02_資安事件及異常紀錄 - 一般 #1094

INCGC-5393-Windows User Removed From Privileged Security Group

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 18:17 - 益利 周

- 檔案 clipboard-202511281817-tskwd.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 10:17:12 TST
End Time: 2025-08-01 10:17:12 TST
Rule Name: windows_user_removed_from_privileged_security_group
Rule Description: In Active Directory Users and Computers Security Enabled groups are simply referred to as Security groups. AD has 2 types of groups: Security and Distribution. Distribution (security disabled) groups are for distribution lists in Exchange and cannot be assigned permissions or rights. Security (security enabled) groups can be used for permissions, rights and as distribution lists. Global means the group can be granted access in any trusting domain but may only have members from its own domain.
Priority: Low
Risk Score: 50
Log Type: WINEVTLOG
Event Type: GROUP_MODIFICATION
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4729
Product Log ID: 1047857316
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
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 Process PID: 856
Target Administrative Domain: TAHOHO
Target Windows SID: S-1-5-21-845223939-707100287-312552118-15112
Target Group Display Name: Domain Admins
Mitre Tactic: Privilege Escalation
Mitre Technique: Account Manipulation

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-202511281817-tskwd.png	61.5 KB	2025-11-28	益利 周