招標規範(資訊部「日誌管理系統」採購案規格書)

壹 設備規格及功能

1.1設備硬體需求：(參考品牌:HP 或 DELL 或 同等品並不得為大陸品牌)

1. 提供 2 個 8 核心 Intel Silver 4309Y *2
2. 提供 64GB(含)以上記憶體，單一記憶體模組為 32GB(含)以上。
3. 提供 10 顆(含)以上支援熱抽換 3.5 吋、6TB(含)以上的 SAS HDD，單一主機須可擴充至 12 顆(含)以上 3.5 吋內接式硬碟。
4. 提供原廠 SAS 磁碟陣列控制器，4GB(含)以上快取記憶體及支援支援 RAID 0、1、5、6、10、50 及 60 功能。
5. 主機須具備 4 埠(含)以上 Gigabit Ethernet 網路介面和 2 埠(含)以上 10Gbps Ethernet 網路介面
6. 提供 2 組 800W(含)以上具備熱抽換以及備援功能之電源供應器。
7. 主機須為 2U(含)以下機架式設計。
8. 提供 Windows Server 標準版或 Red Hat 企業級 Linux 作業系統。
9. 提供 3 年 5x8 原廠保固服務。

1.2設備軟體需求:(不得為大陸品牌)

1. 需提供獨立、可橫向擴充且具高可用架構之日誌管理系統，以確保系統、網路與資訊設備等日誌完整收納。
2. 需提供原廠代理程式(Agent)與無代理程式(Agent)方式收集日誌，原廠代理程式至少需支援 Microsoft Windows 與 Linux 版本，以確保軟體品質與架構整合彈性。
3. 原廠代理程式(Agent)可提供統一遠端安裝介面。
4. 需提供符合本案日誌收容需求之日誌正規化設定。
5. 需提供以下系統與設備類型日誌支援
   a. 作業系統：Microsoft Windows 及 Linux。
   b. 資料庫：Microsoft SQL 及 MySQL。
   c. 網路設備與資安設備：交換器、防火牆、入侵防禦設備及網路安全閘道器。
   d. 應用系統：IIS、Apache、Syslog、SNMP 及 JDBC。
6. 日誌收容需同時保存原始日誌(Raw Events)與正規化(Normalized Events)日誌資料，且提供 SHA-256 以上安全雜湊與數位簽章機制確保資料完整性。需對資料底層檔案進行保護，以確保收容之資料安全。
7. 日誌系統提供日誌路由功能，可自訂即時與歷史日誌過濾開始與結束時間、特殊日誌內容等條件且可以同時制定多種不同路由條件傳送不同日誌給多個系統用，例如同時傳送至日誌管理(Log Management)留存與關聯分析(SIEM)進行分析，已達成最快異常分析效能。

8. 日誌收集提供全路徑(End to End)監控功能，並可監控日誌收集、處理與傳送效能，針對異常狀態提供告警(如 mail)，以維持最佳資料品質。
9. 提供收容之日誌檔案備份管理(Archive)與回存調用(Restore)機制，收容檔案需以壓縮型態儲存以降低系統管理負擔。
10. 需提供網頁使用者介面，支援全文檢索查詢功能，並可點擊查詢結果自動帶入查詢條件進行串查。
11. 需提供日誌橫向擴充能力，不論日誌儲存在哪一台實體日誌收容主機上皆可於任何單一日誌收容主機上跨設備查尋到相關事件。
12. 需提供日誌重傳機制，可依據需求自行定義時間與搜尋條件將儲存的日誌轉拋至其他系統進行二次分析。
13. 提供原始日誌全文資料檢索（Full Index）與選擇性欄位資料檢索功能，透過設定搜尋條件可馬上分析找到相關系統日誌。
14. 系統預設提供 SANS Top 5:Top Users with Failed Logins、Failed Resource Access by Users and Drilldown、Alerts from IDS 等分析性報表以協助管理者分析內部相關資安事件。
15. 保固期間需無償提供 10 張客製化報表。
16. 需提供自訂義報表功能，圖表至少支援圓餅圖、長條圖、區域圖，報表格式至少包含 PDF、HTML、MS EXCEL 等格式。
17. 需提供多使用者功能，依據使用者權限自定義其可查詢之設備日誌內容，例如網路人員只能查詢網路設備等。
18. 需提供系統管理功能，統一更新日誌管理平台與原廠代理程式。
19. 提供之軟體須能接收 700EPS 以上且產品保固 3 年，並且不限日誌來源端設備之數量。
20. 需提供日誌 180 天的儲存空間，本會現有日誌收集 240G/日 180 天約 45T 為 75%水位)故需要 60T。

貳 教育訓練

1. 設備安裝完成後，即可進行教育訓練，課程內容必須包括系統操作與維護，至少辦理兩梯次，每次四小時，並請於驗收前完成。
2. 立約商準備教育訓練計畫，並提供合格教師在指定之時間及地點進行教育訓練課程，並得視使用單位需要延長及增加梯次，立約商並不得另外要求收費。師資人員及其他相關衍生性之所有費用皆由立約商自行負擔。
3. 訓練之日期、地點及受訓人數由公視基金會指定，其相關費用由立約商負擔，立約商應備教育訓練簽到紀錄表。
4. 驗收前，立約商應製作全系統中文操作手冊，作為驗收項目之一。

參 驗收及保固

1. 立約商應於驗收合格後提供原廠和得標商連帶保固三年保固書，及所有安裝於主機內完整軟體功能的License 原廠證明文件，證明為合法License。
2. 保固期間內免費負責標的物之維修、保養換件等維護工作及正常使用狀況下發生故障免費修理與更換非消耗性零組件。若標的物在保固期間內軟硬體有缺失(BUG)，立約商應負責維修或更新改善，並不得索取任何費用。
3. 本案自驗收合格日之次日起，立約商提供軟硬體三年 5*8 保固與維護，須於2小時內提供電話除錯服務，叫修後 4 小時內到府服務，如無法於 24 小時內修復完畢，立約商須無條件提供相容同等級以上之備品。

10 張客製化報表內容如下:

1. 事件收容系統每日主機事件統計
2. 網路設備管理者登入失敗報表
3. 網路設備設備設定變更紀錄報表
4. 作業系統管理者登入成功與失敗報表
5. 作業系統一般帳號登入錯誤事件統計報表
6. 作業系統稽核事件清除報表
7. 作業系統帳號建立報表
8. 作業系統重要服務重啟紀錄報表
9. VPN 設備存取紀錄登入失敗報表
10. VPN 設備下班後存取紀錄報表

、