02_資安事件及異常紀錄 - 一般 #1113

INCGC-12799-Windows Domain Policy Changed

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 17:32 - 益利 周

- 檔案 clipboard-202511281732-d8xds.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: Low
Description:

Start Time: 2025-10-08 22:22:13 TST
End Time: 2025-10-08 22:22:13 TST
Rule Name: windows_domain_policy_changed
Rule Description: This computer's Security Settings i.e Account Policy or Account Lockout Policy policy was modified - either via Local Security Policy or Group Policy in Active Directory
Priority: Low
Risk Score: 50
Log Type: WINEVTLOG
Event Type: SETTING_MODIFICATION
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4739
Product Log ID: 18044378
Opcode: 0
Channel: Security
Device: TAHO-HR.tahoho.com.tw
Principal Hostname: TAHO-HR.tahoho.com.tw
Principal Administrative Domain: TAHOHO
Principal User ID: TAHO-HR$
Principal Windows SID: S-1-5-18
Principal Subject Logon ID: 0x3e7
Principal Process PID: 864
Target Administrative Domain: TAHO-HR
Target Windows SID: S-1-5-21-1213605369-3782942624-4235927201
Mitre Tactic: Defense Evasion
Mitre Technique: Indicator Removal

環境設定調整

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281732-d8xds.png	51.1 KB	2025-11-28	益利 周