資安防護能量簡介

國家中山科學研究院
資訊通信研究所
資安防護組

陳國鐘 c50cgj@ncsist.org.tw
0936-080500

大綱

- 任務簡介
- 產品簡介
- 結語

任務簡介

負責國防科技相關技術研發

- 資訊戰
- 電子戰
- 通信系統
- 指管通情系統
- 遙控及導控系統
- 水下科技

研發成果

指揮管制系統

資訊防護與反制

水下測試

通信車

電子戰干擾系統

本所資安防護能量簡介

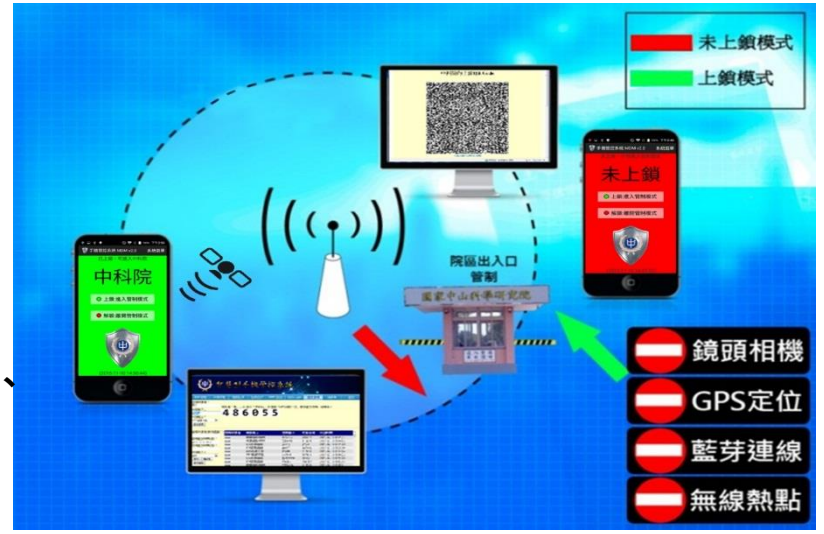
項次	產品內容
1	智慧型手機管控系統(MDM)
2	社群軟體(Line)訊息加密
3	5G資安聯防研究
4	資安防護中心(SOC)
5	網路單向檔案傳輸器
6	安全強健型Linux作業系統
7	資安訊息巨量資料分析
8	資訊安全評估與檢測實驗室(TAF Laboratory)
9	資安健檢鑑識服務
10	資安人員教育訓練

智慧型手機管控系統(MDM)

本系統可有效阻絕手機外洩機敏資訊之管道（如:相機、藍芽、熱點分享、定位等），消除相關資安疑慮風險後，即可將智慧型手機視同一般手機進行管理與運用。

系統特色

- 跨區域管制功能
- 定時自動上鎖功能
- 緊急密碼解鎖功能
- 上鎖/解鎖不須與後端伺服器連線
- 提供快速解鎖模式，同時採用衛星、行動數據及WiFi定位資訊
- 不使用Android的GCM以及iOS的APNS避免通信資訊洩露
- 整合門禁與差勤等系統以達到有效管控目的



社群軟體(Line)訊息加密

本APP可將訊息加密後，透過一般商用通訊軟體(如Line)傳遞密文訊息，接收端於通訊軟體介面上直接點選密文，即可顯示解密結果。

系統特色

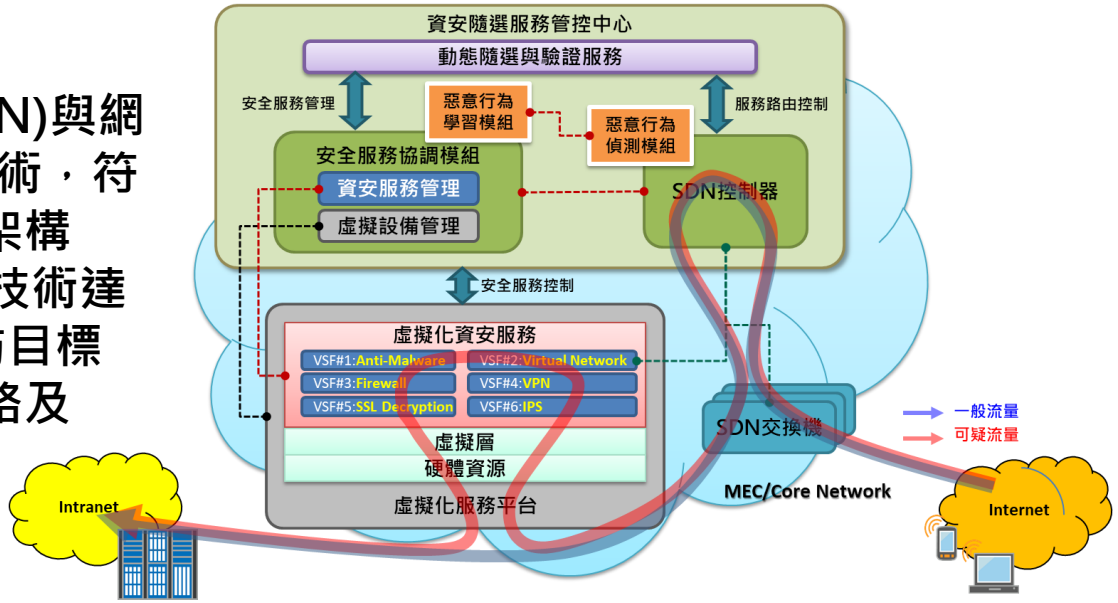
- 操作介面簡單易用
- 不同群組可設定不同密碼
- 使用者雙方可自訂密碼，強化訊息傳送安全
- 可支援Line、Juiker 、WhatsApp三種通訊軟體
- 不影響群組中未安裝訊息加密APP的訊息傳遞
- 群組人數無限制(Line僅支援50人以下之群組加密)

5G資安聯防研究

在5G網路架構中加入虛擬化資安服務，如應用機器學習於惡意行為偵測，運用軟體定義網路達成資安聯防等技術，建立攻防模擬場景，完成5G資安聯防研究，未來持續關注國際5G組織及國際大廠資安發展趨勢，調整安全服務架構。

系統特色

- 5G資安隨選系統
- 運用軟體定義網路(SDN)與網路功能虛擬化(NFV)技術，符合5G主流虛擬化網路架構
- 運用服務功能鏈(SFC)技術達成虛擬化資安服務聯防目標
- 適用於5G虛擬核心網路及網緣運算平台(iMEC)
- 內建虛擬化資安服務正確性驗證功能



資安防護中心(SOC)

本系統收整各項資安警訊，並即時產生視覺化圖表，便利資安人員掌握情資、強化整體資訊安全，其防護範圍包含閘道端防護、端點防護與其他相關資安設備，提升資安縱深防禦之能力。

系統特色

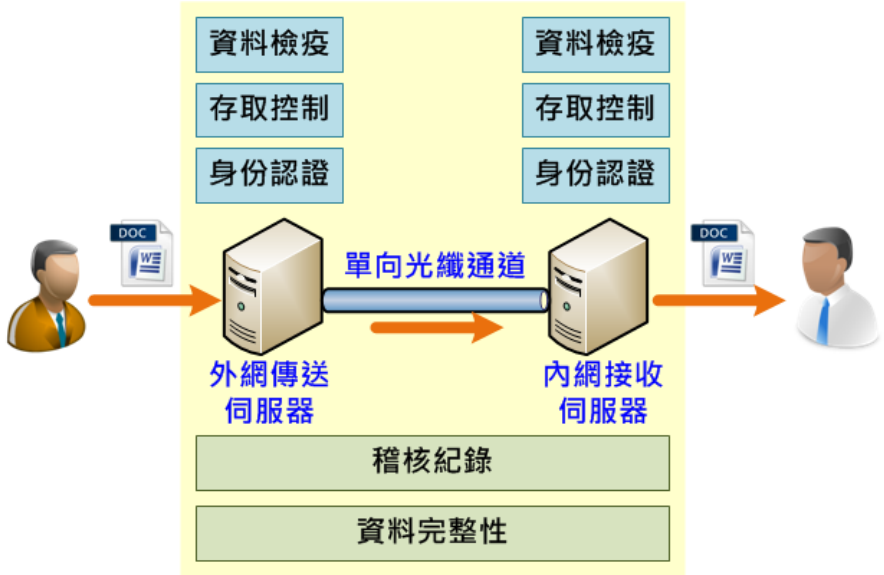
- 客製化事件流程處理
- 視覺化資安事件警示
- 整合式地理情資展示
- 即時網路狀態統計分析
- 互動式資訊收集及圖表操作
- 收容訊息來源包含
  - 入侵偵測
  - 弱點掃瞄
  - 資產安全管理
  - 病毒集控
  - 防火牆及各式網路設備紀錄

網路單向檔案傳輸器

為確保機敏資料不會因連接網路而外流，本所研製網路單向檔案傳輸器，具備單向光纖傳輸通道，提供近乎即時之檔案傳輸功能，搭配資料檢疫功能，可檢測傳輸之檔案是否內含惡意程式，以提升跨網資料傳輸效率，同時確保資料傳輸之完整性與安全性。

系統特色

- 具備資料檢疫功能，確保資料傳送端與接收端之資料安全
- 具備身份認證與存取控制功能，確保僅獲授權之使用者可傳送資料
- 具備資料完整性檢查功能，確保檔案重組後之完整性
- 具備稽核功能，可記錄傳送資料名稱與傳送時間等資訊



安全強健型Linux作業系統

本所自主研改並強化Linux作業系統安全機制，包含特權帳號與周邊裝置管控等安全功能，針對客戶需求客製化安全Linux作業系統，更於106年11月23日舉辦Linux作業系統安全防護技術研討會，促進學研界技術交流並獲得迴響，後續將持續發展與推廣安全強健型作業系統，目標有效降低每年國內對商用作業系統所支付之龐大授權費用。

系統特色

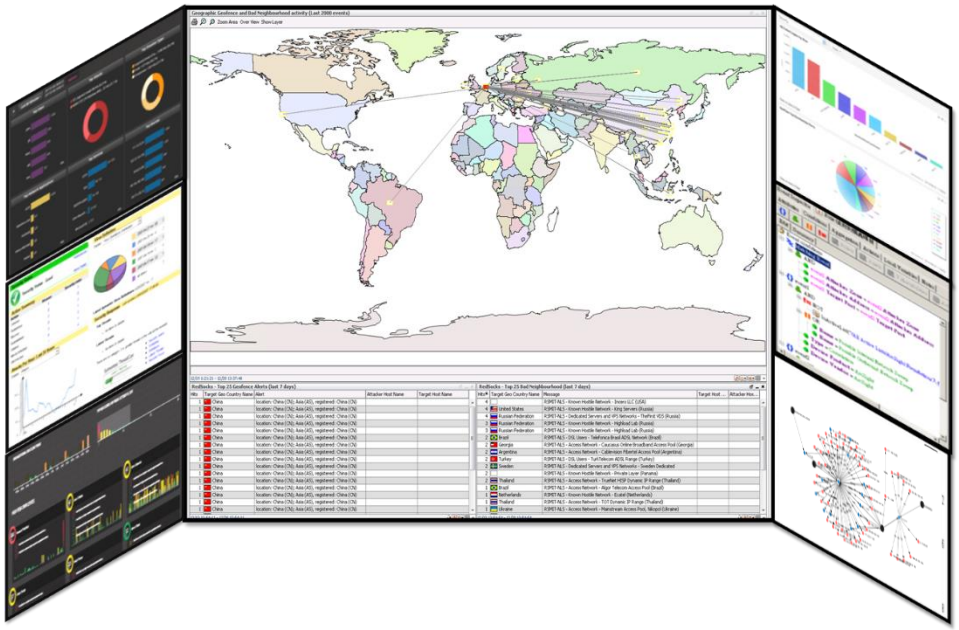
- 核心安全模組研改
- 系統核心模組裁減
- 虛擬化隔離技術
- 安全組態評估與監控
- 客製化SELinux安全政策
- 多合一安全代理程式
  - 資安安全管理
  - 周邊裝置管控
  - 使用者行為分析
  - 系統安全組態管控

資安訊息巨量資料分析

新世代資安監控中心(SOC)將結合巨量資料分析與機器學習等技術，目標在早期發覺傳統資安設備無法偵測的風險行為，協助資安人員早期預警可疑威脅，提升整體資訊安全之防護能力。

系統特色

- 完整收容資安訊息
  - 資安設備警訊
  - 端點防護軟體資訊
  - 系統操作日誌
  - 網路流量特徵
- 巨量資安資料分析
- 改良式機器學習演算法
- 進階持續性威脅感知
- 關聯式圖形顯示
- 資安區域聯防

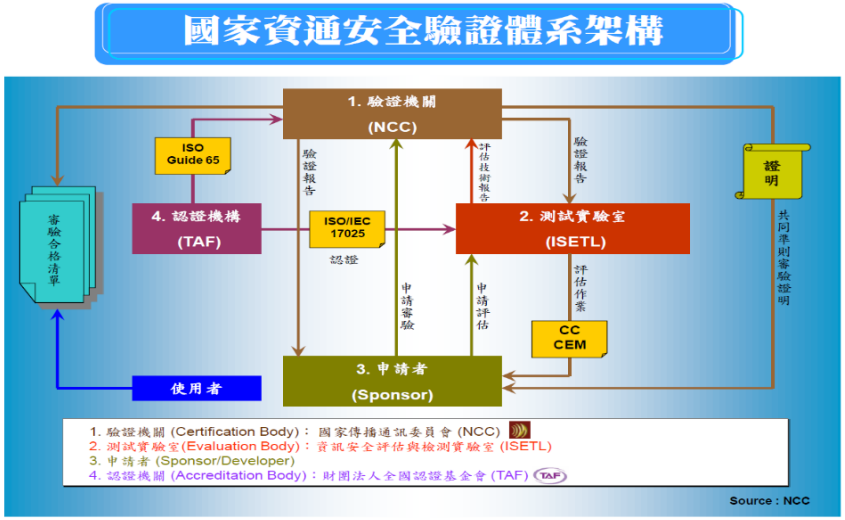


資訊安全評估與檢測實驗室(TAF Laboratory)

行政院為提昇台灣IT軟、硬體產品安全性，本所遵循IT產品安全評估準則(CC，ISO/IEC 15408)及安全評估方法論(CEM，ISO/IEC 18045)國際標準，建置IT產品安全性驗證技術與實驗室。

資訊安全檢測

- 共同準則資通安全產品評估檢測
- 全台唯二可認證EAL4+安全等級
- 行動裝置應用程式安全檢測
- 微軟電腦系統磁碟安全檢
- 資安健檢與鑑識

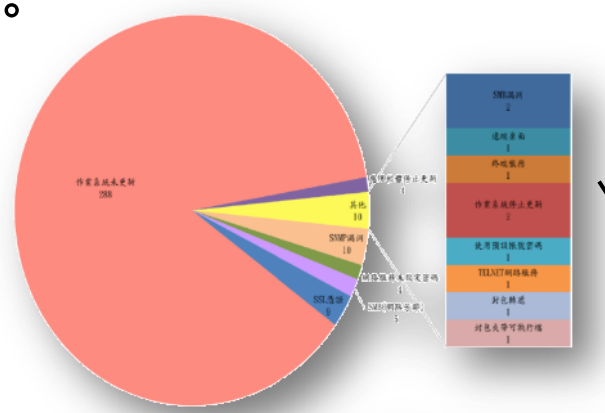


資安健檢/鑑識服務

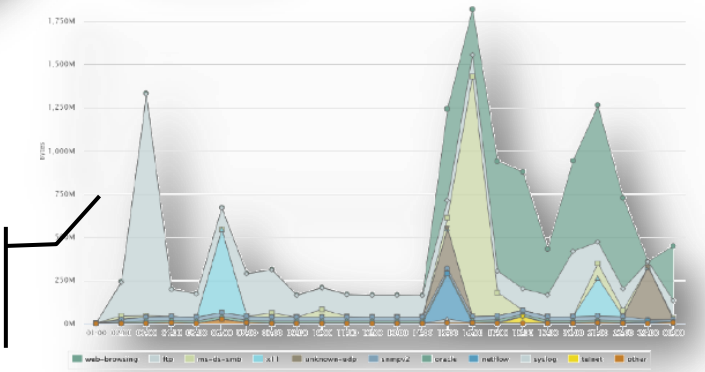
透過弱點掃瞄、潛伏惡意程式查找及滲透測試等技術，檢測網路設備通訊埠、主機系統弱點及目標主機記憶體已執行之惡意程式之潛在風險，以視覺化效果呈現分析結果，進一步提供改善建議。

資安健檢/鑑識

- 弱點掃描
- 網路服務密碼測試
- 潛伏惡意程式查找
- 映像檔活化
- 網路異常封包檢視
- 記憶體鑑識
- 檔案動態行為分析



資安健檢服務



台灣高O公司
資安健檢服務

資安人員教育訓練

主要目的係協助各單位強化其資安防護能力，安排教育訓練課程內容包含網路資安設定、防護、檢測及應變分析等面向，並以課程講解搭配實務操作授課方式，課程由淺入深，增進授課學員資訊安全技術能力。

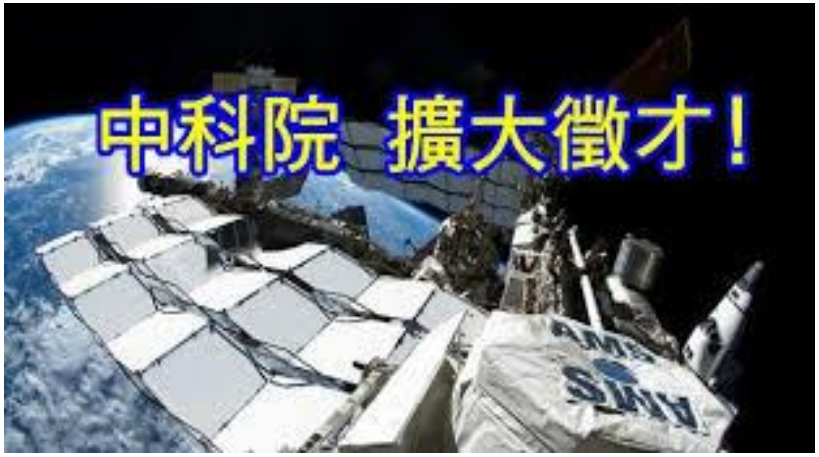
課程概要

- 資安基礎概念介紹
- 資安產品簡介
- 作業系統安全調教
- 網路流量與封包分析
- 漏洞分析與滲透測試
- 資安健檢與鑑識
- 資安防護與事件應變

結語

本所已取得ISO27001:2013認證、稽核員、資訊安全管理系統(ISMS)主導稽核員、道德駭客與資安鑑識調查專家(CHFI)等認證，具備完善資安防護與監控能量。

歡迎有志青年一齊加入~
國防科技資安防護專業研發工作。



簡報結束
感謝聆聽