02_資安事件及異常紀錄 - 一般 #1136

INCGC-13984-Low-Windows Scheduled Task Created

2025-11-13 10:24 - 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 13:03 - 益利 周

- 檔案 clipboard-202512011303-uvqln.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

Details 2025-11-04 17:33

Priority
Low

Description
Start Time: 2025-11-04 17:09:51 TST
End Time: 2025-11-04 17:09:51 TST
Rule Name: windows_scheduled_task_created
Priority: Low
Risk Score: 20
Log Type: WINEVTLOG
Event Type: SCHEDULED_TASK_CREATION
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4698
Product Log ID: 1405353788
Opcode: 0
Channel: Security
Device: TAHOAD.tahoho.com.tw
Principal Hostname: TAHOAD.tahoho.com.tw
Principal Administrative Domain: TAHOHO
Principal User ID: 860712.admin
Principal Windows SID: S-1-5-21-845223939-707100287-312552118-15170
Principal Subject Logon ID: 0x9a78dd89
Principal Process PID: 872
Mitre Tactic: Persistence
Mitre Technique: Scheduled Task/Job

IT Group
TWBU

result
Automated tesks triggered by user login

使用者登入,相關排程自動產生.

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202512011303-uvqln.png	51.4 KB	2025-12-01	益利 周