02_資安事件及異常紀錄 - 一般 #1135

INCGC-14061]-Low-Windows Bruteforce Attempt Detected

2025-11-13 10:22 - 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

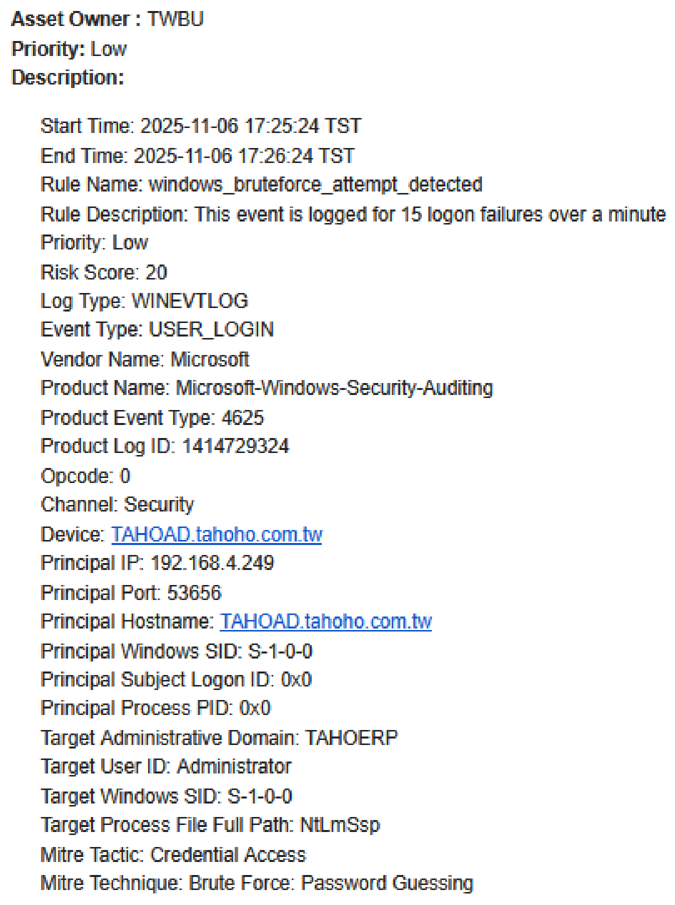
#1 - 2025-12-01 11:59 - 益利 周

- 檔案 clipboard-202512011153-4jna7.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 17:25:24 TST
End Time: 2025-11-06 17:26:24 TST
Rule Name: windows_bruteforce_attempt_detected
Rule Description: This event is logged for 15 logon failures over a minute
Priority: Low
Risk Score: 20
Log Type: WINEVTLOG
Event Type: USER_LOGIN
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4625
Product Log ID: 1414729324
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
Principal IP: 192.168.4.249
Principal Port: 53656
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: TAHOERP
Target User ID: Administrator
Target Windows SID: S-1-0-0
Target Process File Full Path: NtLmSsp
Mitre Tactic: Credential Access
Mitre Technique: Brute Force: Password Guessing

網域認證失敗 導致網域帳號登入錯誤. 排定重新進行網域認證 修復錯誤.

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202512011153-4jna7.png	41.6 KB	2025-12-01	益利 周