Recorded Future®

DATA SHEET

威脅情資模組

主動辨識、調查以及優先處理網路威脅

挑戰

隨著時間不斷演進的環境威脅已變得非常龐大且複雜，企業可以完全保護自己，並避免所有潛在威脅的影響，已變得不切實際，幾乎各種規模與所有產業的企業，都在保護數位資產，避免持續受到攻擊者的侵害，面臨一系列的挑戰，威脅情資的使用和應用是至關重要的一環，充分發揮價值時，它往往是防止資安事件發生的關鍵因素。

解決方案

為了防禦新興的網路威脅，需要即時的分析，Recorded Future 威脅情資模組提供全面檢視的獨特能力，透過情報平台，數十億個實體情報被融合在一起，提供研究、動態分類、連結以及分析，可直接整合到您現有的系統中，以前所未有的速度，讓您輕鬆獲取易於理解的資訊。

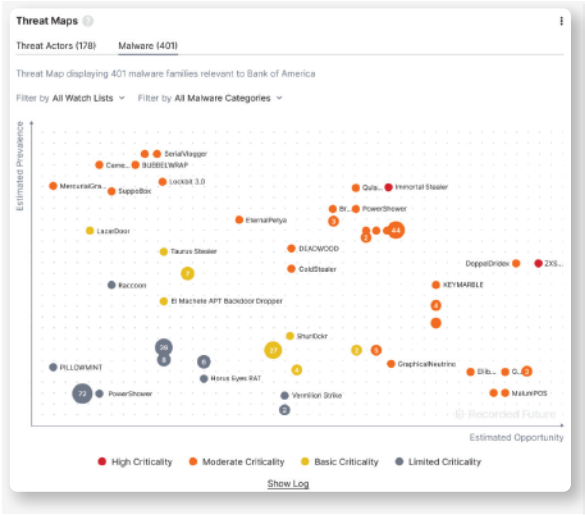
全球最先進的情報平台，能使您快速、有效地做出決策，先進的查詢功能、即時警報以及可視化威脅功能等優勢，提供進行高威脅研究和搜尋威脅封包所需的詳細內容，利用 Recorded Future 威脅情資模組，快速檢測關鍵威脅，並提早應對新興威脅。

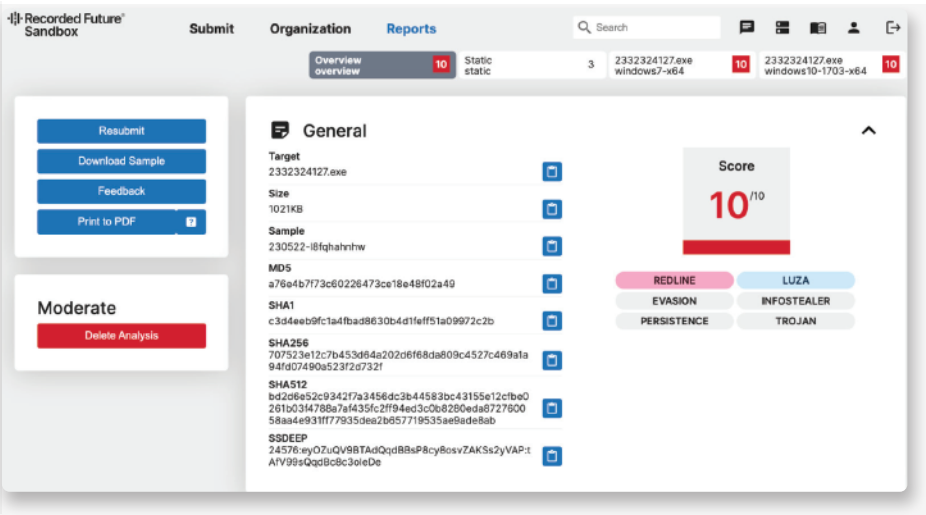
優勢

- 辨識並優先處理與企業相關的威脅
- 迅速偵測威脅，並快速回應
- 可視化封閉的網路來源
- 善加運用現有的安全工具，以最大程度發揮投資效益

主要特色

- 威脅行為者以及惡意軟體的威脅地圖
- 惡意軟體沙箱
- 進階查詢功能
- 自訂警報功能
- 獵捕威脅包
- 開箱即用整合能力





主要特色

功能	詳細內容	實際案例
威脅地圖	自動可視化威脅行為者、第三方以及同行相關的惡意軟體，主動識別、分析並回應網路威脅，優先處理對您影響較大的風險。	一家跨國銀行的威脅情報團隊，成功地減少大量的警報，使團隊能夠專注針對企業與同行相關、優先級最高的威脅行為者。
沙箱	以速度和可擴展性為重點的沙箱解決方案，通過 API 進行自動記錄及擁有完全可自定義的環境，即時控制災害、標記惡意軟體...等，支援您的調查與主動減緩措施。	一家國際金融公司透過使用沙箱解決方案，判定許多惡意軟體和釣魚網域，他們能夠快速地判斷檔案是否為機器人，在調查中節省了大量時間，從沙箱解決方案中獲取的指標，有助於進一步成功遏制惡意軟體。
進階查詢功能	針對您的需求深層地在 Recorded Future 情報資料庫中搜尋，情報可儲存和分享，以便團隊輕鬆存取感興趣的內容。	允許一家軟體公司的團隊對歷史資料中的威脅行為者，執行進一步的研究和分類，該團隊設置特定的查詢方式，監視暗網上有關洩露憑證與感興趣的 IOC (指標) 的資訊。
自訂警報功能	根據您的需求，每當識別到新的情報時，即可透過電子郵件、手機應用程式或平台頁面即時通知您。	當警報辨識出客戶的域名，在俄羅斯的暗網市場中被提及、牽涉洩露憑證時，他們進行調查，尋找感興趣的 IOC (指標) 存取必要的 YARA / Sigma 規則，進一步分析並解決問題。
獵捕威脅包	為您的團隊提供檢測機制，包括 YARA、Snort 和 Sigma 規則，用於搜尋對手、惡意軟體或感興趣的流量。	一家電腦硬體公司每週透過辨識具趨勢的威脅行為者，利用檢測規則 API 獲取 YARA / Sigma 的規則，運用獵捕威脅包，監視他們的環境，提升整體的安全性。
整合	即時提供機器可讀取的情報，透過無縫整合和簡單的應用程式介面 (API)，融合在已在使用的安全技術中。	一家金融公司透過 SIEM 工具整合 Recorded Future，有助於縮短調查時間，尤其是域名與 IP 地址的聲譽，進行更深入的分析，為事件提供更多資訊。

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