02_資安事件及異常紀錄 - 一般 #1132

INCGC-14054-Low-Windows User Added In Global Privileged Security Group

2025-11-13 10:18 - 益利 周

狀態:	Closed-關閉	**開始日期:**	2025-11-13
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 - 2025-12-01 11:35 - 益利 周

- 檔案 clipboard-202512011131-5wzrv.png 已新增

- 狀態 從 New-新增 變更為 Resolved-解決

- 被分派者 設定為 益利 周

- 完成百分比 從 0 變更為 100

Asset Owner : TWBU
Priority: Low
Description:

Start Time: 2025-11-06 13:38:12 TST
End Time: 2025-11-06 13:39:12 TST
Rule Name: windows_user_added_in_global_privileged_security_group
Rule Description: The user in Subject: added the user/group/computer in Member: to the Security Global group in Group:.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. This event is only logged on domain controllers.
Priority: Low
Risk Score: 50
Log Type: WINEVTLOG
Event Type: GROUP_MODIFICATION
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4728
Product Log ID: 31357155
Opcode: 0
Channel: Security
Device: TahoSQL
Principal Hostname: TahoSQL
Principal Administrative Domain: TahoSQL
Principal User ID: itservice
Principal Windows SID: S-1-5-21-1136234096-807217459-3798877357-500
Principal Subject Logon ID: 0x51b321c
Principal Process PID: 980
Target Administrative Domain: TahoSQL
Target Windows SID: S-1-5-21-1136234096-807217459-3798877357-1003

伺服器 TAHOSQL 帳號維護 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-202512011131-5wzrv.png	62.4 KB	2025-12-01	益利 周