02_資安事件及異常紀錄 - 一般 #1133

INCGC-14069-Medium-Windows Tgs Requests Without Preceding Tgt Requests

2025-11-13 10:19 - 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 11:45 - 益利 周

- 檔案 clipboard-202512011139-un5pi.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: Medium
Description:

Start Time: 2025-11-07 09:21:00 TST
End Time: 2025-11-07 09:51:00 TST
Rule Name: Windows_TGS_Requests_without_Preceding_TGT_Requests
Rule Description: This rule aims to identify potential anomalies or security issues where a TGS request appears without the corresponding TGT request, which could indicate unauthorized or unusual behavior.
Priority: Medium
Risk Score: 20
Log Type: WINEVTLOG
Event Type: USER_UNCATEGORIZED
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4769
Product Log ID: 1417186030
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
Principal IP: 192.168.4.49
Principal Port: 49188
Principal Hostname: TAHOAD.tahoho.com.tw
Principal Process PID: 872
Target Administrative Domain: TAHOHO.COM.TW
Target User ID: lochengta.admin
Target Windows SID: S-1-5-21-845223939-707100287-312552118-20227

管理者帳號 lochengta.admin 登入帳號驗證時 缺少 TGT 的 TGS 請求.

此為正常登入行為.
("缺少 TGT 的 TGS 請求" 係因 AD 缺失改善調整導致,尚在調整修正中)

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202512011139-un5pi.png	48.2 KB	2025-12-01	益利 周