FIREEYE™

產品型錄

Threat Intelligence 之訂閱

為您的業務提供資訊，不僅僅是您的設備

重點

- 提供涉及廣泛主題的全面可行的威脅情報
- 提供超越典型攻擊生命週期的可見性，對全域威脅增加語境和優先順序
- 改善資產保護，以做出明智的業務風險決策
- 針對您最可能面臨的威脅和實施者調整資安計畫和資源
- 處理戰術、營運和戰略用例
- 改進資安警報的優先順序和補救措施以及資安漏洞的修補

網路攻擊者比起許多資安組織受過更好的訓練、資金更充裕且人員配置更精良。網路攻擊越來越複雜，造成的破壞也越來越嚴重。找到並留住合格的資安專業人員已是非常困難，而要找到這麼多能夠完全應對這些挑戰所需的人才，成本勢必極為高昂。

資安組織正在設法增強自身資安專業知識水準和有效性。他們需要提高回應能力，並確保針對最可能面臨的威脅調整他們的防禦措施。而又不至於破產。

透過對FireEye Threat Intelligence 之訂閱能夠以經濟有效的方式應對這些挑戰 - 在戰略、營運和戰術層面上提供廣泛的可行且有效的資安洞察。

表 1. FireEye Threat Intelligence 的優點。

情報識別	優點
您因業務、產業或地區而面臨的威脅和實施者	支持您投資並部署適當的資安措施來解決它們
首先需要利用相關的語境洞察調查哪些警報	縮短偵測和提醒疲勞的時間並增加員工知識
首先根據針對類似組織的攻擊來修補哪些漏洞	優先安排修補工作並降低成功攻擊的可能性

FireEye Threat Intelligence 之訂閱專為滿足貴組織的需求而量身定制。訂閱類型包括：

- **Fusion：**全面瞭解目前、過去和未來可能出現的威脅活動。包括 Operational、Cyber Crime、Cyber Espionage 以及來自 Cyber Physical 的大多數內容和附加版本的 FireEye Digital Threat Monitoring。
- **Operational：**惡意軟體技術分析以及已知惡意實施者的相關戰術、技術和程序 (tactics, techniques and procedures, TTP)，包括存取惡意軟體設定檔資料庫、實施者概覽和機器可讀的漏洞指標 (indicators of compromise, IOC)，以獲取有關威脅的增強語境框架。
- **Cyber Physical：**針對工業環境和營運技術 (operational technology, OT) 面臨的網路威脅和風險的可行洞察。包括所有專注於 FireEye OT 和工業控制系統 (industrial control systems, ICS) 的情報。
- **Cyber Crime：**深入評估和跟蹤專門實施金融犯罪的威脅實施者 - 他們的目的、針對的目標以及如何運作。
- **Cyber Espionage：**有關特定國家關聯的指定進階持續威脅 (advanced persistent threat, APT) 群組的情報，包括其針對的目標和使用的 TTP，以幫助資安團隊瞭解和應對即將發生的和正在發生的威脅。
- **Strategic：**圍繞重要產業領域和區域的威脅評估，包括地緣政治、影響網路威脅形勢的事態發展以及對重大網路威脅問題在短期和長期內如何演變的預測。
- **Vulnerability：**對許多技術中已識別軟體漏洞的情報評估，以及對利用和緩解建議的可能性的專有評估。

情報通常以報告的形式呈現。在適用的情況下，將機器可讀的情報和 IOC 與您現有的資安產品 (如 SIEM 和漏洞管理員) 整合。FireEye Threat Intelligence 之訂閱還包括以下幾個資源：

- **FireEye Intelligence Portal：**線上存取您的情報報告以及與您的特定訂閱相關的完整 FireEye Threat Intelligence 歷史資料庫。您可以下載與特定類型的情報相關的 IOC，並執行搜尋以查找有關實施者、惡意軟體、產業和其他主題領域的情報。
- **分析師存取：**存取 FireEye Threat and Technical Intelligence 分析師，以便更加清晰、深入地瞭解實施者、攻擊和風險。您將更好地瞭解某些情報或事件如何與您的興趣直接相關。
- **交付選項：**確定您希望如何交付情報以及交付頻率，包括電子郵件警報和摘要。
- **每日新聞分析：**每日一封電子郵件，跟蹤媒體報導的目前資安故事，以使您詳細瞭解資安形勢。它包括媒體對故事的報導、FireEye 對故事準確性的評估以及相關的 FireEye 情報，以提高您的理解和回應能力。
- **情報 API：**該機器對機器的整合點使您可以在資安和網路營運、漏洞管理和事件回應系統中使用 FireEye 情報和我們的高效 IOC。
- **瀏覽器外掛程式：**該外掛程式將 FireEye Threat Intelligence 的技術整合擴充到您存取的任何網頁。它會自動在網頁上掃描技術指標 (如 IP 位址、網域、雜湊散列)，在情報 API 中查詢任何相關的 FireEye 情報，然後建立指向該情報的超連結。
- **情報工具：**客戶使用這些與情報相關的線上公用程式來查詢特定的網域名稱、IP 位址和威脅，並上傳可疑檔案以進行分析。

即使是最優秀的資安人員也無法瞭解每個主題領域的所有資訊(包括實施者、威脅、漏洞、有效補救、威脅搜尋)。透過對 FireEye Threat Intelligence 之訂閱,您可以擁有全球領先的威脅情報組織 FireEye 的知識、經驗、可見性和分析能力。現在,貴組織的每個人都可以獲取優秀的資安從業人員花費多年時間學到的資訊。

FireEye 優勢

FireEye 比任何人都更為瞭解網路威脅以及對其負責的人士。原因是我們擁有無與倫比的網路活動存取權限和廣泛的威脅情報業務。FireEye 將對手、受害者和攻擊活動資訊與產品遙測資料相結合,生成競爭對手無法比擬的可行威脅情報。我們的情報基於:

- 來自全球 22 個國家/地區的現場研究人員使用 30 多種語言交流,挖掘深層和黑暗網路,以提供有關對抗方法、動機和基礎設施的資訊
- 在客戶位置具有超過 15,000 萬個雙向模式網路感應器,可提供有關哪些威脅正在攻擊我們的全球客戶的資料
- 全球領先的事件回應組織 FireEye Mandiant 提供了針對成功實施攻擊的進階實施者所用的 TTP 進行的違規調查資訊
- 業內最大的威脅相關活動歷史資料庫,根據我們所有專家和技術人員收集的事件和事故資料建立
- 在「Forrester New Wave™:外部威脅情報服務,2018 年第 3 季度」中被評為唯一領導者

專門的客戶支援

三個級別的情報支援和支援可供選擇:

1 級
基準:使用 FireEye Intelligence Portal 並在組織中設定情報 API 所需的基本材料和流程。

2 級
情報協調:基準 + 指定的情報支援經理,查詢存取 FireEye 情報分析師、季度威脅簡報和半年一次的正式審查。

3 級
情報優化:情報協調 + 指定的情報優化分析師,其他分析師查詢、自訂威脅報告以及戰略研討會和威脅簡報。

欲深入瞭解,請造訪:**https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.html** 並閱讀 **Forrester 報告**。

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, Inc.
FireEye 是一間情報主導的資安公司。FireEye 以流暢、可擴充的客戶資安作業延伸,提供了混合創新資安技術、國家級威脅情報以及世界知名的 Mandiant® 諮詢服務的單一平台。藉由此方法,FireEye 得以讓對於準備、預防及回應網路攻擊感到苦惱的組織,消除資安機制的複雜性和重擔。