FIREEYE™

解決方案概要

強化以情報為主的惡意軟體分析

技術分類：惡意軟體分析

重點

- 輕鬆提交檔案以供分析
- 擷取報告並以背景資料添加到ThreatQ
- Query FireEye Malware Analysis (AX 系列) 設備使用來自 ThreatQ 的指標以找出任何該指標相關的警示
- 順暢地新增和移除來自 Malware Analysis 設備的 YARA 規則。

透過結合 FireEye Malware Analysis (AX 系列) 與 ThreatQ 平台，公司可以很快地提交可疑檔案進行分析、結果以報告方式呈現 (報告可新增至 ThreatQ 作為日後查詢使用)，並在 Malware Analysis 設備中修改 YARA 規則。

ThreatQuotient 製作的 ThreatQ

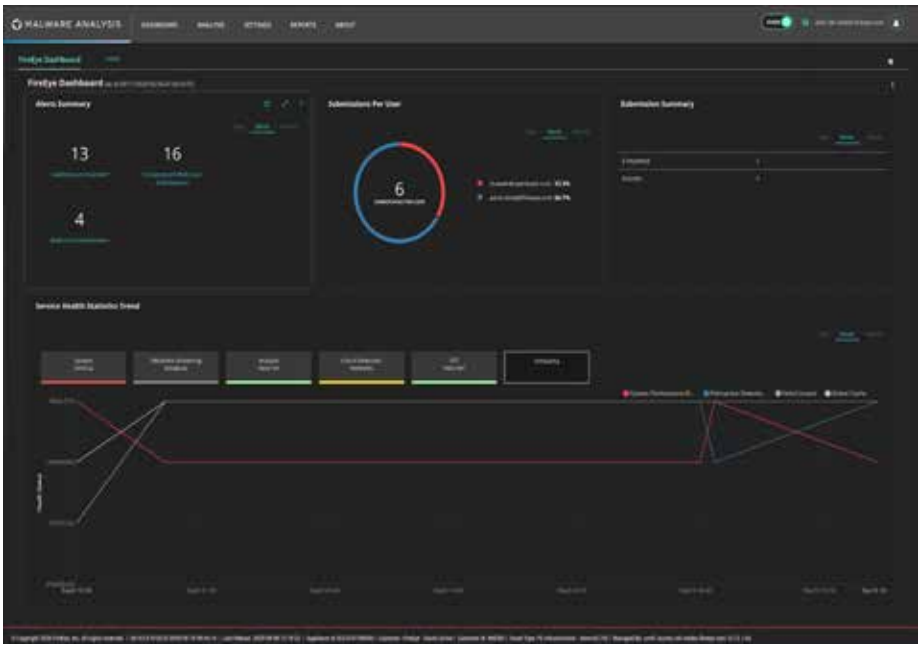
ThreatQuotient 解決方案讓資安作業更有效率，效果也更為顯著。ThreatQ 開放和可擴展平台將不同的安全技術整合到單個安全基礎架構中，可自動執行操作和工作流程，因此工具和人員可達成一致性。資安團隊可以根據公司獨特的風險狀況進行持續的優先等級排序，從而可以將資源集中在最相關的威脅上，並協同調查和回應，以便更快地採取正確的措施。

FireEye 的惡意軟體分析

FireEye 惡意軟體分析是一組鑑識分析解決方案，可讓資安分析人員對於自動設定的強大測試環境進行手動控制，以便用安全的方式執行並檢查網頁、電子郵件附件與檔案中內嵌的先進惡意軟體、零時差與進階持續威脅 (APT) 攻擊。

惡意軟體分析利用 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎，讓內部分析人員能 360 度全方位檢視攻擊，從初次入侵、回呼目的地乃至於後續嘗試的二進位檔下載，都面面俱到。網路罪犯會精心設計攻擊來入侵特定的企業、使用者帳戶或系統，因此分析人員需要有容易使用的鑑識工具，來協助他們快速解決目標性的惡意活動。

THREATQUOTIENT



ThreatQ 與 FireEye Malware Analysis 整合，可支援各種使用案例，例如：

快速輕鬆的提交分析樣本

- ThreatQ 使用者可提交檔案至 FireEye Malware Analysis，以利用 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎，讓內部分析人員能 360 度全方位檢視攻擊，從初次入侵、回呼目的地乃至於後續嘗試的二進位檔下載，都面面俱到。
- 透過預先設定、配備齊全的 Microsoft Windows 和 Apple Mac OS X 虛擬分析環境，MVX 引擎可以完整執行可疑的程式碼，以對常見 Web 物件、電子郵件附件與檔案進行深入檢查。

輕鬆擷取結果

- 惡意軟體分析讓管理員不再需要進行手動惡意軟體分析過程中耗時的虛擬機器環境安裝、基準化與復原作業。
- 資安作業中心分析員可以使用內建的自訂功能和承載檔案觸發的精細化控制。
- 惡意軟體分析可讓鑑識分析人員對符合企業需求的攻擊有全面性的瞭解。

使用 ThreatQ 以更簡化 YARA 偵測管理

關於 ThreatQuotient

ThreatQuotient 的使命在於透過威脅中心平台，提升資安作業的效率與成效。透過將公司已有的流程和技術整合到單一資安架構中，TheatQuotient 加速並簡化相同或跨平台與工具的調查和合作。透過自動化、優先等級劃分與可視化，ThreatQotient 的解決方案減少了干擾，並突顯高優先等級的威脅，好更能集中使用有限資源並支援決策。ThreatQuotient 總部位於北維吉尼亞州，在歐洲和亞太地區有跨國業務往來。若需詳細資訊，請前往 **https://threatquotient.com**。

若需詳細資訊，請聯絡 FireEye Technology Partners 團隊，信箱為：**integrate@FireEye.com**。

FireEye Taiwan | 台灣火眼有限公司
| 10683 台北市信義路四段 6 號 6 樓
+886 2 5551 1268 | FIREEYE |
taiwan@FireEye.com

關於 FireEye

FireEye 是一間情報主導的資安公司。作為客戶資安監控的無縫、可擴展的延伸，FireEye 提供單一平台，將創新的資安技術、國家級別的威脅情報和世界知名的 Mandiant® 諮詢融合在一起。藉由此方法，FireEye 為那些正在努力準備、預防和應對網路攻擊的組織，消除資安機制的複雜性和重擔。