中華龍網

EDR+GCB+DVM–新世代全方位端點安全管理平台

D-RAMP

Dragonsoft Risk Assessment Management Platform

全方位端點安全管理的解決方案

DragonSoft
www.dragonsoft.com

Agenda

1-公司簡介

2-為何需要風險評估管理？

3-功能特色

4-效益

5-我們的客戶

1-公司簡介

中華龍網(DragonSoft)成立於2003年

核心技術：

資訊安全相關軟體平台

致力於：

提供政府/企業完整資安防護需求之產品及服務

發展歷史

2003 中華龍網成立

2004 DVM發表
DVM榮獲CVE認證

2005 榮獲 金峰獎、金炬獎、金像獎、創新研究獎等獎項
DVM5發表

2006 弱點知識庫榮獲CVE認證

2007 參加國際展覽
德國SYSTEMS
新加坡 Communic Asia

2008 榮獲資策會
IT Best Choice 2007
票選第一名

2009 DragonWAF發表

2010 擔任數位時代
數位服務大調查評審

2011 DWP發表
DVM榮獲
全球資訊安全雜誌
SC Magazine五顆星評比

2012 DAS發表

2013 A-PacketMan發表
D-SAM發表

2014 DVM6發表

2016 DVM7.0發表

2017 RAMP發表

預計年底：
IoT、DDOS

2-為何需要風險評估管理？

病毒的演化

1980 年代
第一支電腦病毒問世

單純的病毒感染
(木馬、蠕蟲病毒)

利用弱點散播病毒
(疾風病毒)

間諜軟體及**USB 病毒**

Bot
(殭屍病毒)

APT目標式攻擊

勒索加密病毒

感染方式

早期的磁碟片

隨身碟

網路

系統或網頁程式的漏洞

因應之道

企業經常會詢問：環境內已經有了防火牆、IPS、Mail Spam 等資安設備，為何還是會被駭客入侵系統被植入惡意檔案？

資安攻防的勝敗關鍵

「弱點」的管理

如果系統弱點都已修正補強是否就不會遭受到駭客的攻擊？

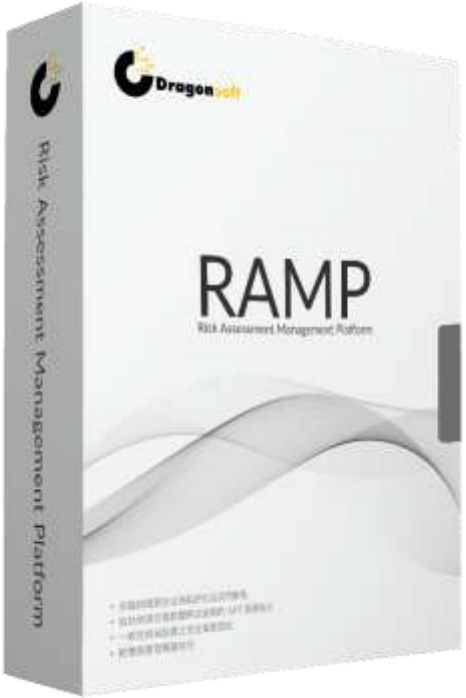
答案是否定的。因為駭客還是可以用其他管道來入侵系統，就像人的身體三餐飲食正常，天天運動睡眠充足，就不會生病了嗎？

為何還要定期做健康檢查？

為的是發現潛在未知風險，同樣的道理，資安健檢的目的是為檢查企業內部是否已遭受到駭客攻擊或是發掘潛在未知風險。

發覺資安死角，為企業資安把脈

企業因應各種攻擊手法的威脅，如何找出自身的資安弱點並進一步強化？



透過中華龍網**自行開發**的 **RAMP** **為企業把脈**

找出潛在或已知的資安風險進而加強防護

風險評估管理平台(RAMP)

DVM
全中文
弱點掃描軟體

找出系統服務潛藏漏洞
及分析安全狀況

+

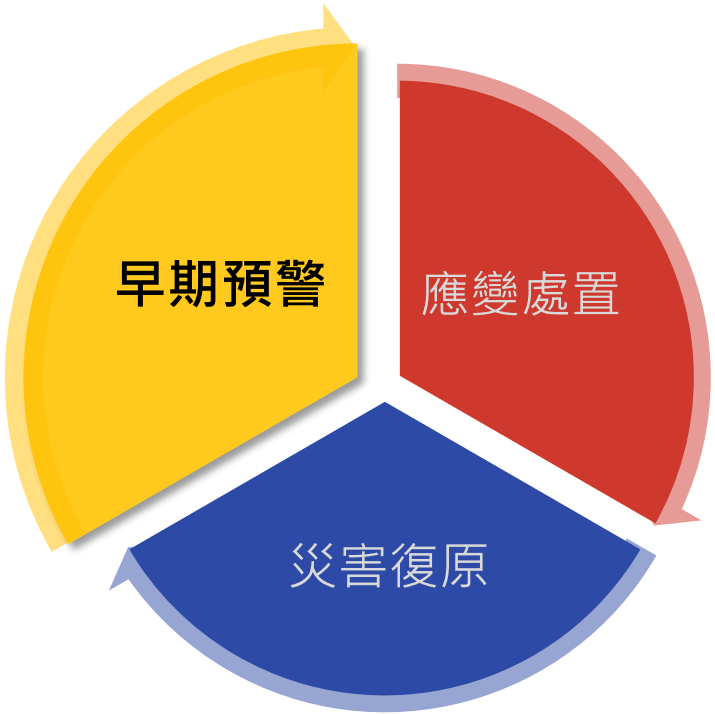
D-GCB
政府資安組
態稽核軟體

一致性規範資通訊終端
設備的安全組態設定

+

D-EDR
端點威脅
掃描軟體

偵測APT惡意程式
（如隱蔽性木馬及後門等）



- 如何掌控內部**軟硬體清單**?
- 如何了解設備環境內**現有的弱點**?
- 檢視目前**資安政策**是否到位?
- 內部web應用程式是否安全?
- 內部**潛在風險**?
- 如果被惡意利用會有什麼影響?
- 什麼時候需要補丁?
- 如果沒有補丁該如何防護?

3-功能特色

資安風險評估管理平台

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)。

弱點追蹤
管理系統

主機與網路安全弱點評估及漏洞管理軟體，檢測已知漏洞。

D-SAM
軟體資產
管理

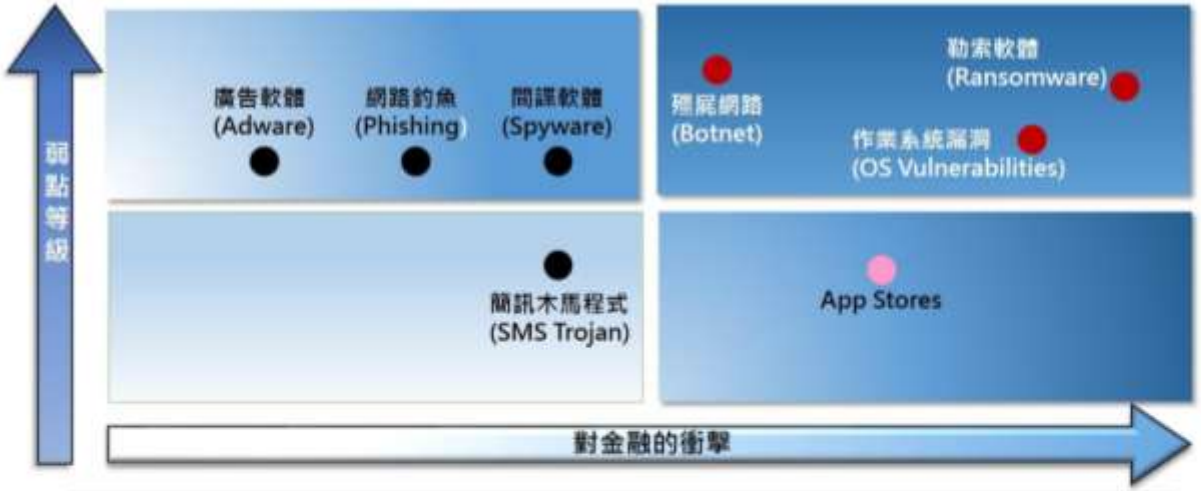
對終端設備導入合規的安全組態設定。

3.1-DVM全中文弱點掃描軟體

DragonSoft Vulnerability Management
找出系統服務潛藏漏洞及安全狀況分析診斷。

DragonSoft
www.dragonsoft.com

網路犯罪的威脅預測



- Juniper Research預估，至2022年，企業每年的網路安全產品開銷將近1350億美元，估計預測期內的複合年均成長率(CAGR)為7.5%。
- 上述預估開銷包含所有網路安全、專用硬體與軟體的採購，以及資訊安全代管服務供應商(Managed Security Services Provider, MSSP)的服務收益，但是並不包括組織內部網路安全人員的薪資。
- 由於人工智慧安全防護相關合約的簽訂，以及物聯網端點覆蓋範圍的擴張，兩者皆需要更高額的支出，因此大企業的網路安全開銷將顯著成長。然而，在企業文化的改革方面，許多組織即使投入大量資金，發展速度依然緩慢。

資料來源：Juniper Research/科技發展觀測平台整理

2017/5/18

執行 / 修補 / 控制 / 持續改善


依據環境評估需要進行檢測之主機
以系統內訂或自訂政策進行掃描
產生報告
發現系統服務風險
進行修補程式測試及修補作業
提升資安防護

弱點掃描相關政策法規1/2

- **ISO-27001 資訊安全管理系統**：定期稽核-每年至少實施**一次**內部資訊安全管理制度稽核作業
- 行政院國家資通安全會報技術服務中心資安服務RFP ：
  ①「**資安健診服務**」
  ②「**資安監控服務**」
  ③「**弱點掃描服務**」
  ④「滲透測試服務」
  ⑤「社交工程郵件測試服務」

弱點掃描相關符合政策法規2/2

政府機關（構）資通安全責任等級分級作業規定

機關屬性 / 等級	資安責任等級區分	管理面	技術面 安全性檢測
A	1. 總統府、國安會、立法院、司法院、考試院、監察院、行政院及直轄市政府。 2. 立法院、司法院、考試院、監察院及行政院等所屬二級機關、相當二級機關之獨立機關。但其業務或組織單純者，得報經其上級機關核准，調整為B級或C級。 3. 凡涉及外交、國防、國土安全，及掌理全國財政、經濟、警政等重要業務之機關，如外交部領事事務局、內政部警政署刑事警察局等。 4. 負責能源、水資源、通訊傳播、交通、金融、緊急救援、高科技園區等關鍵資訊基礎設施之營運機關，如交通部民用航空局飛航服務總臺、臺北市 自來水事業處等。 5. 保有全國性個人資料檔案之機關，如勞動部勞工保險局、衛生福利部中央健康保險署等。	每年至少 **2次**內稽	每年至少辦理**1**次 資安健診
B	1.縣（市）政府。 2. 凡涉及社會秩序及人民財產業務之機關，如地方政府警察局、地方政府地政事務所等。 3. 保有區域性或地區性個人資料檔案之機關，如財政部各區國稅局、地方政府戶政事務所等。	每年至少 **1次**內稽	每**2年**至少辦理**1次** 資安健診
C	其他政府機關及地方政府民意機關。	依各主管 機關規定	依各主管機關規定

WannaCry 勒索病毒肆虐

- WannaCry(WanaCrypt0r 2.0)勒索病毒大規模攻擊所使用的 Windows **Server Message Block（SMB)** 伺服器漏洞 EternalBlue。
- 亦被稱為**CVE-2017-0144**和MS17-10。
- 使用**DVM全中文弱點掃描軟體**定期稽核掃描漏洞，利用修補建議更新系統，可避免勒索軟體的威脅。

DVM報表檢視-CVE-2017-0144

ID： 9608	MS17-010 Microsoft Windows SMB 伺服器的安全性更新 (4013389) (CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146, CVE-2017-0147,CVE-2017-0148)：139	風險等級：高風險
弱點描述	此安全性更新可解決 Microsoft Windows 中的弱點。如果攻擊者傳送蓄意製作的訊息到 Windows SMBv1 伺服器，最嚴重的弱點可能會允許遠端執行程式碼。	
修補建議	大部分客戶都已啟用自動更新，並且不必須採取任何行動，資訊安全更新將自動下載和安裝。沒有啟用自動更新的客戶則必須檢查更新，並手動安裝更新。	
攻擊需求	Remote	
造成危害	N/A	
弱點編號	CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-20	
相關連結	http://twvdb.dragonsoft.com/detail.php?id=9608	

全球勒索病毒攻勢再起
Petya 變種更勝 WannaCry

- 新型勒索軟體 Petya ，2017/6/27開始全球爆發。
- 這次 Petya 不只用了 SMBv1 漏洞 (**CVE-2017-0144**)，更結合 Windows 網路安裝弱點（**CVE-2017-0199**）攻擊。
- 使用**DVM全中文弱點掃描軟體**定期稽核掃描漏洞，利用修補建議更新系統，可避免勒索軟體的威脅。

「Petya」勒索訊息畫面（Sourece：趨勢科技）

DVM報表檢視-CVE-2017-0199

ID： 9606	Microsoft Office 與 WordPad 任意代碼執行漏洞 (CVE-2017-0199)	風險等級：高風險
弱點描述	多款Microsoft產品中存在遠程代碼執行漏洞。遠程攻擊者可藉助特製的文本文件利用該漏洞執行任意代碼。以下產品和版本受到影響：Microsoft Office 2007 SP3；Microsoft Office 2010 SP2；Microsoft Office 2013 SP1；Microsoft Office 2016；Microsoft Windows Vista SP2；Windows Server 2008 SP2；Windows 7 SP1；Windows 8.1。	
修補建議	大部分客戶都已啟用自動更新，並且不必須採取任何行動，資訊安全更新將自動下載和安裝。沒有啟用自動更新的客戶則必須檢查更新，並手動安裝更新。	
攻擊需求	Remote	
造成危害	Gain Access	
弱點編號	CVE-2017-0199	
相關連結	http://twvdb.dragonsoft.com/detail.php?id=9606	

3.2-政府資安組態稽核軟體

Government Configuration Baseline

規範資通訊終端設備(如個人電腦等)的一致性安全組態設定(如：密碼長度、更新期限等)，符合行政院國家資通安全會報技術服務中心GCB規範。

DragonSoft
www.dragonsoft.com

GCB由來

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。

政府組態基準設定(TW GCB)參考美國政府配置基準(US GCB)，針對台灣電腦系統環境所規範出的設定值。TW GCB規範資通訊終端設備的一致性安全組態設定，TW GCB規範能定期稽核及管理，且能有效降低內部電腦遭受攻擊的風險，避免資安疑慮。

CIS Controls

Secure Your Organization

First 5 CIS Controls
Eliminate the vast majority of your organisation's vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control
16: Account Monitoring and Control
17: Security Skills Assessment and Appropriate Training to Fill Gaps
18: Application Software Security
19: Incident Response and Management
20: Penetration Tests and Red Team Exercises

正確組態設定的重要性

美國網路安全協會(SANS)於**2016年公布**CIS Controls for Effective Cyber Defense (Version 6.1)

項次	Security Controls	相關資安弱點
1	Inventory of Authorized and Unauthorized Devices	•裝置未即時進行安全性更新 •裝置使用不當預設組態設定 •BYOD (Bring Your Own Device)
2	Inventory of Authorized and Unauthorized Software	•未即時進行軟體更新 •執行惡意軟體 •侵犯智財權
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	•不當的預設組態設定 •預設帳號與弱密碼 •預設啟用非必要服務
4	Continuous Vulnerability Assessment and Remediation	•未定期執行弱點掃描 •未即時進行弱點修補
5	Controlled Use Administrative Privileges	•使用預設管理員帳戶 •使用具備管理員權限之帳戶 •使用同一組密碼管理多台伺服器主機

防護案例

情境

使用者不小心將含有惡意程式的隨身碟插入公務電腦中

防護

a. 由於組態設定禁止可攜式媒體的自動播放功能，降低感染機率

b. 組態設定強制Windows之安全性更新保持在最新的狀態，因此可大幅減少惡意程式所能利用的漏洞

c. 萬一不幸網域內其他電腦遭受惡意程式感染，組態設定禁止電腦回應廣播的封包，可避免惡意程式的感染範圍擴大

TW GCB項目類型

網通設備(Wireless、Switch、Router、Firewall)

作業系統(Microsoft Windows、Linux、Unix、iOS、Android、VM)

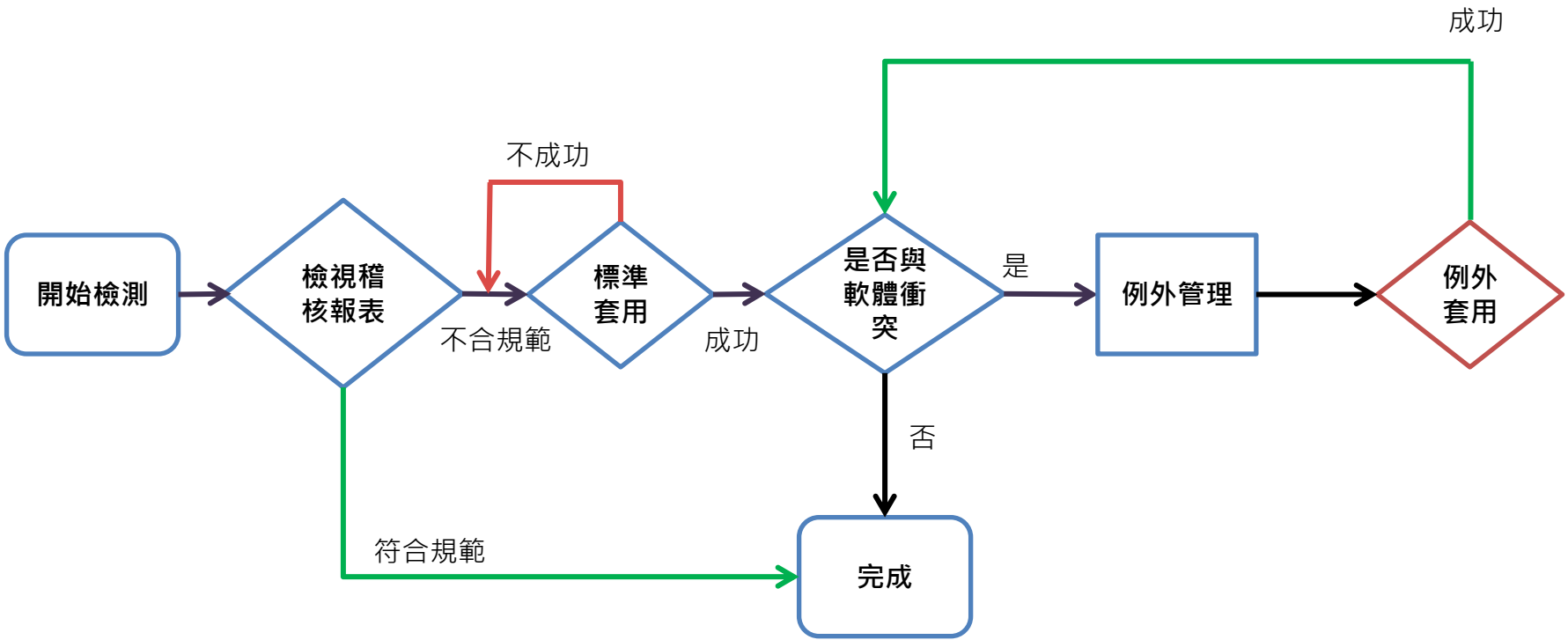
應用程式(Microsoft Office、Web Server、Mail Server、Database)

瀏覽器(IE、Chrome、Firefox、Safari、Opera)

TW GCB發展規劃

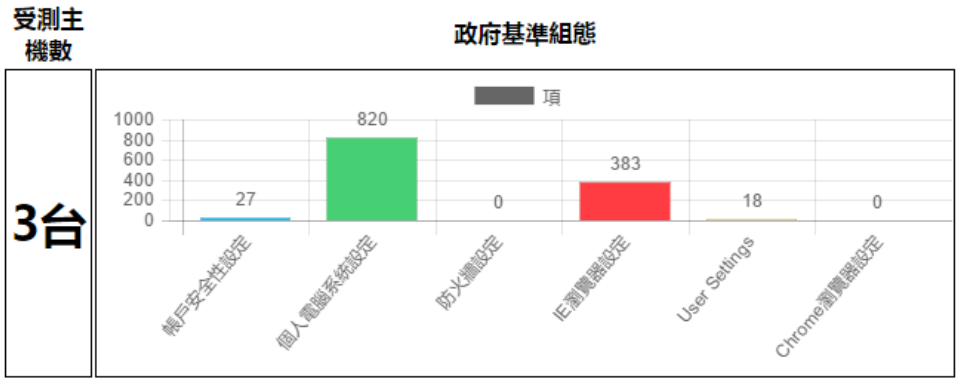
類型	102年	103年	104年	105年	106年	107年
作業系統	Win7 (281項)	Win Server 2008 R2 (332項) RHEL5 (190項)	Win8.1 (340項)		Win10	Win Server 2012/2016
瀏覽器	IE8 (115項)		IE11 (154項)	Chrome (30項)	Firefox	Edge
網通設備			Wireless (19項)	Juniper Firewall (49項)	Cisco Switch	
應用程式				Exchange Server 2013 (49項)	Outlook 2013	Apache

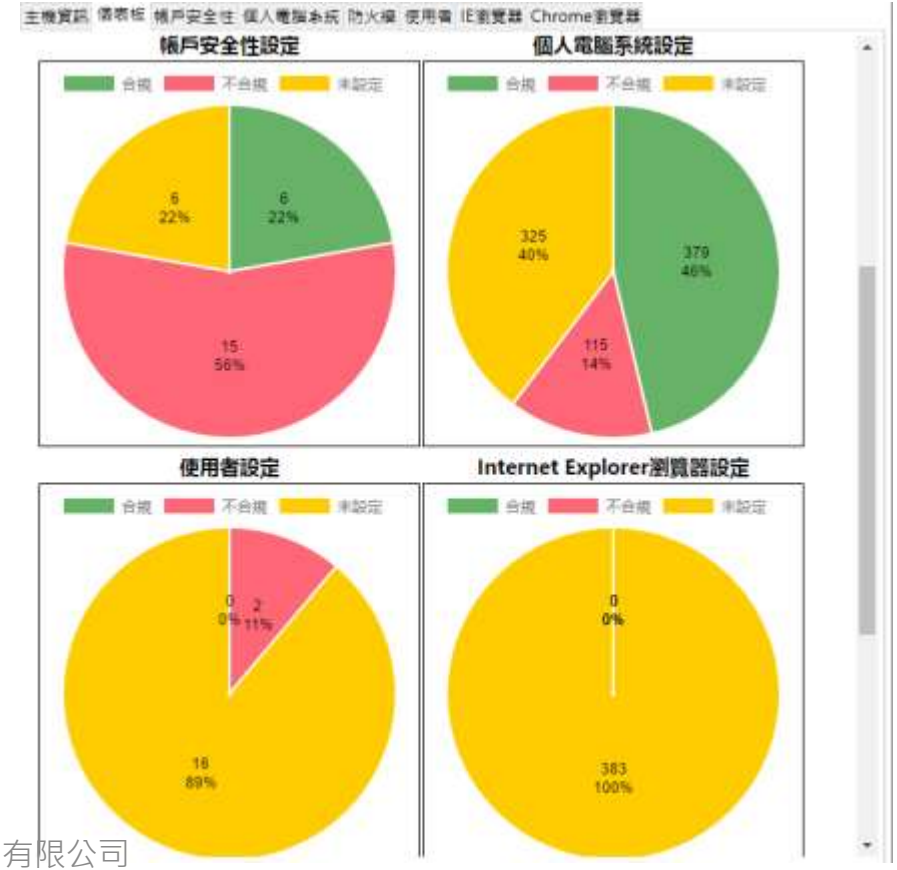
GCB稽核導入流程圖



GCB儀表板檢視

- 可視化儀表板，了解端點設備內目前組態設定狀況。

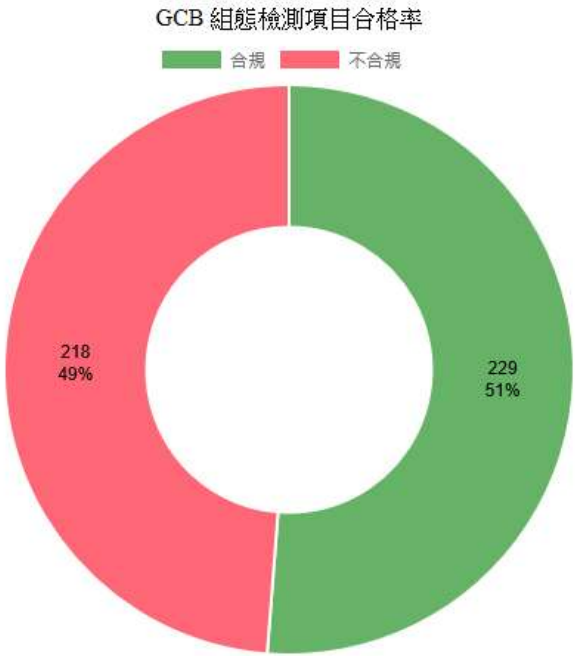




GCB報表檢視

檢測摘要

項目	群組	合格	不合格	總計
1	Account Policy	9	0	9
2	Computer Settings	220	82	302
3	Firewall Settings	0	21	21
4	Internet Explorer	0	115	115



Account Policy

CCE-10760-7	密碼最短使用期限	PASS
CCE-10562-7	密碼最長使用期限	PASS
CCE-10372-1	最小密碼長度	PASS
CCE-10901-7	密碼必須符合複雜性需求	PASS

Computer Settings

CCE-10845-6	以服務方式登入	FALL
CCE-10548-6	增加處理程序工作組	FALL
CCE-10750-8	拒絕本機登入	FALL
CCE-10596-5	拒絕以批次工作登入	FALL

使用D-GCB的效益

- GCB自動化管理工具程式，導入合規組態，減少人工導入的時間。
- 輕量化的掃描方式(Agentless)。
- 因應環境變動及需求改變，可隨時進行GCB修改套用，提升管理效率。
- 有效降低電腦遭受惡意行為攻擊和感染的機率，避免受害主機範圍擴大。

3.3-端點威脅掃描軟體

Endpoint Detection Response

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。

DragonSoft
www.dragonsoft.com

EDR

- 進階持續性威脅（Advanced Persistent Threat，APT）的外部威脅型態興起，具備強烈的攻擊性且隱蔽性高，對於傳統防毒軟體以發揮不了防護作用，導致資安事件日益嚴重。
- 市場研究機構Gartner在2013年首度提出有別於傳統防毒軟體的產品，在防禦與偵測兩端達到平衡，命名為**端點偵測與回應(Endpoint Detection and Response，EDR)**。

功能優勢

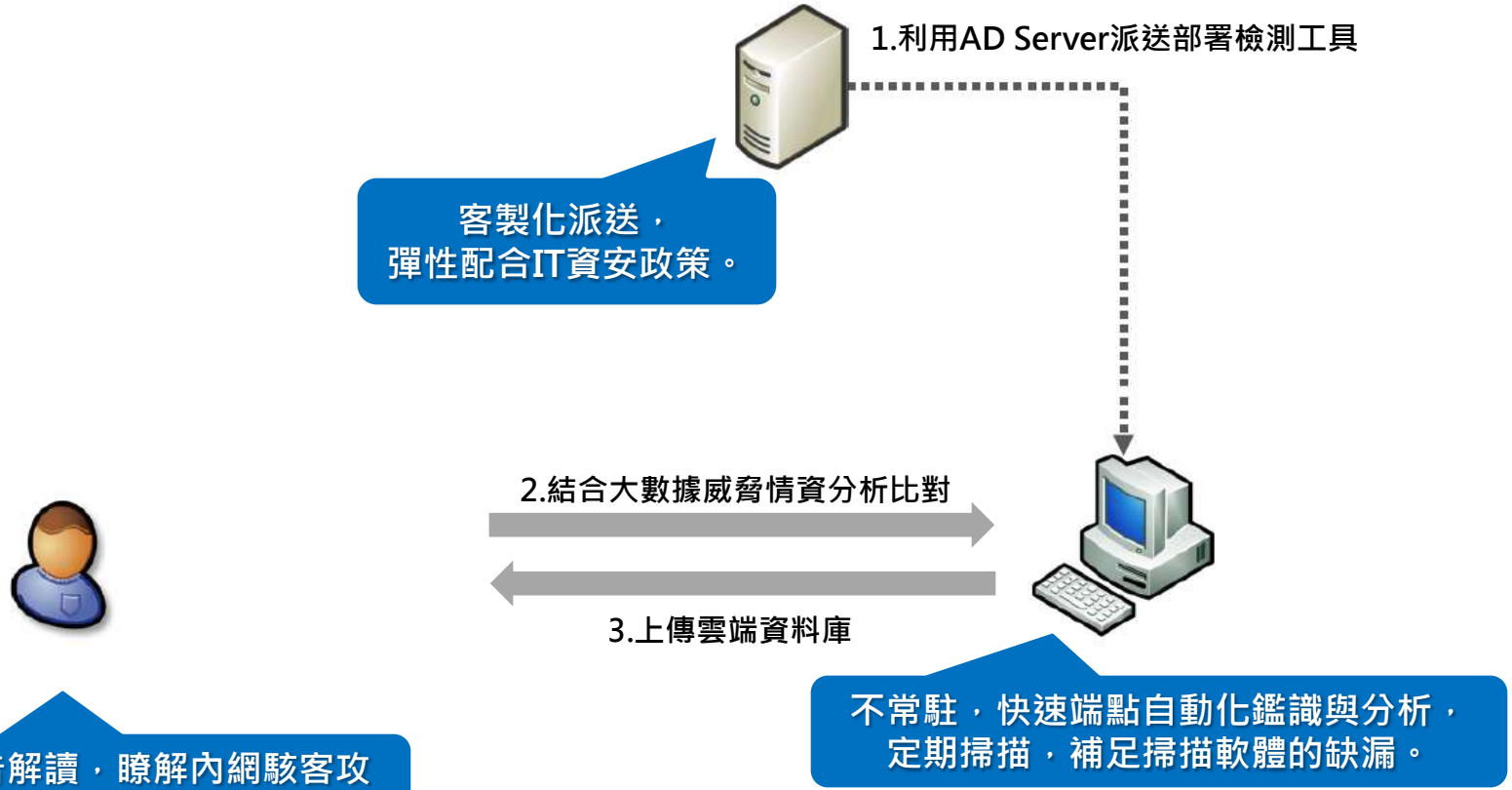
01 大數據威脅情資分析比對

02 回溯駭客活動行為鑑識與分析

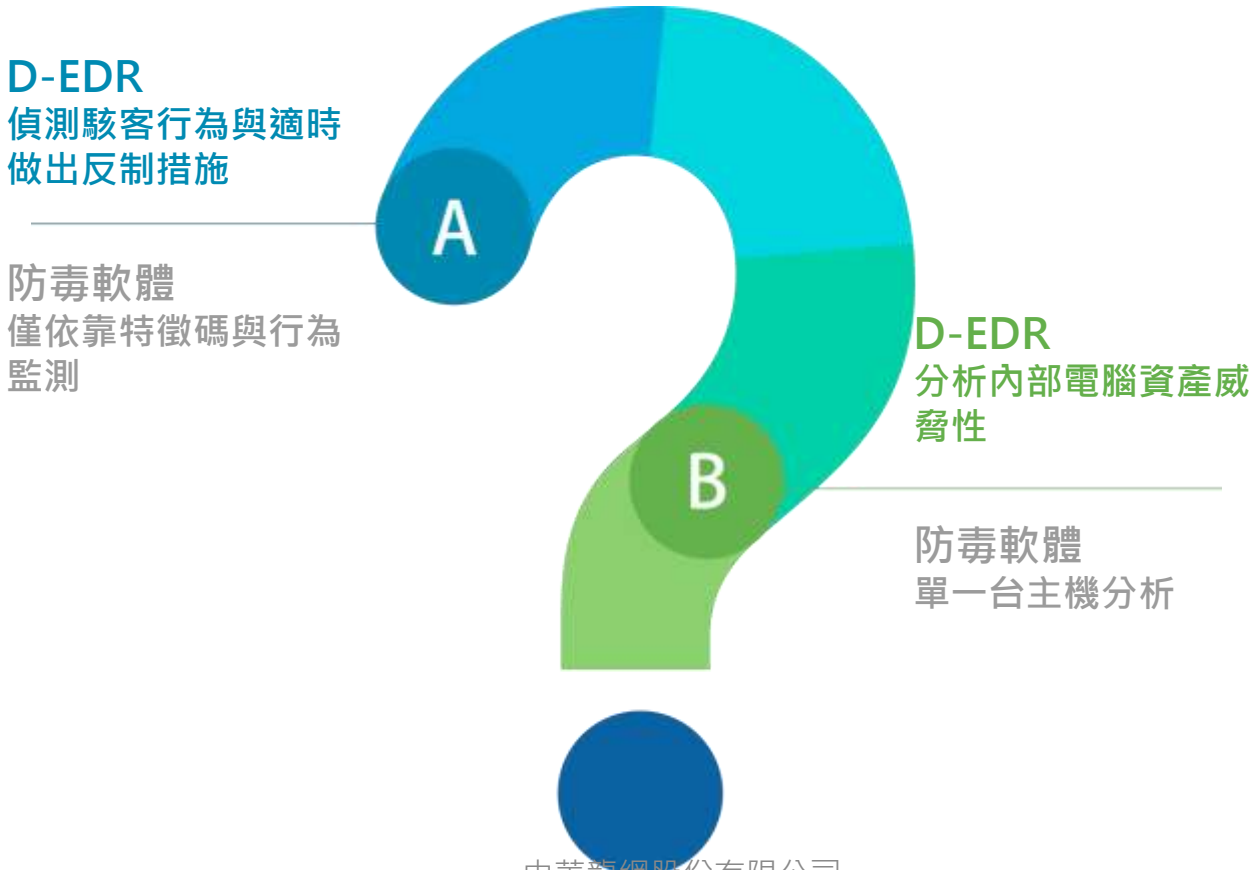
03 提供個人資產威脅報表

04 輕量化遠端佈署掃描

EDR 佈署檢測示意圖


1.利用AD Server派送部署檢測工具
客製化派送，
彈性配合IT資安政策。
2.結合大數據威脅情資分析比對
3.上傳雲端資料庫
不常駐，快速端點自動化鑑識與分析，
定期掃描，補足掃描軟體的缺漏。
報告解讀，瞭解內網駭客攻
擊與端點惡意程式活動情資。

D-EDR與防毒軟體的差異與互補性



3.4-D-SAM軟體資產管理

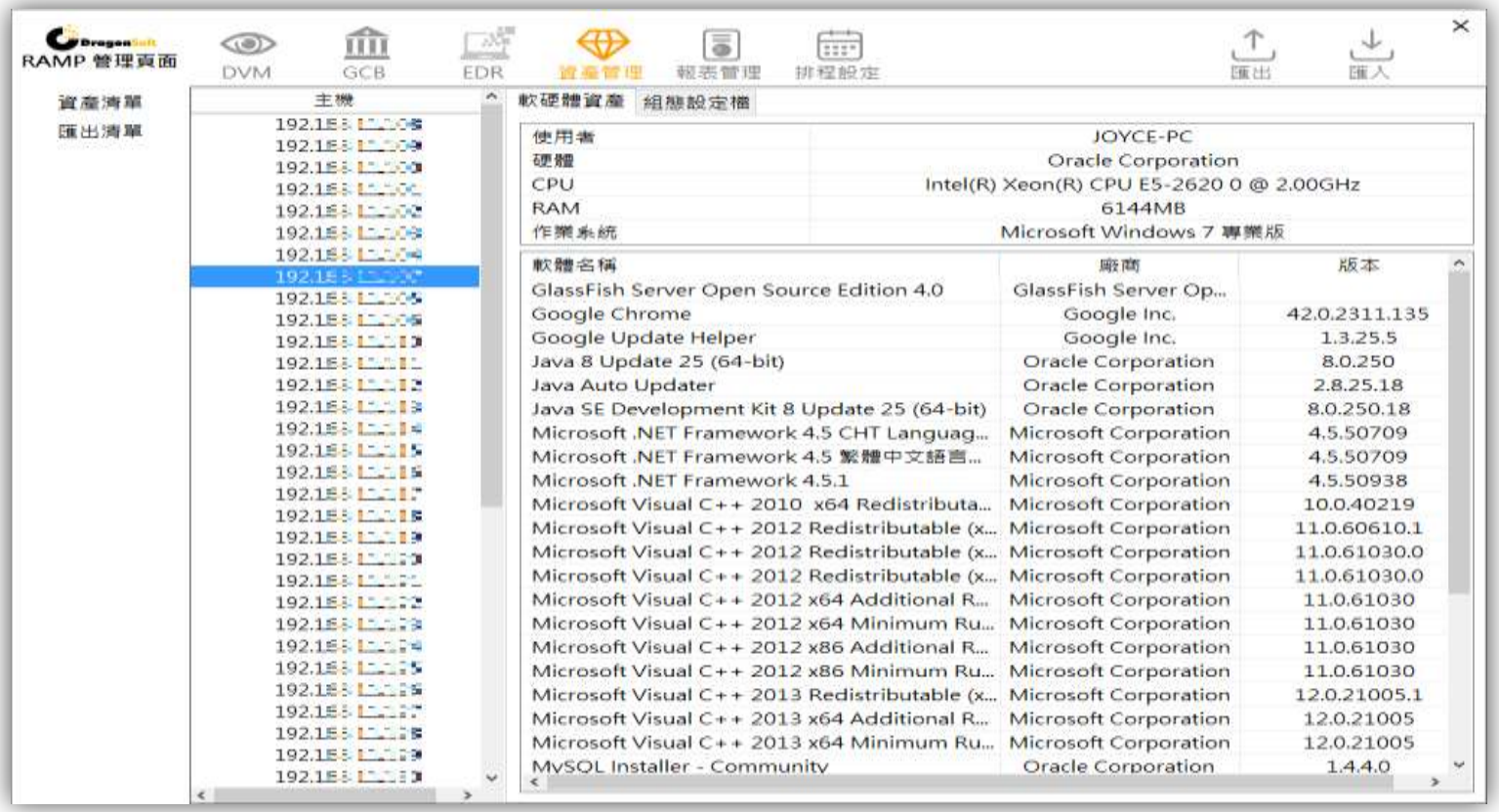
Dragonsoft Software Asset Management

- 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。
- 蒐集政府機關使用之軟體資訊，以強化國家軟體資產安全管理。

D-SAM符合政府政策規劃

- 105.11.18-行政院國家資通安全會報「國家資通訊安全發展方案」行動方案「3.4.1.建置國家軟體資產控管機制」，將推動軟體資產弱點通知服務系統。
- 使用D-SAM蒐集資訊系統軟體資產資料(廠商產品，軟體名稱、版本、版次)將可匯入軟體資產弱點通知服務系統。

資產管理清單


RAMP 管理頁面
DVM
GCB
EDR
資產管理
報表管理
排程設定
匯出
匯入
資產清單
匯出清單
主機
軟硬體資產
組態設定檔
使用者 JOYCE-PC
硬體 Oracle Corporation
CPU Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz
RAM 6144MB
作業系統 Microsoft Windows 7 專業版
軟體名稱 廠商 版本
GlassFish Server Open Source Edition 4.0 GlassFish Server Op...
Google Chrome Google Inc. 42.0.2311.135
Google Update Helper Google Inc. 1.3.25.5
Java 8 Update 25 (64-bit) Oracle Corporation 8.0.250
Java Auto Updater Oracle Corporation 2.8.25.18
Java SE Development Kit 8 Update 25 (64-bit) Oracle Corporation 8.0.250.18
Microsoft .NET Framework 4.5 CHT Languag... Microsoft Corporation 4.5.50709
Microsoft .NET Framework 4.5 繁體中文語言... Microsoft Corporation 4.5.50709
Microsoft .NET Framework 4.5.1 Microsoft Corporation 4.5.50938
Microsoft Visual C++ 2010 x64 Redistributa... Microsoft Corporation 10.0.40219
Microsoft Visual C++ 2012 Redistributable (x... Microsoft Corporation 11.0.60610.1
Microsoft Visual C++ 2012 Redistributable (x... Microsoft Corporation 11.0.61030.0
Microsoft Visual C++ 2012 Redistributable (x... Microsoft Corporation 11.0.61030.0
Microsoft Visual C++ 2012 x64 Additional R... Microsoft Corporation 11.0.61030
Microsoft Visual C++ 2012 x64 Minimum Ru... Microsoft Corporation 11.0.61030
Microsoft Visual C++ 2012 x86 Additional R... Microsoft Corporation 11.0.61030
Microsoft Visual C++ 2012 x86 Minimum Ru... Microsoft Corporation 11.0.61030
Microsoft Visual C++ 2013 Redistributable (x... Microsoft Corporation 12.0.21005.1
Microsoft Visual C++ 2013 x64 Additional R... Microsoft Corporation 12.0.21005
Microsoft Visual C++ 2013 x64 Minimum Ru... Microsoft Corporation 12.0.21005
MySQL Installer - Community Oracle Corporation 1.4.4.0

使用D-SAM的效益

- 控制成本和商務風險，以達到更健全的財務狀態。
- 最佳化現有投資，讓您運用既有的資產發揮更高的成效。
- 透過更高的彈性及靈活度，隨著公司規模及成熟度的擴充需求而成長。

全方位端點安全管理的解決軟體

RAMP

風險管理評估平台

EDR	DVM	GCB
找出隱蔽性木馬的蹤跡	管理現行資產已知弱點	增加駭客入侵困難度

有效偵測出家中較不容易察覺的風險，有效的降低家中設備受損的程度。

針對家中門窗、電器設定做標準檢測，是否符合安全性，降低遭受入侵及受害...等問題。

針對房子外表大範圍檢測與分析，提供屋主有效且完善的修補解決方案。

4-資安風險評估管理平台的效益

1.符合政府政策及相關法令規範要求：

- 個人資料保護法
- 資通安全管理法
- 政府資安責任分級
- 軟體資產弱點通知服務系統

2.強化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，提高資安管理效能。

4.提升政府、企業人員資安意識與觀念。

5.定期進行資安風險評估，幫助企業評估全面性的威脅風險。

5-我們的客戶


政府機關
金融
學校單位
交通
通訊傳播
能源
醫療
其他產業
DragonSoft
www.dragonsoft.com

中華龍網D-GCB政府資安組態稽核
106年30項組態稽核清單

安全性選項	1 帳戶：Administrator帳戶狀態	密碼原則	16 強制執行密碼歷程記錄
	2 帳戶：重新命名系統管理員帳戶		17 使用可還原的加密來存放密碼
	3 帳戶：Guest帳戶狀態		18 密碼必須符合複雜性需求
	4 帳戶：重新命名來賓帳戶名稱	螢幕保護	19 啟用螢幕保護裝置
	5 網路存取：允許匿名SID/名稱轉譯		20 螢幕保護裝置逾時
	6 網路存取：不允許SAM帳戶和共用的匿名列舉		21 以密碼保護螢幕保護裝置
	7 Microsoft網路用戶端：傳送未加密的密碼到其他廠商的SMB伺服器		22 記錄檔大小上限(KB)(安全性)
			23 記錄檔大小上限(KB)(安裝)
	8 關閉自動播放		24 記錄檔大小上限(KB)(系統)
	9 AutoRun的預設行為		
帳戶原則	10 重設帳戶鎖定計數器的時間	互動式登入	25 互動式登入：在密碼到期前提示使用者變更密碼
	11 帳戶鎖定期間		26 互動式登入：不要求按CTRL+ALT+DEL鍵
	12 帳戶鎖定閾值		27 互動式登入：不要求按CTRL+ALT+DEL鍵
密碼原則	13 最小密碼長度	附件管理員	28 開啟附件時通知防毒程式
	14 密碼最長使用期限		29 隱藏移除區域資訊的機制
	15 密碼最短使用期限		30 不要保留檔案附件的區域資訊

1060201中華龍網軟體價格表

組別	項次		品項名稱	授權數	廠牌	得標價格
6	366	DVM	DragonSoft Vulnerability Management全中文弱點掃描軟體-專業版7.5/128U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$197,970
6	370		DragonSoft Vulnerability Management全中文弱點掃描軟體-旗艦版7.5/512U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$441,625
6	372	GCB	DragonSoft GCB 政府資安組態稽核軟體-專業版/128U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$248,731
6	374		DragonSoft GCB 政府資安組態稽核軟體-企業版/256U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$279,188
6	376		DragonSoft GCB 政府資安組態稽核軟體-旗艦版/512U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$350,254
6	378	EDR	DragonSoft EDR (雲端版)端點威脅掃描軟體-專業版/128U/壹年更新與支援/附授權書	1	中華龍網股份有限公司	$303,554
6	379		DragonSoft EDR (雲端版)端點威脅掃描軟體-企業版/256U/壹年更新與支援/附授權書	1	中華龍網股份有限公司	$323,858
6	381		DragonSoft EDR (雲端版)端點威脅掃描軟體-旗艦版/512U/壹年更新與支援/附授權書	1	中華龍網股份有限公司	$405,077
6	383		DragonSoft EDR (白金版)端點威脅掃描軟體/25U/壹年更新與支援/附授權書	1	中華龍網股份有限公司	$506,600
6	384	RAMP	DragonSoft RAMP資安風險評估管理平台-專業版/128U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$619,290
6	386		DragonSoft RAMP資安風險評估管理平台-企業版/256U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$822,336
6	388		DragonSoft RAMP資安風險評估管理平台-旗艦版/512U/壹年更新與支援/附授權書與光碟	1	中華龍網股份有限公司	$1,015,230
6	390	DVM升級	DragonSoft Vulnerability Management全中文弱點掃描軟體-專業升級版/128U/壹年更新與支援	1	中華龍網股份有限公司	$147,208
6	392		DragonSoft Vulnerability Management全中文弱點掃描軟體-企業升級版/256U/壹年更新與支援	1	中華龍網股份有限公司	$197,970
6	393		DragonSoft Vulnerability Management全中文弱點掃描軟體-旗艦升級版/512U/壹年更新與支援	1	中華龍網股份有限公司	$279,188

簡報結束
敬請指教

若有問題歡迎與我們聯繫
鄭羽婷 rainycheng@dragonsoft.com
黃筱雯 wenhuang@dragonsoft.com