106年第二次區域網路連線單位管理會

報告人：臺東區網中心

慈中和

會議程序

- 一、主席致詞
- 二、上次會議事項追蹤
- 三、工作報告(含經驗分享)
- 四、討論提案
- 五、指導與建議
- 六、散會

二、上次會議事項追蹤

- 臺東高中提案：
- 各學院、專科學校及高級中等以下學校原預設為C級單位，但當年辦理專科學校及十二年國教入學考試、甄選、招生等工作之學校，其資安責任等級將升為B級，由於B級單位規定要求必須有具證照之專責資安人員，而臺東地區僅2所高中輪流主辦會考、5所職校輪流主辦免試入學，此狀況下若要符合規定，等同上述學校皆須維持B級單位標準，此狀況希望若有機會區網中心能向教育部反映。

問題回復：已轉達教育部承辦人員

- 原C級自動升級B級單位：「辦理專科學校、十二年國教入學考試、甄選、招生工作等輪流辦理之試務機構與學校。」
- B級單位資安需求較高，例如需要維持證照有效性。
- 有關臺東高中職學校少，如12年國教入學考試，現行做法為東中東女輪流辦理，故每隔一年輪流變B級。
- **目前區網提供的解決方案：臺東區網有編列外部教育訓練費用，故可派送該年度承接資訊工作老師受訓及取得證照。**

三、工作報告

(一)教育部新版弱點掃描服務系統說明

- 網站弱掃申請
- 申請限制
  1. 因弱掃主機資源有限，需限制檢測數量(未來視情況調整)
     - 區網中心、縣市網中心：5個
     - 轄下單位：2個
  2. 排程日期
     - 可供排程的時段:
       - 每日開放3天後~30天內的日期
       - 週一~五，每日有2種時段：
         - 晚間時段(17~24點) ：3個檢測上限
         - 凌晨時段(0~8點)：5個檢測上限

檢測目標：

- 單網站：可選擇排程日期
- 多網站：由系統自動排程

- 排程日期僅為排程參考依據，實際掃描時間需視掃描狀況而定

單站申請


EVS
首頁
網站弱點檢測
系統資訊
Hello 30
登出
檢測申請
縣市
金門縣
單位分類
國小
關鍵字
柏村,中正
查詢
清除
最多可檢測數: 5 待檢測數: 0 可申請數: 5
請選擇欲申請掃描的網站
排程日期
2017-11-07 凌晨時段(0~8點)
網站
縣立中正國小 714603
http://www.jjes.km.edu.tw
[金門縣立中正國小]
縣立柏村國小 714607
http://www.btps.km.edu.tw
[金門縣立柏村國小]
您已了解並遵守: 網站資安弱點掃描同意書
申請

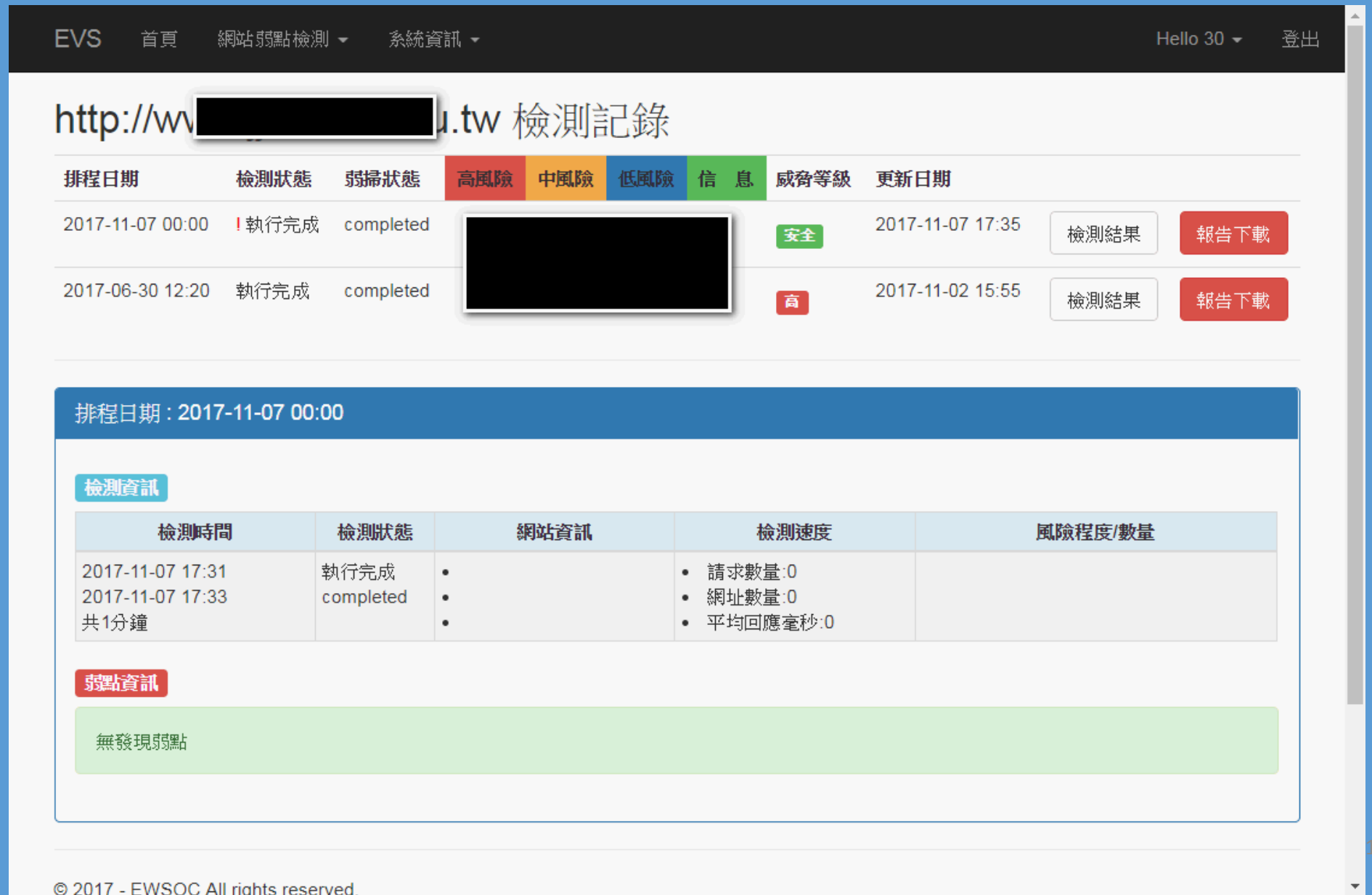
多站申請


EVS
首頁
網站弱點檢測
系統資訊
Hello 30
登出
檢測申請
縣市
金門縣
單位分類
國小
關鍵字
柏村,中正
查詢
清除
最多可檢測數: 5 待檢測數: 0 可申請數: 5
請選擇欲申請掃描的網站
排程日期
多選網站由系統決定掃描時間
網站
縣立中正國小 714603
http://www.jjes.km.edu.tw
[金門縣立中正國小]
縣立柏村國小 714607
http://www.btps.km.edu.tw
[金門縣立柏村國小]
您已了解並遵守: 網站資安弱點掃描同意書
申請

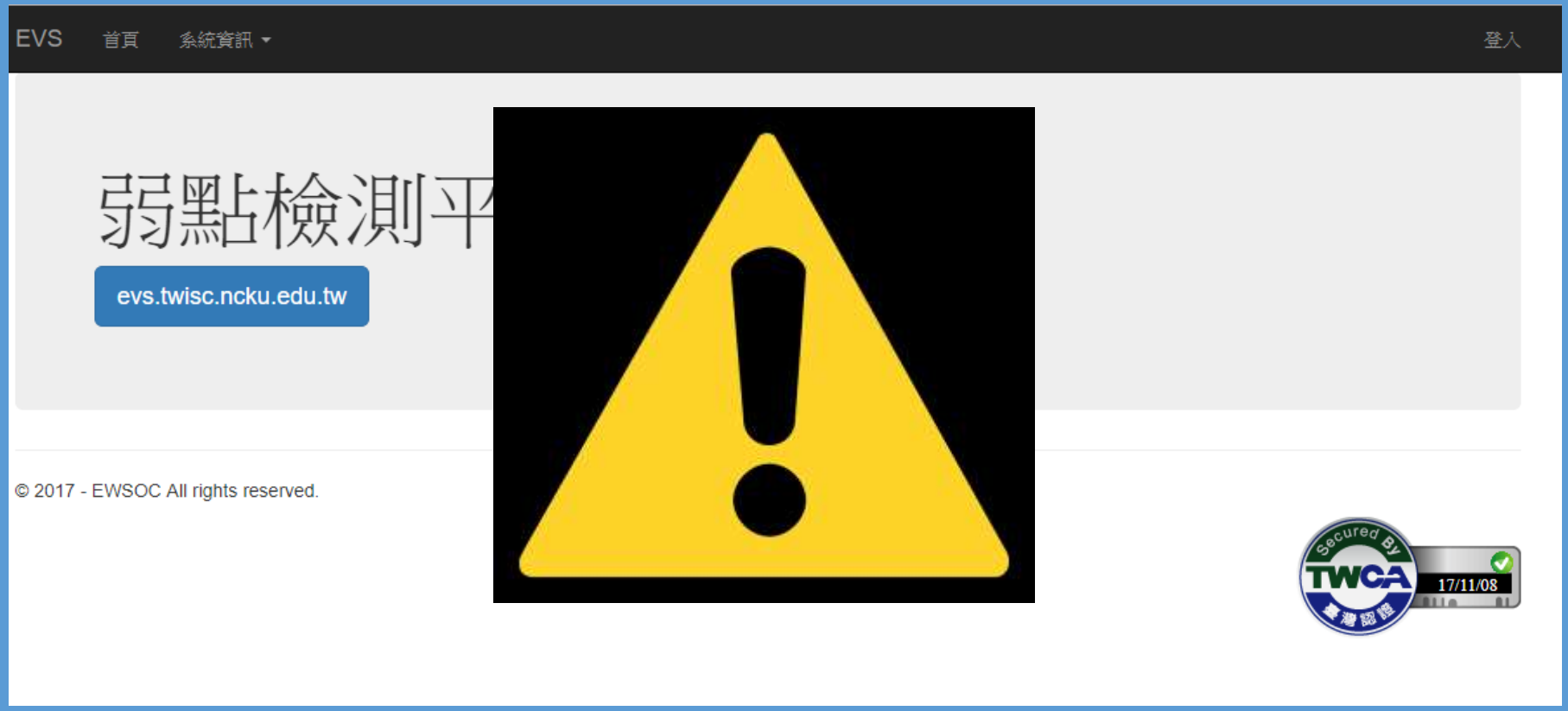
查看、下載檢測結果


EVS
首頁
網站弱點檢測
系統資訊
Hello 30
登出
檢測目標
新增
匯入
匯入範本
單位
縣立中正國小
過濾欄位
主機網域
關鍵字
過濾欄位關鍵字
查詢
清除
← 1 →
| 第 1 頁 / 共 1 頁 | 顯示第 1 - 1 項資料 / 共 1 項
主機網域 | 用途
重要程度
建立時間 ▼
最新檢測時間
最新檢測狀態
http://www.jjes.km.edu.tw
金門縣立中正國小
普通
2017-06-30 12:16
2017-11-07 00:00
! 執行完成
修改
檢測記錄
© 2017 - EWSOC All rights reserved.

查看、下載檢測結果


EVS
首頁
網站弱點檢測
系統資訊
Hello 30
登出
http://ww[redacted].tw 檢測記錄
排程日期
檢測狀態
弱掃狀態
高風險
中風險
低風險
信 息
威脅等級
更新日期
2017-11-07 00:00
執行完成
completed
安全
2017-11-07 17:35
檢測結果
報告下載
2017-06-30 12:20
執行完成
completed
高
2017-11-02 15:55
檢測結果
報告下載
排程日期 : 2017-11-07 00:00
檢測資訊
檢測時間
檢測狀態
網站資訊
檢測速度
風險程度/數量
2017-11-07 17:31
2017-11-07 17:33
共1分鐘
執行完成
completed
請求數量:0
網址數量:0
平均回應毫秒:0
弱點資訊
無發現弱點
© 2017 - EWSOC All rights reserved

新平台使用注意事項


EVS
首頁
系統資訊
登入
弱點檢測平
evs.twisc.ncku.edu.tw
© 2017 - EWSOC All rights reserved.
17/11/08

新平台使用注意事項提醒

- IP白名單：

  由於新平台掃描時會對受測網站進行大量連線請求(Request)，資安設備可能誤判為攻擊，而將平台掃描IP封鎖。

  請各位夥伴協助將以下四個檢測IP列入資安防護設備之白名單

  140.116.221.36、140.116.221.37、140.116.221.38、140.116.221.39

  以利日後弱點掃描作業

新平台使用注意事項提醒

- 各位夥伴拿到的網站平台帳號密碼(包含轄下單位)，需要謹慎保管，避免讓其他非相關人員得知帳號密碼，造成敏感資料外洩。
- 使用新平台同時，各位夥伴可以對教育訓練的相關課程多加了解，提升人員的資安素養

（二）區網近期研習課程內容預計安排如下：

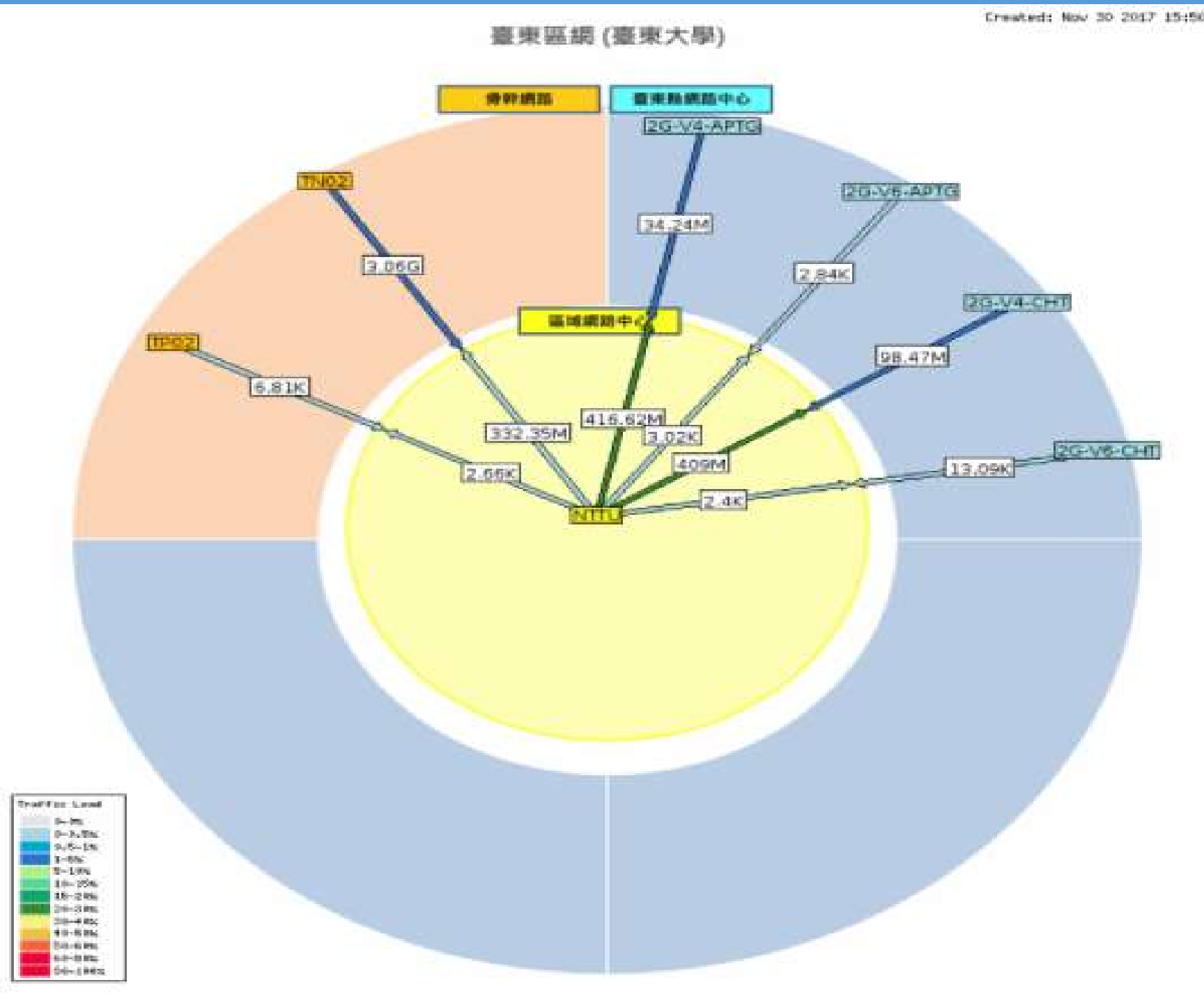
- 12/12-3HR-資訊安全技術
- 12/16-6HR-Proxmox VE開源虛擬化平台實戰
- 12/26-3HR-虛擬化技術實務
- 後續請連線單位提供來年課程興革與建議

(三)協助連線單位IPv6提升改善建議

來年協助學校進行IPv6 設定過程：

- 鑒於部分單位並未專責網管、資訊相關背景人員執行升級作業。
- 部分單位連線設備老舊(防火牆、路由器均使用5年以上)，且無合約委商執行相關調校作業。
- 請連線單位依升級計畫提出需求評估後續提升作業。

流量分布圖
臺東區域網路中心即時



IPv6升級作業調查現況

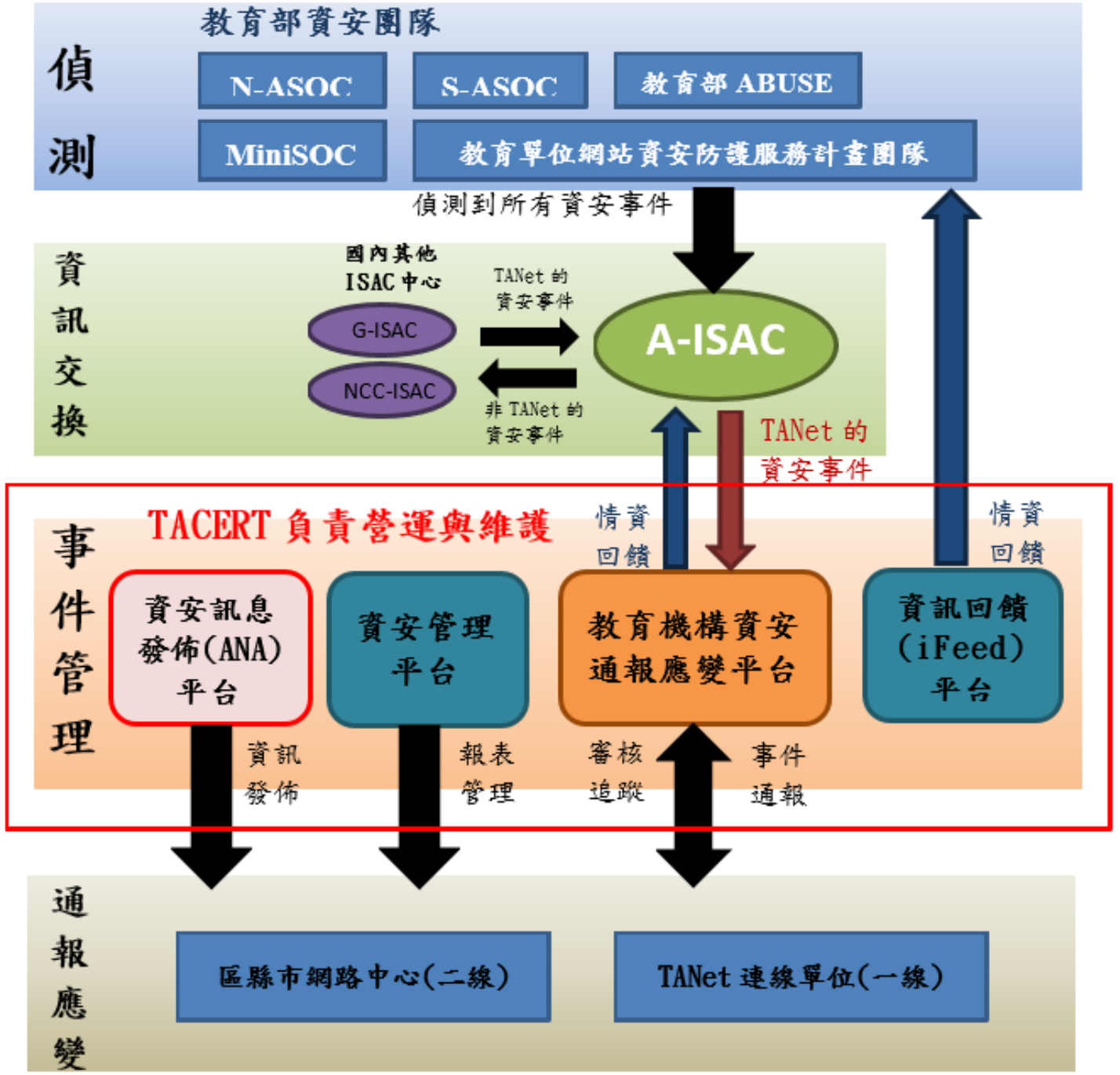
連線單位	分配網段	狀態		分配網段	狀態
臺東大學	2001:288:9001::/48	已設定	成功商水	2001:288:9008::/48	
臺東專科	2001:288:9002::/48	已設定	育仁中學	2001:288:9009::/48	
臺東高中	2001:288:9003::/48		東大附中	2001:288:900A::/48	已設定*
臺東女中	2001:288:9004::/48		史前館	2001:288:900B::/48	
臺東商校	2001:288:9005::/48	已設定	東大附小	2001:288:900E::/48	
公東高工	2001:288:9006::/48	已設定*			
關山工商	2001:288:9007::/48	已設定*			
特教學校	2001:288:900F::/48	已設定*			

*資料時間：**106年11月30日**

(四)近期資安事件處理經驗

1. 資安事件處理與回報
2. 學術網路DDoS清洗機制

教育機構資安通報運作機制



1. 資安事件處理與回報

- 為確保資安事件能夠即時通知與處理，故煩請各連線單位於資安連絡人發生異動時，務必確保資安事件的處理業務能妥善完成交接
- 資安連絡人員至少需有二位，以建立代理人制度

1. 資安事件處理與回報

- 建議將主要負責人員填寫於**第一、二連絡人**
- 教育機構資安通報平台的**帳號密碼**進行交接
- 登入教育機構資安通報平台於「修改個人資料」進行連絡人資訊更新
- 新接任資安連絡人可至中心網站的資安文件下載資安通報應變手冊，了解通報平台基本操作。
- TACERT中心網站資安文件網址：http://cert.tanet.edu.tw/prog/Document-1.php

現行單位資安連絡人現況

OID查詢 | 威脅名單 | 事件單列表 | EWA列表 | 事件類型統計 | 轄下單位密碼更動情況 | DDOS清洗系統

單位名稱	第一連絡人	第二連絡人	第三連絡人	第四連絡人	第五連絡人
國立臺灣史前文化博物館	2017-09-11 16:46:09	2017-09-15 11:10:58			
台東區網中心	2017-09-19 09:18:55	2016-09-05 09:24:06	2017-09-19 10:07:32		2017-09-19 10:05:15
國立臺東高級中學	2017-09-01 14:40:07	2017-09-01 14:51:27	2017-09-01 14:55:34		
國立臺東女子高級中學	2017-09-14 15:46:04	2017-09-14 15:46:57			
國立臺東高級商業職業學校	2016-09-12 14:46:30	2017-09-15 09:51:48			
國立關山高級工商職業學校	2017-09-14 11:51:50	2017-09-14 11:49:58			
國立成功商業水產職業學校	2017-08-29 18:38:10	2017-08-29 18:40:09			
國立臺東大學	2017-09-14 14:58:30	2017-09-18 14:48:39	2017-09-15 10:54:37	2017-09-15 10:56:22	2017-09-04 15:49:38
國立臺東大學附設實驗國民小學	2017-08-23 09:57:43	2016-09-10 16:46:29	2013-09-25 10:03:59		
國立臺東大學附屬體育高級中學	2017-09-05 17:10:28	2017-09-07 13:54:38	2017-09-07 13:57:21		
國立臺東大學附屬特殊教育學校	2017-09-12 08:38:00	2017-09-18 09:48:28			
國立臺東專科學校	2017-09-12 08:54:57	2017-09-12 08:58:05	2016-09-13 17:03:40	2016-09-13 16:36:30	
臺東縣私立育仁高級中學	2016-09-12 15:18:05	2016-09-12 15:19:21			
天主教臺東縣私立公東高級工業職業學校	2017-09-15 15:43:44	2016-09-12 11:31:29			
臺東區域網路中心	2017-09-14 15:05:35	2017-09-18 14:46:26	2017-09-14 15:17:01	2017-09-14 15:19:18	2017-09-04 15:42:24

Page 1/1

1. 資安事件處理與回報

- 為使通報應變流程更有效掌握，通報應變平台之流程畫分為通報流程與應變流程。
- 第一線人員由於處理時間的限制，可先進行通報流程，待完成處理後再進行應變流程。
- 請各單位盡可能通報與應變同時進行。

1. 資安事件處理與回報

- 所有通報應變流程之通報，都必須審核過後才是(教育部規範)正式結束通報流程。
- 如此規劃著眼於不同層級之資安人員可充分掌握所發生之資安事件，並能依輕重等級啟動不同對應之處理機制。

顯示

106年下半年資安事件統計處理時效

資料時間：2017/7/1-2017/11/30

連線單位	平均通報處理時間	平均應變處理時間	平均全部處理時間	資安事件數
國立臺東大學	00:36:16	00:00:00	00:36:16	34
國立臺東大學附設實驗國民小學	00:29:52	00:00:00	00:29:52	4
國立臺東高級商業職業學校	00:10:39	00:00:00	00:10:39	3
國立臺東大學附屬體育高級中學	01:11:57	00:00:00	01:11:57	2
臺東縣私立育仁高級中學	00:25:29	00:00:00	00:25:29	2
國立成功商業水產職業學校	00:56:31	00:00:00	00:56:31	1
國立關山高級工商職業學校	01:38:53	00:00:00	01:38:53	1

資料來源：教育機構資安通報平臺

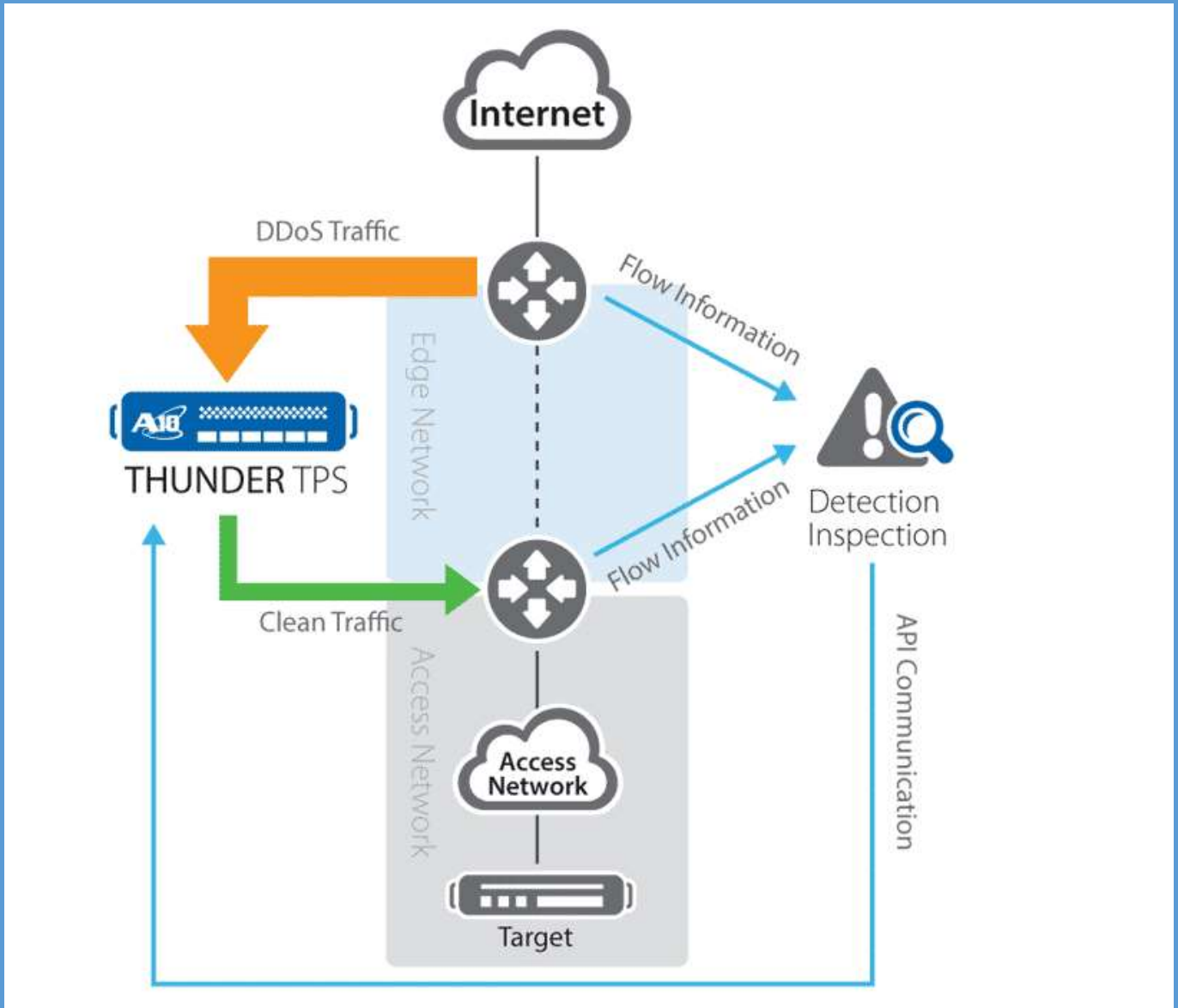
2. 學術網路DDoS清洗機制

- 現今的網路攻擊日益頻繁，規模更大，且複雜度更勝以往。
- 尤其近年來國際間發生多起大規模DDoS(Distributed Denial of Service，分散式阻斷服務攻擊)攻擊事件，而且攻擊規模更頻頻創新高

2. 學術網路DDoS清洗機制

- 有鑑於此，教育部已於S-ASOC及N-ASOC建置TANet流量清洗中心，當TANet內部單位遭受DDoS攻擊時，可透過TANet流量清洗中心過濾掉攻擊封包，讓系統可迅速回復正常。

ASOC現行DDoS清洗服務架構



2. 學術網路DDoS清洗機制

- 教育部TACERT團隊負責開發「DDoS清洗申請系統」以協助二線區縣市網路中心人員以及SOC團隊申請DDoS清洗服務以及管理清洗流程進度使用

2. 學術網路DDoS清洗機制

- 「DDoS清洗申請系統」位於教育機構資安通報回饋平台(https://portal.cert.tanet.edu.tw)中之「資安通報報表 系統」內

DDoS清洗服務申請

報表查詢系統
Developed By TACERT

OID查詢 | 威脅名單 | 事件單列表 | EWA列表 | 事件類型統計 | 轄下單位密碼更動情況 | DDOS清洗系統

清洗IP*	
單位名稱*	【已停用帳號】國立臺東生活美學館 ▼
通訊協定*	TCP ▼
服務說明*	例如:WEB FTP
通訊埠*	例如:80
申請理由	
	送出 (本系統僅適用於TANET部份地區)

四、討論提案

(一)TANet 傑出人員選拔遴選

- 依教育部計字第106030號公告辦理
- 被推薦人符合下列規定，且具有傑出貢獻事蹟者，應擇其中一類別參與選拔：

(一)應用推廣類：運用校園資訊網路環境，提升資訊教育、數位學習、行政資訊化等應用績效，並跨校、跨縣市推廣嘉惠學校。

(二)技術發展類：對TANet及整體校園骨幹網路環境之規劃、建置或所需之軟、硬體設施，開發或導入具創新性之相關新技術，並 能推廣嘉惠各級學校或區、縣市教育網路中心之運作，有效提升校園網路服務之效能及便利性。

(三)管理維運類：對TANet及校園整體骨幹網路設備之維護及網路基礎服務(例如DNS、IP等)之維運、管理或資安之防護、應變處置，能增進TANet網路之效能改善及妥善率提升等績效。

(二)區網來年研習課程建議

- 年度已辦理教育訓練課程如下：
- 01/09-3HR-106年度資安與個資保護宣導研習課程-個資法與資訊安全認知訓練
- 01/10-3HR-106年度資安與個資保護宣導研習課程-個資盤點訓練
- 01/11-3HR-106年度資安與個資保護宣導研習課程-個資風險評鑑訓練
- 03/07-2HR-OpenOffice實務：Writer與Calc應用
- 03/16-2HR-OpenOffice實務：Calc應用
- 05/11-3HR-106年社交工程演練教育訓練
- 08/18-6HR-兒童程式設計教學研習
- 09/27-3HR-機房建置管理規劃研習

研討會預告

- 12/12-3HR-資訊安全技術
- 12/16-6HR-Proxmox VE開源虛擬化平台實戰
- 12/26-3HR-虛擬化技術實務

(三)雲端機房使用需求調查

- 1. 雲端虛擬主機租用管理要點
- 2. 申請方式
- 3. 資源限制

(四)臨時動議

- 臺東大學附屬體育中學提議：

  本校建議於明年可提供網路評估服務，增進網路效能與未來建置經驗，惟缺乏相關規劃建置經驗，建議可提供相關經驗。

(四)臨時動議

- 為協助學術網路使用單位培養資安能量，教育部學術網路資安事件分析與教育中心設計為期三天資安事件分析與應變處理教育訓練課程。本次培訓課程規劃多面相的資安教育訓練課程，內容包含日常資訊系統管理所需的資安技術及處理資安事件時所需之技能，並在課程中，設計多個實際的動手練習，教授實用之技能。
- 參加人數：2人。
- 參加費用:免費，包含食宿，但不包含來往新竹交大交通費用住宿以雙人房為主，如有單人房需求，需自付額外產生費用。

五、指導與建議

六、散會