馬偕紀念醫院全院區

微軟 EDR 及 Defender 系統維護服務需求表

廠商所提標的必須符合下列規範，如有需要可進一步與本院主辦單位進行需求訪談及確認。

一、授權：

(一).期間：自 2026 年 10 月 01 日至 2027 年 09 月 30 日止，共計 12 個月。

(二).範圍：全院區（台北院區暨兒醫、淡水院區、新竹院區暨竹兒、台東院區）。

(三).SLA（Service-Level Agreement）：7*24 免費告警與處理服務，不限次數電話或通訊軟體線上即時支援服務，包含若有需要到院支援服務。

(四).緊急事件處理(IR): 維護期間若發生重大資安事件，需到現場執行資安事件調查，並提供資安事件處理程序，事後必須提出事件調查報告，此服務一年至多兩次。

(五).維護說明：提供每半年到院保養維護，並提供資安威脅鑑識分析報告，除台北及淡水院區需到場外，其它院區可遠端連線（包含協助安裝及後續維護服務）。

二、規格：

(一).需求：

1. 協助分群管理，針對不同部門或掃描單位設定群組，及檢視檢測狀況。
2. 協助掃描參數上設定開啟 Windows Auditing，於端點檢測掃描時自動開啟微軟作業系統稽核日誌，協助設定 Windows 系統稽核日誌最佳化狀態。
3. 協助搜尋功能，可透過電腦名稱、IP、檔案名稱、檔案 MD5，調閱檢測過的電腦報告。
4. 協助儀表板上可檢視出當天所有掃描的電腦數及掃描成功的數量，以及指派掃描的任務數及成功取回的報告份數，和總共發現的高風險電腦數；可設定時間區間，提供該時間區間的風險狀態。

(二).偵測與分析功能需求：

1. 能夠分析與偵測出異常的端點主機，識別出異常的端點活動、檔案、帳號、執行記錄及網路行為，並計算出主機的風險分數 。
2. 可建立調查的工作區，選取欲調查的時間區間，自動匯入於此時間區間內相關的端點主機資料。
3. 依檔案、IP、Domain、帳號等內容新增黑白名單，協助事件的過濾。
4. 視覺化呈現的方式顯示主機間的互動關係，包含主機間登入登出、檔案移動之記錄及內網橫向移動軌跡。
5. 將各異常行為的端點主機以時間軸的方式呈現整個攻擊時序。
6. 可偵測出單位內沒有在掃描內但有與掃描過的電腦互動過的隱藏設備清單。
7. 能夠自訂規則於單位內進行威脅事件的獵捕 (Threat Hunting)，單位可以依檔名、MD5、IP、Domain、主機名稱、帳號 名稱、Command Line 內容、事件等級等條件組合成單位所需的規則。.
8. 每半年提供 HTML/STIX 格式的報告，支援產出中文、英文內容。
9. 協助多種角色權限來使用管理系統。

(三).告警需求：

1. 初步發現威脅事件時，能自動發出端點威脅獵捕告警，內容須包含：
   (1).掃描狀態
   (2).可疑電腦總數
   (3).告警時間及威脅摘要
   (4).描述嚴重程度
   (5).電腦名稱
   (6).IP 位址及威脅指標
2. 系統發出端點威脅獵捕告警後，需自動調查整體場域威脅情況，內容須包含：
   (1).威脅概要
   (2).端點分析
   (3).惡意程式分析
   (4).網路活動分析
   (5).攻擊時序圖
   (6).可疑活動分析
3. 每半年資安威脅鑑識分析報告，可透過自動化分析，提供場域威脅情況，內容須包含：
   (1).資安威脅鑑識分析報告總覽：統計所影響的高風險主機及威脅等級。
   (2).受駭資訊列表：羅列受駭資訊，包括電腦名稱、IP 位址、掃描群組、可疑檔案、及中繼站。
   (3).威脅情態圖：透過威脅情態圖以時間軸方式呈現單位內攻擊事件所移動的軌跡。
   (4).MITRE ATT&CK 攻擊技術統計：以 MITRE 提出的 ATT&CK 框架，將入侵期間可能發生的情況，做出更細部的畫分，報表以統計的方式呈現攻擊所使用的手法。
   (5).惡意程式分析：呈現本次調查分析中所發現惡意程式之資訊及屬性。
   (6).主機分析：呈現本次掃描中所有端點主機狀態，其中包含本次事件中的嚴重程度、端點名稱、端點所在地區、群組（部門）、IP、設備型號及作業系統。
   (7).可疑對外連線分析：呈現調查中端點所連線的惡意中繼站，並顯示其嚴重性、內容（中繼站位址）。
   (8).可疑活動列表：呈現攻擊中所使用的指令。
4. 針對掃描範圍所監控端點輸出資產盤點分析報告，內容須包含：
   (1).統計分析：說明此次統計區間中所有掃描情況及作業系統分布情況。
   (2).新增使用者帳號：區間內掃描端點上所新增的帳號。
   (3).可疑帳號列表：統計遭鎖定的帳號。
   (4).新增主機：統計區間內所新增的主機，可用於確認部署計畫是否符合。
   (5).缺席主機：統計掃描區間內沒有進行掃描的端點主機，可用於確認部署計畫是否符合。
   (6).登入成功帳號排名：統計並呈現有成功登入行為的主機所使用之帳號列表。
   (7).登入失敗帳號排名：統計並呈現有登入失敗行為的主機所使用之帳號列表。