

教育體系資安檢核技術服務中心

Taiwan Academic Network Center for Cyber Security Technology



教育部資通安全稽核技術與經驗分享

報告人

教育體系資安檢核技術服務中心

副級檢核員 蔡文君

簡介

- 前言
- 技術檢測流程
- 技術檢測內容
- 總結報告
- 常見問題
- 意見交流

前言

- 依據受稽單位所提供之基本資料，運用不同面向之資安服務衡量構面及表現指標，採現場、臨機方式進行技術檢核
- 技術檢核結果將為其他部分檢核之參考(如實地稽核)
- 協助發掘學校內部問題，提供修正建議參考



找麻煩？



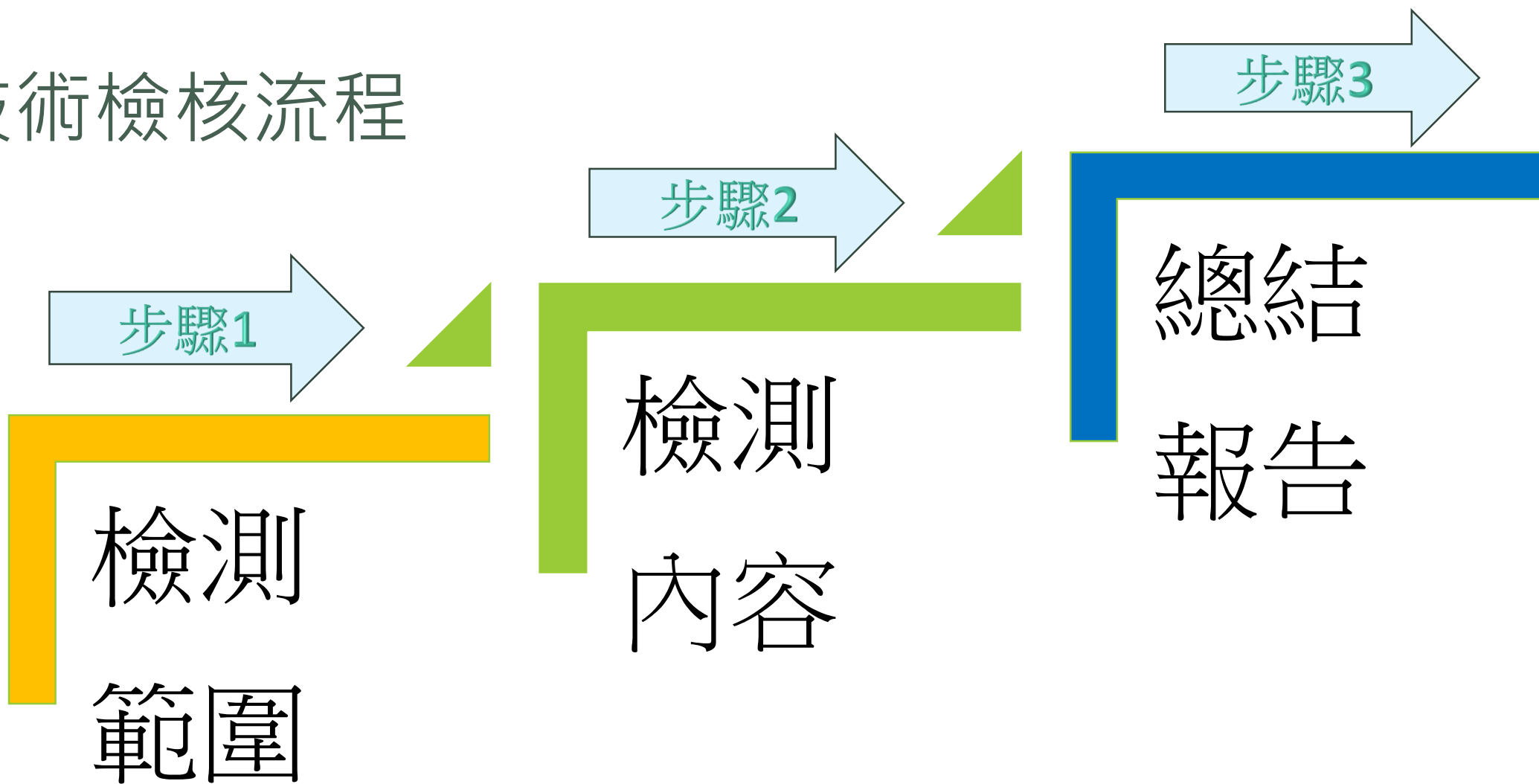


技術檢核(NCCST)

實地稽核(教育部)



技術檢核流程



技術檢測流程(前)：確認檢核範圍

附表三 資通安全責任等級 B 級之公務機關應辦事項

技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	

技術檢測流程(前)：確認檢核範圍

附表三 資通安全責任等級 B 級之公務機關應辦事項

	目錄伺服器設定及防火牆連線設定檢視	
資通安全威脅偵測管理機制	初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。	
政府組態基準	初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。	

技術檢測流程(前)：確認檢核範圍

附表三 資通安全責任等級 B 級之公務機關應辦事項

資通安全 防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
	網路防火牆	
	具有郵件伺服器者，應備電子郵件過濾機制	
	入侵偵測及防禦機制	
	具有對外服務之核心資通系統者，應備應用程式防火牆	

技術檢測流程(前)：確認檢核範圍

資通安全責任等級
(大專院校—**B**級)

機關提供之受檢範圍
(**IP Range**)

個人電腦部署、網路架構、
防火牆設定、**GCB**導入、系
統更新與修補、物聯網設備
及防毒軟體部署及更新情形

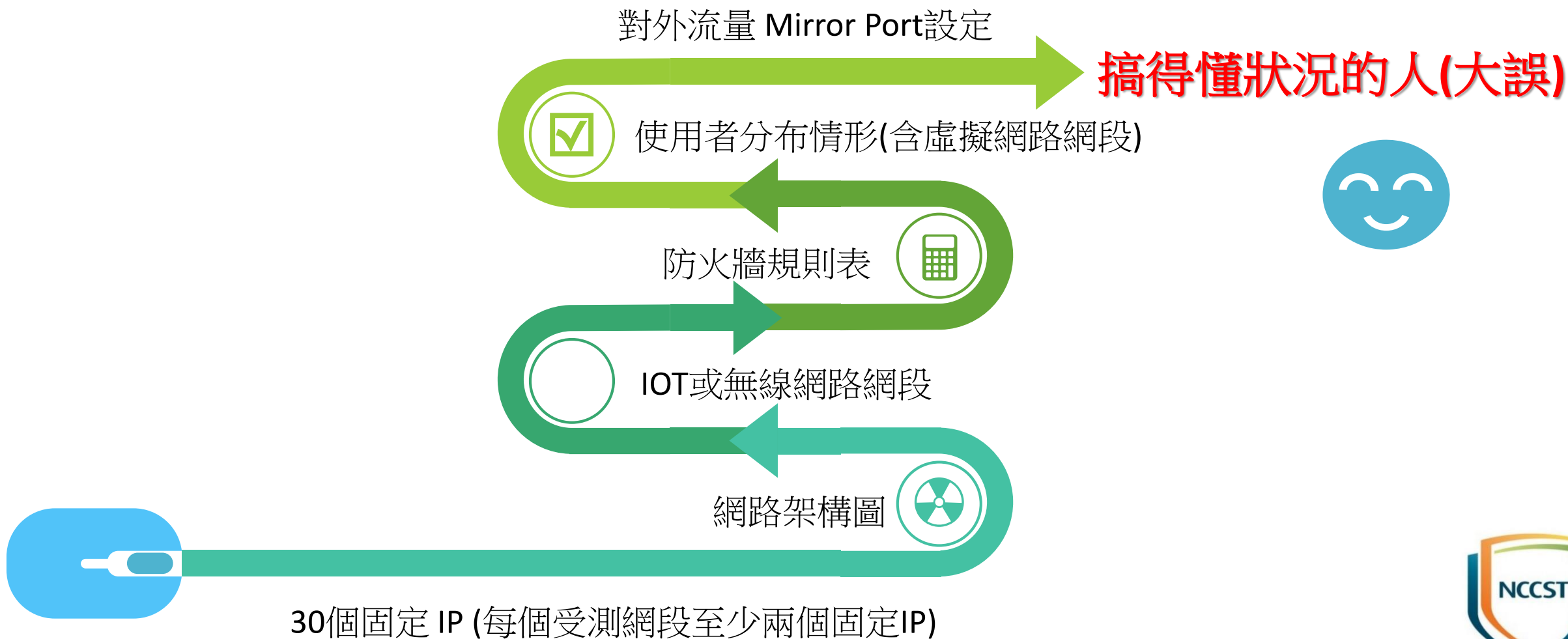


依單位資通安全維護計
畫律定核心與非核心資
通系統目標

(單位如導入**ISMS**，目標應相同)

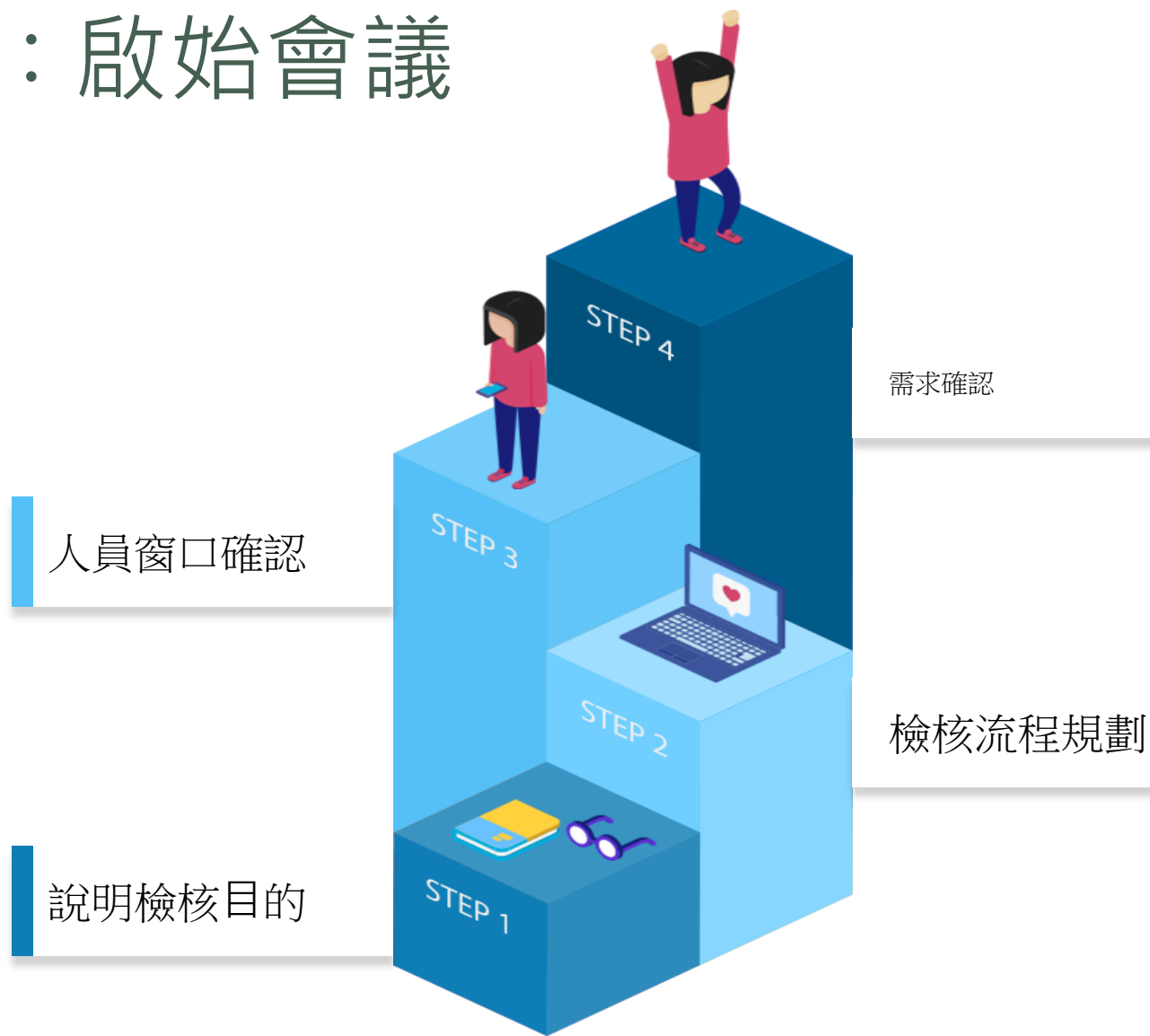


技術檢測流程(前)：受檢方檢核前準備



技術檢測流程 (中)：啟始會議

- 說明檢核目的
- 檢核流程規劃
- 人員窗口確認
- 需求確認



技術檢測內容



使用者電腦安全
檢核



網路惡意活動檢核



核心資訊系統安全
檢核



網路架構檢核



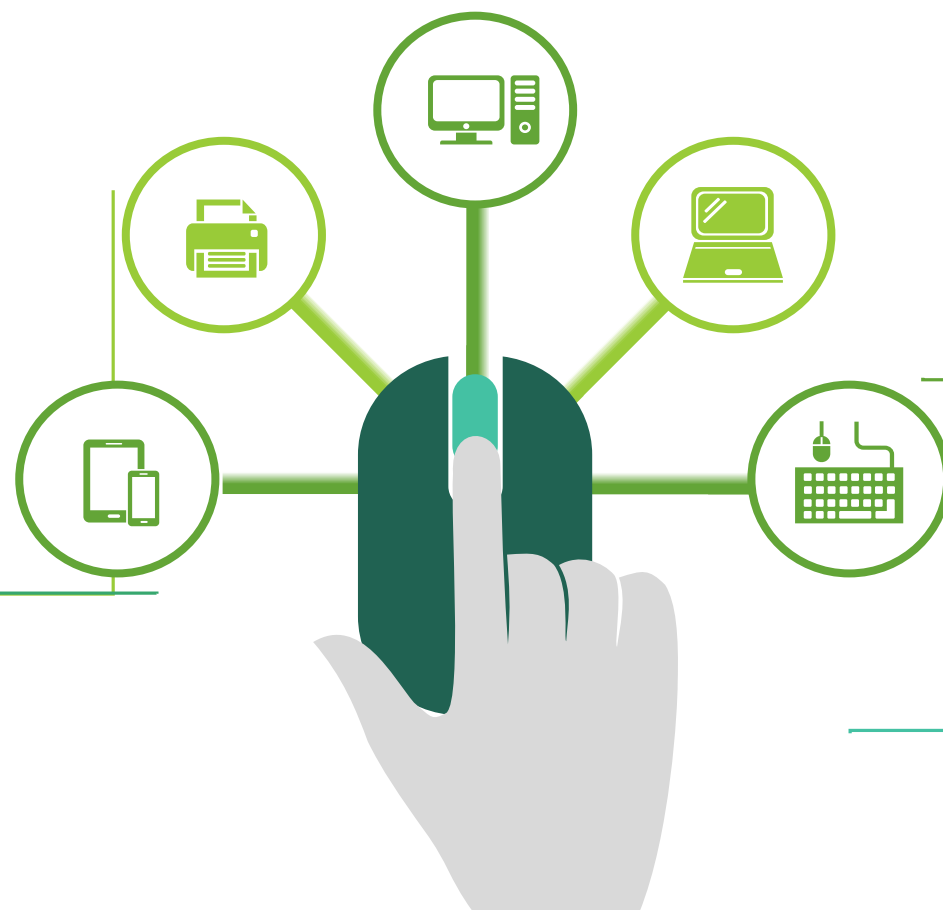
目錄伺服器安全
檢核



物聯網設備檢核



組態設定安全檢核



行政單位

計網中心

教學單位

計畫單位

40%

20%

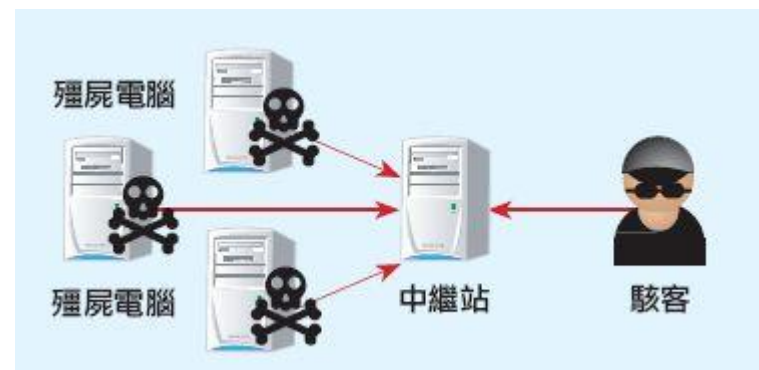
20%

20%



網路惡意活動檢核

- 依行政院國家資通安全會報技術服務中心最新公告之惡意中繼站C2名單(IP & DN)，針對所有使用者網段檢測惡意中繼站阻擋情形
- 伺服器異常網路活動
- 個人電腦異常網路活動
- 網路設備異常網路活動
- 惡意活動檢測→側錄6小時封包，結果進行分析



核心資訊系統安全檢核

目標與作法

內網滲透測試
系統防護基準
GPO/GCB
OWASP TOP 10



存取控制情形
稽核與可歸責性(Log Server)
營運持續計畫(BCP)
檢測前，一定要先備份核心系統作業系統、資料庫與紀錄檔
採灰箱測試，須提供測試帳號
僅針對單位提供之伺服器實施(核心系統清單)



核心資訊系統安全檢核：內網滲透測試風險等級說明

項次	風險等級	說明
1	高	存在已知的弱點或漏洞，且具有立即入侵的可能性，應立即採取補救措施
2	中	存在已知的弱點或漏洞，有較高的可能被利用並攻擊，建議立即採取修正措施
3	低	較不易被利用或攻擊的弱點，不需立即採取補救措施
4	建議	僅存在可能被進一步建議利用之資訊

核心資訊系統安全檢核：弱點類型

項次	說明
1	注入攻擊（INJECTION）
2	無效的身分認證（BROKEN AUTHENTICATION）
3	機敏資料外洩（SENSITIVE DATA EXPOSURE）
4	XML外部處理器漏洞（XML EXTERNAL ENTITIES（XXE）
5	無效的存取控管（BROKEN ACCESS CONTROL）
6	不安全的 的組態設定（SECURITY MISCONFIGURATION）
7	跨網站腳本攻擊（CROSS-SITE SCRIPTING（XSS）
8	不安全的反序列化漏洞（INSECURE DESERIALIZATION）
9	使用已知漏洞元件（USING COMPONENTS WITH KNOWN VULNERABILITIES）
10	紀錄與監控不足風險（INSUFFICIENT LOGGING & MONITORING）
11	應用程式或系統弱點

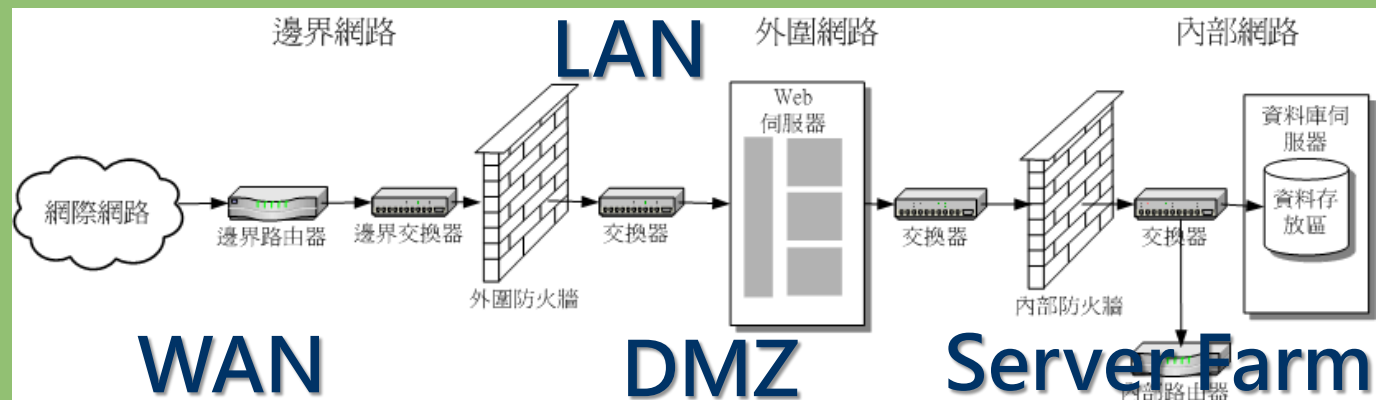


網路架構檢核



訪談為主(透過訪談
與實際檢視方式驗
證)

查看網路架構分區落實情形



網路架構、網路區域間的存取、
入侵偵測/防禦系統、系統本機
安全機制、實體、服務備援機
制



內對外連線、外對內連線、服務區域連線、防火牆規則、資料傳輸、第三方連線控制、遠端連線存取控制、網通設備存取、SNMP設定、校時設定



網域主機安全防護檢核

安全性更新

安全性修補程式(重大 CVE 更新???????)

Microsoft® Update Catalog

KB4571694

Search

Search results for "KB4571694"

Updates: 1 - 3 of 3 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	
2020-08 適用於 x64 系統 Windows Server 2016 的累積更新 (KB4571694)	Windows Server 2016	安全性更新	2020/8/10	n/a	1596.7 MB	Download
2020-08 適用於 x64 系統 Windows 10 Version 1607 的累積更新 (KB4571694)	Windows 10, Windows 10 LTSB	安全性更新	2020/8/10	n/a	854.0 MB	Download
2020-08 適用於 x64 系統 Windows 10 Version 1607 的累積更新 (KB4571694)	Windows 10, Windows 10 LTSB	安全性更新	2020/8/10	n/a	1596.7 MB	Download

© 2020 Microsoft Corporation. All Rights Reserved. | [privacy](#) | [terms of use](#) | [help](#)

安全性更新

防毒軟體

異常程序、常駐程式或自動啟動程式

異常程序

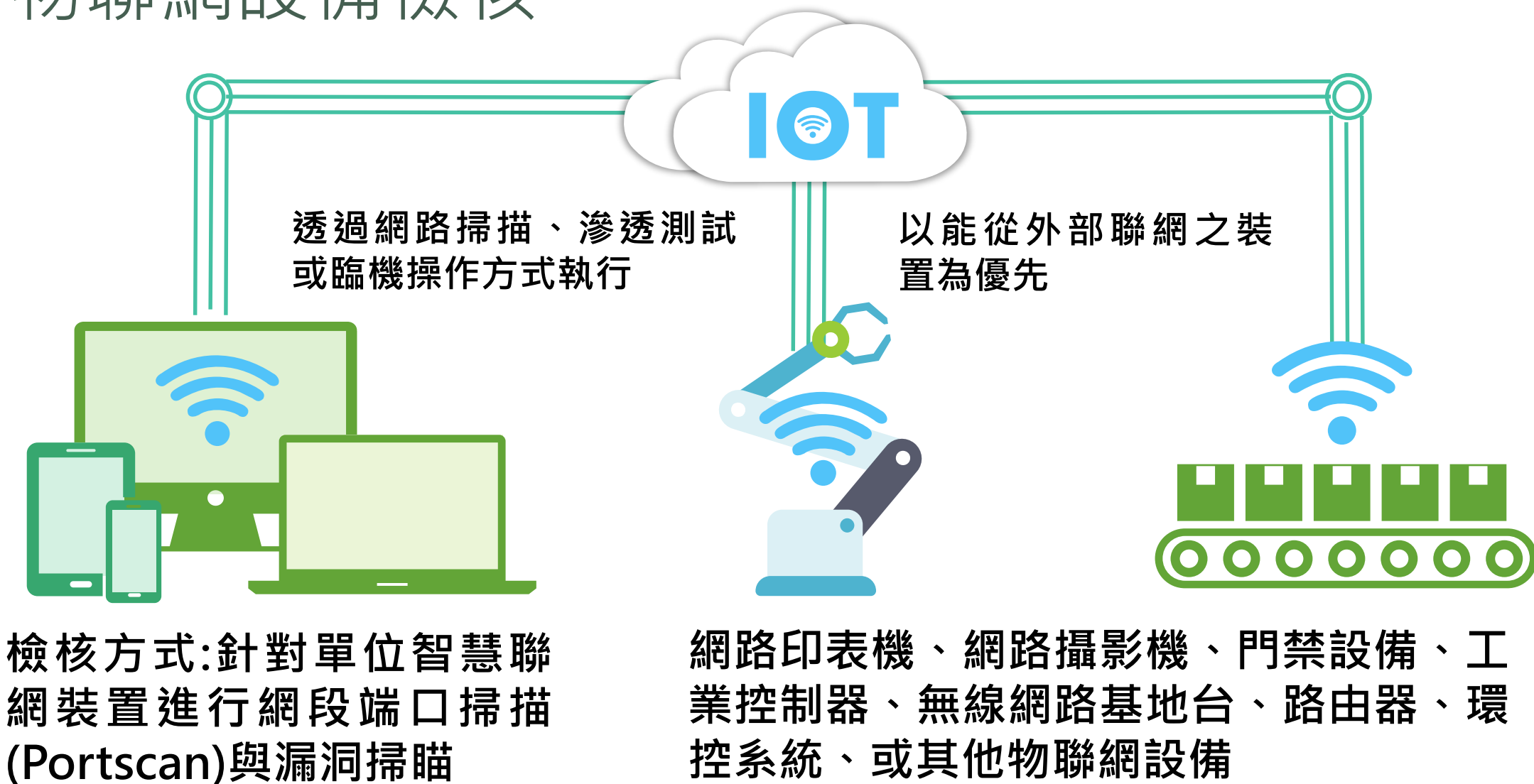
利用工具與人工方式針對目錄伺服器檢核是否遭植入惡意程式
植入mimikatz????

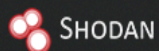
防毒軟體

防毒軟體(Antivirus)安裝、更新與每日掃描情形



物聯網設備檢核





IOT



Explore

Pricing

Enterprise Access

New to Shodan?

Login or Register

Exploits

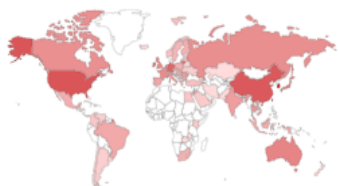
Maps

Images

TOTAL RESULTS

7,376

TOP COUNTRIES



Korea, Republic of	2,987
Taiwan	804
United States	600
China	538
Germany	367

TOP SERVICES

SNMP	2,387
8081	1,111
8083	1,087
HTTPS	631
SSH	327

TOP ORGANIZATIONS

SK Telecom	1,694
Korea Telecom	847
Amazon.com	623
Taiwan Academic Network	354
HiNet	333

TOP OPERATING SYSTEMS

Windows 6.1	6
Unix	2
Windows 10 IoT Enterprise 18363	2

TOP PRODUCTS

lighttpd	2,086
OpenSSH	303

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

301 Moved Permanently

167.172.147.64

Digital Ocean

Added on 2020-12-28 05:31:58 GMT

United States, North Bergen

cloud

HTTP/1.1 301 Moved Permanently
 Server: nginx
 Date: Mon, 28 Dec 2020 05:31:55 GMT
 Content-Type: text/html
 Content-Length: 178
 Connection: keep-alive
 Location: <https://iot-lora.us/>

139.9.136.195

ecs-139-9-136-195.compute.hwclouds-dns.com

Huawei Cloud Service data center

Added on 2020-12-28 05:30:19 GMT

China

cloud

DCE/RPC Endpoint Mapper
 Max Count: 500
 Actual Count: 500
 Number of Entries: 500

Mapped services:
 UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d
 IP Address: 192.168.0.225
 TCP Port: 49664

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d
 ncalsrc: WindowsShutdown

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d
 ...

Daikin IoT

35.162.36.54

ec2-35-162-36-54.us-west-

2.compute.amazonaws.com

Amazon.com

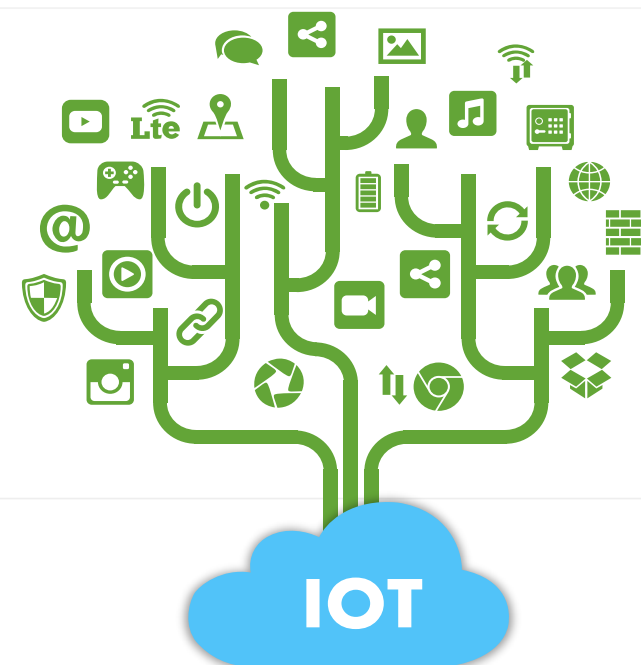
Added on 2020-12-28 05:37:10 GMT

United States

Technologies: Envoy

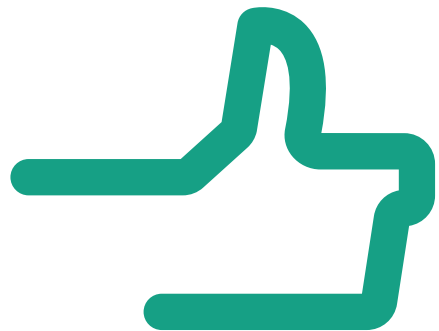
cloud

HTTP/1.1 200 OK
 x-daikin-request-id: undefined
 x-service-id: baded280-48ce-11eb-a9b1-71789d055c72
 content-type: text/html; charset=utf-8
 content-length: 6515
 etag: W/"1973-o3dD0v3xgD1LhFHLdrb6Q"
 set-cookie: daikin-**iot**=s%3APk9ppDqB5U6rBuZHdmkXPworGLLPe0Ai.m3tEMs7x%2F1BFQjTAjgwvqmKZpbBN8xES...





- 學校是否導入AD
- GPO派送情形
- 透過政府組態基準(GCB)進行掃描(遴選五台電腦)，運用盤點程式，針對瀏覽器、網通設備與應用程式進行檢測，並確認組態設定安全防護情形



免害怕?????



- 證據要明確，弱點要能重現
- 更新版本以機關認定為主；除非有重大 CVE(如 [CVE-2020-1472](#) : ZeroLogon，CVSS 風險指標為 10 分)
- 嚴禁插入攻擊代碼或植入惡意木馬
- 客觀且須具同理心
- 簽具保密協議

- 稽核證據整理
- 各項目報告產出 (三日內)
- 技術檢核結果彙整 (一周內)
- 總報告產出 (一周內)

總結報告

資安技術檢核總報告

檢核單位名稱：_____

檢核案件編號：_____

教育體系資安檢核技術服務中心

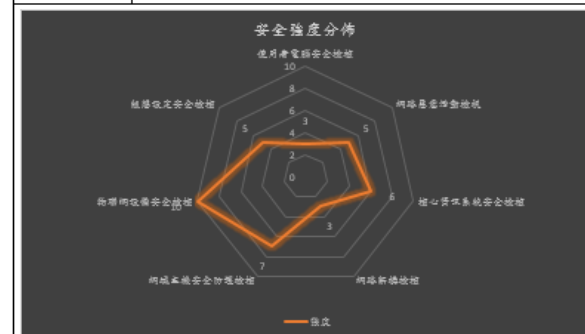
[電子郵件地址]

教育體系資安檢核技術服務中心

文件名稱	資安技術檢核總報告	機密等級	極機密
文件編號	TACCST-B-02-06	版次	V2.0

壹、檢核結果摘要

檢核單位	
報告資訊	○○○年度教育體系資安技術檢核結果報告
機密等級	☒ 極機密 ☐ 機密 ☐ 內部使用
技術檢核團隊	● 主導技術檢核員： ● 技術檢核員：
撰稿人員	
安全強度分佈	



內容摘要：

教育體系資安檢核技術服務中心(以下稱本中心)執行_____ (單位名稱)○○○年度安全技術檢核作業，技術檢核範圍涵蓋七大領域：

1. 使用者電腦安全檢核
2. 網路惡意活動檢核

常見問題



預設帳密

IOT設備

網站(頁)錯誤訊息過度暴露

Patch Update

GCB 導入

NTP校時



網站與資訊設備預設設定(Shodan)

惡意中繼站阻擋率

老師、學生難搞，難防**橫向感染**(lateral movement)

未依SSDLC流程設計軟體(程式)

樹莓派?台灣派? Tinker Board?香蕉派?工業控制器?

OS or Firmware Update

資訊服務是王道??



教育體系資安檢核技術服務中心

Taiwan Academic Network Center for Cyber Security Technology



意見交流



感謝您為資安盡一份心力

教育體系資安檢核技術服務中心

Taiwan Academic Network Center for Cyber Security Technology