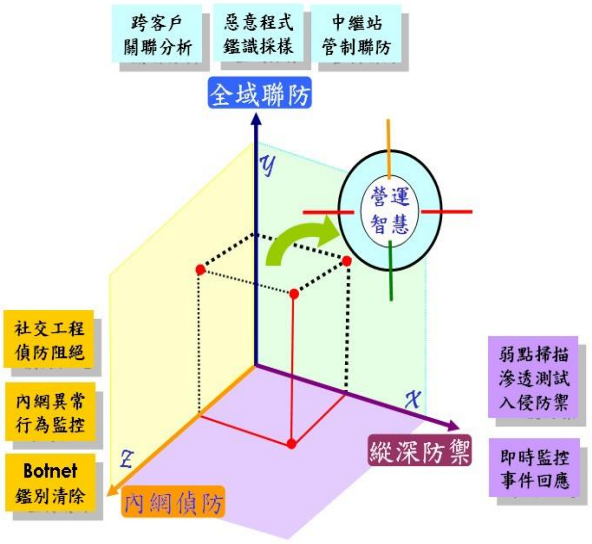
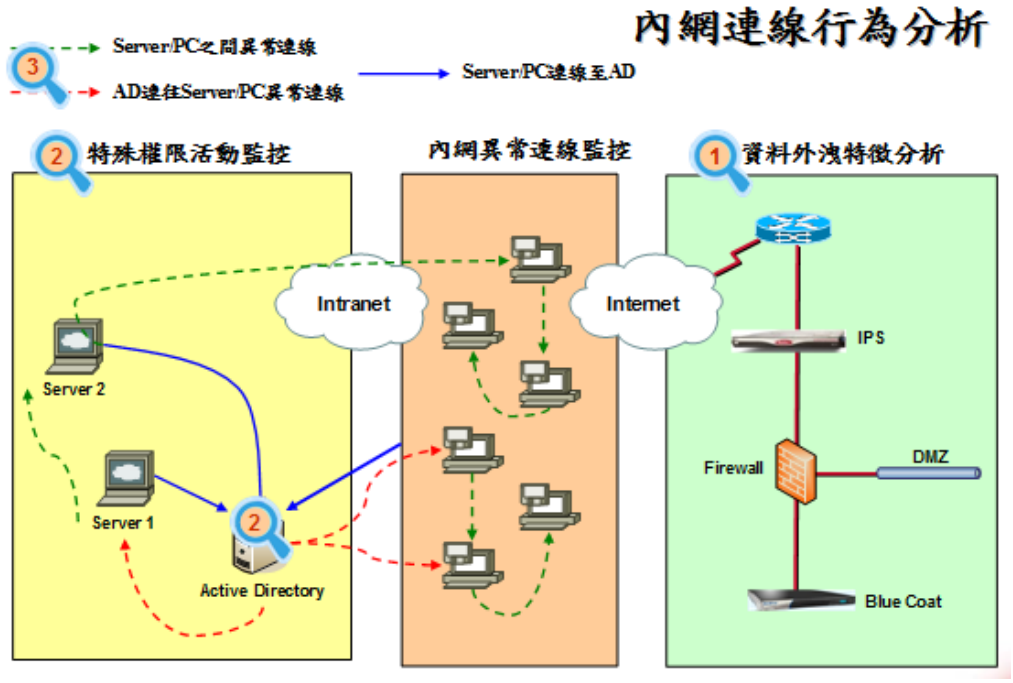
SafeCove AD/WAF/DAM 入侵偵防系統

產品簡介

現今資安事件偵防已面臨極大之挑戰，多數惡意入侵行為皆採行混合多種社交工程攻擊之手法滲透至企業與機關內網，植入惡意程式進行埋伏，再伺機進行惡意攻擊與機敏資料的竊取，其多變的入侵行為與手法為現有防毒與防護系統皆難以防護之處，這也是此類攻擊行為可怕的地方。



SafeCove AD/WAF/DAM 入侵偵防系統，可以針對 Microsoft AD、網頁防火牆（WAF）或資料庫稽核系統（DAM）之日誌記錄與事件進行主動分析，以系統化的方式進行相關存取日誌與事件收集、關連性分析後，對未知型態的入侵事件與社交工程攻擊行為進行事件預警，提供給政府機關作為因應個資安全與資訊安全的管理依據。



產品功能說明

<table>
<tr><th>項目</th><th>內容說明</th></tr>
<tr><td colspan="2">產品功能</td></tr>
<tr><td>Microsoft AD 社交工程偵防功能</td><td>新型態的惡意入侵行為，入侵者在入侵內網後會潛伏一段時間，於內網進行刺探，伺機竊取 domain admins 帳號。本系統將主動對 Microsoft AD 使用者帳號登入與異常活動之行為進行記錄與分析，以主動發覺惡意入侵行為。
日誌與事件稽核項目
<table>
<tr><th>Event ID</th><th>Event 說明</th><th>Event ID</th><th>Event 說明</th></tr>
<tr><td>528 / 4624</td><td>使用者成功登入電腦</td><td>6006</td><td>Event log 已停用</td></tr>
<tr><td>529 / 4625</td><td>使用者名稱或密碼錯誤</td><td>601 / 4697</td><td>嘗試安裝服務</td></tr>
<tr><td>530 / 4625</td><td>非法時間進行登入</td><td>602 / 4698</td><td>排程工作已被建立</td></tr>
<tr><td>531 / 4625</td><td>已停用的帳戶試圖登入</td><td>624 / 4720</td><td>帳號建立</td></tr>
<tr><td>532 / 4625</td><td>過期的帳戶試圖登入</td><td>630 / 4726</td><td>帳號刪除</td></tr>
<tr><td>533 / 4625</td><td>系統不允許該使用者登入</td><td>636 / 4732</td><td>administrators 成員新增</td></tr>
<tr><td>534 / 4625</td><td>不被允許的登入類型</td><td>684 / 4780</td><td>對 administrators 成員設定 ACL</td></tr>
<tr><td>535 / 4625</td><td>帳戶密碼已經過期</td><td>517 / 1102</td><td>稽核紀錄被清除</td></tr>
<tr><td>536 / 4625</td><td>沒有啟用 Net Logon 服務</td><td>680 / 4776</td><td>經由 XX 登入</td></tr>
<tr><td>537 / 4625</td><td>因其他原因而登入失敗</td><td>576 / 4672</td><td>指派特殊權限到新的登入</td></tr>
<tr><td>539 / 4625</td><td>試圖登入時被鎖定</td><td>540 / 4624</td><td>登入成功</td></tr>
</table></td></tr>
<tr><td>WAF 入侵攻擊偵防</td><td>● 網頁應用程式或弱點攻擊行為偵測
● 異常網頁存取行為或探測活動偵測
● SQL Injection/cross site scripting 等攻擊行為偵測</td></tr>
<tr><td>DAM 機敏個資存取與異常行為偵防</td><td>● 監測個資或特定敏感資料存取行為
● 建立資料安全與稽核，資料存取紀錄與證據保存
● 違反資料庫存取政策之行為偵測</td></tr>
</table>

項目	內容說明
技術支援	
資安問題諮詢	● 5x8 線上（電話／電子郵件）資安問題諮詢 ● 客服電話：0800-286-009 ● **選購項目** - 遠端技術支援 ●5x8 電話通知，隔日到場 ●工作內容： 資安事故設備隔離程序 找出並排除可疑惡意程式 找出可疑入侵手法或被駭途徑 系統回復 ●每次啟動至少 4 小時（到府起算），不足 4 小時以 4 小時計

產品授權

產品名稱	授權數量
SafeCove AD/WAF/DAM 入侵偵防系統	任選 Microsoft AD/WAF/DAM 設備 2 台之資安事件監控一年授權

產品售價

- SafeCove AD/WAF/DAM 入侵偵防系統一套（任選 2 設備）NT$89 萬(未稅)

交付項目

- SafeCove AD/WAF/DAM 入侵偵防系統一套與使用授權書

系統硬體需求

- CPU ： Intel 4 核心 2.0 GHz 以上
- 記 憶 體： 4 GB 以上
- 硬碟空間： 500 GB 以上
- 作業系統： Microsoft Windows 2003 Server 標準版 或 Linux 以上

預期效益

- 獲得即時專業資安事件通報，強化資料防護政與管理依據
- 建立有效防護資料外洩之安全預警機制
- 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

聯絡窗口：	
公司：安碁資訊股份有限公司	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