02_資安事件及異常紀錄 - 一般 #1129

INCGC-14139]-Medium-Windows Admin Account Logon To Multiple Servers Within 1 Hour

2025-11-13 10:14 - 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 - 2025-11-28 18:31 - 益利 周

- 檔案 clipboard-202511281830-ceoj3.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: 2025-11-12 13:24:00 TST
End Time: 2025-11-12 14:24:00 TST
Rule Name: Windows_Admin_Account_Logon_To_Multiple_Servers_within_1_hour
Rule Description: This use case detects Admin account logon to more than 5 Servers in less than 1 hour
Priority: Medium
Log Type: WINEVTLOG
Event Type: USER_LOGIN
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4624
Product Log ID: 88149947
Opcode: 0
Channel: Security
Device: TahoSales.tahoho.com.tw
Device Action: ALLOW
Principal IP: 192.168.4.101
Principal Hostname: TahoSales.tahoho.com.tw
Principal Administrative Domain: TAHOHO
Principal User ID: TAHOSALES$
Principal Windows SID: S-1-5-18
Principal Subject Logon ID: 0x3e7
Principal Process PID: 0xafc
Target Administrative Domain: TAHOHO
Target User ID: lochengta.admin
Target Windows SID: S-1-5-21-1350993402-1745725349-3412450649-1185
Target Process File Full Path: User32

管理帳號 在1 小時內登入多台設備

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281830-ceoj3.png	47.9 KB	2025-11-28	益利 周