資料工作表

McAfee Cloud Threat Detection

輕鬆增強 Intel Security 防護機制以判定進階惡意軟體並使規避性威脅現形

一連串的最新分析技術 (包括機器學習) 可識別惡意軟體，並將判定結果轉化為行動，更新防護機制以便日後攔截類似攻擊。

主要優點：

- 降低傷害企業之未知威脅的風險。
- 駕馭巨量資料和機器學習的強大威力。
- 最佳化安全性投資項目。
- 簡化進階威脅分析的部署作業。

由於狡詐的惡意軟體會不斷規避傳統防禦機制，因此這對組織來說是一場硬仗。進階偵測解決方案雖然有所助益，但如果您的資安人員和資源有限，這些解決方案就顯得較為複雜且昂貴。大部分解決方案也不會與防護基礎架構整合，使得應變人員只能倉促行動，因而造成漏洞曝露時間增加。

下一步該怎麼做？極易部署和使用且符合成本效益的進階偵測：McAfee® Cloud Threat Detection。這項便利的新服務可導入現有的 Intel® Security 解決方案，以判定進階惡意軟體並使規避性威脅現形。您可透過這項雲端服務輕鬆地發揮龐大的運算效能，以操作各種最新的分析技術。您可以增強偵測能力，並將現有的安全性投資項目最佳化。

與防護機制整合的偵測

Intel Security 解決方案可利用模擬和信用評價等進階工具，為您提供第一線防禦機制、揪出已知和可能的惡意軟體。但若這些解決方案無法確定某個檔案是否有惡意，它們可以將資料傳送至雲端進行徹底分析。

電腦對決新型的規避性惡意軟體

Cloud Threat Detection 的靜態分析引擎能擷取檔案的詳細資料加以處理。完整的檔案類型涵蓋範圍能就灰色檔案提供重要的背景，進而有效識別有惡意和乾淨的檔案。此外，由於檔案亦會在沙箱環境中執行，因此也會進行行為分析。系統會記錄惡意軟體的一切活動、加以審查，並評估其惡意意圖。檔案是否產生隨機資料夾、將新檔案寫入資料夾並刪除原始檔案？它是否在前往已知網站 (如 Google、Amazon 或 Facebook) 的流量間，偽裝導向至未知或可疑的 URL？這些只是 McAfee Cloud Threat Detection 服務用以分類未知檔案的部分行為例子，這些過程亦會揭露中繼資料、URL、檔案名稱、資料夾位置等資訊，我們會將這些資訊回報給客戶，以便他們調查和瞭解是否有其他電腦遭到入侵。

intel Security

受監督的機器學習

分析週期的每一個步驟都經過 McAfee Labs 管理和調整，進而駕馭電腦、巨量資料及機器學習的強大威力。運用超過 25 年的資料量以及逾 20 億檔案的深入洞見，開發和訓練雲端中巨量資料系統的廣泛分類模型。積極的研究以及持續解譯調查的結果，可持續為機器學習提供資料，讓這些模型隨著惡意軟體技巧與行為的變化和研究的進步一同演進。

著眼於準確度

經驗告訴我們，漏報或誤判往往會帶來重大損害和昂貴的教訓。因此，我們使用的系統包括了檢查和平衡最關鍵的系統檔案和簽署憑證，以確保及時且可靠地判定結果。儘管進階分析能偵測出新型威脅，但我們仍然會交叉參照並關聯惡意軟體產物及其行為和屬性，以將誤判率降至最低。而這是我們結合雲端分析與豐富的防惡意軟體資源後，所帶來的獨特優點之一。

無時不刻作動的偵測功能

每次裁定時，McAfee Cloud Threat Detection 都會通知強制執行原則 (如隔離電腦或啟用防護以攔截類似攻擊) 的來源系統。提供詳細的 IoC 以供進一步調查，以及攻擊後修正和復原時所需的分析資料；而判定結果會在 McAfee Global Threat Intelligence (GTI) 中更新信用評價，以加快對所有使用含 GTI 功能解決方案之組織的防護速度。

反應迅速、價格實惠，適合小型企業

這種雲端型服務，讓您只需要輸入 McAfee 整合產品的加密共用金鑰，即可快速佈建。若您有分散式系統，亦無須將流量回傳至資料中心，直接傳送至雲端即可。我們的專家會負責後續維護事宜，並公開透明地實作更新和升級。以量計價訂閱沒有預付資本支出，因此消弭了入門的成本障礙。

若要深入瞭解，請前往 **www.mcafee.com/tw/products/cloud-threat-detection.aspx**。

McAfee. Part of Intel Security.
台北市 110 基隆路一段
333 號 22 樓 2210 室
886-2-2757-6677
www.intelsecurity.com