Recorded Future®

DATA SHEET

安全維運情資

加速處理警報，使用針對安全工作流程設計的智能引擎

挑戰

隨著威脅不斷增加且快速地變動，導致資安團隊每天都需要面對非常多的警報，研究數千條原始數據通常是手動且受限於人力，即使是經驗豐富的資安分析師也可能感到如牛負重，由於時間上的不足，且在資安工具中缺乏足夠的背景和資訊，難以確定該警報代表何種關鍵事件，抑或重複或誤報，同時真正的獨立事件可能會意外漏網。過多的警報，且資源不足以及訊息有限的情況下，使得資安團隊感到不堪重負。

解決方案

Recorded Future 安全維運情資模組讓資安團隊能夠有效地處理警報，偵測過去未察覺的威脅，並在不干擾業務運作的情況下封鎖威脅，此模組被設計成可整合現有的安全工作流程與工具，為分析師提供全面的情報，不增加額外的複雜性。

Recorded Future 自動搜集、分析並產生情報，來自各種公開網站、暗網和技術來源，結合世界一流的研究，加速應對。使用 Recorded Future 安全維運情資模組，使用者可獲取高風險指標的現成數據，提供分析師在企業尚未被影響情況下，識別威脅。此解決方案為來自防火牆、代理、防毒軟體以及其他安全日誌的內部網路，提供有價值的背景資訊。

安全維運情資可整合到 SIEM、SOAR、EDR 或 XDR 工具中，用於警報分類和威脅檢測的情境，提供即時的風險評分與關鍵指標的證據，協助分析師快速排除，確定警報的優先順序，並在需要進一步調查時，獲取更多資訊，不再依賴手動彙整相互關聯和分類訊息的需求， 大幅縮減檢測、調查和應對真實威脅所需的時間。

優勢

- 充分發揮現有安全工具的投資價值
- 偵測過去未被發現的威脅
- 減少 40% 調查時間
- 提升平均偵測時間 (MTTD) 與平均回應時間 (MTTR)

主要特色

- 提供即時風險評分和相關背景資訊
- 支援整合安全資訊與事件管理 (SIEM) 安全事件與回應 (SOAR)、端點安全性 (EDR)
- 提供覆蓋最廣泛的資料來源
- 儀表板首頁顯示威脅主題趨勢和專家研究

成果

調查時間縮短 40%

Recorded Future 安全維運情資模組省去了長時間的手動研究，提供即時風險並透明化關鍵證據，使團隊能夠快速且有效地做出決策。

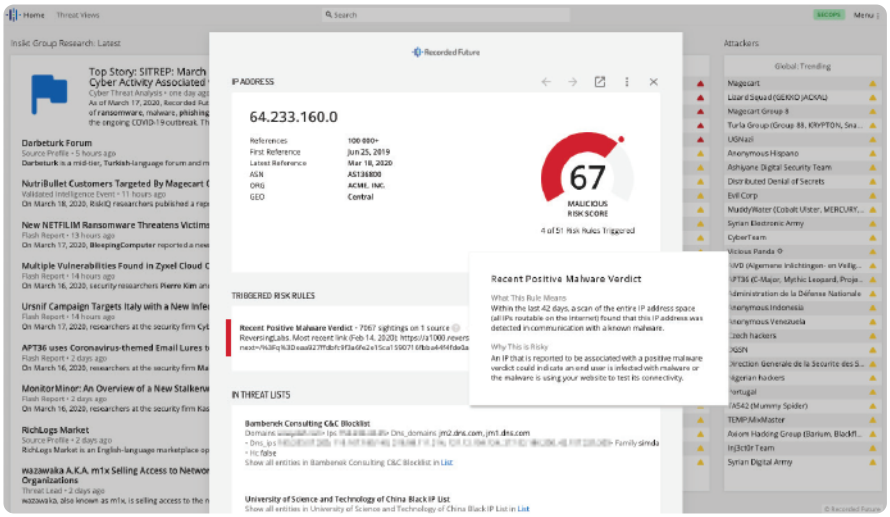
高達 20% 偵測更多威脅

安全維運情報模組整合並將風險清單與有關 IP、域名、入侵防護系統 (IPs) 與整合惡意軟體相關的訊息，有效地偵測威脅並快速應對，降低風險。

降低客戶 50% 調查時間

提供分析師在已使用的工具中，獲取敵對的基礎設施、目標以及覆蓋最全面的情報機會，減少複雜性，協助客戶更有效地採取行動。

*想要深入了解 Recorded Future 為客戶帶來的商業價值，請參閱 Forrester 報告：Recorded Future 威脅情報平台的總體經濟影響™



案例情報清單顯示有關 IP 地址的全面情報，包括風險評分、專家分析以及透明化情報原始來源等。

為何需要安全維運情資?

透過自動化分析情報，將情報整合至安全資訊與事件管理 (SIEM) 與工作流程中，我們相信已將安全監控的準確性和營運效率提升了三到四倍。

沖繩科技大學
長瀨慶太 資安長

FAIRLINE
Quality Service Through Team Work

台北總公司
台北市內湖區
瑞光路583巷32號5樓
電話：02-2658-1818

台中辦事處
台中市北屯區文心路四段83號19樓301室

高雄辦事處
高雄市三民區民族一路80號27樓之2 A08室

關於 RECORDED FUTURE

Recorded Future 是全球最大的情報公司，雲端的情報平台在敵對方、基礎設施和目標方面提供了最全面的覆蓋，通過整合持續的自動數據收集與分析以及人工分析，Recorded Future 即時提供對龐大數據的可視性，讓客戶采取積極的行動並瓦解敵對的勢力，保護人員、系統和基礎設施的能力。總部位於波士頓，擁有遍佈世界各地的辦事處和員工，Recorded Future 與超過 1,700 家企業和政府機構合作，覆蓋超過 75 個國家。

www.recordedfuture.com @RecordedFuture