

區網會議

史詩妤

113.6.25





CONTENTS

01

宣導事項

02

資安通報

03

弱掃平台

Logo Here



01

宣導事項



宣導事項

- 如果有發生資安事件請自行通報。
- 通報要在**1**小時內完成。
- 應變時間
 - 1~2級事件**72**小時內
 - 3~4級事件**36**小時內

Logo Here



02

資安通報



教育機構資安通報平台



網址:

<https://info.cert.tanet.edu.tw/prog/index.php>

- 更新聯絡人資訊
- 定期修改密碼
- 通報與應變

教育機構資安通報平台

- 更新聯絡人資訊

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱:臺北區域網路中心(1)
使用者:李墨軒

主管機關:臺北區域網路中心(1)
聯絡電話:02-3366-5513#
E-Mail:judyshih@ntu.edu.tw

教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw

回首頁
修改個人資料
修改資安長資料
登出

通報
通報/應變
自行通報
事件單處理狀態

| 事件單編號 | 發佈時間 | 距通報時間(小時) | 流程 |
|--------------------------|------|-----------|----|
| Page 1/1 | | | |
| 尚有75張EWA預警單未處理，請按此查閱相關資訊 | | | |

教育機構資安通報平台

- 更新聯絡人資訊

回首頁
修改個人資料
修改資安長資料
登出

通報

通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計

| 帳號名稱 | 帳號狀態 | 帳號管理 | |
|---------|------|--------------------------------|----|
| 第三資安連絡人 | 已開啟 | <input type="checkbox"/> 關閉此帳號 | 送出 |
| 第四資安連絡人 | 已關閉 | <input type="checkbox"/> 開啟此帳號 | 送出 |
| 第五資安連絡人 | 已關閉 | <input type="checkbox"/> 開啟此帳號 | 送出 |

[帳號管理說明文件下載](#)

教育機構資安通報平台

- 通報與應變
- 通報時間1小時內

| 事件單編號 | 單位名稱 | 發佈時間 | 距通報時間 | 流程 |
|---------------|------|---------------------|-------|------|
| <u>203374</u> | | 2022-12-12 08:15:23 | 29 | 新進工單 |

教育機構資安通報平台

- 通報與應變
- 通報時間查詢

回首頁
修改個人資料
修改資安長資料
登出

通報

通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
事件統計
演練資訊
情資資料下載

事件統計

開始日期: 結束日期: 查詢

| 資安事件數 | 平均通報處理時間 | 平均應變處理時間 | 平均全部處理時間 |
|-------|----------|----------|----------|
| 209 | 00:00:52 | 00:12:25 | 00:13:17 |

Page 1/1

教育機構資安通報平台

- 通報與應變
- 事件附檔下載

教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw

工單狀態

事件單編號 搜尋

第一頁 | 上一頁 | 下一頁 | 最終頁

| 事件編號 | 發佈編號 | 單位 | IP | LOG檔 |
|--------|---|-------------|----|------|
| 210700 | NTUSOC-105-202404-ntuasoc-20240416-081801 | 臺北區域網路中心(1) | | 下載 |
| 210240 | NISAC-105-202402-00000062 | 臺北區域網路中心(1) | | 下載 |
| 208999 | TWCERTCC-105-202311-00000096 | 臺北區域網路中心(1) | | 下載 |
| 208772 | TWCERTCC-105-202310-00000575 | 臺北區域網路中心(1) | | 下載 |
| 207753 | TWCERTCC-105-202309-00000255 | 臺北區域網路中心(1) | | 下載 |
| 206915 | NTUSOC-105-202308-403-0889 | 臺北區域網路中心(1) | | 下載 |

Logo Here



03

弱掃平台



弱掃平台

網址:

<https://evs.ncku.edu.tw/>

- 各校有一組帳密
- 可自行申請掃描

弱掃平台

- 定期弱點掃描

| 辦理項目 | 辦理內容 | A級單位 | B級單位 | C級單位 | D級單位 |
|-------|----------------------|------|------|-------|------|
| 安全性檢測 | 全部核心資通系統 網站安全弱點檢測 | 每年2次 | 每年1次 | 每2年1次 | X |

弱掃平台

- 區網中心網站弱掃數量統計

| 年度 | 臺北一區 | 臺北二區 | 桃園區 | 竹苗區 | 新竹區 | 臺中區 | 南投區 | 雲嘉區 | 臺南區 | 高屏澎區 | 宜蘭區 | 花蓮區 | 臺東區 | 小計 |
|-----|------|------|-----|-----|-----|-----|-----|-----|-----|------|-----|-----|-----|------|
| 108 | 278 | 159 | 35 | 374 | 98 | 142 | 30 | 265 | 163 | 508 | 22 | 26 | 30 | 2130 |
| 109 | 462 | 133 | 36 | 88 | 270 | 257 | 52 | 254 | 266 | 706 | 59 | 41 | 46 | 2670 |
| 110 | 341 | 151 | 15 | 50 | 128 | 97 | 33 | 199 | 240 | 391 | 61 | 20 | 15 | 1741 |
| 111 | 201 | 177 | 7 | 71 | 142 | 406 | 54 | 235 | 372 | 271 | 82 | 42 | 48 | 2108 |
| 112 | 200 | 180 | 70 | 63 | 68 | 332 | 40 | 339 | 209 | 389 | 63 | 29 | 17 | 1999 |
| 113 | 163 | 108 | 5 | 11 | 5 | 262 | 13 | 62 | 185 | 171 | 34 | 17 | 20 | 1056 |

弱掃平台

- 網站弱掃後處理建議
 1. 務必針對中、高風險網站優先修補
 2. 已不須掃描的網站，請至EVS平台註記網站已停用
 - 登入EVS平台→網站弱點檢測→檢測目標→查詢→修改→停用

弱掃平台

• 網站弱掃後常見異常狀況

- 掃描時間過長，系統自動中斷掃描。
- 弱掃報告仍然有效，建議依報告修補弱點後，再進行複測。

| 排程日期 | 檢測狀態 | 弱掃狀態 | 高風險 | 中風險 | 低風險 | 合規 | 嚴重等級 | 更新日期 | 檢測結果 | 弱掃報告 |
|------------------|------|-----------|-----|-----|-----|----|------|------------------|------|------|
| 2021-12-06 01:00 | 執行失敗 | aborting | 22 | 8 | 8 | 6 | III | 2021-12-06 06:18 | 瀏覽 | 報告下載 |
| 2020-01-30 01:00 | 執行完成 | completed | 31 | 136 | 36 | 21 | III | 2020-01-30 06:19 | 瀏覽 | 報告下載 |
| 2020-01-09 09:00 | 執行失敗 | aborting | 24 | 108 | 25 | 16 | III | 2020-01-09 16:14 | 瀏覽 | 報告下載 |

檢測失敗可能原因：

1. 掃描時間超過7小時
2. 網站於該時段過於忙碌，無法回應掃描的連線要求
3. 防火牆-等資安設備阻擋掃描之IP(163.28.114.8, 163.28.114.9, 140.116.221.36~39, 163.28.52.142, 163.28.84.125)

無法下載報告原因：

1. *異常：掃描時間少於1分鐘，各風險數為0
2. *異常：各風險數為null
3. *逾期：超出可下載時間(排程日起60天內)

排程日期：2021-12-06 01:00

| 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 |
|------|----------------------------------|------------------|--|---|-----------------------------|
| | 開始: 2021-12-06 01:00 06 08:07 | 執行失敗 aborting | • OS: Unknown • Server: • Technologies: • 響應式網頁 | • 請求數量:179822 • 網址數量:286 • 平均回應量秒:2 | 高風險: 22 中風險: 8 低風險: 8 合規: 6 |

共427分鐘

弱掃平台

• 網站弱掃後常見異常狀況

- 不論執行完成/失敗，只要掃描少於1分鐘，不會產生弱掃報告

1. 掃描時間太短有可能是掃描異常，因此建議排查之可能原因：資安設備阻擋、該網址/IP未開啟Web服務、網路異常...

| 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 | 檢測結果 | 弱掃報告 |
|------------------|------|-----------|-----|-----|-----|----|------|------------------|------|------|
| 2021-12-03 01:00 | 執行完成 | completed | | | | | 安全 | 2021-12-03 01:18 | 瀏覽 | *異常 |
| 2021-11-03 01:00 | 執行完成 | completed | | | | | 安全 | 2021-11-03 01:17 | 瀏覽 | *異常 |
| 2021-08-06 01:00 | 執行完成 | completed | 1 | 1 | 6 | 5 | 高 | 2021-08-06 01:35 | 瀏覽 | 報告下載 |

檢測失敗可能原因：

1. 掃描時間超過7小時
2. 網站於該時段過於忙碌，無法回應掃描的連線要求
3. 防火牆..等資安設備阻擋掃描之IP(163.28.114.8, 163.28.114.9, 140.116.221.36~39, 163.28.52.142, 163.28.84.125)

無法下載報告原因：

1. *異常：掃描時間少於1分鐘，各風險數為0
2. *異常：各風險數為null
3. *逾期：超出可下載時間(排程日起60天內)

排程日期：2021-11-03 01:00

| 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 |
|--|-------------------|---------------------------------|----------------------------|------|---------|
| 開始: 2021-11-03 01:00 結束: 2021-11-03 01:01 | 執行完成 completed | OS: Server: Technologies. | 請求數量: 網址數量:1 平均回應毫秒. | 共1分鐘 | |



**THE END
THANK YOU**