TLP:GREEN

台灣電腦網路危機處理暨協調中心 (TWCERT/CC) 服務簡介

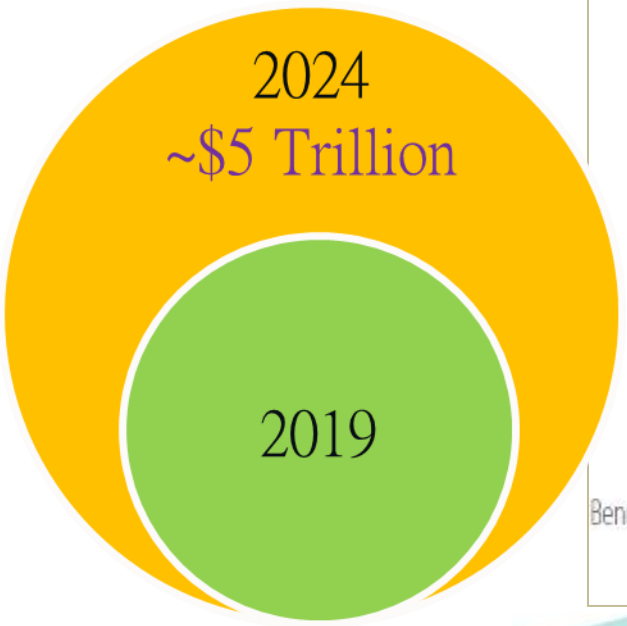
台灣網路資訊中心(TWNIC)
組長 林志鴻 博士

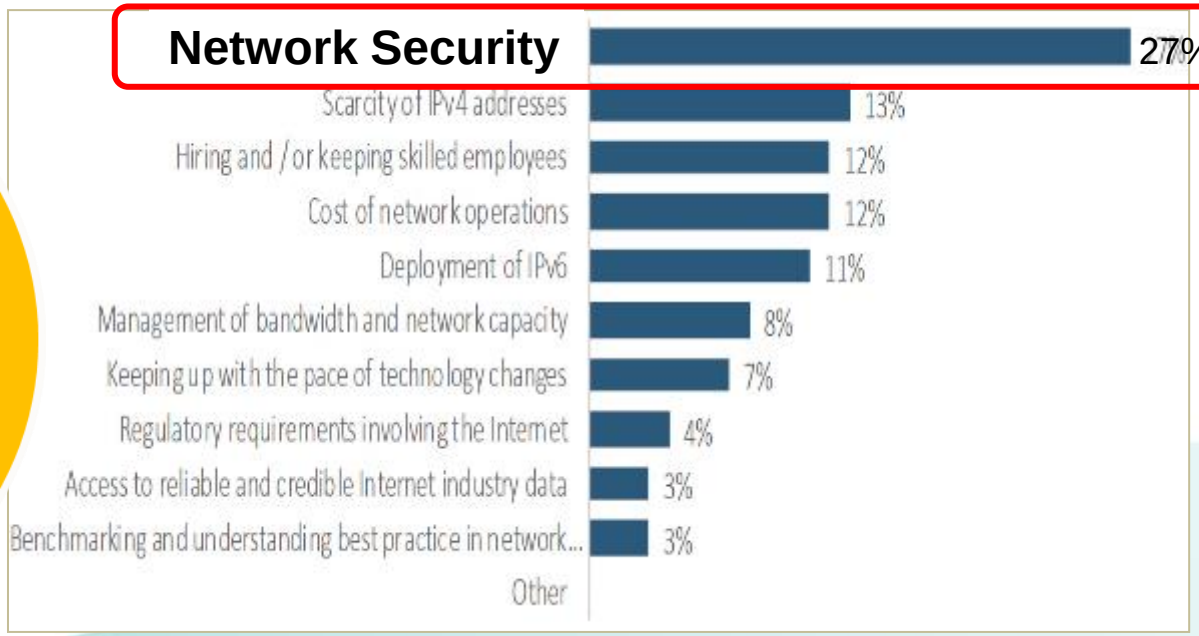
2021.12.17

Outline

- 概述
- 資安威脅與應處
- TWCERT/CC 資安聯盟
- 資安服務說明

資安為數位經濟重要挑戰





- Cost of data breaches due to the Cybercrime
  - $5 Trillion globally in 2024
  - average annual growth of 11%

  [Juniper research, 2019]

- Security is the biggest challenge for internet service provider

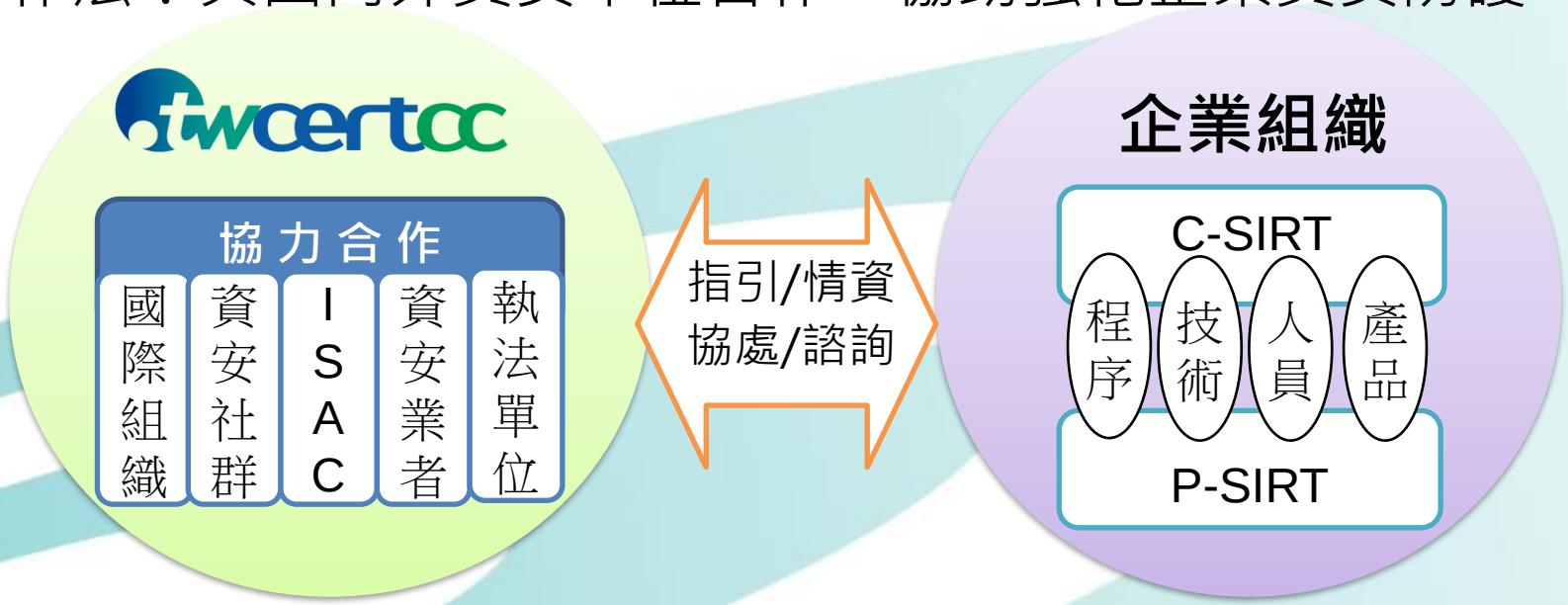
  [APNIC, 2018]

主要資安攻擊面向

Applications & Services		• Phishing • SQL-Injection • XSS • …
Data/Storage		• Ransomware • Data Breach • …
Communication Networks		• DDoS • DNS attack • BGP Hijacking • Man-in-the-Middle ….
Computer Systems/Device		• HeartBleed • Rootkit • Fireless Attack…

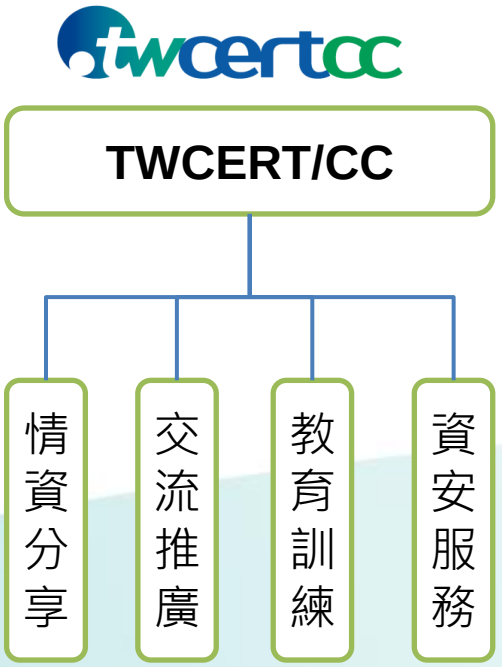
TWCERT資安聯盟定位

- 目的
  - 為強化企業資安聯防，藉由資安聯盟，進行威脅情資共享，促進資安經驗交流與聯防，冀於流程、技術、人員、產品等面向，強化整體數位韌性
- 會員資格
  - CERT/CSIRT組織、資安業者、一般企業、教育學術單位、公協會、法人團體等
- 作法：與國內外資安單位合作，協助強化企業資安防護



TWCERT資安聯盟運作機制

- 以TWCERT/CC聯盟，建立信任管道，促進企業資安聯防
- 積極參與本聯盟會議與活動，並分享近期重大資安事件處置狀況
  - TW-ISAC 平台
  - E-mail與Line 群組
- 會員可獲取 TWCERT/CC之資安情資，參與教育訓練、資安趨勢研討與交流等活動，以**技術、產品、流程、人員**等4大面向，促進資安防護強化



資安服務概要-技術面

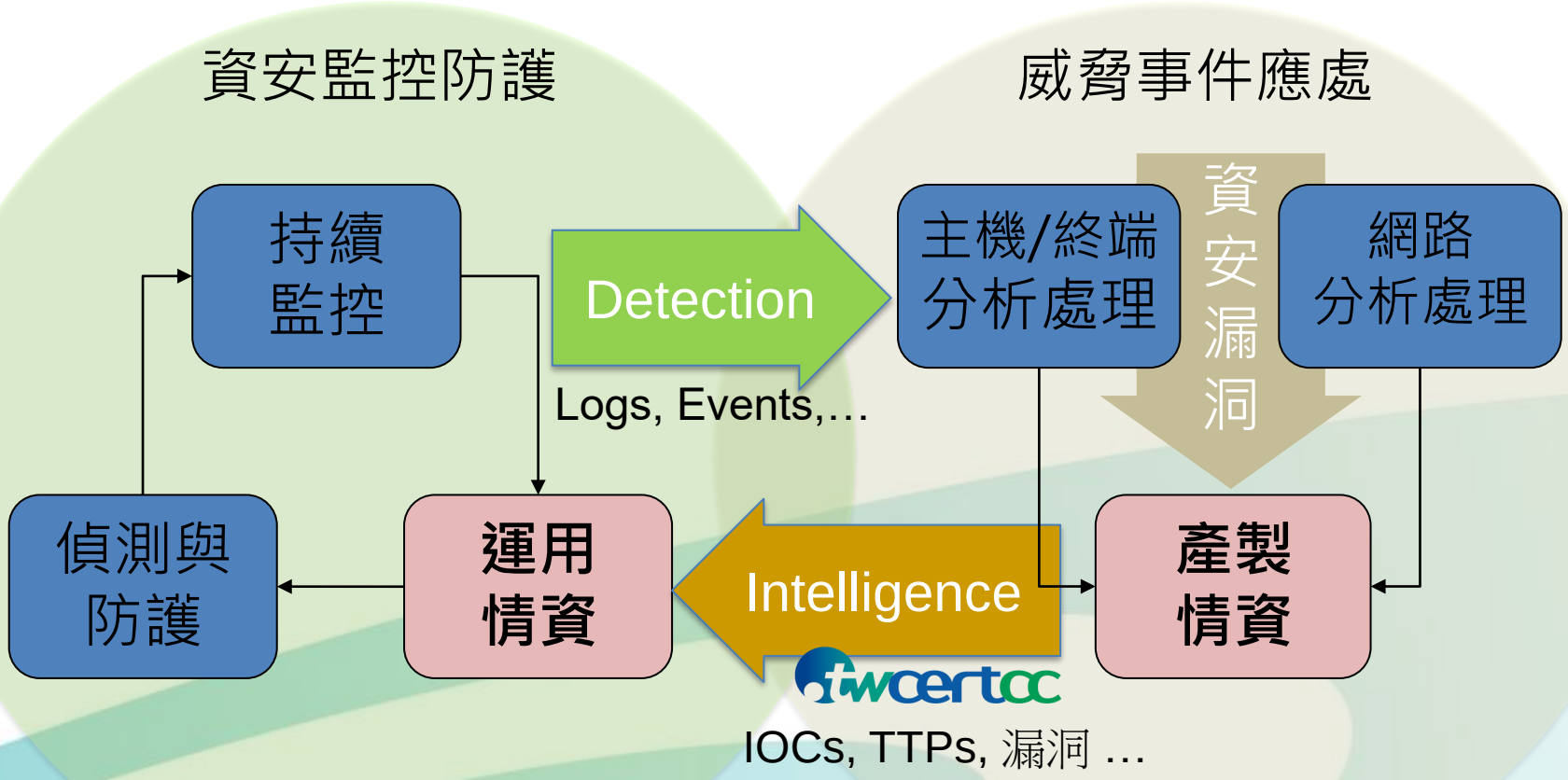
- **資安跨域聯防與情資分享**
  - 資訊去識別化 (Anonymization)
  - 遵守情資交換協定 (Traffic Light Protocol, TLP)，確保妥適運用
- **釣魚網站協處**
  - 跨境協處偽冒企業網站之釣魚網站
  - phishingcheck.tw
- **惡意檔案檢測**
  - 檢測可疑檔案，避免機敏檔案外洩
  - 整合靜態檢測與沙箱(Sandbox)之動態分析機制，檢知潛藏惡意程式
  - viruscheck.tw

TLP 情資交換協定

- RED 限與會者
- AMBER 限參與者組織內
- GREEN 限資安社群間
- WHITE 公開資訊

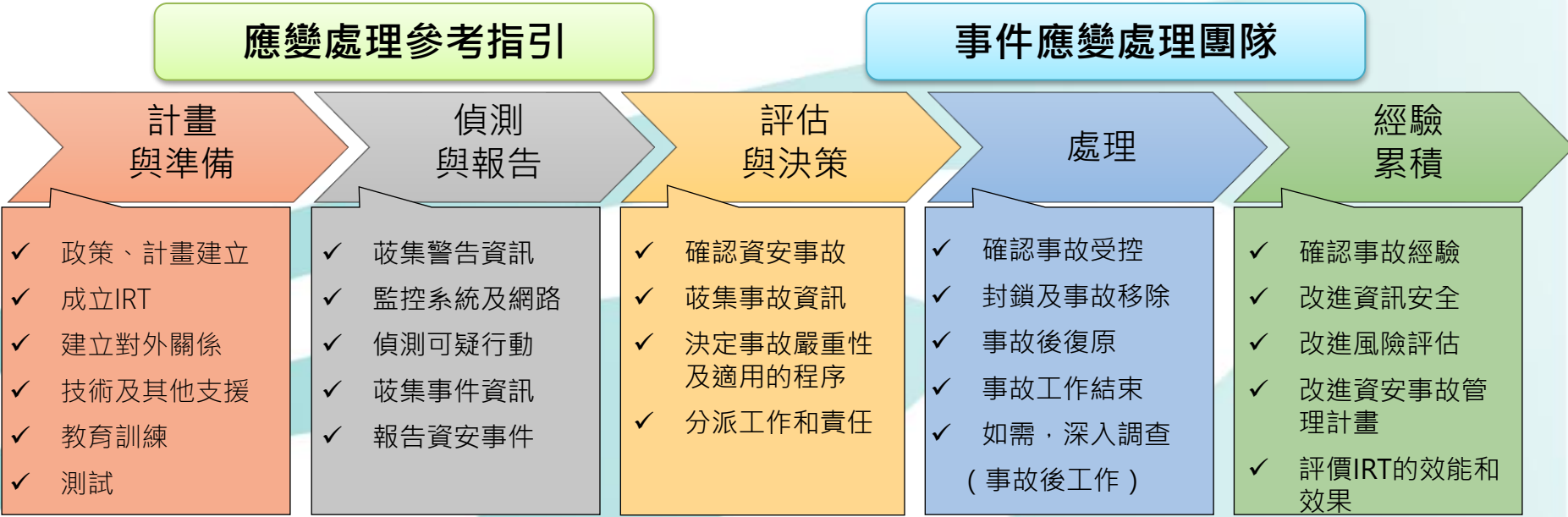
資安跨域聯防與情資分享

資安監控防護 vs. 威脅事件應處

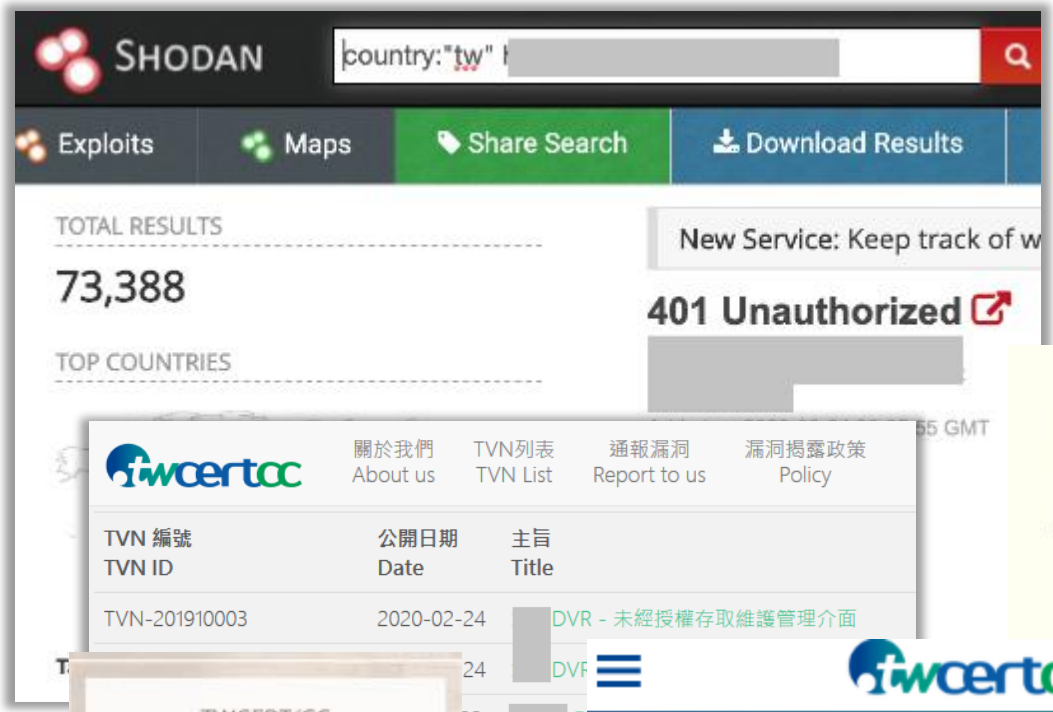


資安服務概要-產品面

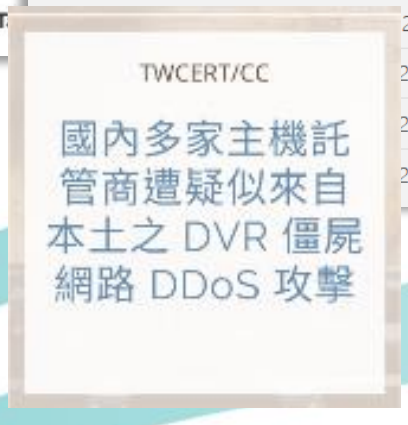
- CVE漏洞協處
  - 協調國內企業修補產品漏洞，以防遭駭客利用
- 供應鏈資安機制
  - 根據產業特性，提供供應鏈資安檢核指南、諮詢、檢核服務
- 產品資安事件應變
  - 推動產品資安事件應變，依據PSIRT精神，協助制定應變指引



產品漏洞遭利用發動資安攻擊



美英資安機關警告，全球約6萬餘台NAS遭感染，[redacted]提醒用戶須回復出廠預設後再作更新



CVE資安漏洞揭露

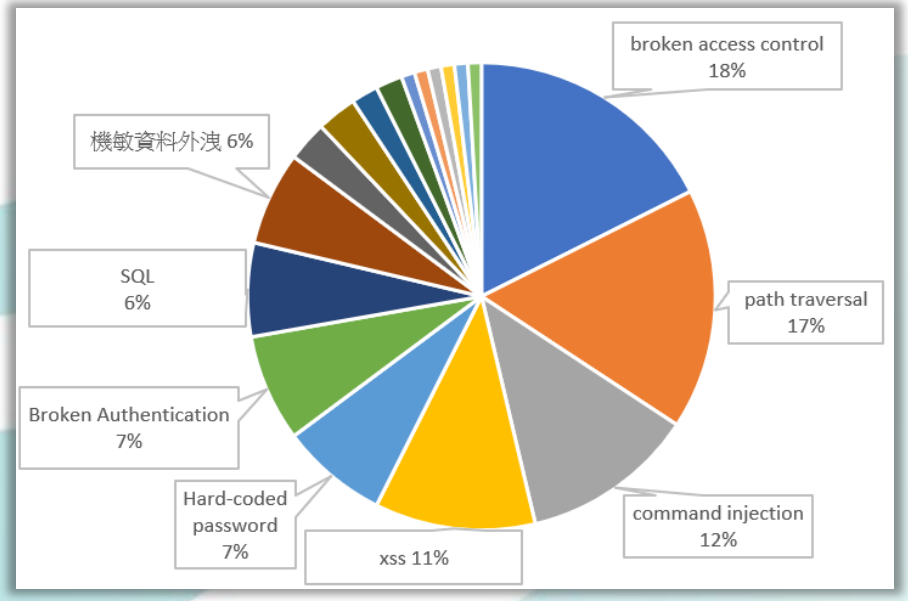
- TWCERT/CC 為MITRE授權之CNA (CVE Numbering Authorities)，針對我國ICT產品漏洞，提供可信賴的通報管道，審核並發布CVE編號，以協助企業掌握修復產品漏洞提升我國產品安全

MITRE

- 全球**198** CNAs (32 國)
- 台灣 **6**個CNAs
  - **TWCERT/CC**
  - Synology
  - QNAP
  - Zyxel
  - MediaTek
  - ASUSTOR
- USA: **107**
- Japan: **7**
- South Korea: **4**
- China: **11**
- Germany: **8**

CVE漏洞處理概況

- TWCERT/CC 已審核並發布超過200個CVE漏洞編號
- 2021年1Q~3Q已審核並發布133個CVE
  - 產品類型：系統平台-46、IOT裝置-52、資訊主機-35
  - 嚴重程度：Critical-38、High-28、Medium-67
  - 威脅類型：Broken access control、Path traversal、Command Injection
- 當新的CVE漏洞發布時，TWCERT/CC同步公告漏洞預警資訊並通知ISAC、企業聯盟等，以預先進行相關防範



2021 TWCERT/CC CVE漏洞類型

漏洞揭露資訊品質獲國際肯定

- 經NIST/NVD 評核，列為品質最佳之Provider等級

NIST NVD

Authority	Category	Acceptance Level
Adobe Systems Incorporated	CWE	Provider
CERT@VDE	CWE	Provider
Dell	CWE	Provider
GitHub, Inc.	CWE	Provider
ICS-CERT	CWE	Provider
Jenkins Project	CWE	Provider
McAfee	CWE	Provider
QNAP Systems, Inc.	CWE	Provider
Red Hat, Inc.	CWE	Provider
SAP SE	CWE	Provider
Schneider Electric SE	CWE	Provider
Siemens AG	CWE	Provider
SUSE	CWE	Provider
Synology Inc.	CWE	Provider
TWCERT/CC	CWE	Provider
Wordfence	CWE	Provider
WPScan	CWE	Provider
Zero Day Initiative	CWE	Provider

- 全球共198 CNA (32 國)
- Provider 等級
  - CWE- 18個組織
  - CVSS v3.1- 8個組織

@2021/11/6

Authority	Category	Acceptance Level
Adobe Systems Incorporated	CVSS v3.1	Provider
GitHub, Inc.	CVSS v3.1	Provider
Juniper Networks, Inc.	CVSS v3.1	Provider
Oracle	CVSS v3.1	Provider
Palo Alto Networks, Inc.	CVSS v3.1	Provider
Qualcomm, Inc.	CVSS v3.1	Provider
TWCERT/CC	CVSS v3.1	Provider
Wordfence	CVSS v3.1	Provider

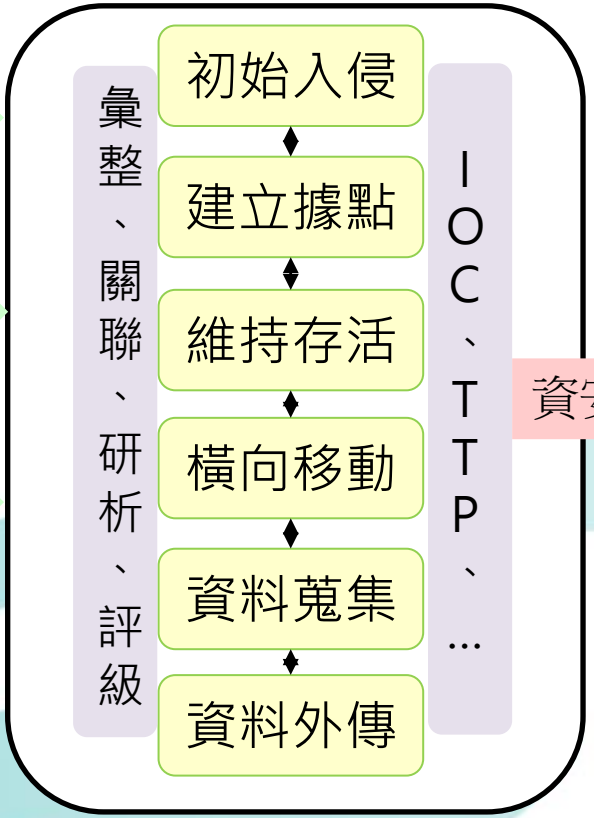
運用情資強化威脅應處

國際威脅情資
(各國CERT, 資安組織)

國內跨域情資
(ISAC, 企業聯盟)

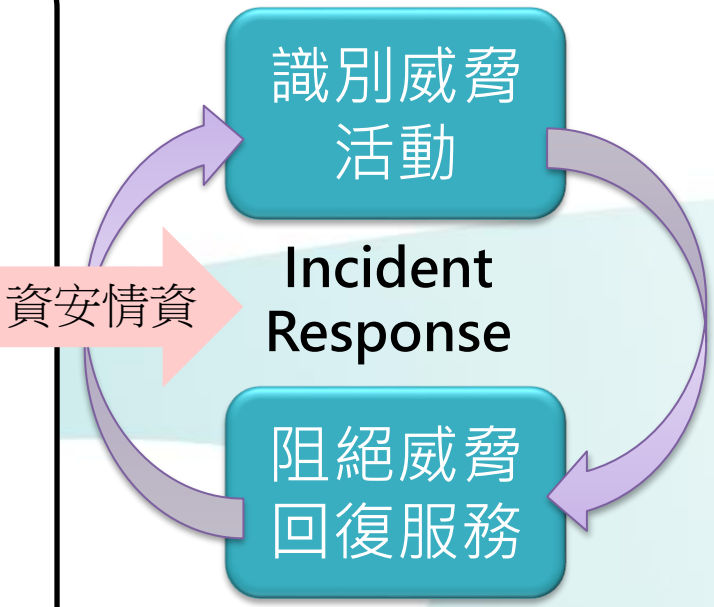
產品漏洞資訊
(CVE, TVN)

資安服務
(Phishing/Virus檢測)



資安情資

民間單位



資安服務概要-流程面

- 依我國產業特性，提供企業資安參考指南
  - 研析資安文獻：國際標準 (ISO、NIST)、國際資安組織 (FIRST、APCERT、ENISA)、國內資安單位
  - 藉由國內高科技產業與資安專家座談，匯集多方建議，建立參考指南
- 參考指南類別
  - 資安事件處理類
    - 勒索軟體、後門程式處理
  - 企業安全防護類
    - 企業網路防護、IOT/OT 安全防護
  - 資安應變小組類
    - CSIRT : 基本應變、事件協處準備
    - PSIRT : 針對產品/服務的漏洞風險，提供處置建議

勒索軟體防護專區

- 協助企業組織對抗勒索軟體威脅，提供事前預防、事中處理與事後回復之指南與檢核表
- 網址：https://antiransom.tw

使用者可從勒索軟體防護專區尋找各式指南與多樣資源

事前預防	勒索軟體預防指南
	勒索軟體預防檢核表
	勒索軟體防護成熟度自評說明 (CISA CSET RRA)
事中處理	勒索軟體處理指南
	勒索軟體處理檢核表
	勒索軟體辨識與解密工具 (ID Ransomware、No More Ransom)
	臺灣資安服務廠商清單 (經濟部工業局ACW資安產業自主能量)
事後回復	勒索軟體事後回復指南
	勒索軟體事後回復檢核表
	勒索軟體防護成熟度自評說明 (CISA CSET RRA)

資料來源：antiransom.tw，iThome整理，2021年10月

iThome

幫助國內企業組織對抗勒索軟體，臺資安通報機
防護專區，可協助事前、事中與事後因應

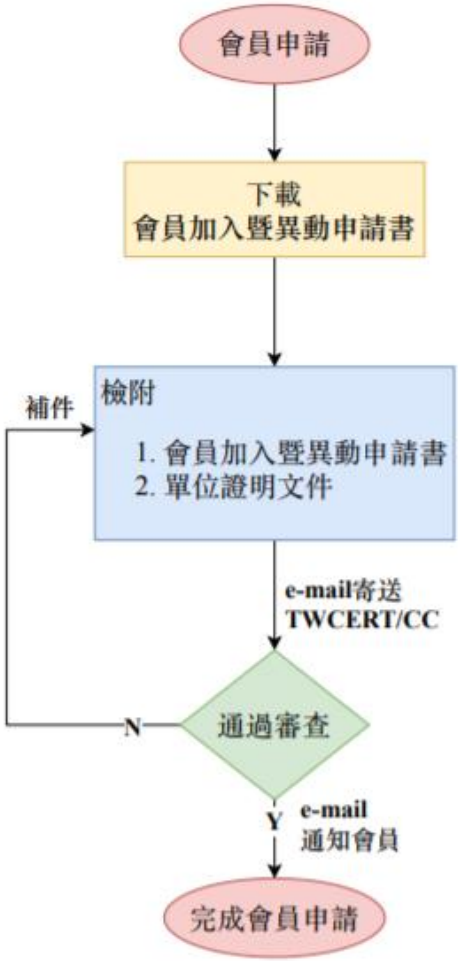
不少企業對於勒索軟體攻擊等資安事件的處理，已做好應變與復原計畫的準備，然而，還是有許多企業無任何規畫，在10月初TWCERT/CC推出勒索軟體防護專區的獨立入口網站，希望讓普遍大大小小企業至少都能有基本的著手方向，並結合No More Ransom平臺與CISA CSET的RRA防勒索軟體成熟度自評工具的資源說明。

資安服務概要-人員面

- 藉由教育訓練、資安分享會議/論壇等，提升人員資安意識，強化資安威脅防護，減緩資安事件衝擊，並透過交流活動促進成員合作

- 舉辦資安教育訓練
  - ✓ 威脅防護課程 (社交工程，人員防護，勒索軟體)
  - ✓ 資安實務研討
- 資安經驗分享
  - ✓ 國內外資安新聞
  - ✓ 資安趨勢與駭侵事件
  - ✓ 資安經驗分享
- 成員交流活動
  - ✓ 聯盟成員交流
  - ✓ 合作議題討論
  - ✓ 建立聯繫管道

TWCERT 資安聯盟入會說明



「台灣 CERT/CSIRT 聯盟」會員申請暨異動申請書

申請日期：民國＿＿＿年＿＿＿月＿＿＿日

會員基本資料			
機關/單位統編		證券代號	□上市 □上櫃
機關/單位名稱*			
會員新申請或異動申請(異動時請填寫有異動的欄位)			
□新申請或□異動資料			
機關/單位負責人*			
聯絡人資料*	姓名/職稱		
	Email		
	電話	(　　)	#
對外IP/網段資料* (如:1.11.22.121、1.11.222.128/25 僅適用於資安情資通報)	□新增 □刪除		
會員終止申請			
□本機關/單位提出終止申請，原因：			
會員同意暨簽名或用印			
□*已閱讀、瞭解並同意本申請書所註明之注意事項，及台灣 CERT/CSIRT 聯盟會員規章，詳見 TWCERT/CC 網站(twcert.org.tw)。			
機關/單位部門主管簽名 或 機關/單位用印*		申請人簽名*	
(申請或異動時，請附上工商/變更登記證或相關文件)		(請申請人親簽)	

官網/社群/電子郵件多元服務管道

PGP KEY
TWCERT/CC PGP Public Key
Key ID : 0x1E9D1F1B

官　網：	www.twcert.org.tw
社群媒體：	www.facebook.com/twcertcc/
電子信箱：	twcert@cert.org.tw


Thank You!