

區網會議

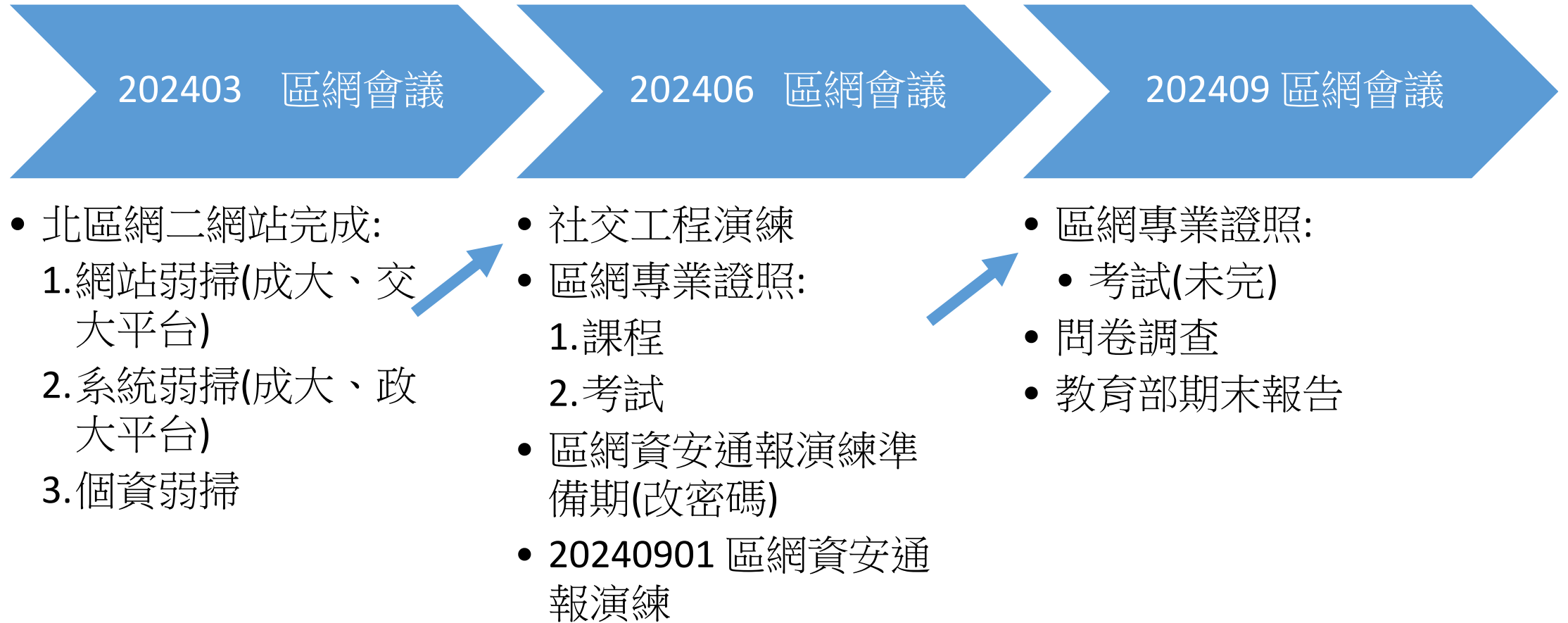
資安

報告: 李明潔
20240925

outline

- 北區網二記事
- 弱掃的分類及資源
- 2024弱掃的行程
- 弱掃前注意事項
- 網站弱掃執行狀況
 - IOT資安

北區網二記事



弱掃的分類及資源

- Web應用程式安全測試

- Burp Suit
- OWASP ZAP
- **HCL AppScan (交大)**
- **Acunetix (成大)**
- Fortify WebInspect

可掃三種特殊狀況:

1. 沒有https網域憑證
2. 開發中(還沒完成的網站)
3. 登入網站

- 系統弱掃

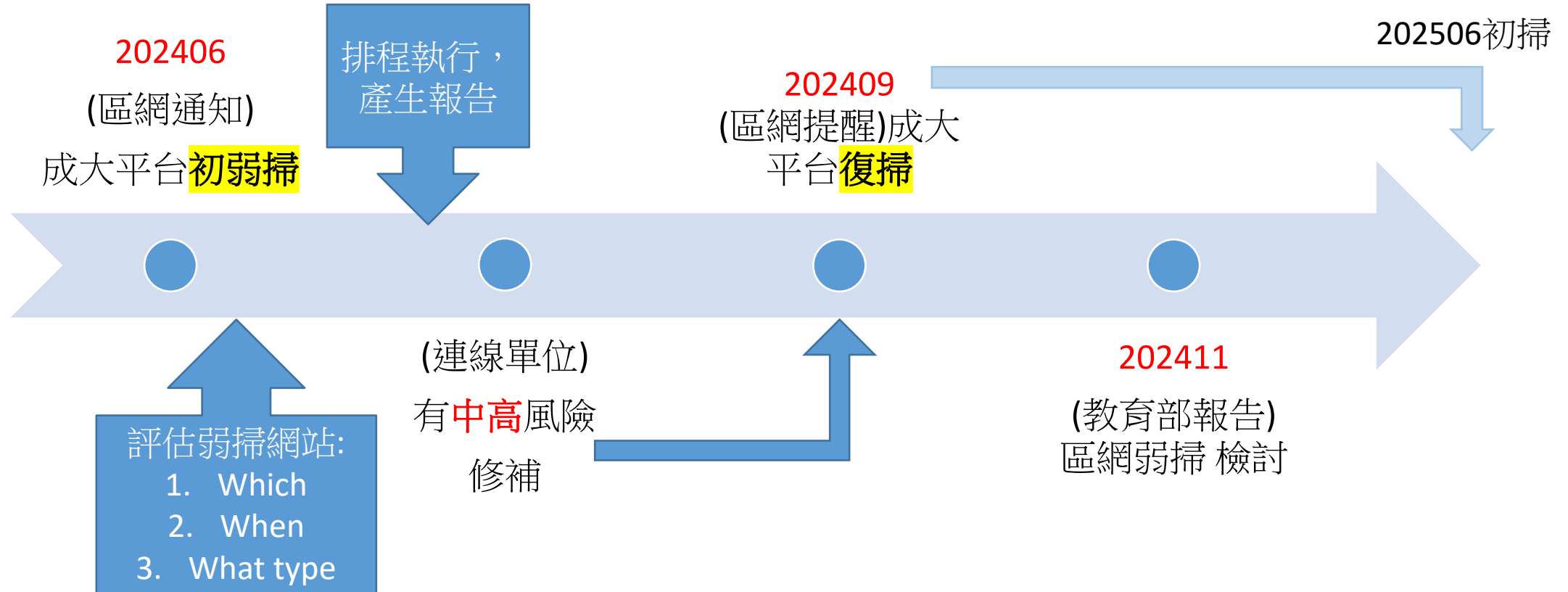
- **Nessus (向成大申請)**
- Nessus (向政大申請) (更新)
- OpenVAS

教育部提供的免費資源

- 個資弱掃

- **PrivacyID 檔案型個資盤點工具 (向成大申請)**

2024弱掃的行程



• Web應用程式安全測試 弱掃前注意事項

- 請完成備份網站程式、資料庫，設定檔最重要，以下弱掃前置作業檢核
- 備份：
 - 弱掃前，請備份網站，因弱掃可能造成資料遺失毀損等狀況。
- 防火牆允許弱掃平台來源ip:
 - 交大:140.113.27.234 ，成大: 163.28.52.142(主)，163.28.114.9 (備援)
- 關閉防毒軟體
 - 建議掃描期間關閉
- 整理網站目錄
 - 網站的漏洞往往藏在未整理的目錄裡及檔案太多掃描太久自動中斷掃描，建議整理
- 將弱掃排程在非必要服務時間，或公告弱掃時間
 - 因弱掃時會影響網站服務效能，建議排在非必要服務時間弱掃
 - 若無法避開服務時間，請提前公告網站弱掃的時間，提醒使用者該時段網站服務有可能會受影響

網站弱掃執行狀況(1/2)

No	Tr2rc 連線單位	平台	2024	2024 高/中	2023 及以前	備註
1	世華	成大	2024/09/11	5/25		
2	華	成大	2024/05/29	0/2		執行失敗
		交大	2024/01/10	1/190		
3	東	成大	2024/06/20	1/5		
4	中	成大			2023/11/14	
5	醒	成大	2024/07/11	1/16		
6	聖	交大	2024/01/16	0/43		
7	景	成大	2024/06/13	0/3		
8	臺	市科大	2024/09/20	0/4		
9	警				無	
10	格		2024/06/24	0/3		
11	台	育學院			2023-09-28	
12	耕	康管理專科			2021/07/02	
14	馬	學院	2024/05/29	1/33	2023-09-04	
15	德	健康學院	2024/08/01	0/0	2023-10-20	
16	基	台灣浸會神學院	2024/08/20	1/20		
17	海		2024/06/20	0/0		
18	穀		2024/06/21			
19	莊				無	
20	崇				無	
21	復				無	2021-10-25 有排
22	景	成大	2024/06/07	0/7		
23	開	成大	2024/06/14	6/2		
24	秀	(特教通報網)			2022/12/26	
25	豫		2024/07/15	0/3		
26	淡	成大	2024/06/21	0/1		


Note: mjlee 20240925

網站弱掃執行狀況(2/2)

No	Tp2rc 連線單位	平台	2024	2024 高/中	2023 及以前	備註
27	政大附中	成大	2024/03/20	0/0		
28	基大附中	成大	2024/08/16	0/0		
29	海大附中	成大	2024/07/09	0/0		
30	醒大附中	成大	2024/06/24	0/15		
31	清大附中	成大	2024/06/03	3/13		
32	餐大工				無	
33	政大國小		2024/07/03			
34	遠大 I 區域網路中心	成大	2024/06/19(已排程)		2023-09-13	
35	政大	交大	2024/07/15	1/9		
36	輔大				2021/11/17	
37	銘大					
38	永大商		2024/05/24	0/2		
	聖心附中				2019/01/01	
39	聖心小學					輔大聖心高中、國小使用相同單位代碼(171308)
40	基大工		2024/03/05	0/0		
41	二大附中		2024/06/25			
42	基大		2024/08/06	0/0		
43	城二家		2024/05/24	18/119/95		執行失敗嚴重風險 16 高風險 119

IOT資安

[南區ASOC通報]ASOC發現政大區網所屬轄下單位，疑似為網路物聯網設備(網路印表機網路攝影機網路IP分享器)，可能...



@narlabs.org.tw

收件者 mjlee@nccu.edu.tw

副本 @nccu.edu.tw; asoc_support@narlabs.org.tw; @mail.moe.gov.tw; @mail.moe.gov.tw

回覆

全部回覆

轉寄

...

2024/9/5 (週四) 上午 02:32

您已於 2024/9/5 下午 04:19 轉寄這封郵件。

政大區網IoT風險清單.xlsx
26 KB

親愛的夥伴您好

主旨	ASOC 發現政大區網所屬轄下單位，疑似為網路物聯網設備(網路印表機\網路攝影機\網路 IP 分享器)，可能存在資安風險，請採取適當管控措施，以提升學術網路資訊安全。
情資名稱	貴單位(政大區網)所屬轄下單位，疑似為暴露在外網之物聯網設備(網路印表機\網路攝影機\網路 IP 分享器)，可能存在資安風險。
內容說明	ASOC 發現貴單位(政大區網)所屬轄下單位，疑似為網路物聯網設備(如網路印表機、網路攝影機、網路 IP 分享器)，可能存在資安風險，請採取適當管控措施，以提升學術網路資訊安全。詳細 IP 清單請參閱附件檔案。
建議措施	1. 請確認該裝置是否需要讓外部 IP 存取，並檢視防火牆規則，避免非經授權之系統存取；若否，則建議移至內部網路並限制特定 IP 才可管理該系統與使用服務。 2. 評估系統上非必要的服務或程式建議移除或關閉。

附件為八月份本次掃到的 IoT 清單，給區網長官參考，若有誤判煩請回報，感謝您。

謝謝 & 問題