臺灣基督教門諾會醫療財團法人

Mennonite Christian Hospital

次世代端點防護軟體-徵求建議書說明文件

Request For Proposal

2025/03/18

目錄

1. 專案描述

1.1. 專案名稱

本專案名稱為臺灣基督教門諾會醫療財團法人（以下簡稱甲方）「次世代端點防護軟體」（以下簡稱本專案）。

1.2. 專案目標

為維護主機及端點安全，藉由本案之執行成果，以分析及偵測威脅之資安防護能力來保護各端點、主機，並依據檢測結果提出作出改善，藉由端點防護提升端點安全防護成效。

1.3. 專案期程

1.3.1. 專案期限：2025 年 12 月 1 日前完成系統轉換。系統訂閱期間自 2025 年 12 月 1 日 至 2028 年 12 月 1 日，共 3 年。

1.3.2. 本專案決標前如因故暫緩、延期或變更需求，甲方將另行通知，投標廠商不得提出要求相關損失責任。

1.4. 名詞定義

1.4.1. 時間：以下本專案所稱「日、時、分」，皆以 ☑日曆時間　☐工作時間 為計。

1.4.2. 驗收完成日：指完工後經甲及廠商雙方通過驗收簽名日。

1.4.3. 年度業務正常運轉率：1-(系統非規劃性失效分鐘數 / (365*24*60))

1.4.4. 臺灣基督教門諾會醫療財團法人：包含美崙總院、壽豐分院及所屬相關機構。

1.4.5. 美崙總院：定義為臺灣基督教門諾會醫療財團法人門諾醫院。

1.4.6. 壽豐分院：定義為臺灣基督教門諾會醫療財團法人門諾醫院壽豐分院。

1.4.7. 次世代端點防護軟體： Next Generation Endpoint Protection Platforms，新一代之端點防護系統，以端點電腦之程式行為判斷是否遭電腦病毒、惡意軟體、蠕蟲等進行侵害、盜用。補足以病毒特徵碼作為判斷依據之缺點。

1.5. 廠商資格

1.5.1. 非經濟部投資審議委員會公告之「陸資投資資訊產業事業清冊」廠商。

1.5.2. 營業項目具資訊軟體服務且資本總額新台幣 5000 萬元以上之公司行號。

1.5.3. 須為採購標的之原製造廠商或原廠授權之經銷商。

1.5.4. 廠商須有國內建置導入經驗之實績。

1.5.5. 技術維護人員需有原廠授權認證資格。

2. 現況說明

2.1. 現行主機作業系統

2.1.1. Linux Base 作業系統。

2.1.2. Mac OS 作業系統

2.1.3. Windows 作業系統

2.1.4. Windows Server 作業系統

2.2. 現行使用之 XDR 次世代端點防護軟體

Paloalto Cortex XDR Pro with Host Insights add-on，授權數量：1967 套-

2.3. 現行 MDR 數量：280 套

3. 需求說明

3.1. 數量

機構	XDR / 台	MDR / 台	
		User	Server
美崙總院	1924	115	173
壽豐分院	236	0	2
合計	2160	115	175

3.2. 建置需求(延用現用標的廠牌者不適用)

需協助拆除現行之 XDR 及建置新 XDR，需在 12 月 1 日 前完成 XDR 代理程式的部署，將採取批次推送策略，優先安裝於高風險區域設備，確保所有設備皆能成功註冊並運行且回到後台管控。並提供安裝報告，確認新安裝之 XDR 已安裝至全院設備。

3.3. MDR 需求

3.3.1 威脅偵測：

提供的 24*7 監控，以檢測潛在的威脅。這包括監控網絡流量、端點活動、日誌數據等，並使用高級分析技術（如行為分析、威脅情報）來識別異常活動。

3.3.2 事件響應：

當 MDR 服務檢測到威脅時，專家團隊會即時進行響應，這可能包括隔離受感染的設備、封鎖惡意流量、協助組織恢復正常運營等。

3 .3.3 威脅緩解：

根據偵測到的威脅，MDR 團隊可以採取立即行動，如封鎖惡意 IP 地址、禁用受影響的帳戶等，以快速中斷攻擊鏈。

3.3.4 威脅情報和分析：

MDR 團隊利用行為分析技術來識別異常模式和潛在威脅，這些分析通常基於過去的攻擊模式和數據趨勢。

3 .3.5 報告和持續改進：

根據偵測到的威脅和事件，MDR 服務提供安全改進建議，並在每月提供報表。每季召開定期會議，幫助組織加強其防禦能力，減少未來攻擊的風險。

3.4. 整合第三方軟體：

透過 Webhook 或 SysLog 來達到觸發警報時傳送訊息至三方軟體。

3.5. 軟體需求及適用範圍

提供該次世代端點防護軟體為取得授權使用的商用軟體合法授權，於合約期間，授權使用於甲方各機房主機及電腦。

3.6. XDR 軟體功能

3.6.1. 行為分析與威脅偵測：

建立正常操作行為基準，監控應用程序和系統活動，對異常行為（如異常的檔案

存取或網路流量）發出警報。

3.6.2. 端點偵查與回應：

3.6.2.1. 事件調查：記錄端點上的事件，分析威脅來源、攻擊路徑和影響範圍。

3.6.2.2. 即時回應：根據威脅的嚴重性，採取措施如阻斷網絡連接或終止惡意進程。

3.6.2.3. 離線掃描：在切斷網路的狀態下掃描裝置上有無惡意來源，並回傳數據至後台。

3.6.2.4. 應用程式查詢：可透過 Agent 識別端點上安裝之應用程式，並識別安全漏洞。

3.6.2.5. 包含防毒功能：自動識別帶有惡意程序、引響系統面的軟體，並做阻攔隔離。

3.6.3. 主動威脅防禦

3.6.3.1. 威脅情報整合：整合全球威脅情報，識別最新攻擊手法。

3.6.3.2. 實時監控：掃描靜態檔案和實時監控系統活動，攔截網絡上的可疑活動。

3.6.4. 網路威脅防護

3.6.4.1. 主機防火牆：阻擋未授權或惡意流量、防範橫向移動攻擊。

3.6.4.2. 入侵防護系統（IPS）：監控和攔截網路攻擊。

3.6.4.3. 深度包檢查（DPI）：分析網絡數據包，識別並阻止惡意代碼。

3.6.5. 應用控制與黑白名單

3.6.5.1. 應用管理：定義並管理允許執行的應用程式。

3.6.5.2. 應用隔離：提供沙箱環境中運行應用，保護系統安全。

3.6.6. 自動化回應與補救

3.6.6.1. 威脅隔離：自動隔離受感染的設備或檔案。

3.6.6.2. 補救措施：自動刪除惡意檔案，修復受損的系統。

3.6.7. 集中管理與報告

3.6.7.1. 統一管理控制台：集中管理所有端點，設定防護策略。

3.6.7.2. 詳細報告：可生成自定義的安全報告，包括威脅概況、趨勢分析等。

3.6.7.3. 安全事件報表：(主動送出)與安全事件相關的詳細報告，包括事件的類型、來源、影響範圍、處理狀態等。

3.6.7.4. 威脅分析報表：生成並獲取威脅分析報告，這些報告通常包含威脅的來源、特徵、影響和緩解措施等。

3.6.7.5. 合規性報表：生成符合特定法規和標準的合規性報告，這些報告可能包括安全配置審核、事件響應審核等。

3.6.7.6. 系統運營報表：提供關於安全系統運營狀況的報告，資源利用率、事件響應時間、系統健康狀態等。

3.6.7.7. 日誌審計報表：提取與安全日誌相關的審計報告，這些報告可以包括訪問控制、變更歷史、日誌篩選等內容。

3.6.7.8. 威脅情況報告：定期生成並獲取組織面臨的威脅情況報告，幫助了解當前的威脅趨勢和攻擊行為。

4. 專案管理

4.1. 廠商須於簽約 2 星期內召開專案啟始會議，向甲方說明專案執行計劃書，並至少每 2 星期召開一次定期專案會議；除此例行會議外，甲方有權要求廠商隨時提供相關工作資料及召開臨時會議，廠商不得拒絕或藉故拖延。

4.2. 廠商須就甲方環境並評估相關資源風險後，規劃並實施各階段建置時程。若遇需變更 需求規格或合約之時程，則須先召開專案會議取得協議，再經甲方確認同意後實施。

4.3. 系統建置應按複選議價表或最後議價文件及徵求建議書說明文件(詳附件)，惟建置過程中會因甲方工作流程及雙方資訊技術考量而異動原需求，故最終驗收功能與介接項目，須於驗收前經雙方討論，並由甲方使用單位確認，異動項目請廠商製表說明之。

4.4. 甲乙雙方應依照建置計劃書所訂之施工責任介面施工。

4.5. 本專案所須之資源與人力，包含成立專案小組及擬定本標的物之建置計劃書、佐證資料範本等相關文書、行政作業均由廠商負責，並依進度需要增加人力。

4.6. 廠商必須選派本專案負責人及相關負責人參加，會中必須由本專案負責人提報目前工作進度及所遭遇問題之解決方案。

4.7. 廠商必須於標的物建置完成上線測試日起，提供系統維護人 1 名駐甲方 15 日 ☑ (5x8) ☐ (7x8) ☐ (7x24)，期間廠商如有未到場情事發生，則將依其未在場時數順延，直到駐點期滿止。※如為現行之產品則不需提供此服務

4.8. 本專案進行中，甲方有權要求提出更換不適任之專案人員，廠商不得藉故拖延及拒絕。

4.9. 執行本專案期間，廠商同意甲方得視狀況要求廠商人員在甲方所提供之場所工作。

4.10. 廠商須提供建置過程之文件，如會議紀錄及交付驗收時檢附之文件。各項文件共享方式須符合甲方保密及資安規範，文件內容除非有必要否則不應含有個資。

4.11. 因甲方因素延誤相關交付期程，得於 10 日前通知更改完廠商成日期，且不計入廠商遲延。

4.12. 廠商因不可抗力之事由（如天災、地變、罷工、戰爭）及其他非可歸責於廠商之事由，致使延誤本約完成期限，廠商應於專案會議通過後以正式公函提出申請，自該等事由消滅日起，順延同等期間交付各工作項目，不計入廠商之遲延。

5. 教育訓練

5.1. 廠商須於交貨後、驗收前，依建置計劃書所訂之教育訓練計劃，配合甲方時間、地點，為相關人員進行包含但不限於以下的操作及維修教育訓練，並得配合甲方實際需求延長教育訓練時數。

5.1.1. 系統操作訓練：☐無；☑每年至少乙梯次原廠認證教育訓練。

5.1.2. 故障排除訓練：☑無；☐至少乙梯次，每次 1 小時以上。

5.2. 教育訓練課程辦理前，廠商應於上課前 7 天交付足夠數量之教材及講義書面或電子檔、簽到表，供上課學員使用及作為驗收依據。若參加原廠訓練，則廠商須負責為甲方安排所有相關事項。

5.3. 廠商所有提供之教育訓練課程需配合導入甲方 E-learning 課程，並於保固維護期間，依甲方通知持續提供相關訓練課程。

6. 驗收

6.1. 系統軟硬體設備若於交貨時停止生產或升級，經甲方負責人同意後廠商得以功能最新且不低於本標的物所定之規格所需之產品替換。

6.2. 交付標的物之規格、數量、時程應完全符合本案要求，除本條第一項之情形外，如有不符者，甲方有權要求廠商更換或補足之，廠商不得異議。更換或補足須於 5 日內完成，乙方如未能於期限內完成手續時，視同逾期交貨。

6.3. 廠商應免費提供甲方因執行驗收程序所必要之一切人員及設備，如廠商無法提供時，甲方得聘任第三者為之，其所需費用由廠商負擔，並由廠商貨款中扣除。

6.4. 本案完成系統上線後，通過試運轉 30 日後始得辦理驗收，試運轉(驗證)期間異常改善，廠商應接獲甲方通知後，於 7 日內完成改善並於改善後次日起驗證 7 日無異常方視為完成改善。※如為現行之產品則不需試運轉

7. 付款方式

本專案交付期程依下列約定辦理：

期數	項目	檢附文件	請款額度
一	西元 2025 年 11 月 15 日前完成建置，通過試營運並完成驗收	☑版權證明及軟體授權證明 ☑教育訓練明細佐證文件 ☑教育訓練教材及操作手冊電子檔	X
二	西元 2025 年 12 月 1 日正式上線	☑院區安裝報告	總價金

8. 保固維護責任

8.1. 單一聯絡窗口事故排除及技術諮詢服務，該員須為廠商專任、年資 2 年以上人員。

8.2. 保固責任：

除天然災害或不當操作造成損壞外，提供標的物□硬體_年；□電池_年；☑訂閱期間之免費維護保固、功能訂閱、授權及升級等服務。

8.3. 定期維護：

8.3.1. 維護項目：

☑無

□ 軟體維護須每季定期至維護標的所在地，進行現場或遠端維護服務，包含系統效能、資源耗用等分析及調校。

□硬體維護須每季定期至維護標的所在地，進行現場維護服務，其範圍包括清理、調整、檢視和測試等並免費更換正常使用下損壞之零件。

8.3.2. 廠商應於每次維護完成後，提供甲方維護、建議事項，並由雙方簽名確認維護紀錄。

8.3.3. 現場維護服務後於維護結果會議報告，包含：維護項目、系統運行狀況、系統資源使用狀況等。

8.3.4. 廠商應於每年度期末提供次年度維護計劃。

8.3.5. 停機維護須經甲方同意後執行，廠商應以不妨礙甲方正常工作時間為原則。

8.4. 服務水準：

8.4.1. 廠商保證維護標的年度業務正常運轉率達 99%以上，除外情況：端末設備、甲方例行性、有預警計畫性停機或地震、火災等天然災害因素，則不計入系統中斷時數。

8.4.2. 提供 □5x8 □7x8 ☑7x24 小時報修服務。接獲技術諮詢或維護請求時，得以電話、電郵或通訊軟體回應及使用遠端連線方式處理，連線方式由甲方提供，且須符合甲方之管理規範。如無法透過電話、電郵、通訊軟體或遠端連線方式處理時，依下述服務水準要求現場維護。

8.4.3. 情況等級由甲方判定或並依現場情況之變化提升或降低故障等級：

狀況	情境	回應支援方式		完修期限
緊急	影響全院事件	30 分鐘內	現場或遠端支援	接獲通知起 8 小時內完修或完整功能替代品上線
嚴重	設備或軟體故障，系統已無法維持高可用性狀態或營運持續計畫環境處於失效狀態	8 小時內	現場或遠端支援	接獲通知起 2 日內完修或完整功能替代品上線
一般	弱點修補、系統設定調整、報表提供等	16 小時內	現場或遠端支援	接獲通知起 20 日內完修或完整功能替代品上線

9. 資通安全要求

9.1. 有關雙方之專業技術、病人隱私、業務機密(含全部文件合約內容及發票金額等)，雙方保證不得洩漏或交付第三者。

9.2. 資安防護分級：

9.2.1. 依據「資通安全責任等級分級辦法」揭示，本系統參照其分級原則，評估系統等級為「S」。【註：「*」未涉及資通安全應用軟體開發】

9.2.2. 系統防護基準如 SSDLC 採取措施及驗證查核表(詳附件)。合約期間廠商須維持維護標的評估系統等級為「S」且配合甲方不定期進行查核；惟如查核結果未達控制措施，廠商須於 1 個月內完成改善並達控制措施。

9.3. 安全重點要求：

9.3.1. 留在甲方施行單位內部處理機密性、敏感性或是關鍵性的應用系統項目。

9.3.2. 執行事項應經甲方施行單位核准。

9.3.3. 廠商發現疑似資通安全事件時，應即時通報甲方專案負責人，並提供資安事件相關資訊，於資安事件處理過程中，若涉及民、刑事法律行動，應進行蒐證與證據保留。

9.3.4. 應與甲方共同管理和解決所有界定的問題及施行應用系統異動的管理程序。

9.3.5. 應遵守資訊安全相關法律規範。

9.3.6. 建置系統之鐘訊，須符合甲方時間來源同步要求。

9.3.7. 建置系統之服務水準，須符合甲方營運持續計畫之業務回覆時間要求。

9.3.8. 建置系統應提供各組件規格及版本，做為甲方建構管理之基礎資訊。

9.3.9. 建置系統適用之作業系統版本，當有更新版本時，本系統之符合性須主動通知甲方。

9.3.10. 應依甲方施行單位要求裝設防毒軟體。若該系統無法安裝時，應採取其他防護措施，且須經由甲方同意。

9.3.11. 依據資通安全責任分級辦法附表十之源碼掃瞄要求，應配合甲方工具及監督下執行弱點與原始碼掃描。

9.3.12. 若遇提供之服務變更時（例如：系統或設備更換、維護水準調整），應經甲方評估相關風險同意後再實施。

9.3.13. 廠商應確保開發之系統或網站應用程式無留有任何形式之後門。

9.3.14. 廠商欲連線甲方設備須事前經安全檢測，通過後方可使用。

9.3.15. 相關硬體及軟體產生之任何資料，非經甲方同意，不得傳輸至甲方以外之網路(如：設備校正數據資料)。

9.3.16. 依據資通安全責任分級辦法附表十之備份及營運持續要求，系統之資料備份與災難還原機制應配合甲方現有設備及環境進行規劃，制訂完善備份(援)程序及回復程序，詳細說明系統(含本系統使用之軟體、應用系統、系統內登錄之資料等)毀損之回復措施，系統如遭逢重大天然災害或人為意外時，能迅速重建系統及還原所有資料。廠商應配合甲方業務持續營運管理相關作業，並符合現況說明中之各項 RTO 及 RPO 標準。

9.3.17. 甲方保有對廠商執行檢查及稽核的權利，甲方得依需要對廠商專案相關工作之執行、資料之處理及執行之紀錄，進行實地現場訪視或調閱資料，廠商應以合作態度及於合理時間內配合甲方或委託之專業機構稽核作業，提供相關書面資料或協助約談相關人員，廠商不得有異議。廠商經檢查或稽核結果發現不符合資安規範，須於接獲甲方通知期限內改善。

9.3.18. 廠商於合約終止後，應歸還屬於甲方之資產(含硬體、軟體、資料和系統存取權限等)。

9.3.19. 不得使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。

9.4. 資訊系統原碼：

基於保障甲方關鍵系統維運，得提供資訊系統原始碼，於每期期末無償交付甲方最新版次之資訊系統原始碼。惟套裝軟體可排此條款。

9.5. 安全檢測作業：

□原碼掃描安全檢測：

依據資通安全責任分級辦法附表十之源碼掃瞄要求，新版程式發佈前須經過原碼檢測，每次程式更新上線前，廠商須先提交預備發佈之原始碼進行原碼檢測，並配合改善前兩

級高風險問題，報告結果須無前兩級高風險等級問題，方可進行後續新版上線作業，整體作業流程須於 1 個月內完成。

☑弱點掃描安全檢測：

依據資通安全責任分級辦法附表十之弱點掃瞄要求，甲方每年執行一次弱點掃描檢測作業，廠商須處理報告內容屬於前兩級高風險等級之弱點。直到甲方複掃報告中無前兩級高風險弱點才視為完成，整體作業流程於 1 個月內完成。

□行動化應用軟體（Mobile App）安全檢測：

本案若含行動化應用軟體（Mobile App），應通過經濟部工業局訂定之檢測項目，方可上架應用程式商店及提供民眾下載使用；前述檢測作業，應由符合經濟部工業局公告「行動應用 App 基本資安自主檢測推動制度」規範之認證合格檢測實驗室辦理，相關檢測費用由廠商負擔。（相關規範詳見行動應用資安聯盟網站

[https://www.mas.org.tw] ）

□滲透測試：

依據資通安全責任分級辦法附表十之滲透測試要求，甲方每 2 年執行一次滲透測試作業，廠商須處理報告內容屬於前兩級高風險等級之弱點。直到甲方複掃報告中無前兩級高風險才視為完成，整體作業流程於 1 個月內完成。

10. 個資保護要求

依據個資法及個資法施行細則，委託廠商配合辦理個資保護要求事項如下所述。

10.1. 廠商個人資料保護措施(二擇一)：

□ 廠商得提供其主管機關要求之「個人資料安全維護計畫」，說明委託蒐集、處理或利用個人資料之範圍、類別、特定目的及期間。廠商應依據個資法善盡個資保護管理之責。

□ 廠商應於簽約時向甲方進行個人資料保護管理狀況報告，並交付附件「委外廠商個資安全管理自評表」，甲方得視需要，進行實地稽核。

10.2. 廠商人員承辦或接觸甲方個資委外業務時，應簽訂「外部人員保密切結書(**詳附件**)」並遵守甲方「個資保護管理政策」相關規定。

10.3. 廠商人員於受託業務執行期間若有異動，應事先通知甲方專案負責人，並重新簽署保密切結書。

10.4. 廠商應防止個人資料洩漏並禁止盜用。

10.5. 廠商禁止為合約範圍外之影印、複製、加工及利用。

10.6. 廠商若要將個人資料相關作業再委託第三者，必須徵得甲方同意授權後，始得為之；複委託之機關亦應遵守本合約所要求之個資保護管理相關規範。

10.7. 廠商應於合約終止或解除並啟動退場機制時，返還或銷毀/刪除因受委託而蒐集處理利用之個人資料。

10.8. 廠商若發現有違反個人資料保護法事件，必須即時通知甲方，說明事件的原委與應變措施，若有任何損失發生，則須負賠償責任。

10.9. 合約期間傳遞之資料載體(包括但不限於隨身碟/可攜式硬碟/光碟片等儲存媒體)於使用

完畢，必須確保資料已於載體中以無法復原方式刪除或銷毀。

10.10. 應用系統內個資遭外洩或侵害情事，廠商必須於第一時間通報甲方，並說明目前已採取之因應措施與受影響程度。

10.11. 甲方得視需要，邀請專家學者共同至廠商處所，就個資保護之實體安全、存取控制、通訊與作業管理及個人資料保護法施行細則第 8 條之要求，對廠商進行稽核作業，廠商不得拒絕。

11. 內容釋義附則

上述內容及相關附件有疑義時，以甲方解釋為主，甲方保有解釋及修改之權。

12. 聯絡資訊

12.1. 資訊室：黃榆皓/03-8241035/benny0825@mch.org.tw

12.2. 資源開發管理中心：黃月櫻/03-8241568/pur04@mch.org.tw

13. 附件

☑ SSDLC 採取措施及驗證查核表

☑ 外部人員保密切結書

☐ 個人資料安全維護計畫

☑ 委外廠商個資安全管理自評表

☐ 建議書撰寫大綱