02_資安事件及異常紀錄 - 一般 #1111

INCGC-12779-Windows Brute Force Attempt Detected Logon Type 3

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 18:19 - 益利 周

- 檔案 clipboard-202511281820-tu6y3.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: Medium
Description:

Start Time: 2025-10-08 15:38:00 TST
End Time: 2025-10-08 15:48:00 TST
Rule Name: Windows_Brute_Force_Attempt_Detected_Logon_Type_3
Rule Description: Logon Type 3 Bruteforce
Risk Score: 90
Log Type: WINEVTLOG
Event Type: USER_LOGIN
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4625
Product Log ID: 1308915716
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
Principal IP: 192.168.4.249
Principal Port: 65415
Principal Hostname: TAHOAD.tahoho.com.tw
Principal Windows SID: S-1-0-0
Principal Subject Logon ID: 0x0
Principal Process PID: 0x0
Target Administrative Domain: ULPU
Target User ID: sztmaster
Target Windows SID: S-1-0-0
Target Process File Full Path: NtLmSsp

上水 網域帳號連線測試

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281820-tu6y3.png	37.6 KB	2025-11-28	益利 周