CyberForensic SYSTEM

即 時 網 路 封 包 鑑 識 系 統

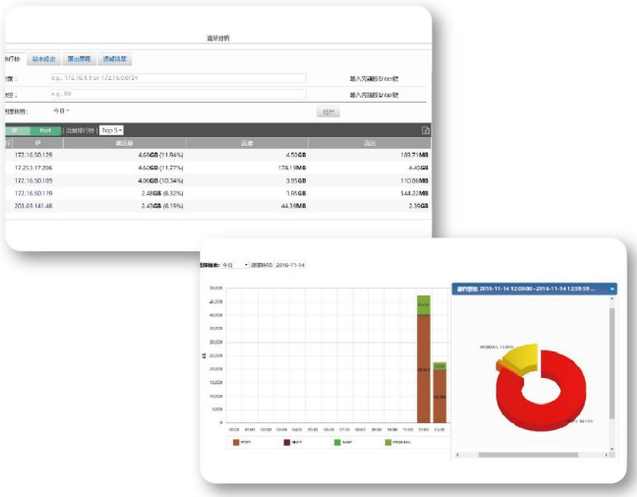
網路 封包鑑識/效能偵測/流量分析 專家

具備了閘道型資安設備，如防火牆、IPS、WAF、防毒牆…等多面向的阻擋和防禦工具，為何資安事件還是層出不窮？
過於嚴謹的管理機制會造成管理者及使用者的困擾；過於鬆散的管理行為，容易形成資安事件及資料外洩漏洞。網路的便利性及安全性，往往是天平兩端。
事件常發生在『**正常行為**』，而『**使用習慣**』是最大原因。不論是蓄意或粗心，因為『**使用習慣**』的疏忽或非理性行為，常對機關造成不可預期的傷害。如何『**建立有效的稽核機制**』及『**將網路災情限縮到最小**』，是在無法完全阻絕資安事件發生的前提下，機關可以努力的方向。
如何達到以上目的？現實生活中，當車禍/傷人/偷竊等事件發生時，人們常利用路口監視器檢視有那些關係人？發生時間？發生地點？如何發生及發生過程，恨不得事發過程『**全都錄**』，事件發生時可『**循線追查**』。CFS如同機關的網路監視器，協助監控網路出入口，資安事件發生時『**有跡可循**』。
CFS之網路安全解決方案，包含『**保密性**』、『**完整性**』、『**可用性**』等安全三要素。除了可提供即時網路內容做為監控網路及稽核依據之外，在效能偵測部分，提供多樣化流量統計分析報表；在資訊安全部分，提供特徵比對及告警。完整的『**人事時地物**』等資訊之保存及呈現，適合應用在網路效能監控、網路環境調校、網路使用稽核、資安事件追蹤調查與跡證留存。

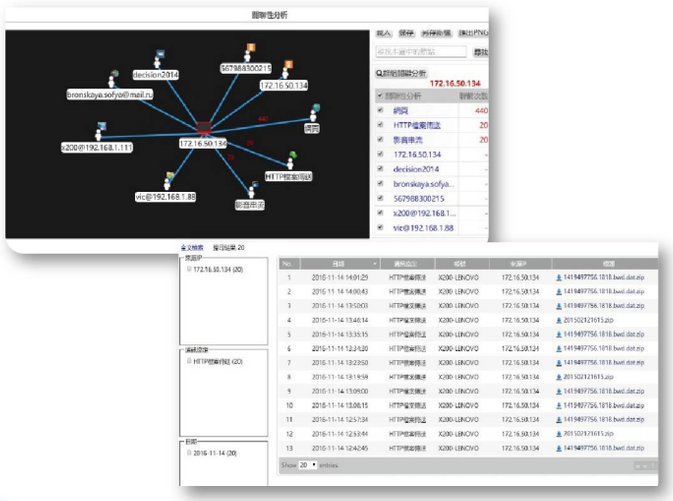
功 能 特 色

- 提供網路流量分析機制，內建網路流量分析統計報表，支援自動/手動 產出。統計資料從網路層到應用層，管理者可隨時檢視網路效能進行調校
- 提供網路行為解析機制，包含郵件、社群、網頁、檔案…等，即時呈現用戶網路使用資訊
- 提供資料庫連線行為監控機制，紀錄內部用戶或外部維護廠商針對資料庫之連線資訊
- 支援惡意檔案/惡意網站 告警機制，隨時掌握資安事件
- 提供檔案傳送告警機制，即時掌握機敏檔案流向
- 提供關聯性分析機制，了解事件『人事時地物』
- 提供網路巨量資料分析機制，協助改善網路環境
- 提供CFS系統使用者分權機制，不同使用者擁有不同使用權限
- 支援自動備份，可利用『**DRMS資料保存管理系統**』長期保存巨量資料並可隨時查詢
- 支援分散式架構，可利用『**CMS中央管理系統**』管理CFS及DRMS
- 可與異質平台整合

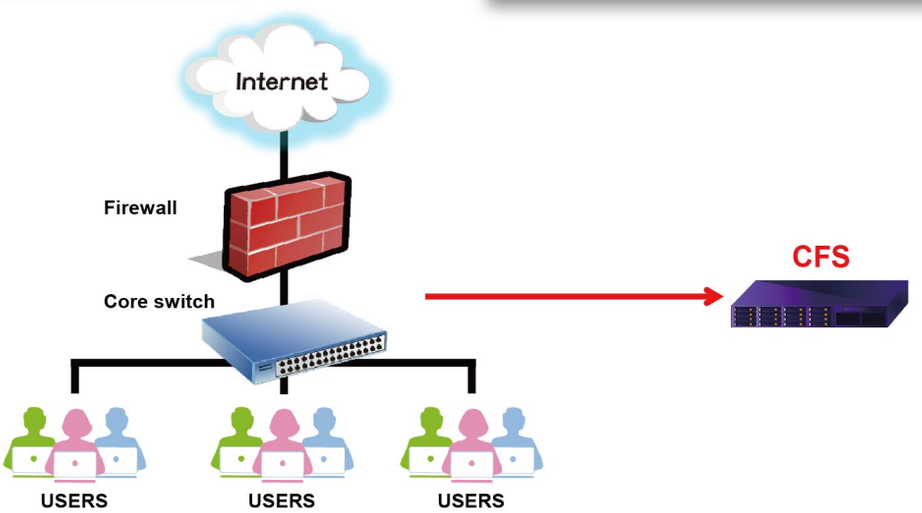
報表



關聯性分析



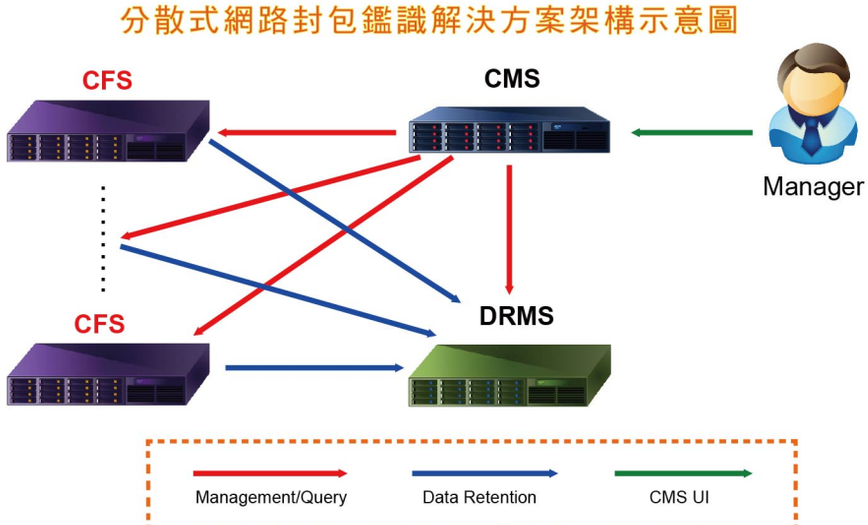
建置架構示意圖



分散式網路封包鑑識解決方案

包含即時網路封包鑑識系統(CFS, Cyber Forensic System)、資料保存管理系統(DRMS, Data Retention Management System)與中央管理系統(CMS, Center Management System)。不論網路規模大小或分散集中，可針對需求彈性設計。

分散式網路封包鑑識解決方案架構示意圖



CFS即時網路封包鑑識系統，專業網路安全解決方案

定興科技股份有限公司
DECISION GROUP INC.
www.edecision4u.com| www.internet-recordor.com.tw
TEL: (02) 2766-5753 | FAX: (02) 2766-5702 | 台北市松山區民生東路五段36巷4弄31號4樓