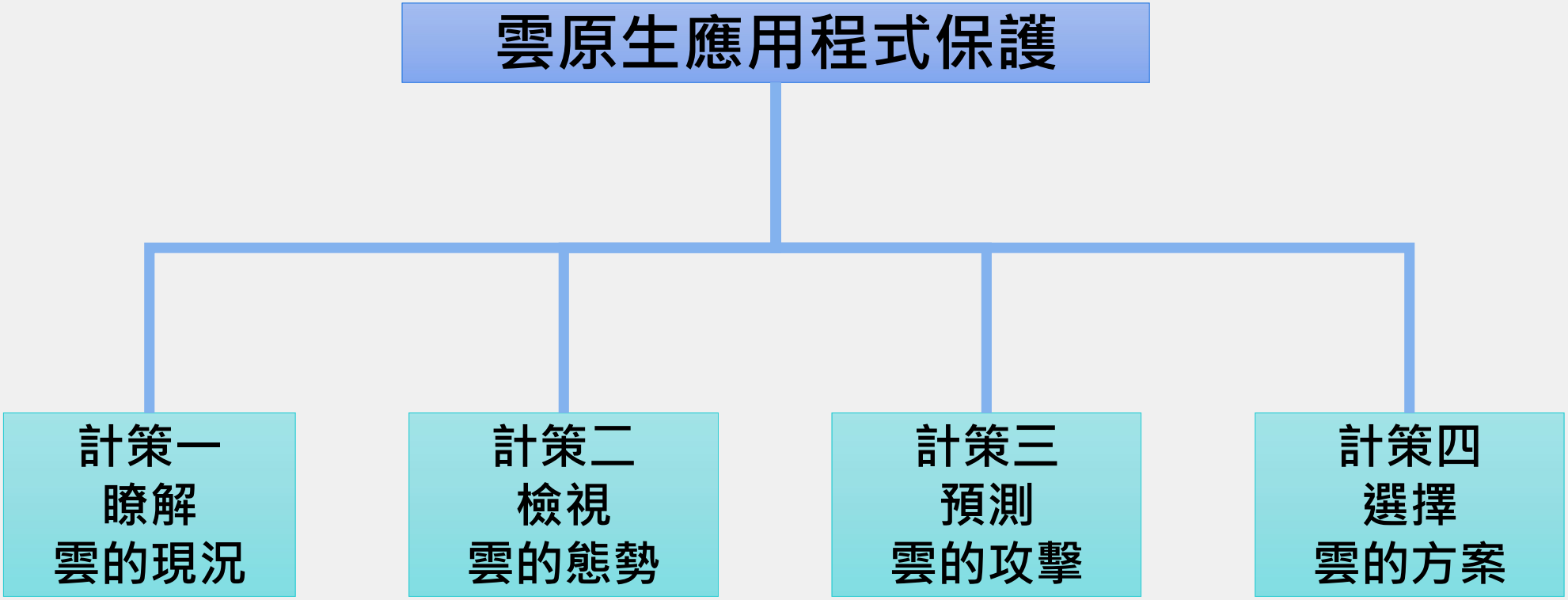
FORTINET | 2025 Fortinet 資安嘉年華
Resilience Powered by AI and Cybersecurity

雲原生應用服務保護平台 CNAPP

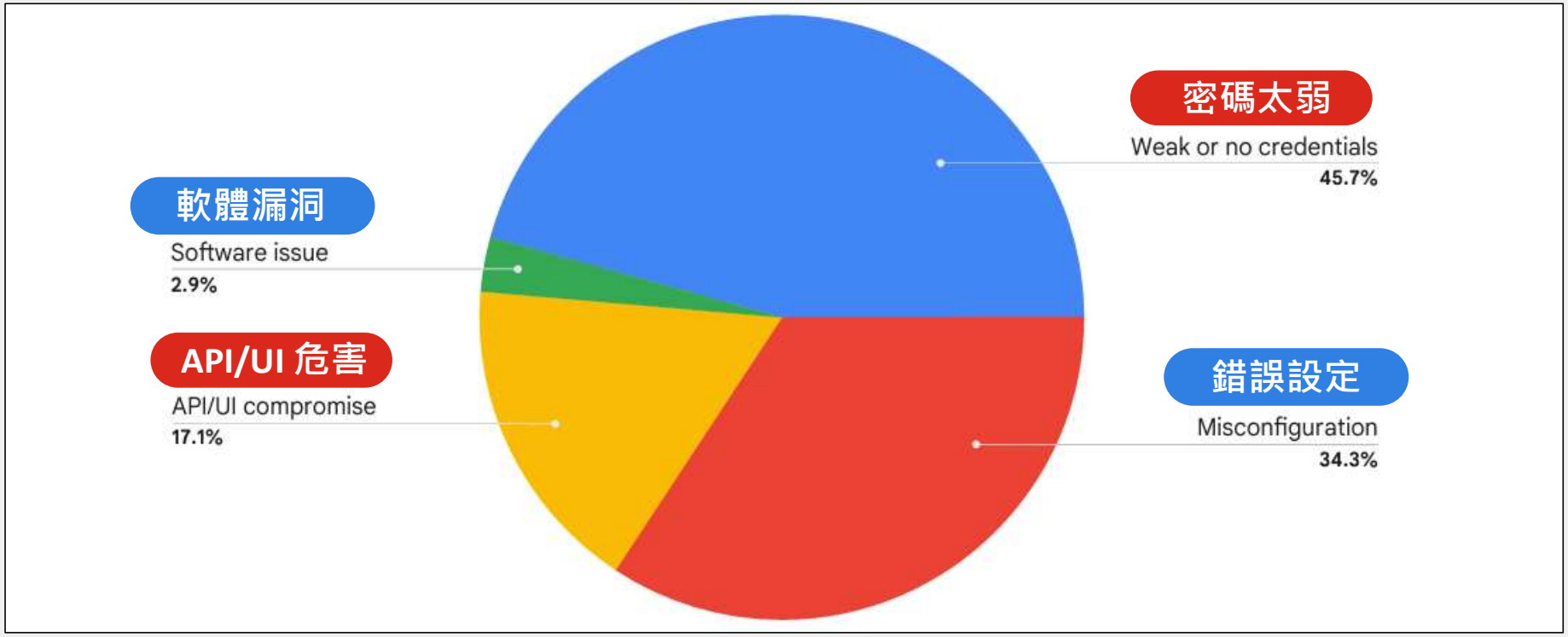
James Wang 王仁德
Fortinet 雲端領域資安技術顧問



瞭解雲的現況

4 大資安問題

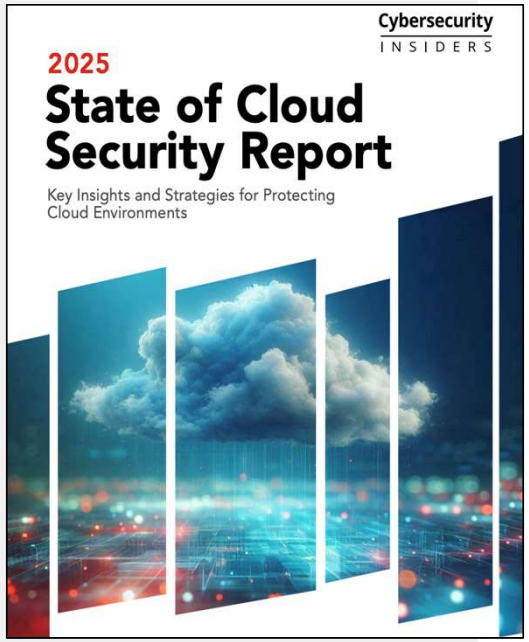
80% 雲端事件都是人為??



參考來源 : H1 2025 Threat Horizons Report

3 大維運挑戰

你的雲端安全嗎?!



64% 缺少能力

跨雲威脅及時偵測與回應

Cloud Network Firewall	Rating	Security Effectiveness	Rated Throughput (Mbps)	Price per Mbps
Amazon Web Services (AWS) Network Firewall	Caution	0.00%	813	$2.65
Check Point CloudGuard Network Security Nex-Gen Firewall	Recommended	100.00%	390	$4.38
Cisco Secure Firewall Threat Defense Virtual	Caution	53.50%	167	$10.62
Forcepoint NGFW	Recommended	96.66%	573	$2.85
Fortinet FortiGate Next-Generation Firewall	Recommended	100.00%	795	$2.25
Google Cloud Platform (GCP) NGFW Enterprise	Caution	0.00%	835	$3.16
Juniper Networks vSRX Next Generation Firewall	Recommended	99.80%	637	$2.91
Microsoft Azure Firewall Premium	Caution	0.00%	3,641	$0.66
Palo Alto Networks VM-Series Next-Gen Virtual Firewall w/ Advanced Threat Prevention (PAYG)	Recommended	99.61%	570	$3.29
Versa Networks NGFW	Recommended	99.90%	2,000	$1.27

除了 CyberRatings 內部開發的測試工具外，我們還使用 Keysight CyPerf v5.0 軟體測試平台對雲端防火牆進行了測試。企業可以透過 Keysight 提供的兩週免費試用版輕鬆進行類似的測試。有關 CyPerf 攻擊庫的更多詳細信息，請訪問： https://www.keysight.com/us/en/products/network-test/cloud-test/cyperf.html

2 大工具難處

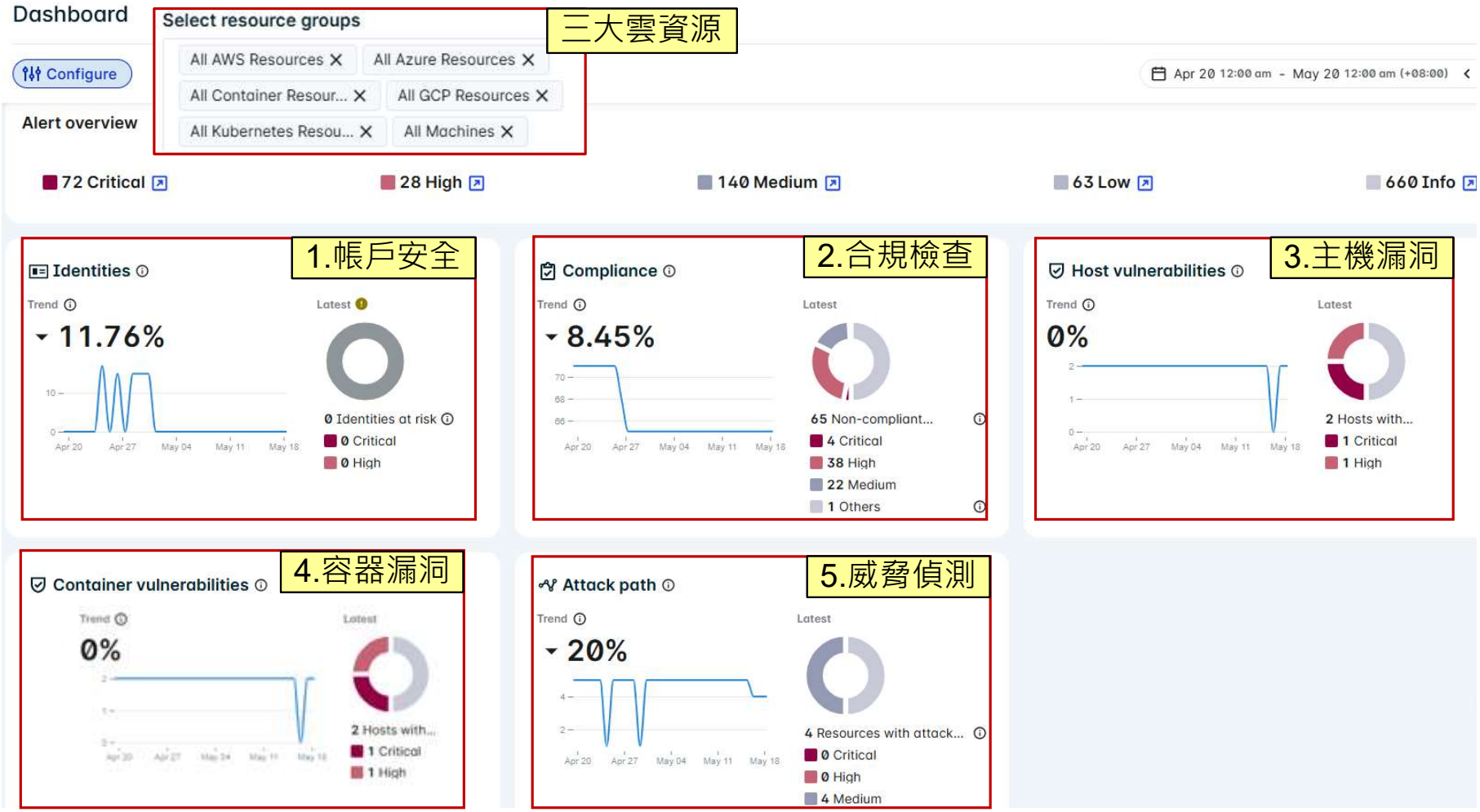
工具不是多就比較好歐!

- **難處一：系統分散多套**
  - 平均 6-10 個工具
  - 複雜分散
  - 覆蓋死角
- **難處二：系統無法整合**
  - 分散難整合
  - 問題難關連
  - 應變難排查

檢查雲的態勢

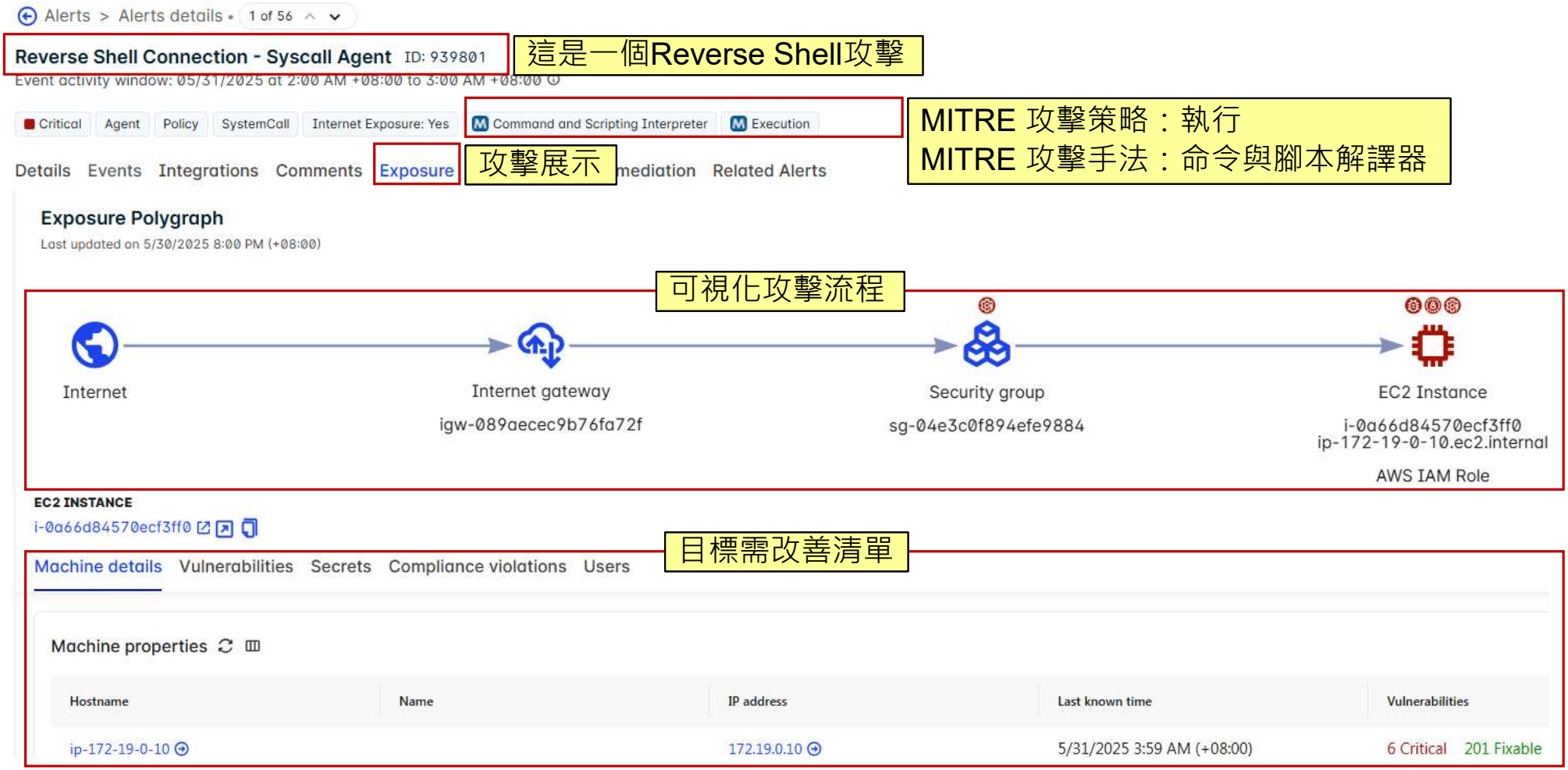
FortiCNAPP 多雲一目了然

AI 三雲 7x24 監控



FortiCNAPP 攻擊一網打盡

AI 事件快速應變



FortiCNAPP 回應一步到位

AI 輔助管理

沒有CNAPP前

會會、會會、萬萬會 ...

FortiCNAPP 回應一步到位

AI 輔助管理

引進CNAPP之後

AI 告訴你攻擊手法

警報939801詳細分析

根據警報939801的詳細資訊,此警報是由Lacework的主機型代理程式 (Host-based Agent) 偵測到反向Shell連線 (Reverse Shell Connection) 而觸發。以下是此警報的關鍵資訊:

- **警報名稱:** Reverse Shell Connection - Syscall Agent
- **警報描述:** 偵測到重複的違規事件,執行了 `/bin/sh`
- **警報類別:** Policy (策略)
- **警報子類別:** SystemCall (系統呼叫)
- **警報來源:** Agent (代理程式)
- **警報嚴重性:** Critical (嚴重)
- **觸發的策略ID:** lacework-global-667

反向Shell連線的安全風險

反向Shell是一種常見的攻擊技術,攻擊者在取得目標系統的初始存取權後,會建立反向Shell來獲得持續的遠端存取。反向Shell的運作方式是讓受害者的機器作為Server端,主動連線到攻擊者的機器 (Client端)。這使得攻擊者能夠規避防火牆限制,維持對受感染系統的控制。

AI 指導你如何緩解

回應反向Shell攻擊的建議

您提供的警報939801資訊顯示,Lacework代理程式偵測到一個反向Shell連線。反向Shell通常被攻擊者用來在入侵系統後維持持續的遠端存取。以下是一些建議,可有效回應和減緩反向Shell攻擊對雲端環境的風險:

事件回應

1. **調查警報:** 釐清偵測到的活動是否為預期或正常操作的一部分。檢視警報詳細資料,包括受影響的主機/容器、進程詳細資訊和網路連線。
2. **遏制影響:** 如果活動可疑,請隔離受影響的系統以防止進一步擴散。這可能涉及網路分割、封鎖可疑IP位址或讓系統離線。
3. **執行鑑識分析:** 進行徹底調查以找出根本原因、攻擊途徑和潛在的攻擊者活動。收集並分析相關日誌、記憶體轉儲和磁碟映像。
4. **消除威脅:** 一旦瞭解事件,請刪除攻擊者引入的任何惡意軟體、後門或未經授權的變更。這可能需要從乾淨的狀態重建受影響的系統。

AI 提醒你預防再發生

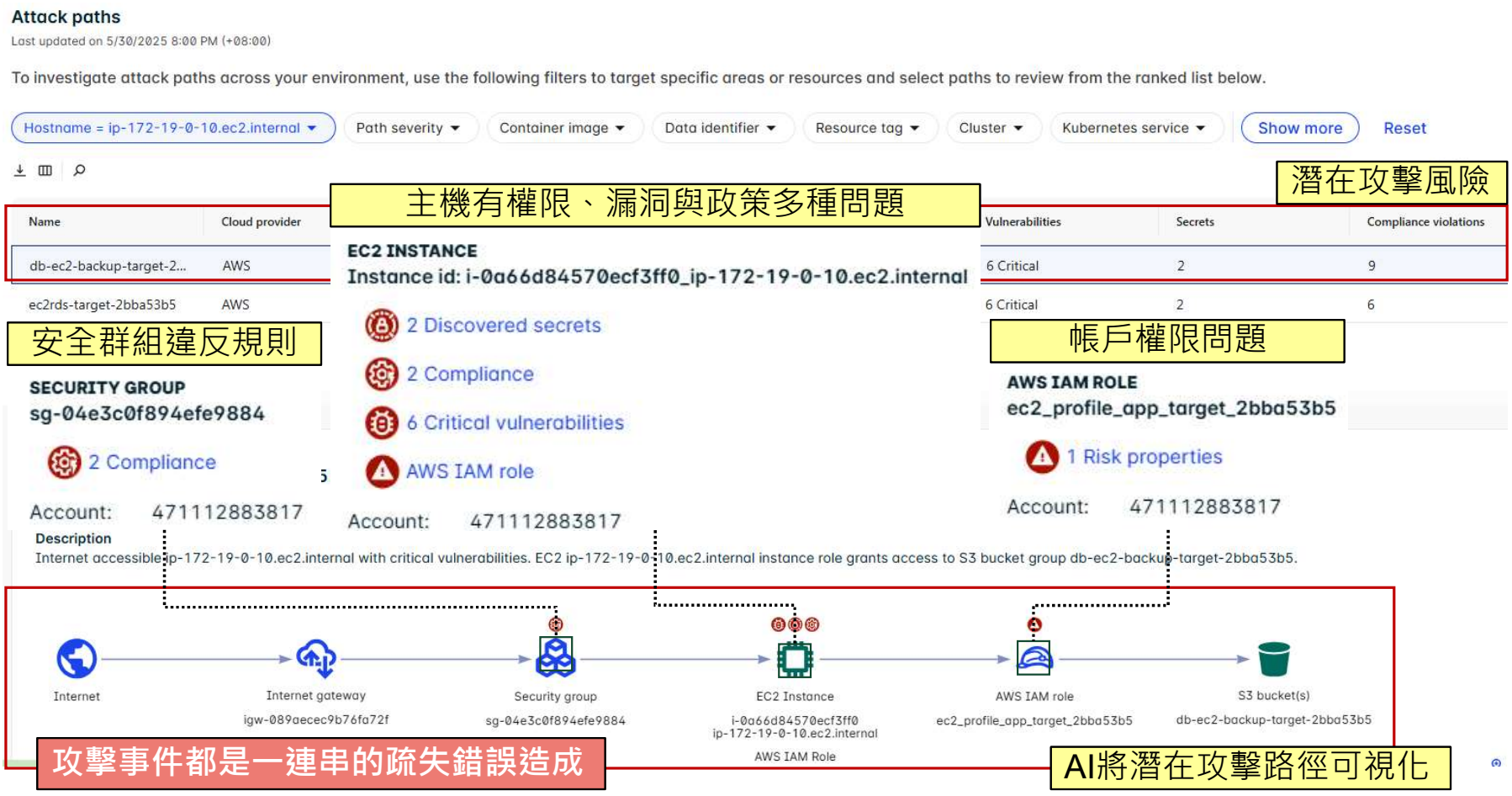
降低反向Shell風險

1. **加強存取控制:** 實施強大的身份驗證機制 (例如多因素驗證) 並遵循最小權限原則。定期檢視和更新使用者權限。
2. **強化系統:** 應用安全最佳實踐,例如修補漏洞、停用不必要的服務以及配置嚴格的防火牆規則。使用強化的作業系統映像和容器基礎映像。
3. **實施網路分割:** 將您的雲端環境分割成不同的安全區域,以限制攻擊的影響範圍。使用網路存取控制來限制區域之間的通訊。
4. **監控和偵測異常:** 利用Lacework等工具持續監控雲端環境中的可疑活動。設置警報並及時回應潛在威脅。
5. **教育和培訓員工:** 提供安全意識培訓,教導員工識別網路釣魚、社交工程等常見的攻擊手法。建立明確的事件回報程序。

預測雲的攻擊

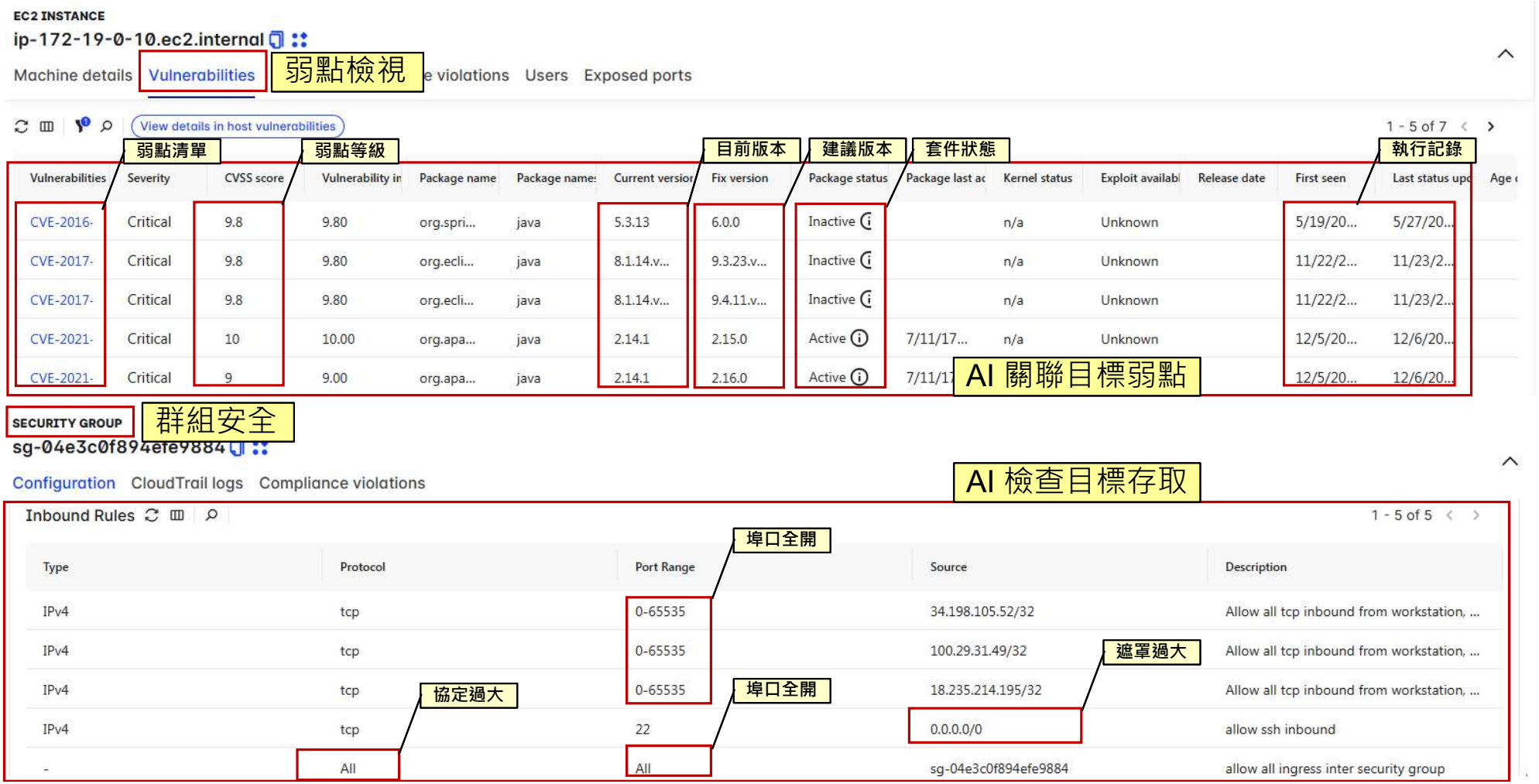
FortiCNAPP 攻擊路徑料敵先機 (Attack Path)

AI 攻擊預知預警



FortiCNAPP 事件問題料事如神

AI 危險弱點預告



FortiCNAPP 檢視組態防微杜漸

AI 持續修正雲端 (帳號、設定、合規、活動)

選擇雲的方案

為什麼選擇FortiCNAPP

FortiCNAPP – 給企業效益

風險預測

避免企業雲端攻擊

持續檢查虛擬機器、容器和工作負載，以便在風險被利用之前解決它們。

威脅偵測

解決人力與技能不足

全面檢查雲端資源，主動告知漏洞、錯誤配置和過度權限，強化團隊合作。

AI 應變

縮短回應於數分鐘

偵測、調查和回應異常行為和威脅，阻擋洩漏的憑證、勒索軟體和加密挖掘。

雲端萬變，先知先勝
FortiCNAPP，預見即防禦

風險預測

避免企業雲端攻擊

持續檢查虛擬機器、容器和工作負載，以便在風險被利用之前解決它們。

威脅偵測

解決人力與技能不足

全面檢查雲端資源，主動告知漏洞、錯誤配置和過度權限，強化團隊合作。

AI 應變

縮短回應於數分鐘

偵測、調查和回應異常行為和威脅，阻擋洩漏的憑證、勒索軟體和加密挖掘。

FORTINET

2025 Fortinet 資安嘉年華

Resilience Powered by AI and Cybersecurity