

主動式防禦

# 託管威脅狩獵服務

Managed Threat Hunting Services (MTHS)

利用中芯數據 MTHS 使您將擁有一支能夠識別未知威脅的獵人團隊，利用我們對攻擊者策略和技術的了解，不斷尋找隱藏在您環境中的威脅，使您能夠在損害發生之前採取行動。

## 我們可以在您的環境中檢測到什麼？

### 勒索軟體和惡意軟體

檢測用於傳遞惡意可執行檔的策略和工具

### 新興攻擊技術

識別對手進行初始訪問、偵察和橫向移動的手段

### 網路進階威脅 (APT)

偵測橫向移動或其他惡意網路活動的跡象



## 我們怎麼回應您環境的威脅？

一般的 MDR 或 MSSP 廠商僅將 EDR 的告警轉發給您，僅提供告警監控與處理建議，但實際事件處理仍需您親自執行。

### 我們的 MTHS 是包含 DFIR

因此，我們的通報不只是提供建議，而是直接給您明確的答案。每項通報均經過我們的專家深入分析與調查，並以時間軸與清晰的語言編寫完整的威脅上下文，讓您輕鬆理解威脅的根本原因與範圍。

< 5min 從發現到處理，一次到位。

### 主動

即時分析所有告警  
主動通報惡意程式

### 查找

通報當下立即提供  
未知惡意程式路徑  
未知惡意中繼站

### 清理

一鍵清除惡意程式  
隨時諮詢詳細狀況



發現未知威脅並採取行動



有效阻斷攻擊鍊各階段的威脅

## 您能透過我們中文的自動化平台做什麼？

我們的IPaaS回應編排功能提供了從環境中，終止所有攻擊者的存在和活動的方法！

- ✓ 遏止資安事件，自動化消除威脅，全球中繼站連線阻擋。
- ✓ 通報即是資安事件，完整提供攻擊說明及詳細解決方案。
- ✓ 單位設備管理，清楚掌握設備資安狀況，定期月報產出。



The dashboard displays the following key metrics:

- 端點活動總量: 2184835
- 告警總量: 8535
- IIH 總量: 184
- 未關單: 1
- 事件單: 1

Other visible sections include:

- 主機狀態:** 連線中主機 (14), 已安裝主機 (44), 主機近七天為回報 (30).
- 主機數量趨勢:** A line chart showing host quantity trends from 2025-02-20 to 2025-02-26.
- 端點安全狀態:** A gauge chart showing potential threats (潛在威脅) and known threats (已知威脅).
- 鑑識調查狀態:** A bar chart showing analyzed alerts (已分析告警) and pending analysis (分析中告警) for dates from 2025-02-21 to 2025-02-28.
- 授權狀態:** Platform: Main cluster, 權限數量: 100, 到期時間: 2025-12-31.

**功能亮点：**

- 直觀告警分析**: 全面掌握單位安全狀況、直觀瞭解告警分析情形、端點回報資料即時掌握。
- 端點設備的安全狀況**: 端點回報狀況掌握、遠端移除不麻煩、高風險設備通報全整理、直覺式程式盤點。
- 事件快速反應**: 資安事件快速處理、第一時間來龍去脈掌握、遠端清除惡意程式、中繼站全面阻擋、專業人員狀況確認。
- 定期監控與管理**: 每月報告掌握單位狀況、告警分析說明、通報全面整理、端點回報狀況紀錄。

中芯數據 Cyber Defense Center 作為您企業內部資安團隊的延伸，協助企業共同防禦進階威脅。 [www.corecloud.com.tw](http://www.corecloud.com.tw)

詳情內容請洽中芯數據  
台北 02 6636-8889 新竹 03 621-5128  
台中 04 3606-8999 高雄 07 976-8909