GoSecure

惡意程式獵人

ActiveDefense™
搭載數位 DNA®

CounterTack Active Defense™

基於行為檢測及分析惡意程式

主動防禦（Active Defense™）以受到進階持續性威脅端點的深入能見度和快速發現，保全企業安防團隊。

適用於企業安防的 Active Defense

憑藉可分析及檢測記憶體中所執行惡意代碼無與倫比的能力，Active Defense 讓您的團隊能穩健控管各項調查，迅速且簡易地精確找出受到影響的系統，並確定侵害範圍，進而排除這些威脅。

Active Defense 搭載可識別記憶體中所執行各程序特定行為特徵的專利數位 DNA® 技術。數位 DNA 經驗證能幫助安防團隊檢測出基於簽章方法無法發現的零時差、rootkit 惡意程式及瞄準式攻擊等各種新興惡意程式。

一旦識別出威脅，Active Defense 的收集及分析工具讓您能確定最初侵入點、隔離所留存惡意檔案和系統變更，並產生威脅情資以加強端點抵擋未來攻擊。藉由簡化事件反應生命週期，Active Defense 讓您無須高價聘請大批技術高超分析人員，就能將作業快速擴展至數十萬個端點。

針對新興不斷演變威脅的快速自動化事件反應

Active Defense 可為事件反應各階段提供相關能力，其中包括：

監測：針對惡意行為主動掃描實體記憶體中程序。

檢測：使用數位 DNA 行為分析，對讓您能辨認侵害指標及檢測新興惡意程式的特徵進行評分。

分析：只需點選一下就能收集及分析來自實體記憶體和磁碟的重要數位人造物。

反應：藉由在企業範圍內自動化這些操作，檢視聚合狀態並支援大規模一致性事件反應。

憑藉數位 DNA® 簡化惡意程式檢測

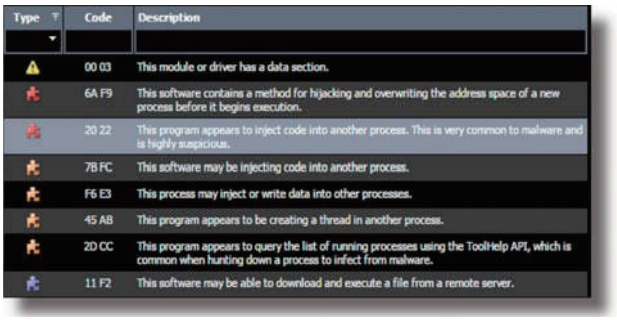
數位 DNA 自動化反向操縱記憶體中所有代碼，並檢查惡意行為。行為係對照來自 CounterTack 惡意程式基因組資料庫的特徵進行匹配，歸類為好、壞或中性，並施加規則和權重以計算各模組整體嚴重性評分，呈現為全面威脅概況的一部分。

Active Defense 為企業作好準備

- 可擴展基礎架構
- 依需求進行掃描
- 簡化代理者部署

可配置式操縱板視圖為使用者提供有關網路涵蓋範圍、數位 DNA（DDNA）評分及掃描歷程紀錄等相關指標總覽視圖。

獨立特徵面板詳細顯示特定行為，並對惡意程式個別部分提供快速觀察見解，重點提示不同威脅群組偏好的手段和技術。



DDNA 可識別間諜木馬程式 Epic Turla rootkit 惡意程式型可疑行為，例如：注入代碼及攔截另一程序位址空間。

CounterTack Active Defense

基於行為檢測及分析惡意程式

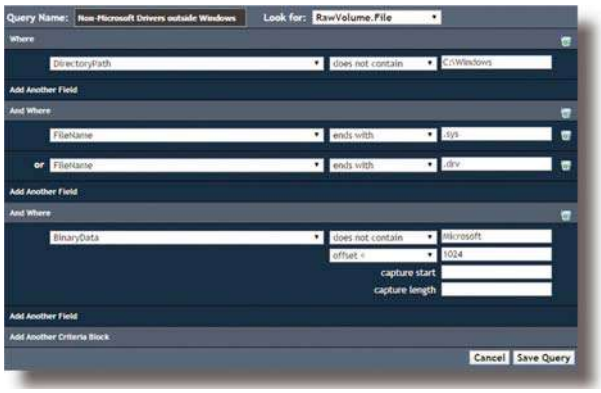
針對已知指標掃測系統

Active Defense 能快速進行掃描，且精心設計使對端點效能的影響降至最低。這些掃描甚至能探測檔案、模組、資源運用及其他系統物件的最低層級屬性，並用於搜尋原始實體記憶體、即時作業系統、磁碟容量等。

以使用者所定義掃描快速掃測企業整個系統，前所未有檢視主機層級威脅。

掃描策略可瞄準實體記憶體、作業系統或所連接驅動機任何層面。

使用者很容易就能建立自身 Active Defense 掃描策略或查詢，掃描指標、與最新威脅或惡意程式行為相關聯的數位人造物，CounterTack 對其稱為全球查詢（Global Queries）的掃描策略庫提供定期更新。總而言之，這些掃描策略讓您能充分運用最新威脅情資，針對有關您的企業組織不斷演變的影響指標進行瞄準式搜尋。



Active Defense 容易使用的掃描建立器圖形使用者介面（GUI），讓您能針對有關企業組織的威脅即時建立查詢。

使用 CounterTack 全球查詢（Global Query）指標或自訂指標和掃描策略，您可充分運用數位 DNA 產生的最新威脅情資，針對您的環境特定指標進行瞄準式搜尋。用於建構掃描策略的查詢係以表達式為基礎且容易使用。

事件分析

使用掃描策略，Active Defense 讓您能收集重要資料而幫助驗證是否已遭遇安防事件。

時間安排：系統活動的時段檢視，其中包括來自事件日誌、網路連線及全球資訊網和預取快取的資料。

容量映射：類似 Windows® Explorer 格式檔案系統的可瀏覽快照，其中包括各檔案屬性和下載連結。

元資料：程序、模組及服務的可搜尋清單，以及類似開啟檔案運用和網路插座的低層級資料。

檔案：匹配特定掃描或來自清單的檔案，以及從記憶體刻出的完整實體記憶體快照和個別模組。

自動化反向操縱及分析實體記憶體，揭露零時差、rootkit 惡意程式及其他隱蔽威脅。

與其他產品整合

- McAfee ePolicy Orchestrator 集中式安全性管理軟體
- Verdasys Digital Guardian 數位資安軟體
- HP ArcSight 企業威脅與風險管理平台（Enterprise Threat and Risk Management Platform）
- IBM Q1 Labs QRadar 整合式資安防禦軟體

Active Defense 安裝需求

Active Defense 伺服器：

- Windows Server 2008 R2 64 位元
- Windows Server 2012 64 位元
- Windows Server 2012 R2 64 位元

支援端點系統

- Windows XP（32 位元 & 64 位元）
- Windows Vista（32 位元 & 64 位元）
- Windows 7（32 位元 & 64 位元）
- Windows 8 & 8.1（32 位元 & 64 位元）
- Windows 10（32 位元 & 64 位元）
- Windows Server 2008（R2）
- Windows Server 2012（R2）

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com