一、資安監控 SOC 服務暨相關設備維護三年之規格

資安監控 SOC 服務暨相關設備維護三年之規格	
服務期間	民國 116 年 01 月 01 日至 118 年 12 月 31 日
說明	產品名稱/規格
一、	資安監控 SOC 服務三年
	1.本案廠商提供設備： 監看標的如下可擴充額度可增至 20 台。 2.監看標的： 2.1 Hontai_AD/DNS server 2.2 Hontai_AD_bolemei(tec-fweb) 網路投保網站 2.3 Hontai_AD_tec-dbs(DB) 網路投保資料庫 2.4 Hontai_Cisco 4503_Switch(1)核心交換器 2.5 Hontai_Cisco 4503_Switch(2)核心交換器 2.6 Hontai_DAM_Imperva 2.7 Hontai_DNS Server 1(內部 DNS) 2.8 Hontai_DNS Server 2(外部 DNS) 2.9 Hontai_Firepower_2110_IPS 2.10 Hontai_Fortigate_FW(內網) 2.11 Hontai_IBM AIX_DB 2.12 Hontai_Imperva X2010_WAF 2.13 Hontai_PaloAlto_FW(外網) 2.14 Hontai_Symantec_AV
	服務內容說明： 1.資安監控 SOC 服務每週 7 天每天 24 小時每年 365 天(7x24x365)。 2.高風險資安案件四小時內通報及後續追踪。 3.資安事件熱線協助處理。 4.輔導協助入侵案件排除。 5.資安監控 SOC 服務不限次數資安電話諮詢服務。 6.每月提供「SOC 詳細中文電子案件報表」。 7.每年提供：4 次 SOC 季簡報會議，並每年提供一次 SOC 年度彙整簡報、SOC 年度彙整中文電子案件報表。 8.提供中文 Web 網站登入案件查詢服務。 9.資安事件依威脅性自動區分從低至高風險為第一、二、三、四級，並依約定方式 7x24 快速通報緊急聯絡人（手機、簡訊、mail)。 10.資安監控 SOC 服務不定期 email 重大資安資訊及新公佈重要弱點提醒。 11.專案期間提供專屬工程師。 12.資安事故緊急回應服務(ERS)到場最多 3 次。

	13.全域曝險偵測服務，從網際網路端發動主動偵測，持續識別企業外部服務的系統弱點、漏洞等。
二、	WAF iMperva X2010 設備一台，甲方設備。
	1.iMperva WAF X2010 一台，如故障無法維修，原廠於 2022/10/25 已 EOSL(End of Service Life），汰換費用另計。 2.提供每季人力到場設備維護、檢視及技術諮詢。 3.提供不限次數每週上班 5 天 x 每日 8 小時電或、eMial 技術支援服務。 4.原廠已 EOSL 無法提供的服務，如不含備品機服務、原廠開 Case、漏洞修補、版本升級等。
三、	Cisco Firepower IPS 2110 一台，甲方設備。
	1. Cisco Firepower IPS 2110 一台保固，硬體序號：JMX2313Y05J。 2. 訂閱防護授權 3 年：Defense Threat、Malware & URL。 3. 升級中央管理平台 FMC-KVM-2-K9 一式於甲方的微軟 HyperV 虛擬環境。 4. 保固維護服務含原廠 MA 升級三年保固。 5. 提供每季到場設備維護、檢視及技術諮詢。 6. 提供不限次數每周上班 5 天 x 每日 8 小時電話、技術支援服務。 7. 服務期內設備故障送修，次工作日可提供備品機(含安裝服務)。
四、	Silicom IBS1UP-US 4 網段 Bypass Switch 一台，甲方設備。
	1. Silicom IBS1UP-US 4 網段 Bypass Switch 一台保固，主機序號:2010195806。卡版序號：2011162515、2011162516、2011162517、2011162518。 2. 三年保固維護服務含原廠 MA 升級三年保固。 3. 提供每季到場設備維護、檢視及技術諮詢。 4. 提供不限次數每周上班 5 天 x 每日 8 小時電話、技術支援服務。 5. 服務期內設備故障送修，次工作日可提供備品機(含安裝服務)。
五、	託管式偵測及回應服務(MDR)60 台主機，需搭配 SOC 服務。
	1.保固維護服務含原廠 MA 升級保固。 2.提供 Server 版端點 CrowdStrike License*60 個。 3.提供到場安裝教學，軟體採派送安裝。 4.安裝端點軟體主機有「軟體線上自動更新」及「雲端惡意程式分析」。 5.安裝端點軟體主機有「7x24 全年無休之 SOC 遠端監看通報服務」及「遠端資安案件調查服務」。 6.每月寄送 MDR 資安報告電子檔。 7.每季提供 MDR 季簡報會議及季簡報電子檔。 8.每年提供 MDR 年度簡報電子檔。 9.提供 24 小時資安案件諮詢專線。 10.提供中文 Web 網站登入案件查詢服務。
六、	付款方式:均分三年三次，每年 3 月開、寄發票，月結 30 天。