

TACERT 臺灣學術網路危機處理中心團隊 製 2018/5



ロッシュ

- `	前言	. 2
ニ、	系統說明	. 2
三、	操作說明	. 4
(1)	系統網址及登入說明:	. 4
(2)	OID 查詢(單位 OID 暨聯絡人查詢系統)	. 5
(3)	威脅名單(惡意網站威脅來源清單公告系統)	. 6
(4)	事件單列表(資安事件報表系統)	. 8
(5)	EWA 列表(資安預警事件報表系統)	. 9
(6)	事件類型統計(資安攻擊類型趨勢統計系統)	11
(7)	轄下單位密碼更動情況	12
(8)	DDoS 清洗系統(DDoS 清洗服務申請系統)	12

一、前言

教育機構資安通報平台自 99 年啟用,資安事件單之數量亦逐年增加。 TACERT 營運時得知管理單位對於事件單之追蹤及統計之需要,因此於 101 年 度開發「教育機構資安通報平台報表系統(以下簡稱資安通報報表系統)」,系統 網址:<u>https://portal.cert.tanet.edu.tw</u>,以利管理單位進行追蹤及統計使用。

二、系統說明

101 年度 TACERT 開發「教育機構資安通報平台報表系統(以下簡稱資安通 報報表系統)」,提供二線區縣市網管理人員使用,已完成開發「單位 OID 查 詢」、「惡意網站威脅來源清單公告」、「資安事件報表系統」、「資安預警事件報 表系統」與「資安攻擊類型趨勢統計」等子系統。106 年陸續新增「轄下單位 密碼更動情況系統」及「DDoS 清洗服務申請系統」。

	資安通	朝報	表系統		
A1 單位OI 暨聯絡人查詢系統OID 暨聯絡人查詢系統	A3 資安事件單報表系統	A4 資安預警單報表系統	A5 資安事件類型統計系統	A6 轄下單位密碼更動情況	A7 DDoS 清洗服務申請系統

資安通報報表系統功能表如圖1所示,系統功能說明如表1所示。

圖1 資安通報報表系統功能表

功能	使用人員	功能說明
A1 單位 OID 暨 聯絡人查詢 系統	二線人員	區縣市網路中心管理人員與 TACERT 營運團隊可以查詢單位 於通報平台內更新的資安連絡人連絡資訊與單位 OID 資訊
A2 惡意網站清 單公告系統	二線人員	區縣市網路管理人員可以於此處瀏覽與下載「惡意網站威脅 來源清單」的公告資訊。 TACERT 營運團隊每週匯整由各個資安偵測團隊所偵測的 「惡意網站威脅來源清單」,並每週定期更新「惡意網站威 脅來源清單」。 *107 年 5 月新增「下載技服威脅清單」功能,可個別下載由 「行政院國家資通安全會報技術服務中心」所提供的完整惡 意網站威脅來源清單。
A3 資安事件單 報表系統	二線人員	各區縣市網路中心管理人員或 TACERT 管理人員可於此處利 用「單位名稱」或「日期區間」,快速查詢與下載其轄下連 線單位的資安事件報表資料,以利進行統計與進行更進一步 之追蹤。
A4 資安預警單 報表系統	二線人員	各區縣市網路中心管理人員或 TACERT 管理人員可於此處利 用「單位名稱」或「日期區間」,快速查詢與下載其轄下連 線單位的資安預警事件報表資料,以利進行統計與進行更進 一步之追蹤。
A5 資安事件類 型統計系統	二線人員	提供所有學術網路資安事件攻擊事件量、事件類型統計報 表,讓使用者可了解目前的資安事件攻擊趨勢,進而加以防 範。
A6 轄下單位密 碼更動情況	二 <mark>線人員</mark>	提供各區縣市網路中心管理人員查詢轄下單位密碼更新狀況,以利追蹤轄下單位是否有確實完成每年度密碼更新作 業。
A7 DDoS 清洗系 統	二線人員	提供二線區縣市網路中心管理人員協助轄下連線單位申請 「DDoS 清洗服務」使用,以及查詢其清洗流程。

表1資安通報報表系統功能說明

三、操作說明

下列將針對系統及子功能進行操作說明,並佐以畫面以利操作。

(1) 系統網址及登入說明:

STEP 1.

系統網址:<u>https://portal.cert.tanet.edu.tw</u>

選擇「資安通報報表系統」,如圖2。

al.cert.tanet.edu.tw ×		~ # C	授尋	₽ + 1 ₩ ₩
COMPUTER EMERGENCY RESPONSE TEAM		台灣學術網路危機。 TAIWAN >>> 教育机	^{國理中心} 幾構貪安通報	報回饋平台
	催 限二三線人員使用	省交通報報表系统		
	僅限發單單位使用	教育機構查安通報回饋平台		
	僅限發單單位使用	文件管理系统		

圖 2

STEP 2.

於登畫面鍵入<u>審核用帳號、密碼(</u>英文+OID 帳號,如 Z2.16.....)及驗證 碼,如圖 3。

Š	
Login:	
Password:	
6237N	

圖 3

STEP 3.

介面說明:

A. 登入後於上方右側顯示登入帳號及「登出」功能,如圖4中① 所示。

B. 中央上方顯示子功能頁籤,點選可開啟對應子功能,如圖4中② 所示。

2)	報表查 Developed	訽系統 I By TACER	т					
	OID查詢	威脅名單	事件單列表	EWA列表	事件類型統計	藝下單位密碼更動情況	DDOS清洗系統	z2.16.886.111.100008 教育部態好登出
						報表系統 provided by TACER		
						回 4		

圖 4

(2) OID 查詢(單位 OID 暨聯絡人查詢系統)

```
STEP 1.
```

選擇「OID 查詢」開啟單位 OID 暨聯絡人查詢系統,如圖 5。

報表查 Developed	<mark>詢系統</mark> d By TACER							
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	z2.16.886.111.100	0008 教育部您好登出
					報表系統 provided by TACER	σ		
					圖 5			
	STE	EP 2.						
	А.	開啟單	位 OII)暨聯絡	人查 詢系約	施後,將列:	出貴單位轄-	下所有單位
	及單	置位連續	洛人資;	料,如圖	圖 6 中① 所	示。		
	B .	左上方	可針對	單位 0	ID 及名稱進	進行搜尋動作	乍,輸入進行	亍搜尋的

OID 及名稱後,點選「送出」(因瀏覽器定義不同,請勿以 Enter 查 詢),如圖 6 中② 所示。



報表查詢系統 Developed By TACERT OID畫版 M#37 #	端率列表 EWA列表	事件期388計 新下單位後期至動物及 DDOS非走系统		22.16.586.113.10000
四或學校名稱	<u>e</u>)		
OID 14.13.15676	單位名稱 [測試用] 高雄 市立資安國民小 學	第一理結人 理結電話 第二連結人 第三	-連絡人 [第四連絡人	第五連結人
6.886.101.20003.20005	教育部			
16.886.101.20003.20005.20001	國立獲譯施	1		
16.886.101.20003.20005.20003	國立歷史博物館			
6.886.101.20003.20005.20004	間立臺灣科學教育部			

圖 6

- (3) 威脅名單(惡意網站威脅來源清單公告系統)
 - STEP 1.

選擇「威脅名單」開啟惡意網站威脅來源清單公告系統,如圖7。

威脅名單	事件單列表	EWA列表	事件類型統計	藝下單位密碼更動情況	DDOS消	洗系統	z2.16.886.111.100008 教育部您好
		搜尋		Show 下載TANET病 Last modified: 2018/05/16 15:	找 薪清單 下 48:57	「載技服威脅清單	
第一頁 上一頁 下	一頁 最終頁						
公告來源	發現日	期	I	P ş	這網址	攻撃類型	國家
S-ASOC	2018-05-12					網路攻擊	Hong Kong
S-ASOC	2018-05-12					網路攻擊	Ukraine
S-ASOC	2018-05-12					網路攻擊	China
S-ASOC	2018-05-12					網路攻擊	United States
S-ASOC	2018-05-12					網路攻擊	Poland
S-ASOC	2018-05-11			1		網路攻撃	China
S-ASOC	2018-05-11	Ĩ				網路攻撃	China
S-ASOC	2018-05-11			1		網路攻擊	Belarus
S-ASOC	2018-05-11			1		網路攻撃	Venezuela
S-ASOC	2018-05-11			1		網路攻撃	Venezuela
S-ASOC	2018-05-11			1		網路攻擊	Macedonia
S-ASOC	2018-05-11			1		網路攻擊	Netherlands
C ACOC	2010 05 11	ł		1		Skillt & reveal	Natharlanda

STEP 2.

A. 開啟惡意網站威脅來源清單公告系統後,將列出最新一次更新之威 脅名單列表,如圖 8 中① 所示,目前表列近三個月資訊,且固定於每 星期三更新。

B. 中央上方可針對表格內欄位進行搜尋動作,輸入進行搜尋之內容後,點選「Show」,如圖 8 中② 所示。

C. 如需下載該威脅名單,點選「下載 TANet 威脅清單」即可取得最 近三個月的完整惡意威脅名單,如圖 9 中①所示;如需個別下載技服 中心提供的所有惡意威脅清單,點選「下載技服威脅清單」即可取 得,如圖9中②所示。

D. 威脅清單內容為機敏性資料,故下載清單會出現「威脅清單內容為機敏性資料,僅供公務使用,嚴禁外流並依公務密件相關規定處理!」的提示視窗,提醒使用者留意,點選「確定」即可下載該清

單。

eu e	BY TACER							
	威脅名單	事件事列表 E	WA列表 事件類	弦統計 	密碼更動情況 DDOS;	清洗系統	22.16.886.111.10	10008 一致時間急
		0						
~		e	授聘	Show	「載IANEI版飾清單」	下載改服服飾清單		
1)				Last modified	1: 2018/05/16 15:48:57			
-11	上一面 下一	「夏」最終夏						
13	合來源	登現日期	1	IP	亮音網址	内整结型	R	家
S-AS	OC	2018-05-12			A.8704017.345	網路攻鬆	Hong Kong	
S-AS	OC	2018-05-12				細胞攻撃	Ukraine	
-AS	OC	2018-05-12				網路攻擊	China	
-AS	OC	2018-05-12				網路攻撃	United States	
-AS	oc	2018-05-12				網路攻擊	Poland	
-AS	00	2018-05-11				網路攻擊	China	
-AS	00	2018-05-11				新服各攻撃 (4)300 年10 年5	China	
-AS	00	2018-05-11				回報告4又離 4回版2157#2	Venezuola	
-ASI	00	2018-05-11				合理的4次3章 经贸易1分3章	Venezuela	
-AS	oc	2018-05-11				編輯功整	Macedonia	
AS	0C	2018-05-11				4曜8功盤	Netherlands	
-AS	00	2018-05-11	î			结理语言 TOT 意思	Netherlands	
從 IE 合 By	·匯入 G Gd 余統 / TACERT 嫡名單	oogle G G Suite 事件單列表 EW	portal.c 本演單內 處理? VA列表 事件類及	erttanet.edu.tw 顯示 音為機敏性資料僅供公務 総計 格下単位者	使用。酸菜外流並依公務要件格 使用。酸菜外流並依公務要件格 受更動情況 DDOS済	IIII / IIIII / IIII / IIIII / IIII / IIIII / IIII / IIII / IIIII / IIIII / IIIII / IIIIII	22.16.886.111.100	9008 教育部態
從 IE d By	E團入 G Go 系統 Y TACERT X爾名單	oogle G G Suite 都件單別表 EW	portal. 本演單內 處理? VA列表 事件和 搜尋	ert.tanet.edu.tw 顧示 音為現数性質料僅供公務 総定	使用, 酸禁外流並依公藉要件将 德史動情況 DDOS 差 下載TANET成發清軍1 2018/05/16 15:48:57	i願規定 確定 <u>) 文載支服成</u> 資清單	22.16.886.111.100	9008 教育部態
從IE () () () () () () () () () (EAGGG	oogle G G Suite 事件單列表 EW	portal.c 本演單內 處理? 小列表 事件類 搜尋	ert.tanet.edu.tw 顧示 查為機敏性資料僅供公發 強助 轄下単位答 ① Show Last modified:	使用.最禁外流並依公務硬件相 使用.最禁外流並依公務硬件相 使更動情況 DDOS <u>一下載TANET成藝清單</u> [2018:05:16 15:48:57	 職規定 確定 PK5年 2) 本好支服成斎清單 	z2.16.886.111.100	9008 数育部数
從IEE 注) d By 夏 〕 二 告 ※ 節 。	■入 G GG 系統 TACERT 始名単 上一頁 下一頁 發現日期	oogle G G Suite 事件單列表 EW [1]最終頁 [1]P	portal.c 本语單內 處理? 少A列表 事件類及 搜尋 一	terttanet.edu.tw 願示 查為機敏性資料僅供公務	使用, 戴禁外流並依公務硬件相 穩更動情況 DDOS済 下載TANET成發清單」 2018.05/16 15:48:57	 職規定 確定 定支款 2) *就技克服成勞清單 政撃頻型 	22.16.886.111.100	9005 数育課盤
從IE 約 d By 夏 二 二 二 二 二 二 二 二 二 二 二 二 二	ELA G Ga 余統 / TACERT 續名單 並現日期 2018- 05-13	oogle G G Suite 事件取列表 EW [1]最終頁 [1]P	portal. 本语單內 處理? 少A列表 事件知 提尋	ert.tanet.edu.tw 顧示 音為機敏性資料僅供公務 (動) (Show Last modified 意創知	使用,戴禁外流並依公務硬件相 概更動情況 DDOS T款TANET 成發遺單 2018.05/16 15:48:57	IIII 規定 確定 文字表統 2) 「就対東服成脅清單 攻撃類型 upache Struts rer	z2.16.886.111.100	9005 教育部部 1005 教育部部 1005 教育部部
從IEE 前, d By 夏]] ;告 源 ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	ELA G GG 余統 / TACERT ☆現日期 2018- 05-13 2018- 05-13	oogle G G Suite 事件事列表 EW [最終頁 IP	portal. 本演單內 處理? 少A列衣 事件知 提尋 一	eer.tanet.edu.tw 顧示 查為機敏性資料僅供公發	使用.最美外流並依公務审件相 每更勤勞況 DDOS <mark>下載TANET成發清單. </mark> 2018/05/16 15:48:57 SERVER-APACHE A execution attempt SQL SA brute force	職規定 構定 大手系統 2 一 一 数支服成斎清單 の 文型積型 Appache Struts rei a login attempt T	z2.16.886.111.100 note code DS v7/8	DOOS 数育部您 回家 China Korea
從 IE	■入 G GG 系統 / TACERT 協会工業 登現日期 2018- 05-13 2018- 05-13	oogle G G Suite 事件單列校 EW i L最終頁 IP	portal. 本演單內 處理?	tert.tanet.edu.tw 願示 查為機敏性資料僅供公務	使用.最繁外流並依公務定件样 德史動情況 DDOS活 下載TANET成動法量 2018.05/16 15:48:57 SERVER-APACHE A <u>execution attempt</u> SQL SA brute force SERVER-OTHER Re <u>force attempt</u>	電視定 後定 文文を基 2) 「載技規脱成脅清單 の文撃頻型 upache Struts rer e login attempt T emote Desktop P	z2.16.886.111.100 mote code DS v7/8 rotocol brute	0003 数育部部 回家 China Korea United States
從 IE () () () () () () () () () ()	 正入 G G 余統 八 TACERT (第名単) <	oogle G G Suite 事件事列表 EW [假祭頁 IP	portal. 本演單內 處理? 少A列表 事件來 授尋	tert.tanet.edu.tw 顧示 查為機敏性資料僅供公發	使用.最美外流並依公務审件相 每更勤勞況 DDOS 下載TANET成發清單. 2018/05/16 15:48:57 SQL SA brute force SQL SA brute force SERVER-OTHER Re force attempt	職規定 構定 支ま紙 文学教授型 なななが予算 の文学教授型 Apache Struts rer e login attempt T emote Desktop P emote Desktop P	z2.16.886.111.100 note code DS v7/8 rotocol brute rotocol brute	DODA I 数育部推 回家 China Korea United States United Kingdom
從 IE () () () () () () () () () ()	ELA G GG 条約 (TACERT) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT) (第名単) (TACERT)	oogle G G Suite 事件單列校 EW i I最終頁 IP	portal. 本演單內 處理?	tert.tanet.edu.tw 願示 查為機敏性資料僅供公務	使用.最繁外流並依公務要件样 使用.最繁外流並依公務要件样 等更動情況 DDOS活 下款TANET成發活軍」 2018.05.16 15:48:57 SERVER-APACHE A execution attempt SQL SA brute force SERVER-OTHER Re force attempt SERVER-OTHER Re force attempt	alin 明定 確定 2) 本 就支服成斎清單 取 撃類型 apache Struts rer e login attempt T emote Desktop P emote Desktop P emote Desktop P	22.16.886.111.100 22.16.886.111.100 mote code DS v7/8 rotocol brute rotocol brute rotocol brute	Doos 数育部部 Doos 数育部部 区内ina Korea United States United Kingdom United Kingdom
後 IE () (B) (B) (C) (C) (C) (C) (C) (C) (C) (C	 正入 G G 泉統 木ACERT 満名単 ガーズの目前 第4日期 2018- 05-13 2018- 05-13	oogle G G Suite 事件率列表 EW [假終頁 IP	portal.(本语單內 處理?	tert tanet.edu.tw 願示 查為機敏性資料僅供公發 強助 第下単位表 Show Last modified: 意納吐	使用	職規定 構定 文学系統 文学系統 文学系統 文学教授型 なな なな なな なな なな なな なな	z2.16.886.111.100 mote code DS v7/8 rotocol brute rotocol brute rotocol brute rotocol brute	008 数育部批 008 数育部批 China Korea United States United States United Kingdom United Kingdom
後 IE	EL G G G G G G G G G G G G G G G G G G G	oogle G G Suite 事件單列表 EW I 服然頁 IP	portal. 本演單內 處理?	tert.tanet.edu.tw 顧示 查為機動性質料僅供公務 () Show Last modified:	使用最繁外流並依公務要件相 使用最繁外流並依公務要件相 安全動情況 DDOS派 下載TANET成發清單.1 2018/05/16 15:48:57 2018/05/16 15:48:57 2018/05/16 15:48:57 SERVER-OTHER Reforce attempt SERVER-OTHER Reforce attempt SERVER-OTHER Reforce attempt SERVER-OTHER Reforce attempt SERVER-OTHER Reforce attempt	電視定 確定 2) 本説女服成斎清單 文学教型 な学教型 な学教型 に な学教型 に な学教型 に な学校 の の な学校 の の の の の の の の の の の の の	22.16.886.111.100	DOOS 数 好選集 DOOS 数 好選集 China Korea United States United Kingdom Wingdom Korea China
後1日 第 1 1 1 1 1 1 1 1 1 1 1 1 1	■入 G G	oogle G G Suite 事件率列表 EW 【旧錄詞 【P	portal.c 本语單内 處理?	tert.tanet.edu.tw 願示 音為機敏性質相僅供公務 (1) Show Last modified:	使用.最繁外流並依公務定件样 使用.最繁外流並依公務定件样 等更動情況 DDOS# F載TANET成錄法量工 2018.05/16 15:48:57 SERVER-APACHE A execution attempt SQL SA brute force SERVER-OTHER Re force attempt SERVER-OTHER Re force attempt	職規定 改革 文本 文本 文本 文本 文本 文本 文本 文	22.16.886.111.107 22.16.886.111.107 mote code DS v7/8 rotocol brute	Doos 数育部部 Doos 数育部部 China Korea United States United States United Kingdom Korea China China
後 IE () () () () () () () () () (oogle G G Suite 事件取例表 EW [殿絵頁 IP	portal. 本演單內 處理? 少A列表 事件來 授尋	tert tanet.edu.tw 願示 查為機敏性資料僅供公發 (1) Show Last modified 意趣处	使用.最禁外流並依公務率件样 使用.最禁外流並依公務率件样 安史勤勞況 DDOS系 下載TANET成發清單.1 2018/05/16 15:48:57 SERVER-APACHE A execution attempt SERVER-OTHER Re force attempt	職機定 改革 文学教理 文学教理 ななななの ななななの ななななの ななななの たので で で で で で で で で で	22.16.886.111.100 z2.16.886.111.100 mote code DS v7/8 rotocol brute rotocol brute rotocol brute rotocol brute rotocol brute rotocol brute rotocol brute rotocol brute	DODS I 数百部部 DODS I 数百部部 China Korea United States United Kingdom Korea China China China
	ELA G G G S	oogle G G Suite 事件事列表 EW I 最終頁 IP	portal. 本演單內 處理?	tert.tanet.edu.tw 願示 查為機敏性資料僅件公務 () Show Last modified:	使用.最繁外流並依公務率件样 使用.最繁外流並依公務率件样 等更動情況 DDOS活 下該TANET成錄法軍」 2018.05.16 15:48:57 SQL SA brute force SQL SA brute force SERVER-OTHER Re force attempt SERVER-OTHER Re force attempt	電視定 電定 2) 本好支服成斎清單 文学教理 取参教理 取参教理 和文学教理 中国の日をStruts rere e login attempt T emote Desktop P emote Desktop P	22.16.886.111.100 22.16.886.111.100 anote code DS v7/8 rotocol brute rotocol brute	Duos 較育選編 Duos 較育選編 China Korea United States United Kingdom Korea China China China

圖 9

(4) 事件單列表(資安事件報表系統)

STEP 1.

選擇「事件單列表」開啟資安事件報表系統,如圖 10。

報表 Develop	E 洵 系統 ed by tace															
OID透射	威脅名單	事件單列表	EWA列表	441-3652801	轄下單位會	等王動的況	DDOS清洗系統	I					22.16.996.11	121000000000000000000000000000000000000	le fermilite er	盤出
革位搜尋		狀態搜尋	• (開始日期	國專件	結束日期	3 前方	羅出報表								
							3		(最終實							
	事件單編 3 版	·····································	OIDNo	軍(立名稿	等 事件類 級 型	攻撃類型	事件發生時間	發佈時間	通報時間	應發時間	通報審核時間	應變審核時間	IP	重覆工單	
	1426					1級 INT	殭屍電腦(Bot)	2018-05-14	2018-05-14	2018-05-16	2018-05-16	2018-05-16	2018-05-16		否	

0% 394	989	dt.								77.44
1428	1 卷殿	INT	殭屍電腦(Bot)	2018-05-14 10:26:00	2018-05-14 10:45:34	2018-05-16 13:49:35	2018-05-16 13:49:35	2018-05-16 14:11:53	2018-05-16 14:11:53	否
1420	1.6股	INT	對外攻擊	2018-05-01 16:08:10	2018-05-01 16:30:21	2018-05-01 16:37:44	2018-05-01 16:37:44	2018-05-01 16:52:19	2018-05-01 16:52:19	否
141	1.6股	INT	系統被入侵	2018-04-26 12:08:07	2018-04-26 12:30:44	2018-04-26 15:54:05	2018-04-26 15:54:05	2018-04-26 16:50:31	2018-04-26 16:50:31	西
140:	1.8股	INT	對外攻擊	2018-04-10 10:37:00	2018-04-10 10:50:26	2018-04-10 16:30:55	2018-04-10 16:30:55	2018-04-10 17:14:42	2018-04-10 17:14:42	否
1391	1 6辰	INT	射外攻離	2018-03-30 08:04:00	2018-03-30 09:11:29	2018-03-30 10:20:33	2018-03-30 10:20:33	2018-03-30 13:43:45	2018-03-30 13:43:45	香
139	1 点辰	INT	對外攻擊	2018-03-29 11:45:00	2018-03-29 13:50:35	2018-03-30 13:32:57	2018-03-30 13:32:57	2018-03-30 13:43:27	2018-03-30 13:43:27	香
139	1.6辰	INT	其它類型的入機 攻擊	2018-03-29 09:15:00	2018-03-29 09:41:10	2018-03-29 10:40:40	2018-03-31 14:27:24	2018-03-29 10:42:45	1999-01-01 00:00:00	否
139:	1.6년	INT	對外攻擊	2018-03-23 16:08:07	2018-03-23 16:20:32	2018-03-23 17:06:59	2018-03-23 17:06:59	2018-03-23 17:13:35	2018-03-23 17:13:35	否
1381	1.68	INT	系統被入侵	2018-03-14 12:22:10	2018-03-14 12:30:54	2018-03-15 15:19:17	2018-03-15 15:19:17	2018-03-15 15:41:52	2018-03-15 15:41:52	否
1375	165	INT	射外攻撃	2018-03-13 07:59:00	2018-03-13 08:30:44	2018-03-13 09:04:34	2018-03-14 09:39:12	2018-03-13 13:43:57	1999-01-01 00:00:00	香
137	18冊	INT	對外攻擊	2018-03-10	2018-03-12	2018-03-12	2018-03-12	2018-03-12	2018-03-12	否

圖 10

STEP 2.

A. 開啟資安事件報表系統後,將列出貴單位轄下管理之事件單列表, 如圖 11 中① 所示。

B. 中央上方可針對單位、狀態及時間等條件進行搜尋,完成條件輸入後,點選「顯示」,如圖 11 中② 所示。

C. 如需匯出報表,完成修件輸入後,點選「匯出報表」後點選「下載 excel 結果」即可取報表,如圖 12 中①②所示。

報表查	 詞系統 d by TACERT													
OID#200	威脅名單 事件	I列表 EWA列表 4	PATRICIPAL ANTI-	102 103 105 10	動構成	DDOS清洗系統						27.16.886.11	1000681	OF BA
軍位授尋	厭	該授尊 事件開始	日期 🔯	事件结束	(日期)	1 顯示	羅出報表							
	事件單編 截 渡	OIDNo	軍位名稱	等級	事件類型	攻撃減型	事件發生時間	發佈時間	通報時間	應該時間	通報審核時間	應變審核時間	IP	重覆工單
	141			1級	INT	条統被入侵	2018-04-26 12:08:07	2018-04-26 12:30:44	2018-04-26 15:54:05	2018-04-26 15:54:05	2018-04-26 16:50:31	2018-04-26 16:50:31		否
	140:			1級	INT	對外攻擊	2018-04-10 10:37:00	2018-04-10 10:50:26	2018-04-10 16:30:55	2018-04-10 16:30:55	2018-04-10 17:14:42	2018-04-10 17:14:42		否
	139			1級	INT	對外攻擊	2018-03-30 08:04:00	2018-03-30 09:11:29	2018-03-30 10:20:33	2018-03-30 10:20:33	2018-03-30 13:43:45	2018-03-30 13:43:45		否
	139			1級	INT	對外攻離	2018-03-29 11:45:00	2018-03-29 13:50:35	2018-03-30 13:32:57	2018-03-30 13:32:57	2018-03-30 13:43:27	2018-03-30 13:43:27		杳
	139			1級	INT	其它類型的入侵 攻撃	2018-03-29 09:15:00	2018-03-29 09:41:10	2018-03-29 10:40:40	2018-03-31 14:27:24	2018-03-29 10:42:45	1999-01-01 00:00:00		否
	139	(1)		1級	INT	對外攻擊	2018-03-23 16:08:07	2018-03-23 16:20:32	2018-03-23 17:06:59	2018-03-23 17:06:59	2018-03-23 17:13:35	2018-03-23 17:13:35		否
	138			1級	INT	系統被入侵	2018-03-14 12:22:10	2018-03-14 12:30:54	2018-03-15 15:19:17	2018-03-15 15:19:17	2018-03-15 15:41:52	2018-03-15 15:41:52		否
	137			1級	INT	對外攻擊	2018-03-13 07:59:00	2018-03-13 08:30:44	2018-03-13 09:04:34	2018-03-14 09:39:12	2018-03-13 13:43:57	1999-01-01 00:00:00		酉
	137			1級	INT	對外攻擊	2018-03-10 06:08:07	2018-03-12 08:20:35	2018-03-12 09:43:58	2018-03-12 09:43:58	2018-03-12 09:52:17	2018-03-12 09:52:17		晋
	136			1級	INT	殭屍電腦(Bot)	2018-03-05 10:51:00	2018-03-05 11:11:10	2018-03-05 13:04:02	2018-03-07 07:48:49	2018-03-05 13:46:50	1999-01-01 00:00:00		否
	136			1級	INT	對外攻擊	2018-03-05 09:48:26	2018-03-05 10:00:36	2018-03-07 08:52:26	2018-03-07 08:52:26	2018-03-07 09:20:44	2018-03-07 09:20:44		否
	136			1級	INT	殭屍電腦(Bot)	2018-02-26 10:32:00	2018-02-26 14:00:27	2018-02-26 14:49:43	2018-02-26 16:04:02	2018-02-26 15:09:02	1999-01-01 00:00:00		否
	136			2級	INT	其它類型的入侵 攻撃	2018-02-23 08:10:14	2018-02-23 10:23:27	2018-02-23 10:23:27	2018-02-23 10:23:27	2018-02-23 10:33:13	2018-02-23 10:33:13		否
	134			1級	INT	其它類型的入侵 政程	2018-01-25 00:00:00	2018-01-29 10:51:15	2018-01-29 11:22:05	2018-01-31 15:46:31	2018-01-29 11:28:12	1999-01-01 00:00:00		否

圖 11

報表查詢系統 Developed By TACER	т												
OID查询 成音名單	事件單列表	EWA列表 事	1983-2869) # # T- Witz Haves	更勤慎况 DD	osmaan (1)				1	16.586.111.1000	061 数间部组	19 一般出
軍位搜尋	秋態複載	• 事件開始E	期 🔲 平件結3	東日期	100 日本 1000	#表							
÷					2	jexcel結果							
事件單編 通 載	報来 源	OIDNo	單位名稱	等 事件表 型 14% INT	₫ 攻撃類型 ※は対1点	事件發生時間	發佈時間 2018-04-26	通報時間	應變時間 2018-04-26	通報審核時間 2018-04-26	應變審核時間 2018.04.26	IP	
140				1級 INT	對外攻擊	12:08:07 2018-04-10	12:30:44 2018-04-10	15:54:05 2018-04-10	15:54:05 2018-04-10	16:50:31 2018-04-10	16:50:31 2018-04-10		
139				1級 INT	對外攻擊	10:37:00 2018-03-30 08:04:00	10:50:26 2018-03-30 09:11:29	16:30:55 2018-03-30 10:20:33	16:30:55 2018-03-30 10:20:33	17:14:42 2018-03-30 13:43:45	17:14:42 2018-03-30 13:43:45		
139				1飯 INT	對外攻擊	2018-03-29 11:45:00	2018-03-29 13:50:35	2018-03-30 13:32:57	2018-03-30 13:32:57	2018-03-30 13:43:27	2018-03-30 13:43:27		
139				189 INT	其它類型的人使 攻撃 動风作数	2018-03-29 09:15:00 2018-03-23	2018-03-29 09:41:10 2018-03-23	2018-03-29 10:40:40 2018-03-23	2018-03-31 14:27:24 2018-03-23	2018-03-29 10:42:45 2018-03-23	1999-01-01 00:00:00 2018-03-23		
138				1級 INT	系統被入侵	16:08:07 2018-03-14	16:20:32 2018-03-14	17:06:59 2018-03-15	17:06:59 2018-03-15	17:13:35 2018-03-15	17:13:35 2018-03-15		
137				1級 INT	對外攻擊	12:22:10 2018-03-13 07:59:00	12:30:54 2018-03-13 08:30:44	15:19:17 2018-03-13 09:04:34	15:19:17 2018-03-14 09:39:12	15:41:52 2018-03-13 13:43:57	15:41:52 1999-01-01 00:00:00		
137				1級 INT	對外攻擊	2018-03-10 06:08:07	2018-03-12 08:20:35	2018-03-12 09:43:58	2018-03-12 09:43:58	2018-03-12 09:52:17	2018-03-12 09:52:17		
136				15% INT	種開電腦(Bot)	2018-03-05 10:51:00	2018-03-05 11:11:10 2018-03-05	2018-03-05 13:04:02	2018-03-07 07:48:49 2018-03-07	2018-03-05 13:46:50 2018-03-07	1999-01-01 00:00:00 2018-03-07		
136				1級 INT	到7743(单 殖院電腦(Bot)	2018-03-03 09:48:26 2018-02-26	2018-03-05 10:00:36 2018-02-26	08:52:26 2018-02-26	08:52:26 2018-02-26	2018-03-07 09:20:44 2018-02-26	09:20:44		
136				2級 INT	其它類型的入後 内態	10:32:00 2018-02-23 08:10:14	14:00:27 2018-02-23 10:23:27	14:49:43 2018-02-23 10:23:27	16:04:02 2018-02-23 10:23:27	15:09:02 2018-02-23 10:33:13	00:00:00 2018-02-23 10:33:13		
報表查詢 Developed By OID查询	STEP 選擇 系統 TACERT	1 . 「 EWA 事件單列表	列表」 EWA预表 #	用啟	資安預	警事作	牛報表 DDOS潮	£ 余 統	,女口 z2.1	圖 13	o 00008 教育	部態好餐	登出
					報表系統 pro	vided by TACER	I)						
					B	13							

STEP 2.

A. 開啟資安預警事件報表系統後,將列出貴單位轄下管理之預警事件
 單列表,如圖 14 中① 所示。

B. 中央上方可針對單位、狀態及時間等條件進行搜尋,完成條件輸入後,點選「顯示」,如圖 14 中② 所示。

C. 如需匯出報表,完成條件輸入後,點選「匯出報表」後點選「下載 excel 結果」即可取報表,如圖 15 中①②所示。

報表書	前系統 ed by tacer	T												
010±#	威脅名單	事件取得	EWA	時表 事件知道	1993日 韩下耶位的	可更勤的 况	DDOS演选者	SRE .				22,16,898,111.	1000001 第1日日	8.8.11-餐出
軍位搜尋		长大市 石	招募	 事件開始日 	H 🖸 4	伴結束日期		副期示目	重出報表	1				
			-							3				
	第一頁 上一頁	下一貫 最終	II.											1
Û	1942 0150		9C Bab		010	事件分	21 Hart 184			-			百百事件 ag	
	学校石桶	EWA	5455		OID	類	派神时间	夺敬		土目		IP	编號 情 形	
		NTUSOC- 201805-0	EWA-			可疑連 線	2018-05- 18 09:00:05	low					未處	
		NTUSOC- 201805-0	EWA-			可能建建	2018-05- 14	low					144 155	
		TACERT-E	WA-			其他	08:30:09 2018-05-	high	1				195	
		20180511 00007	L-				11 09:20:05						法判	
		TACERT-E 2018051	WA-			其他	2018-05- 11	high					(四) (四)	
		00018					09:40:12						判断	
		NTUSOC- 201805-0	EWA- 154			可能速	2018-05- 10 14:00:04	low					未處	
		MJIB-EW/	A-			永統疑	2018-05-	low					- [月編 代編 代編	
						開告	15:40:57						判断	
		NCCST-EV 201805-0	016			余統疑 存在弱	2018-05- 03	medium					読報	
	11		6		1		1	图	1	4				
								回	1					
報表在	詞系統 sd By TACER	r												
OID验训	威争名單	###98	EWA:	nte entrais	alikat in Takazaki	5200R	DDOS激洗食	"(T)				22,16,886,111.	LOODON - BLIEFE	ani BB
Two 244 (100 mm)		have	an en l	- Fur or much res		20.20000000				1				
単位投母		名天夜訳	0644	• ● 叶两次日日	al mala	1236931246	(Net I	NCG YARAR					
							2		Rexcel結	果				
	第一頁(上一頁)	下一頁 (最終	a l	· · ·										
	第 一			F101 A /5 AA			事件。					馬 置 縦 事 認	autor a	
	人	4685 5519	(学校石槽	C WA SHILL	OIL		分類 9	5 Mb#3403	谷酸	土田	IP.	件情態形	原因	
				NTUSOC- EWA-			可疑 20	018-04- li	w			長さ		
				201804- 0420			15	5:30:04		0		理		
	10.00			NTUSOC- EWA- 201804-			可疑 20 連線 21	018-04- 5 3:40:05	w			未處理		
				0377 NTUSOC-			可疑 20	018-04- 0	w			未		
				EWA- 201804- 0225			該重金数 17 08	7 8:40:09				處理		
				NTUSOC- EWA-			可疑 20 連線 10	018-04- 0 5	w			未處		
	-			0180 NTUSOC-			ा ज्राह 20	018-04-	w	ç		理		
	THE			EWA- 201804- 0181			連線 10	5 8:30:15				處理		
	10.00			NCCST- EWA-			余統 20 疑存 10	018-04- n 5	nedium			未慮		
			-	ineree i			Presson II 22	as and shall				1 1-20		

圖 15

- (6) 事件類型統計(資安攻擊類型趨勢統計系統)
 - STEP 1.

選擇「事件類型統計」開啟資安攻擊類型趨勢統計系統,如圖 16。

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	z2.16.886.111.100008 教育部態好 登出
報表系統 provided by TACERT	

圖 16

STEP 2.

A. 開啟資安攻擊類型趨勢統計系統後,將列出貴單位轄下單位已結案 之事件統計資料,如圖 17 中① 所示。且統計出目前貴單位平均審核 統計,以供貴單位參考,如圖 17 中②所示。

B. 中央上方可針對單位及時間等條件進行搜尋,完成條件輸入後,點選「顯示」,如圖 17 中③所示。

報表查 Develope	詢系統 d By TACER						
OID查詢	威脅名軍	事件軍列表	EWA列表	事件類型統計	轄下單位密碼更動情況	兄 DDOS清汫	i系統
3							
單位名稱	事件	開始日期	~		顯示		
~							
	Auto 2.5. 5454. 55.		h here here to serve h hered		The second secon	where the state state	
	理線單位	半#	自通報處理時間	半均應變處理時間	半均全部處理時間	資安事件數	
		26:	51:40	00:04:23	26:56:03	228	
		02:	19:39	27:38:44	29:58:23	18	
		21:	22:16	14:20:56	35:43:11	9	
		01:	01:21	29:12:08	30:13:28	6	
		01:	12:03	00:00:00	01:12:03	5	
		02:	05:40	00:01:09	02:06:48	4	
		00	07:58	36:22:52	36:30:49	2	
		02:	41:10	00:00:00	02:41:10	1	
		00:	00:00	00:00:00	00:00:00	1	
		01:	57:52	00:00:00	01:57:52	1	
		01:	27:29	00:00:00	01:27:29	1	
		00:	00:00	00:00:00	00:00:00	1	
Page 1/1							
	二級單	位	(2)				
平均通報審核	時間平均應變	審核時間 平均	醫核時間				
01:08:11	00:00:0	0 01:0	8:11				
[]	一級單位						
半均通報時間	半均應變時間	半均處理時間					
06:30:21	06:04:02	12:34:23					

(7) 轄下單位密碼更動情況

選擇「**轄下單位密碼更動情況」**開啟轄下單位密碼更新狀況系統,將顯 示出所有轄下單位的連絡人密碼更新狀況,如圖18。

表査詞系統 reloped By TACERT 連調 MG67軍 事件専列表	EWA列表 事件和型版計	格下單位他碼更動情況 DDOS清洗系統			
東 (千一東)前於東					
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
	2017-08-17 16:34:43	2017-08-18 13:28:30	2017-08-17 16:22:19		
	2017-08-16 10:55:01	2017-08-16 10:58:15	2017-08-16 10:59:40	2017-08-16 11:02:51	2017-08-16 11:05:51
	2016-09-02 15:15:16	2017-09-19 14:07:52	2016-08-23 11:03:37		
	2018-04-16 15:12:43	2015-09-08 10:05:57			
	2017-08-14 10:56:52	2016-08-18 14:02:12	2014-10-07 09:37:35	2014-10-03 11:15:51	
	2017-08-14 08:34:59	2018-04-17 11:52:33			2017-10-23 09:00:07
	2015-09-09 17:11:55	2015-09-10 17:04:19	2015-09-11 15:25:01		1
	2017-08-24 08:46:21	2017-09-04 17:28:37	2017-08-28 08:37:18	2017-08-28 07:51:44	2017-08-28 07:52:59
	2015-12-23 10:23:25	2015-12-23 10:25:41	2015-12-23 10:32:45		
	2017-08-24 11:31:34	2017-06-06 15:43:03	1		2015-10-12 15:46:31
	2015-12-23 10:23:25 2017-08-24 11:31:34	2015-12-23 10:25:41 2017-06-06 15:43:03	2015-12-23 10:32:45		2015-10-12 15:46:31

圖 18

(8) DDoS 清洗系統(DDoS 清洗服務申請系統)

STEP 1.

A.選擇「**DDoS 清洗系統**」開啟 DDoS 清洗服務申請系統,如圖 19 中 ①所示。

B.若要申請 DDoS 清洗服務,點選「新增申請單」,如圖 19 中②所示。

報表查	詢系統 d By TACER				($\widehat{\mathbb{D}}$				L	
OID查询	威脅名單	事件审判表	EWA列表	\$ff-\$0588.01	轄下單位密碼更動情況	DDOS清洗糸鏡					a series deserves
						(2	新增申請單				
编辑			申請時間		清洗印		通訊協定	通訊埠	狀態		
pr 1/1								 	 		
							圖 19				

STEP 2.

點選「新增申請單」後,系統產生如圖 20 所示的表單,平台會自動篩 選出其轄下的連線單位列表供使用者選擇,使用者將相關資訊(*為必填 欄位)填入「送出」即可。

清洗IP*		
單位名稱*	教育部	•
通訊協定*	TCP V	
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)	

圖 20 DDOS 清洗申請單表單內容

STEP 3.檢視 DDoS 工單資訊

A. 點選「DDOS 清洗系統」功能將顯示所有 DDOS 工單資訊,如圖 21 所示,其中「狀態」說明如下。

狀態:待處理(二線人員新增DDOS工單) 處理中(SOC人員正在處理) 處理完成(已處理完成) 失敗(SOC處理該工單失敗,無法清洗)

	<mark>報表査</mark> Develope	<mark>詢系統</mark> d By TACER	т					_				
	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	DDOS清洗	功能			
								新增申請單				
	語就	102017-02-151	11:19:11	申詞問		140	清洗IP	tcp	通訊藝定	通 調埠	狀態 待處理	檢視
Paj	șe 1/1											
											1.将處理 2.處理中 3.處理完成 4.處理失敗	

圖 21 檢視 DDoS 工單資訊

B. 點選「檢視」即可查詢該工單,如圖 22 所示,其中「回覆意見」為 SOC 對於該 DDOS 工單的回覆(例如:無法清洗的原因)。

編號 12 申請時間 2017-03-07 09:52:35 清洗IP 通訊協定 tcp 服務說明 WEB 通訊埠 80 狀態 待處理 申請理由 // // // // // // // // // // // // //			close or Esc Key
申請時間 2017-03-07 09:52:35 清洗IP	編號	12	
清洗IP Image: Constraint of the second of	申請時間	2017-03-07 09:52:35	
通訊協定 tcp 服務說明 WEB 通訊埠 80 狀態 待處理 申請理由 ////////////////////////////////////	清洗 <mark>IP</mark>		
服務說明 WEB 通訊埠 80 狀態 待處理 申請理由 遭受攻擊 回覆意見 ////////////////////////////////////	通訊協定	tcp	
通訊埠 80 狀態 待處理 申請理由 遭受攻擊 回覆意見	服務說明	WEB	
狀態 待處理 申請理由 遭受攻撃 回覆意見	通訊埠	80	
申請理由 遭受攻撃 回覆意見	狀態	待處理	
凹復意見	申請理由		
	回復意見	//	

STEP 4. 教育機構資安通報平台自動產行「自行通報」事件單 當 SOC 中心完成清洗後,會登入 DDoS 清洗系統將工單狀態改為「處理完 成」,此時平台會自動產生一張自行通報事件單(如圖 23 所示)至「教育機 構資安通報應變平台」,連線單位需依照「教育機構資安通報應變流程」完 成填寫通報應變->二線區縣市網路中心通報審核->TACERT 團隊通報審核, 此 DDoS 攻擊事件單才算完整結案。

The black of the		70 Hunt PC	Lassa	1
發佈編號	TANET- DDOS- 2018491673	發佈時間	2018-04- 09 16:10:29	
事件類型	其它類型的入 侵攻擊	發現時間	2018-04- 09 16:07:03	
事件主旨	貴單位遭受外部	DDOS攻擊		
事件描述	貴單位所申請的	DDOS清洗服務	务已完成清洗	
手法研判	無			
處理建議				建議實單位觀察是否仍持續受到DDOS攻 擊的影響,請點選INT事件類型中的其它,並 輸入DDOS字樣
參考資料				
1. 通報型	態:	自行通知	PHE .	
生物通知的	藍路孝 :	TANET	-DDOS-2018	491673
C3 /14 ADATICA				
2. 事件發	生時間:	2018-0	04-09 16:07:	:03
3. 設備資	料:			
	I P 位背	f:		
	網際網路位置	£:		ŕ
	設備 <u>密</u> 脾、機和	80 :		
	0, C (H) (R) ((H) (R) (H) (R) (H) (R) (H) (R) (R) (R) (R) (R) (R) (R) (R) (R) (R	E		
	作業系統	九		
	受駭應用軟飾	豊 :		
已裝置	之安全防護軟備	豊:		
		防毒軟體防火牆	檀: :	