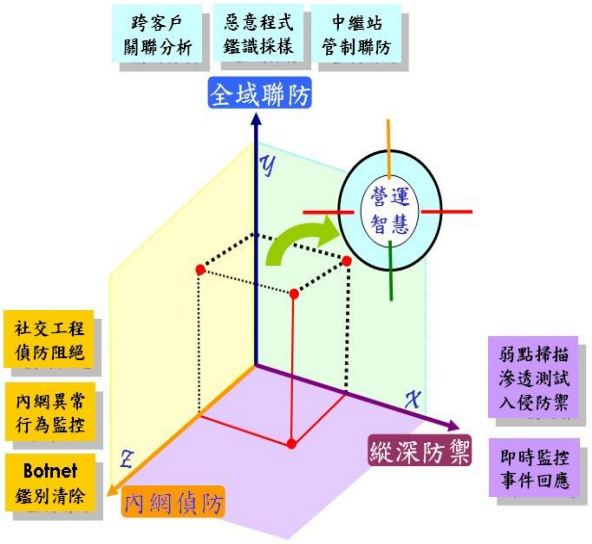
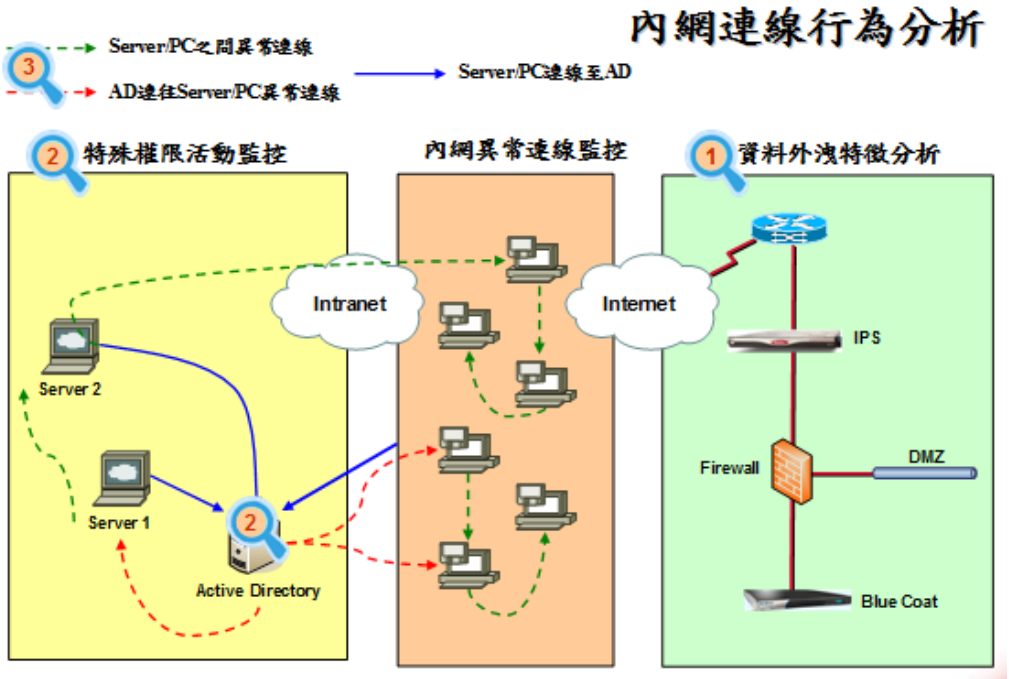
SafeCove AD/WAF/DAM 入侵偵防包(每年訂閱)

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 入侵偵防包，以本公司雲端資安智能監控平台，搭配於用戶端安裝的資安事件收集模組，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>
</table>

產品授權

產品名稱	授權數量
SafeCove AD/WAF/DAM 入侵偵防包(每年訂閱)	可支援監控 Microsoft AD/WAF/DAM 等設備，監控 1 台設備之資安事件監控

產品售價

- NT$89 萬(含稅)

交付項目

- SafeCove AD/WAF/DAM 入侵偵防包使用授權(每年訂閱)
- 含資安事件收集模組一年使用授權

資安事件收集模組硬體需求

- 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

- 自動偵測 AD /WAF/DAM 等資安攻擊事件，即時資安事件通報，強化資安防護與管理
- 建立防護資料外洩之安全預警機制
- 獲取早期預警通知，有效防制資安威脅