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。
   可支援IP與主機名稱(Host Name)對應設定。
2. 可支援設備狀態監控功能。
3. 可支援關聯性分析功能，能將NetFlow及sFlow與Syslog 資料結合。
4. 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。

■ 功能規格

客戶端需準備軟體安裝之虛擬主機資源規格如下

- CPU：2.0 GHz 8core
- RAM：32G (含)以上
- Disk：1T (SSD or Fast) (含)以上
- OS：Ubuntu 18.04~20.04
- VM Format： VirtualBox 6.1.26 以上平台 OVA (約10G)
- 網路卡：Intel 以太網路 I350 QP 1Gb 網路卡

uniXecure
聯絡窗口：林愔予
聯絡電話：02-8798-6088
0939-786-153