資安 SOC 監控服務與資安相關設備維護三年規格及建議廠商

一、資安 SOC 監控服務與資安相關設備維護三年規格

服務期間	民國 113 年 01 月 01 日至 115 年 12 月 31 日
說明	產品名稱/規格
一、	SOC 資安監控服務三年
	1.本案廠商提供設備： [監看標的]現況 13 台，可增至 15 台 2.宏泰設備： 2.1 外網防火牆(PA820x1) 2.2 內網防火牆(FTG301E) 2.3 AD Server 2.4 外部 DNS Server 2.5 內部 DNS Server 2.6 防毒主機(賽門鐵克) 2.7 Hontai_IBM 2.8 Hontai_Cisco 4503_Switch(1) 2.9 Hontai_Cisco 4503_Switch(1) 2.10 Hontai_AD_bolemei(tec-fweb) 2.11 Hontai_AD_tec-dbs(DB) 2.12 iMmperva DAM VM150 2.13 Cisco Firepower IPS 2110
	服務內容說明： 1.全天候每週 7 天每天 24 小時每年 365 天(7x24x365)遠端監看資安事件。 2.四小時內高風險資安案件通報及後續追踪。 3.資安事件熱線協助處理。 4.協助輔導入侵案件的排除。 5.SOC 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.提供客戶中文 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.SOC 不定期 mail 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。

二、	WAF iMperva X2010 一台，甲方設備。
	1.甲方設備故障汰換費用另計。 2.提供每季人力 1 次例行到場設備維護檢視及技術諮詢。 3.提供不限次數每周上班 5 天 x 每日 8 小時上班時間技術支援。
三、	Log Server NP-RPT-B-TW-EOJN 一台，甲方設備。
	1.甲方設備故障汰換費用另計。 2.提供每季人力 1 次例行到場設備維護檢視及技術諮詢。 3.提供不限次數每周上班 5 天 x 每日 8 小時上班時間技術支援。
四、	IPS Cisco Firepower 2110 一台，甲方設備。
	1.甲方設備 Cisco Firepower 2110 一台三年保固、Cisco Firepower Management Center for VMware7.0.1.1 一台 DELL R640 三年保固。 2.保固維護服務含原廠 MA 升級三年保固。 3.提供每季一次例行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 小時上班時間技術支援及維修服務。 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、	Silicom IBS1UP-US 4 網段 Bypass Switch 一台，甲方設備。
	1.甲方設備 Silicom IBS1UP-US 4 網段 Bypass Switch 一台三年保固維護服務含原廠 MA 升級三年保固。 2.提供每季一次例行到場設備維護檢視及技術諮詢。 3.提供不限次數每周上班 5 天 x 每日 8 小時上班時間技術支援及維修服務。 4.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)。
六、	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 版端點軟體 CrowdStrike 或同等級含以上 License*60 個。 3.提供到場安裝教學，軟體採派送方式安裝。 4.安裝端點軟體主機享有「軟體線上自動更新」及「雲端惡意程式分析」。 5.安裝端點軟體主機皆享有「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.每月寄送上月「MDR 資安案件報告電子檔」。 7.每季提供一次 SOC 季簡報會議及季簡報電子檔。 8.每年提供一次 SOC 年度簡報電子檔。 9.提供 24 小時資安案件諮詢專線。 10.提供客戶專屬帳密登入之中文資安案件查詢網站。 11.資安事故緊急回應服務(ERS) by Case 另計費用。
七、	付款方式:總價均分三年 12 期，按季付款，於每季首月開寄發票，月結 30 天。