RAPID7

Threat Command

進階外部威脅情報解決方案

主動監控明暗網中數千個來源，
協助企業迅速做出明智決策，
緩解外部威脅！

許多個資及企業機密早已外流，如何建立資安情報網？

Rapid7獨特的搜尋引擎，
可從網路上最深和最難到達的地方收集情報，
以識別企業在其它情況下可能永遠找不到的威脅。

Rapid7 Threat Command 具以下特色：

資產威脅導向

過濾網路大數據產生的雜訊，並專注於威脅相關問題。使用企業獨特的品牌和數位足跡資產，Rapid7 Threat Command平台可以快速識別與威脅脈絡化，並針對即將發生的攻擊發出警報。

一鍵式修復

面對威脅，簡化後續的反應流程，立即將可疑網域發送到阻止列表（黑名單），快速啟動威脅清除。在不斷收到補救狀態通知的同時，持續追蹤惡意活動直到威脅清除。

專業分析師協助

可直接與Rapid7的情報專家互動，透過網路分析師獨特的“由外而內”視角並了解威脅參與者的思考和運作方式，以獲取更多背景資訊並啟動更深入的資安鑑識與調查。

多維度威脅分析

加入時間軸維度，時時透過監控和驗證威脅，以了解完整的威脅脈絡，並與特定威脅的多個input及參數進行關聯分析。

隱蔽式數據偵察

無論其威脅來源如何，可低調地識別與偵查威脅，不引起關注，避免造成企業處於危險之中。

警報分析器

透過機器學習及人工智慧，可以快速確認威脅狀態。同時，警報分析器能夠提供微調警報確認，進而讓SOC團隊花費更少的時間來整理不相關的警報。

六大效益

適用產業：
金融 / 製造 / 石化 / 零售 / 電子商務 / 遊戲 / 醫療/ 通訊 等

- 即時威脅可視化
- 加速威脅緩解
- 改善SecOps效率
- 品牌安全意識
- 主動資安防禦
- 降低資安風險

All-In-One 威脅情資解決方案，從威脅偵查、鑑識到緩解與清除。

難以觸及的外部威脅

在現今的網路世界中，到處都蘊藏了潛在的攻擊資訊，包含了公開的明網 (Clear Web) 與表網 (Surface Web)，還有地下網路環境，所謂的深網 (Deep Web) 及暗網 (Dark Web)。若企業想要儘早掌握威脅情資，得知是否已然成為駭客攻擊的目標，勢必需要在網路世界裡追溯、查找相關數位足跡。正因為如此，許多資安分析專家會嘗試潛伏到這些無法直接存取的網路環境中，從旁觀察駭客們之間的互動，打探各種可能的、非法的攻擊與個資交易行為。

識別、評估、緩解外部威脅

Rapid7 Threat Command 可以根據企業的數位足跡，採取自動分析與偵測查找，透過簡易的步驟進行外部威脅緩解。將情報與企業資產進行關聯性分析，對於有效的威脅防護至關重要，面對企業、員工、原始碼、品牌和客戶的外部威脅，能夠主動識別、評估及修復，與市場上或傳統的的其他威脅情資解決方案不同，省去了繁重的操作與工作，有效地降低威脅情報的複雜性，擁有威脅情資即時性的優勢。透過 Rapid7 Threat Command，可預先獲得威脅情資並針對即將發生的攻擊提供事先預警，超前部署！

將外部情報轉化為安全行動

Rapid7 Threat Command 是市場上唯一的 All-In-One 解決方案，旨在應對網絡威脅殺傷鏈各個階段的挑戰，從攻擊指示到妥協，再到調查和補救。透過 Rapid7 Threat Command，將協助企業了解每種威脅、IOC、CVE、洩露的數據庫和駭客互動如何影響到企業運作。

All-In-One威脅情資解決方案

Rapid7 Threat Command 通過將外部情報對應到企業獨特的數位資產，不斷發現針對企業的關鍵威脅，可以從明網、深網和暗網中，提供量身定制的資安情報，依據嚴重性提供不同類別的安全警報，主要包含了風險類型 (例如：網絡釣魚、品牌安全、資料外洩等)、外部來源 (例如：黑客論壇、社交媒體、黑市等)。同時，也提供互動式儀表板可以輕鬆將情報轉化為行動、管理警報、簡化操作並降低風險。透過一鍵修復，直接在警報中協調跨跨團隊合作，落實威脅修復的生命週期。

智慧資安科技股份有限公司｜核心資安團隊
114台北市內湖區基湖路35巷13號8號
T+886-2-8798-6088分機1100
林玉萍 mobile：0955-228-402｜E-mail：rachellin@unixecure.com.tw