

110 年度臺灣學術網路危機處理中心資安研討會

一、計畫目的

臺灣學術網路危機處理中心(Taiwan Academic Network Computer Emergency Response Team, 簡稱 TACERT)為加強臺灣學術網路(TANet)網站安全防護能力，辦理「110 年度臺灣學術網路危機處理中心資安研討會」，本次研討會重點在於加強各校資安人員的資安防護能力。

二、辦理單位

- 指導單位：教育部
- 主辦單位：臺灣學術網路危機處理中心(TACERT)
協辦單位：北區教育學術資訊安全監控中心(N-ASOC)
南區教育學術資訊安全監控中心(S-ASOC)
AISAC 暨 miniSOC 計畫團隊(逢甲大學)
教育單位網站資安防護服務計畫(國立成功大學)
- 參與對象：臺灣學術網路區域網路中心、各縣市教育網路中心、公私立大專院校、公私立高中職網路管理或資安相關負責人員

三、課程資訊

因應本土疫情關係，本年度研討會改以視訊直播方式，請參與者先以網路報名方式自行選擇參加梯次，待會議前三天本單位會寄研討會視訊直播連結至報名者的電子郵件信箱。

1. 8 月 20 日個資防護暨資通安全健診作業方式簡介

「資安事件通報應變作業與個資防護」課程，講解學術網路資安現況及分析未來資安趨勢，期使學員了解目前資安攻擊手法；此外，宣導資安觀念與本年度資安施行規畫，同時對於如何強化個人資料安全，提出防護建議。

此外，依據資通安全管理法於技術面的要求，各機關需依照資通安全責任等級分級辦法定期對管轄之系統進行資通安全健診作業。此議程會介紹實務作業上的檢測方式，及說明常見的高風險檢測結果，並提供些許簡易的惡意程式檢測方式，以協助系統管理者能強化系統防護。

時間	議題	講師
9:10~9:30	連線測試	
9:30~10:30	資安事件通報應變作業與個資防護	TACERT-郭家瑋
10:30~10:40	中場休息	
10:40~12:00	網路架構檢視介紹	中華資安-李尚倫

12:00~13:00	中午休息時間	
13:00~14:00	網路惡意活動檢視介紹	中華資安-李尚倫
14:00~14:10	中場休息	
14:10~15:10	主機惡意程式檢視介紹	中華資安-曾昭銘
15:10~15:20	中場休息	
15:20~16:10	防火牆連線設定檢視介紹	中華資安-李尚倫
16:10~16:30	Q&A 及會後測驗	TACERT

2. 8月27日開源碼主從式稽核記錄系統建置

身為管理者，最頭痛的事情，應該就是要從多如牛毛的稽核記錄中分析出有意義的資訊，通常原生的稽核記錄均是以檔案型態儲存，並不容易從中解析有意義之事件，因此本課程將說明如何將稽核記錄導入資料庫，以資料庫的方式及主機型入侵偵測系統，來幫助使用者能快速的從稽核記錄找出異常行為

此課程重點在教授開放原始碼資安軟體。建議參與此課程之學員需對Linux作業系統有基礎認識。

時間	議題	講師
9:10~9:30	連線測試	
9:30~10:40	主機稽核 LOG 簡介	TACERT-吳惠麟
10:40~10:50	中場休息	
10:50~12:00	主從式稽核系統建置	TACERT-吳惠麟
12:00~13:00	中午休息時間	
13:00~14:00	主機型入侵偵測系統建置	TACERT-吳惠麟
14:00~14:10	中場休息	
14:10~15:10	主機型入侵偵測系統建置	TACERT-吳惠麟
15:10~15:20	中場休息	
15:20~16:10	主機型入侵偵測系統建置	TACERT-吳惠麟
16:10~16:30	Q&A 及會後測驗	TACERT-吳惠麟

四、報名方式

- (一)、報名網址 <https://tacert.mis.nsysu.edu.tw>，本研討會為免費參加，採視訊直播方式進行，請參與者先以網路報名方式自行選擇參加梯次，待會議前三天本單位會寄研討會視訊直播連結至報名者的電子郵件信箱。
- (二)、參與者參加視訊會議時，請將登入名稱改為「單位名稱-姓名」，並於視訊會議結束後，需完成會議問卷以及線上測驗，才可取得相關研習時數或研習證明電子檔。
- (三)、聯絡電話：(07)525-0211；E-mail：training@cert.tanet.edu.tw。