



# uniXecure 跡證保存系統帳號管理 擴充模組

## ■ 商品介紹

提供機關跡證保存平台，提供機關既有網路、資安設備與伺服器主機均能支援Syslog或是Flow流量資料的輸出功能，協助完整記錄及保存各項紀錄。

## ■ 商品特色

因應稽核需求，提供之跡證保存平台應可支援以下蒐集功能

1. 可支援AD功能變數名稱解析。
2. 可支援IP與主機名稱(Host Name)對應設定。
3. 可支援設備狀態監控功能。
4. 可支援關聯性分析功能，能將NetFlow及sFlow與Syslog 資料結合。
5. 能針對登入(Login)登出(Logout)日誌進行分析，主動發覺密碼猜測攻擊，登入異常等事件。
6. 提供針對客戶端AD帳號資料進行記錄保存及監控作業。

## ■ 功能規格

客戶端需準備軟體安裝之主機資源規格如下：

實體機(或虛擬機)：

- CPU: 8core
- RAM: 32G (含)以上
- Disk: 140G (SSD or Fast) (含)以上
- VMware ESXi 6.0 (含)以上

uniXecure

聯絡窗口：吳建和

聯絡電話：02-8798-6088 #5770

0936-105-665

電子郵件：fosterw@unixecure.com.tw