APEXSYS 病毒事件監控及自動防護系統

病毒偵防隊（Virus- SOC）為智慧型之病毒防護管理平台，架設於防毒軟體之上、且相容於所有防毒軟體！

系統內容包含：

＊ 病毒監控防護：異常行為分析、病毒防禦、病毒事件追蹤管理、病毒路徑跟蹤、自動防禦機制

＊ Windows 惡意程式收集器：可收集系統活動資訊，根據自訂的規劃作出相應的通報訊息、主動通知管理者目前 Client 端之主機狀況，並追蹤後續事件發展。

・病毒偵防隊架構說明：

＊Client Agent 功能：

・防毒 Virus Action Log

・病毒十大藏身地點監控（Regedit）

・自動防護功能：Hosts 黑名單防護（c:\WINNT\system32\drivers\etc\hosts）

・DNS 反查 127.0.0

・自動回傳下列資訊至 V- SOC 管理系統：

＊Virus Log

＊Action regedit

＊Client PC Name or IP

＊V-SOC Agent 功能：

・Virus Log 資料庫

・Regedir 資料庫

・黑名單資料庫

・事件追蹤功能

・報表分析功能

・自動回傳下列資訊至 V- SOC 管理系統：

＊Regedit Action 事件

＊可疑程式 or 連線行為

＊可疑連結之 IP / Domain

APEXSYS Server 功能：

- 事件分析
- 入侵手法分析
- 黑名單資料庫 (IP / Domain)
- 自動更新下列資訊至 V- SOC Agent 中繼管理平台
  - ＊Regedit Action 事件
  - ＊可疑程式 or 連線行為
  - ＊可疑連結之 IP / Domain

・病毒偵防隊之特色與優勢：

1. 系統易於安裝及使用
2. 全中文繁體操作界面
3. 具備連線記錄功能
4. 啟動管理檢測功能
5. 具備惡性程式檢測功能：支援所有檔案類型
6. 具備行為模式檢測能力
7. 具備異常行為分析功能
8. 具備病毒事件追蹤管理功能
9. 具備病毒路徑跟蹤功能
10. 具備自動防護機制
11. 具備集中日誌功能
12. 可集中安裝和管理
13. 具備個人端電腦資訊顯示功能
14. 具備遠端診斷功能
15. 具備自動通報訊息功能
16. 具備事件追蹤功能
17. 具備中毒事件追蹤關單機制功能
18. 具備黑名單資料庫功能
19. 具備黑名單機碼比對機制
20. 具備報表分析功能
21. 具備偵測可疑連結功能
22. 具備病毒監控功能