區網會議

史詩妤

113.12.30

CONTENTS

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

- 填寫/修改資安長資訊
- 更新聯絡人資訊
- 通報與應變

教育機構資安通報平台

- 填寫/修改資安長資訊

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
203374	[redacted]	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

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

教育機構資安通報平台

- 113年度1~11月台北區網1資安單事件分類 Top 10

資安單事件分類	計數
內部主機疑似進行惡意程式連線	667
內部主機進行惡意程式連線	475
內部主機疑似進行挖礦程式連線	292
[漏洞通報]Wordpress伺服器資安漏洞通報(xmlrpc.php)	72
[漏洞通報]物聯網設備Fortinet存在CVE漏洞，請盡速更新。	71
內部主機疑似連線至惡意中繼站	61
[重大漏洞通報]Windows伺服器PHP 遠端程式碼執行 (CVE-2024-4577) - PHP CGI 參數注入弱點	53
內部主機嘗試密碼暴力破解	44
[漏洞通報]FTP伺服器疑似可使用匿名(弱密碼)登入	36
內部主機疑似資訊洩漏	29

Logo Here

03

弱掃平台

網站弱掃平台

網址:
https://evs.ncku.edu.tw/

- 各校有一組帳密
- 可自行申請掃描

網站弱掃平台

- **申請弱掃注意事項**

1. 申請弱掃網站應有**SSL憑證**
2. 優先掃描**核心系統、含個資資料網站**
3. 大學、大專院校、高中職：5個

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

網站弱掃平台

- 申請弱掃注意事項

4. 避免同時段掃描多個網站

因弱掃時會快速發送**大量的請求(requests)**

有可能影響受測網站效能，或資安設備的異常狀況

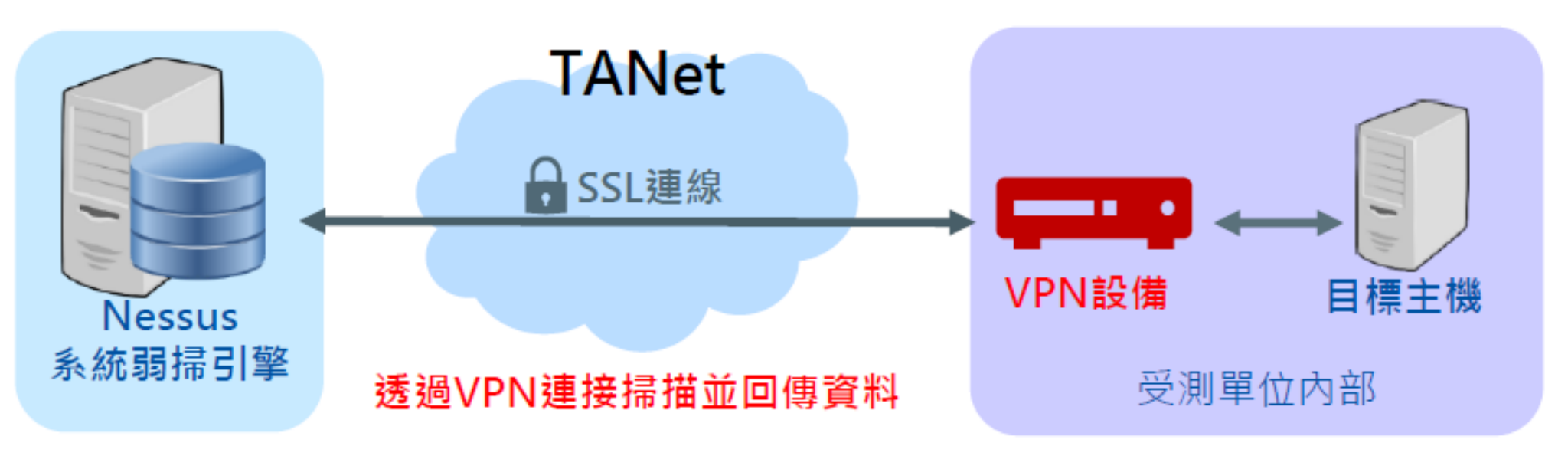
建議**避免同單位多個網站都集中在同一時段弱掃**

網站平均回應時間	29毫秒
平均請求數量	155794個

→ 平均每秒發送43個請求

系統弱掃平台

- 成大弱掃團隊提供系統弱掃服務



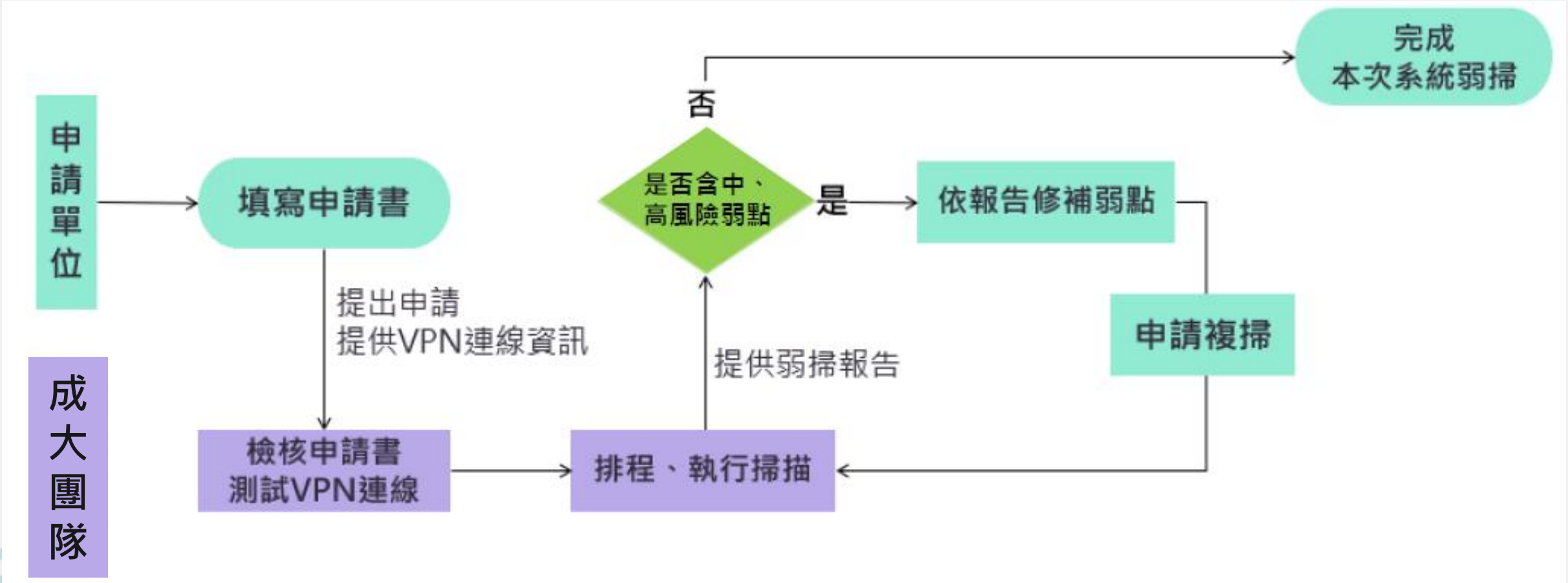
系統弱掃平台

- 申請系統弱掃須知

1. 請學校提前3週寄信到成大弱掃團隊官方信箱 evs_service@mail.moe.gov.tw 申請掃描，說明有幾個系統需要掃描、預計排程日期
2. 成大單位會回信提供申請掃描文件，請學校回填申請資料
3. 資料審核通過後，提供 VPN 連線資訊，即按排程時間掃描
4. 掃描完成後提供系統弱掃報告

系統弱掃平台

- 系統弱掃服務流程



系統弱掃平台

- 系統弱掃報告範例

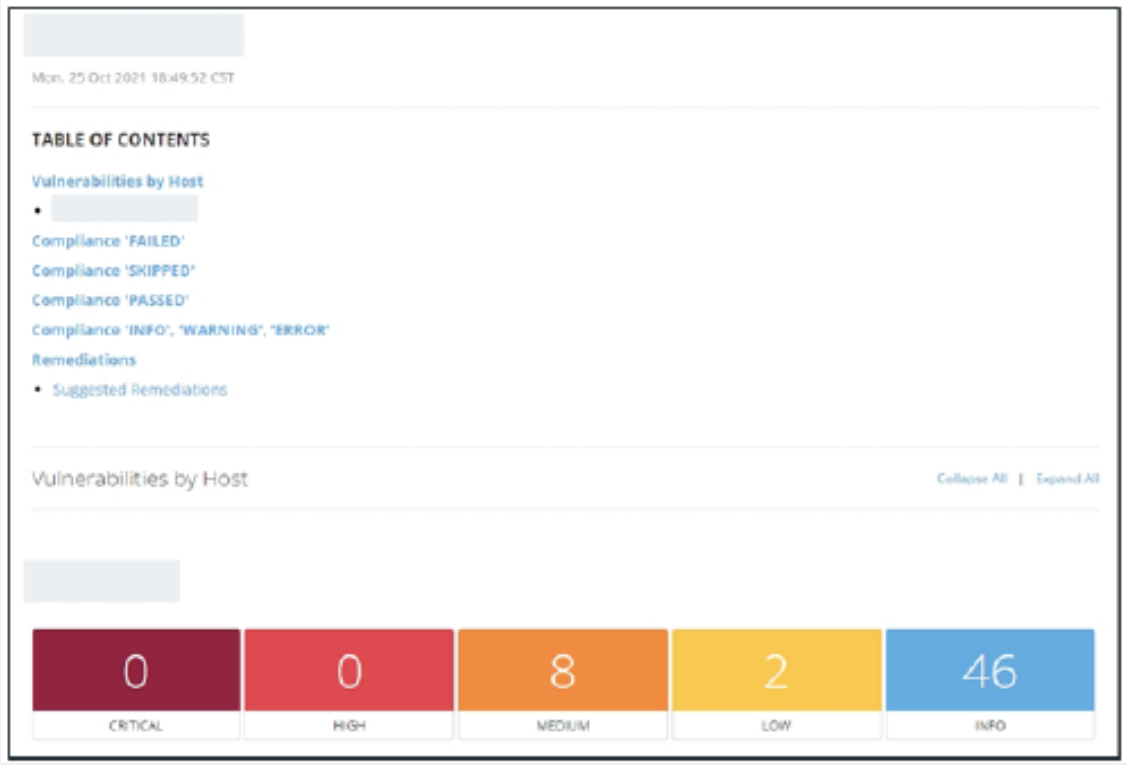

Mon, 25 Oct 2021 18:49:52 CST

TABLE OF CONTENTS

Vulnerabilities by Host

- [redacted]

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

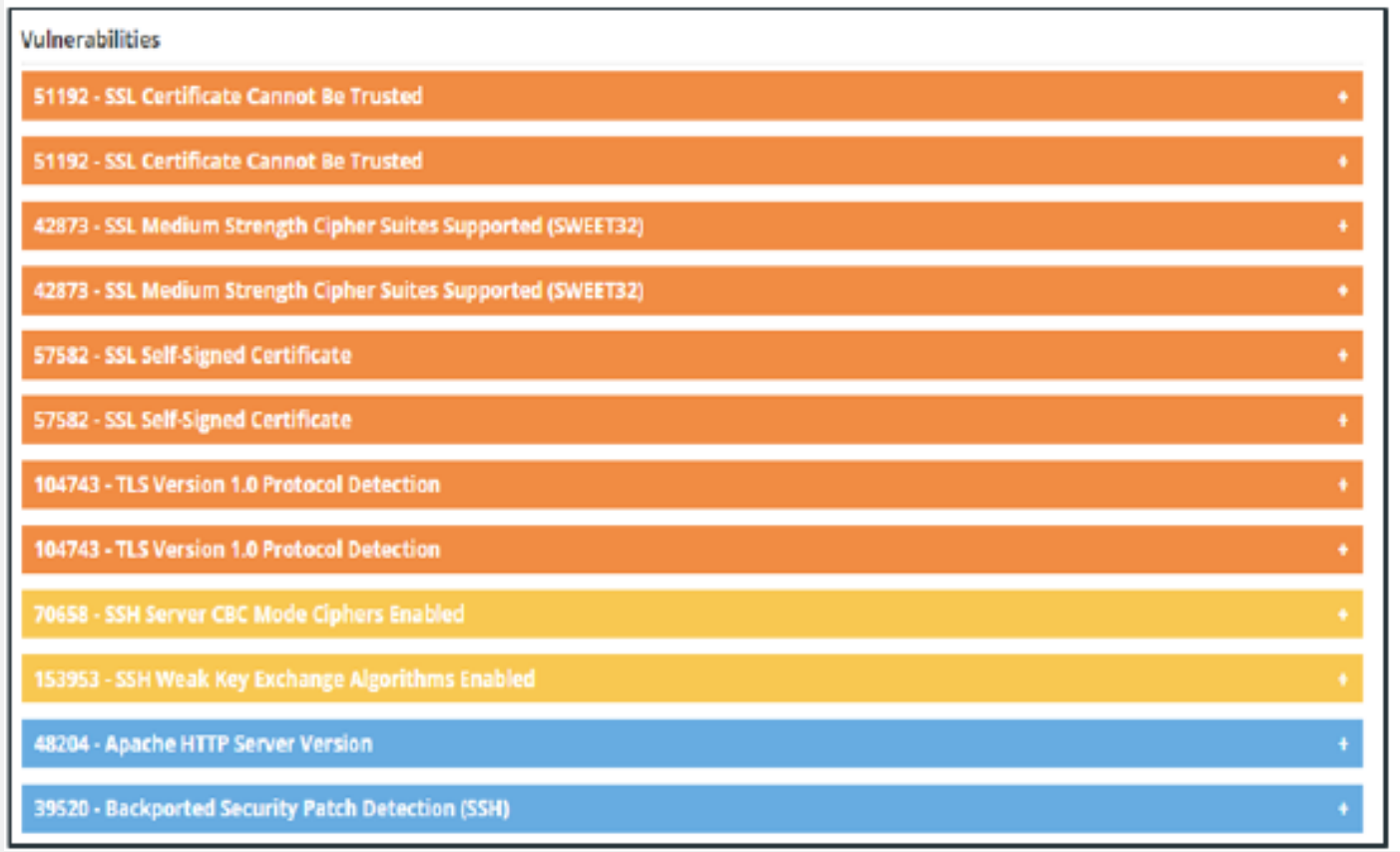
- Suggested Remediations

Vulnerabilities by Host

Collapse All | Expand All

[redacted]

0	0	8	2	46
CRITICAL	HIGH	MEDIUM	LOW	INFO


Vulnerabilities

51192 - SSL Certificate Cannot Be Trusted

51192 - SSL Certificate Cannot Be Trusted

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

57582 - SSL Self-Signed Certificate

57582 - SSL Self-Signed Certificate

104743 - TLS Version 1.0 Protocol Detection

104743 - TLS Version 1.0 Protocol Detection

70658 - SSH Server CBC Mode Ciphers Enabled

153953 - SSH Weak Key Exchange Algorithms Enabled

48204 - Apache HTTP Server Version

39520 - Backported Security Patch Detection (SSH)

THE END
THANK YOU