02_資安事件及異常紀錄 - 一般 #1095

INCGC-5397-Windows User Account Enabled

2025-11-10 17:46 - Joy Liao

狀態:	Closed-關閉	**開始日期:**	
優先權:	Normal	**完成日期:**	
被分派者:	益利 周	**完成百分比:**	100%
分類:		**預估工時:**	0:00 小時
概述			

歷史

#1 - 2025-11-28 18:15 - 益利 周

- 檔案 clipboard-202511281815-zbp77.png 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

Asset Owner : TWBU
Priority: Low
Description:

Start Time: 2025-08-01 09:06:00 TST
End Time: 2025-08-01 10:06:00 TST
Rule Name: windows_user_account_enabled
Rule Description: This event is always logged after event 4720 - user account creation. This event is logged both for local SAM accounts and domain accounts.
Priority: Low
Risk Score: 20
Log Type: WINEVTLOG
Event Type: USER_CHANGE_PERMISSIONS
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4722
Product Log ID: 1047743497
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
Device Action: ALLOW
Principal Hostname: TAHOAD.tahoho.com.tw
Principal Administrative Domain: TAHOHO
Principal User ID: b10005
Principal Windows SID: S-1-5-21-845223939-707100287-312552118-15112
Principal Subject Logon ID: 0x1a977c1b6
Principal Process PID: 856
Target Administrative Domain: TAHOHO
Target User ID: B10005.admin
Target Windows SID: S-1-5-21-845223939-707100287-312552118-20352
Mitre Tactic: Persistence
Mitre Technique: Account Manipulation

帳號維護 - 新建帳號權限調整

#2 - 2026-01-12 13:07 - Joy Liao

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281815-zbp77.png	52.4 KB	2025-11-28	益利 周