

E-Detective®

網路封包鑑識系統

全方位網路行為之
稽核、審計、側錄、鑑識暨
數位資產保存設備

Internet Content Monitoring and Forensics Analysis

台灣銀行採購部LP5-990074電腦週邊設備用品第三組
資訊安全鑑識分析設備

組別	三	三	三
項次	66	67	68
品名	資訊安全鑑識分析設備		
	效能200Mbps	效能450Mbps	效能900Mbps
廠牌	DECISION	DECISION	DECISION
型號	ED G-200	ED G-500	ED G-900
設備圖示			
網路流量負載	200Mbps(含)以上	500Mbps(含)以上	900Mbps(含)以上
CPU	3.0GHz(雙核)	2.0GHz(雙核)	2.0GHz(雙核)
RAM	4G	4G	4G
HDD	320G(含)以上	320G(含)以上	320G(含)以上
網路埠	4個10/100/1000 Base-Tx	2個10/100/1000 Base-Tx (含MiniGBIC(SFP) 擴充槽)	2個10/100/1000 Base-Tx (含MiniGBIC(SFP) 擴充槽)
系統支援模式	Span Mode/ Sniffer Mode	Span Mode/ Sniffer Mode	Span Mode/ Sniffer Mode
關鍵字搜尋	✓	✓	✓
支援多國語系	繁中/簡中/英文	繁中/簡中/英文	繁中/簡中/英文
安裝於19"機架	✓	✓	✓
專屬Linux作業系統	✓	✓	✓

可分析 802.3 ethernet、TCP、UDP、VoIPv4、IP Fragment 等封包

以 Web 介面進行設定及管理，使用者登入介面及登入後之 Web 管理介面為 SSL 加密

備份功能

提供自動備份、手動備份、FTP備份等匯出功能

可燒錄成光碟備份

側錄重組還原功能 (採用Deep packet inspection 方式識別封包)

郵件(SMTP/POP3/IMAP)：包含日期/時間、帳號、寄件者、收件者、副本、主旨、檔案大小、附加檔

網頁郵件(WebMail)：包含日期/時間、帳號、寄件者、主旨、網頁郵件種類、附加檔

可側錄之WEBMAIL種類	YAHOO MAIL、YAHOO 2.0、GMAIL、HOTMAIL、HINET、SEEDNET、PCHOEM、URL、SINA、YAM、GIGA、163.net mail.tom.com、mail.163.com、sohu.com、INTLJOB、GO2CANDA、MEDIAHUB、PRODATA、WINDOWS LIVE
---------------	--

網頁(HTTP)：包含日期/時間、帳號/IP、URL、主機名稱(Host)、檔案名稱及內容、大小、上傳/下載、影音串流

檔案傳輸(FTP)：包含日期/時間、Server IP、Source IP、User ID(帳號)、上傳/下載、FTP伺服器、檔案名稱及內容

檔案傳輸(P2P)：包含日期/時間、帳號、寄件者、主旨、網頁郵件種類、附加檔

可側錄之P2P種類	Foxy、ezpeer+、eDonkey、eMule、BitTorrent、BitTornado、BitComet、uTorrent、BitSpirit、Azureus、BitLord、BitBuddy Flashget 1.81、BitTyrant、Kazza、LimeWare、BearShare
-----------	---

TELNET：包含日期/時間、帳號或Source/Destination IP、密碼、伺服器、檔案內容及大小

即時通訊(IM)：包含日期/時間、Source IP、使用者代號(Sender IP)、對談者代號(Receiver IP)、紀錄檔、附加檔

可側錄之IM種類	MSN(包含WEB MSN)、ICQ、YAHOO、QQ、SKYPE、UT、GOOGLETALK、IRC、AOL
----------	---

線上遊戲(On-Line Game)：包含楓之谷等80種以上的線上遊戲側錄

可側錄之線上遊戲種類	MSN(包含WEB MSN)、ICQ、YAHOO、QQ、SKYPE、UT、GOOGLETALK、IRC、AOL
------------	---

VoIP：支援SIP協定，可記錄日期/時間、帳號、發話者、對談者、模式、codec、檔案名稱、對談時間

系統資訊

硬碟	提供硬碟容量、已使用空間、可用空間、可用空間百分比等資訊
系統記憶體	提供記憶體類型、容量、可用空間、可用空間百分比等資訊
線上IP資訊	提供線上IP清單、包括連線IP數、連線狀態、電腦IP、電腦名稱、最後存在時間、群組
	提供 刪除/新增/匯入IP功能；被拒絕(未被側錄)的IP清單；隱藏IP功能，可隱藏特定IP資訊；忽略IP功能，可特別設定不需側錄的IP

報表功能：可即時統計並產出所需報表，異常事件分析報表及TOP N排行報表

首頁總表	提供每日、每週，全部之側錄彙整總表，包括筆數及流量
個人報表	提供個人每日、每週，全部之側錄彙整總表，包括筆數及流量
每日報表	每日寄送前一日之側錄彙整總表
流量統計報表	根據該網路協定、提供每日、每週、全部之流量報表
使用者排行	根據該網路協定、提供每日、每週、全部之使用者排行
網路服務使用率分布表	提供各類網路協定使用率百分比圖表
網頁瀏覽排行榜	提供TOP N的使用網頁，可進一步提供某個網頁最常被哪些用戶使用，並以IP或帳號顯示；且可再繼續點選產出該用戶當日或當週的所有網路協定使用情形

管理功能

系統服務設定	提供保存原始封包、側錄網路流量、帳號反查、SNMP Read Community、功能
側錄服務設定	提供各項網路側錄服務 啟動/停止 功能
設定側錄檔案大小	可設定相關網路服務所側錄之檔案大小超過設定值時不儲存
權限設定	可針對不同的系統使用者設定不同的使用權限
硬碟容量管制	當硬碟容量到達設定值，可設定覆蓋最舊的資料檔或ISO檔
IP流量監控	提供包含IP之送出流量，收入流量，總流量等資訊
匯入AD資訊	可匯入AD與IP之對應表，以AD帳號呈現資料，做更精確的稽核
側錄檔案清單	提供檔案、副檔名、數量、檔案大小、MD5雜湊值等資訊
書籤	可將全文檢索搜尋結果記錄為書籤(Bookmark)，並可再匯出查詢內容實體為ISO檔

搜尋功能：依所需條件鍵入相關表格內，進行全文檢索搜尋，結果會產生於所有網路協定

IP反查功能：可追查來源端或目的端IP及IP擁有者

告警功能：可設定寄送硬碟將滿警告信；另可以網路協定為基礎，系統使用者可設定相關條件，若用戶觸發條件，系統會寄送告警信給所設定之郵件帳號

具備 IPv4 / IPv6 雙協定 (Dual Stack) 技術，同時提供 IPv4 與 IPv6 處理能力

經銷商：



定興科技股份有限公司
DECISION GROUP INC.

企業網站：www.decision.com.tw

產品網站：www.edecision4u.com(英文網站)

www.internet-recorder.com.tw(中文網站)

地址：台北市民生東路五段36巷4弄31號4樓

電話：+886 227665753 傳真：+886 227665702

Email：decision@decision.com.tw

sales@decision.com.tw