馬偕紀念醫院全院區
軟體 API 監控平台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、專案數量：

本專案提供 100U (含以上)之授權數量，實際安裝之標的須配合院方實施

二、服務期間：

自系統正式啟用之日起，為期一年。

三、系統架構：

1. 須支援本地佈署，VM 或容器化運行方式，VM 硬體資源由中心提供，以利未來架構調整彈性。
2. 須具備 Web 管理介面連線方式需為 HTTPS (TLS 1.2(含)以上版本。
3. 須具備 Web 管理介面使用者帳號密碼登入機制。
4. 須具備稽核軌跡留存功能，以利未來稽核及審查檢視。
5. 須提供 API 介面供其他系統整合使用 。
6. 需提供系統備份及復原之相關程序。
7. 須具備支援地端或雲端部署模式。
8. 須具備 Active Testing 功能，可於開發階段檢測 API 安全。
9. 須具備整合 CI/CD 流程進行自動化檢測。
10. 產品本身須具備符合 PCI DSS 4.0,SOC 2 等合規認證。

四、API 弱點及 API 類型辨識功能：

1. 採持續不中斷的方式部署 API 安全防護機制,能即時偵測異常行為或攻擊，並提供即時告警與事件回應能力，確保 API 的可用性與安全性;須支援多種資料收集方式,如下列方式且不限:

(i)流量鏡像 (Traffic Mirroring)

(ii)端對端全程加密外掛(Plugin)收集主機 API 資訊，

(iii)內容傳遞網路(CDN)流量轉拋

(iv)網路設備轉拋(WAF or SLB)

2. 針對 API 流量，辨識出包含但不限於網域名稱、IP、Method、API Path、API 類型、認證方式、資料類型、敏感數據之資訊。
3. 須具備自定義之群組分類，並設定單一 API 或群組可存取之權限及對應負責人。
4. 須具備支援匯入 API 規範文件，並自動比對實際運行 API 與規範文件之一制性 ;建立完整 API 清單，並透過持續自動盤點,確保高風險 API 資產符合作業遵循要點並同時具備產生 API 規範文件 (OpenAPI Specification) 功能。
5. 須具備可識別 OWASP API Security TOP 10(包含但不限於)相關風險，並由系統 Web 介面呈現。
6. 須具備分析 API 使用情況,如:

(i)支援正規表示式自定義資料類型與識別中文內容

(ii)識別 API 中的資料類型和敏感數據使用情況並自動添加 PII 、Sensitive、PCI 等資料標籤並建立 Baseline 行為模型，以便及早發現異常或攻擊行為。

7. 須具備系統日誌、事件通報可整合至 SIEM/syslog 平台功能。
8. 須具備 API 自動盤點與風險評分功能。
9. 須具備可識別認證機制異常與敏感資料使用狀況功能。
10. 須具備提供威脅事件說明與補救建議功能。
11. 須具備支援多節點 API 流量收集。

五、報表功能：

1. 須具備自定義系統報告及產出格式 (例如 excel 或 csv 等)。

2.須具備弱點事件自動告警功能。
3.須具備可於 Web 介面上進行弱點事件處置（例如處理狀態或標示誤判等）功能。
4.須具備辨識 API 是否提供外部網路（Internet）存取的功能。
5.須具備自動將測試結果對應至相關合規框架（如 PCI-DSS、ISO 27001），生成合規性報告。

六、廠商資格：

廠商需於投標時提供經銷授權證明

售後服務：（請將下列條件列於報價單中與合約內）

1.本產品為一年期訂閱制服務。
2.本專案包含到場系統安裝與建置服務，內容包含系統部署、規則部署與策略規劃，以及標籤（Tag）與安全政策（Security Policy）之設計與設定並提供循環掃描 script。
3.本專案包含系統安裝服務及相關教育訓練共 1 次，教育訓練時數至少達 2 小時（含）以上。
4.自驗收日起提供一年保固服務。保固期間內，廠商應提供免費維護與技術支援服務，以確保系統維持正常運作。
5.除即時風險告警與事件通知外，廠商將每三個月到場進行一次系統健康檢查與風險檢視，內容包含：

(i). 確認目前 API 風險狀況與暴露情形
(ii). 檢查平台監控與告警功能是否正常運作
(iii). 檢視是否存在高風險攻擊事件或異常行為
(iv). 提供相關風險改善與安全強化建議