.168.0.2 for today?

The web filter logs for the source IP 192.168.0.2 for today have been displayed. You can review the logs in the web filter log view section. If you need any further analysis or another operation, please let me know.

What's new in FortiAnalyzer 7.6 | What can I do with FortiAI

Fortinet | Total logs for analysis: 45 days 2 hours | 50 | Monthly token usage 0.0% | 0/1024

FortiAI 列出有關 192.168.0.2 (client001) 今天的 Web filter 事件清單，您可以在 Web filter event 部分查看日誌。
如果您需要任何進一步的分析或其他操作，請告訴我。



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，精準評估潛在風險



The screenshot displays the FortiAI interface within the FortiAnalyzer SOC. The left sidebar contains navigation options: Dashboards, Device Manager, FortiView, Log View, Logs, Log Settings, Fabric View, Incidents & Events, FortiAI, Reports, and System Settings. The main panel is divided into two sections. The top section, titled 'FortiGate', shows a table of logs with columns: #, Date/Time, Device ID, User, Source, Destination IP, Service, and Host. The bottom section, titled 'FortiAI', shows a chat interface with a bot icon and a text input field.

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host
1	2024-11-07 1	FGVM01TM24002		192.168.0.2	104.18.29.80	HTTPS	coinh
2	2024-11-07 1	FGVM01TM24002		192.168.0.2	104.18.28.80	HTTPS	coinh
3	2024-11-07 1	FGVM01TM24002		192.168.0.2	208.94.116.246	HTTP	malw
4	2024-11-07 1	FGVM01TM24002		192.168.0.2	208.94.116.246	HTTP	malw

Incident Details for client001

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

Can you show me the web filter logs for srcip 192.168.0.2 for today?

The web filter logs for the source IP 192.168.0.2 for today have been displayed. You can review the logs in the web filter log view section. If you need any further analysis or another operation, please let me know.

What's new in FortiAnalyzer 7.6 What can I do with FortiAI

Give me the reputation for the ip 104.18.29.80

FortiAI

Monthly token usage 0.0%

0/1024

幫我對 104.18.29.80 做 IP 信評調查



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，精準評估潛在風險



FortiAI 對 104.18.29.80 信評檢查的結果為惡意 IP 位址，有潛在的犯罪活動記錄，雖然該 IP 活動率低，但仍建議對該 IP 進行以下緩減建議：

1. 加強對該 IP 位址進出的流量進行監控。
2. 若該 IP 不是業務往來所需或不是營運所需連線，請考慮在防火牆上封鎖該 IP。
3. 針對與該 IP 位址的任何通訊連線設定告警。
4. 對使用者進行資安宣導，建議他們避免造訪非業務需求網站、可疑網站，並不可隨意下載檔案。



Reputation Check for IP 104.18.29.80

- Positive Detections: 1
- Total Scans: 94
- Detection Ratio: 1.06%
- Detected Engines:
 - Criminal IP
- Last Scan Date: 2024-11-07 07:03:09

Based on the reputation check, the IP 104.18.29.80 has a low detection ratio but is detected as malicious by the "Criminal IP" engine.

Concern:

- The IP has been flagged for potential criminal activity.

Mitigation Recommendations

1. Monitor Traffic:
 - Enhance monitoring on traffic to and from this IP address.
2. Block IP:
 - Consider blocking this IP on your firewall if it's not a legitimate business partner or necessary for operations.
3. Alerting:
 - Set up alerts for any communication attempts to this IP address.
4. Educate Users:
 - Inform users about potential threats and advise them to avoid accessing suspicious sites or downloading unknown files.

FortiAI

Getting reputation of 104.18.29.80...

Give me the reputation for the ip 104.18.29.80



Reputation Check for IP 104.18.29.80

- Positive Detections: 1
- Total Scans: 94
- Detection Ratio: 1.06%
- Detected Engines:
 - Criminal IP
- Last Scan Date: 2024-11-07 07:03:09

Based on the reputation check, the IP 104.18.29.80 has a low detection ratio but is detected as malicious by the "Criminal IP" engine.

Concern:

- The IP has been flagged for potential criminal activity.

Mitigation Recommendations

1. Monitor Traffic:
 - Enhance monitoring on traffic to and from this IP address.
2. Block IP:
 - Consider blocking this IP on your firewall if it's not a legitimate business partner or necessary for operations.
3. Alerting:
 - Set up alerts for any communication attempts to this IP address.
4. Educate Users:
 - Inform users about potential threats and advise them to avoid accessing suspicious sites or downloading unknown files.

What's new in FortiAnalyzer 7.6

What can I do with FortiAI

Give me the reputation for the ip 104.18.29.80

Monthly token usage 0.0%

0/1024



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，與端點防護自動聯防



The screenshot displays the FortiAI interface within the FortiAnalyzer SOC. The left sidebar shows navigation options like Dashboards, Device Manager, FortiView, Log View, and Logs. The main panel shows a log entry for a security event. A table lists log entries with columns for #, Date/Time, Device ID, User, Source, Destination IP, Service, and Host. The source IP 192.168.0.2 is highlighted in yellow. A text box at the bottom left contains a command in Chinese: "請將 192.168.0.2 (client001) 端點執行隔離，並在該事件報告中添加註記 '此端點後續需要進行本機鑑識與修復'" (Please isolate the endpoint 192.168.0.2 (client001) and add a note to the event report: "This endpoint needs local forensic analysis and repair"). On the right, the FortiAI chat interface is open, showing a reputation check for IP 104.18.29.80. The chat window includes a search bar, a list of positive detections, total scans, detection ratio, and detected engines. It also provides mitigation recommendations such as monitoring traffic, blocking IP, alerting, and educating users. The bottom of the interface shows the FortiNET logo, total logs for analysis, and monthly token usage.

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host
1	2024-11-07 1	FGVM01TM2400		192.168.0.2	104.18.29.80	HTTPS	coinh
2	2024-11-07 1	FGVM01TM2400		192.168.0.2	104.18.28.80	HTTPS	coinh
3	2024-11-07 1	FGVM01TM2400		192.168.0.2	208.94.116.24	HTTP	malw
4	2024-11-07 1	FGVM01TM2400		192.168.0.2	208.94.116.24	HTTP	malw

請將 192.168.0.2 (client001) 端點執行隔離，並在該事件報告中添加註記 "此端點後續需要進行本機鑑識與修復"

Reputation Check for IP 104.18.29.80

- Positive Detections: 1
- Total Scans: 94
- Detection Ratio: 1.06%
- Detected Engines:
 - Criminal IP
- Last Scan Date: 2024-11-07 07:03:09

Based on the reputation check, the IP 104.18.29.80 has a low detection ratio but is detected as malicious by the "Criminal IP" engine.

Concern:

- The IP has been flagged for potential criminal activity.

Mitigation Recommendations

- Monitor Traffic:
 - Enhance monitoring on traffic to and from this IP address.
- Block IP:
 - Consider blocking this IP on your firewall if it's not a legitimate business partner or necessary for operations.
- Alerting:
 - Set up alerts for any communication attempts to this IP address.
- Educate Users:
 - Inform users about potential threats and advise them to avoid accessing suspicious sites or downloading unknown files.

Could you quarantine 192.168.0.2 and add a comment to the incident "this endpoint needs remediation"



FortiAI with FortiAnalyzer Demo

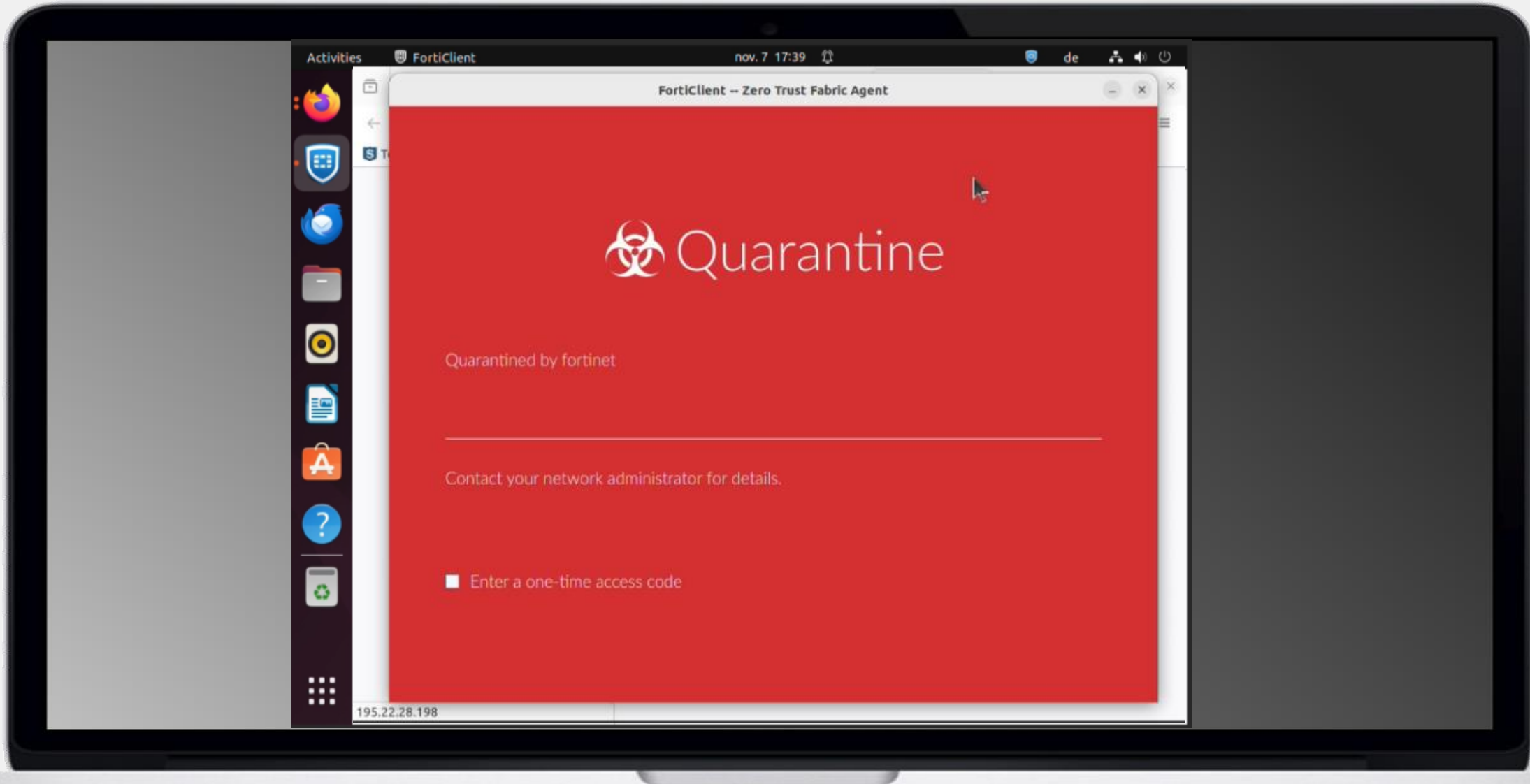
FortiAI 透過自然語言互動應答，與端點防護自動聯防





FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，與端點防護自動聯防





FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，自動生成事件摘要



FAZ-SOC

Incident Analysis

High FortiAI-Demo: Web request to Malicious Websites detected

Edit Layout Export Incident Enrich Execute Playbook Run Report Quarantine Refresh

Incident Summary

Incident Number: IN00000004

Incident Name: FortiAI-Demo: Web request to Malicious Websites detected

Incident Date / Time: 2024-11-07 17:35:09

Incident Update Date / Time: 2024-11-07 17:39:03

Incident Category: Denial of Service (DoS)

MITRE Tech ID: T1021.004 SSH, T1071.001 Web Protocols, T1071.004 DNS, T1102 Web Service

Severity: High

Status: New

Affected Endpoint: client001

Affected Endpoint/User

Affected Endpoint/User: fortinet

Last Seen: 2024-11-07 17:35:09

Topology: client001

Addresses: MAC: 02:09:0f:00:02:01, IP: 192.168.0.2

Operating System: Debian

Comments

FortiAI 2024-11-07 17:39:03 This endpoint needs remedion.

Affected Assets

Endpoint	User	IP Address	MAC Address
client001		192.168.0.2	02:09:0f:00:02:01

Incident Timeline

From 2024-11-07 17:35:09 To 2024-11-07 17:34:57 (Total 1 Event)

Reset Zoom

Close



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，自動生成事件摘要



The screenshot displays the FortiAI interface within the FortiAnalyzer environment. The left sidebar shows the navigation menu with 'Incidents & Events' selected. The main panel shows an incident analysis for 'FortiAI-Demo: Web request to Malicious Websites detected' (IN00000004). The incident details include a high severity, draft status, and affected endpoint 'client001'. The incident timeline shows a single event on 2024-11-07 at 17:35:09. A chat window on the right is open, showing a conversation with the FortiAI bot. The chat history includes a request to generate a summary report, and the current input is 'Please generate a summary report of my investigation.' A blue box highlights the input text, and a blue arrow points from the text to the chat input field.

Incident Analysis

High FortiAI-Demo: Web request to Malicious Websites detected IN00000004

Edit Layout Export Incident Enrich % Execute Playbook Run Report Quarantine

Incident Summary

Incident Number: IN00000004

Incident Name: FortiAI-Demo: Web request to Malicious Websites detected

Incident Date / Time: 2024-11-07 17:35:09

Incident Update Date / Time: 2024-11-07 17:39:03

Incident Category: Denial of Service (DoS)

MITRE Tech ID: T1021.004 SSH, T1071.001 Web Protocols, T1071.004 DNS, T1102 Web Service (4 entries selected)

Severity: High

Status: New

Affected Endpoint: client001

Incident Timeline

From 2024-11-07 17:35:09 To 2024-11-07 17:34:57 (Total 1 Event)

17:10 17:15 17:20 17:25 17:30 17:35 17:40 17:45 17:50

FortiAI

Please generate a summary report of my investigation.

Incident Summary Report

Incident Details

Incident ID: IN00000004

- Name: FortiAI-Demo: Web request to Malicious Websites detected
- Endpoint: client001
- Category: Denial of Service (DoS)
- Severity: High
- Status: Draft
- Description: (Not provided)
- Reporter: Auto-Raised

Events Summary for Today

Event Group: Default-Risky-Destination-Detection-By-Threat

- Event Date: 2024-11-07
- Summary: Multiple high-severity risky destinations detected
- Key Details:
 - Attack Type: Risky Destination Detection
 - Vulnerable Component: Network security
 - Severity: High
 - Target Information:
 - Endpoint IP: 192.168.0.2 (client001)
 - Endpoint Name: client001

Monthly token usage 9.7%

0/1024

請產出這次 client001 事件調查的摘要報告

Please generate a summary report of my investigation.



FortiAI with FortiAnalyzer Demo

FortiAI 透過自然語言互動應答，自動生成事件摘要



The screenshot displays the FortiAI interface within the FortiAnalyzer console. The left sidebar shows the navigation menu with 'Incidents & Events' selected. The main panel shows an incident summary for 'FortiAI-Demo: Web request to Malicious Websites detected' (IN00000004). A chat window on the right shows a user request: 'Please generate a summary report of my investigation.' and the AI's response: 'The summary report of your investigation has been successfully generated. If you need to download or review the report, you can find it in the incident management or reporting section. If you need any further assistance, please let me know.' A download button is visible in the chat response.

Incident Summary

Incident Number	IN00000004
Incident Name	FortiAI-Demo: Web request to Malicious Websites detected
Incident Date / Time	2024-11-07 17:35:09
Incident Update Date / Time	2024-11-07 17:39:03
Incident Category	Denial of Service (DoS)
MITRE Tech ID	T1021.004 SSH

Analysis & Recommendations

- Remediation:
 - Recommendation: Perform comprehensive endpoint network monitoring.
- Action Plan:
 - Isolate the affected endpoints.
 - Conduct a thorough malware and threat scan.
 - Update all security patches and software.
 - Implement stricter network traffic monitoring policies.
 - Educate employees on recognizing and avoiding threats.
- Lessons Learned: Continuous monitoring and rapid response mitigating security threats. Implementing advanced threat mechanisms and ensuring frequent security updates can reduce vulnerabilities.

Additional Comments

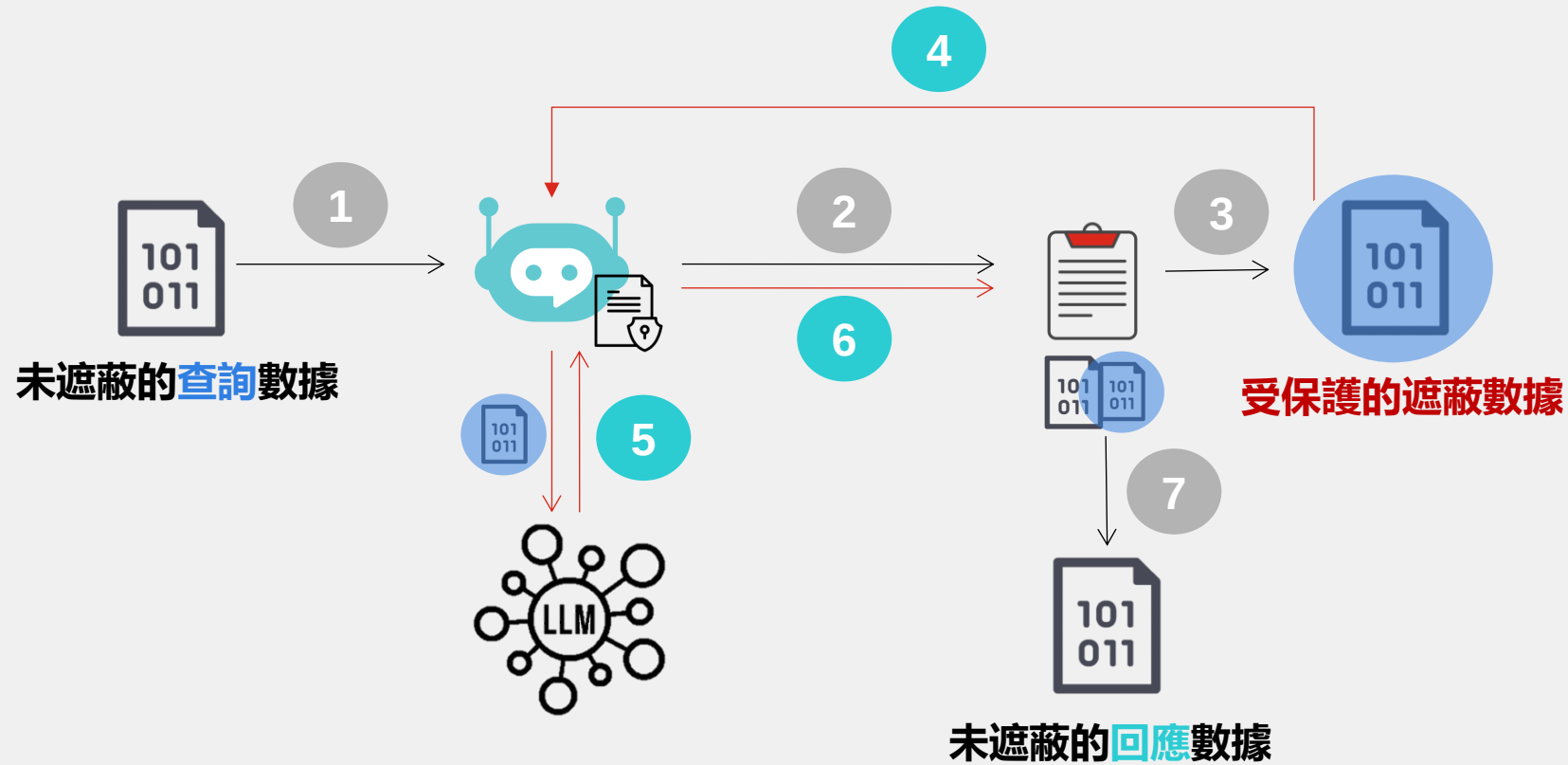
- Note Added: This endpoint needs remediation.

The summary report of your investigation has been successfully generated. If you need to download or review the report, you can find it in the incident management or reporting section. If you need any further assistance, please let me know.

[Download](#)

Monthly token usage 9.7%

FortiAI 保護客戶數據隱私安全 (Data Privacy)



受保護的數據列表

- ✓ IoT devices
 - MAC, vendors and hostnames
- ✓ FortiGate device name
- ✓ The "root" keyword
- ✓ VDOM names
- ✓ IPv4 and IPv6 addresses
- ✓ MAC addresses



FortiAI for FortiManager



CONFIDENTIAL

Access Limited to Authorized Personnel

FortiManager 被忽略的能量



設定即忘

- FortiManager 功能很強大，但常常忘了要在哪裡配置設定。
- 客戶有時會習慣直接在 FortiGate 配置設定。



大材小用

- FortiManager 功能很強大，但許多客戶並未充分利用它。
- 他們經常僅僅用於政策配置，大多數客戶只使用了 20% 功能。



獨立使用

- 大部分獨立運作，錯過了將 FortiManager 與其他 Fortinet 解決方案整合。
- 儘管擁有強大的管理平台，許多客戶仍未能實現高水平的整合。



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



The screenshot displays the FortiManager (FMG-VM64) interface. The left sidebar contains navigation menus for Dashboard, Device Manager, Policy & Objects, SD-WAN Manager, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiAI, FortiGuard, and System Settings. The main area shows the 'Managed FortiGate (6)' section with a connectivity status of '6 Connection Up'. Below this is a table of managed devices:

Device Name	Config Status	Host Name	IP Address
Br-1	✓ Auto-update	FortiGate-VM64	10.254.1.1
HUB-1	✓ Auto-update	FortiGate-VM64	10.254.1.2
FGT-AI-Script-Demo	✓ Synchronized	FGT-AI-Script-Demo	10.3.13.1
FGT-AI-IoT-Vulnerability-3	✓ Synchronized	FGT-AI-IoT-Vulnerability-3	10.3.13.1
FGT-AI-IoT-Vulnerability-2	✓ Synchronized	FGT-AI-IoT-Vulnerability-2	10.3.13.1
FGT-AI-IoT-Vulnerability-1	✓ Auto-update	FGT-AI-IoT-Vulnerability-1	10.3.13.1

On the right, the 'FortiAI Assistant' chat window is open, showing a conversation with 'admin'. The assistant provides guidance on VPN configuration and monitoring.

FortiAI Assistant

Hi admin. To proceed, please select an assistant.

Hi admin, I am your VPN configuration assistant. I can help you write scripts to provision VPN topologies and check VPN tunnel status:

- VPN Configuration Setup:**
 - Site-to-site VPN:** provides secure, scalable, and high-performance connectivity between multiple locations, ensuring data privacy and seamless resource sharing across different network environments.
 - Dialup VPN:** offers secure, flexible remote access for individual users, enabling encrypted connections to corporate networks from any location, ensuring data privacy and seamless access to resources.
- VPN Tunnel Monitoring:**
 - Check VPN Tunnel Status:** I can help to check the current status of VPN tunnels
 - Diagnose VPN Tunnel:** I can help to diagnose the possible issues for a downed VPN tunnel

At the bottom of the chat window, there are buttons for 'Script Assistant', 'VPN Assistant', and 'IoT Device Analysis'. A hand icon is pointing to the 'VPN Assistant' button.

0/1024



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



FMG-VM64

ADOM: root

admin

Create a site-to-site VPN configuration, I would like to upload my own topology diagram

Upload Topology Select Devices

Add files by drag & drop here or Add Files

Upload Image (Max 5MB)

Please upload your network topology diagram or select devices to provide more information and continue.

Extender Manager

Fabric View

FortiAI

FortiGuard

System Settings

Create a site-to-site VPN configuration, I would like to upload my own topology diagram

0/1024



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



The screenshot displays the FortiAI Assistant interface within a web browser. The interface has a top navigation bar with 'ADOM: root' and a user profile 'admin'. Below the navigation bar, there are two tabs: 'Upload Topology' (selected) and 'Select Devices'. The main area shows a network topology diagram with a central 'Internet' cloud. On the left, a box labeled 'Br-1' has 'port4' (14.1.1.2/24) connected to the Internet and 'port5' (20.1.1.1/24) connected to a box labeled 'pc1' (20.1.1.2). On the right, a box labeled 'HUB-1' has 'port4' (14.1.1.4/24) connected to the Internet and 'port5' (20.1.2.1/24) connected to a box labeled 'pc2' (20.1.2.2). Below the diagram, there is a status bar that says 'Processing image...' with a circular progress indicator. A red box highlights this status bar. In the bottom left corner, there is a sidebar with a 'Fabric View' icon and a list of items: 'FortiAI', 'FortiGuard', and 'System Settings'. In the bottom right corner, there is a small icon of a person and the text '0/1024'.

Upload Topology Select Devices

Br-1 port4 14.1.1.2/24 port5 20.1.1.1/24 pc1 20.1.1.2

Internet

HUB-1 port4 14.1.1.4/24 port5 20.1.2.1/24 pc2 20.1.2.2

Processing image...

ADOM: root admin

FortiAI Assistant

Upload Topology Select Devices

Br-1 port4 14.1.1.2/24 port5 20.1.1.1/24 pc1 20.1.1.2

Internet

HUB-1 port4 14.1.1.4/24 port5 20.1.2.1/24 pc2 20.1.2.2

Processing image...

Please upload your network topology diagram or select devices to provide more information and continue.

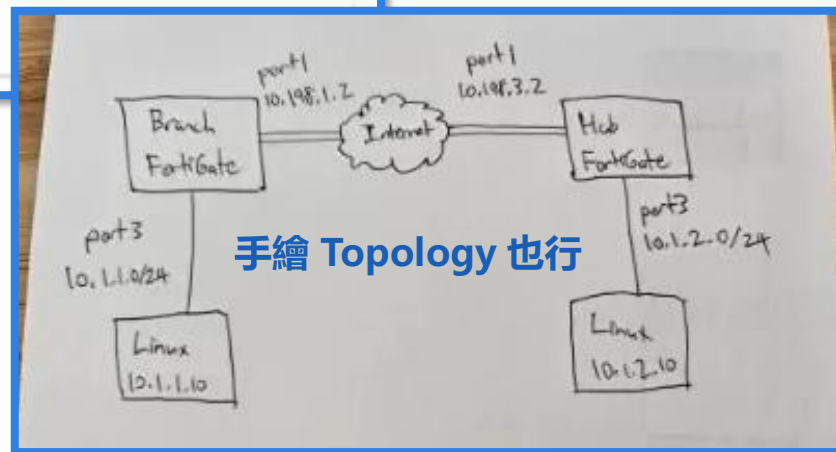
Fabric View

FortiAI

FortiGuard

System Settings

0/1024





FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



The screenshot displays the FortiManager web interface. On the left, a summary box titled "Summary:" contains the following information:

- Site "Br-1" has one WAN interface with an IP address of 14.1.1.2/24 on port4. It also has one LAN interface with an IP address of 20.1.1.1/24 on port5. The LAN interface is associated with a subnet having an IP address of 20.1.1.2.
- Site "HUB-1" has one WAN interface with an IP address of 14.1.1.4/24 on port4. It also has one LAN interface with an IP address of 20.1.2.1/24 on port5. The LAN interface is associated with a subnet having an IP address of 20.1.2.2.

Below the summary, a red-bordered box contains the text: "Is this information correct? Confirming will continue to send this information to FortiAI." Below this box are "Confirm" and "Reset" buttons.

On the right, the "FortiAI Assistant" window is open, showing a network topology diagram. The diagram includes two sites, "Br-1" and "HUB-1", connected via an "Internet" cloud. "Br-1" has a WAN interface (port4) with IP 14.1.1.2/24 and a LAN interface (port5) with IP 20.1.1.1/24. "HUB-1" has a WAN interface (port4) with IP 14.1.1.4/24 and a LAN interface (port5) with IP 20.1.2.1/24. Below the diagram, a message says "Processing image..." and another prompt asks the user to "Please upload your network topology diagram or select devices to provide more information and continue." Below this is another summary box with the same information as the one on the left, followed by a confirmation prompt: "Is this information correct? Confirming will continue to send this information to FortiAI." with "Confirm" and "Reset" buttons.



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



The screenshot displays the FortiManager web interface. A blue banner at the top reads: "The generated scripts configure a site-to-site VPN between the two FortiGate devices." Below this, the left sidebar shows the navigation menu with categories like Provisioning Templates, Firmware Templates, Monitors, Policy & Objects, SD-WAN Manager, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiAI, FortiGuard, and System Settings. The main content area shows a list of devices under the "For-VPN (0)" category. A table lists the devices with columns for checkboxes, Device Name, Config Status, Host Name, and IP Address.

	Device Name	Config Status	Host Name	IP Address
☐	Br-1	✓ Auto-update	FortiGate-VM64	10.254.1.1
☐	HUB-1	✓ Auto-update	FortiGate-VM64	10.254.1.2
☐	FGT-AI-Script-Demo	✓ Synchronized	FGT-AI-Script-Demo	10.3.13.1
☐	FGT-AI-IoT-Vulnerability-3	✓ Synchronized	FGT-AI-IoT-Vulnerability-3	10.3.13.2
☐	FGT-AI-IoT-Vulnerability-2	✓ Synchronized	FGT-AI-IoT-Vulnerability-2	10.3.13.3
☐	FGT-AI-IoT-Vulnerability-1	✓ Auto-update	FGT-AI-IoT-Vulnerability-1	10.3.13.4

On the right, the "FortiAI Assistant" panel provides detailed instructions for each FortiGate:

- 1. **Firewall Address Configuration:** Sets up the local and remote subnets with routing enabled.
- 2. **IPSec Phase 1 Configuration:** Defines the parameters for the VPN tunnel initiation, including the WAN interface, encryption proposals, and the remote gateway address.
- 3. **IPSec Phase 2 Configuration:** Specifies the parameters for the data encryption within the tunnel established in Phase 1, including the encryption proposals, and the source and destination address types and names.
- 4. **Static Route Configuration:** Adds a static route to the VPN tunnel interface for the remote subnet.
- 5. **Firewall Policy Configuration:** Creates inbound and outbound policies to allow traffic between the local and remote subnets through the VPN tunnel.

Ensure to replace `<PLACEHOLDER_FOR_YOUR_PRESHARED_KEY>` with a strong pre-shared key for enhanced security.

0/1024



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



Br-1_VPN_SCRIPT

```
config firewall address
  edit "to_HUB-1_local"
    set allow-routing enable
    set subnet 20.1.1.1/24
  next
  edit "to_HUB-1_remote"
    set allow-routing enable
    set subnet 20.1.2.1/24
  next
end

config vpn ipsec phase1-interface
  edit "to_HUB-1"
    set interface port4
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes
    set comments "VPN: to_HUB-1 [Generated by FortiAI]"
    set remote-gw 14.1.1.4
    set psksecret <PLACEHOLDER_FOR_YOUR_PRESHARED_KEY>
  next
```

Copy code Save script

HUB-1_VPN_SCRIPT

```
config firewall address
  edit "to_Br-1_local"
    set allow-routing enable
    set subnet 20.1.2.1/24
  next
  edit "to_Br-1_remote"
    set allow-routing enable
    set subnet 20.1.1.1/24
  next
end

config vpn ipsec phase1-interface
  edit "to_Br-1"
    set interface port4
    set peertype any
    set net-device disable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes
    set comments "VPN: to_Br-1 [Generated by FortiAI]"
    set remote-gw 14.1.1.2
    set psksecret <PLACEHOLDER_FOR_YOUR_PRESHARED_KEY>
  next
```

Copy code Save script



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



The screenshot shows the FortiManager GUI for a device named FMG-VM64. The left sidebar contains a navigation menu with options like Dashboard, Device Manager, Scripts, Provisioning Templates, Firmware Templates, Monitors, Policy & Objects, SD-WAN Manager, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, Fabric View, FortiAI, FortiGuard, and System Settings. The main content area displays the 'Scripts' section, which includes a table of scripts generated by FortiAI. The table has columns for Name, Type, Target, Comments, Members, and Last Modified. Three scripts are listed: 'Br-1_VPN_SCRIPT', 'Create Firewall Address', and 'HUB-1_VPN_SCRIPT'. Red arrows point to the 'Script (3)' header and the 'Script Group (0)' section.

Name	Type	Target	Comments	Members	Last Modified
Br-1_VPN_SCRIPT	CLI	Device Database	Script generated by FortiAI		2024-08-06 08:32:27 PDT
Create Firewall Address	CLI	Device Database	This script creates a firewall address for t...		2024-07-16 12:11:15 PDT
HUB-1_VPN_SCRIPT	CLI	Device Database	Script generated by FortiAI		2024-08-06 08:32:47 PDT



FortiAI with FortiManager Demo

FortiAI 釋放 FortiManager 在 VPN 佈建的潛力



The screenshot displays the FortiManager (FMG-VM64) web interface. The left sidebar shows the navigation menu with 'Scripts' selected under 'Device Manager'. The main panel shows a table of scripts with the following data:

Name	Type	Target	Comments	Members	Last Modified
Script (3)					
☒ Br-1_VPN_SCRIPT	CLI	Device Database	Script generated by FortiAI		2024-08-06 08:32:27 PDT
☐ Create Firewall Address	CLI	Device Database	This script creates a firewall address for t...		2024-07-16 12:11:15 PDT
☐ HUB-1_VPN_SCRIPT	CLI	Device Database	Script generated by FortiAI		2024-08-06 08:32:47 PDT
Script Group (0)					

A red box highlights the 'Run Script' button, and a hand icon points to it. Below the table, the text 'Install VPN Configuration to' is displayed in blue. Two red arrows point from this text to two FortiGate device icons labeled 'HUB-1' and 'Br-1'.



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager interface for the 'FMG-VM64-KVM' device. The left sidebar menu has 'SD-WAN Manager' and its 'Network' sub-item highlighted with red boxes. The main content area is in the 'Monitor' tab, showing a map of the United States with a network topology overlay. A red box highlights a specific link labeled 'port1 (WAN1)'. At the bottom, there are two donut charts: 'Devices by Link Status' and 'Devices by SLA Status'. A 'FortiAI Assistant' window is overlaid on the right side of the screen, displaying the message 'Hi admin. To proceed, please select an assistant.' and three buttons: 'Script Assistant', 'VPN Assistant', and 'IoT Device Analysis'. A blue arrow points from the FortiAI logo icon in the top right corner of the slide to the FortiAI Assistant window.



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager SD-WAN Manager interface. The left sidebar shows the navigation menu with 'SD-WAN Manager' highlighted. The main area shows the 'Monitor' tab for the 'CorpA' device group, displaying a map of the United States with VPN tunnel connections. A red box highlights the 'Monitor' tab and the 'SD-WAN Manager' menu item. A blue box highlights the 'Check the status of VPN tunnels' text in the FortiAI Assistant chat window.

FortiAI Assistant Chat Window:

Hi admin, I am your VPN configuration assistant. I can help you write scripts to provision VPN topology and check VPN tunnel status:

- VPN Configuration Setup:**
 - Site-to-site VPN:** provides secure, scalable, and high-performance connectivity between multiple locations, ensuring data privacy and seamless resource sharing across different network environments.
 - Dialup VPN:** offers secure, flexible remote access for individual users, enabling encrypted connections to corporate networks from any location, ensuring data privacy and seamless access to resources.
- VPN Tunnel Monitoring:**
 - Check and Diagnose VPN Tunnel:** I can help to check and diagnose the possible issues for a downed VPN tunnel

Script Assistant | **VPN Assistant** | IoT Device Analysis

Check the status of VPN tunnels



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager web interface. On the left, the 'SD-WAN Manager' menu item is highlighted. The main content area shows the 'Monitor' tab for SD-WAN tunnels, with a map of North America and a list of down tunnels. A red box highlights the text 'Would you like to run a diagnose?'. On the right, the 'FortiAI Assistant' panel is open, showing a list of IPsec VPN tunnel statuses. A red box highlights the text 'Would you like to run a diagnose?' in this panel as well.

SD-WAN Manager - Monitor

Warning: Image is not...

Devices: Monitor

SDWAN Monitor Template View

Show Down Tunnels Only: CorpA

These VPN tunnels are down:

- Cloud-VPN1
- HUB1-VPN1
- HUB2-VPN1

Would you like to run a diagnose?

FortiAI Assistant

Check the status of VPN tunnels

Thank you, you have selected the device Br2 to diagnose.

IPsec VPN Tunnel Status

Tunnel Name	Phase 1 Name	Phase 1 Status	Phase 2 Name	Phase 2 Status
Cloud-VPN1	Cloud-VPN1	down	Cloud-VPN1	down
Cloud-VPN2	Cloud-VPN2	up	Cloud-VPN2	up
HUB1-VPN1	HUB1-VPN1	down	HUB1-VPN1	down
HUB1-VPN2	HUB1-VPN2	up	HUB1-VPN2	up
HUB2-VPN1	HUB2-VPN1	down	HUB2-VPN1	down

These VPN tunnels are down:

- Cloud-VPN1
- HUB1-VPN1
- HUB2-VPN1

Would you like to run a diagnose?



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager web interface. On the left, the 'SD-WAN Manager' menu item is highlighted. The main panel shows the 'Monitor' tab for SD-WAN tunnels. A map of North America is visible in the background. In the foreground, a blue-bordered window displays the configuration for two VPNs: 'Br2 - Cloud-VPN1' and 'Cloud-Gateway - VPN2_0'. The status of 'Br2 - Cloud-VPN1' is 'status.operational: down', while 'Cloud-Gateway - VPN2_0' is 'status.operational: up'. A red box highlights the 'status.operational' field for 'Br2 - Cloud-VPN1'. To the right, the 'FortiAI Assistant' window is open, showing a chat interface with the text 'Yes, please run a diagnose' and 'AI Assistant is processing the request...'. A red arrow points from the 'status.operational: down' field in the VPN configuration to the 'AI Assistant' window.

FMG-VM64-KVM

Add Device Device Group Install Wizard

Warning: Image is not

Dashboard

Device Manager

Policy & Objects

SD-WAN Manager

Network

Templates

Overlay Orchestration

Devices Monitor

Edit All Devices Filters

SDWAN Monitor Template View

Show Down Tunnels Only CorpA

Br2 - Cloud-VPN1

Cloud-Gateway - VPN2_0

vd: root/0

name: Cloud-VPN1

serial: 5

version: 2

status.admin: up

status.operational: down

type: static

local: 0.0.0.0

vd: root/0

name: VPN2

serial: 2

version: 2

status.admin: up

status.operational: up

type: dynamic

local: 10.198.9.2

FortiAI Assistant

Yes, please run a diagnose

AI Assistant is processing the request...

Br2 - Cloud-VPN1

Cloud-Gateway - VPN2_0

vd: root/0

name: Cloud-VPN1

serial: 5

version: 2

status.admin: up

status.operational: down

type: static

local: 0.0.0.0

remote: 10.198.9.2

mode: main

dpd: on-demand retry-count 3 in

auth: psk

dhgrp: 14 5

xauth: none

interface: port1

auto-discovery-sender: disable

auto-discovery-receiver: enable

phase2s:

Cloud-VPN1 proto 0 src 0.0.0.0/0

policy: yes

vd: root/0

name: VPN2

serial: 2

version: 2

status.admin: up

status.operational: up

type: dynamic

local: 10.198.9.2

mode: main

dpd: on-idle retry-count 10 inter

auth: psk

dhgrp: 14 5

xauth: none

interface: port1

virtual-interface-addr: 10.10.223

auto-discovery-sender: disable

auto-discovery-receiver: disable

add-route: disable

phase2s:

VPN2 proto 0 src 0.0.0.0/0.0.0.0:

policy: yes

0/1024



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager web interface. On the left, the 'SD-WAN Manager' menu item is highlighted. The main panel shows the 'Monitor' tab for SD-WAN tunnels, with a map of North America. A red box highlights the 'Monitor' tab and the 'SD-WAN Manager' menu item. The 'FortiAI Assistant' panel on the right displays the 'Diagnosis Results' for a VPN tunnel. The results indicate that the operational status of the VPN tunnel is down, which could indicate the administrative status of the underlying interface is down. A red box highlights the 'Would you like to continue with applying the fixes?' prompt at the bottom of the diagnosis results panel.

Diagnosis Results:

- The operational status of the VPN tunnel is down. This could indicate the administrative status of the underlying interface is down.
- The operational status of the VPN tunnel is down. This could indicate the administrative status of the underlying interface is down.
- The operational status of the VPN tunnel is down. This could indicate the administrative status of the underlying interface is down.

Would you like to continue with applying the fixes?



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager web interface with the FortiAI Assistant chatbot active. The chatbot is providing instructions and recommendations for resolving VPN issues. The interface includes a top navigation bar with 'FMG-VM64-KVM', 'Add Device', 'Device Group', and 'Install Wizard'. The main content area shows a chat window with the following messages:

Yes, please apply the fixes

I have tried to fix the errors and the changes are summarized below. You can review and perform an install to the devices. Then check the VPN status again.

- Br2/system/interface/port1: enabled the administrative status
- Br2/system/interface/port1: enabled the administrative status
- Br2/system/interface/port1: enabled the administrative status.

Would you like to install these changes to the devices?

Please install

The Install Wizard is opened, please review and proceed within the Install Wizard.

The bottom of the interface shows a sidebar with 'Reports', 'FortiGuard', and 'System Settings'. The main area displays 'Devices by Link Status' and 'Devices by SLA Status' with corresponding donut charts. The Fortinet logo is visible in the bottom left corner.



FortiAI with FortiManager Demo

FortiAI 引導 FortiManager 在 VPN 故障排除的復原能力



The screenshot displays the FortiManager interface with the FortiAI Assistant overlay. The left sidebar shows the navigation menu with options like Dashboard, Device Manager, Policy & Objects, SD-WAN Manager, Network, VPN Manager, AP Manager, FortiSwitch Manager, Extender Manager, FortiView, Log View, Fabric View, Incidents & Events, FortiAI, Reports, FortiGuard, and System Settings.

The main area shows the "Install Wizard - Select Devices to Install (2/4)" dialog. It contains a table with the following data:

Device Name	IP Address	Platform
Branches		
CloudGateway		
DataCenter		
☒ Br2	192.168.100.104	FortiGate-VM64-KVM
☐ Cloud-Gateway	192.168.100.105	FortiGate-VM64-KVM
☐ HUB1	192.168.100.101	FortiGate-VM64-KVM
☐ HUB2	192.168.100.102	FortiGate-VM64-KVM

A red box highlights the "Br2" row, and a red arrow points from it to a FortiGate device icon. Below the icon, the text "Install fixed Configuration to Br2 FortiGate" is displayed.

The right side of the interface shows the "Diagnosis Results" section, which lists the operational status of the VPN tunnel and the administrative status of the underlying interface. It includes a "Would you like to continue with applying the fixes?" prompt and a "Yes, please apply the fixes" button.

Below the diagnosis results, there is a summary of the changes and a "Please install" button. The bottom of the interface shows the "Monthly token usage 17.3%" and a progress bar.

FortiAI 釋放 FortiManager 的潛力



設定即忘



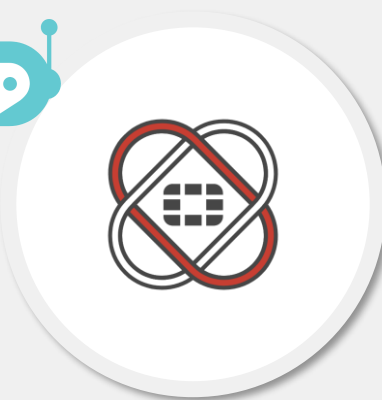
- 管理者與 FortiAI 有高度互動性和對話性。
- 人們將會更頻繁地使用它。



大材小用



- 成為工作中不可或缺的一部分。
- FortiAI 可以利用更多功能和能力來解決客戶的問題。



獨立使用



- 解決了方案之間的獨立使用問題。
- 借助 FortiAI，這些解決方案可以在幕後進行整合和自動化。



FortiAI for FortiSOAR



CONFIDENTIAL

Access Limited to Authorized Personnel

現今 SOC 與 NOC 面臨的維運挑戰

不僅需要佈署防護型資安解決方案，還需要建立自動化預警生態系統



**太多供應商
資訊難統整**



**大量日誌告警
關聯分析困難**



**複合式新形
態攻擊威脅**



**缺乏有經驗
的資安人員**



**手動回應緩慢
費工耗時易出錯**

現今 SOC 與 NOC 迫切的需求



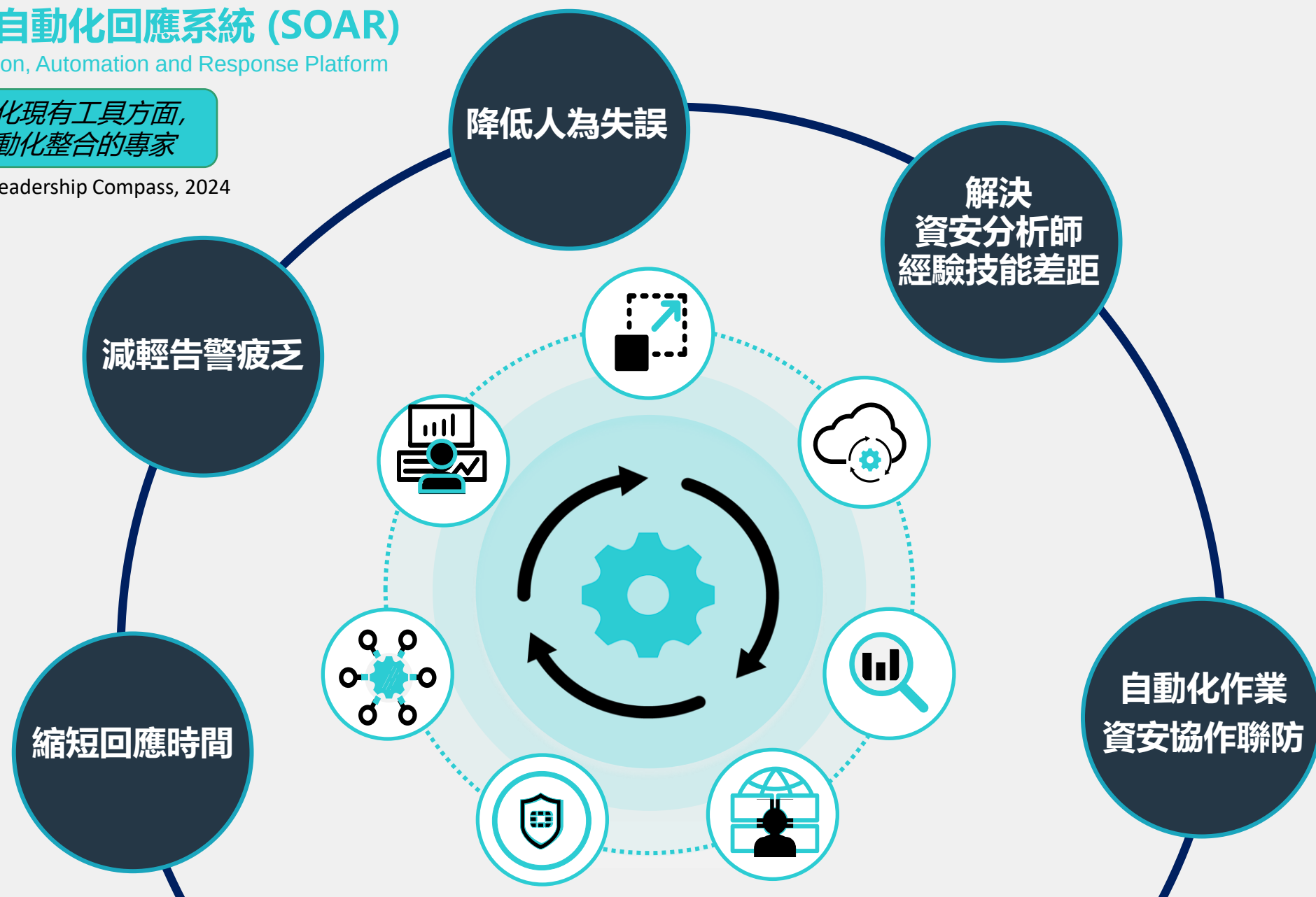
現今 SOC 與 NOC 迫切的需求 : SOAR

安全協調，自動化回應系統 (SOAR)

Security Orchestration, Automation and Response Platform

在自動化和最大化現有工具方面，
SOAR 堪稱自動化整合的專家

- KuppingerCole SOAR Leadership Compass, 2024

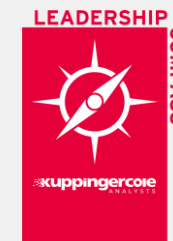


What is FortiSOAR

Security Orchestration, Automation & Response

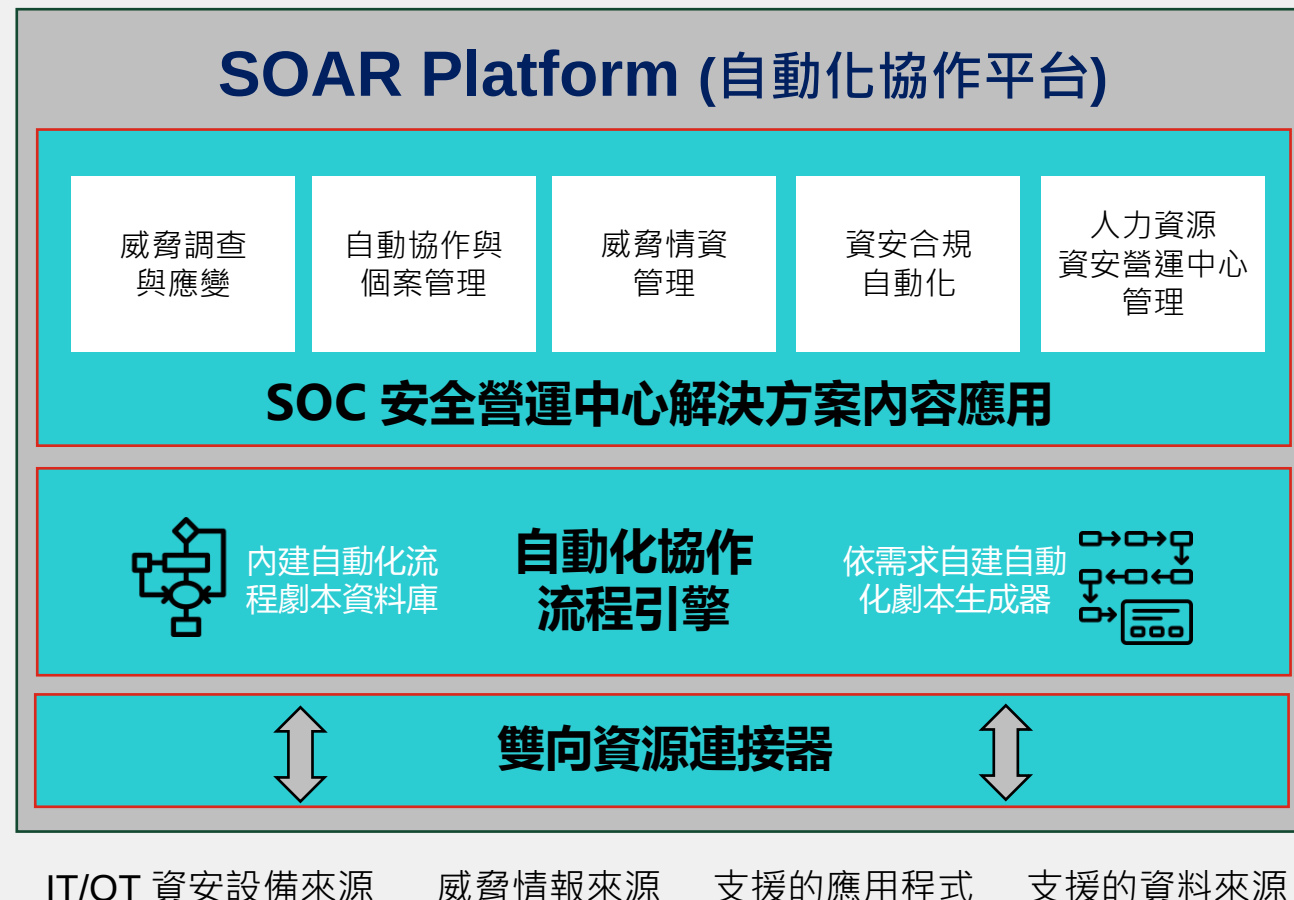
安全協調，自動化回應系統 (SOAR)

A leader in the KuppingerCole 2024
& 2023 SOAR Leadership Compass



SOAR 自動化協作平台，能夠做到：

- **Connects (連結)**
 - 連接至外部任何應用程式、系統或數據來源
- **Executes (執行)**
 - 透過預設或自訂的自動化流程劇本 (playbook) 執行各種自動化作業流程
- **Supports (支援)**
 - 支援安全運營 (SecOps) 解決方案內容應用
- **Extends (擴展)**
 - 可將自動化作業流程擴展至網路運營中心(NOC)或任何其他功能的系統



SOAR 自動化協作平台普遍面臨的挑戰 (知易行難)

How to Investigating ?



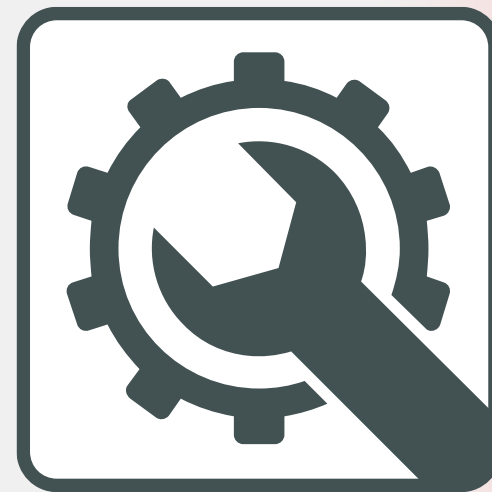
資安事件調查該從何著手？

Response Plans ?



事件回應計畫如何制訂？
自動化劇本內容如何解讀？

Playbook Generation ?



自動化流程劇本如何建立？

導入生成式 AI 自動化流程建立與執行的好幫手



資安事件調查該從何著手？

- 提供告警的詳細資訊及最佳應對措施。
- 分析相關惡意軟體及其攻擊者的背景。
- 探討惡意軟體的作動機制、傳播方式及攻擊者慣用手法。
- 檢視對應該威脅攻擊者常用的 MITRE ATT&CK 戰術與技術。



讓我來幫忙

FortiAI 協助威脅事件調查



事件回應計畫如何制訂？ 自動化劇本內容如何解讀？

- 提供勒索軟體告警應變計畫步驟。
(如隔離受感染主機、通報資安團隊 ...等)
- 解讀 HTML 語法中的輸入字串語意。
- 解讀想了解的特定 Jinja 模板語法用途與運作邏輯。



讓我來幫忙

FortiAI 協助擬定應變計畫



自動化流程 Playbook 生成？

- 建立自動化流程聯動防火牆封鎖惡意 IP/Domain，並發送 Line 通知管理者。
- 針對觸發重大告警的資產啟動 Qualys 弱點掃描，並將掃描結果與該資產關聯分析後產出報告。
- 一旦發現弱點，自動在 ServiceNow 建立派工單 (Tickets)，進入 IR 事件處理流程。



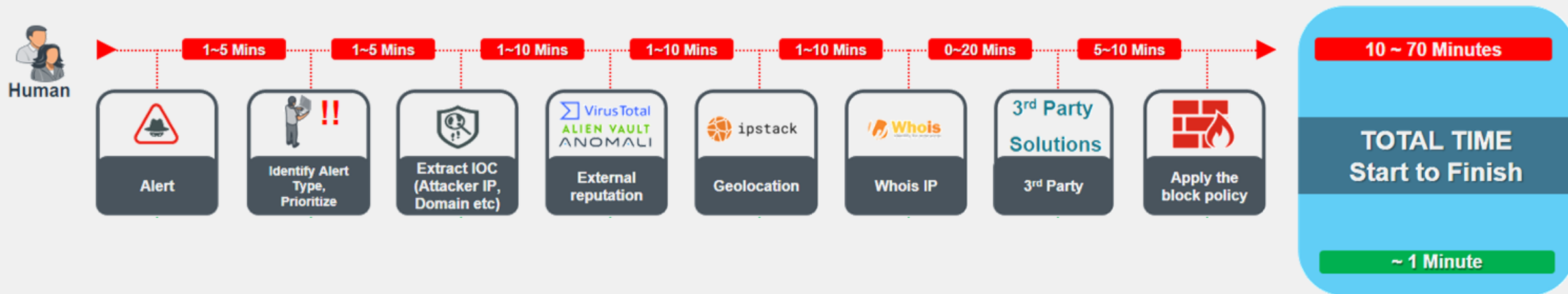
讓我來幫忙

FortiAI 協助自動化劇本生成

應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 自動化協作系統作業流程圖示

SOC 資安事件協作處理流程：異常行為與 IOC 威脅與攻擊分析



MTTR(Mean Time To Response) 資安事件平均回應處理時間



導入 FortiSOAR 自動化協作系統，大幅提升 SOC 營運效率並降低人為作業失誤



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – FortiAI 解讀資安事件，並將事件摘要彙報予管理者

Incident: Test Incident

Minimal Incident-1 | Test Incident

Last Modified 10/25/2024 08:47 PM by Playbook | Under Investigation In War Room - 1

+ Add Tags

告警訊息與資安事件調查該從何著手？

Below information, with sensitive details masked as much as possible, will be shared with the connected AI solution. Review, edit as needed, and confirm sharing.

Name Outbound connection from [IP-1] to [IP-2] on port 31337

PH_RULE_MALICIOUS_OUTBOUND_CONNECTION

Description	Incident Source	Incident Target	Incident Reporting IP	Reporting Device	First Occurred	Last Occurred	Incident Category	Incident Sub-Category	Attack Technique	Incident Details
	[IP-1]	[IP-2]	[IP-1]	[IP-1]	2023-12-08 09:02:30 +00:00	2023-12-08 09:27:30 +00:00	Security	Command and Control	T1043 - Commonly Used Port	ipProto:6

Type Beaconsing

Status Investigating

Severity High

Submit & Get AI's Response Edit Cancel

Graph Elements

- Alerts
- Incidents

Test Alert Test Incident

Indicators Timeline Correlations Tasks Attachments Source

FortiAI PREVIEW

FortiSOAR AI Assistant

透過 FortiAI 解讀資安事件，並將事件摘要彙報予管理者

Hi there! How can I help you today?

請幫我解讀告警事件

Generate Alert Summary

Alert Summary

An outbound connection was detected from a source IP address, denoted as 192.168.60.132, to a destination IP address, 103.224.212.222, over port 31337. This port is recognized for its use in command and control (C2) activities associated with malicious operations. The alert has been generated based on a rule identifying potentially harmful outbound connections, specifically tagged as PH_RULE_MALICIOUS_OUTBOUND_CONNECTION. Details of the incident provided include the source IP (192.168.60.132), target IP (103.224.212.222), the reporting IP (which is the same as the source IP - 192.168.60.132), and the device from which the report originated (also 192.168.60.132). The initial occurrence of the incident was logged on December 8, 2023, at 09:02:30 UTC, with the last occurrence noted on the same day at 09:27:30 UTC. The incident falls under the security category with a sub-category designation of 'Command and Control'. The attack technique associated with this activity is identified by Technique ID T1043, indicating the use of a commonly used port for potential malicious communication. The type of activity detected is labeled as 'Beaconsing,' a term often used to describe a pattern of communication where a compromised system sends regular signals to an attacker-controlled server to indicate its readiness for instructions or data exfiltration. The incident is assigned a high severity rating and is currently in an investigating status. Despite the suspicious nature of the activity, no indicators were found during the time of the report that would classify the IP addresses involved as malicious or suspicious based on their reputation.

Add as a comment



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – FortiAI 解讀資安事件，並給予適當的處置建議彙報予管理者

Incident: Test Incident

Minimal Incident-1 | Test Incident

Last Modified 10/25/2024 08:47 PM by Playbook | Under Investigation In War Room - 1

+ Add Tags

告警訊息與資安事件接續該如何處置？

Below information, with sensitive details masked as much as possible, will be shared with the connected AI solution. Review, edit as needed, and confirm sharing.

Name Outbound connection from [IP-1] to [IP-2] on port 31337

PH_RULE_MALICIOUS_OUTBOUND_CONNECTION

Description	Incident Source	Incident Target	Incident Reporting IP	Reporting Device	First Occurred	Last Occurred	Incident Category	Incident Sub-Category	Attack Technique	Incident Details
	[IP-1]	[IP-2]	[IP-1]	[IP-1]	2023-12-08 09:02:30 +00:00	2023-12-08 09:27:30 +00:00	Security	Command and Control	T1043 - Commonly Used Port	ipProto:6

Type Beaconing

Status Investigating

Severity High

Submit & Get AI's Response Edit Cancel

Graph Elements

- Alerts
- Incidents

Test Alert Test Incident

Indicators Timeline Correlations Tasks Attachments Source

FortiAI PREVIEW

FortiSOAR AI Assistant

透過 FortiAI 解讀資安事件，並給予適當的處置建議彙報予管理者

請給我接續處置建議

Generate Response Recommendations

Response Recommendations

- Immediately Isolate Affected Systems:
 - Disconnect the identified systems from all networks. This can prevent the spread of the malware to other networked devices.
- Identify the Compromised IP Address:
 - Investigate the identified malicious IP address from the indicators list and block it on firewalls, proxy servers, and other network defense measures.
- Apply Relevant Patches and Updates:
 - Ensure that all systems are patched, and security updates are applied to prevent exploitation of known vulnerabilities that could be utilised by the DragonFly malware.
- Conduct a Full System Scan:
 - Utilize updated antivirus and anti-malware software to scan the affected system for all traces of the malware.
- Change Credentials:
 - Following contamination, ensure that all system passwords are changed, especially if they may have been compromised.
- Forensic Analysis:
 - Perform a forensic investigation to understand the malware's ingress point, its behavior, and to identify any data it may have compromised.
- Backup Important Data:
 - Ensure that critical data is backed up and stored securely, separate from network connections that could be vulnerable to malware.



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 將事件升等至戰情室與資安分析師群共同會勘鑑識

Incident: Test Incident

Minimal Incident-1 | Test Incident

Last Modified 10/25/2024 08:47 PM by Playbook | Under Investigation In War Room - 1

此事件為高危等級，FortiAI 建議執行資安鑑識分析

Below information, with sensitive details masked as much as possible, will be shared with the connected AI solution. Review, edit as needed, and confirm sharing.

Name Outbound connection from [IP-1] to [IP-2] on port 31337

PH_RULE_MALICIOUS_OUTBOUND_CONNECTION

Incident Source	Incident Target	Incident Reporting IP	Reporting Device	First Occurred	Last Occurred	Incident Category	Incident Sub-Category	Attack Technique	Incident Details
[IP-1]	[IP-2]	[IP-1]	[IP-1]	2023-12-08 09:02:30 +00:00	2023-12-08 09:27:30 +00:00	Security	Command and Control	T1043 - Commonly Used Port	ipProto:6

Type Beaconsing

Status Investigating

Severity High

Submit & Get AI's Response Edit Cancel

Graph Elements

- Alerts
- Incidents

Test Alert Test Incident

Indicators Timeline Correlations Tasks Attachments Source

FortiAI PREVIEW

FortiSOAR AI Assistant

請幫我將事件升級並開啟戰情室

Escalate this incident to warroom and add indicator 1.1.1.1

Looks like the current incident is still open. To escalate this incident to the war room, you should consider the following steps:

1. Indicate Urgency: Ensure clear communication about why this incident requires war room attention, especially considering its status is open.
2. Add Indicator: Include the indicator 1.1.1.1 as part of the incident details, highlighting its significance to the ongoing investigation.

If you wish, I can assist you in drafting an escalation message or help with any specific actions!

Add as a comment

請 FortiAI 將事件升等，並開啟戰情室與資安分析師群共同會勘鑑識

yes assist me

The war room for the incident has been successfully set up. You can access it [here](#). However, there was an issue while trying to link the indicator 1.1.1.1. The system returned an error, indicating that the indicator could not be found. Please check if the indicator exists or if there are any formatting issues. If you need further assistance with this or any other action, feel free to ask!



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 將事件升等至戰情室與資安分析師群共同會勘鑑識

Indicator: 1.1.1.1
No Reputation Available ▼ Indicator-1 | 1.1.1.1
Last Modified 10/25/2024 09:16 PM by CS Admin

Setup War Room

Provide inputs required to Setup War Room

Status
Draft ▼

War Room Title *

高危事件戰情室，請資安分析師群共同會勘鑑識

War Room Description

今日 12:30:35 於防火牆事件發現疑似 IOC 連線，
請資安官、資安分析師、威脅研究員共同會勘鑑識

Setup

View Detailed Playbook Execution Flow ↗

FortiAI PREVIEW
FortiSOAR AI Assistant

請幫我將事件升級並開啟戰情室
Escalate this incident to warroom and add indicator 1.1.1.1

Looks like the current incident is still open. To escalate this incident to the war room, you should consider the following steps:

1. Indicate Urgency: Ensure clear communication about why this incident requires war room attention, especially considering its status is open.
2. Add Indicator: Include the indicator 1.1.1.1 as part of the incident details, highlighting its significance to the ongoing investigation.

If you wish, I can assist you in drafting an escalation message or help with any specific actions!

Add as a comment

請 FortiAI 將事件升等，並開啟戰情室與資安分析師群共同會勘鑑識

yes assist me

The war room for the incident has been successfully set up. You can access it [here](#).
However, there was an issue while trying to link the indicator 1.1.1.1. The system returned an error, indicating that the indicator could not be found. Please check if the indicator exists or if there are any formatting issues.
If you need further assistance with this or any other action, feel free to ask!

應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 生成 IOC 威脅攻擊自動化授權阻擋作業流程



FortiAI PREVIEW
FortiSOAR AI Assistant

請幫我建立一份作業劇本，自動阻擋在 VirusTotal 信譽評等具危害標示的 IP 與 Domain

Generate a playbook for me to get the reputation of the "[vars.src_ip]" in virustotal and whoisrdap

Here's a suggested playbook outline for review. You can edit this as suitable and proceed to generate the playbook template.

Form ▾ **FortiAI 依需求，自動生成自動化作業劇本**

Select a node...

- ▼ Step 2 [2]
 - name : **Authenticate with VirusTotal API**
 - type : action
- ▼ Step 3 [2]
 - name : **Submit IOC for reputation check with VirusTotal**
 - type : action
- ▼ Step 4 [2]
 - name : **Retrieve results from VirusTotal**
 - type : action
- ▼ Step 5 [2]
 - name : **Authenticate with WhoisRDAP API**
 - type : action
- ▼ Step 6 [2]
 - name : **Perform WHOIS query using the IOC**
 - type : action
- ▼ Step 7 [2]

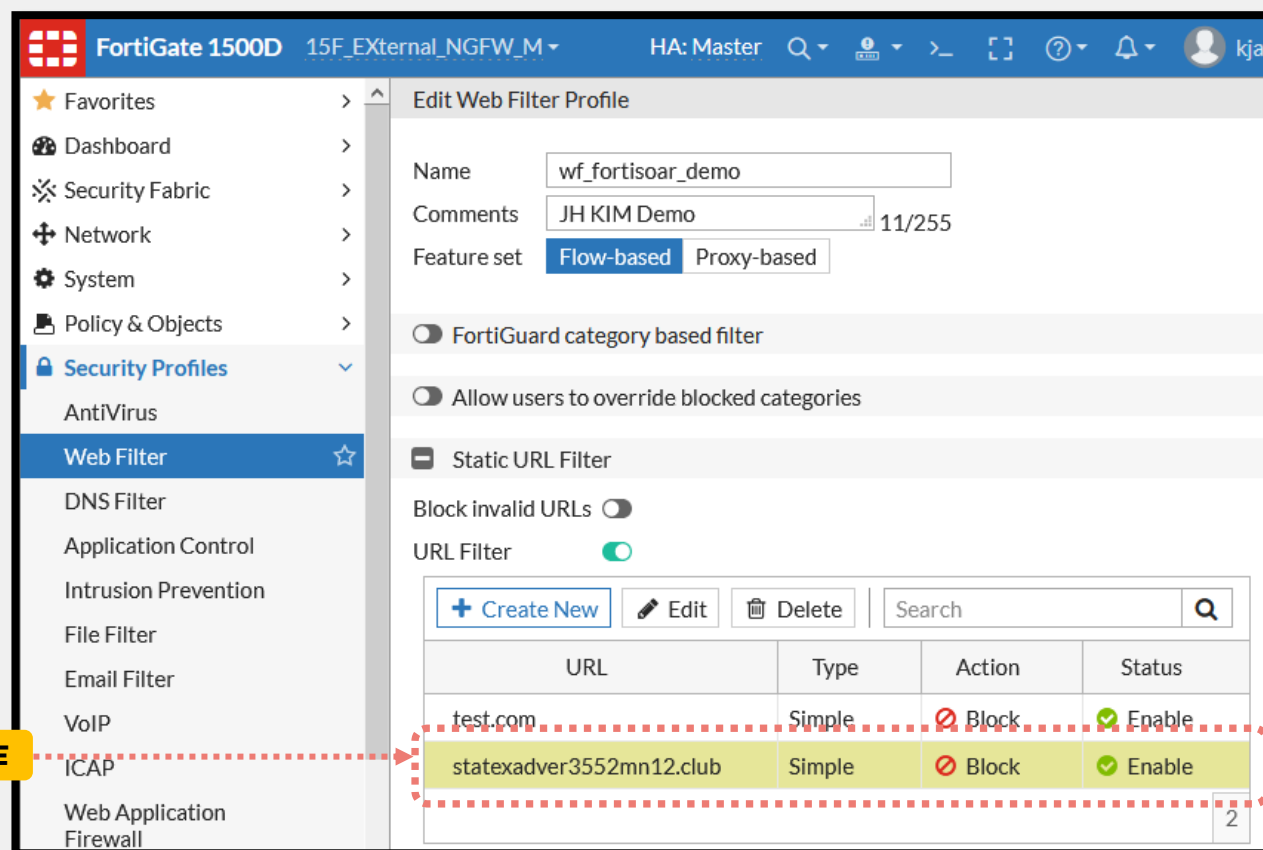
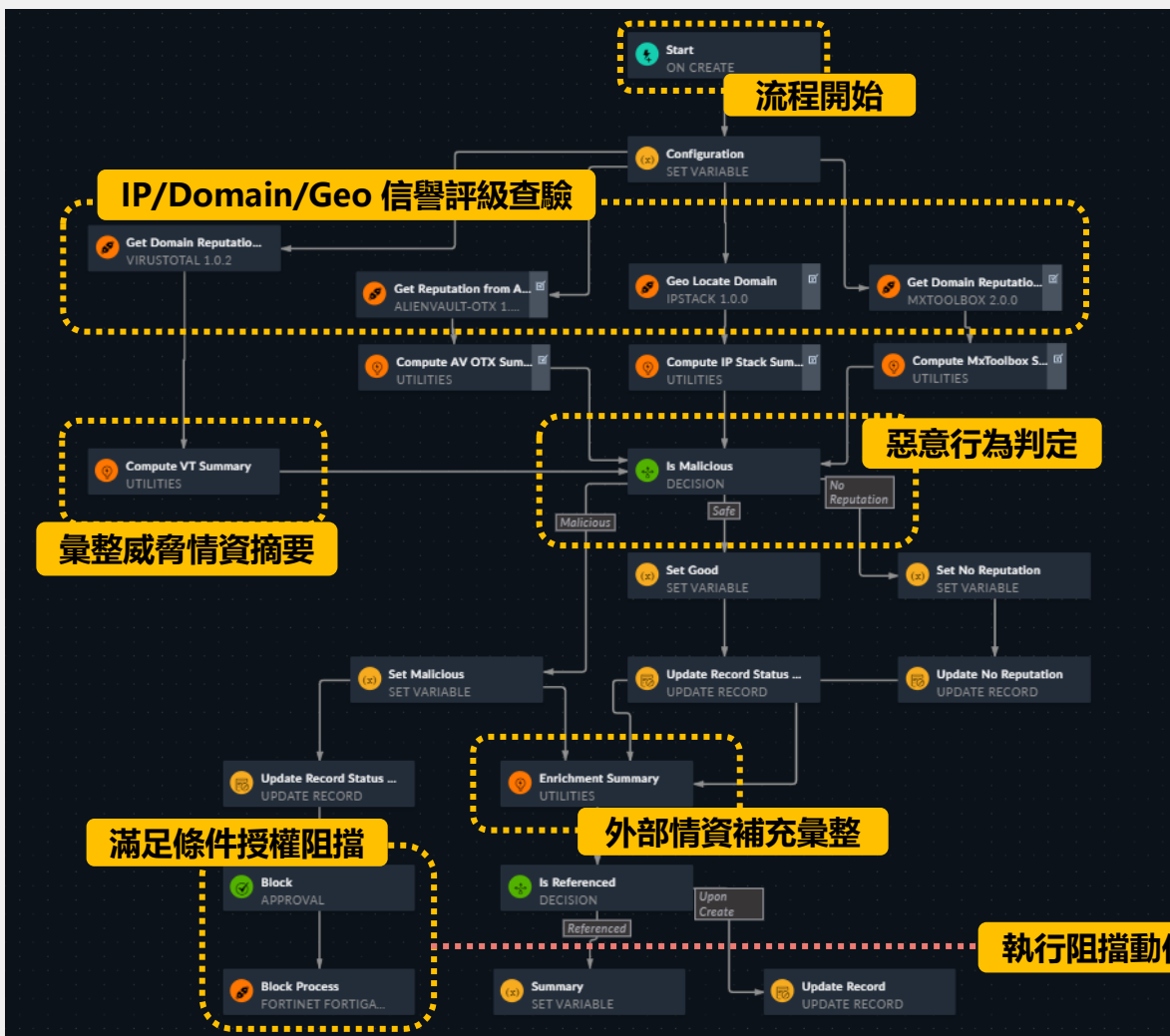
Click on the "Ok, Generate Playbook" button below to paste a playbook/block with above instruction on the designer page.

Ok, Generate Playbook



應用範例 – 安全威脅分析自動化作業流程

AI 智能 SOC 平台 (FortiSOAR) – 透過 FortiAI 生成 IOC 威脅攻擊自動化授權阻擋作業流程





FORTINET®