DragonSoft
tw.dragonsoft.com

RAMP

Risk Assessment Management Platform

資安風險評估管理平台

RAMP是結合檢測、掃描及風險評估的一套全方位端點安全管理平台，協助政府與企業強化內部整體防護安全並發掘潛在漏洞風險

D-RAMP | 資安風險評估管理平台

產品概觀

藉由 DVM 找出系統服務潛藏漏洞及分析安全狀況；再透過 GCB 一致性規範資通訊終端設備的安全組態設定（如：密碼長度、更新期限等），降低資安風險；最後經由 EDR 偵測防毒軟體無法偵測的 APT 惡意程式（如隱蔽性木馬及後門等）及分析重要端點設備是否遭駭各入侵、監聽、綁架或成為殭屍電腦，以降低政府單位及企業機密資料外洩的危險。

資安風險評估管理平台是由中華龍網自主研發的一套全方位資安防護系統。結合了全中文弱點掃描軟體(DVM)、政府資安組態稽核軟體(D-GCB) 及端點威脅掃描軟體 (D-EDR)，提供完整檢測、掃描及風險判別的安全管理平台。並符合政府政策及管理規範要求，能協助政府與企業強化組織整體防護安全。

產品特色

1. 符合政策法規及管理規範：
   - 個人資料保護法
   - 資通安全管理法
   - ISO 27001 資訊安全管理系統
   - 國際標準規範 (CVSS/CVE)
   - ISMS 資訊安全管理制度
   - 電子支付機構資訊系統標準及安全控管作業基準辦法
   - 行政院國家資通安全會報技術服務中心資安服務 RFP
   - 軟體資產弱點通知服務系統
2. 強化政府與企業整體資安系統架構與環境防護能力。
3. 提供視覺化圖示報告，快速掌握內部風險評估狀態。
4. 簡潔易懂的介面與檢測流程，協助系統管理者快速上手進行檢測評估與修復。
5. 強化資訊資產管理機制，節省管理時間與成本。

DVM | 全中文弱點掃描軟體

產品概觀

全中文弱點掃描軟體 (DragonSoft Vulnerability Management, DVM) 針對不同環境，進行網路安全弱點評估以「安全漏洞掃瞄(Security Scanner) 與弱點風險管理 (Vulnerability Risk Management) 兩大功能」，協助掌握現行內部存在的安全威脅，集中管理內部主機找出系統服務潛藏漏洞及安全狀況分析診斷，是資安與網管人員不可或缺的管理工具。

DVM 檢測項目包含安全漏洞偵測、弱點稽核檢測、帳號及設置稽核檢測，並支援風險評估以及統計等功能，同時具備資料庫掃描器，支援資料庫的漏洞檢測及安全風險評估。

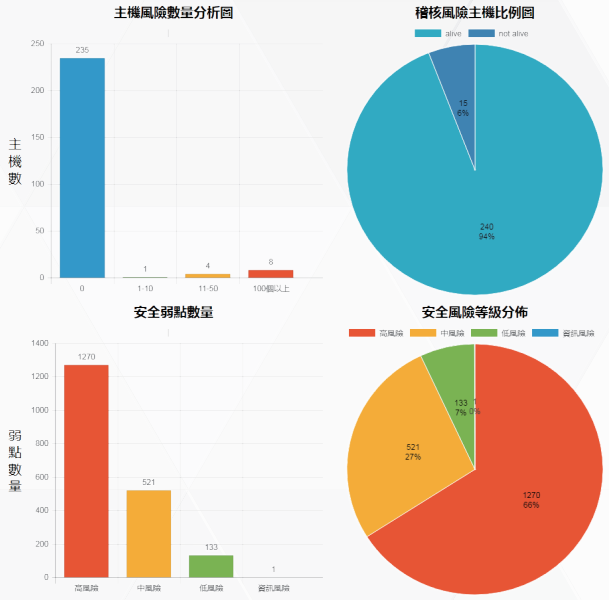
產品特色

1. 符合國際標準規範(CVE)
2. 開放式資料庫系統格式
3. 資產設備管理能力
4. 收集系統服務資訊
5. 非暴力式交叉稽核
6. 弱點修補建議與評估
7. 前、後差異化報表比對

掃描流程

產品效益

- 符合政策法規及管理規範
- 掌握端點設備潛在風險與弱點
- 定期更新弱點資料庫，提供完整且快速的弱點資訊
- 視覺化儀表板與報表整合分析弱點



- 附加軟體資產管理系統 (Dragonsoft Software Asset Management, D-SAM)，能取得端點設備的資產清單，能讓管理者掌握現行的資產清單，亦能針對內部營運狀況做資產汰換，提升效益。

使用者	WIN-3SFQ1D3UHIF	
硬體	Oracle Corporation	
CPU	Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz	
RAM	4096MB	
作業系統	Microsoft Windows Server 2008 R2 Enterprise	
軟體名稱	**廠商**	**版本**
LocalGPO	Microsoft Corporation	3.0.60.0
Microsoft .NET Framework 4.5.1	Microsoft Corporation	4.5.50938
Microsoft Office Access MUI (Chinese (Traditi...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Enterprise 2007	Microsoft Corporation	12.0.4518.1014
Microsoft Office Excel MUI (Chinese (Traditio...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Groove MUI (English) 2007	Microsoft Corporation	12.0.4518.1014
Microsoft Office Groove Setup Metadata MUI...	Microsoft Corporation	12.0.4518.1014
Microsoft Office IME (Chinese (Traditional)) 2...	Microsoft Corporation	12.0.4518.1014
Microsoft Office InfoPath MUI (Chinese (Trad...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Office 64-bit Components 2...	Microsoft Corporation	12.0.4518.1014
Microsoft Office OneNote MUI (Chinese (Tra...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Outlook MUI (Chinese (Tradi...	Microsoft Corporation	12.0.4518.1014
Microsoft Office PowerPoint MUI (Chinese (T...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Proof (Chinese (Traditional))...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Proof (English) 2007	Microsoft Corporation	12.0.4518.1014
Microsoft Office Proofing (Chinese (Tradition...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Publisher MUI (Chinese (Tra...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Shared 64-bit MUI (Chinese ...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Shared 64-bit MUI (English) ...	Microsoft Corporation	12.0.4518.1014
Microsoft Office Shared MUI (Chinese (Tradit...	Microsoft Corporation	12.0.4518.1014

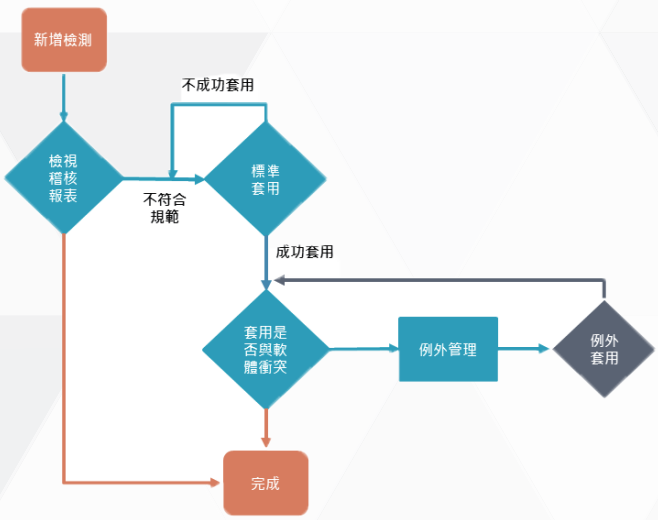
D-GCB | 政府資安組態稽核軟體

產品概觀

美國政府組態基準設定 (US GCB) 是由美國國家標準與技術研究所 (NIST) 針對駭客入侵相關數據所提出的有效安全建議值。US GCB主旨在於規範 IT 配置基準，加強系統強化程序，且改善及維護電腦安全的有效配置設定。TW GCB 則是參考美國政府配置基準，針對台灣電腦系統環境所規範出的設定值。

D-GCB 能針對政府機關單位的資通訊軟體進行檢測，測試端點設備是否符合 TW GCB 組態設定值，進而降低內部電腦遭受攻擊的風險，避免資安疑慮。

GCB稽核導入流程圖

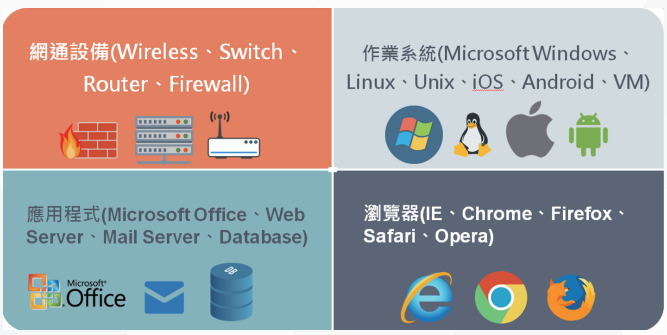


產品效益

- 軟體自動化稽核、套用，提供完整組態歷程。
- 免安裝程式 (Agentless)，透過遠端方式掃描。
- 因應例外事件，使用者可自訂例外組態管理。
- 可視化儀表板與圖示報表評估組態狀態。
- 完整組態備份與還原，有助於回溯套用組態。

稽核項目

1. 帳戶安全性 (Account Policy)：
   對於密碼原則、帳戶鎖定原則等組態進行檢測。
2. 個人電腦系統 (Computer Settings)：
   針對安全性選項、使用者權限指派、網際網路通訊設定、自動播放等組態進行檢測。
3. 防火牆設定 (Firewall Settings)：
   Windows 防火牆公用設定檔、私人設定檔、網域設定檔等組態進行檢測。
4. 使用者設定 (User Settings) ：
   使用者螢幕保護裝置、網際網路通訊、網路共用、附件管理員等組態進行檢測。
5. IE 瀏覽器 (Internet Explorer)：
   Internet Explorer 內部網路區域、信任的網站區域等區域進行 JAVA 權限、登入選項、Active X 控制項等設定檔等組態進行檢測。
6. Chrome 瀏覽器 (Google Chrome)：
   對於 Google Chrome 內容設定、HTTP 驗證政策、密碼管理員、設定遠端存取選項、擴充功能等組態進行檢測。



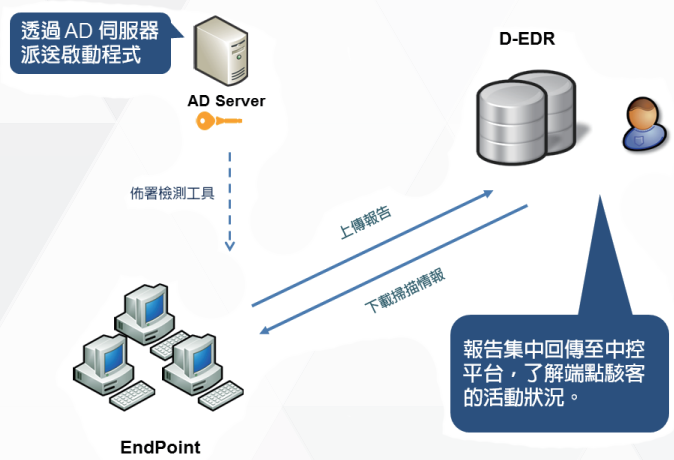
D-EDR | 端點威脅掃描軟體

產品概觀

近年來進階持續性威脅 (Advanced Persistent Threat, APT) 崛起，其以複雜精密的技術監控並竊取特定目標的重要資料，具備強大的攻擊性與隱蔽性，導致資安問題日益嚴重，防毒軟體更是防護不了。端點威脅掃描軟體 (End-point Detection Response, EDR) 透過遠端佈署，在不依賴病毒碼之下，偵測 APT 惡意程式，找出可能遭受攻擊的來源，協助管理者有效且快速地掌握 APT 惡意程式與駭客行為蹤跡。

檢測流程

1. 客製化派送各端點佈署掃描,透過單位內派送系統，派送至各端點檢測掃描
2. 將端點回傳之檢測檔與雲端大數據資料庫進行比對，端點採集各系統資訊，併於本機端直接分析併產出鑑識報告
3. 將檢測結果上傳於 EDR 資料，端點鑑識報告統一回傳集中至雲端平台



產品效益

- 偵測找出潛伏端點內的 APT 惡意程式。
- 掃描完成後即產出相關情資報表，提供給管理者處理。
- 彈性化佈署派送，可搭配單位內使用的派送系統派送。

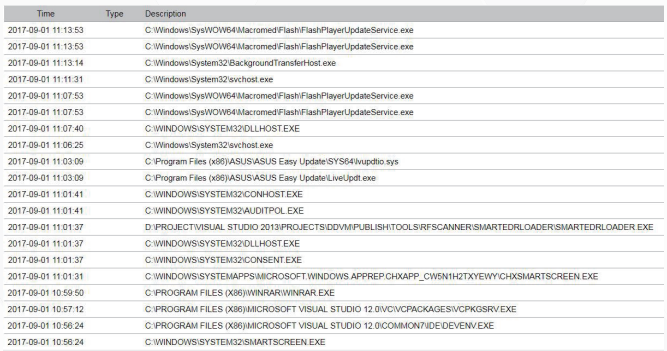
功能特色

一、獨家記憶體分析：

透過獨家分析引擎，找出防毒軟體無法偵測的潛在惡意程式，提供完整的資訊。

二、駭客活動記錄重播及分析：

透過偵測找出可疑檔案，進而分析電腦的使用者記錄，包含瀏覽過的網頁、執行過的程式、開啟過的檔案，並回溯分析產生關聯分析報表。



三、免安裝程式 (Agentless)：

透過遠端佈署掃描，免安裝形式的檢測模型，以客製化方式派送，因應各單位特性採用不同彈性配置，快速部署掃描。

DVM

專門為政府及企業在網路安全弱點實施及網路安全漏洞管理方面所開發的最佳解決方案。

GCB

目的在於規範資通訊終端設備的一致性安全設定，降低成為駭客入侵管道，進而引發資安事件之疑慮。

EDR

防護重要端點設備不受惡意程式入侵，防止遭到駭客入侵、監聽、綁架或成為殭屍電腦，降低政府單位及企業機密資料外洩的危險。

SAM

提供政府及企業對於軟體資產管理及最佳化的做法，確保各項軟體投資，及有效使用軟體資產。

CPS

資訊安全客製化專案/產品開發服務

ISS

提供各項資訊安全檢測服務

中華龍網股份有限公司
台北市中山區朱崙街 89 號 5 樓
5F., No.89, Zhulun St., Zhongshan Dist., Taipei City 104, Taiwan (R.O.C.)
Tel : +886-2711-6661 ;Fax : +886-2711-9997 ;http://tw.dragonsoft.com/