

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。
- **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。
- **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。

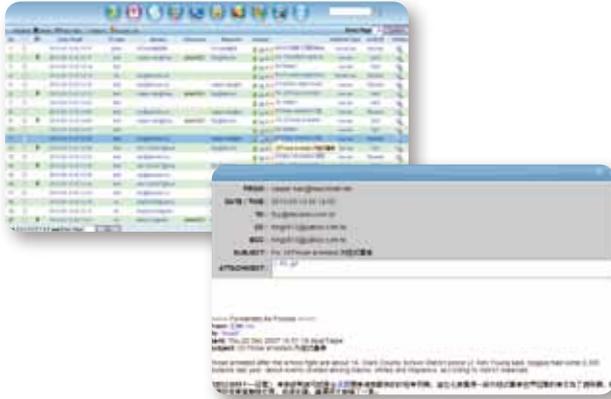
## 支援協定

 <b>E-MAIL</b> POP3, SMTP, IMAP, Web Mail (Yahoo Mail, G Mail, Hot Mail... )	 <b>Instant Message</b> MSN, ICQ, Yahoo, QQ, UT, SKYPE, Google Talk	 <b>Social Network Service</b> Facebook, Twitter, Plurk, Sina, Sohu, Tencent, 163, Kaixin, Renren, Qzone
 <b>HTTP</b> Web Page (Request, Response), File Download/Upload, Video Stream (FLV)	 <b>File Transfer</b> FTP, P2P, Dropbox, Evernote, CIFS (With EDGS Version)	 <b>Others</b> 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。



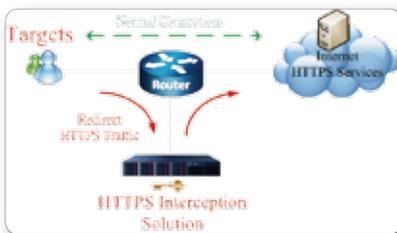
## ● 通訊關聯分析

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

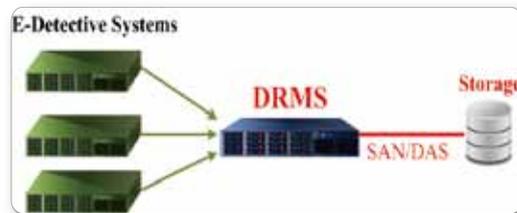


No.	Date	Time	Source	Destination	Protocol	Bytes	Direction
1	2012/01/01 00:00:00	00:00:00	192.168.1.1	192.168.1.2	TCP	1024	Out
2	2012/01/01 00:00:01	00:00:01	192.168.1.2	192.168.1.1	TCP	1024	In
3	2012/01/01 00:00:02	00:00:02	192.168.1.1	192.168.1.3	TCP	1024	Out
4	2012/01/01 00:00:03	00:00:03	192.168.1.3	192.168.1.1	TCP	1024	In
5	2012/01/01 00:00:04	00:00:04	192.168.1.1	192.168.1.4	TCP	1024	Out
6	2012/01/01 00:00:05	00:00:05	192.168.1.4	192.168.1.1	TCP	1024	In
7	2012/01/01 00:00:06	00:00:06	192.168.1.1	192.168.1.5	TCP	1024	Out
8	2012/01/01 00:00:07	00:00:07	192.168.1.5	192.168.1.1	TCP	1024	In
9	2012/01/01 00:00:08	00:00:08	192.168.1.1	192.168.1.6	TCP	1024	Out
10	2012/01/01 00:00:09	00:00:09	192.168.1.6	192.168.1.1	TCP	1024	In
11	2012/01/01 00:00:10	00:00:10	192.168.1.1	192.168.1.7	TCP	1024	Out
12	2012/01/01 00:00:11	00:00:11	192.168.1.7	192.168.1.1	TCP	1024	In
13	2012/01/01 00:00:12	00:00:12	192.168.1.1	192.168.1.8	TCP	1024	Out
14	2012/01/01 00:00:13	00:00:13	192.168.1.8	192.168.1.1	TCP	1024	In
15	2012/01/01 00:00:14	00:00:14	192.168.1.1	192.168.1.9	TCP	1024	Out
16	2012/01/01 00:00:15	00:00:15	192.168.1.9	192.168.1.1	TCP	1024	In
17	2012/01/01 00:00:16	00:00:16	192.168.1.1	192.168.1.10	TCP	1024	Out
18	2012/01/01 00:00:17	00:00:17	192.168.1.10	192.168.1.1	TCP	1024	In
19	2012/01/01 00:00:18	00:00:18	192.168.1.1	192.168.1.11	TCP	1024	Out
20	2012/01/01 00:00:19	00:00:19	192.168.1.11	192.168.1.1	TCP	1024	In

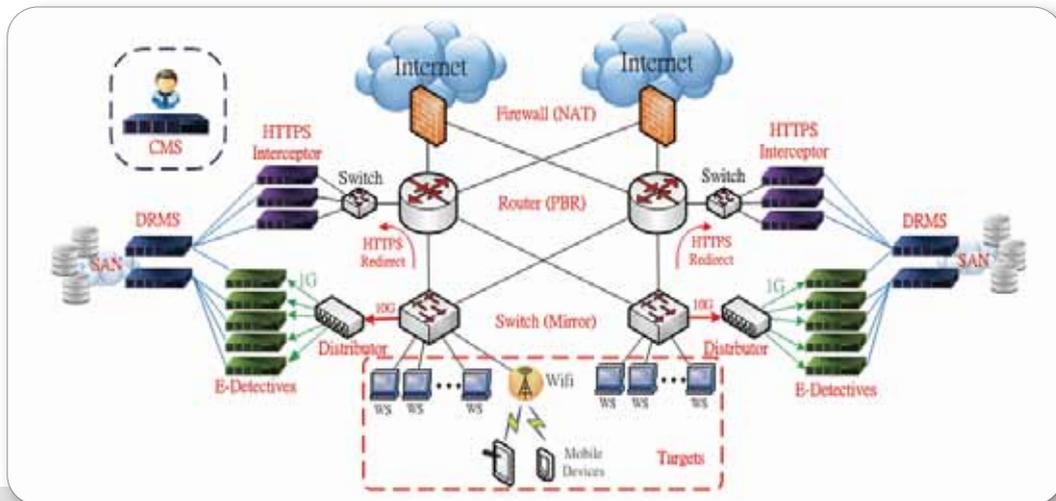
## ● HTTPS選購套件



## ● 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

