資料工作表

FireEye Threat Analytics Platform

運用即時威脅情報辨識威脅、加速回應。

重點

- 將即時 FireEye 威脅情報套用在企業事件流上，以辨識威脅和加速回應
- 無須投資基礎架構
- 利用現有企業安全架構中的事件，提供一致的威脅回應記劃
- 提供對威脅發動者檔案的多元檢視功能，提升對威脅型態的瞭解
- 以隨選即用的入口網站存取管理事件，進而提升分派、追蹤和解決事件的效率
- 提供量身訂做的策略服務以符合貴企業的需求

FireEye® Threat Analytics Platform (TAP) 係爲一套雲端解決方案，以 FireEye 即時威脅情報分類所產生的事件資料，讓安全團隊辨識和有效回應網路威脅。

多數重視網路安全的企業無不花費大量資源累積記錄和事件資料，以滿足法規和合規的需求。然而，提到分析和回應先進攻擊，很少機制能擷取這些資料庫中的數值。FireEye Threat Analytics Platform 讓安全團隊可將傳統的系統事件與 FireEye 威脅情報整合，進而更有效回應威脅。

即時威脅情報可辨識威脅

FireEye Threat Analytics Platform 將最完整、最全方位的即時威脅情報運用在企業系統所產生的事件流，以找出入侵傳統安全解決方案的人。安全團隊可隨時隨需取得必要資訊，快速調查和提供有效回應。

提升威脅能見度

FireEye Threat Analytics Platform 利用 FireEye 威脅防護平台對威脅發動者檔案和行爲的多元檢視機制，提升對威脅型態的整體瞭解。

將警告排序以加速事件回應

FireEye Threat Analytics Platform 提供經分類的警告，進而加速和提升事件回應措施。本平台可快速決定可疑事件的影響範圍，讓安全團隊可做適當回應。並可轉移至警告內任一個領域，以找出相關使用者、端點和攻擊者的基礎架構。

低廉的擁有成本

此款雲端解決方案無須投資基礎架構，只要數小時即可在現有環境中設定完成。費用係根據分析的資料量來計算，沒有隱藏成本，可因應更多裝置和用戶。

簡化事件管理

本平台可分派、追蹤和測量任務完成的效率，進而簡化事件的管理和優先順序。事件回應者可將最新發現的資料連結到現有事件、加入註解、標註牽涉的資產和搜尋事件相關資料。

匯集事件資料以利事件回應措施

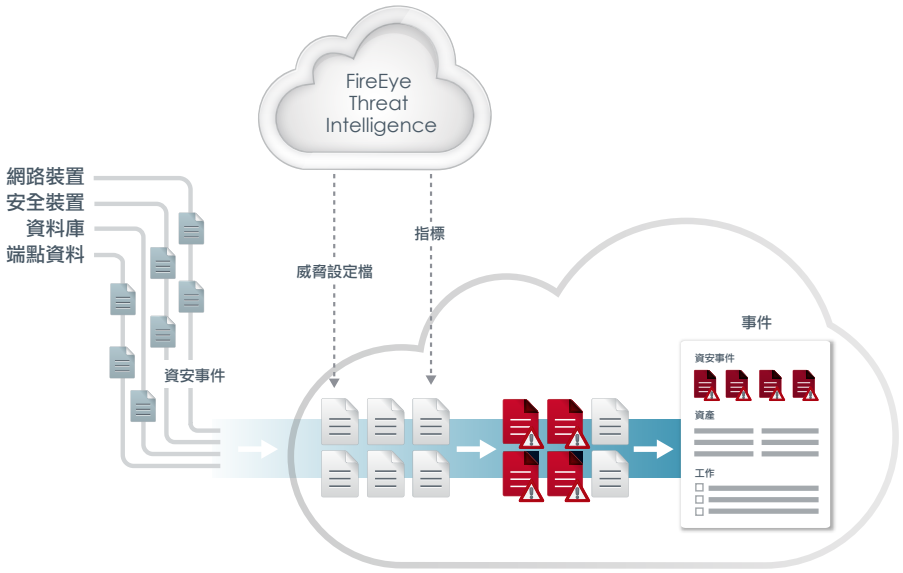
本平台盡可能保留線上資料和讓企業可隨需搜尋，功能彈性。可從使用者介面匯出搜尋結果，用於其他事件回應管理工具。

更快分析以決定威脅規模

FireEye Threat Analytics Platform 可讓您在幾秒內快速搜尋上百億筆事件，並將事件記錄與 FireEye 威脅情報相關聯，以判定威脅的所在和影響。此外 TimeWrinkle™ 功能會顯示事件發生前後的事件。

量身訂做的策略服務產品

FireEye Threat Analytics Platform 提供自訂服務產品。Mandiant 並提供安全營運諮詢服務和基本服務。此外，還有 FireEye Threat Analytics Platform 啓動服務，可快速加速 FireEye Threat Analytics Platform 的建置及與客戶現有安全措施的整合。



FireEye
Threat Analytics Platform