

共同供應契約電腦軟體標 (案號：LP5-100011)			
廠商編號	11-LP5-8930	廠商名稱	安碁資訊股份有限公司
組別	項次	產品名稱	契約金額
六	114	SafeCove 資安事件監控及分析系統 (2 個 Device 授權)	620,126

## SafeCove 資安事件監控及分析系統(2 devices)

### 資訊安全環境評估－發掘潛在的問題

	一般MIS的資安管理思維－冰山的一角	
	監控交通流量	巨觀的管理觀點，能得知異常行為發生（如流量暴增），但無法得知問題的來源
	建置防毒系統	可監控已知病毒防禦狀況，但無法得知變種或新種病毒肆虐
	導入 FW, IDS, IPS	<b>FW:</b> 通聯記錄量大，不易進行實務運用，僅能建構既定之交通流量政策 <b>IDS:</b> 僅能測知已知型態之攻擊行為 <b>IPS:</b> 阻擋誤判率高，可能阻擋正常行為
掌控網路行為模式的新思維－凸顯問題全貌		
同時監控重要設備	基於設備間關聯性經驗智慧，蒐集分析防火牆與IDS間跨時間、跨設備的行為線索	
研判合理網路行為	組構網路行為，研判行為模式之合理度，推論篩選問題	
鑑識問題追蹤來源	追蹤問題癥結與來源，鑑識攻擊手段	
定義防禦政策手法	對症下藥，補強防禦政策與網路架構，設計有效之防禦手法	

### 產品簡介

SafeCove 資安事件監控及分析系統，可以提供防火牆、入侵偵測系統、入侵防禦系統的資安事件監控及分析統計報表。透過 SafeCove 資安事件監控及分析系統，可以將防火牆、入侵偵測系統、入侵防禦系統所產生的資安日誌，以系統化的方式進行收集、關連性分析後，定期產生週報表，提供給客戶作為資訊安全的管理依據。

### 產品說明

項目	內容說明
<b>產品功能</b>	
分析功能	<ul style="list-style-type: none"> <li>● Firewall/IDS/IPS 週報表 (PDF 格式)</li> <li>● 透過 email 發送</li> <li>● Firewall 週報表內容包括：               <ul style="list-style-type: none"> <li>+ Firewall 每日連線數量統計圖</li> <li>+ Firewall 每日通過連線數量統計圖</li> <li>+ Firewall 每日阻擋連線數量統計圖</li> <li>+ Firewall 通過連線主機分析</li> <li>+ Firewall 阻擋連線主機分析</li> <li>+ Firewall 通過目標 Port 分析</li> <li>+ Firewall 阻擋目標 Port 分析</li> </ul> </li> <li>● IDS/IPS 週報表內容包括：               <ul style="list-style-type: none"> <li>+ IDS/IPS 每日事件量統計圖</li> <li>+ IDS/IPS 觸發事件分析</li> <li>+ IDS/IPS 連線來源主機觸發事件分析</li> <li>+ IDS/IPS 連線目標主機觸發事件分析</li> </ul> </li> </ul>
Firewall 監控功能	<ul style="list-style-type: none"> <li>● 木馬/後門程式/惡意程式/新種病毒</li> <li>● 網路蠕蟲活動偵測</li> <li>● P2P 行為偵測</li> <li>● 惡意中繼站連線</li> <li>● 異常流量偵測</li> <li>● 網路掃描刺探 (外對內 -- 內對外)</li> <li>● 阻斷服務攻擊 (外對內)</li> </ul>
IDS/IPS 監控功能	<ul style="list-style-type: none"> <li>● 大範圍外部攻擊行為</li> <li>● 木馬/後門程式活動偵測</li> <li>● SQL Injection 行為偵測</li> </ul>
<b>資安事件協助處理</b>	
遠端桌面協助	<ul style="list-style-type: none"> <li>● 點數卡 (有效期一年)</li> <li>● 提供客戶資安問題協助</li> <li>● 惡意程式採樣, 快速蒐集可疑檔案樣本</li> </ul>
現場協助處理	<ul style="list-style-type: none"> <li>● 點數卡 (有效期一年)</li> <li>● 5x8 電話通知, 隔日到場</li> <li>● 工作內容：               <ul style="list-style-type: none"> <li>+ 資安事故設備隔離程序</li> <li>+ 找出並排除可疑惡意程式</li> <li>+ 找出可疑入侵手法或被駭途徑</li> <li>+ 系統回復</li> </ul> </li> <li>● 每次啟動至少 4 小時 (到府起算), 不足 4 小時以 4 小時計</li> </ul>
<b>技術支援</b>	
資安問題諮詢	<ul style="list-style-type: none"> <li>● 5x8 線上 (電話/電子郵件) 提供客戶資安問題諮詢</li> <li>● 客服電話：0800-286-009</li> </ul>

## 產品授權

產品名稱	授權數量	點數卡
SafeCove 資安事件監控及分析系統	提供客戶現有資安設備 2 台之監控及分析報表	<ul style="list-style-type: none"><li>● 遠端桌面協助 20 次</li><li>● 現場協助處理 20 小時</li></ul>

## 交付項目

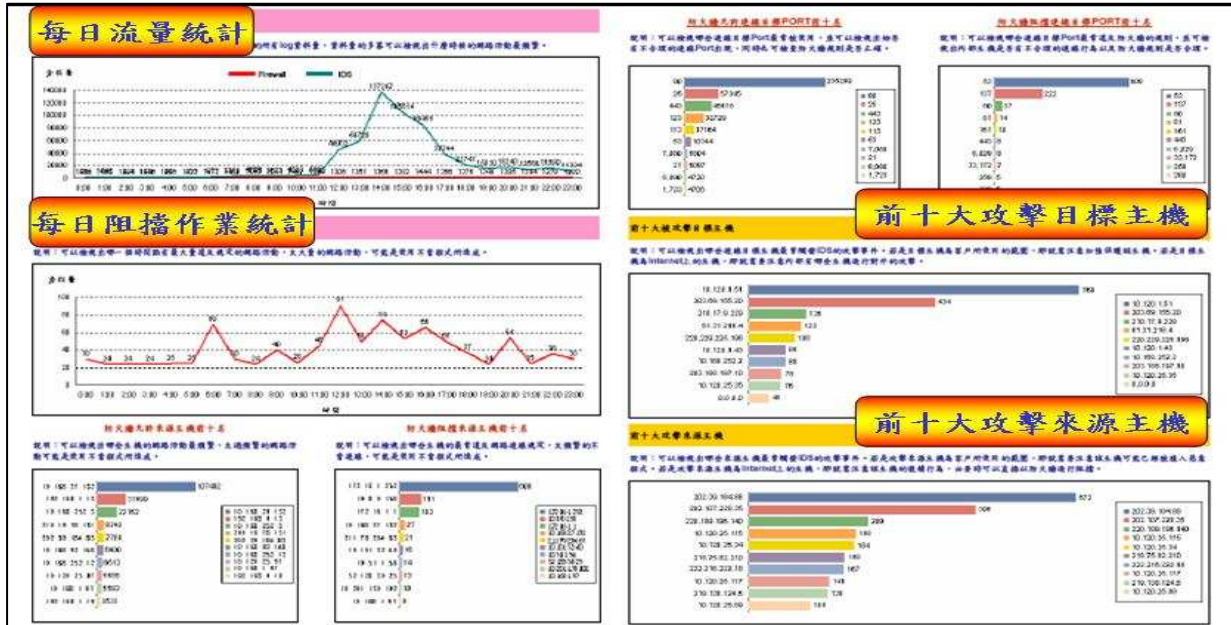
- SafeCove 資安事件監控及分析系統一套
- 遠端桌面協助點數卡
- 到場協助處理點數卡

## 預期效益

- 定期獲得專業整體資安事件報表，作為制訂安全政策的管理依據
- 建立有效的主動式防駭安全機制
- 資安事件發生時，可以儘快找出事件來源，以便有效防範事件擴散
- 獲取早期預警通知，有效防制新的資安威脅

## 報表範例

Firewall 週報表	說明
Firewall 每日阻擋連線數量統計圖	違反 Firewall 安全設定政策而遭阻擋的網路連線活動，可能為外部刺探、內部主機設定錯誤，或是異常程式所造成。大量阻擋的連線行為會造成 Firewall 的負載增加。
Firewall 通過連線主機分析	<ol style="list-style-type: none"> <li>1. 連線來源主機排名： 對於允許連線數量頻繁之內部來源主機，應檢視活動的頻繁度是否符合該主機應有之營運型態。</li> <li>2. 連線來源主機排名↔依目標主機（含目標 Port）： 依據 Firewall 的前十名允許連線來源主機，以及每個來源主機各自連往哪些目標主機的連線數量前十名排行，可以瞭解前十名來源主機的主要連線對象，並進一步分析其連線之目的與可能之應用型態。</li> <li>3. 連線來源主機排名↔依目標 Port： 調查 Firewall 允許連線的前五名連線來源主機使用之前三名 Port 排行。</li> <li>4. 連線來源與目標主機配對排名： 由同一來源主機↔同一目標主機的允許連線配對統計，可以得知特定的兩個主機間成功的通訊最為頻繁，進而依據主機功能屬性推論營運應用型態。</li> </ol>



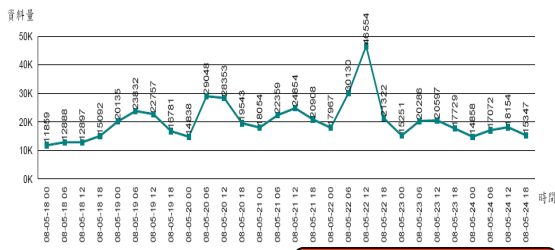
Firewall 週報表樣本

IDS/IPS 週報表	說明
IDS/IPS 每日事件量統計圖	IDS/IPS 的流量統計，可以用來檢視 IDS/IPS 事件的多寡。
IDS/IPS 連線目標主機觸發事件分析	<ol style="list-style-type: none"> <li>1. 目標主機排名： 對於觸發事件量最高的目標主機，需追查這些主機是否有遭到惡意攻擊的行為。</li> <li>2. 目標主機↔觸發事件配對排名： 取事件觸發量最高的前十名目標主機，列出該主機觸發的前十名事件種類，可以檢視目標主機被觸發的各種 IDS/IPS 事件，依主機與事件屬性追查觸發原因。</li> </ol>

捌、IDS/IPS每日事件量統計圖

**每日事件量統計圖**

說明：前端監控設備每日傳送至後端SOC平台的IDS/IPS的流量統計，可以用來檢視IDS/IPS事件的多寡。

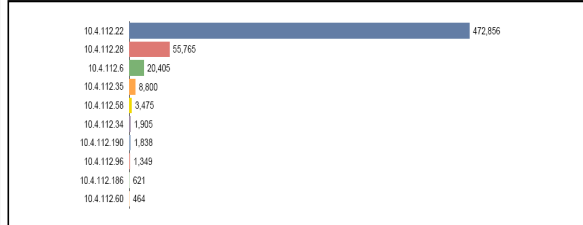


拾、IDS/IPS連線來源主機觸發事件分析

**觸發事件來源主機排名**

一、來源主機排名

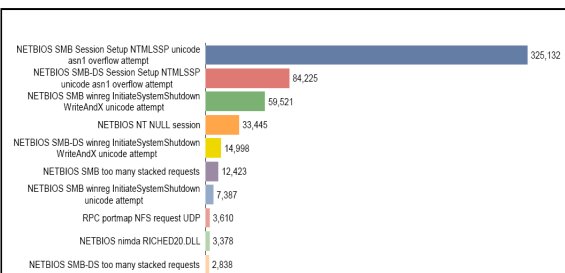
說明：對於觸發事件量最高的來源主機，需追查這些主機是否有惡意的攻擊行為。



一、觸發事件排名

**觸發事件排名**

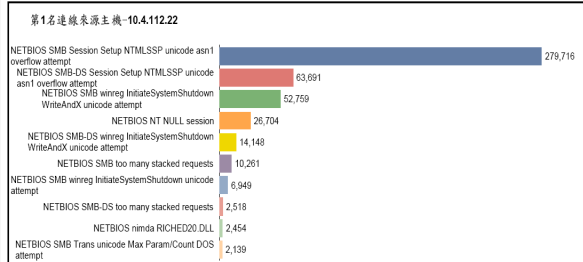
說明：IDS/IPS觸發量最高的前十名事件，若非預期事件所大量觸發，需檢視事件觸發原因。



二、來源主機-觸發事件配對排名

**來源主機、觸發事件配對排名**

說明：取事件觸發量最高的前十名來源主機，列出該主機觸發的前十名事件種類，可以檢視來源主機觸發的各種IDS/IPS事件，依主機與事件屬性追查觸發原因。



**IDS/IPS 週報表樣本**

聯絡窗口：

公司：安基資訊股份有限公司

地址：台北市大安區信義路四段 6 號 9 樓

聯絡人：張文棟

電話：(02)2784-1000 轉 6076

傳真：(02)2784-1092

手機：0956-260-588