02_資安事件及異常紀錄 - 非法入侵 #1125

INCGC-13930-Windows Bruteforce Attempt Detected

2025-11-10 17:46 - Joy Liao

狀態:	Resolved-解決	**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
版本:			

概述

歷史

#1 - 2025-11-28 15:48 - 益利 周

- 檔案 clipboard-202511281537-0hyxw.png 已新增

- 追蹤標籤 從 一般 變更為 非法入侵

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

Details 2025-11-03 16:43

Priority
Low

Description
Start Time: 2025-11-03 16:15:12 TST
End Time: 2025-11-03 16:16:12 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: 87736120
Opcode: 0
Channel: Security
Device: TahoSales.tahoho.com.tw
Principal IP: 10.10.150.14
Principal Port: 60760
Principal Hostname: TahoSales.tahoho.com.tw
Principal Windows SID: S-1-0-0
Principal Subject Logon ID: 0x0
Principal Process PID: 0x0
Target Administrative Domain: RPABOOT
Target User ID: itservice
Target Windows SID: S-1-0-0
Target Process File Full Path: NtLmSsp
Mitre Tactic: Credential Access
Mitre Technique: Brute Force: Password Guessing

IT Group
TWBU

檔案

clipboard-202511281537-0hyxw.png	53.5 KB	2025-11-28	益利 周