



TWCERT/CC 公私協力防護策略

國家資通安全研究院

通報應變中心 孫偉哲主任



台灣電腦網路危機處理暨協調中心(<https://www.twcert.org.tw/>)

主責國內民間企業資安防護，國際交流共享情資



The screenshot displays the TWCERT/CC website interface. At the top, the TWCERT/CC logo is on the left, and navigation links for '遠距辦公資安專區', '回首頁', '網站導覽', '訂閱電子報', and 'English' are on the right. Below the logo, a horizontal menu includes '新聞公告 News', '資安服務 Services', '資安宣導 Advocacy', '相關網站 Links', and '關於我們 About us', followed by a search icon. The main header reads 'Taiwan Computer Emergency Response Team / Coordination Center'. The central banner features the title '台灣電腦網路危機處理暨協調中心' and four service icons: '國際資安事件聯防 International Collaborative Cyber Defense', '跨國資安情報交流 Cross-National Cyber Intelligence Exchange', '企業資安通報轉介 Entrepreneurial Cybersecurity Incident Referral', and '情資收集資安宣導 Cyber Intelligence Collection and Cybersecurity Outreaches'. At the bottom of the banner are buttons for '申請加入聯盟', 'PGP公開金鑰', and '連絡我們'. On the right side, a large circular graphic titled '簡易資安事件通報' contains a form with fields for '通報者或通報單位 Consultant', '電子信箱 E-mail', and '事件狀況描述 Description'. Below this form are two buttons: '我要通報' and '延遲通報'.

Taiwan Computer Emergency Response Team / Coordination Center

台灣電腦網路危機處理暨協調中心

-  國際資安事件聯防
International Collaborative Cyber Defense
-  跨國資安情報交流
Cross-National Cyber Intelligence Exchange
-  企業資安通報轉介
Entrepreneurial Cybersecurity Incident Referral
-  情資收集資安宣導
Cyber Intelligence Collection and Cybersecurity Outreaches

申請加入聯盟 PGP公開金鑰 連絡我們

簡易資安事件通報

通報者或通報單位 Consultant

電子信箱 E-mail

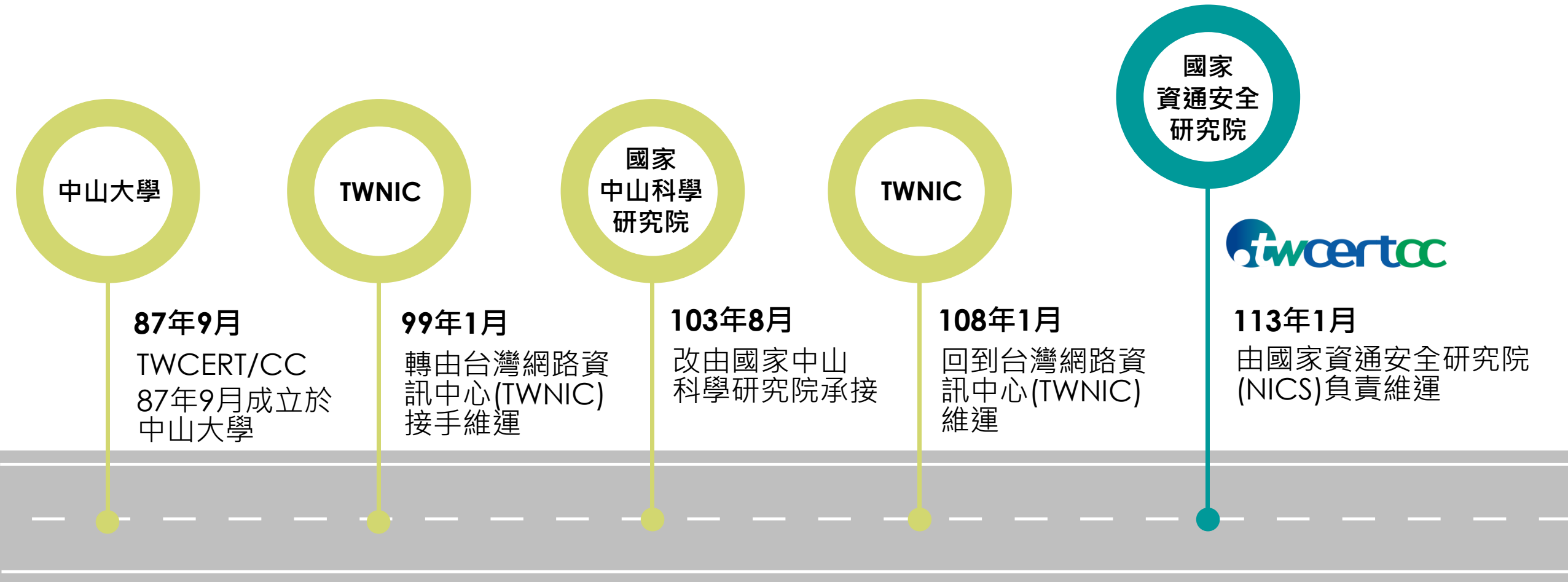
事件狀況描述 Description

我要通報

延遲通報

TWCERT/CC歷史沿革

台灣電腦網路危機處理暨協調中心(TWCERT/CC)



TWCERT/CC 服務總覽



情資分享

- ① 建立多元情資分享管道，促進跨域資安合作
- ② 彙整國內資安組織情資，持續分享交流



應變協調

- ① 協調資安事件處理團隊，協助資安事件應變處理
- ② 漏洞通報及CVE審查發放
- ③ 惡意檔案檢測服務



國際合作

- ① 參與國際資安組織活動
- ② 建立國內外溝通管道
- ③ 掌握資安威脅趨勢



意識提升

- ① 推動台灣CERT/CSIRT聯盟，強化資安聯防體系
- ② 透過社群媒體與宣導活動，提升民間資安意識

重點推動策略(1/2)

● 推動策略：主動偵蒐、主動掃描、主動察覺

- 結合長期公務機關資安防護經驗，**偵測蒐集**民間企業APT攻擊事件，掌握受駭目標，與警調單位合作，協助其事件處理並提供強化建議，強化公私協力鏈結



- 針對對外服務具**重大影響弱點**(CVE)，透過官網、TWISAC、N-ISAC週知民間企業，同時協助TWISAC會員進行掃描，主動通知未修補會員進行修補

重點推動策略(2/2)

● 推動策略：強化公私領域駭侵情資交流與通透性

- 重大緊急事件**預警**、自研**情蒐**、常用**弱點**、參考**指引**等資訊，結合N-ISAC、TWCERT官網、TWISAC會員、社群平台推播等管道即時提供會員參考，提升情資通透性與應處時效性，提升民間企業資安防護意識
- 鼓勵企業回饋自身事件應處後**駭侵情資**與**惡意程式**樣本，配合VirusCheck服務，協助樣本分析與情勢研判，助於其他公私領域防護有效性



重大事件
自研情蒐
弱點公告
參考指引



領域機關
民間單位
企業會員

● TWISAC會員資安情資

—綜整公私領域所獲與自研情資，加強提供會員之情資有效性

漏洞情資



- 針對CVE分數達8.8之資安漏洞發布情資，提醒企業組織儘速完成更新
- 每週蒐整KEV公告遭利用之漏洞，標示是否為勒索軟體利用之安全漏洞
- 外部情資通報企業設備存在之安全性漏洞

IoC情資



彙整各情資單位提供IoC情資，不定期提供會員參用，類型包含APT、BOT、Mining、Ransome等

攻擊活動預警



研析外部通報我國企業攻擊事件情資，發現共通性攻擊活動，發布攻擊活動預警，協助企業提早防範駭客攻擊活動

攻擊事件通報

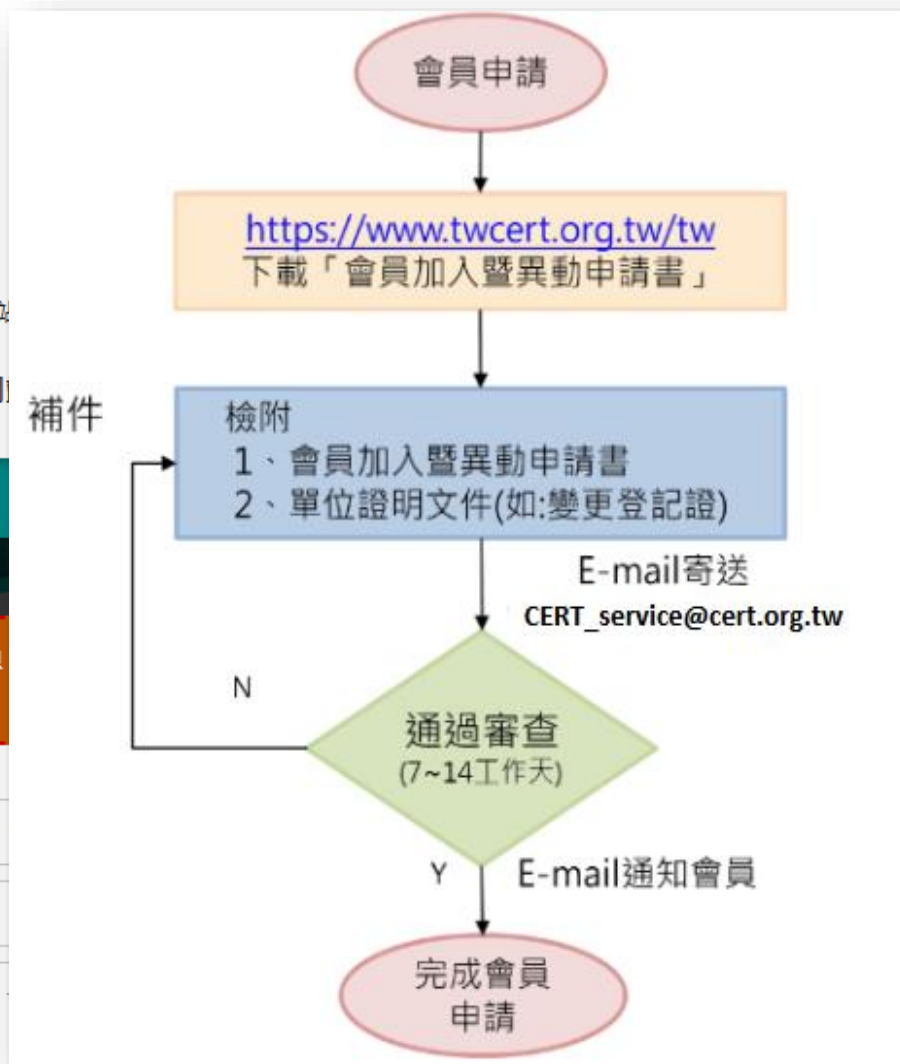


接獲外部情資/偵測發現攻擊事件情資，將攻擊事件相關資訊提供受駭企業進行應處，以降低事件影響

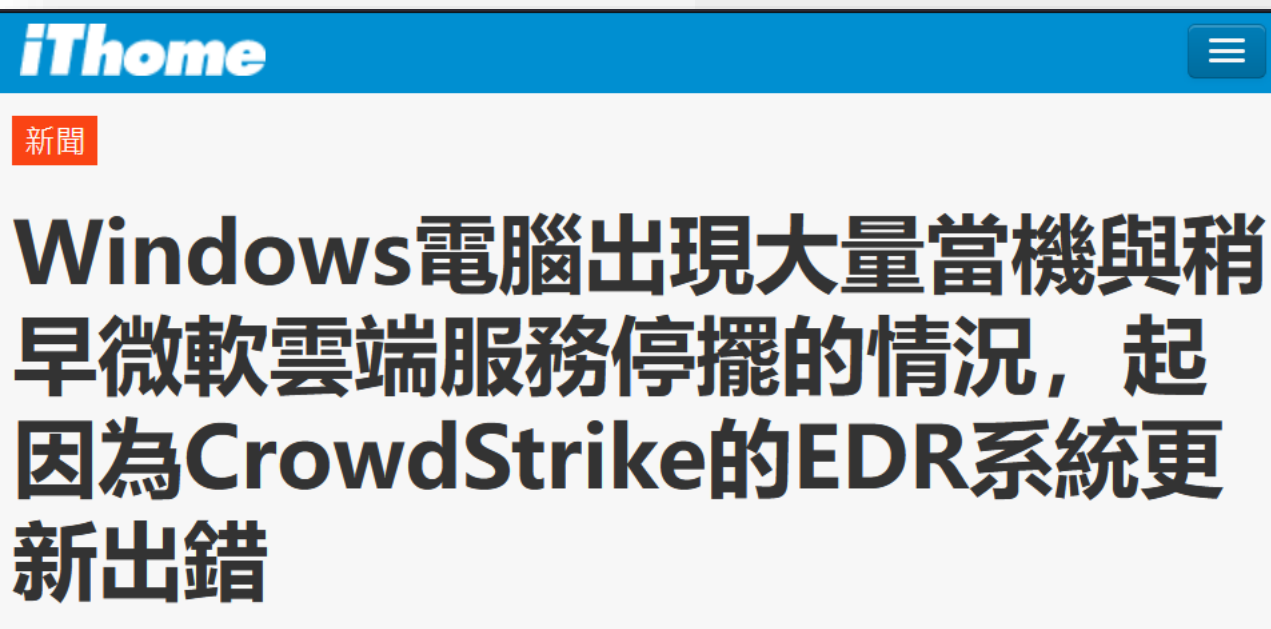
聯盟會員申請方式

● TWISAC會員加入方式

- 官網/資安服務/資安聯盟規章與會員申請
- 檢附「變更登記證」或其他企業非陸資證明



- 針對近期CrowdStrike事件，TWCERT/CC亦收集官方緩解措施並提醒企業會員與民眾參考，以協助受影響使用者應處



1年7月19日資安公司CrowdStrike的Falcon Sensor更新程式出現故障，導致全球各地Windows電腦出現藍色畫面當機(BSOD)狀況，全球企業包括航空公司、醫院、運輸機構及媒體公司等，許多Falcon Sensor市佔率為前幾名，因此這次更新問題導致大量Windows電腦多機構的運營

結論

- TWCERT/CC透過公私協力協助民間企業強化資安防護，鼓勵企業踴躍加入TWCERT/CC會員共同聯防
- 現階段在缺乏相關法源下，以宣導推廣方式鼓勵企業進行自身事件通報並提供相關情資，以利聯防助益
- 持續辦理資安推廣訓練活動，以提升民間企業資安防護意識



報告完畢 敬請指教



twcertcc

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