資安事件通報與應變

TWCERT/CC

台灣電腦網路危機處理暨協調中心

課程簡介

課程目標

- 掌握資安事件處理原則與程序
- 檢視組織內部資安事件應變作業程序之適切性與有效性

課程重點

- 資安事件識別與判斷
- 資安事件處理原則與程序

課程規劃

時間	內容
13:00-13:50	資安事件概述
13:50-14:00	中場休息
14:00-14:40	資安事件案例分享
14:40-14:50	中場休息
14:50-15:30	資安事件應變與處理

課程大綱

- **資安事件處理簡介**
  - 資安事件基本概念
  - 資通安全事件通報及應變辦法
- **資安事件案例分享**
- **資安事件應變與處理**
  - 事前準備
  - 事中應變
  - 事後改善

【資安事件處理簡介】

資安事件基本概念

資安事件基本概念 (1/14)

什麼是**資安事件**?

為什麼要**處理資安事件**?

資安事件基本概念 (2/14)

- **資通安全**
  - 指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以**確保其機密性、完整性及可用性**
- **資通安全事件**
  - **指系統、服務或網路狀態** 經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅
- **資通系統**
  - 指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統

※資通安全管理法，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297

資安事件基本概念 (3/14)

Equifax就資料外洩事件與FTC和解，和解金額上看7億美元

美國第三大消費者信用報告業者Equifax在2017年被駭客入侵，導致1億多位消費者的個資外洩，其實美國政府曾在事發前警告Equifax內部系統有安全漏洞，但Equifax卻未有效修補，才釀成此一重大資安事件

GoDaddy被駭客竊走公司程式碼，並在代管服務植入惡意程式多年

在去年底部分用戶反映網站遭到重導向攻擊後，GoDaddy才發現代管服務遭駭，導致公司程式碼被竊及植入惡意程式，進而波及用戶網站

若能**及早發現**，**及早處理**，是不是就...

資料來源: iThome

資安事件基本概念 (4/14)

Uber前安全長Joe Sullivan因蓄意隱瞞資料外洩事件被起訴

Uber前安全長Joe Sullivan於任內對資料外洩事件隱匿不報，並支付了價值10萬美元的比特幣予駭客訂定保密協議，遭美國司法部以妨礙司法及隱匿重大犯罪起訴

調查顯示，駭客在2016年成功入侵Uber，盜走了5,700萬名Uber乘客與司機的資料，內含乘客姓名、電子郵件帳號及行動電話號碼，以及60萬名美國Uber司機的駕照資料。

- 事件發生一年後曝光，**損害擴大**
- 公司臨法律訴訟和巨額罰款
- 公司**信譽受損**，並失去了大量客戶信任

資料來源: iThome

資安事件基本概念 (5/14)

- 資安事件處理的目的是儘快恢復營運，並進行損害控制避免事件擴大，預防事件發生

- 事件根因分析與改善
- 事件回顧與強化

- 預防事件的發生
- 事件處理的前置準備

- 事件通報
- 分析與影響評估
- 損害控制與復原

資安事件基本概念 (6/14)

識別資安事件

什麼是資安事件

通報資安事件

分析與影響評估

- 影響等級
- 事件類型

損害控制與復原

緊急止損，預防擴散

事後改善處置

事件根因分析

擬定補強措施

資安事件基本概念 (7/14)

What

- 指**系統、服務或網路狀態**經鑑別而顯示可能有**違反資通安全政策**或**保護措施失效**之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅

(資通安全管理法第3條)

When

- 公務機關知悉資通安全事件後，應於一小時內依**主管機關指定之方式**及對象，進行資通安全事件之通報

(資通安全通報及應變辦法第4條)

How

- 主管機關指定之方式：國家資通安全通報應變網站(https://www.ncert.nat.gov.tw/)辦理通報業務

(資安署官網 - 資安法常見問題)

資安事件基本概念 (8/14)

- 資通安全的核心目標 CIA 資安鐵三角 (CIA triad)

機密性(Confidentiality)

- 確保資訊只被授權的個人或系統存取

防止資料外洩

完整性(Integrity)

- 確保資料在傳輸、儲存及處理過程中，資料保持正確性和一致性

防止未經授權的修改或破壞

可用性(Availability)

- 確保合法使用者在需要時能夠可靠地存取資訊和系統

防止非預期服務/運作中斷

資安事件基本概念 (9/14)

OpenAI遭DDoS攻擊，ChatGPT斷線近24小時

本周ChatGPT及API服務陸續發生數次斷線，OpenAI維護團隊研斷事故原因是來自DDoS

可用性

Jansport、North Face母公司去年被駭，3500萬筆用戶資料被竊走、訂單延遲交付

機密性

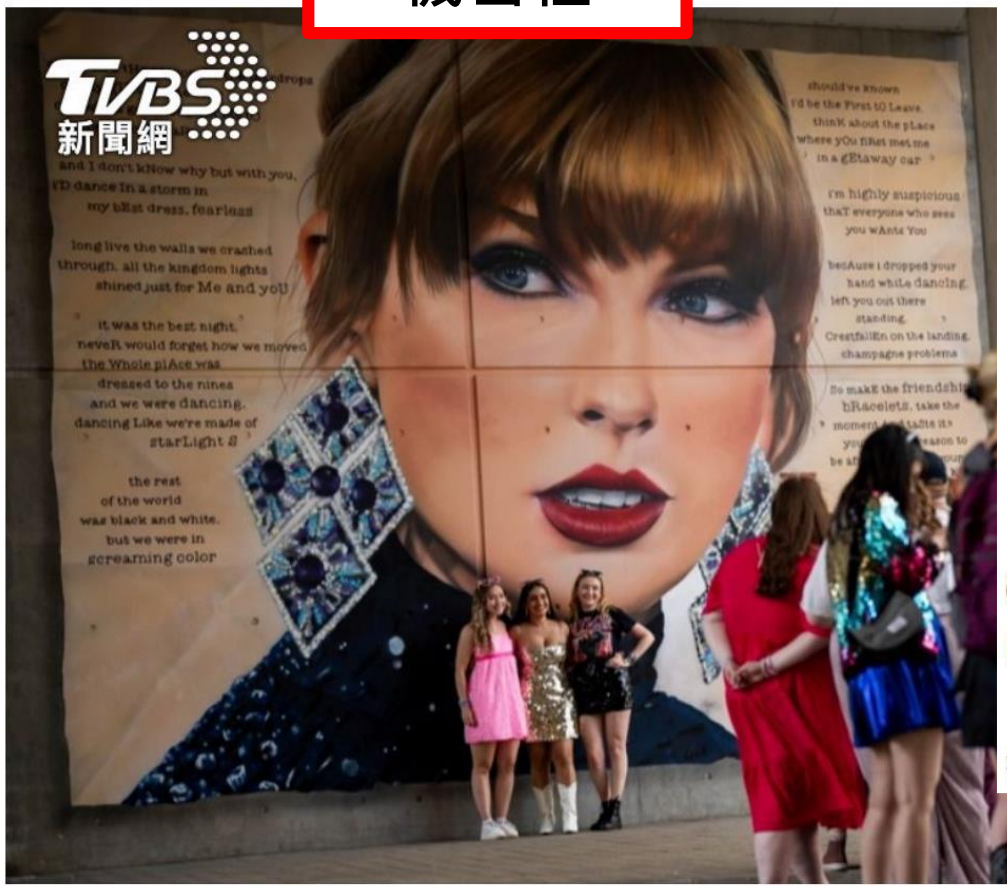
資料來源: iThome

資安事件基本概念 (10/14)

泰勒絲演唱會購票個資被駭 遭勒索百萬美元贖金

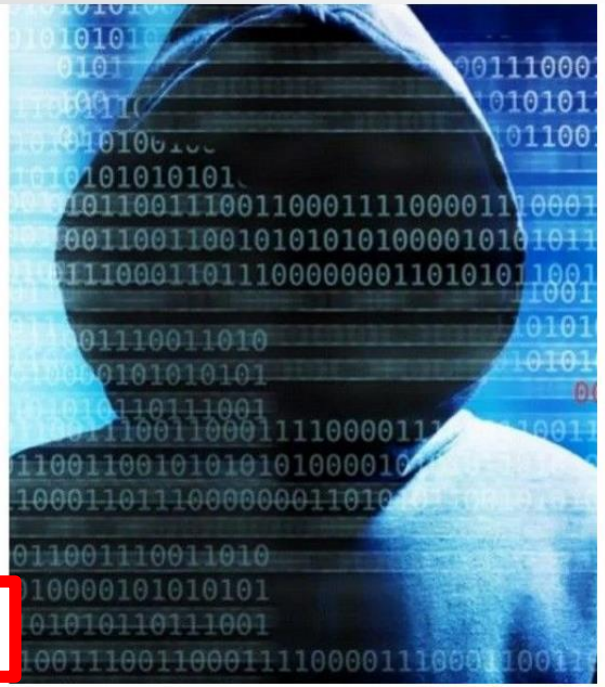
編輯 龔芸可 / 責任編輯 編輯組 報導
發佈時間：2024/07/06 16:39
最後更新時間：2024/07/06 20:1

機密性



駭客組織ShinyHunters聲稱其駭得大量泰勒絲「The Eras Tour」巡演的購票者個資。（圖 / 達志影像美聯社）

▼角川遭駭客攻擊。（圖 / 翻攝自KADOKAWA、資料照）



KADOKA

可用性

6 月初角川集團網域伺服器受到大規模攻擊，導致官方網站、角川旗下電子商城 ebten、Niconico 影音平台 Niconico 直播無法正常運作。根據 NHK 新聞報導，駭客集團「BlackSuit」承認犯案竊取了公司包含商業合約、業務企劃、用戶個資等多達 1.5 TB 數據，甚至向角川勒索贖金，否則 7 月會陸續公開機密資料。

機密性

資料來源: iThome

資安事件基本概念 (11/14)

新聞

駭客利用NVR視訊監控影像儲存主機與路由器的零時差漏洞，散布變種Mirai殭屍病毒

資安業者Akamai發現駭客正在利[illegible]控影像儲存主機（NVR）與路由器的零時差漏洞，散布JenX Mirai變種病毒，建立

完整性

美晶片設備商MKS Instruments遭勒索軟體攻擊，影響生產系統！供應鏈風險受關注，應材因供應商資安事故估下季營收少2.5億美元

完整性

可用性

新聞

配置錯誤讓微軟AI研究單位的GitHub儲存庫外洩38TB私有資料

資安業者Wiz發現微軟員工在共用存取簽章（SAS）權杖上的配置錯誤，讓微軟38TB的私有資料因此外洩

機密性

資料來源: iThome

資安事件基本概念 (12/14)

資料來源: iThome

資安事件基本概念 (13/14)

- 資安事件類型

非法入侵	網頁攻擊	設備問題	阻斷服務 (Dos/DDoS)
• 系統遭入侵 • 植入惡意程式 • 異常連線 • 發送垃圾郵件 • 資訊外洩	• 網頁置換 • 惡意留言 • 惡意網頁 • 釣魚網頁 • 網頁木馬	• 設備故障/毀損 • 電力異常 • 網路服務中斷 • 設備遺失	• 服務中斷 • 效能降低

資安事件基本概念 (14/14)

- 事件發生原因

非法入侵

- 作業系統漏洞
- 弱密碼/密碼遭暴力破解
- 應用程式漏洞
- 網站設計不當
- 廠商維護環境或管理疏失
- 無法確認事件原因
- 其他
- 社交工程

無法確認事件原因

無相關紀錄檢視
相關紀錄遭異常刪除/變更
受限於資安人力/預算無法調查
逕行重建無法調查
系統汰換逕行下架
事件調查後仍無法確認原因

網頁攻擊

- 作業系統漏洞
- 弱密碼/密碼遭暴力破解
- 應用程式漏洞
- 網站設計不當
- 廠商維護環境或管理疏失
- 無法確認事件原因
- 其他
- 人為疏失
- 設定錯誤

其他

- 作業系統漏洞
- 弱密碼/密碼遭暴力破解
- 應用程式漏洞
- 網站設計不當
- 廠商維護環境或管理疏失
- 無法確認事件原因
- 其他
- 人為疏失
- 設定錯誤
- 設備異常/毀損
- 電力供應異常
- 社交工程

設備問題

- 設備異常/毀損
- 電力供應異常
- 人為疏失
- 設定錯誤
- 商維護環境或管理疏失
- 無法確認事件原因
- 其他

阻斷服務(Dos/DDoS)

- 阻斷服務(Dos/DDoS)

Exercise – 識別資安事件

- 印表機被透過FTP植入挖礦程式

YES

NO

資通系統

指用以蒐集、控制、**傳輸**、**儲存**、流通、刪除資訊或對資訊為其他處理、使用或分享之系統

Exercise – 識別資安事件

- 印表機被透過FTP植入挖礦程式

YES

NO

資通系統遭植入惡意程式，即**完整性受衝擊**，構成資安事件

Exercise – 識別資安事件

- 官網排定於週六下午進行版本更新作業，故服務中斷3小時，已事先公告該更新作業

YES

NO

Exercise – 識別資安事件

- 官網排定於週六下午進行版本更新作業，故服務中斷3小時，已事先公告該更新作業

YES

NO

預期性的服務中斷作業，機關已有**相關配套措施**，評估**未影響日常業務**，未違反資通安全政策並保護措施未失效

Exercise – 識別資安事件

- 台電無預警斷電，緊急切換至UPS，持續提供系統服務

YES

NO

Exercise – 識別資安事件

- 台電無預警斷電，緊急切換至UPS，持續提供系統服務

YES

NO

台電無預警斷電，惟**系統服務未受影響**，評估機密性、完整性及可用性未受衝擊

Exercise – 識別資安事件

- 同仁瀏覽網站時，誤觸惡意連結，連至惡意下載站下載惡意程式，該惡意程式即時被防毒軟體偵測並隔離刪除

YES

NO

Exercise – 識別資安事件

- 同仁瀏覽網站時，誤觸惡意連結，連至惡意下載站下載惡意程式，該惡意程式即時被防毒軟體偵測並隔離刪除

YES

NO

檔案**即時**被隔離刪除，**保護措施未失效**，評估機密性、完整性及可用性未受衝擊

【資安事件處理簡介】

資通安全事件通報及應變辦法

資通安全事件通報及應變辦法 (1/2)

- 依資通安全管理法第十四條第四項及第十八條第四項規定訂定之

資安法+6項子法

- **資通安全事件通報及應變辦法**
- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全情資分享辦法
- 特定非公務機關資通安全維護計畫實行情形稽核辦法
- 公務機關所屬人員資通安全事項獎懲辦法

資通安全事件通報及應變辦法

1. **總則**
   - 明定資安事件分級
   - 明定資安事件通報作業之基本通報項目
2. **公務機關資安事件通報應變**
   - 明定通報流程與審核作業
   - 明定資安事件通報規範、應變規範
3. **特定非公務機關資安事件通報應變**
   - 明定通報流程與審核作業
   - 明定資安事件通報規範、應變規範
4. **附則**
   - 配合事項

資通安全事件通報及應變辦法 (2/2)

01 **通報**

知悉後１小時內填報

「4」、「3」級事件：成立緊急應變小組

02 **審核**

「2」、「1」級事件：８小時內

「4」、「3」級事件：２小時內

※ 等級是否適切？

03 **事件處理及損害控制**

「2」、「1」級事件：７２小時內

「4」、「3」級事件：３６小時內

04 **事件調查處理及改善報告**

改善報告呈主管機關

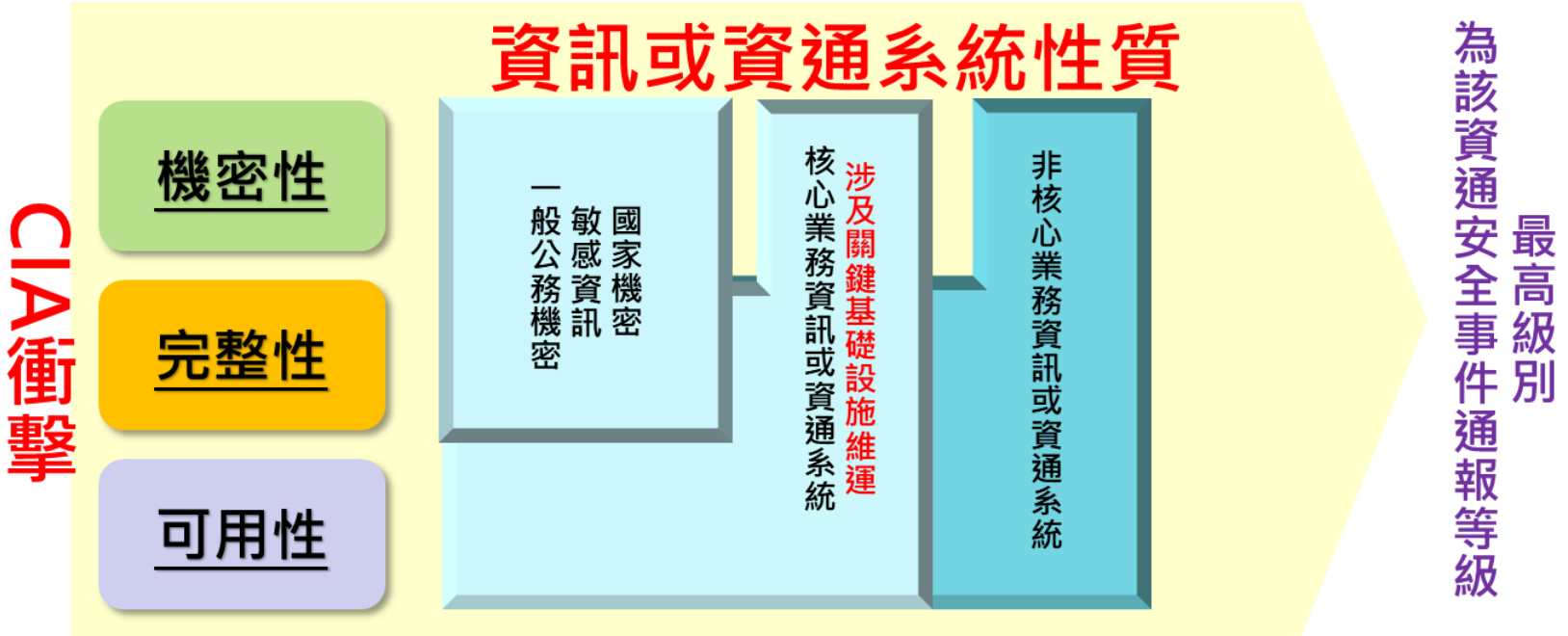
公務機關→上級機關/監督機關→交送「1~4級」

應於１個月內提交，視情況可提出延後提交申請

資安事件等級評估 (1/6)

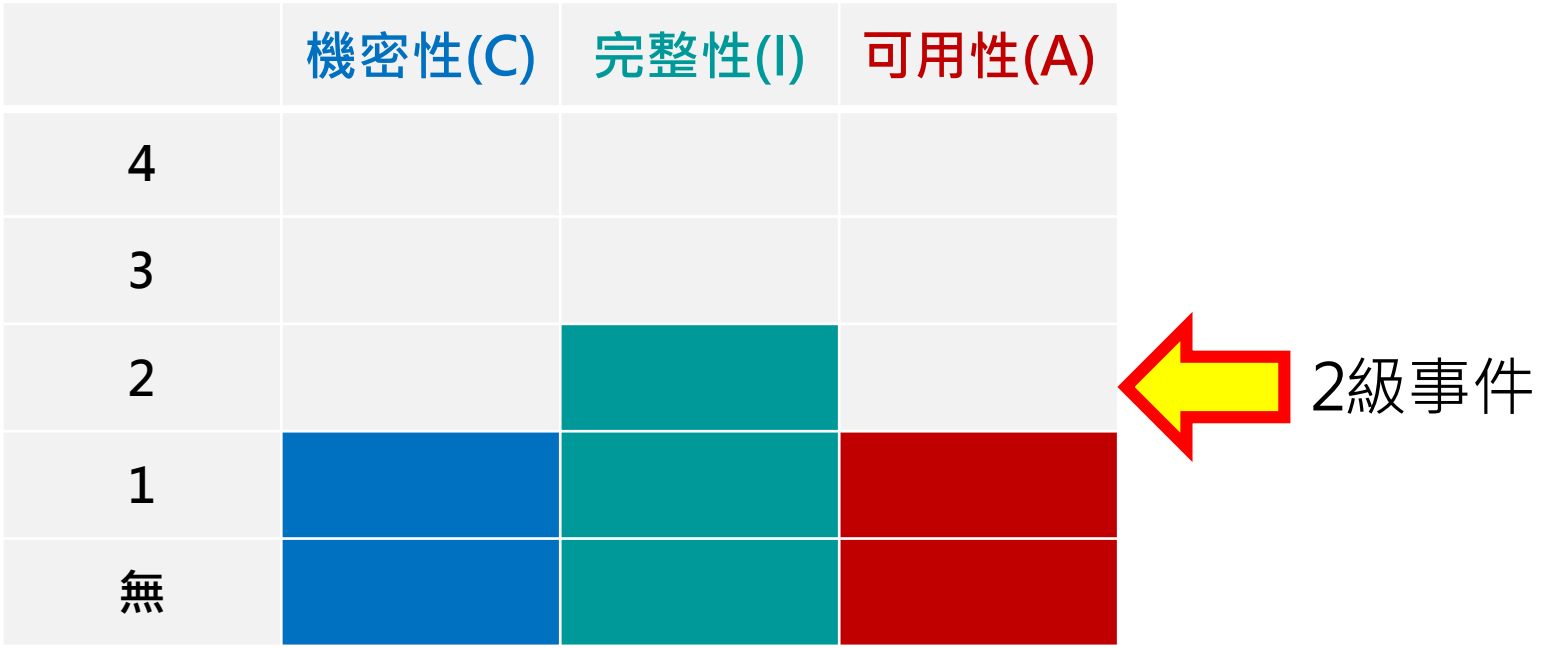
- 資安事件影響等級評定須考量三面向衝擊性
  - 「機密性」衝擊
  - 「完整性」衝擊
  - 「可用性」衝擊

綜合評估資安事件造成之「機密性」、「完整性」及「可用性」衝擊，核判影響等級。



資安事件等級評估 (2/6)

- 資通安全事件由輕至重分「1」、「2」、「3」、「4」四個等級
- 評定資通安全事件分級時，將以資訊或資通系統性質與其CIA衝擊性，綜評該事件等級



資安事件等級評估 (3/6)

- 機密性衝擊評估標準

影響等級		說明
輕微 ↕ 嚴重	1級	非核心業務資訊遭輕微洩漏。
	2級	非核心業務資訊遭嚴重洩漏。
		未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
	3級	一般公務機密、敏感資訊遭輕微洩漏。
		未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏。
		涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
	4級	國家機密資料遭洩漏。
		一般公務機密、敏感資訊遭嚴重洩漏。
		涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏。

- 敏感公務資料：指政府機關(構)持有或保管之資訊，雖非屬密級文件，但所載資訊若遭洩漏，將危害組織或個人之權益。
- 密級公務資料：指政府機關(構)持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。
- 國家機密資料：指為確保國家安全或利益而有保密之必要，對政府機關(構)持有或保管之資訊，經依國家機密保護法核定機密等級者。

資安事件等級評估 (4/6)

- 完整性衝擊評估標準

影響等級		說明
輕微 ↕ 嚴重	1級	非核心業務資訊或非核心資通系統遭**輕微竄改**。
	2級	非核心業務資訊或非核心資通系統遭**嚴重竄改**。
		未涉及關鍵基礎設施維運之**核心**業務資訊或**核心**資通系統遭**輕微竄改**。
	3級	未涉及關鍵基礎設施維運之**核心**業務資訊遭**嚴重竄改**。
		一般公務機密、敏感資訊、涉及關鍵基礎設施維運之**核心**業務資訊或**核心**資通系統遭**輕微竄改**。
	4級	一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊遭**嚴重竄改**。
		核心資通系統遭**嚴重竄改**。
		國家機密遭竄改。

- 輕微竄改/嚴重竄改：由政府機關(構)依竄改所造成之影響**自行認定**其嚴重性。

資安事件等級評估 (5/6)

- 可用性衝擊評估標準

影響等級		說明
輕微 ↕ 嚴重	1級	非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。
	2級	非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。
		未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。
	3級	未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作
		涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。
	4級	涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

- 可容忍中斷時間：政府機關(構)應考量業務性質及影響程度等因素，評定各項核心業務或重要資訊基礎建設可容許的中斷時間。

資安事件等級評估 (6/6)

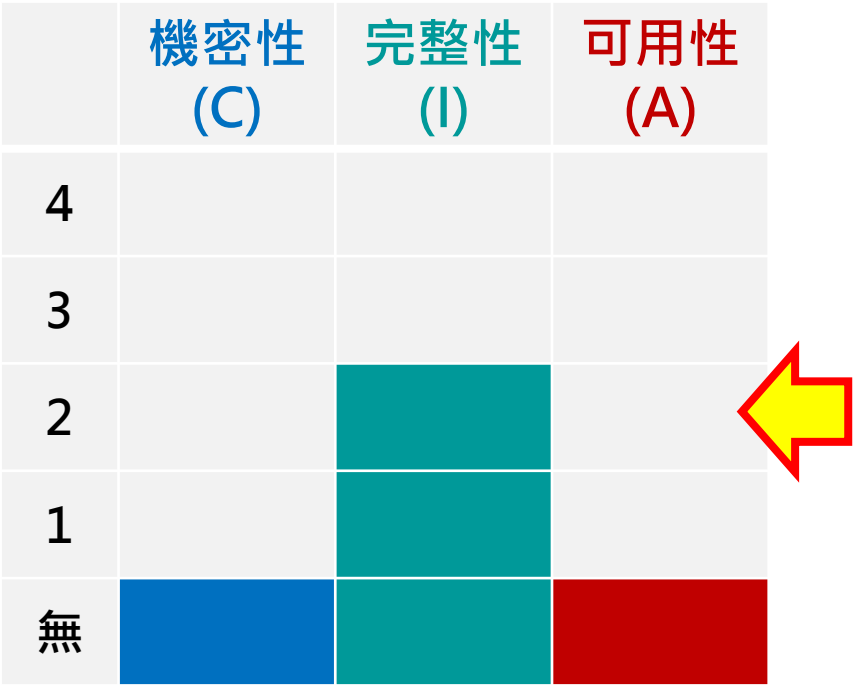
	機密性(C)		完整性(I)		可用性(A)	
	輕微洩漏	嚴重洩漏	輕微竄改	嚴重竄改	<可容忍時間	>可容忍時間
非核心業務/系統	1級	2級	1級	2級	1級	2級
核心業務/系統 (未涉及CI)	2級	3級	2級	3級	2級	3級
核心業務/系統 (涉及CI)	3級	4級	3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級	4級	4級	4級		

資安事件等級參考案例 (1/2)

案情提要

- A機關自行發現內部一系統遭勒索軟體加密，該系統支援**核心業務運作，未涉及關鍵基礎設施相關運作**，目前已用備援系統代替使用
- A機關資訊人員針對受駭系統進行還原程序處理，並清查其餘系統，沒有被加密之情形

機密性	因此次事件未造成資料外洩情形，選擇「無需通報」
完整性	此設備為未涉及關鍵基礎設施運作核心業務使用，其系統已遭變更竄改，故選擇「2級」
可用性	因此次於事件無系統或設備運作受影響，故選擇「無需通報」



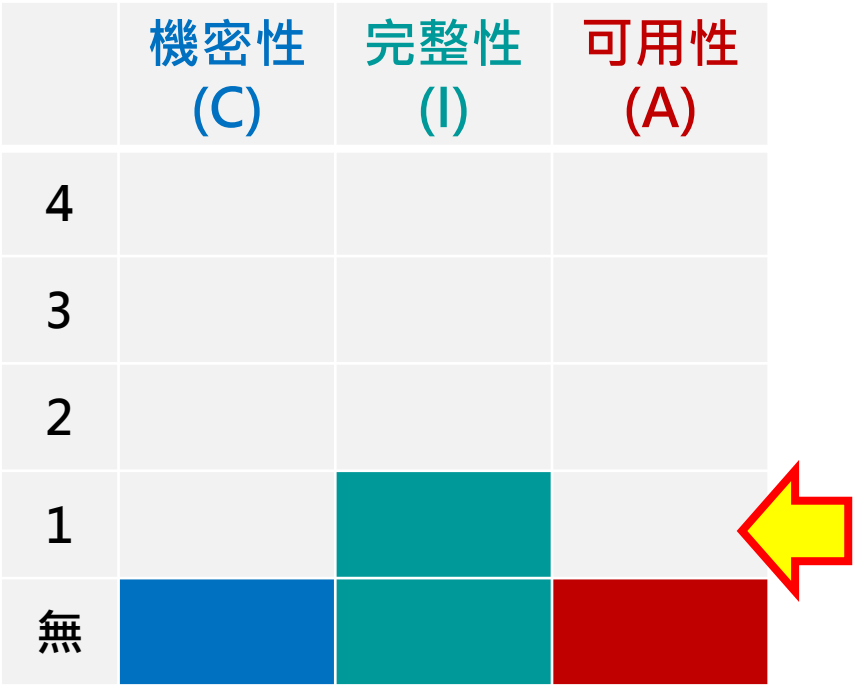
2級事件

資安事件等級參考案例 (2/2)

案情提要

- B機關接獲網頁攻擊警訊，網站主機遭駭客入侵，並**植入一惡意網頁**，網站主機主要用途是**放置單位形象網頁**
- B機關人員接獲通知後，馬上將網站備份程式復原至網站主機，同時進行全面系統檢測

機密性	因此次事件未造成資料外洩情形，選擇「無需通報」
完整性	網站遭植入惡意程式，該網站**未**用以執行核心業務，判定為非心業務系統遭輕微竄改，選擇「1級」
可用性	因此次於事件無系統或設備運作受影響，選擇「無需通報」



1級事件

事件等級判斷方式

1. 機密性、完整性、可用性是否受到衝擊
2. 受影響之系統/資料為「核心(涉及CI)/核心(未涉及CI)/非核心」系統
3. 外洩之資料是否涉及「一般公務機密/敏感資訊/國家機密」

Exercise – 事件等級 (1/10)

- **台電無預警停電，又UPS電力耗盡，導致C機關機房資訊設備無法正常運作，影響時間3小時**

機房的資訊設備為核心或非核心系統

可容忍中斷時間

Exercise – 事件等級 (2/10)

- 台電無預警停電，又UPS電力耗盡，導致C機關機房資訊設備無法正常運作，影響時間3小時

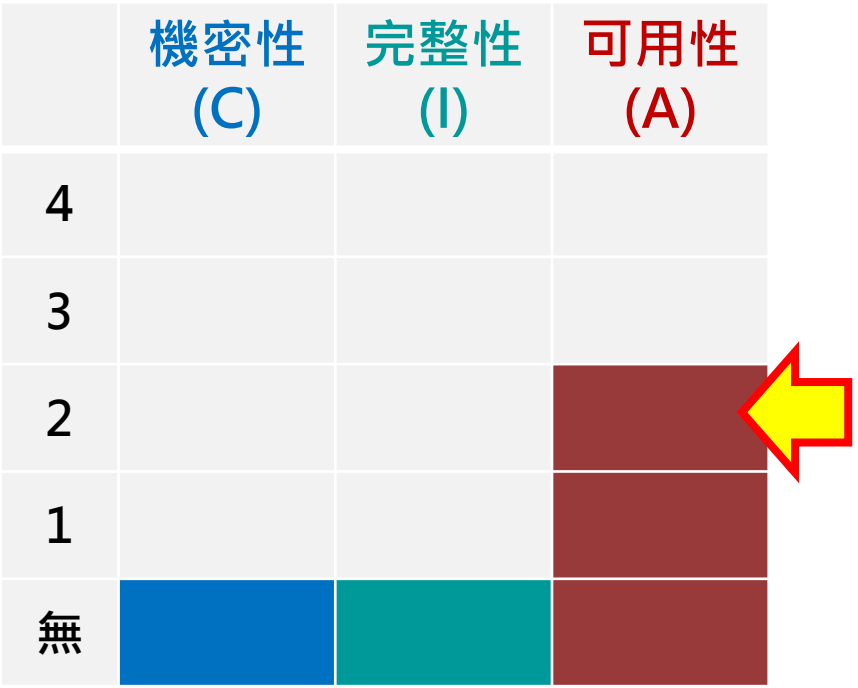
	機密性(C)		完整性(I)		可用性(A)	
	輕微洩漏	嚴重洩漏	輕微竄改	嚴重竄改	<可容忍時間	>可容忍時間
非核心業務/系統	1級	2級	1級	2級	1級	2級
核心業務/系統 (未涉及CI)	2級	3級	2級	3級	2級	3級
核心業務/系統 (涉及CI)	3級	4級	3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級	4級	4級	4級		

Exercise – 事件等級 (3/10)

- 台電無預警停電，又UPS電力耗盡，導致C機關**機房資訊設備無法正常運作**，影響時間3小時

機密性	因此次事件未造成資料外洩情形，選擇「無需通報」
完整性	因此次事件未有資料遭竄改，選擇「無需通報」
可用性	未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於**可容忍中斷時間內**回復正常運作

2級事件



Exercise – 事件等級 (4/10)

- D機關外點監視器對外攻擊其他設備

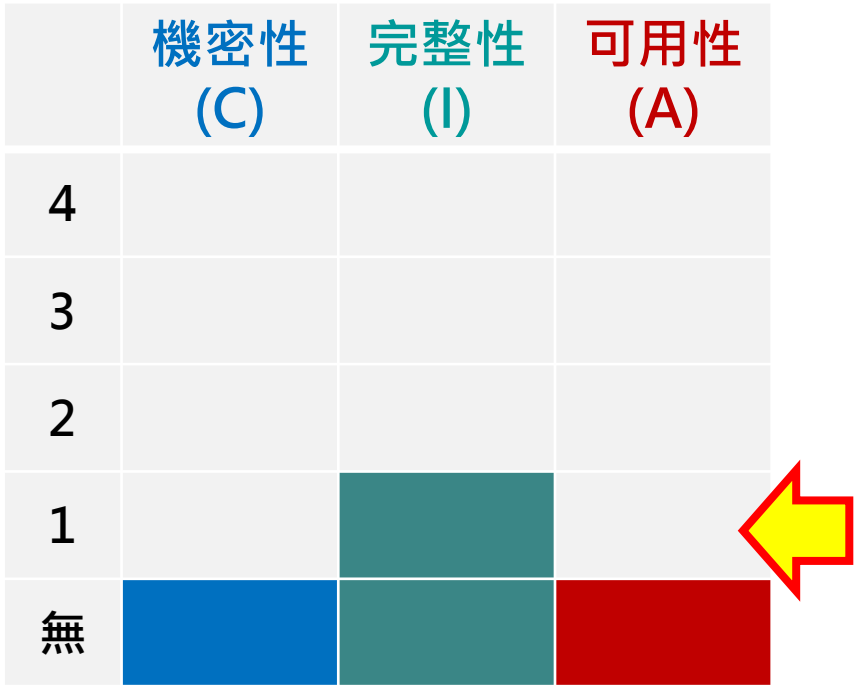
	機密性(C)		完整性(I)		可用性(A)	
	輕微洩漏	嚴重洩漏	輕微竄改	嚴重竄改	<可容忍時間	>可容忍時間
非核心業務/系統	1級	2級	1級	2級	1級	2級
核心業務/系統 (未涉及CI)	2級	3級	2級	3級	2級	3級
核心業務/系統 (涉及CI)	3級	4級	3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級	4級	4級	4級		

Exercise – 事件等級 (5/10)

- D機關外點監視器對外攻擊其他設備

機密性	因此次事件未造成資料外洩情形，選擇「無需通報」
完整性	非核心業務資訊或**非核心資通系統**遭輕微竄改
可用性	因此次於事件無系統或設備運作受影響，故選擇「無需通報」

1級事件



Exercise – 事件等級 (6/10)

- E機關網站公告資料未遮蔽個資，導致1筆民眾個資外洩

	機密性(C)		完整性(I)		可用性(A)	
	輕微洩漏	嚴重洩漏	輕微竄改	嚴重竄改	<可容忍時間	>可容忍時間
非核心業務/系統	1級	2級	1級	2級	1級	2級
核心業務/系統 (未涉及CI)	2級	3級	2級	3級	2級	3級
核心業務/系統 (涉及CI)	3級	4級	3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級	4級	4級	4級		

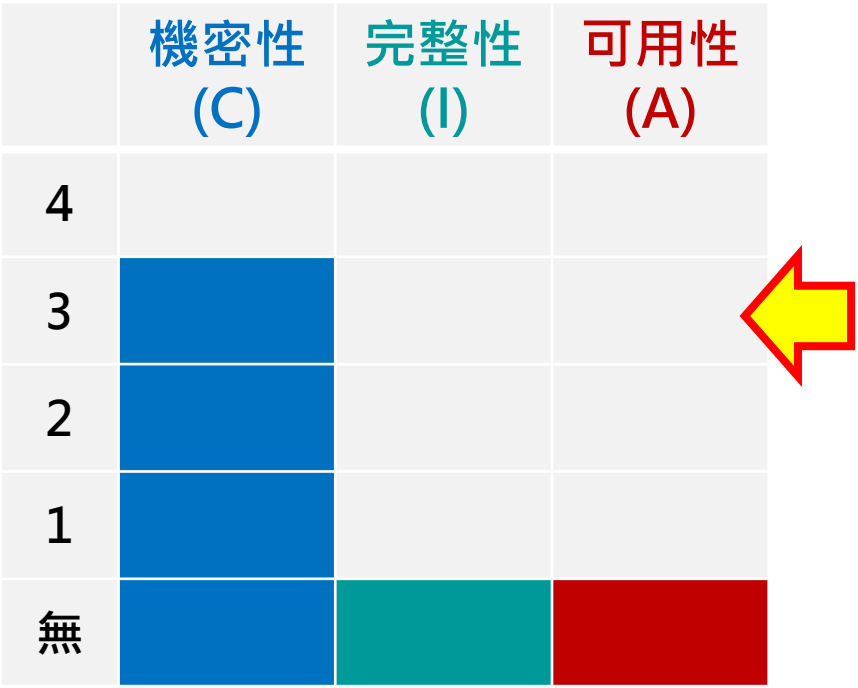
四、所稱敏感資訊，指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。

Exercise – 事件等級 (7/10)

- E機關網站公告資料未遮蔽個資，導致1筆民眾個資外洩

機密性	**敏感資訊**遭輕微洩漏
完整性	因此次事件未有資料遭竄改，選擇「無需通報」
可用性	因此次於事件無系統或設備運作受影響，故選擇「無需通報」

3級事件



Exercise – 事件等級 (8/10)

- **F機關10幾台資訊設備遭勒索軟體加密，導致系統服務中斷，受影響之設備包含核心資通系統**


是否有備援系統/資料可持續支援業務運作


若無備援系統/資料可持續支援業務運作，可容忍中斷時間為何


設備遭竄改的程度

Exercise – 事件等級 (9/10)

- F機關10幾台資訊設備遭勒索軟體加密，導致系統服務中斷，受影響之設備包含核心資通系統

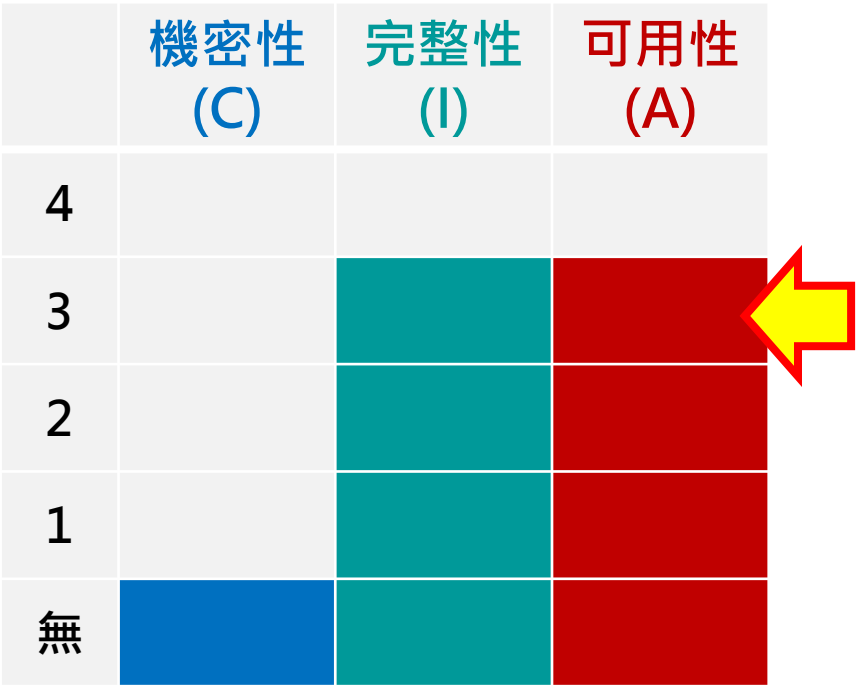
	機密性(C)		完整性(I)		可用性(A)	
	輕微洩漏	嚴重洩漏	輕微竄改	嚴重竄改	<可容忍時間	>可容忍時間
非核心業務/系統	1級	2級	1級	2級	1級	2級
核心業務/系統(未涉及CI)	2級	3級	2級	3級	2級	3級
核心業務/系統(涉及CI)	3級	4級	3級	4級	3級	4級
一般公務機密、敏感資訊	3級	4級	3級	4級		
國家機密	4級	4級	4級	4級		

Exercise – 事件等級 (10/10)

- **F機關10幾台資訊設備遭勒索軟體加密，導致系統服務中斷，受影響之設備包含核心資通系統**

機密性	因此次事件未造成資料外洩情形，選擇「無需通報」
完整性	未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改
可用性	未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作

3級事件



【資安事件案例分享】

駭客攻擊流程

網路偵察

蒐集目標系統的資訊

- 網路掃描
- 公開資訊
- 網路架構
- Port

入侵系統

透過系統弱點入侵

- 破解密碼
- 系統漏洞
- 社交工程

擴散與控制

取得控制權並擴散

- 植入後門程式
- 透過工具竊取帳密
- 橫向掃描
- 橫向連線

達成目的

達成攻擊目的

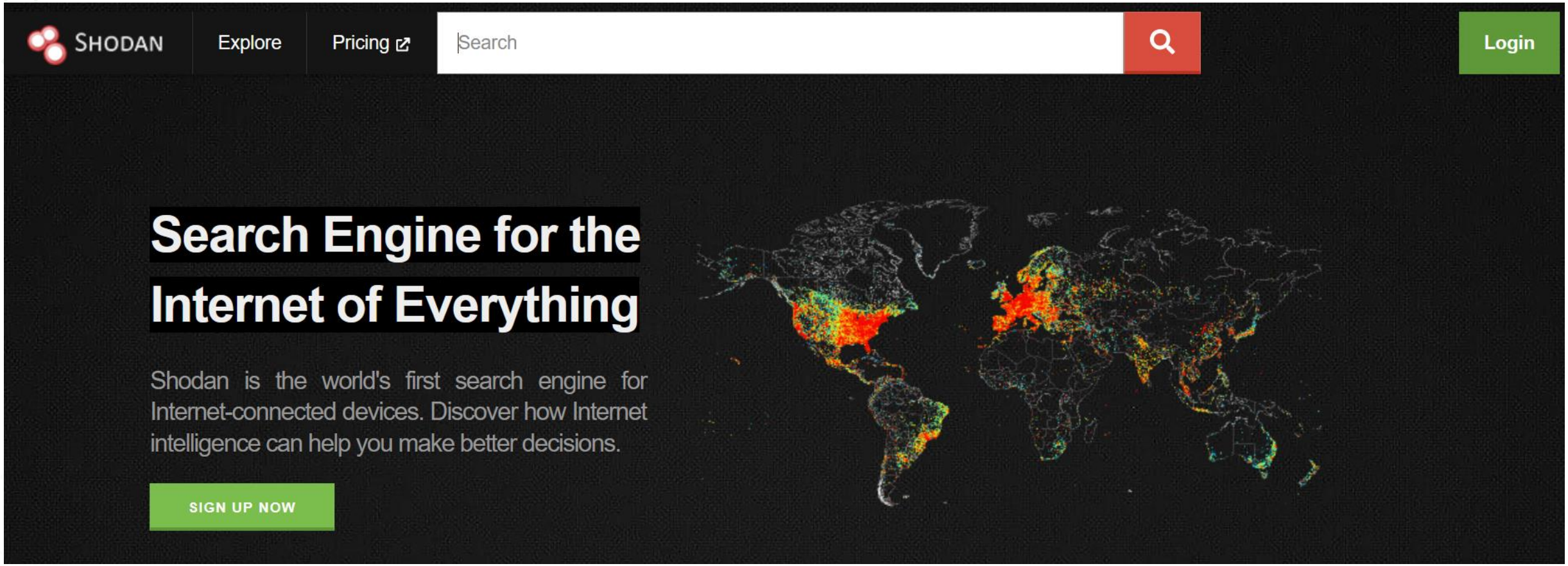
- 竊取重要資料
- 勒索贖金
- 癱瘓系統運作

網路偵察 – Whois

- Whois(https://www.whois365.com/tw/)
  - 查詢網域名稱的註冊資訊

網路偵察 – Shodan (1/4)

- Shodan(https://www.shodan.io/)
  - 搜尋公開在網路上的設備，如監視器與伺服器



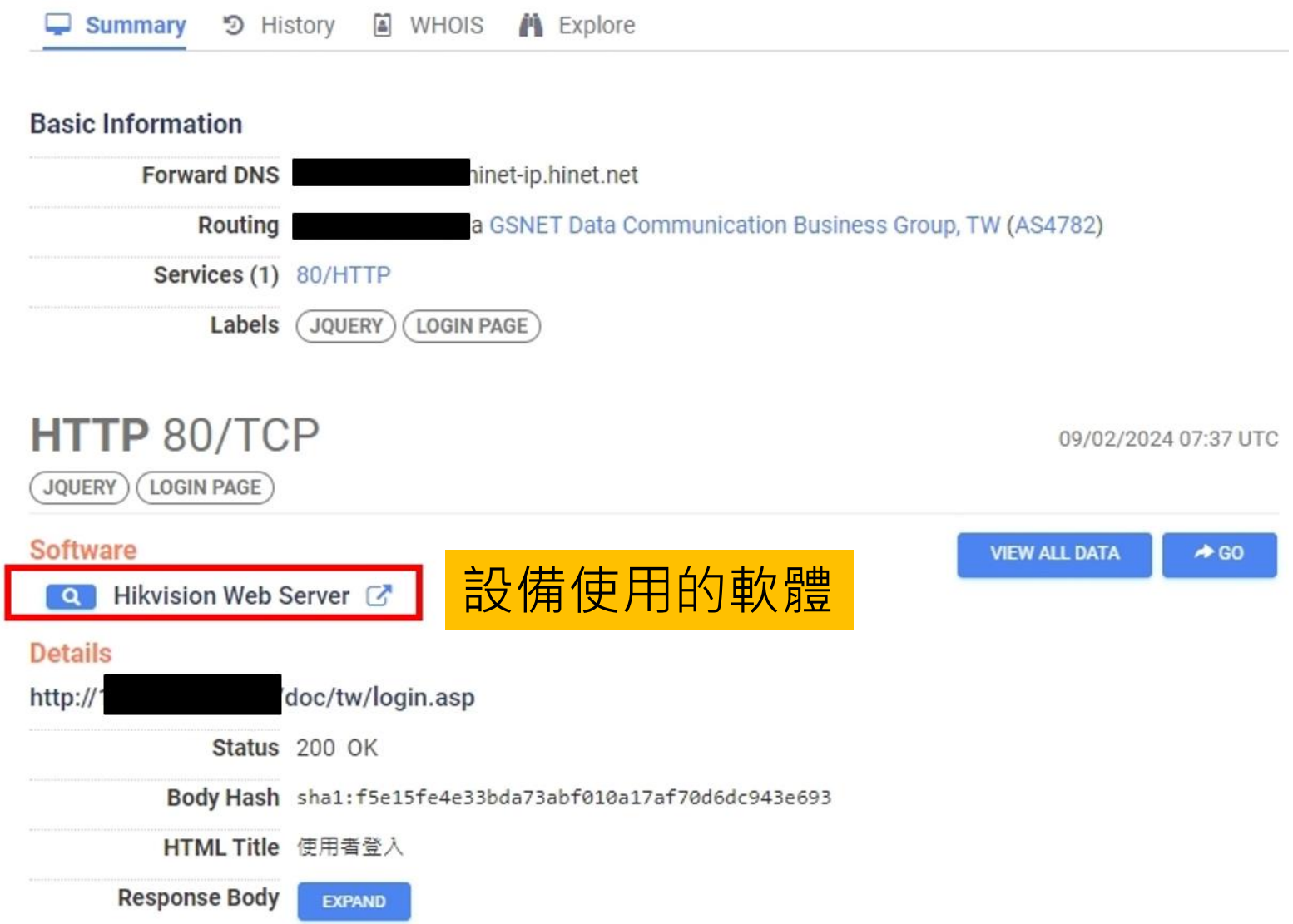
網路偵察 – Shodan (2/4)

- Shodan(https://www.shodan.io/)
  - 搜尋公開在網路上的設備，如監視器與伺服器

篩選條件	說明	範例
net	搜尋指定的ip 或網段	net:117.56.XX.XXX
product	搜尋指定產品/軟體	product:DVR
country	搜尋指定國家代碼	country:TW
port	搜尋指定的連接埠	port:23
os	搜尋指定作業系統	os:windows

網路偵察 – Shodan (3/4)

網路偵察 – Shodan (4/4)



設備使用的軟體

Exercise

- 搜尋任意IP
- 找出網路上有開port 23的DVR設備

SHODAN | Explore | Downloads | Pricing | product:DVR port:23

TOTAL RESULTS

153

TOP COUNTRIES

Viet Nam 37

View Report | View on Map | Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

[redacted]120
[redacted]Sayar
[redacted]public

CTRING login:

[redacted].230
[redacted]ce
[redacted]erinburg

Welcome to the DS2 command line processor
Username:

網路偵察 – Google Hacking (1/2)

- 透過Google的搜尋語法，找尋網站的資訊

語法	說明	範例
site	搜尋特定網域的內容	site:example.com
inurl	搜尋 URL 中包含特定關鍵字的頁面	inurl:/admin
intitle	搜尋頁面標題中包含特定關鍵字的頁面	intitle:"admin login"
filetype:	搜尋特定類型的檔案	filetype:pdf
intext:	搜尋頁面內容中包含特定關鍵字的頁面	intext:"password"
“” (雙引號)	搜尋包含精確關鍵字的頁面	intext:"password"

網路偵察 – Google Hacking (2/2)

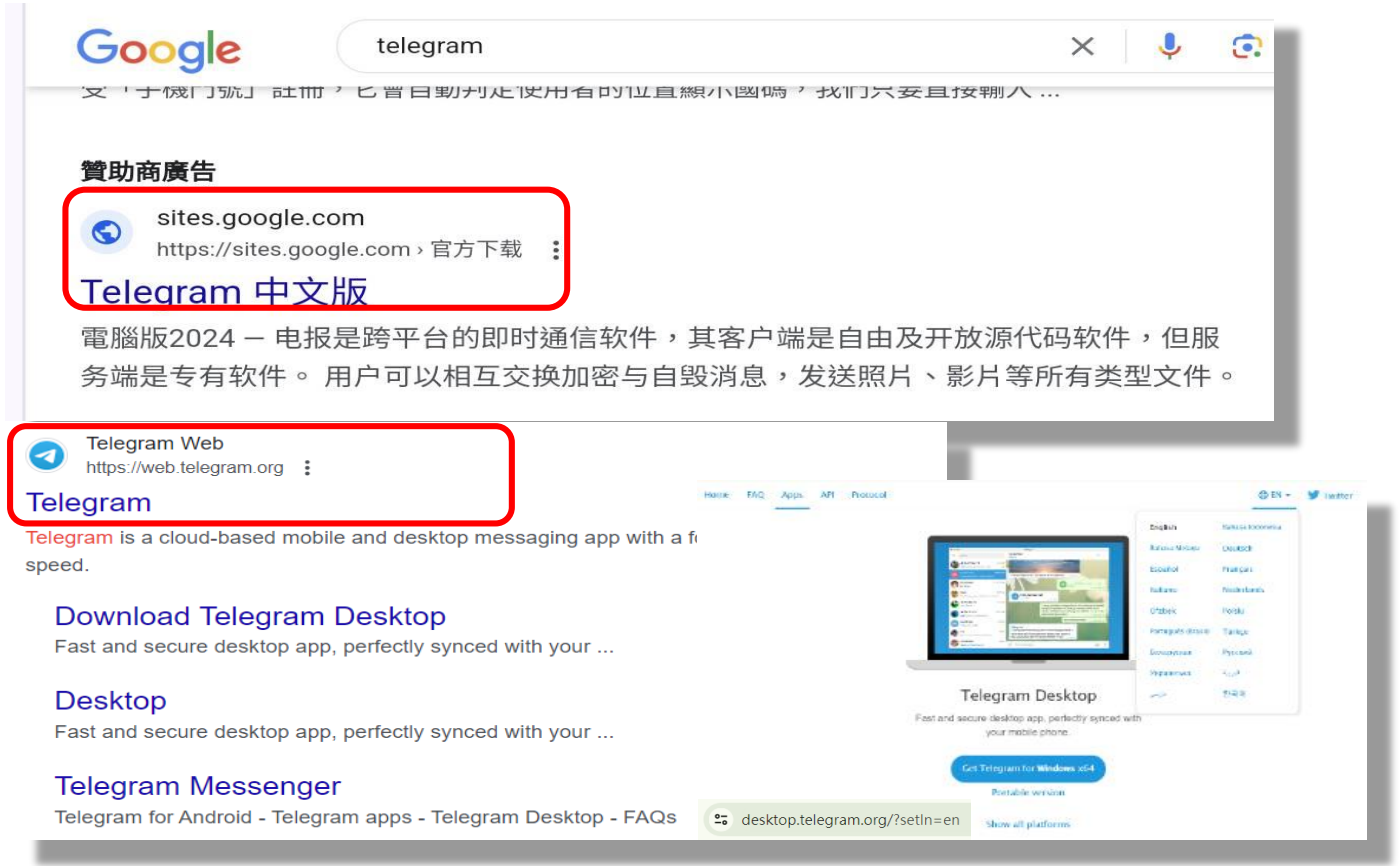
https://www.nics.nat.gov.tw/core_business/cybersecurity_talent_development/Roadshow_Seminars/

Exercise

- 透過Google的搜尋語法，尋找網站的公開目錄
- 搜尋含有特定字元的公開文件(pdf檔)

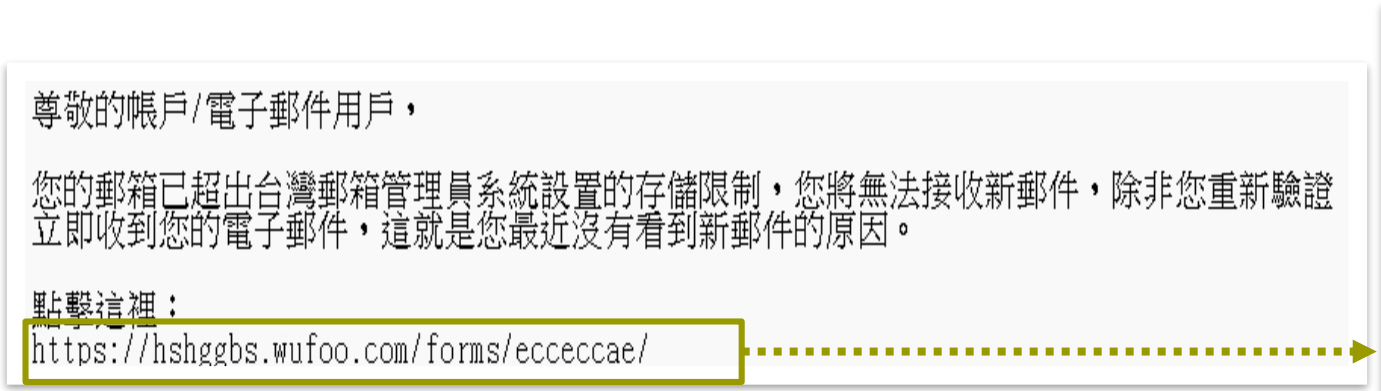
常見入侵手法 – 社交工程 (1/2)

- 政府機關有偽冒程式之異常連線
- 調查發現是同仁於公務電腦安裝Telegram程式，透過Google搜尋發現有中文版，十分高興的下載了**偽冒的安裝檔**，導致公務電腦受駭



常見入侵手法 – 社交工程 (2/2)

- 駭客發送大量社交工程郵件，誘騙受害者輸入郵件帳號與密碼。並再利用取得的該帳號向受害者其他同仁發送社交工程郵件，以提高信件的可信度，進一步誘騙更多人受害



常見入侵手法 – 應用程式漏洞

- 今年6月多個政府機關發現資訊設備遭**執行異常指令**，並嘗試對外下載惡意程式
- 檢視**Access Log**，發現**PHP漏洞(CVE-2024-4577)漏洞**攻擊特徵

Windows的“Best-Fit”特性會讓CGI程序把0xAD轉換為字元“-”

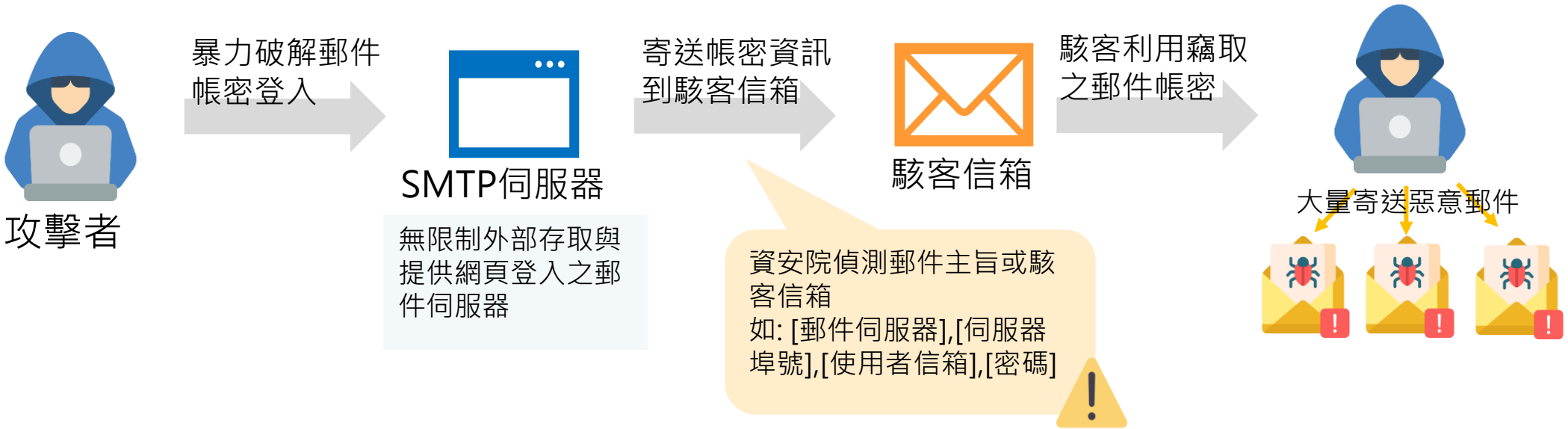
POST /php-cgi/php-cgi.exe?%ADd+cgi.force_redirect%3D0+%ADd+cgi.redirect_status_env+%ADd+allow_url_include%3D1+%ADd+auto_prepend_file%3Dphp://input

Unicode編碼為“=”

POST /php-cgi/php-cgi.exe?
-d cgi.force_redirect=0 //通常會設定成1來阻止直接執行PHP程式，設定成0即跳過這個保護機制
-d cgi.redirect_status_env //設置了CGI模式下的重定向環境變數，確保PHP可以在CGI模式下正常執行
-d allow_url_include=1 //允許從遠端URL載入PHP文件
-d auto_prepend_file=php://input //攻擊者可以把惡意的PHP程式放在HTTP請求裡，伺服器會自動執行程式

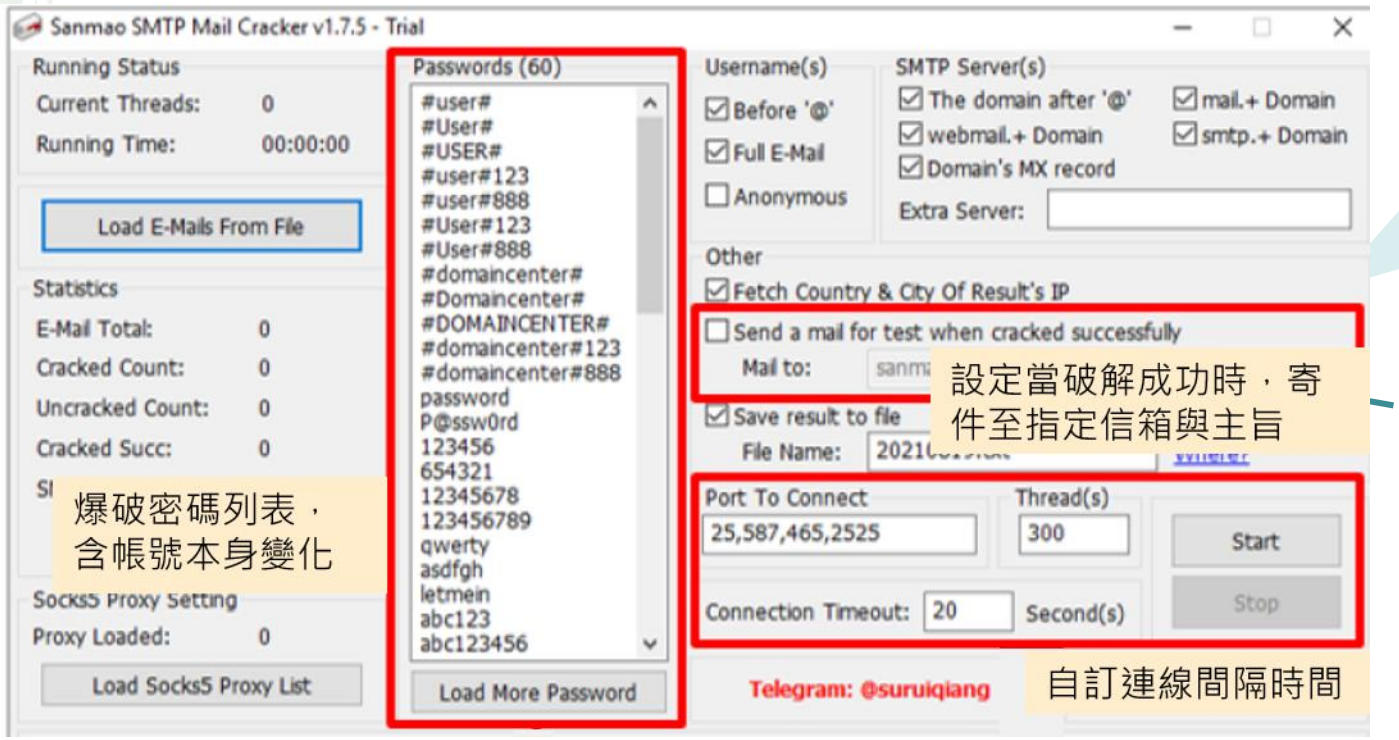
常見入侵手法 – 弱密碼遭破解(1/2)

- 多個機關郵件帳號密碼外洩
- 經機關調查發現多為設置弱密碼遭成功暴力破解
- 機關雖規定密碼設置原則，人員為方便記憶而將密碼設置為 **Aa123456**或與**帳號相似密碼**



https://www.nics.nat.gov.tw/core_business/cybersecurity_talent_development/Roadshow_Seminars/

常見入侵手法 – 弱密碼遭破解(2/2)



駭客可利用帳密暴力破解工具(如Sanmao SMTP Mail Cracker)，制定密碼表、爆破成功後回傳之信件主旨及連線間隔時間

受駭偵測之主旨列表

You get a new smtp WITID/[SSL狀態]/[使用者信箱]/[密碼]

[使用者信箱];[使用者信箱];[密碼];[郵件伺服器];[伺服器埠號];0;[帳密驗證方式]

[郵件伺服器]:[使用者信箱]:[密碼]:[使用者信箱]:[SSL狀態]::::0

[郵件伺服器],[伺服器埠號],[使用者信箱],[密碼]

https://www.nics.nat.gov.tw/core_business/cybersecurity_talent_development/Roadshow_Seminars/

常見攻擊標的 – 物聯網設備

- **印表機或監視器**等庶務設備，主要支援機關內部業務運作，開放外部網際網路存取，易受到未授權之存取或攻擊
- 設備可能存在**預設密碼**或**漏洞**，使得駭客可以入侵並進行各種攻擊

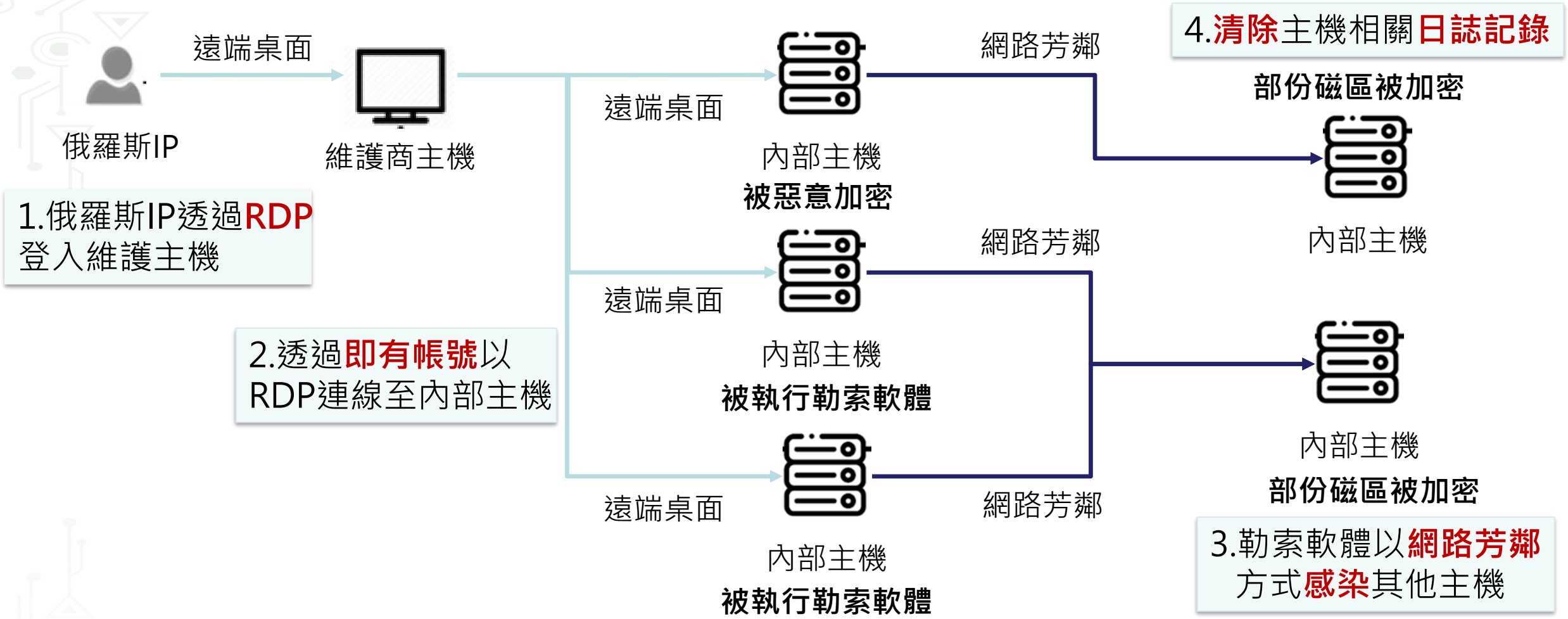
來源IP	來源Port	目的IP	目的Port	協定	應用	起始時間	結束時間	上傳	下載
攻擊IP	64071	機關IP	21	TCP	ftp	2024/3/29 06:15	2024/3/29 06:16	1262	1081

案件說明

- 發現多個機關資訊設備開啟FTP服務且遭上傳挖礦相關程式
- 部分機關表示受駭設備為印表機或監視器，未設置密碼或使用弱密碼/預設密碼，後續評估無連網需求，多以斷網處理

案例分析-內部主機遭勒索加密(1/2)

各主機間連線不會經過防火牆阻擋



案例分析-內部主機遭勒索加密(2/2)

網路偵察

- 攻擊前幾天已有不同國家登入維護商主機記錄

入侵系統

- 俄羅斯IP透過遠端桌面成功登入維護商主機
- 登入的帳號為非Windows預設帳號，代表攻擊者攻擊前應已蒐集到一些資訊

擴散與控制

- 維護商主機可存取不同網段主機
- 攻擊者透過遠端桌面與既有帳號成功連線多部主機
- 攻擊者執行勒索軟體之前會先在目標主機安裝WinRAR 程式或 Process Hacker 或兩者皆裝 (部份攻擊程式加密壓縮)
- 以**網路芳鄰**方式加密其他主機

達成目的

- 多台主機遭勒索軟體加密

近期資安事件案例分享 (1/3)

網通設備疏於更新或使用弱密碼導致存在資安風險，遭利用成為殭屍網路設備

郵件帳號或網站帳號設置弱密碼遭暴力破解，導致郵件帳號遭惡意利用或網站功能遭利用上傳惡意程式

供應鏈廠商遭駭成為入侵跳板

官網遭DDoS攻擊，導致無法正常提供網站服務

人員資安意識不足，開啟惡意郵件或瀏覽網頁時點擊惡意連結，導致設備受駭而資料外洩

網站上傳功能未限制檔案上傳類型，遭利用上傳惡意程式

近期資安事件案例分享 (2/3)

郵件帳號或網站帳號設置弱密碼遭暴力破解，導致郵件帳號遭惡意利用或網站功能遭利用上傳惡意程式

- 密碼設置弱密碼，如：帳號與密碼相同
- 密碼設置常見密碼，如：Aa123456
- 密碼設置鍵盤排序的密碼，如：1qaz@WSX
- 密碼提示訊息暴露過多資訊
- 點擊社交工程郵件，並於釣魚頁面登打帳密

- 避免設置常見、與帳號相似或鍵盤排序等具規則之弱密碼
- 定期變更密碼，並且不得與前幾次相同

近期資安事件案例分享 (3/3)

多數物聯網裝置缺乏有效控管，導致遭駭客入侵利用於各種攻擊，如DDoS攻擊與殭屍網路等

- 多個**網路服務暴露於網路上**，如：RDP、VNC及Telnet等遠端管理通訊協定
- 可透過網際網路直接存取相關服務與管理介面
- 使用**預設密碼/弱密碼**
- **疏於更新**導致存在已知漏洞被利用

- 關閉不必要的網路服務
- 使用具複雜度之密碼
- 定期檢視並更新設備系統/韌體版本
- 評估汰換或加強防護已停止更新或支援之產品

【資安事件處理簡介】

資安事件應變與處理

資安事件應變與處理

事前準備

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

事中應變

通報資安事件
- 資通安全事件通報及應變辦法

損害控制與復原
- 資通安全事件通報及應變辦法

紀錄蒐集
- 修正各機關資通安全事件通報及應變處理作業程序

事後改善

矯正與改善措施
- 資通安全事件通報及應變辦法

事前準備 – 訂定通報應變機制 (1/4)

事前準備 ▶ 事中應變 ▶ 事後改善

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

通報資安事件
- 資通安全事件通報及應變辦法

損害控制與復原
- 資通安全事件通報及應變辦法

紀錄蒐集
- 修正各機關資通安全事件通報及應變處理作業程序

矯正與改善措施
- 資通安全事件通報及應變辦法

事前準備 – 訂定通報應變機制 (2/4)

- 公務機關第2章第9條與第10條，明定機關應設置內部「資安事件通報作業」與「資安事件應變作業」規範

項目	資安事件通報作業	資安事件應變作業
目的	知悉資安事件發生時，迅速依作業規範執行通報作業，並確保相關人員熟悉作業流程	發生資安事件時，可依作業規範保留必要事件紀錄，防止災情擴大，並釐清事件發生經過
規範事項	➢ 判定事件等級之流程及權責 ➢ 事件之影響範圍、損害程度及機關因應能力之評估 ➢ 資通安全事件之內部通報流程 ➢ 通知受資通安全事件影響之其他機關之方式 ➢ 前四款事項之演練 ➢ 資通安全事件通報窗口及聯繫方式 ➢ 其他資通安全事件通報相關事項	➢ **應變小組之組織** ➢ 事件發生前之演練作業 ➢ 事件發生時之損害控制機制 ➢ 事件發生後之復原、鑑識、調查及改善機制 ➢ 事件相關紀錄之保全 ➢ 其他資通安全事件應變相關事項

事前準備 – 訂定通報應變機制 (3/4)

資通安全事件通報及應變管理程序

- 公務機關

公務機關資通安全事件通報及應變管理程序

（範本）

目錄

- 特定非公務機關

特定非公務機關資通安全事件通報及應變管理程序

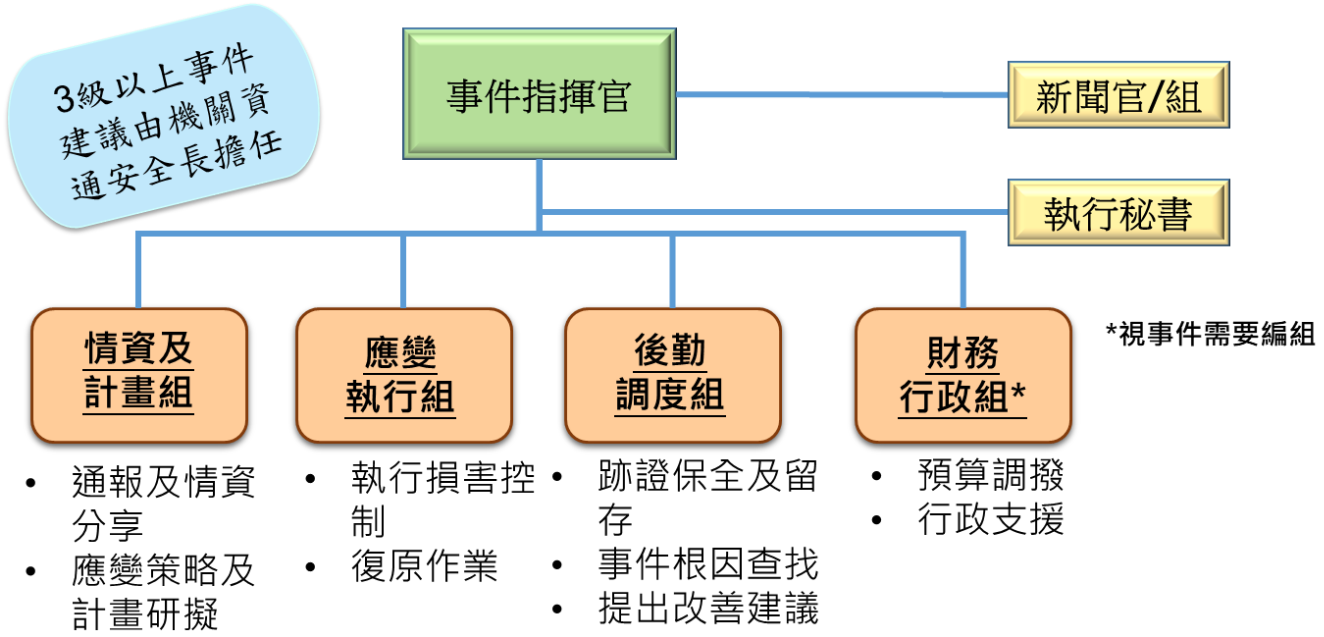
（範本）

目錄

- 資通安全署提供公務機關與特定非公務機關「資通安全事件通報及應變管理程序」範本，提供機關作為相關規範制定之參考
- 資通安全署網站>>資安法規專區>>範本文件

事前準備 – 訂定通報應變機制 (4/4)

- 資通安全事件通報及應變小組係依照組織目標，提供必要服務項目，並輔以專業人員協助處理資安事件



各機關得以現有分組為基礎，依各機關編制及業務分工，經機關資通安全長同意後調整通報應變小組組成及各分組代表，另得視資通安全事件或機關資通環境需要調整各分組任務。

事前準備 – 偵測與分析 (1/20)

事前準備 ▶ 事中應變 ▶ 事後改善

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

通報資安事件
- 資通安全事件通報及應變辦法

損害控制與復原
- 資通安全事件通報及應變辦法

紀錄蒐集
- 資通安全事件通報及應變辦法

矯正與改善措施
- 資通安全事件通報及應變辦法

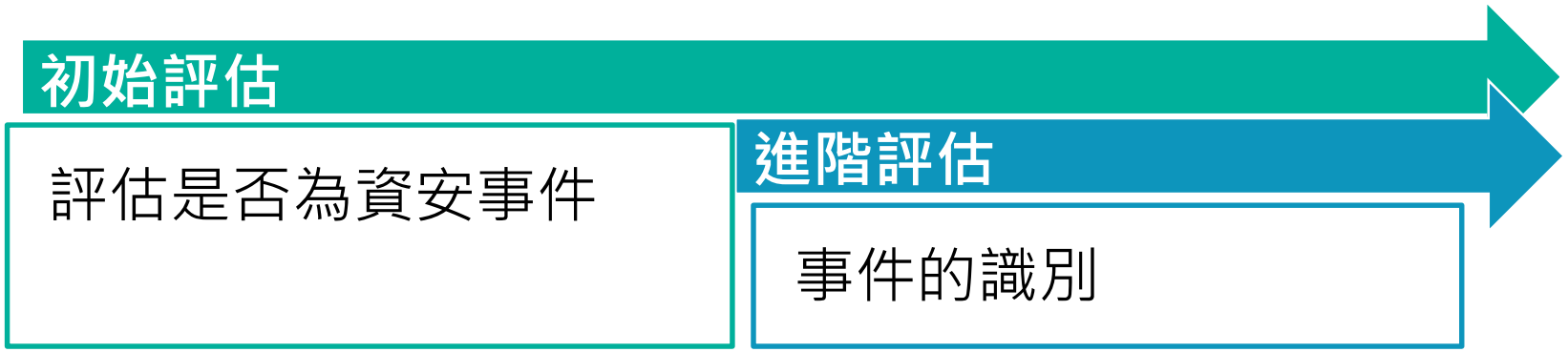
事前準備 – 偵測與分析 (2/20)

- 依據組織訂定網路與資訊系統管理辦法，蒐集並分析資安徵兆，判斷是否為一個資安事件(Incident)
  - 例如一棟裝有火災警報器的建築物
    - 誰被授權啟動火災警報開關?
    - 誰被授權決定是否安全無虞，可以重新回到建築物?

- 可能攻擊來源
  - 外部/可移動式媒體
  - 消耗資源
  - 網站
  - 電子郵件
  - 偽裝
  - 不當使用
  - 設備的偷竊或遺失

事前準備 – 偵測與分析 (3/20)

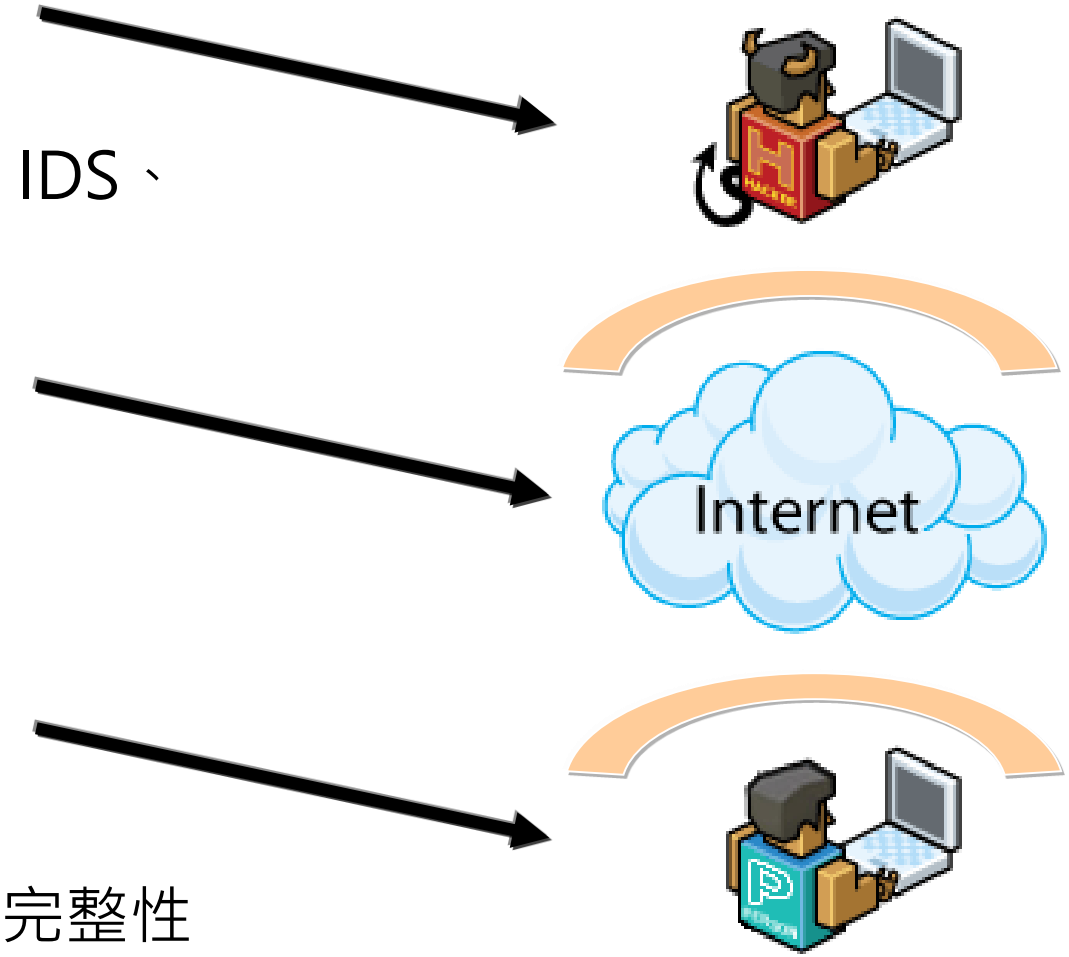
- 判斷發現的資安徵兆是不是資安事件
  - 機關可專注於處理常見攻擊類型的事件，因應不同類型的事件制定不同的因應策略



某單位內部網路遭外部駭客攻擊

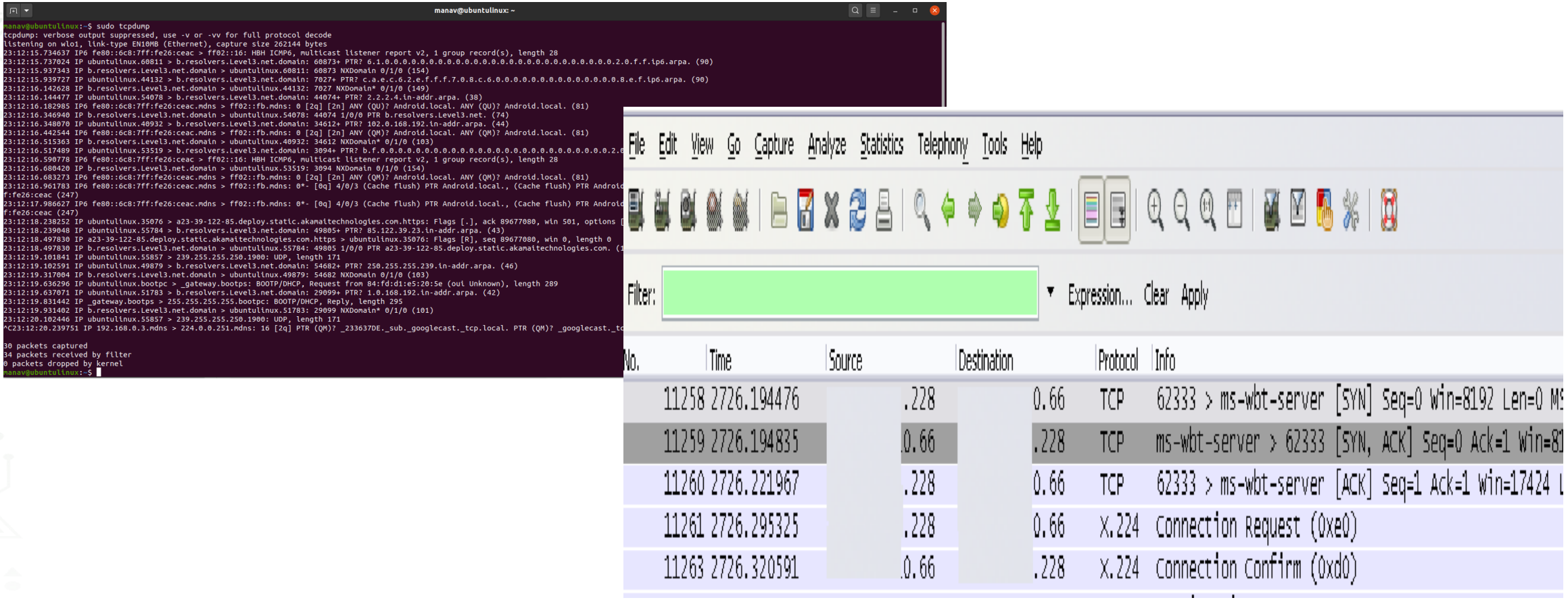
事前準備 – 偵測與分析 (4/20)

- **網路端防護偵測**
  - –識別在網路上發生的徵狀
  - –Firewall、Router、Network-Based IDS、IPS、DMZ系統等
- **主機端防護偵測**
  - –識別需進出主機的資料
  - –個人Firewall/IPS、主機端Firewall等
- **系統防護偵測**
  - –識別發生在系統上的行為
  - –防毒軟體、使用者端安全工具、檔案完整性檢查工具、使用者發現的電腦異常行徑等



事前準備 – 偵測與分析 (5/20)

- 網路端防護偵測範例
  - –透過tcpdump或wireshark等工具，可偵測網路封包內容



事前準備 – 偵測與分析 (6/20)

- 系統管理者可透過常用指令，檢查下列項目找出異常行為，用以協助系統管理者去找出一些問題，並用以尋求事件處理小組的協助

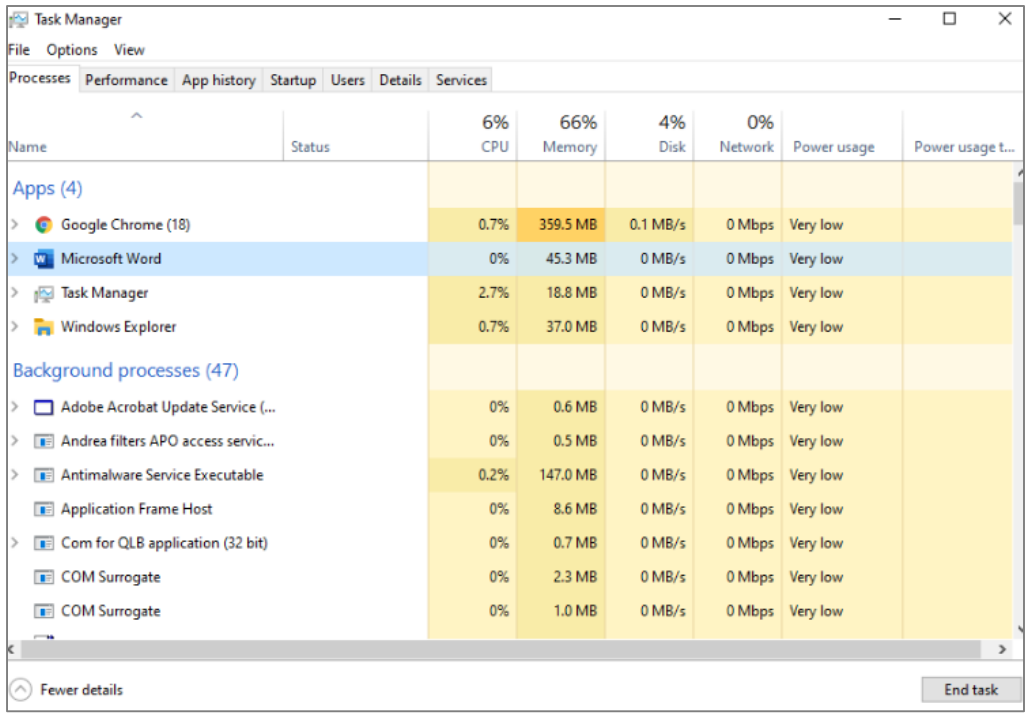
序號	檢查項目	序號	檢查項目
1	程序與服務	5	帳號
2	檔案	6	日誌檔內容
3	網路使用量	7	其他不尋常的事件
4	排程工作	8	其他協助的工具

- 但總有些限制...
  - –不是所有的攻擊行為都可以被偵測出來的，但我們將盡量找出跡象
  - –這些指令可以幫助系統管理者去釐清：他們系統的「正常」狀態

事前準備 – 偵測與分析 (7/20)

Windows常見指令 – 異常程序

- 執行工作管理員(開始→執行→輸入taskmgr.exe)
  - –觀察不正常/非預期的程序
  - –特別觀察那些使用者名稱為”SYSTEM”或”Administrator”(或是隸屬於Administrator群組的使用者)的程序



事前準備 – 偵測與分析 (8/20)

Windows常見指令 – 異常服務

- 若要用Command-Line方式來檢測異常程序，可輸入以下兩種指令
  - C:\> tasklist
  - C:\> wmic process list full (較詳細)
- 要檢查異常服務與服務設定，可以輸入：C:\> services.msc
- 取得正在執行的服務列表，可輸入：C:\> net start
- 服務與執行程序的對應列表：C:\> tasklist /svc

事前準備 – 偵測與分析 (9/20)

Windows常見指令 – 網路狀態

- 透過windows常見網路指令檢視主機網路使用狀態

常見指令	說明	備註
C:\> net view \\127.0.0.1	檢測檔案分享功能，確認每項設定都屬於業務需求	
C:\> net session	檢視有誰連線進入該主機	
C:\> net use	檢視該台主機是否有與其他台主機建立連線	
C:\> nbtstat –S	檢視NetBIOS的行為	
C:\> netstat -na	檢視開啟的TCP與UDP埠	-nao 可顯示Process ID
C:\> netsh advfirewall show	Windows內建的防火牆設定，可透過下列指令進行檢查	

事前準備 – 偵測與分析 (10/20)

主機端防護偵測範例

- 透過netstat指令，可檢視執行的服務

檢查服務列表(Port列表)

- Internet Assigned Numbers Authority(IANA)
  - http://www.iana.org/assignments/port-numbers
- 木馬、後門
  - http://www.trojanhunter.com/trojanhunter/portlist/

事前準備 – 偵測與分析 (11/20)

Windows常見指令 – 異常排程工作

- GUI介面
  - 開始→程式集→附屬應用程式→系統工具→排程工作
- Command-Line模式
  - C:\> schtasks
    - 檢查異常排程工作，特別是使用Administrator群組的使用者，或使用SYSTEM，或是空白的使用者名稱
    - “at” 指令僅可以顯示透過at指令下達的排程，而不會顯示schtasks下達的排程
    - “schtasks” 指令可顯示用 “at” 及 “schtasks” 排程的工作

事前準備 – 偵測與分析 (12/20)

- 檢查Administrator群組中，新的、非預期的帳號
  - C:\> lusrmgr.msc
  - 點選 “群組” ，並點選Administrator
- 透過Command-Line模式，檢查使用者列表
  - C:\> net user
- 透過Command-Line模式，檢查Administrator群組中的使用者列表
  - C:\> net localgroup administrators

事前準備 – 偵測與分析 (13/20)

- 可透過事件檢視器來檢視日誌
  - C:\> eventvwr.msc
- 檢查可疑的事件
  - “Event log service was stopped”
  - “Windows file Protection is not active on this system”
  - “The MS Telnet Service has started successfully”
- 檢查大量登入失敗紀錄或是被鎖定的帳戶

事前準備 – 偵測與分析 (14/20)

- 可用來檢測TCP與UDP埠的工具
  - Fport(http://www.mcafee.com/us/downloads/free-tools/fport.aspx)
  - TCPView(http://www.microsoft.com/technet/sysinternals)
- 程序分析工具
  - Process Explorer(https://technet.microsoft.com/en-us/sysinternals/bb896653)
  - 與Process Monitor(https://technet.microsoft.com/en-us/sysinternals/bb896645)

事前準備 – 偵測與分析 (15/20)

Windows常見指令 – 異常檔案

- 檢查系統內之檔案是否有非屬系統檔案且為隱藏屬性的執行檔，在Command-Line模式下輸入指令
  - C:\> dir *.exe /AS/AH/S
- ※ 檢查是否有出現隱藏屬性的執行檔

事前準備 – 偵測與分析 (16/20)

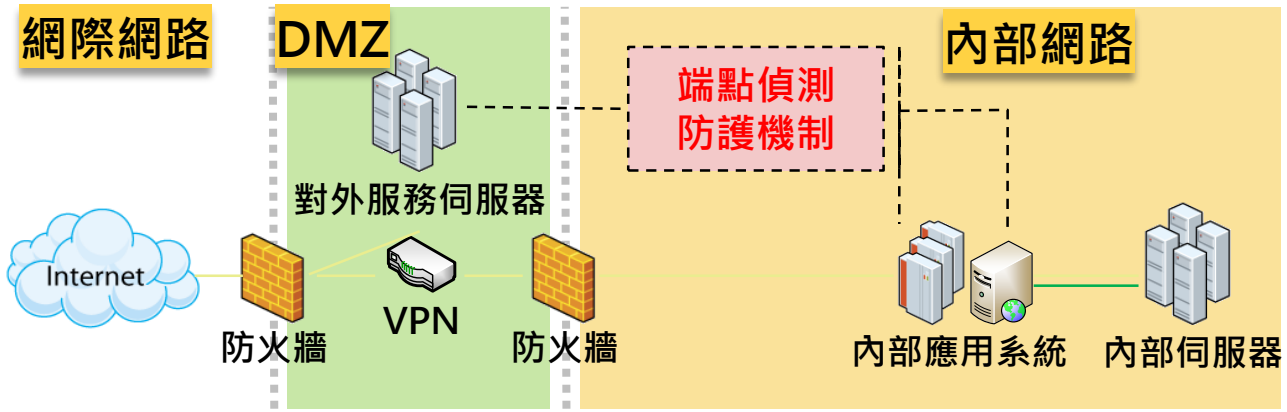
Windows常見指令 – 異常註冊機碼

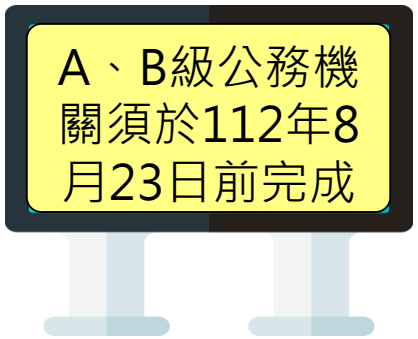
- 系統管理者可藉由檢查是否存有奇怪的註冊機碼，檢視是哪些異常檔案會於登入系統時被啟動
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
  - HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
  - 放置於HKLM與HKCU的機碼需要被檢驗
  - 可透過登錄編輯程式的GUI介面進行檢查(開始→執行→輸入regedit)
- 或可在Command-Line模式下，使用reg指令進行查詢
  - C:\> reg query hklm\software\microsoft\windows\currentversion\run

事前準備 – 偵測與分析 (17/20)

- 端點偵測及應變機制(Endpoint Detection and Response, EDR)之建置與資料回傳，已納入資通安全責任等級A、B級公務機關應辦事項要求
- EDR納入監控範圍，並搭配資訊資產與端點偵測進行關聯分析，注意內網橫向擴散情形

  –針對所有受駭標的進行處置，避免造成更嚴重的資安事件





事前準備 – 偵測與分析 (18/20)

- 分級作業辦法應辦事項 - 技術面

辦理事項	辦理內容	A	B	C	D	E
安全性檢測	全部核心資通訊系統弱點掃描	每年2次	每年1次	2年1次	X	X
	全部核心資通訊系統滲透測試	每年1次	2年1次	2年1次	X	X
資通安全檢診	網路架構檢視、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、目錄伺服器及防火牆連線設定檢視	每年1次	2年1次	2年1次	X	X
政府組態基準(公務機關)	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	1年內	1年內	X	X	X

事前準備 – 偵測與分析 (19/20)

- 分級作業辦法應辦事項 - 技術面

辦理事項	辦理內容	A	B	C	D	E
資通安全威脅偵測管理機制	依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄	1 年內	1 年內	X	X	X
資通安全弱點通報機制(VANS)	依主管機關指定之方式提交資訊資產盤點資料	1 年內	1 年內	2 年內	X	X
端點偵測及應變機制	(公務機關)依主管機關指定之方式提交偵測資料	2 年內	2 年內	X	X	X

事前準備 – 偵測與分析 (20/20)

- 分級作業辦法應辦事項 - 技術面

辦理事項	辦理內容	A	B	C	D	E
資通安全防護 防護措施之啟用並持續使用之及適時進行軟硬體之必要更新或升級	防毒軟體	1年內	1年內	1年內	1年內	X
	網路防火牆	1年內	1年內	1年內	1年內	X
	具電子郵件伺服器者，應備電子郵件過濾機制	1年內	1年內	1年內	X	X
	入侵偵測及防禦機制	1年內	1年內	X	X	X
	具對外服務之核心資通系統者，應備應用程式防火牆	1年內	1年內	X	X	X
	進階持續性威脅攻擊防禦措施	1年內	X	X	X	X

事前準備 – 資安教育 (1/3)

事前準備 ▶ 事中應變 ▶ 事後改善

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

通報資安事件
- 資通安全事件通報及應變辦法

損害控制與復原
- 資通安全事件通報及應變辦法

紀錄蒐集
- 修正各機關資通安全事件通報及應變處理作業程序

矯正與改善措施
- 資通安全事件通報及應變辦法

事前準備 – 資安教育 (2/3)

- 使用者資安意識與訓練，使其認知其行為對機關的影響
  - 令使用者了解正確使用網路、系統及應用程式
  - 熟悉並遵循機關制定的政策與程序
  - 依據機關制定的政策與程序，維護網路、系統及應用程式
- 藉由提高使用者對資安事件的認識，以期減少事件發生的機率

事前準備 – 資安教育 (3/3)

- 分級作業辦法應辦事項 - 認知與訓練

辦理事項	辦理內容	A	B	C	D	E
資通安全教育訓練	資通安全專職人員 每人每年至少接受１２小時以上之資通安全專業課程訓練或職能訓練	至少 ４人	至少 ２人	至少 １人	X	X
	資通安全專職人員以外之資訊人員	每人每二年至少接受３小時以上之資通安全專業課程訓練且每年３小時以上資通安全通識教育訓練			X	X
	一般使用者及主管	每人每年３小時以上 資通安全通識教育訓練				
資通安全專業證照及職能訓練證書	資通安全專職人員分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。	至少 ４人	至少 ２人	至少 １人 (僅證照)	X	X

事中應變 – 通報與應變 (1/6)

事前準備 ▶ 事中應變 ▶ 事後改善

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

通報資安事件
- 資通安全事件通報及應變辦法

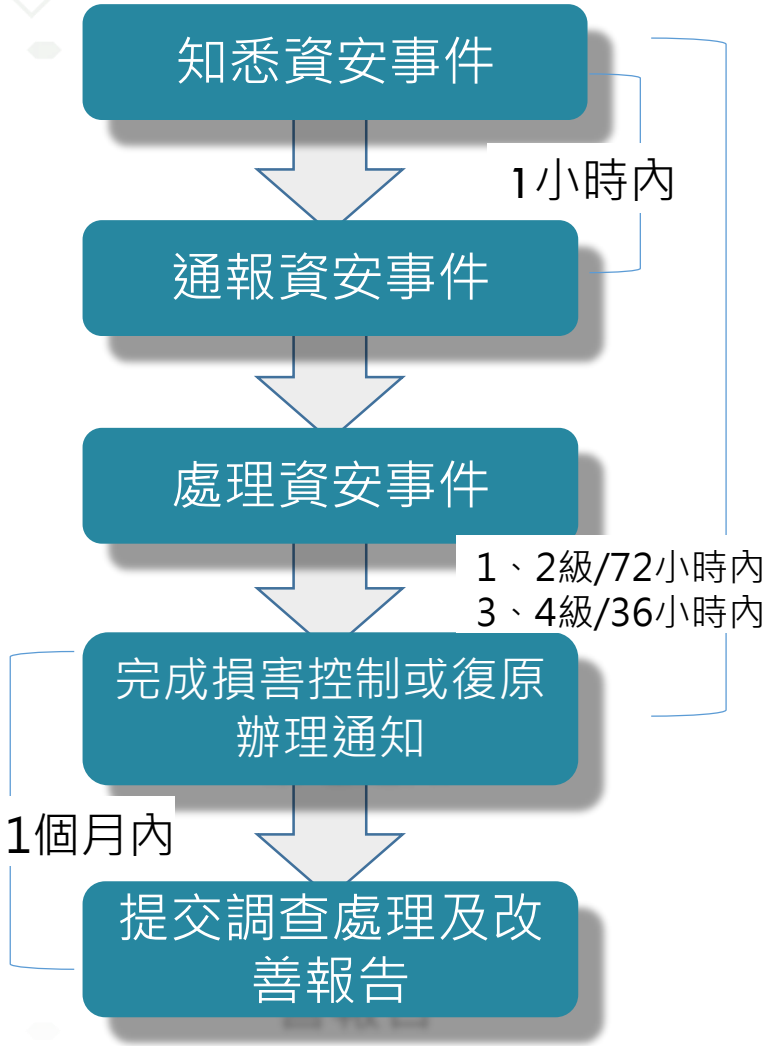
損害控制與復原
- 資通安全事件通報及應變辦法

紀錄蒐集
- 修正各機關資通安全事件通報及應變處理作業程序

矯正與改善措施
- 資通安全事件通報及應變辦法

事中應變 – 通報與應變 (2/6)

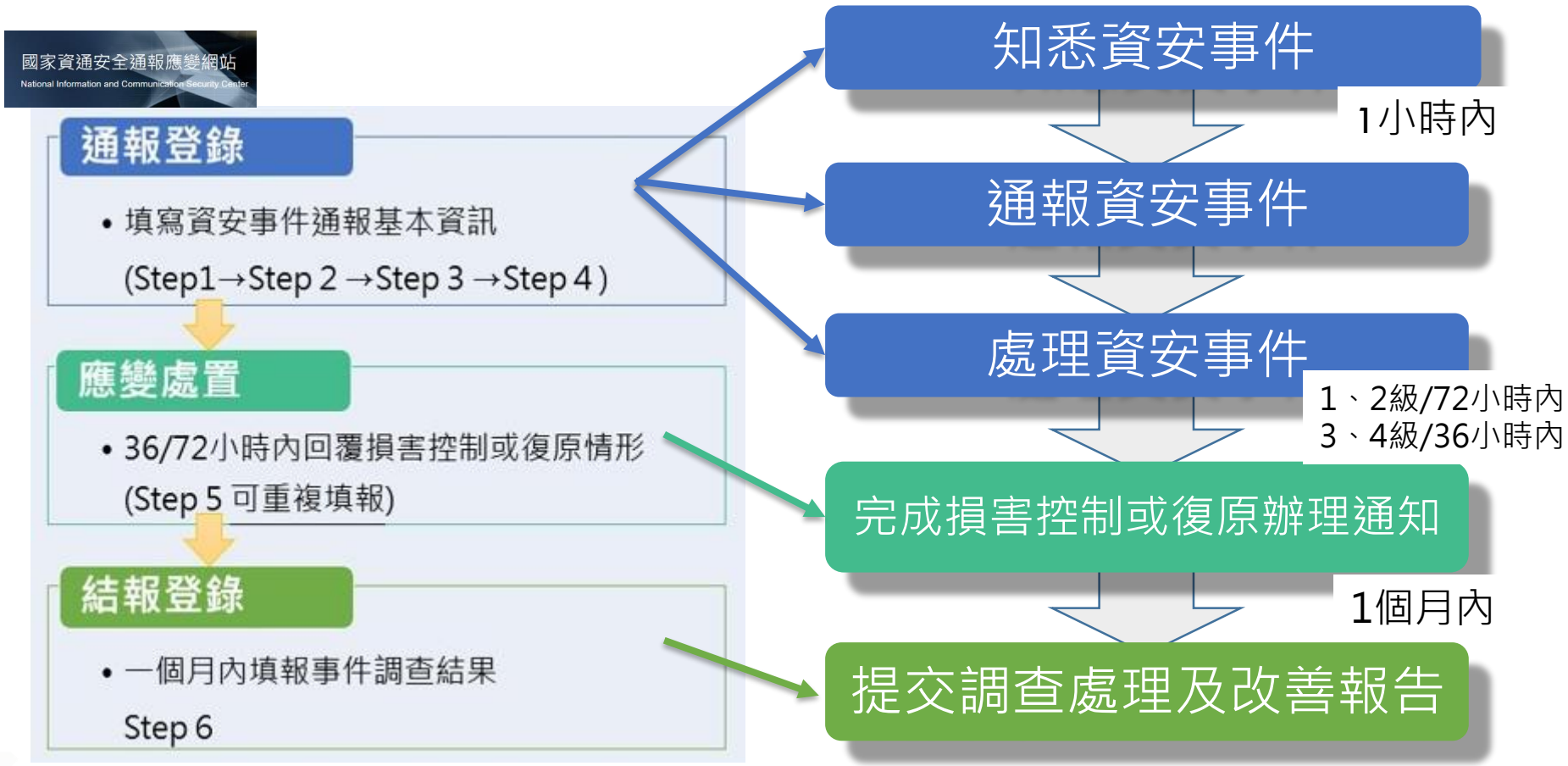
- 公務機關資通安全事件通報作業流程



- 公務機關應於**知悉**資安事件後，**1小時內**向上呈報相關事件資訊
- 依通報等級於限定時間內，完成損害控制或復原並辦理通知
  - 「1」、「2」級事件：72小時
  - 「3」、「4」級事件：36小時
- 完成損害控制或復原作業後，於1個月內送交調查、處理及改善報告

事中應變 – 通報與應變 (3/6)

- 對照國家資通安全通報應變網站，通報及應變作業流程為「通報登錄」、「應變處置」及「結案登錄」等3階段



事中應變 – 通報與應變 (4/6)

事件分析與影響評估

- 當在進行評估時，需要判斷此事件會造成多大影響
  - 影響多廣？影響多少平台或是應用程式？
  - 利用的弱點是甚麼？這個弱點是否仍然存在？
  - 截至目前為止，受影響系統的價值？存在系統裡資料的價值？
  - 遭利用的弱點是否可以透過網路遠端操控？
  - 此弱點是否可公開取得？是否曾在最近公布？

事中應變 – 通報與應變 (5/6)

封鎖根除與復原

- 當災情停止擴大時，則要開始清理攻擊者的傑作
- 判斷資安事件的原因與徵狀
  - 用先前偵測分析階段與封鎖階段得到的資訊
  - 嘗試將攻擊隔離開來，並判斷這些攻擊是如何被執行的

事中應變 – 通報與應變 (6/6)

封鎖根除與復原

長期封鎖

- 系統必須要保持運作而無法進行離線
- 暫時幫助系統繼續營運
- WAF阻擋、防火牆阻擋

移除惡意程式

- 移除造成資安事件的原因
- 後門、惡意程式、病毒
- 建議完整的進行安裝程序

強化防護能量

- 採行適當的保護措施
- 更新系統修補程式

弱點分析

- 系統弱點、網路弱點
- 弱掃工具
- 利用同弱點攻擊多台主機

系統復原

- 修補完畢後的測試計劃
- 恢復上線仍需持續觀測

事中應變 – 紀錄蒐集 (1/5)

事前準備 ▶ 事中應變 ▶ 事後改善

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

通報資安事件
- 資通安全事件通報及應變辦法

損害控制與復原
- 資通安全事件通報及應變辦法

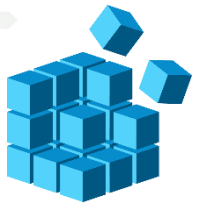
紀錄蒐集
- 修正各機關資通安全事件通報及應變處理作業程序

矯正與改善措施
- 資通安全事件通報及應變辦法

事中應變 – 紀錄蒐集 (2/5)

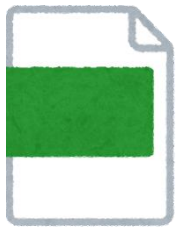
- 事件應變小組完成損害管制後，應蒐集分析相關紀錄，以掌握事件影響範圍與事件發生原因
  - 蒐集相關防護設備紀錄檔
  - 建立鑑識映像檔
- 事件應變小組應依組織內網路/資訊系統架構蒐集相關系統紀錄，包含
  - 防火牆紀錄
  - 網站日誌檔
  - 入侵偵測紀錄
  - 防毒軟體偵測紀錄

事中應變 – 紀錄蒐集 (3/5)



Registry

- **SAM** — 取得**使用者資訊**，如：User Account、Last Login
- **SYSTEM**
- **SOFTWARE**
- **SECURITY** — 確認**系統設定**，如：Network History、Wireless SSID、USB
- **NTUSER** — 取得**使用者活動**，如：Program Execution、File Opening、USB

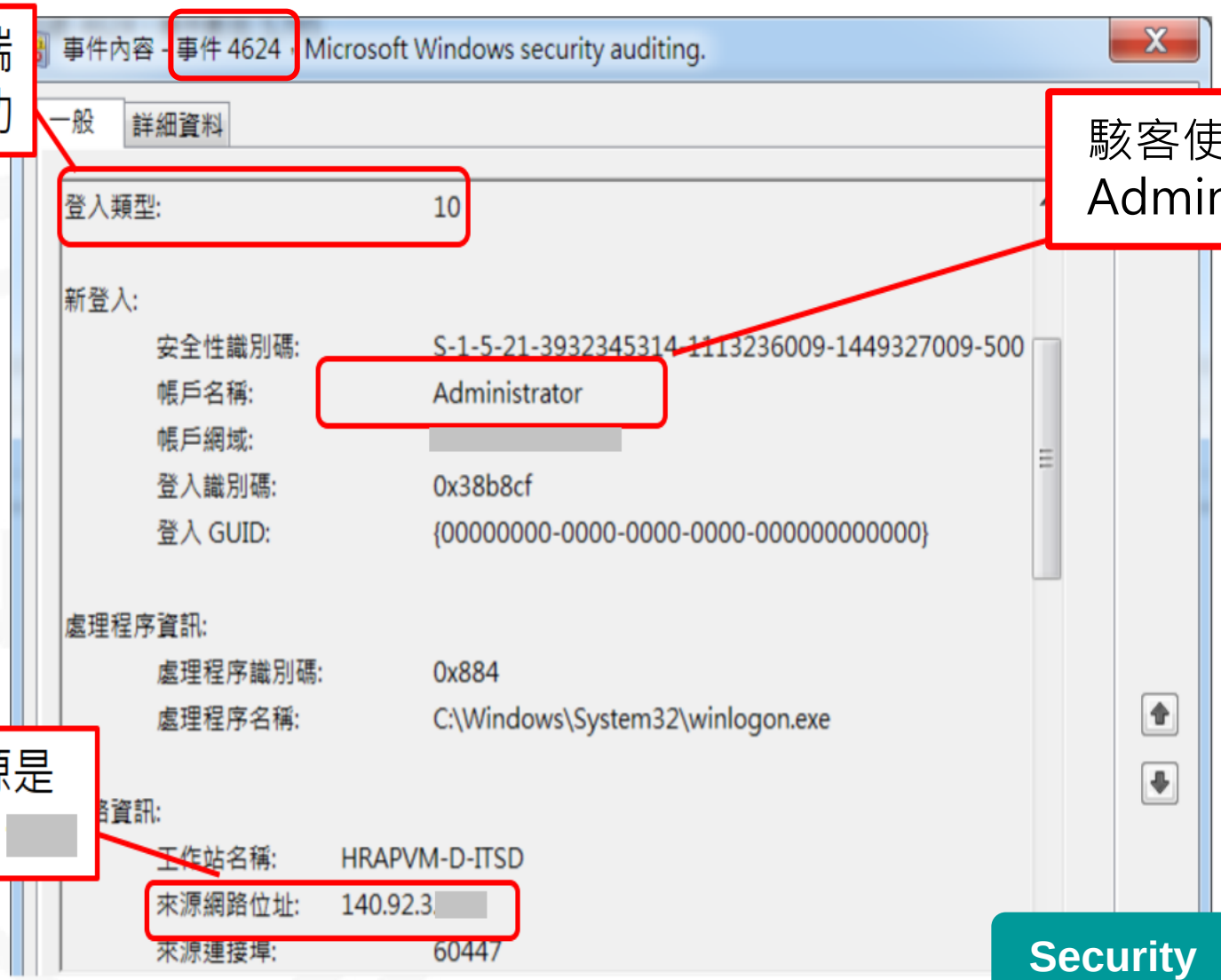


Event Log

- **Application** — 記錄**應用程序**生成的事件，如： MS SQL 無法訪問資料庫、病毒警報
- **Security** — 管理稽核及**安全性**記錄檔，如：登入成功/失敗
- **System** — **作業系統**或其組件記錄的事件，如：重新開機時服務啟動失敗

事中應變 – 紀錄蒐集 (4/5)

駭客利用遠端桌面登入成功



駭客使用的帳號為 Administrator

駭客來源是 140.92.3.

Security

Event ID	info
4624	Successful Logon
4625	Failed Logon
4634/4647	Successful Logoff

登入類型	內容
3	使用者透過網路芳鄰登入
10	使用者透過遠端桌面登入

事中應變 – 紀錄蒐集 (5/5)

- 各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌，確保資安事件發生時所保有跡證足以進行事件根因分析

責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄	• 作業系統日誌(OS event log) • 網站日誌(web log) • 應用程式日誌(AP log) • 登入日誌(logon log)
B	機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄	

註：若資訊系統已向上集中者，則可由上級機關保存。

事後改善 (1/5)

事前準備 ▶ 事中應變 ▶ **事後改善**

訂定通報應變機制
- 資通安全事件通報及應變辦法第9條、第10條

偵測與分析
- 資通安全責任等級分級辦法 – 技術面

資安教育
- 資通安全責任等級分級辦法 – 管理面

通報資安事件
- 資通安全事件通報及應變辦法

損害控制與復原
- 資通安全事件通報及應變辦法

紀錄蒐集
- 資通安全事件通報及應變辦法

矯正與改善措施
- 資通安全事件通報及應變辦法

事後改善 (2/5)

- 依據事件分析結果，確認事件根因並進行修補與改善，以避免再次發生類似之資安事件
- 藉由事件回顧與強化，檢視與完善相關程序

事後改善 (3/5)

- 了解如何偵測和應變處置類似的攻擊，以改進現有防禦
- 了解如何預防未來類似的攻擊，改進預防措施
- 鑑於目前防禦措施在本次事件中的表現，評估其成本效益
- 評估事件造成的損害並確認不會有其他衍生的損害

事後改善 (4/5)

- 對於事件處理的經驗，可透過事後學習報告的方式，持續累積經驗
  - 讓所有受影響部門的成員一同來檢視編撰的報告，達成共識
  - 事後學習會議(最好能在系統回復兩周內進行)

- 評估相關決策是否存在改善需求，找出適當的處理方法並修正異常做法
  - 執行過程程序
  - 技術精進
  - 改善事件處理的能力

事後改善 (5/5)

- 7個容易犯的錯誤
  - 未能即時回報與請求協助
  - 不完整的紀錄或是未進行記錄
  - 錯誤處理/損毀證物
  - 不能正確建立映像檔
  - 不能封鎖與復原攻擊情形
  - 不能預防再次感染
  - 不能執行事後學習結果

資安事件偵測與分析範例(1/2)

可能遭受攻擊類型	症狀	說明
DDOS	1. 服務異常緩慢 2. 伺服器 CPU 或記穩體使用率飆高 3. 大量不完整的三相交握封包 4. 網路流量異常升高	• 目的在耗盡目標電腦的網路或系統資源 • 使服務暫時中斷或停止，導致使用者無法存取服務
勒索軟體	1. 硬碟讀寫率飆升 2. 附檔名遭修改 3. 檔案被加密，無法開啟 4. 彈出付款、聯絡方式視窗或以文字檔方式存在桌面	• 大部份的檔案會被勒索軟體加密 • 特徵為硬碟讀寫率、 CPU 或記憶體使用率大幅提升 • 受加密的檔案副檔名會被修改，部份勒索軟體的家族可從此副檔名判別
惡意程式	1. 彈出視窗廣告畫面 2. 硬碟空間大量耗損 3. 出現可疑網路連線 4. 建立可疑網路連線 5. 瀏覽器首頁重新導向 6. 系統效能緩慢	• 目的可能為破壞系統、竊取資料或其他惡意行為 • 常見惡意程式：木馬、後門程式、間諜軟體、廣告軟體等

資安事件偵測與分析範例(2/2)

事件類型	緊急處理
遭受DDOS	• 使用具備抵禦DDoS的**進階防火牆** • **限制流量**但不關閉服務 • 設置存取**控制清單(ACL)**阻擋可疑IP位址的存取 • 允許的情況下**增加頻寬**以降低攻擊能力 • 網頁服務使用**reCAPTCHA**防止自動連線 • **限制最大連線數量**，縮短idle timeout時間 • **網路流量清洗**
勒索軟體攻擊	• 立即**斷開受感染設備**與所有網路的連接 • **監控**網路流量 • 盤點其他可能受影響的設備，並對這些設備執行**防毒軟體掃描** • 根據勒索軟體名稱、副檔名等資訊，**查找該病毒的類型** • 在**No More RansomProject**的網站上，尋找解密工具
感染惡意程式	• **隔離**受感染系統，避免擴散感染 • **阻斷**惡意程式嘗試通聯的網路 • 使用TCPView**偵測網路行為** • 使用AutoRuns查看可疑程式是否於**系統開機後自動執行** • 使用Process Explorer查看是否有**可疑的程式**正在執行 • 在主機端和防火牆上關閉所有**不必要的TCP/UDP Port** • 利用Msert(微軟掃毒軟體)**找出可疑檔案**，並將其刪除

參考範例 – 分散式阻斷服務 (1/5)

- 請以分散式阻斷服務(DDoS)為題，製作一份應變程序，分別說明事前、事中、事後應考量之項目與內容

參考範例 – 分散式阻斷服務 (2/5)

- 不同資安事件類型，「資安事件應變處理程序」3階段之應變處置項目不盡相同，建議應依事件需求建立不同事件應變程序

事前準備

- 維護系統及網管人員/廠商聯繫資訊
- 調校系統/服務設定
- 設置網路流量/系統資源監控機制
- 建置/申請雲端備援
- 申請/建置流量清洗服務
- 申請內容傳遞網路CDN服務
- 啟用網路/防護設備DDoS防禦功能

事中應變

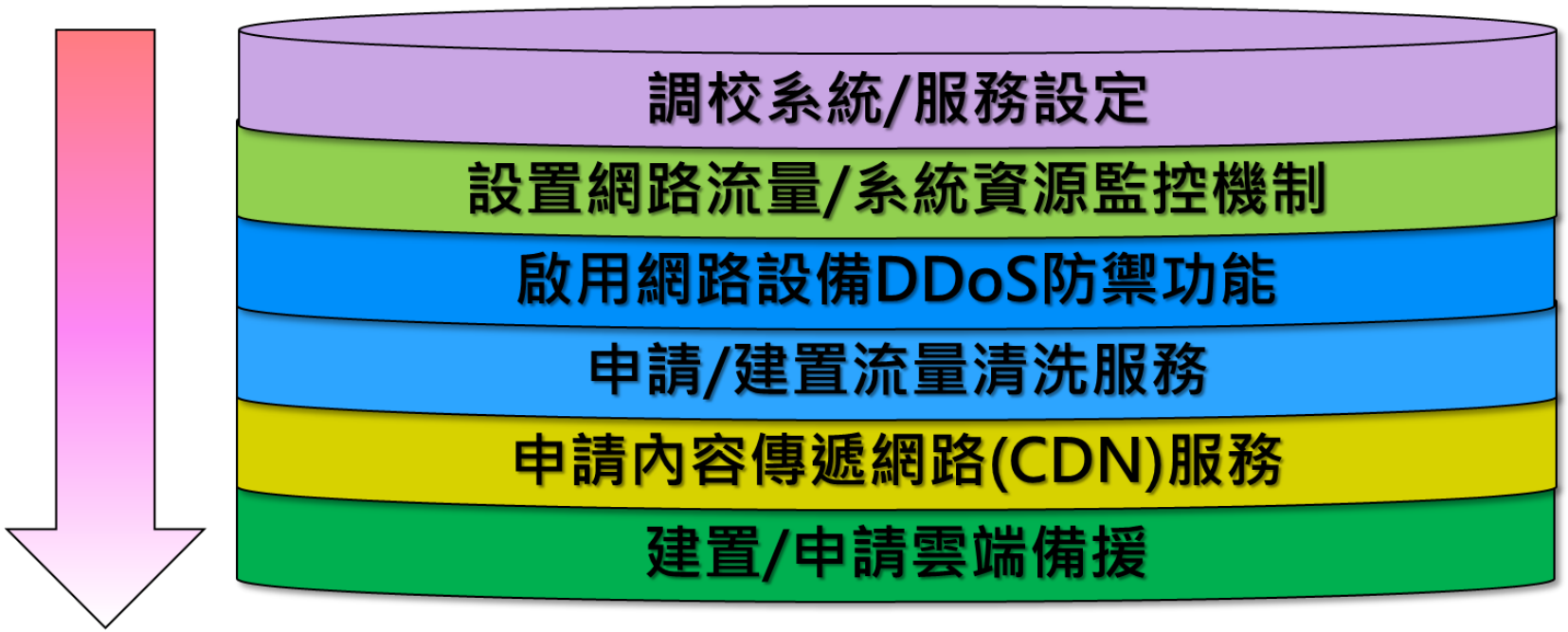
- 攻擊事件分析
- 啟用流量清洗服務
- 啟用雲端備援
- 協請GSN維運小組協助
- 攻擊事件通報

事後改善

- 復原資訊設備運作
- 持續監控網路流量
- 記錄事件處理過程
- 攻擊事件結報

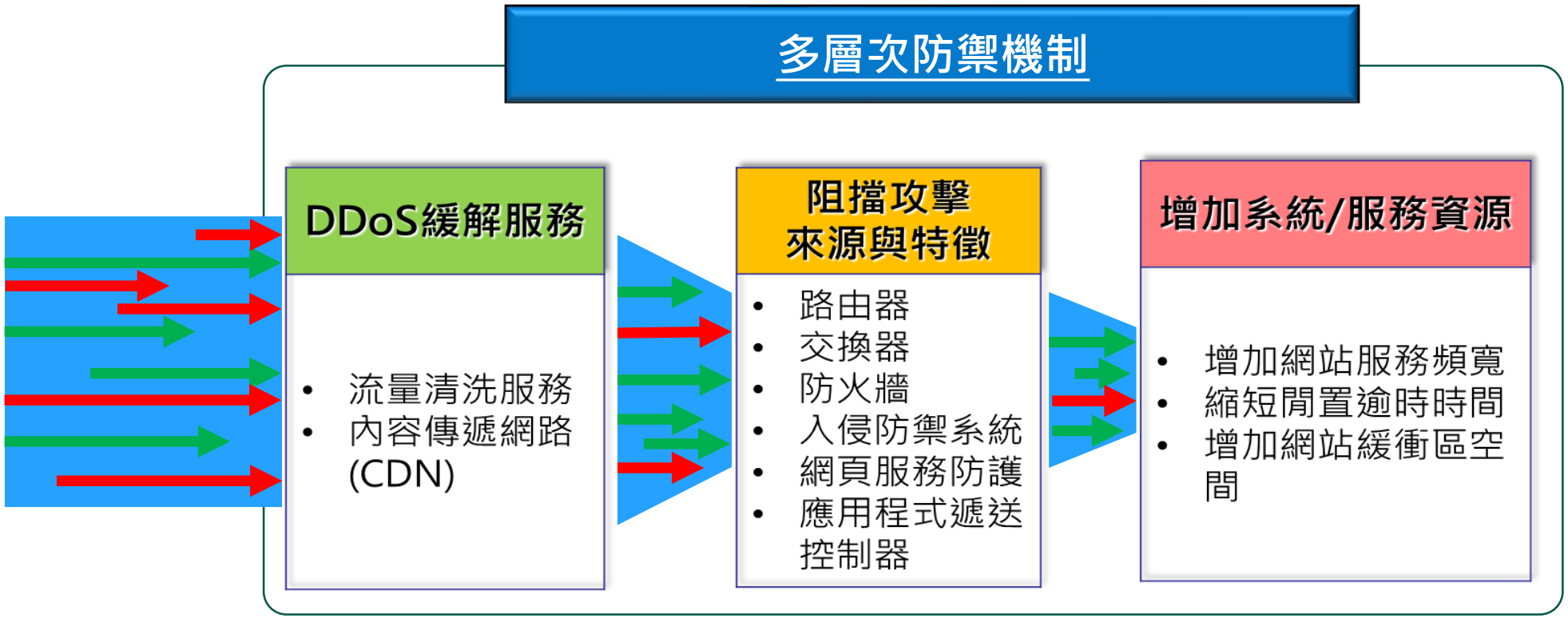
參考範例 – 分散式阻斷服務 (3/5)

- 機關在事前應視內部資源情況，**調校系統/服務項目**，並**申請/建置DDoS相關防護設備**，以強化DDoS防禦能量



參考範例 – 分散式阻斷服務 (4/5)

- 當發現攻擊流量時，機關可內部設置多層次DDoS防禦機制阻擋攻擊流量



參考範例 – 分散式阻斷服務 (5/5)

- 確認DDoS攻擊已停止，即可評估恢復系統設定，或停用備援機制，以恢復系統業務正常運作

復原資訊設備運作

資訊設備若於受到DDoS攻擊後已進行關機，抑或停止/限制提供部分網路服務，應評估是否恢復其正常運作

持續監控網路流量

持續監控網路流量，密切注意DDoS攻擊是否再度發生

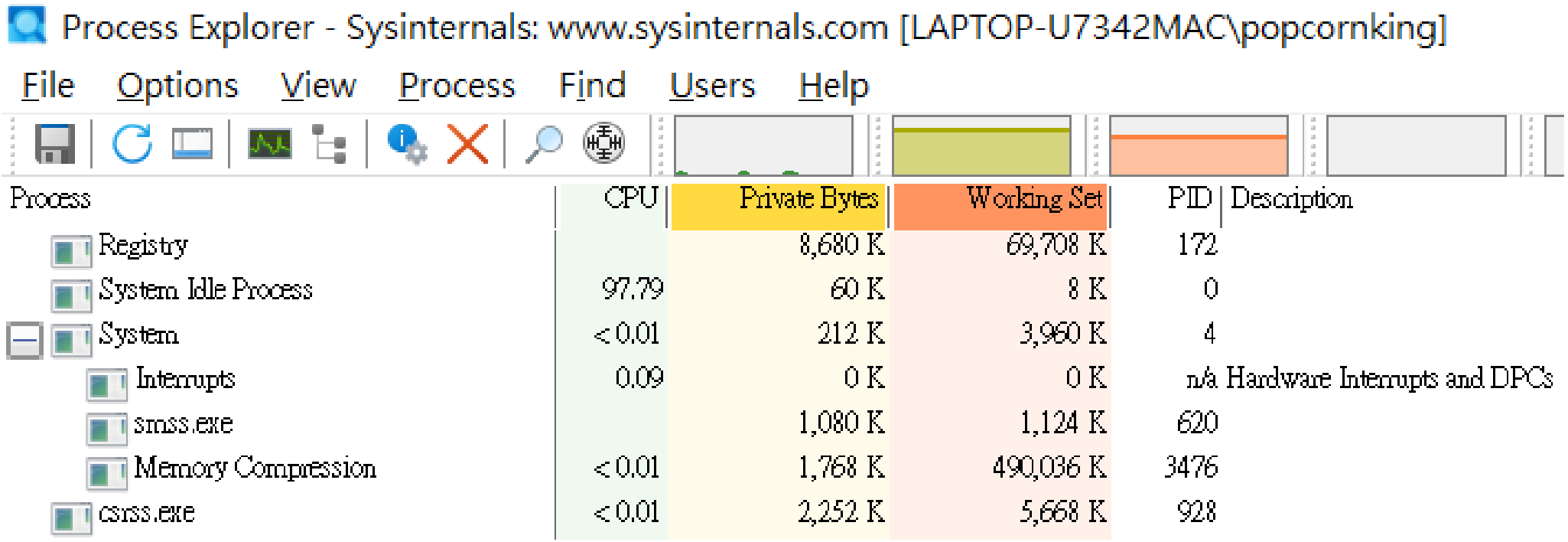
記錄事件處理過程

記錄事件發生過程與處理程序，包含**攻擊原因及手法**等資訊，以及因應該次DDoS攻擊所採取之**應變措施或解決方案**與後續處理情形

【練習】

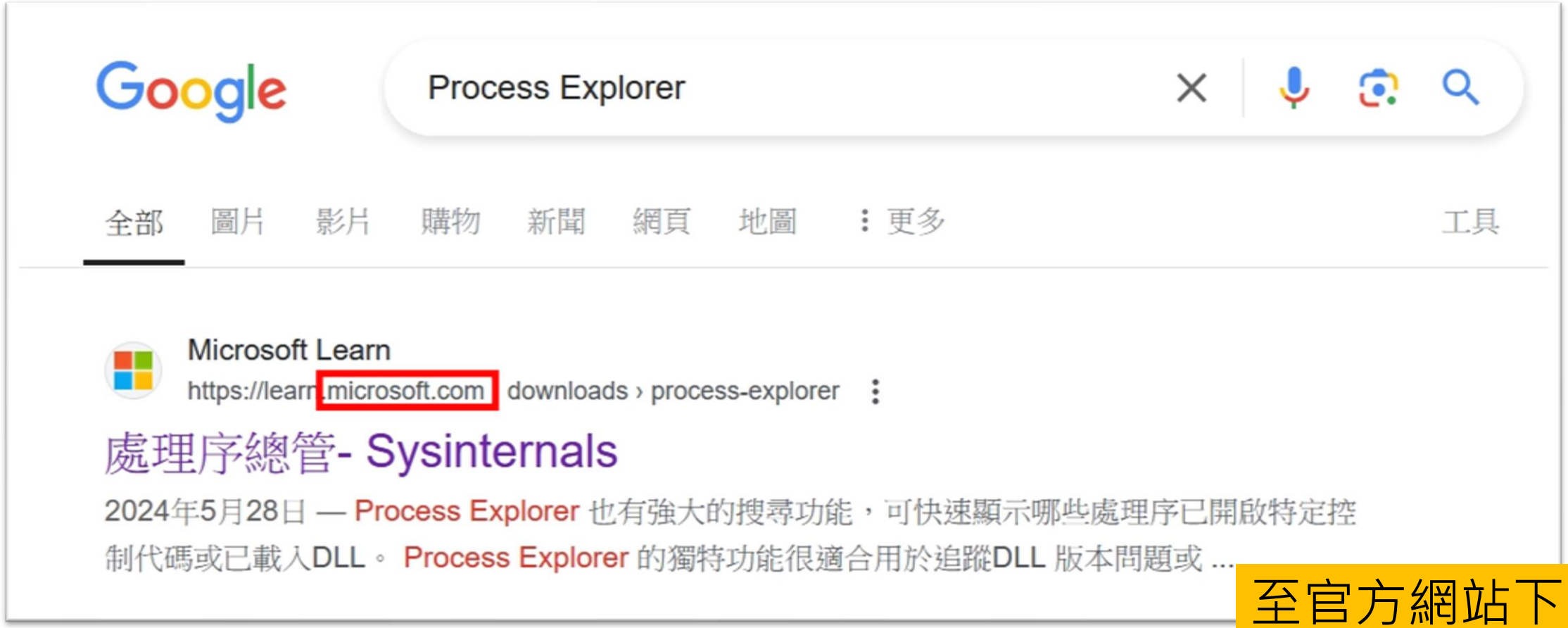
Process Explorer (1/8)

- Process Explorer
  - 微軟所提供的工具之一，用以查詢主機目前**正在執行的程式**，提供各程序相關資訊，且可**結合VirusTotal**進行惡意程式辨識



Process Explorer (2/8)

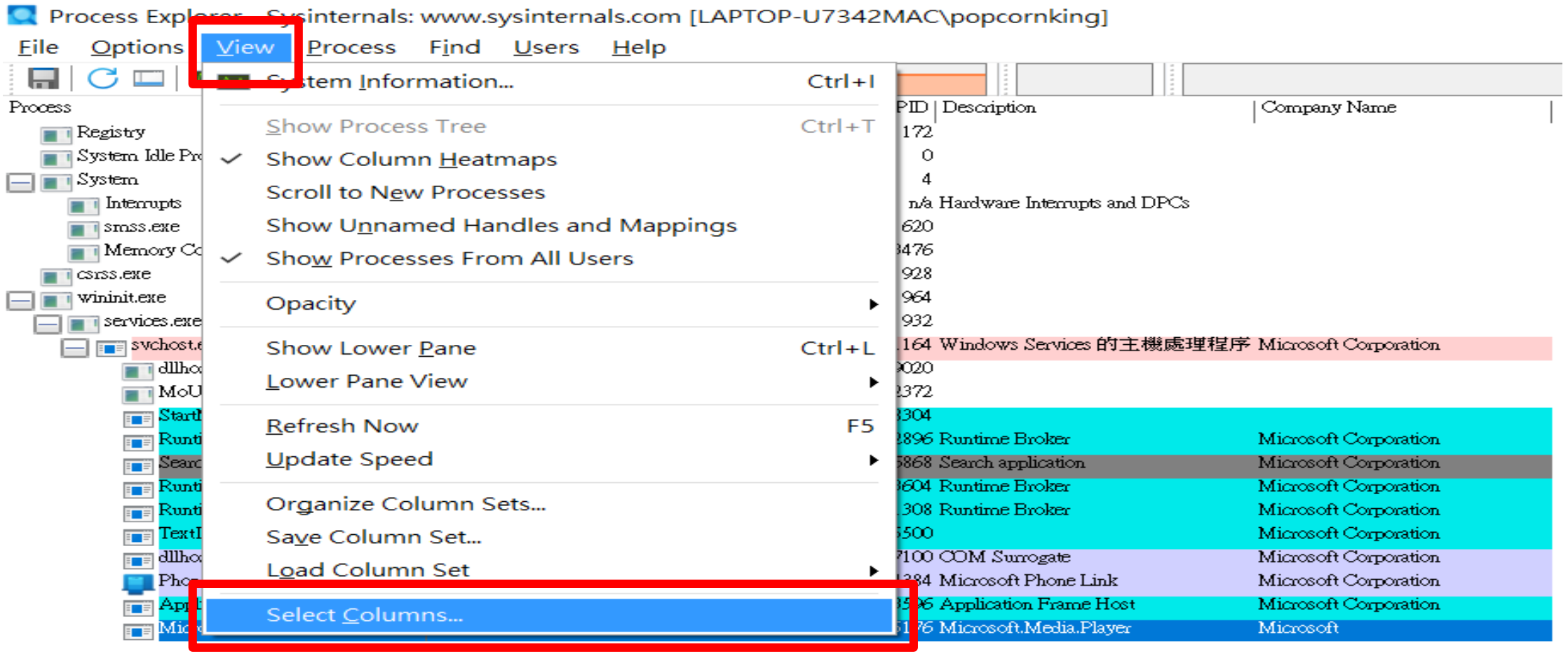
- 至官方網站下載Process Explorer
  - https://download.sysinternals.com/files/ProcessExplorer.zip



至官方網站下載

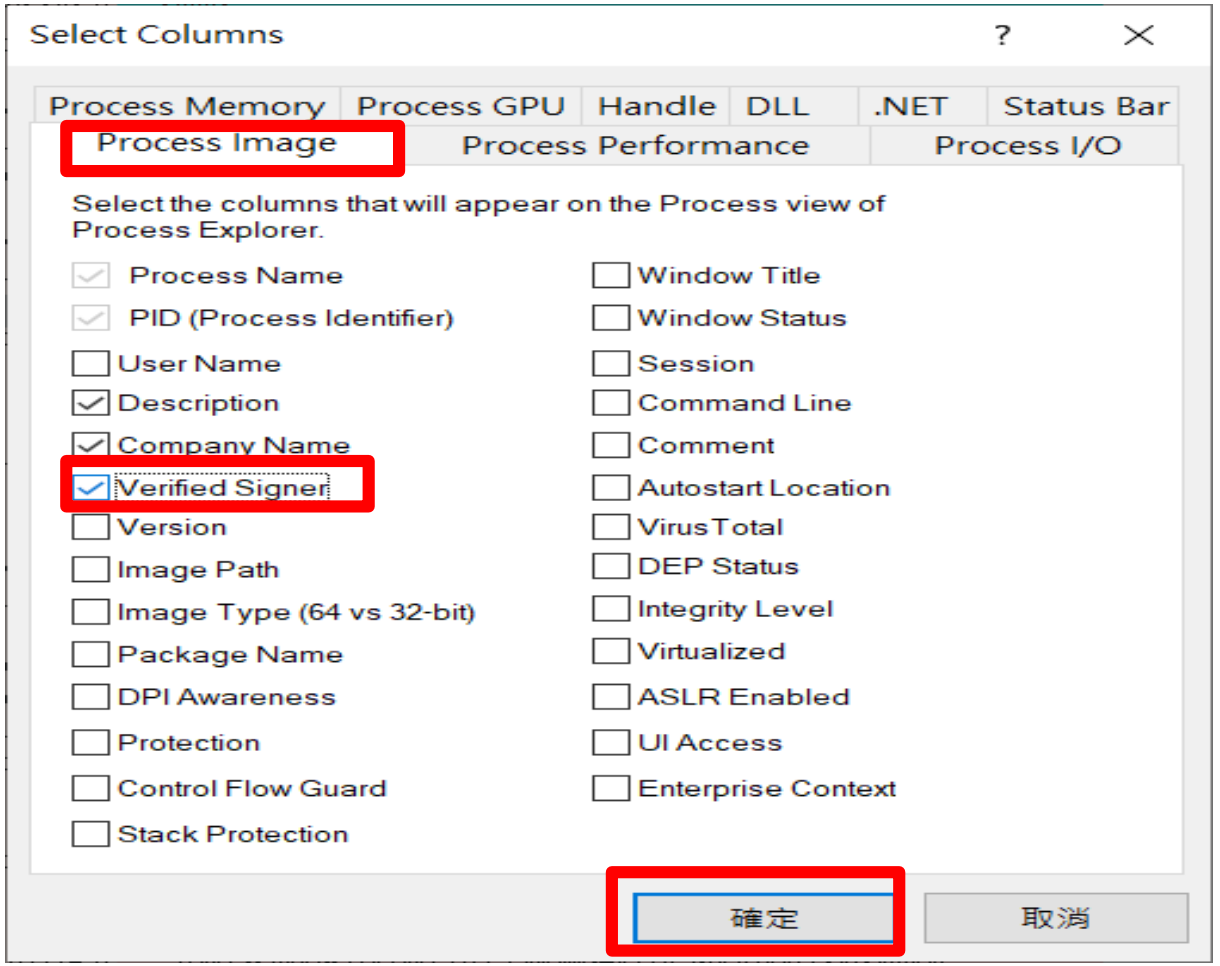
Process Explorer (3/8)

- 電腦執行中的惡意程式檢測
  - –啟動Process Explorer，並點選View→SelectColumns…



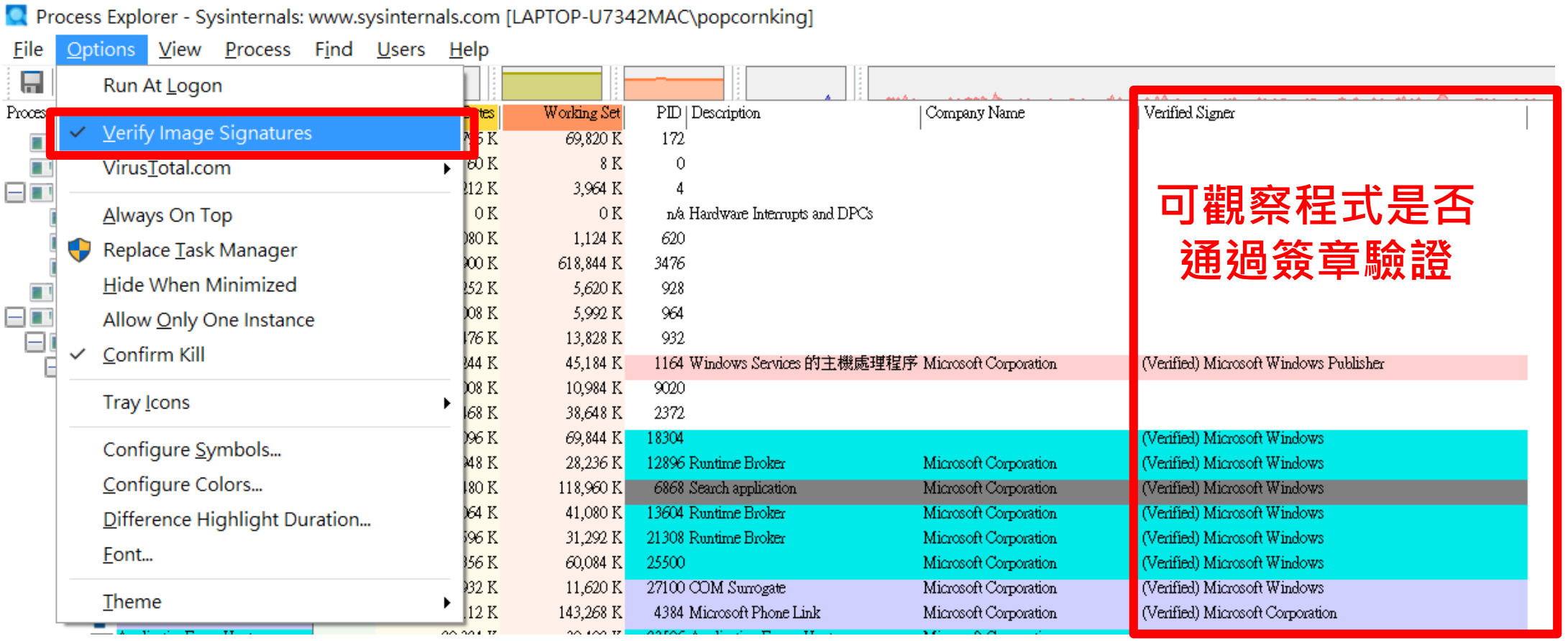
Process Explorer (4/8)

- 電腦執行中的惡意程式檢測
  - 在Process Image標籤中，將Verified Singer勾選



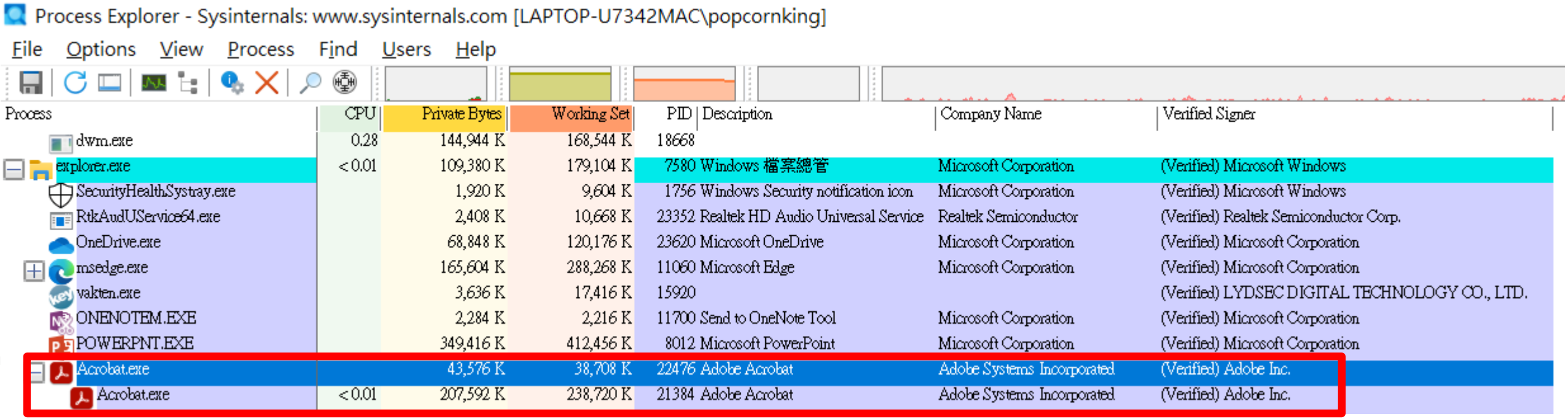
Process Explorer (5/8)

- 電腦執行中的惡意程式檢測
  - 點選Options→Verify Image Singnatures



Process Explorer (6/8)

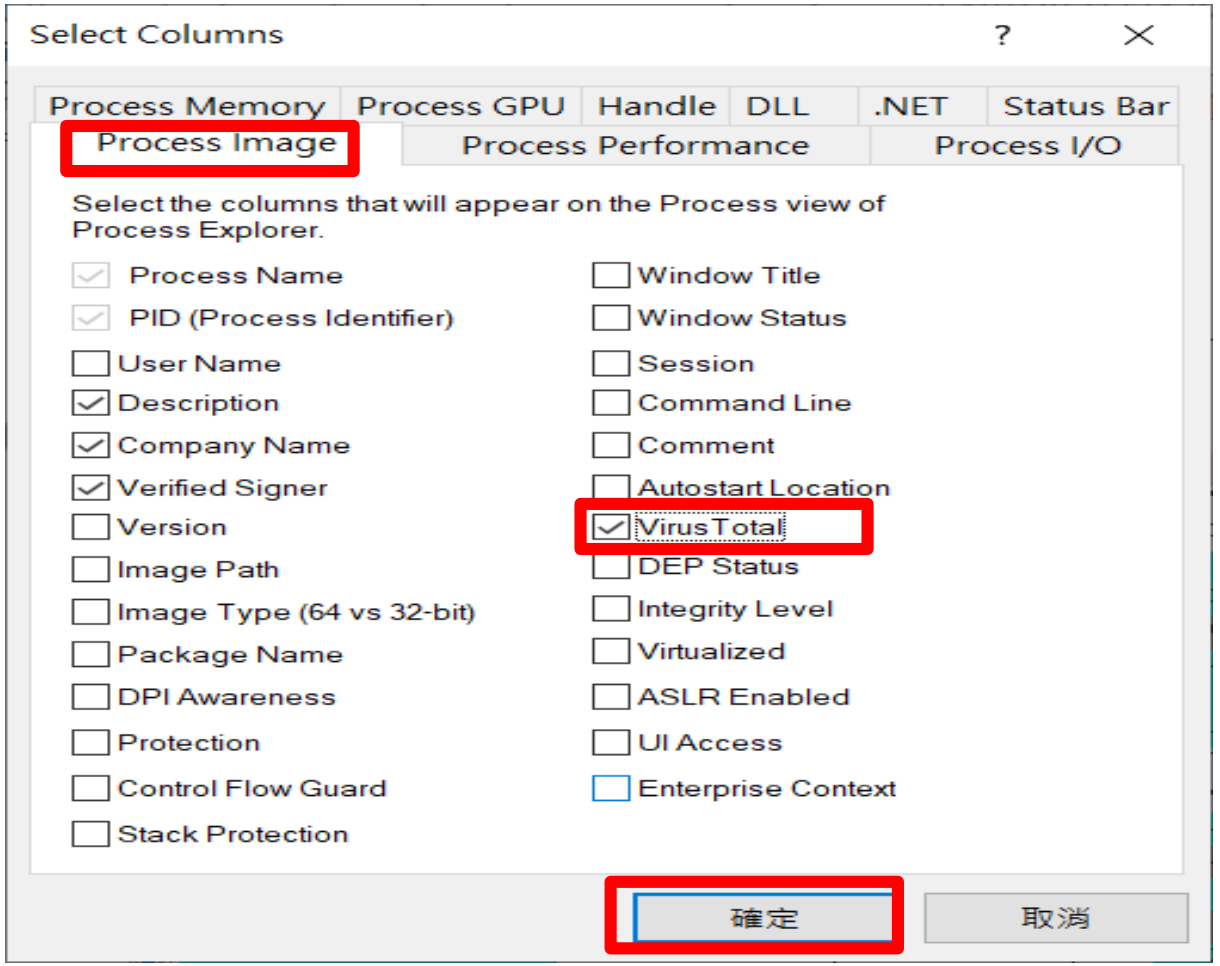
- 簽章驗證的意義？
  - 近年來只要是稍有規模的軟體公司，均對資安十分重視，在發布軟體的時候會附上該公司簽署的數位簽章
  - 若簽章驗證無誤，代表此軟體從公司發布之後，未曾被修改過



有簽章驗證可以確保是Adobe 的PDF reader，而不是駭客做的PDF reader

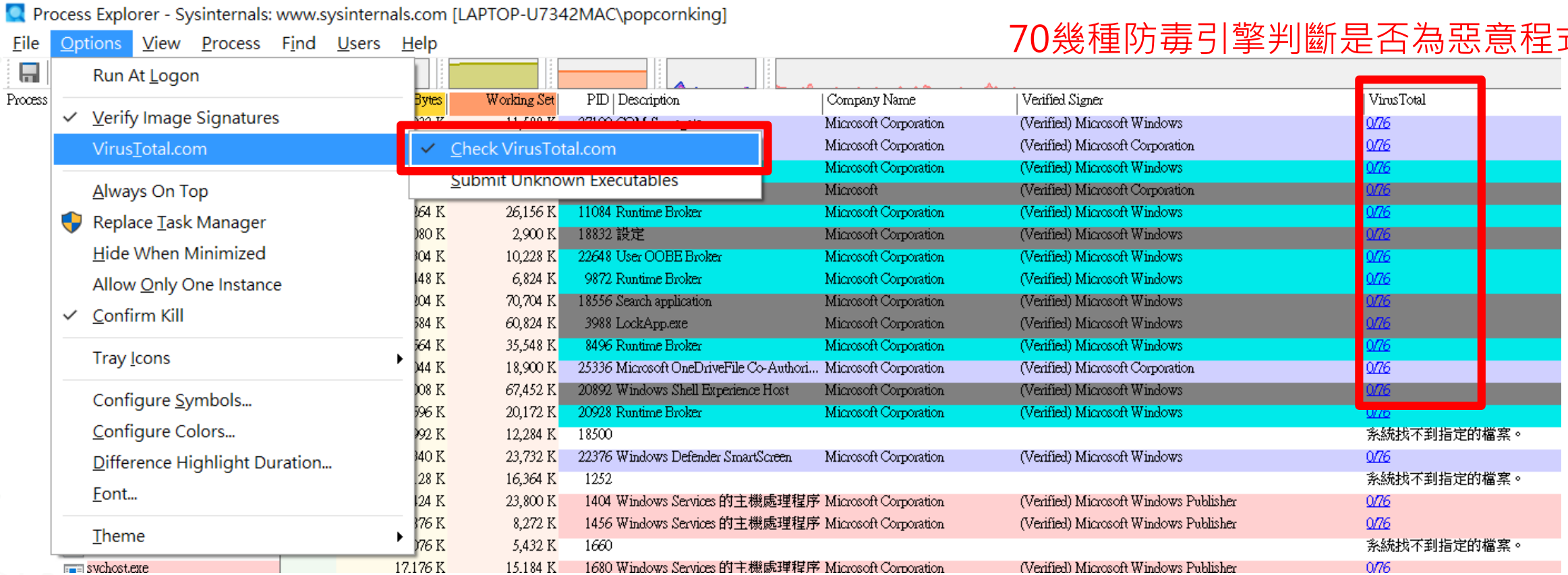
Process Explorer (7/8)

- 電腦執行中的惡意程式檢測
  - 在Process Image標籤中，將VirusTotal勾選



Process Explorer (8/8)

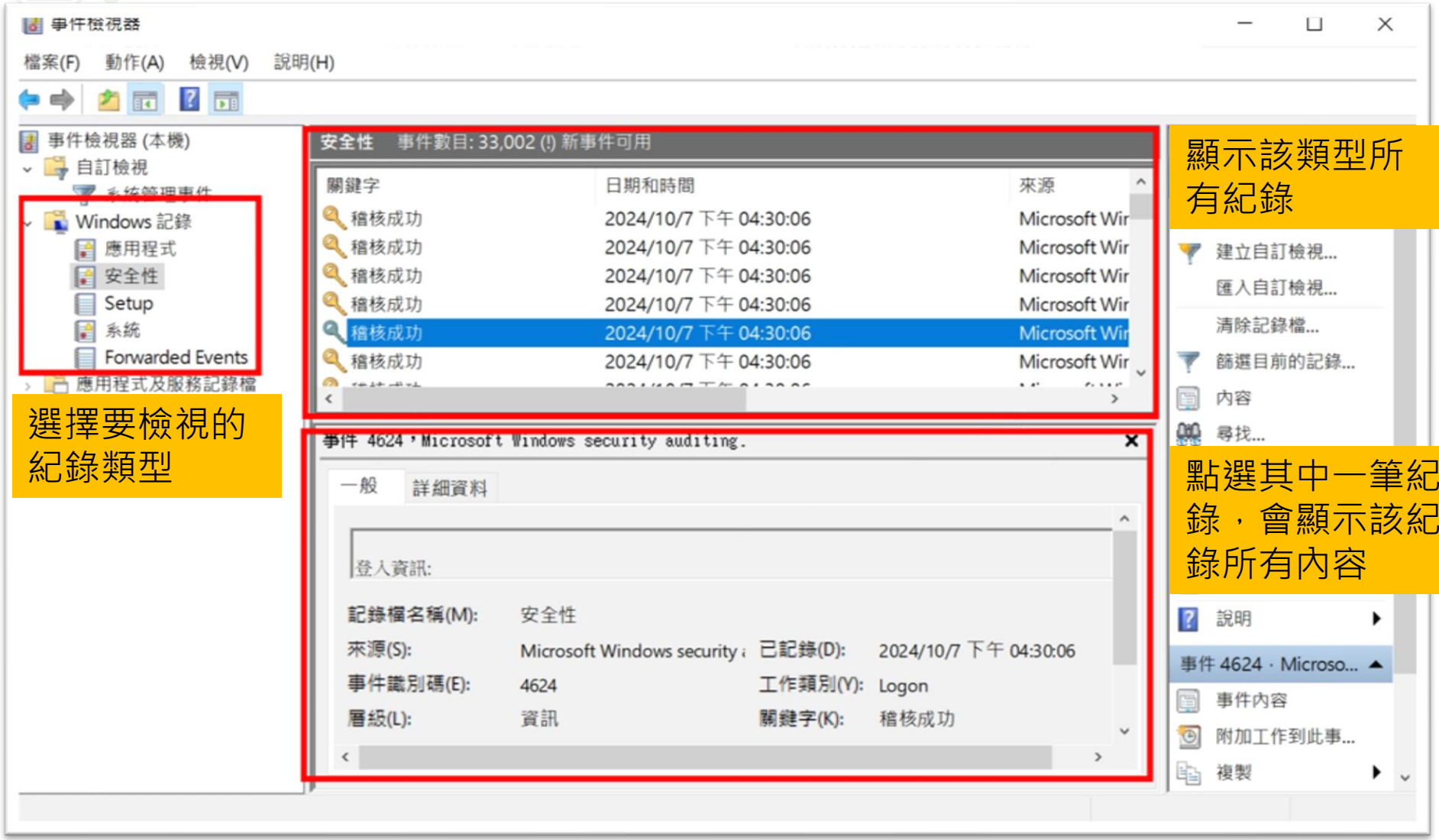
- 電腦執行中的惡意程式檢測
  - 點選Options→VirusTotal.com→CheckVirusTotal.com



Event log介紹 (1/7)

- 系統運作過程中會留下各種事件日誌和紀錄，方便系統管理員掌控系統上發生的各種狀況，以確保系統正常穩定且安全的運作
- 開啟Windows Event log
  - –Windows系統管理工具→事件檢視器

Event log介紹 (2/7)



Event log介紹 (3/7)

- Event log是windows內建的日誌紀錄，預設會自動記錄系統中重要的事件系統

Event Log	紀錄格式(副檔名)	作業系統	檔案路徑
舊版	*.evt	Windows XP Windows 2000 Windows 2003	NT 5 C:\Windows\System32\config
新版	*.evtx	Windows Vista Windows 7 Windows 8 Windows 10 Windows 11	NT 6 C:\Windows\System32\winevt\logs

Event log介紹 (4/7)

- 紀錄類型主要可以分為三類

紀錄類型	紀錄內容
安全性 Security	存取控制(Access Control)和安全設定的相關紀錄 ex.使用者登入紀錄、帳密錯誤紀錄
系統 System	系統服務(Windows Services)、系統運作及驅動程式的相關紀錄 ex.系統服務停止、電腦重開機
應用程式 Applications	應用程式所產生且無關系統的紀錄 ex.防毒軟體掃描結果紀錄、MSSQL連線錯誤紀錄

Event log介紹 (5/7)

- Security Log 是最常用來稽核的類型，比較重要的紀錄內容
  - 使用者驗證與登入登出
  - 使用者的行為
  - 檔案和資料夾的存取
  - 安全設定的修改
- Security Log僅可由系統程式lsass.exe 進行記錄，其他程式無法修改，故可作為良好的參考資訊

Event log介紹 (6/7)

- 類型概要

類型	內容
錯誤	重大錯誤，例如服務無法啟動
警告	可能是發生錯誤的前兆，例如磁碟空間不足
資訊	應用程式及服務的成功操作紀錄，例如Event Log服務啟動成功
稽核成功	安全性稽核成功，例如使用者成功登入
稽核失敗	安全性稽核失敗，例如使用者登入時打錯密碼

Event log介紹 (7/7)

- 事件編號可參考Microsoft官方資料
  - https://learn.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

目前的 Windows 事件識別碼	舊版 Windows 事件識別碼	潛在危險程度	事件摘要
4618	N/A	高	已發生受監視的安全性事件模式。
4649	N/A	高	已偵測到重新執行攻擊。 可能是設定錯誤的錯誤所造成的無害誤判。
4719	612	高	系統稽核原則已變更。
4765	N/A	高	SID 歷程記錄已新增至帳戶。
4766	N/A	高	嘗試將 SID 歷程記錄新增至帳戶失敗。
4794	N/A	高	嘗試設定目錄服務還原模式。
4897	801	高	已啟用角色分離：
4964	N/A	高	特殊群組已指派給新的登入。

Event log判讀 (1/9)

- 可能有駭客登入，如何稽核使用者帳戶？
  - 相關的Security Event ID
    - 528/540/4624：登入成功
    - 682/4778：中斷後再連回
    - 529~537/539/4625：登入失敗
    - 538/4634：登出
    - 576/4672：使用管理者權限登入

Event log判讀 (2/9)

- 登入稽核紀錄較重要的有三項
  - 登入類型
  - 帳戶名稱
  - 來源網路位址

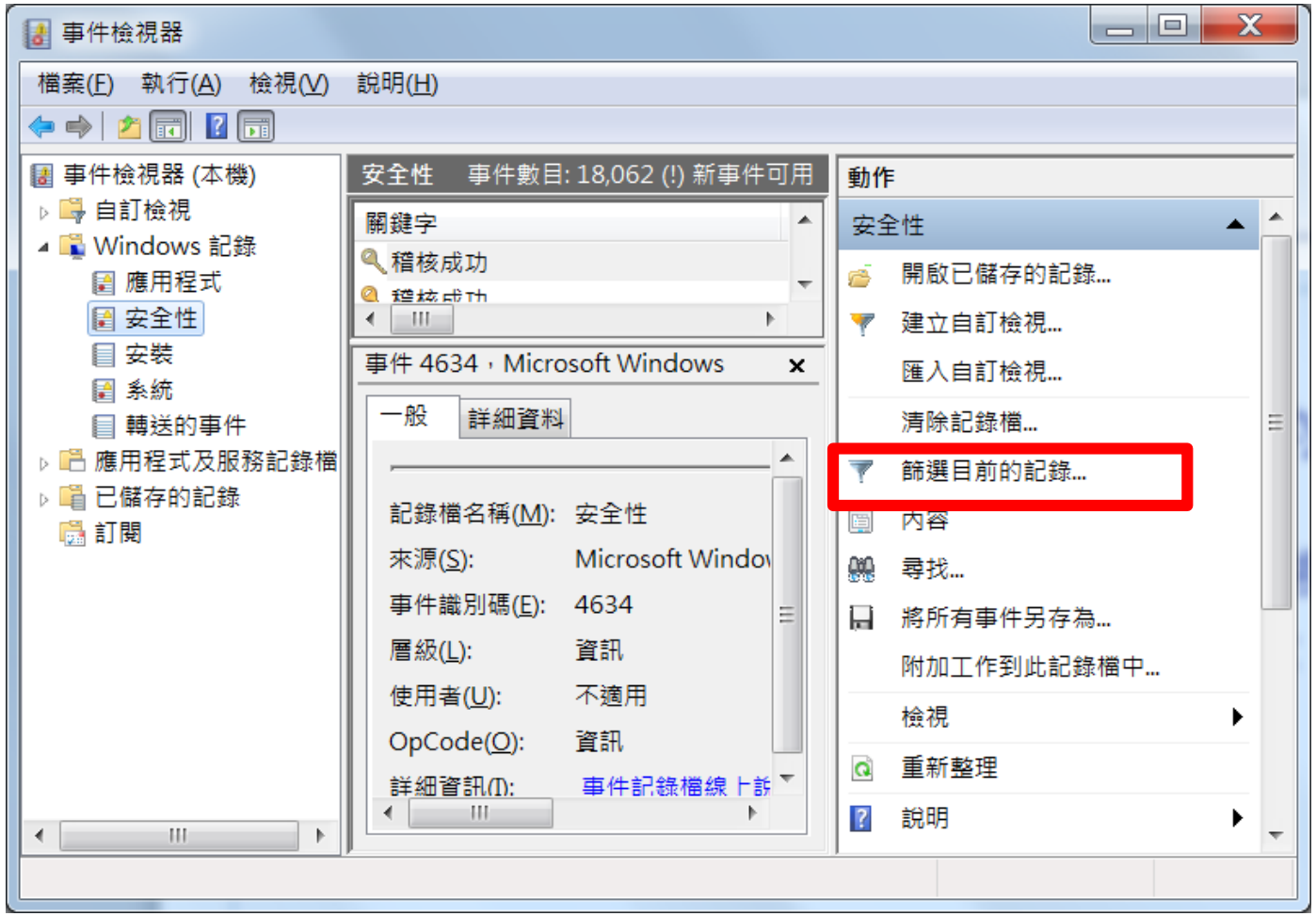
Event log判讀 (3/9)

- 登入類型解析

類型	內容
2	使用者於電腦前直接登入
3	使用者透過網路芳鄰登入
4	利用排程(scheduledtasks)的方式登入
5	微軟服務登入
7	使用者解鎖螢幕
8	使用者透過網路芳鄰登入，但未加密，僅有部分老舊管理工具會出現
9	使用者登入後用其他使用者權限執行程式(RunAs)
10	使用者透過遠端桌面登入
11	使用者於電腦前利用快取憑證(cached credentials)登入
12	使用者利用快取憑證透過遠端桌面登入
13	使用者利用快取憑證解鎖螢幕

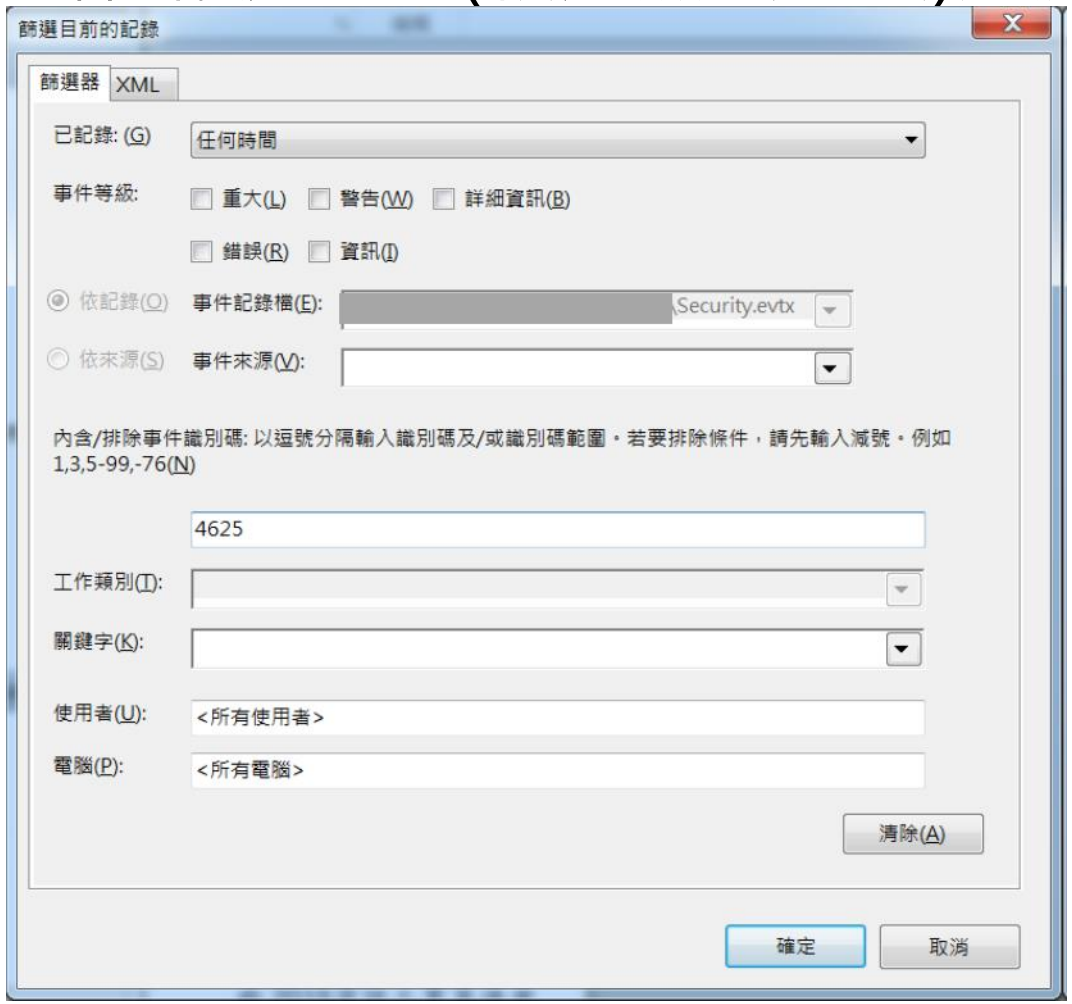
Event log判讀 (4/9)

- 應用1：查看駭客是否有嘗試暴力破解密碼
  - 「安全性→篩選目前的紀錄」



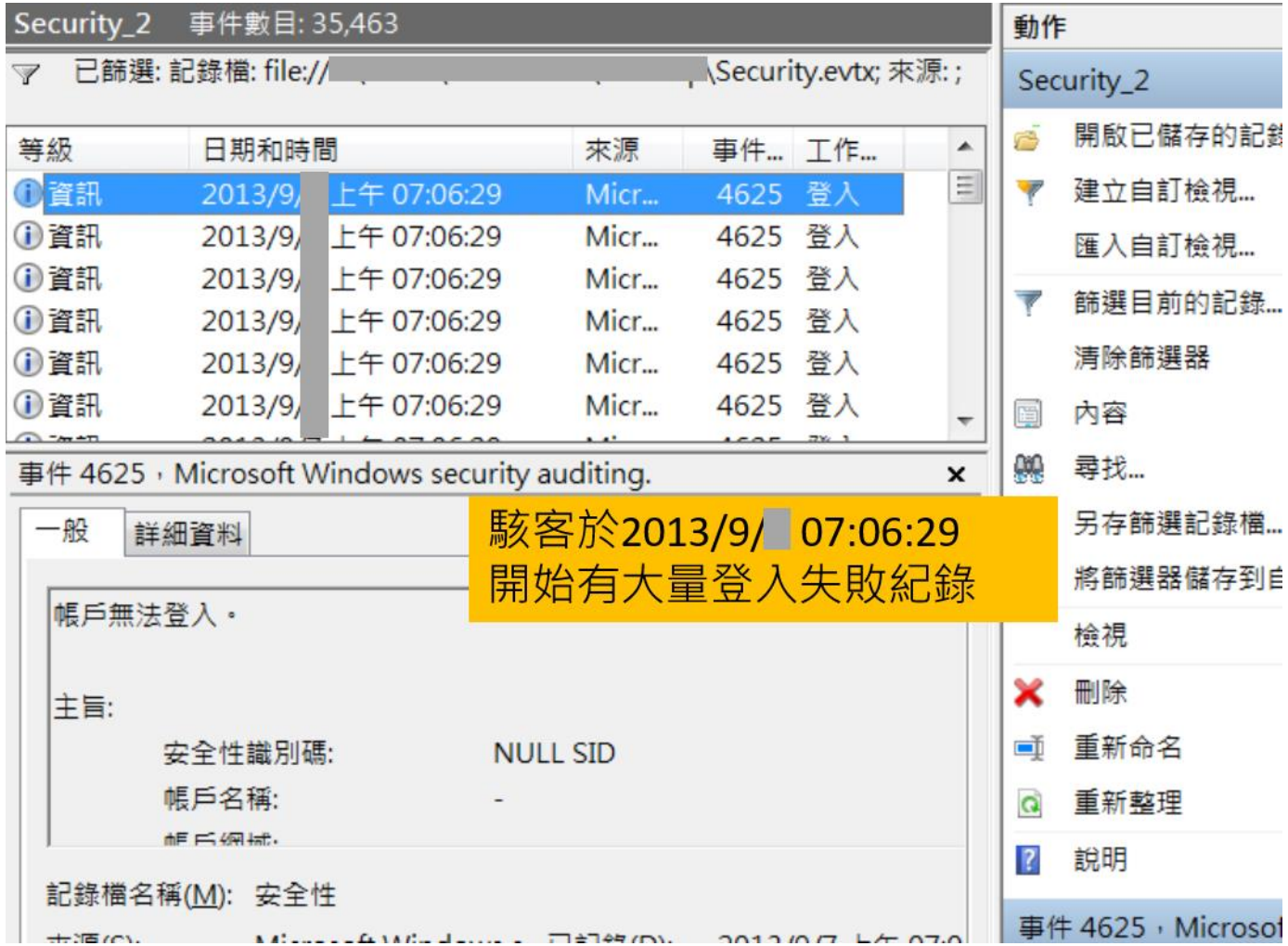
Event log判讀 (5/9)

- 於篩選器用事件編號4625(帳戶無法登入)過濾紀錄

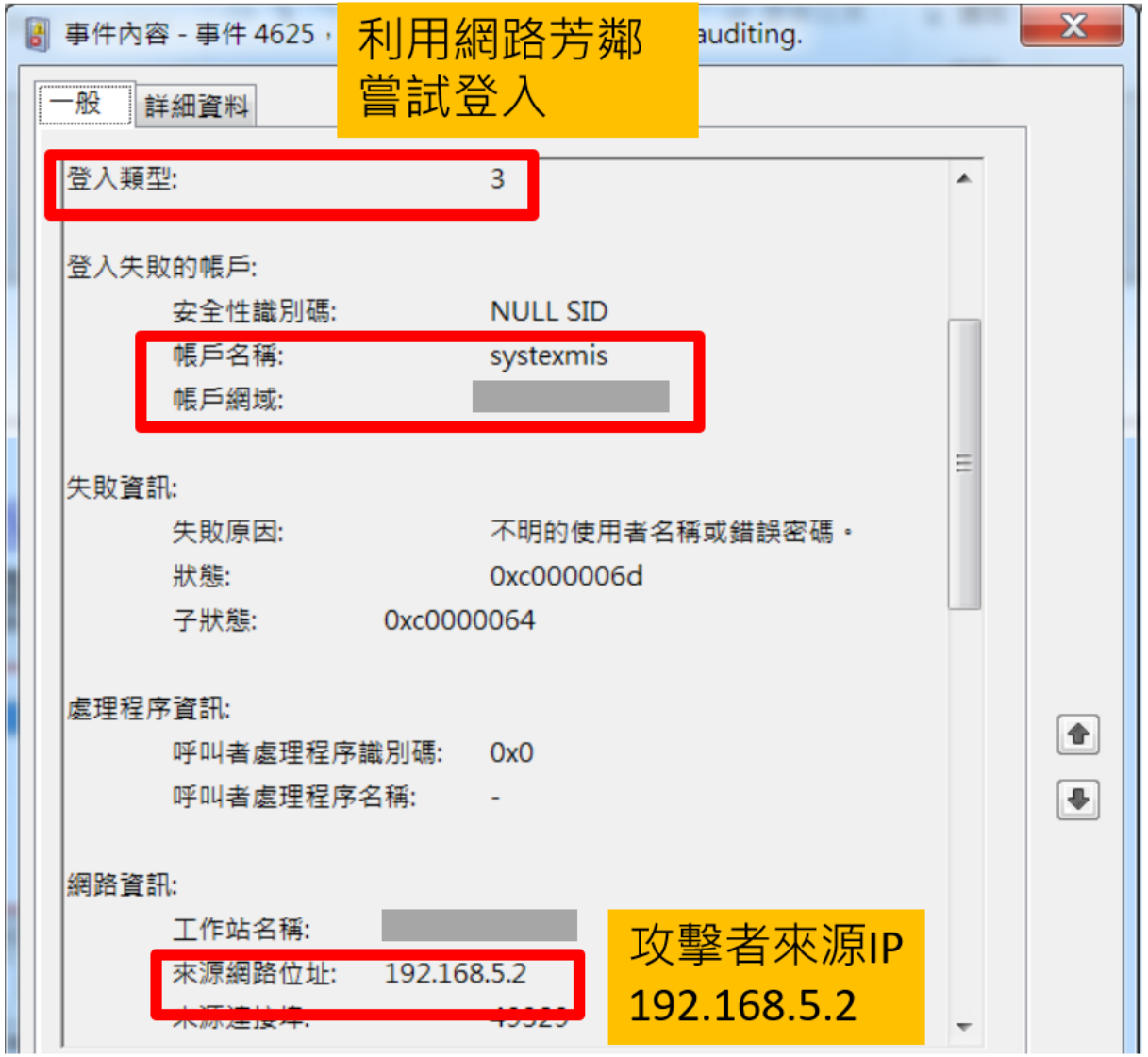


Event log判讀 (6/9)

- 查看駭客是否有嘗試暴力破解密碼

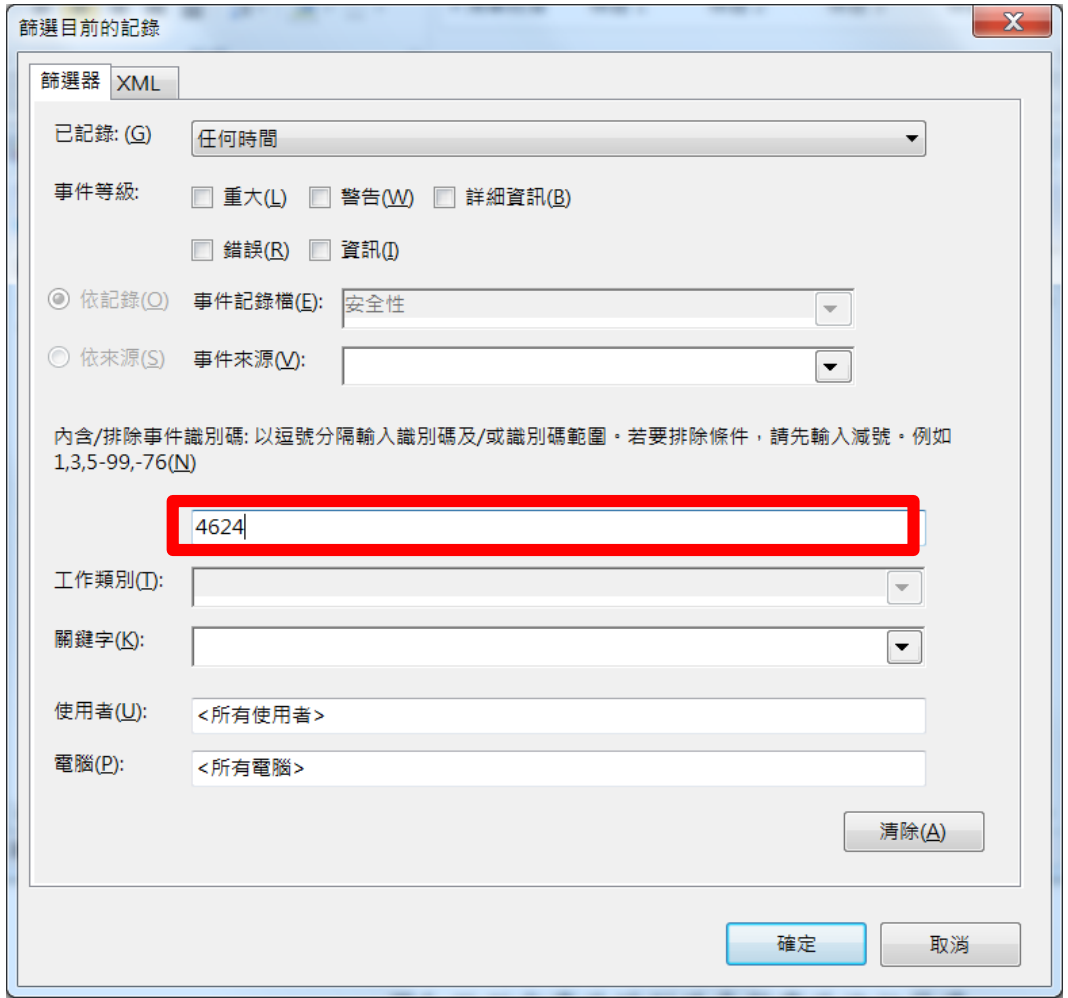


Event log判讀 (7/9)



Event log判讀 (8/9)

- 應用2：查看是否有駭客登入紀錄
  - –於篩選器利用事件編號4624(已成功登入帳戶)過濾紀錄

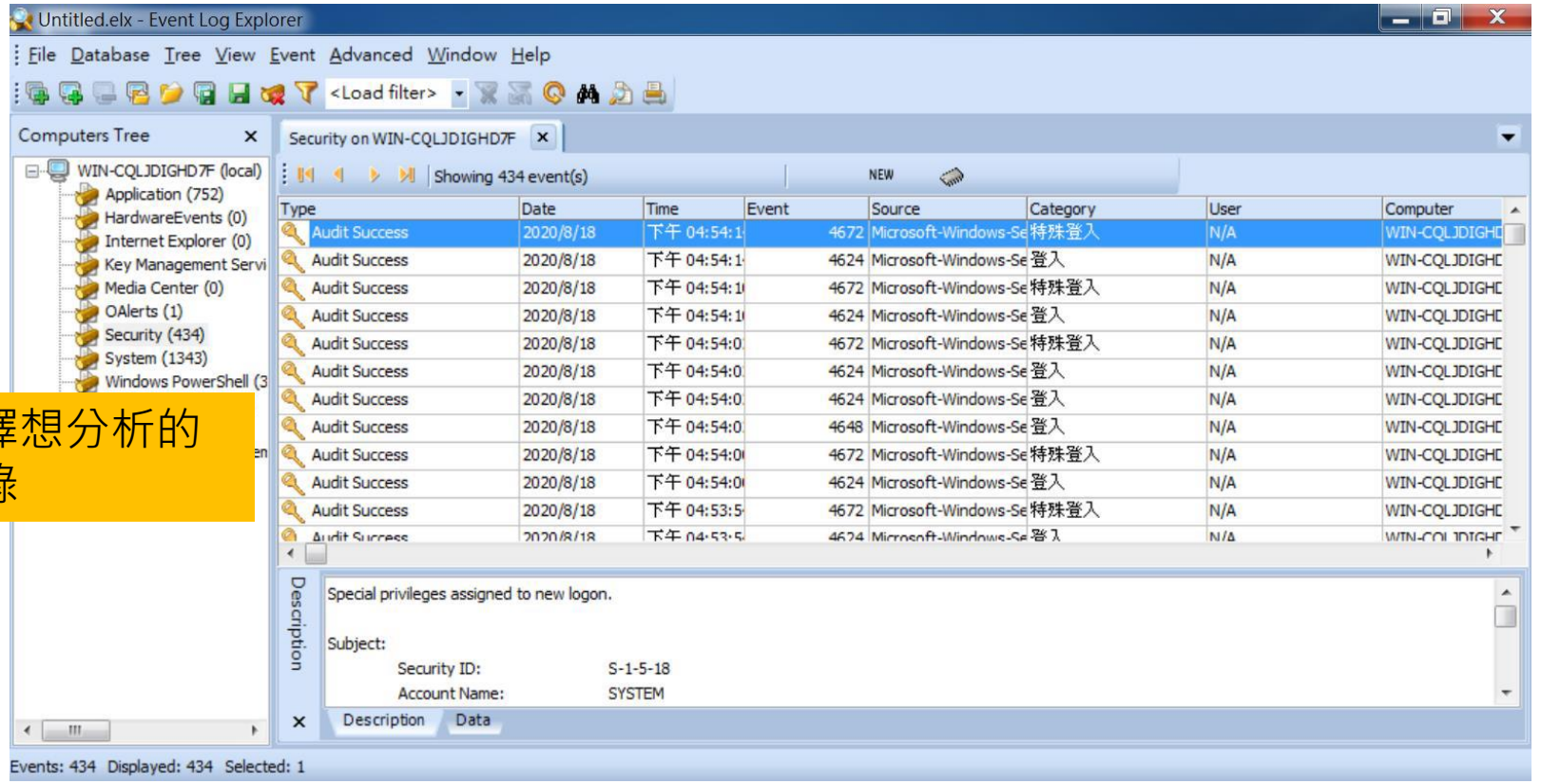


Event log判讀 (9/9)

- 點選該紀錄後，進一步判讀相關資訊

Event Log Explorer

- 由於微軟內建的事件檢視器較為陽春，故多數分析人員多採用其他第三方工具對日誌進行檢視，免費的工具中最有名的即為Event Log Explorer



報告完畢 敬請指教

國家資通安全研究院
National Institute of Cyber Security