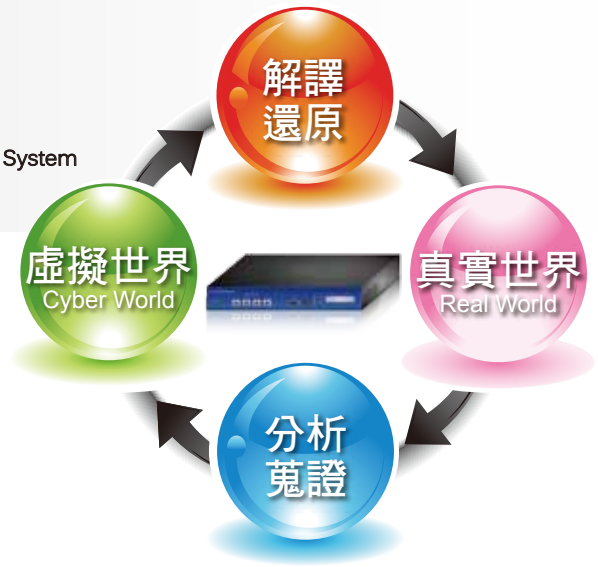
網路行為即時監控與鑑識系統

E-DETECTIVE®

Real-Time Network Forensics and Lawful Interception System



E-Detective 除了可以擷取網路封包、並即時解譯多種不同的網路應用協定外，內建的多樣分析報表與工具，非常適合各種單位應用在資訊洩漏安全事件發生後的追蹤、調查、與蒐證。有了E-Detective，單位資安管理系統(ISMS)更加完整。

特色

- **全面監控與稽核企業內部網路行為**
  直接由網路擷取資料，不須安裝用戶端軟體，不論用戶平台資料全部一把抓，易於維護與擴充。
- **網路封包擷取後即時解譯**
  資料還原速度越快，稽核人員越能掌握調查時效
- **提供效能強大的資料搜尋工具**
  可快速依據稽核人員設定的各種搜尋條件獲取資料與檔案，內建獨步業界之關聯式搜尋，更是提供稽核人員連接虛擬世界與真實世界之利器。
- **支援中介資料匯出**
  強大解譯的還原能力，可結合稽核人員結合既有的分析工具，更能使其工具功能發揮加乘的效果。
- **網路稽核不求專家**
  還原資料呈現直覺易懂，不需網路專家，一般稽核人員均可輕易了解。
- **支援解譯協定眾多**
  提供業界最多的協定解譯能力，最多的解譯資訊，稽核人員不再霧裡看花
- **內建多樣報表與分析工具**
  除解譯還原資料外，提供各種分析報表與統計圖，如各協定分析與使用狀況統計、系統資源使用統計、網路關鍵字出現統計等，使稽核人員更能掌握全面狀況
- **SSL內容攔截選購套件**
  可配合使用者環境，針對HTTPS連線，提供破譯選購套件，使網路稽核不再有漏網之魚。
- **可適用大型網路**
  包含網路封包擷取與解譯系統(E-Detective)、解譯資料保存與匯出系統(DRMS, Data Retention Management System)、與中央管理系統(CMS, Center Management System)，構成完整的稽核系統，不論網路規模大小，或分散集中，更能針對客戶稽核需要彈性設計，以符合客戶需要。

支援協定

E-MAIL

POP3, SMTP, IMAP, Web Mail(Yahoo Mail, G Mail, Hot Mail...)

Instant Message

MSN, ICQ, Yahoo, QQ, UT, SKYPE, Google Talk

Social Network Service

Facebook, Twitter, Plurk, Sina, Sohu, Tencent, 163, Kaixin, Renren, Qzone

HTTP

Web Page(Request, Response), File Download/Upload, Video Stream (FLV)

File Transfer

FTP, P2P, Dropbox, Evernote, CIFS(With EDGS Version)

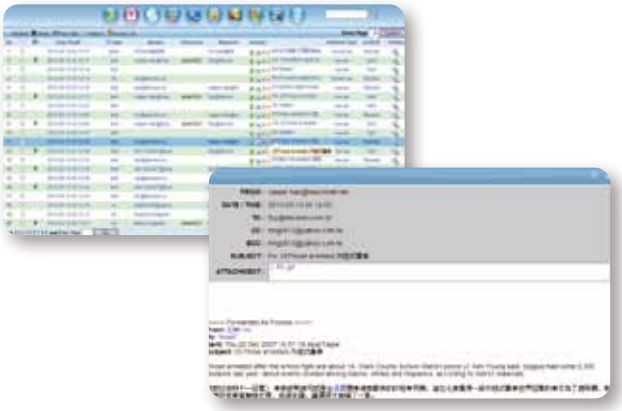
Others

Telnet, Online Game, VoIP, SQL(By EDGS Version), Unknown Connections

報表與分析工具

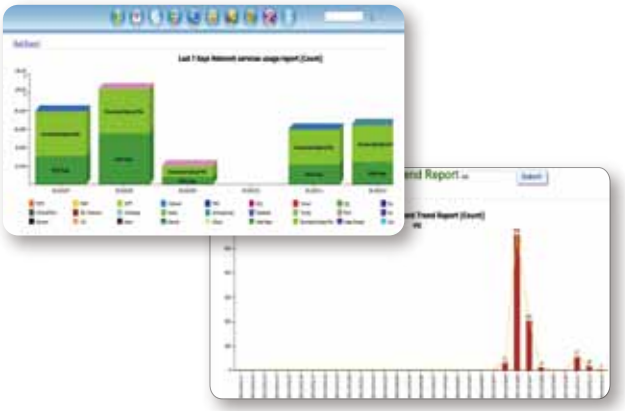
還原資料清單與顯示

資料直接呈現，淺顯、直覺、且易懂。



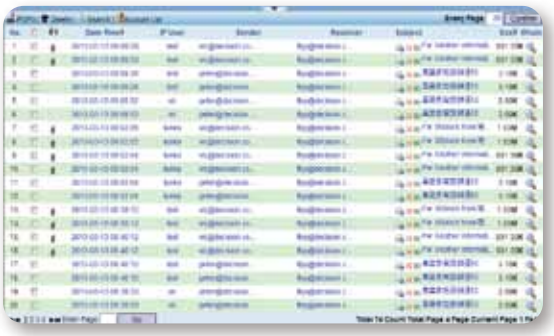
還原資料統計與分析

稽核人員更能掌握使用者網路行為的各種狀況與趨勢。

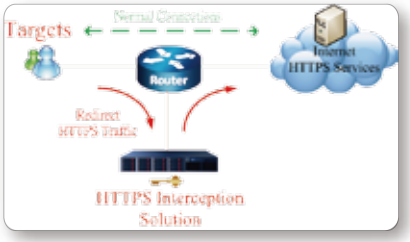


通訊關聯分析

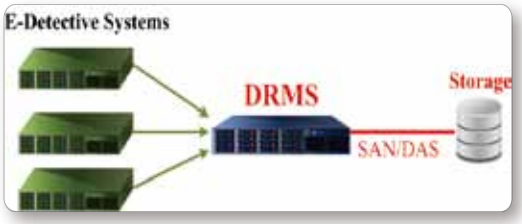
使用者通聯分析與關聯功能、提供稽核人員連接虛擬世界與真實世界的橋梁



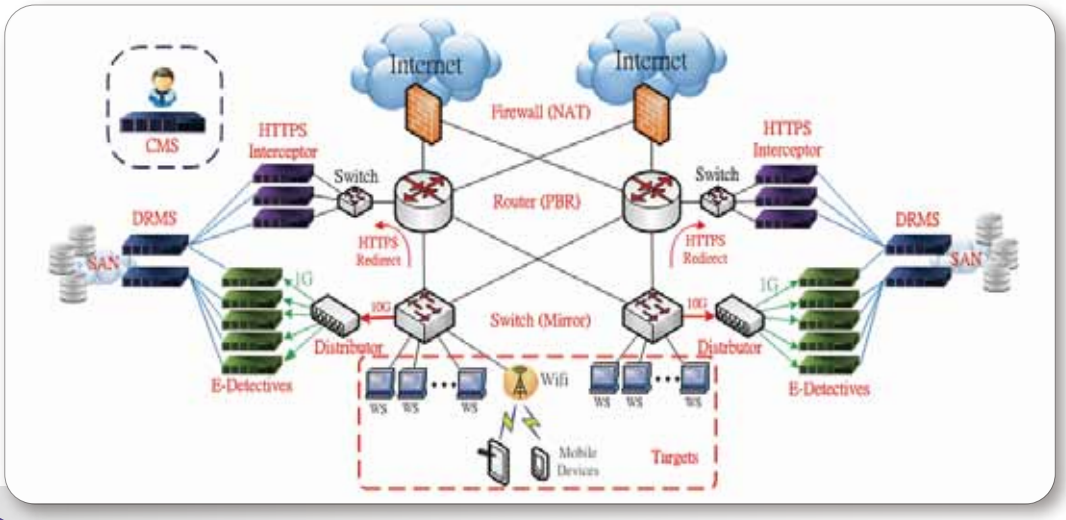
HTTPS選購套件



資料保存系統(DRMS)選購套件



大型分散式網路架構設計



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