CyberForensic

網路數位內容鑑識系統 SYSTEM

CFS為網路數位內容鑑識系統，功能包含網際網路封包之偵測、解譯、內容管理、資料儲存與查尋等，並提供保留網路原始封包功能，且可透過統計分析製作各類網路活動報表。管理者可透過報表資料了解每位使用者的網路行為，包括電子郵件、社群網站、網頁瀏覽、網頁傳檔、FTP傳檔、SQL Command及Telnet等。

管理介面

- 提供Web管理介面，管理人員便於登入操作。
- 支援HTTPS及SSH，管理者於操作時保有資料完整性及機密性。

流量分析模組

- 可針對特定目標之IP位址或網段、類型（TCP/UDP/ICMP或輸入連線的Port）及時間區段（指定日期時間），查詢特定時間區段網路流量的使用排行榜記錄。
- 提供單日、單週、全部(單月)流量及各網路服務數量之統計報表匯出。
- 可透過網路流量追查各時段使用者排行榜，並直接可了解排行榜使用者之各種網路 服務使用狀況及內容資料。
- 可依據IP、網段、協定類型、時間範圍等條件進行統計，內容包含：
  - IP或Port之流量統計排行榜
  - IP或Port佔所有統計流量之百分比
  - 特定IP或Port之IP to IP之封包數及總流量統計排行榜

網路服務使用統計

- 統計包含電子郵件、社群網站、網頁瀏覽、網頁傳檔、FTP傳檔、SQL Command及Telnet等特定通訊協定之網路流量。

原始封包保留

- 具備原始封包保留功能，可重建所擷取之網路原始封包。

檔案清單及搜尋

- 系統解譯側錄之檔案後，會以清單方式列出記錄，管理者可選擇不同的副檔名格式過濾清單顯示的檔案類型，亦可進一步搜尋特定檔案出現於那些通訊協定。

全文檢索搜尋

- 提供複合條件搜尋功能，可依協定、日期、時間、IP/ACCOUNT、關鍵字等於系統內查找記錄內容並可針對結果製作成書籤匯出。
- 於全文檢索及條件式搜尋之結果產出後，可進階利用『IP』、『通訊協定』、『日期』、『帳號』等條件，以勾選(單一或複選)方式進行結果過濾。
- 提供檔案比對功能，可將特定檔案上傳至系統，利用特徵值進行搜尋及比對，就算變更檔名或副檔名也可以比對。

書籤記錄

- 可將『關鍵字』、『條件規則』或『敏感檔案』設定為搜尋條件，並建立成書籤記錄，且可將搜尋條件的查詢結果匯出成ISO或CSV文件。

事件管理

- 管理者可以建立由『關鍵字』或『條件規則』組合之告警條件，並且可建立成為『書籤』或『告警』的通知規則。
- 管理者可於『訊息中心』檢視所有的系統事件與告警訊息，亦可使用搜尋功能快速查詢事件記錄。

個資告警

- 可針對不同個資條件進行筆數告警設定，觸發條件時系統會寄送通知信給管理者。

敏感檔案告警：

- 可選擇特定檔案上傳至系統，觸發條件時系統會寄送通知信給管理者。

圖形化關聯性分析

- 提供以用戶的account和IP為主的關聯性分析，可從解析結果的任一IP找出與該IP相關聯的網路協定。
- 關聯式分析圖表以三層式架構呈現，第一層顯示以account或IP作為關聯搜尋的起點。第二層再以account或IP為條件進行延伸，顯示與該用戶的account或IP有關係之IP或通訊協定，例如使用者使用之裝置IP或協定項目。第三層再從該裝置IP延伸出去，可進一步查看各個協定項目之關聯性，包含與哪些IP或account有網路行為等，皆可透過關聯式分析功能查詢。

架　構

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