中華民國人壽保險商業同業公會

114年保險科技運用共享平台

「資通安全威脅偵測管理(SOC)委外服務案」

需求規格書（7月至12月）

中華民國113年12月

壹、 專案概述

一、 專案名稱

114 年保險科技運用共享平台「資通安全威脅偵測管理(SOC)委外服務案」(以下簡稱本案)。

二、 專案目標

期透過本案提供本會監控環境部署、資安監控服務、資安事件處理及資安威脅偵測管理機制等 4 項資安服務。

(一) 提供資安監控所需之資料收集器部署服務。

(二) 提供每週 7 日、每日 24 小時全天候即時遠端監控服務。

(三) 對於資安監控範圍之資安事件，進行事件應變、事件分析及追蹤等。

(四) 蒐集國內外資安組織之資安威脅資訊，即時提供資安預警通報與建議防護措施。

三、 專案範圍

(一) 為本案之資安監控範圍，監控範圍說明詳見下文「表 1 監控範圍清單」所示。

(二) 資安監控範圍應納入「資通安全責任等級分級辦法」應辦事項之「資通安全防護」辦理項目、端點偵測及應變機制(EDR)及核心資通系統等之資通設備紀錄與資訊服務或應用程式紀錄。

四、 專案期間

自簽約日至 114 年 12 月 31 日止。

貳、 專案工作項目

本案主要工作包含監控環境部署、資安監控服務、資安事件處理及資安威脅偵測管理機制等，分別描述如下。

一、 監控環境部署

(一) 監控範圍

SOC 監控範圍應納入「資通安全責任等級分級辦法」應辦事項之「資通安全防護資通安全防護」辦理項目、進階持續性威脅攻擊防禦措施(APT)、端點偵測及應變機制(EDR)及核心資通系統等之資通設備紀錄與資訊服務或應用程式紀錄。

表 1 監控範圍清單(本會保留監控範圍項目異動之權利(新增/刪除/修改)。

序號	監控範圍項目	項目說明	數量
1	網路防火牆	分析網路連線異常行為，防範服務過載、訊息洪流、DoS阻斷服務及違反網路阻斷機制行為	**4**
2	入侵偵測及防禦機制(IDS/IPS)	▪網路型 IPS/IDS 即時監控及攔阻本會各網段異常傳輸的封包，透過檢查網路封包內容的方式，防範入侵行為。 ▪主機型 IPS/IDS 分析重要主機與應用系統上的一些日誌檔案或目錄，透過檢查主機上檔案目錄的狀態機密性、可用性與完整性，防範入侵行為(如保護程式/程序/檔案/目錄/資料，不被非授權存取、竊取、破壞、篡改與置入等)。	**4**（內建於網路防火牆）
3	應用程式防火牆(WAF)	偵測與防護網際網路 Web 應用程式攻擊行為，如 OWASP 公布之攻擊等(如 XSS、Injection Flaws 等)。	**2**
4	本會之核心資通系統	▪監控本會核心資通系統異常事件，防範非授權/異常存取、不當使用、竄改、置入惡意程式等。 ▪若為網站應用系統，監控網站異常事件，防範如網頁遭置換、網頁遭置入惡意程式與惡意留言等。	**一式**
5	端點偵測及應變機制(EDR)	▪將感應器和回應功能置於端點處，能夠在駭客進行攻擊時加以識別及阻止。 ▪結合監控、分析、報告、回應和取證等防禦措施。	**139**

6	防毒軟體	整合機關防毒系統(如防毒伺服器，防毒閘道器)以其日誌。 ▪ 資料分析風險之監控防護。	**139**

(二) 資料收集器部署

1. 資料收集器(Data Acquisition)需可從不同資安設備透過 SYSLOG、SNMP、SMTP 或特定的方式與傳輸格式，將事件紀錄主動或被動傳輸至資安監控中心予監控系統進行分析。(資料收集器功能要求，詳見附件 2)。
2. 資料收集器的部署工作包括網段部署、安裝、設定、系統調校及重要資安事件 Rule 導入等。
3. 廠商發現事件收集設備故障，必須於 24 小時以內修復完成或調換同等級以上之相容設備。(註：小時數皆為日曆天) 。
4. 全年故障次數、總時間與搶救恢復時限作為指標，一般全年故障次數不可超過 5 次，故障總時間不可超過 52 小時，每次須於 24 小時內完成修復。

(三) 部署作業

1. 簽約後 14 日曆天內，勘查本會現有網路環境與需求，交付「資安防護監控部署建議報告」。
2. 「資安防護監控部署建議報告」經本會認可後，須於時限內完成資安設備與資料收集器部署作業，所部署之資料收集器不得影響各項資安設備與整體監控系統之正常運作。項目完工時，須由本會及得標廠商相關負責人雙方簽字認可，全部完成後須函請本會召開查驗會議。

二、 監控服務

(一) 得標廠商應設置資安監控中心(以下簡稱 SOC)，提供本專案資安監控服務。得標廠商之 SOC 須符合下列規定：

1. SOC 須提供每週 7 日、每日 24 小時全年無休即時遠端監控服務。
2. SOC 需於國內實際運作，並有每日 24 小時全年無休之專職輪班人員。得標廠商應提供專職輪班人員名冊及聯絡方式予本會，人員異動時亦須知會。
3. SOC 機房應具備門禁、監控、錄像、空調、防火/煙、機電等安全設施。監控系統須具備加密、備份及備援機制，且須配備資安軟硬體設備以維資料安全。
4. 本會得視需要派員前往 SOC 實地查訪,以確認符合本文件規範要求。

(二) 建立監控事件處理暨追蹤管理平台

1. 廠商應提供事件監看平台畫面,予本會人員能透過網頁查詢事件分類、事件通報、事件處理、事件管理、日誌紀錄及相關資安統計圖表。
2. 監控過程之通報事件須可自動轉入追蹤管理平台，
3. 事件通知流程可設定每個不同的事件狀態皆可通報給不同的對象。
4. 配合本會作業流程或管理制度，導入事件處理流程及處理標準程序。

(三) 監控事件處理

工作內容如下：

1. 監控過程中所有資安事件之即時處理追蹤。
2. 協助本會資安事件緊急應變處理及後續矯正預防事宜。
3. 隨時監控資訊儀表板內容並提供資安防護作業相關分析報表。
4. SOC 服務資安相關設備日常管理維護調校及緊急故障排除。
5. 協助處理資安政策變更時,相關軟硬體資安組態設定及版本異動作業。
6. 須進行受駭之原因分析和影響範圍之確認，並協助本會將資安事件造成的漏洞關閉，以避免進一步的擴散。
7. 每日須提供監控服務工作紀錄(包括監控紀錄、事件處理紀錄、事件追蹤紀錄及其他資訊業務需求紀錄等)以電子郵件寄予本會資安聯絡人。

(四) 監控中心之監控與事件通知

1. 廠商收集日誌後，透過資安監控機制進行整合與關聯，產生資安監控相關文件。
2. SOC 分析人員對資安監控相關文件進行影響性評估，並產生「情資分析相關文件，廠商應即時以適當方式(以電話、手機簡訊、電子郵件、網頁、傳真等)通知本會資安聯絡人，俾利本會進行情資處理。

(五) 資安事件通知

1. 分析監控事件針對如下項目，應即時通知(以電話、傳真、手機簡訊、電子郵件擇一方式)本會資安聯絡人。
   (1) Intranet 與 Internet 疑似入侵個人電腦、伺服主機、本會網站及網路設備之行為。
   (2) 植入惡意程式或竄改電腦設備之設定、紀錄，隱藏足跡，進行側錄鍵盤或畫面、竊取資訊、或將受駭電腦設備作為跳板攻擊其他電腦系統等行為。
   (3) 可能造成資料外洩或占用本會頻寬之連線行為。
   (4) 非法（如刺探、攻擊及入侵等）來源 IP、非法存取目的之連線行為。
   (5) 短時間內被防火牆重複阻擋之連線行為。
   (6) 持續之網路及主機刺探掃描行為。
   (7) 與惡意中繼站 IP 或已知黑名單 IP 之連線行為。
   (8) 帳號建立、刪除及特殊權限變更行為。
   (9) 非正常存取伺服主機或個人電腦行為。
   (10) 依據電子郵件系統可提供之紀錄加以分析，提供利於管理者判讀之電子郵件信箱使用者異常登入行為報表與警訊。
   (11) 監控標的之程式/程序/檔案/目錄/資料，被非授權存取、竊取、破壞、篡改與置入等異常行為。
   (12) 感染惡意程式、感染病毒或惡意程式行為。

(13) 特殊權限帳號異常登入。

通知內容至少應包含事件發生時間、風險等級、攻擊方法與路徑分析，以及相對應緊急應變措施建議。

(六) 監控服務報告

每月/季 15 日前廠商得以電子郵件提供上個月/季之監控事件統計、資安監控服務狀況等中文化報表予本會，協助本會管理者瞭解現行網路用戶之使用情形，監控中心應定期提供月報、季報予本會，而其應依資通安全責任等級分級辦法之相關規定提交監控管理資料，月報/季報內容參考附件 1。

三、 資安事件處理

(一) 廠商依據「資通安全管理法」與「資通安全事件通報及應變辦法」規定判斷監控事件是否為資安事件。

(二) 當資安事件發生後，本會除依廠商通知內容之應變措施處置外，可要求廠商派員至本會協助事件處理，廠商應於接到通知後 4~6 小時內派員至本會，廠商不得拒絕。

(三) 廠商於收到資安日誌並判斷為高風險以上之資安事件時，應於 60 分鐘內進行事件分析及通報。

(四) 資安事件處理工作範圍包括：

1. 廠商必須進行受駭之原因分析和影響範圍之確認，並協助本會將資安事件造成的漏洞關閉，以避免進一步的擴散。
2. 檢測疑似被入侵之主機系統，針對系統資訊、日誌檔及惡意程式進行蒐集，日誌檢視以一年為原則(含線上與離線日誌)。
3. 針對蒐集的資訊進行證物保存、磁碟映像檔分析、惡意程式分析及網路流量分析。以動態或靜態方法分析惡意程式功能，瞭解駭客入侵之主要目的。
4. 將磁碟映像檔、惡意程式及網路封包等分析結果加以彙整進行關聯分析，以研判駭客入侵手法與時間、影響範圍及威脅程度等。

(五) 廠商須於資安事件通知後依合約約定之工作日內提出資安事件處理報告，其內容應包含事件發生時間、來源與目標 IP、駭客所在位置、攻擊方法與路徑及影響分析，以及系統復原、事件排除、修補及防禦等措施建議(包括系統重新安裝與設定、系統隔離修護、調整防火牆、更新系統安全或防毒軟體修正檔、弱點修補或新增防禦設備等建議)，以提供予本會設置防禦措施。

四、 資安威脅偵測管理機制

依「資通安全責任等級分級辦法」第 11 條及附表二之規定，本會應依規定完成資安威脅偵測管理機制建置，並持續維運。

(一) 資安威脅預警服務範圍為廠商發現及蒐集國內外資安組織之資安威脅情資，至少包括：

1. 病毒資訊警訊：如趨勢科技及 Symantec 等防毒廠商中級以上病毒警訊。
2. 系統弱點公告：如 NCCST、Microsoft、SecurityFocus、各國 CERT 等國內外資安組織公告。
3. 網頁攻擊資訊：如 Zone-H、OWASP 資安組織公告等。
4. 新聞事件：如 CNN、Google 及 Yahoo 等國內外資安新聞。
5. 廠商發現之威脅：如 Zero-Day 事件。

(二) 國內外資訊安全威脅發表後 3 日，廠商應整理相關訊息於資安入口網站，並以電子郵件通知本會，廠商提供資安威脅預警通報服務，內容包括：資訊安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資訊安全漏洞與補救措施、資訊安全事件報導、漏洞分析、修補方式或對策。

(三) 廠商提供之警訊通報內容以中文為主。

參、 管理需求

一、 廠商資格

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述：

(一) 凡在政府機關登記合格，無不良紀錄之廠商（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。專案人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

(二) SOC 服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。

(三) 投標廠商須實施資訊安全管理制度，通過 ISO 27001:2022、ISO 27701:2019、ISO 20000:2018 或其他類似驗證，並於專案執行期間持續有效，以保護資安監控所取得之資料。

(四) SOC 服務涉及資通訊軟體、硬體或服務等相關事務，不得提供及使用大陸廠牌資通訊產品，服務如涉及使用雲端工具，應確保本會利用服務之所屬一切資料存取、備份、及備援之實體所在地，應為我國管轄權所及之境內。

(五) SOC 服務團隊人力要求

1. 服務人員須年滿 18 歲以上，身體健康無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士，於履約期間不得同時於大陸地區工作。
2. 專案人員應包含專案負責人/專案經理與技術人員（如監控維運、資安事件處理人員）。每位技術服務人員應具備以下專業要求，擇 1 證照，以確保服務水準，並於建議書中檢附成員姓名、員工證明(如勞健保證明)、專業證照等影本以供審核。
3. 每位技術人員依服務項目應具備專業要求，擇 1 證照。

(1) SOC 監控：擇 1 證照

- CEH(EC-Council Certified Ethical Hacker)。
- CND(EC-Council Certified Network Defender)。
- CSA(EC-Council Certified SOC Analyst)。
- CTIA(EC-Council Certified Threat Intelligence Analyst)。
- CySA+(CompTIA Cybersecurity Analyst)。
- 其他資安相關專業證照。

(2) 資安事件處理：擇 1 證照

- CEH(EC-Council Certified Ethical Hacker)。
- CHFI(EC-Council Computer Hacking Forensic Investigator)。
- CND(EC-Council Certified Network Defender)。
- ECIH(EC-Council Certified Incident Handler)。
- ECSA(EC-Council Certified Security Analyst)。
- 其他資安相關專業證照。

二、 服務水準規範協定(SLA)與罰責

(一) SOC 服務各項服務水準協定（Service Level Agreement，SLA），以必須達成該項工作服務項目要求為依據，透過客觀的證據或指標，做為品質管制，以預防各項不符合作業的事項發生，降低委外作業的風險，詳細服務水準規範如下表：

項次	項目	服務水準	未達水準罰則	罰則說明
1	監控環境部署	依專案作業時程要求佈署完成資安防護監控機制 ▪ 簽約後2個月內完成部署，且每一項目之可用性與設定調整須通過本會測試。 ▪ 監控設備造成本會網路系統作業中斷或嚴重流量阻塞達 30 分鐘，發生達 3 次則更換同等級以上效能較高之設備。 ▪ 資安設備與資料收集器安裝故障，必須於 24 小時內修復完成或調換同等級以上之相容設備。	扣2點	若服務水準持續未達成，每1日扣2點

		▪ 監控設備全年故障/中斷次數不超過 5 次，故障總時間不超過 52 小時。未達全年服務水準扣 5 點。 ▪ 若非歸究於乙方之責任時,則不列入計算。		
2	監控服務	1.本專案為 7x24 小時全天候監控 ▪ 整體監控服務中斷超過 4 小時後，每逾 4 小時扣點。 ▪ 單項監控服務中斷超過 8 小時後，每逾 4 小時扣點。 ▪ 若非歸究於乙方之責任時,則不列入計算。 2.資安事件通知 ▪ 監控系統須能偵測入侵事件。若經本會入侵行為測試、本會「攻防演練」或遭入侵，監控系統未能發現者則扣 2 點。 ▪ 得標廠商在資安事件發生時,於即時進行資安事件通知。若服務水準未達成每單一事件扣點。	扣 1點	依事件日誌與監控設備維運日誌，列舉相關事實
3	資安事件處理	▪ 廠商於收到資安日誌並判斷為高風險以上之資安事件時，應於60分鐘內進行事件分析及通報。 ▪ 資安事件完成緊急處理並於資安事件管理平台回報後，應於14個工作日內提出含案件資訊、攻擊手法、修補防禦等措施建議的事件調查報告。 ▪ 資安事件單紀錄及附件日誌紀錄保存，須異地備份，日誌保存以五年為原則(含線上與離線)。若因單一事件延誤通報導致事件擴散則扣點。	扣 2點	經本會主管核可，每項缺失扣 2 點
4	資安威脅偵測管理機置	▪ 資安威脅情資發布後,3日內由廠商執行資安威脅預警通報，含建議設置之防禦措施並做成通報紀錄隨月報寄送。	扣 1點	經本會主管核可，每項缺失扣 1 點

(二) 相關說明：

1. 承作廠商無法達成相關工作項目服務水準，SLA 罰則依每期付款時結

算，其罰款(違約金)計算方式為每期罰則點數x契約總價千分之一。工作項目如遇有重複計罰狀況，以罰則較高者為準。

2. 應交付之項目或文件，如有超過完工交付期限，每延遲 1 日(以日曆天計，星期日、國定假日及其他休息日均應計入，不滿 1 日以 1 日計算)，本會得按契約總價之千分之一計算懲罰性違約金，款項可自契約總價或履約保證金項中扣抵。

3. 違約金上限以契約總價之 20%為上限。如違約金逾 20%時，本會得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。

4. 得標廠商應於議價後所提成本分析中，詳列各項工作項目成本，如於驗收時，經審查發現有不合格之工作項目，得標廠商應依期限予以改正。如未改正，本會有權扣除該項工作之款項。

5. 得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付本會之文件經本會審閱時，所發現錯漏處達 10 處以上，或業經本會要求修訂仍未修訂者，本會得按每字新台幣 500 元計算懲罰性違約金，並自付款項中扣抵；其有不足者，得通知廠商繳納或自履約保證金扣抵。

三、 品質需求與驗收標準

(一) 品質需求

1. 為確保專案如期如質完成，廠商應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。

2. 得標廠商訂定品質管理流程，本會得以稽核。

3. 得標廠商於專案期間應辦理啟始會議與結束會議，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本會備考。

4. 得標廠商於本專案服務使用之工具軟體，均應出具合法授權之證明。

(二) 驗收標準

得標廠商應依貳、專案工作項目之服務需求，以及符合服務水準協定(SLA)中所列事項，完成專案工作，並依本說明文件所訂之交付時程，完成相關文件與紀錄之交付。

(三) 驗收方式

依據實際建置計畫與設備，詳細規劃驗收流程與測試項目，由本會審查通過後據以進行測試及驗收。廠商依履約所供應或完成之標的，將符合契約相關規定，具備一般可接受之專業及技術水準，無減少或滅失價值或不適於通常或約定使用之瑕疵，且為新品。

廠商應依進度完成各期工作，交付有關工作項目成果或文件通知本會辦理驗收，本會應於接獲承包廠商交付之成果或文件，兩星期內函送審查結果，如有問題，承包廠商應於接獲通知，兩星期內完成修正並函送本會辦理複驗。

四、 業務保密安全責任

(一) 廠商基於 SOC 服務需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽定保密協議書。

(二) 廠商對特別以文字標示或口頭明示為機密資料者，非經本會書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，廠商應負完全責任。

(三) 廠商對於可能接觸與 SOC 服務相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書。

(四) 契約終止時，廠商應將有關 SOC 服務過程中處理之任何形式資訊，整理歸檔後退還本會或經本會同意後銷毀。

(五) 履約期間造成保密及安全事件，得歸咎於廠商之責任時，廠商應負所有法

律及賠償責任。

(六) 本會對廠商保留實地稽核權，以確保廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

肆、 得標廠商應交付項目

一、 交付項目與時程

(一) 履約保證金：決標日起 2 週(日曆天)內交付新臺幣貳拾萬元整。

(二) 工作計畫書：決標日起 2 週(日曆天)內交付。

(三) 資安防護監控部署建議報告：依工作計畫書載明之交付時程。

(四) 監控服務(月)報告：每月 15 日前。

(五) 資安事件處理報告：依合約規定。

二、 交付文件格式

(一) 監控服務(月/季)報告以電子郵件方式提供，其他各項文件應提供電子檔 1 份(以光碟或本會同意之儲存媒體及提交方式)。

(二) 必要時本會得要求派員親臨說明。

三、交付項目說明

交付項目	內容說明
工作計畫書	▪ 工作計畫書應以廠商投標時之「建議書」為基礎，並依採購評選意見修改 ▪ 內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、工作項目、時程說明、工作進度稽核點及品質管理流程
資安防護監控部署建議報告	文件內容應包括網路架構現況說明、建議部署之資安設備項目與數量、資料收集器數量及部署作業說明
監控服務報告	事件通知或警訊發布統計、監控與警示系統監控情形、資安事件處理說明、資安威脅預警情形及評估建議改善項目
資安事件處理報告	文件內容應包括事件發生時間、來源與目標 IP、駭客所在位置、攻擊方法與路徑及影響分析，以及系統復原、事件排除、修補及防禦等措施建議

伍、　投標廠商服務建議書製作規定

一、服務建議書格式

(一) 紙張：宜用 A4 規格。

(二) 繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明廠商名稱、廠商地址、本案名稱及日期，裝訂線在左側。

(三) 目次：應標示各章節之出處頁碼。

(四) 廠商投標建議書之份數為 1 式 2 份。

二、服務建議書內容

(一) 專案概述

1. 專案名稱
2. 專案目標
3. 專案時程

(二) 廠商說明

1. 廠商簡介
2. 公司營運狀況，包含參與人員名單、能力證明及廠商經驗說明

(三) 專案計畫

1. 專案服務內容項目
2. 組織與人力配置
3. 專案時程、品質、風險管理與交付項目計畫，包含工作項目、時程規劃及查核點
4. 本案帶來之預期效益
5. 本案 SLA 之承諾

(四) 其它

陸、 附件

- 附件 1 監控月報/季報內容

I. 監控月報/季報內容

A. 事件通知或警訊發布統計

B. 發生事件編號，事件名稱，事件處理結果

C. 持續追蹤的資安事件列表

D. 造成受監控設備停止或受影響時間

E. 受影響 IP 列表

II. 監控與警示系統監控情形

A. 情資分析單處理狀態與數量

B. 本會內員工連接中繼站(IP、DNS)數量

C. 惡意軟體攻擊類型說明與數量

D. 受攻擊服務統計圖表

III. 資安事件處理說明

A. 處理紀錄說明 B. 提供防禦措施說明

IV. 資安威脅預警情形

A. 資安威脅預警公告

B. 資安威脅預警建議

C. 資安威脅預警諮詢

V. 評估建議改善項目

- 附件 2　監控系統應具備之功能

一. 資料收集功能

1. 可依需要於本會暨所屬單位及駐外機構提供資料收集器，集中收納當地相關的資安訊息經加密後，即時將訊息傳回主系統進行分析、監控及應變處理。
2. 可統一收集來自防火牆、IDS/IPS 系統、弱點掃描系統、防毒、防駭軟體、作業系統、資料庫系統等紀錄。
3. 提供被監控納管設備之事件紀錄收集功能。
4. 至少可支援下列訊息傳送的協定：SYSLOG、SNMP、SSH、FTP、 SQL Query 等，並提供未支援格式之解決方案。
5. 可自行定義事件的蒐集格式，以利特定非標準系統的訊息整合。 F.系統可提供即時(Real-Time)及批次(batch)收集資料之功能。
6. 至少可收集下列產品的事件紀錄（除下述系統及設備，未來本專案若有新擴充系統及設備，須可支援該系統及設備事件紀錄之蒐集）：
    i. 作業系統：Sun Solaris、HPUX、AIX、RedHat Linux、 Microsoft、FreeBSD 等。
    ii. 防火牆/VPN：Check Point、Cisco PIX、Juniper、Fortinet、D-Link 等。
    iii. 網路型入侵偵測系統：Juniper、ISS、Cisco、Tipping Point、 McAfee 等。
    iv. 主機型入侵偵測系統：ISS RealSecure Server Sensor、Symantec HIDS 等。
    v. 弱點掃描系統：ISS Internet Scanner、FoundScan 等。
    vi. 防毒軟體：Symantec Norton Antivirus、TrendMicro、Kaspersky 等。
    vii. 路由器：Cisco Routers、D-Link 等。
    viii. 其他：Microsoft IIS、Apache、Netscape Server 及其他安全閘道等。
    ix. 可保留被監控納管元件所產生的原始事件紀錄。
    x. 與其他監控系統設備間資料須利用加密模式傳送，資料傳送時須經過壓縮，確保不會影響本會現行資訊作業。

二. 即時監控功能

1. 系統布建於本會，須採中文化方式的操作界面。
2. 採多層式架構，至少具備事件紀錄收集、資安監控中心管理平台（Manager）、

後端資料庫（DB）及管理介面（Console）。

3. 具備事件紀錄檔標準化功能，可針對不同設備的紀錄檔進行標準化作業，其紀錄欄位至少包括：source ip、destination ip、destination port、source hostname、target hostname、date、time…等。
4. 內建多種事件分類，可將不同品牌(如 Check Point、PIX、 Netscreen)的同類防護設備(如防火牆)針對類似網路活動的紀錄檔進行標準化後，形成標準化單一事件，以便於統一管理。事件之分類亦可由使用者自訂、新增或編修。
5. 可支援備援機制，當主要監控系統發生錯誤時，可由備援系統接手，不影響實際運作。
6. 提供預設的圖形報表查詢，入侵偵測系統的查詢、防火牆系統的查詢及防毒軟體的查詢…等。
7. 可透過客製化設定，只監控某種程度的事件，例如事件攻擊達到自定之次數以上或較重要的設備等，才發出告警或採取自定的反應。
8. 提供圖形化的 LOG 分析功能，可將要查詢的紀錄檔以圖形化來顯示其相互關係。
9. 可即時設定關聯的條件，並能顯現關聯結果。
10. 提供群組權限管理功能，可限制群組觀看、刪除、新增、修改暨權限等，並具備稽核功能，記錄每個使用者的操作情形。
11. 提供遠端圖形化介面管理工具，方便管理迅速管理資訊安全設備。
12. 提供管理介面客製化程式，管理者可以自行編修管理介面，以符合單位之特性。
13. 本系統架構須提供安全的資料傳送通道，提供可採用如 SSL、3DES 或其它加密演算法之加密傳送機制。

三. 進階事件分析功能

1. 具備快速事件分析功能，可呈現事件的視覺化分析圖。

2. 提供客製化或 Script 工具，允許使用者預先訂定針對特定種類事件 (如弱點稽核系統或入侵偵測系統)的交叉分析以產生報表形式（如長條圖、圓形圖或立體圖）。
3. 可以收納上述監控中心系統平台事件檔，進行事後分析。
4. 提供預設的圖表樣板，至少包括：圓形圖、線圖、時間表、長條圖、歷史趨勢圖。

四. 事件關聯分析系統

1. 對於資料收集器回傳的資安事件，可立即透過事件關聯分析系統進行自動化的分析。
2. 除系統內建的關聯分析規則外，可依需求自行定義關聯分析規則。
3. 關聯分析規則至少能分析下列攻擊行為：
    i. 刺探行為
    ii. 弱點掃描行為
    iii. 密碼猜測行為
    iv. 網站攻擊行為
    v. 後門或間諜行為
    vi. 病毒/蠕蟲傳染或擴散行為
    vii. 惡意程式下載行為
    viii. 黑名單位址的連線行為
4. 應支援圖形化的關聯分析規則設定界面，以利規則的調整。
5. 配合本會及駐外機構提供之 VPN 及個人電腦之防護系統相關事件資訊判別攻擊來源屬內部或外部網路，並自動解析攻擊來源的國家，針對攻擊來源可有不同的關聯分析標準。

五. 事件集中儲存及管理系統

1. 所有資安事件包含原始事件紀錄，可集中保存於系統內，且保留 1 年以上的資料量。
2. 原始資料須以壓縮方式保留，以免佔據太多磁碟空間。

3. 可設定自動刪除過期資料區間，以避免資料滿載而造成系統無法運作，提供再確認功能為佳。

六. 資安案件管理

1. 資安事件經關聯分析確認為異常行為時，可透過本系統來進行案件管理。
2. 內建流程引擎可自行透過圖形化的界面，設定資安案件管理的流程及簽核層級。
3. 可自行設計各類表單及其對應的自動化流程。
4. 內建權限控管的設定，相關的資安事件及案件只能允許相關人員查看或回應。
5. 案件的通報等級，可以依據資產的重要性自動調整，當重要的資產遭受攻擊時，可發送較高等級的通報。
6. 可支援地圖顯示功能，將資安案件發生的區域透過地圖的方式來展示。

七. 資安入口網站

1. 使用者可利用瀏覽器或 GUI 方式登入。
2. 具資產選取功能，使用者自資產樹狀結構選取欲檢視之項目後，即顯示對應的資安事件資料。
3. 根據使用者權限，限制其所能檢視與選取的資產。
4. 具時間選取功能，使用者選擇事件顯示的時間範圍
5. 具事件過濾功能，使用者可依事件來源 IP、時間、事件名稱與類型、嚴重性、目標 IP、TCP 或 UDP 埠編號等條件篩選檢視的事件。
6. 資安事件檢視需包含來源 IP、目的 IP、事件名稱、事件日期、事件時間、TCP 通信埠、UDP 通信埠...等欄位。
7. 使用者可選取預設檢視視窗的任意列項目後，展開該列對應之詳細事件列表。
8. 詳細資料顯示功能，使用者點選事件名稱欄位後，可顯示其事件對應之說明、

改善措施與管理者上載之改善修補檔案程式。

9. 具有權限控管功能，可區分系統管理員與一般使用者可使用之功能。並可個別定義各主機或主機群組資料的存取權限。
10. 可依據監控設備設定其對應的使用者權限。

八. 資安新聞台

1. 資安監控中心可透過資安新聞台來發佈資安訊息及資安預警通報。
2. 資安新聞可自訂新聞分類。

九. 案件追蹤管理功能

1. 使用者登入系統時，須能自動顯示待處理案件。
2. 須具有可依序傳遞表單給多名使用者，表單具有資料欄位、輸入欄位（供特定使用者輸入資料）以及系統欄位（系統填入之資料，不允許使用者變更）等功能，並可連結其他檔案。
3. 可預先設定流程步驟、各步驟對應的動作與對應的使用者成為流程範本。
4. 可依據事先規範之作業流程傳送案件，於案件追蹤系統中查詢與管制，並提供管理統計報表，所提供之作業流程至少包括：
   A. 資安通報流程。
   B. 資安報表流程。
   C. 緊急應變流程。
   D. 資安聯防流程。
   E. 案件開啟時，須可提供螢幕顯示、電子郵件、手機簡訊(SMS)等警示機制之通報功能，通知本會資安人員或其他相關人員，並能記錄通報時間及對方回應時間。
   F. 須具備案件逾時未處理之告警機制，包含通知本會資安監控中心維運人員、代理人及其主管。
   G. 已開啟案件之資安事件，須可於監控視窗進行標示或提供過濾功能。

十. 報表管理功能

1.
2. 為進行入侵事件快速分析及後續處理，系統需提供詳細的智識庫，針對本會資安監控中心所發出之攻擊警訊，可詳述事件的攻擊方式、攻擊型態、嚴重性、如何回應、受影響平台及修復弱點等相關資訊。
3. 為資訊作業自動化，並簡化報表製作過程，系統具備自動排程產生報表之能力，，並以電子郵件附檔方式寄送給自訂的相關管理人員或群組。
4. 為配合資訊稽核需求，可針對報表指定以符合時間區間、來源 IP 區間以及目的 IP 區間等過濾條件之事件資料進行報表之製作。
5. 中文化資訊安全管理報表需提供 TOP N 攻擊來源、TOP N 目標主機、TOP N 事件。
6. 報表可依據本會稽核需求，統計案件處理數據。
7. 報表可輸出成多種格式，至少包含 Word、HTML、PDF 等格式。

十一. 容錯與擴充機制

1. 本專案資安監控中心系統及資料庫應規劃提供 Active-Backup 或 Active-Active 容錯機制，以提供 7 X 24 （全天候）系統持續運作的能力。

十二. 本專案範圍內所提供相關之管理平台及報表，得標廠商皆須提供中文化之平台介面。