核能研究所資安防護

經驗分享

報告人：曾慶沛

111年5月4日

大綱

- 資訊安全整合
- 資訊安全管理面
- 核能研究所資安防護架構
- 資安防護建置歷程
- 資安監控平台
- 案例

資訊安全整合

偵測

網路封包資料（節點、Flow）
資安事件警告
入侵偵測(防毒、IDS、IRS、Firewall)
端點偵測

分析

端點偵測及應變機制(EDR)
延伸式偵測及回應(XDR)

防禦

入侵防禦系統IPS
弱點掃描
滲透測試
威脅情資

資安事件
駭客、病毒

管理

資訊安全管理 (ISMS)
資安風險管理
安全性資訊與事件管理 (SIEM)
事件調查、鑑識、復原及改善機制

監控

網路流量分析 (NTA)
不同平台事件記錄與分析（防火牆、Router、Switch、Server...）

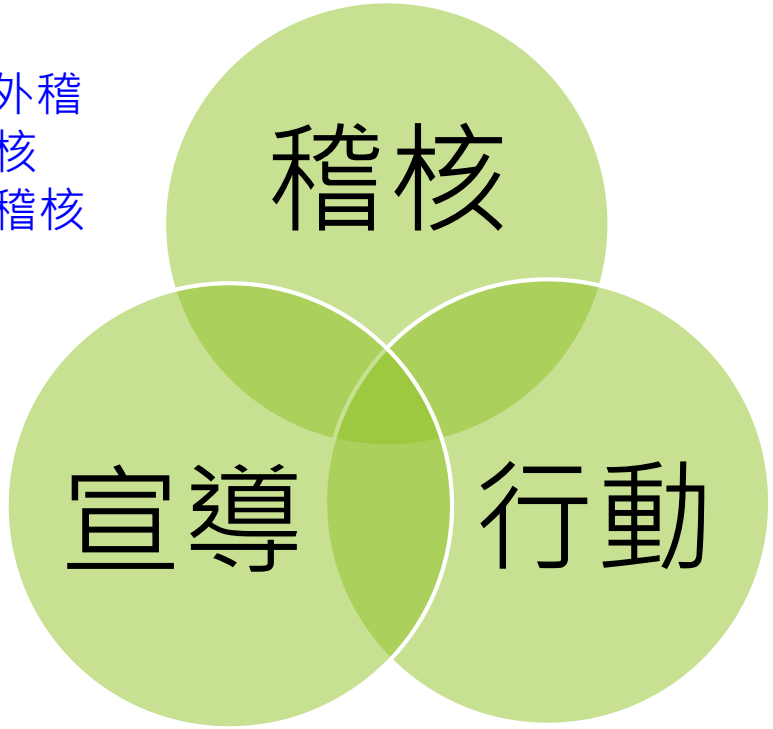
資訊安全管理面

成立資訊安全推展委員會

- 資訊安全 (Information Security)：
  - 機密性 (Confidentiality)：資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
  - 完整性(Integrity)：對資產之精確與完整安全保證的特性。
  - 可用性(Availability)：已授權實體在需要時可存取與使用之特性。
- 資訊安全實施計畫
- 資訊安全稽核
  - 政風資安稽核
  - 職安會資訊稽核
- 資訊安全行動
  - 制定資訊安全作為

核研所的資訊安全管理

ISMS內稽、外稽
政風資安稽核
職安會資訊稽核

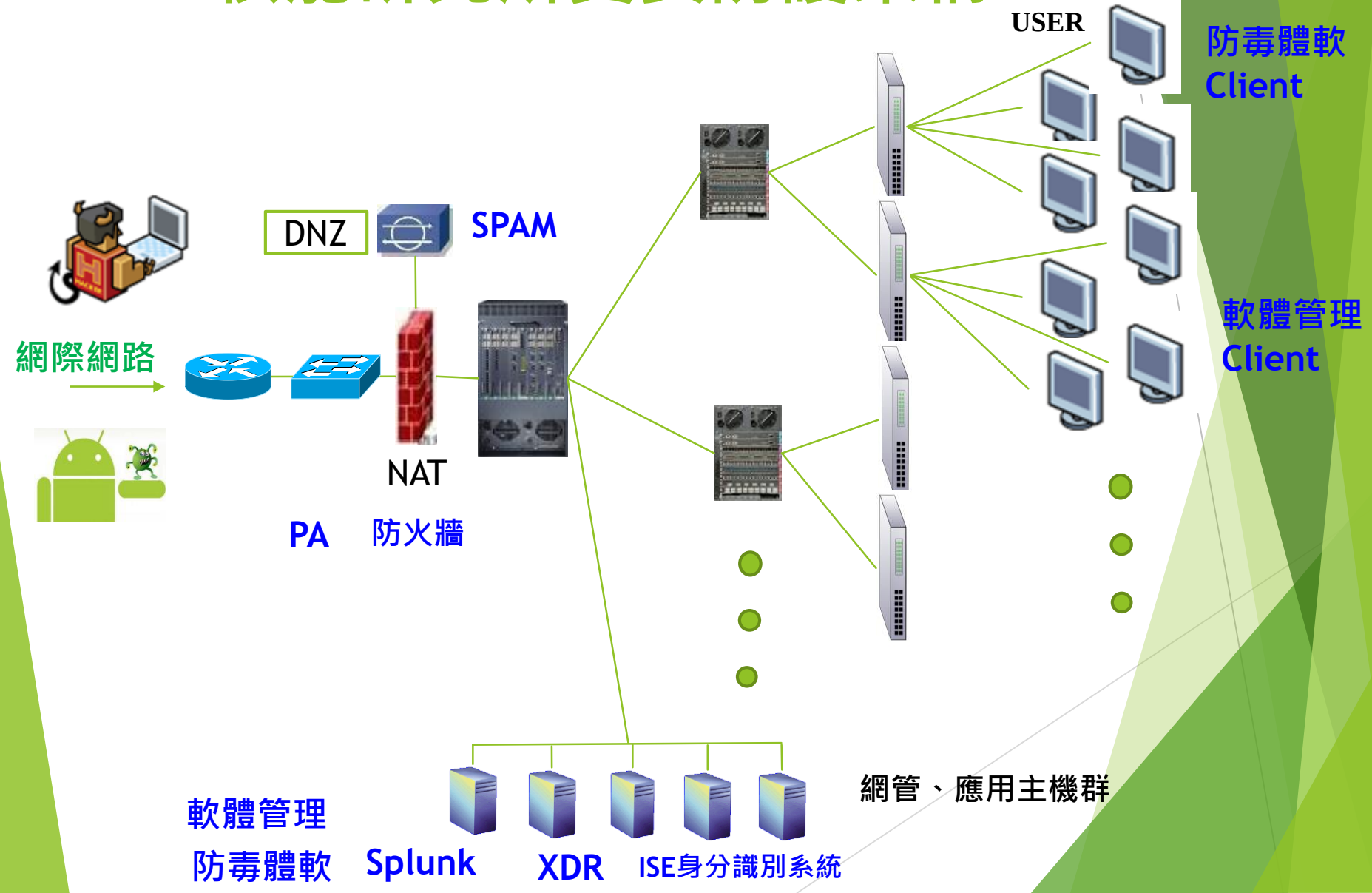


社交工程
資安政策
教育訓練

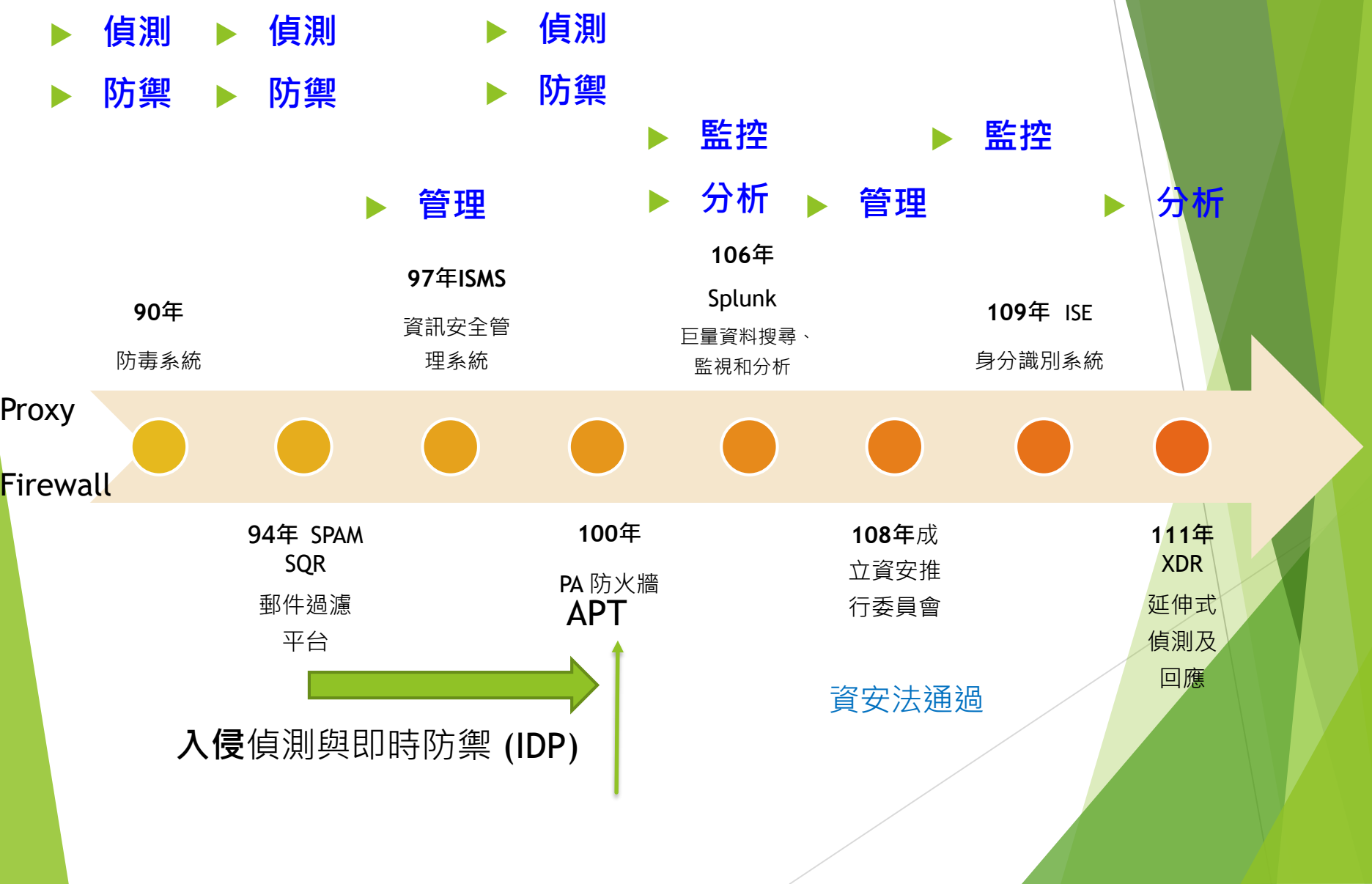
- 導入最新版本ISMS (ISO:27001:2013)
- 動Windows作業系統更新
- 電腦全面安裝防毒軟體
- 定期更新防毒軟體資料庫
- 導入XDR
- 資通安全威脅偵測管理，以Splunk持續監控中
- 持續佈署政府組態基準
- 弱點掃描，每月一次
- 滲透測試，排定於ISMS中委外辦理
- 導入Vans (資通安全弱點通報機制)
- 資通安全防護

Kaspersky、Spam及Palo Alto等資安系統持續有效運作中，並定期檢視相關紀錄。

核能研究所資安防護架構



資安防護建置歷程


偵測
防禦
偵測
防禦
偵測
防禦
管理
監控
分析
管理
監控
分析
90年
防毒系統
97年ISMS
資訊安全管理系統
106年
Splunk
巨量資料搜尋、監視和分析
109年 ISE
身分識別系統
Proxy
Firewall
94年 SPAM
SQR
郵件過濾平台
100年
PA 防火牆
APT
108年成立資安推行委員會
111年
XDR
延伸式偵測及回應
入侵偵測與即時防禦 (IDP)
資安法通過

資安稽核-稽核平台

- 稽核工具：Splunk Enterprise 大數據監控平台

圖 Splunk Enterprise 監控畫面

資安監控-監控工具

- Splunk Enterprise 大數據監控平台

圖 Splunk Enterprise 監控畫面

資安監控-監控分析

- 稽核工具：Splunk Enterprise 大數據監控平台

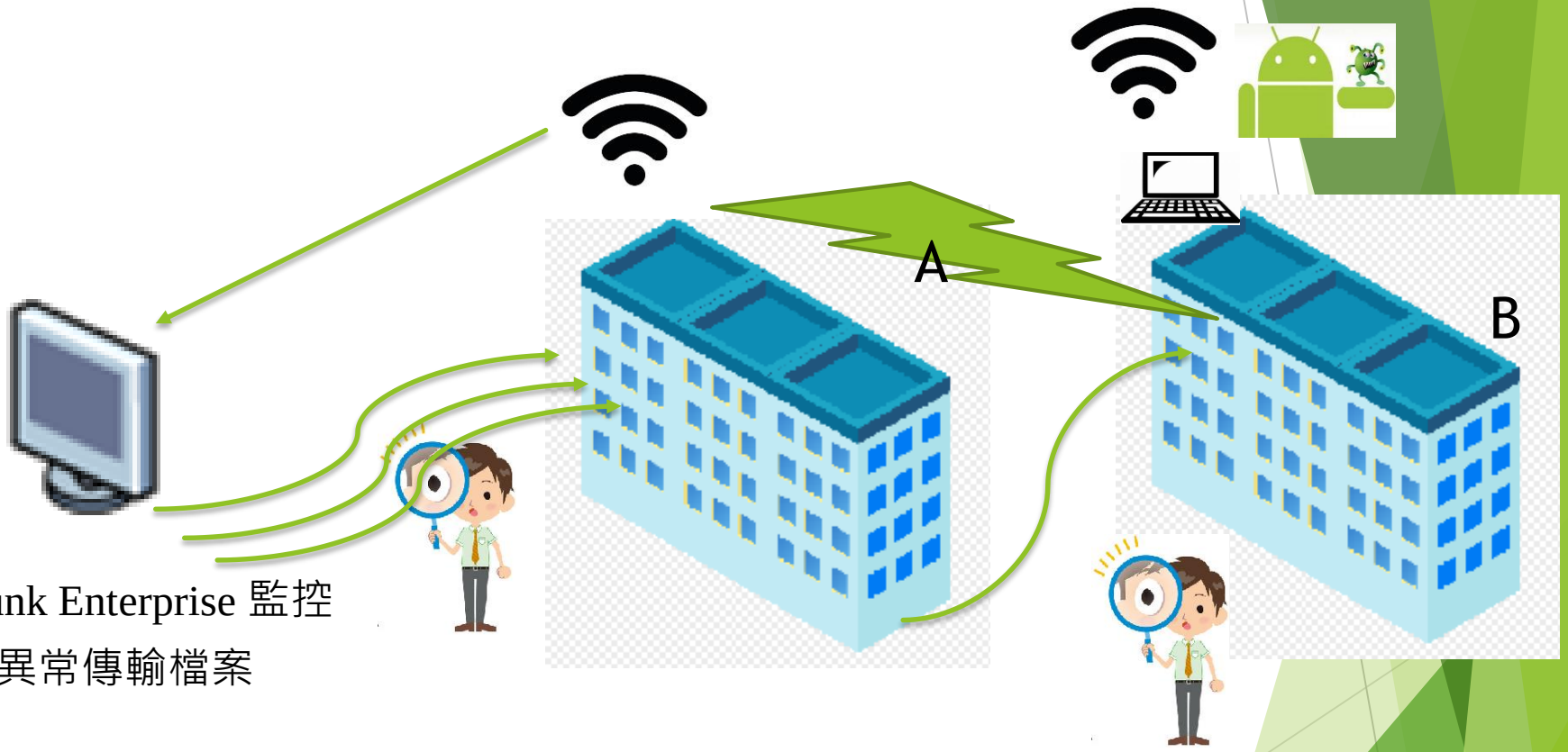
軟體清單

	cn	ou	operatingSystem	AppName	AppBuild	Ap
1	J0653A	綜計組	Windows 10 企業版	Microsoft Windows QFE	1.0.0	SM
				SMR_WEB	16.0.4266.1001	Mi
				Microsoft Office 專業增強版 2016	1.1.1	臺
				土銀網銀憑證安控元件安裝檔 1.0	1.00.0000	KO
				FTP Utility	12/14/2015 3.2.2.0	Ca
				Windows 驅動程式封裝 - Castles Technology (EZUSB) SmartCardReader (12/14/2(5 3.2.2.0)	10.1.6003	您
				EZUSB Driver	1.0	sk
				預算管理系統	1.00.000	宥
				SYBASE OCS 1.0	5.1.50918.0	Mi
				代收代支管理系統	19.00	Ig
				PDF Viewer Installer	16.0.4849.1000	Mi
				Microsoft Silverlight	6.3.4.2	Th
				7-Zip 19.00 (x64)	1.00.000	SH
				商務用 Skype 基本版 2016	20.134.0705.0008	Mi

電腦內安裝的軟體清單

圖 Splunk Enterprise 監控畫面

案例一



Splunk Enterprise 監控

異常傳輸檔案

案例二

今天 ▾

符合 4 個事件，共 207,574 個

工作 ▾

4 results　每頁 50 個 ▾

	_time	source_ip	電腦名稱	dest_ip	dest_location	bytes	application
1	2021/12/16 11:00:34	192.168	J0879A	163.29.207.132	Taiwan ROC		web-browsing
2	2021/12/16 10:59:40	192.168	I2465A	152.199.43.245	United States		web-browsing
3	2021/12/16 10:57:19	192.168.	I1441A-6218	91.250.100.76	France		web-browsing
4	2021/12/16 10:57:19	192.168.	I1441A-6218	91.250.100.76	France		web-browsing

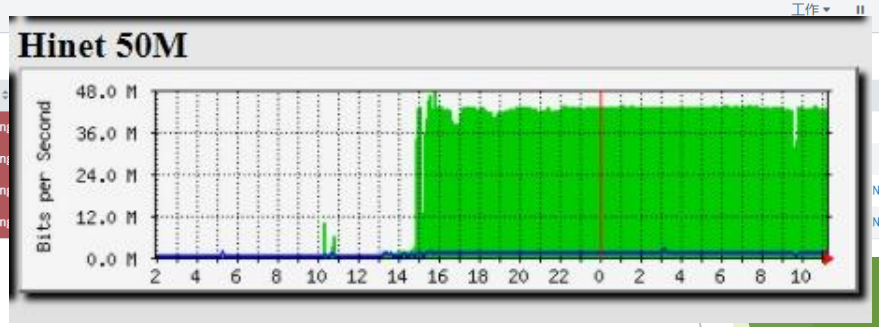


圖 監控紀錄

- **監控可疑上傳檔案事件**
  - A組筆電疑似往中國持續傳輸檔案

    稽查結果：手機內裝中國通訊軟體，

    處理：同仁已不使用本所 wifi
  - B組筆電疑似往中國持續傳輸檔案：導致流量持續上升，並佔滿本所其中一條對外頻寬

    稽查結果：筆電內被植入木馬，且未安裝本所防毒軟體

    處理：掃毒，安裝防毒軟體
  - 透過 Splunk Enterprise 監控流量

未來展望與問題

展望

- ISO精神：建立完整制度，持續修正改善
- 人才培養：教育訓練
- 建立全方位防護：資安整合是全方位，無法單打獨鬥

問題

- 人力不足
- 籌措經費

感謝聆聽指教!!!