02_資安事件及異常紀錄 - 一般 #1103

INCGC-9218-Windows Multiple Failed Login Attempts Then Success

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 17:54 - 益利 周

- 檔案 clipboard-202511281755-trzjk.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: High
Description:

Start Time: 2025-09-08 10:47:06 TST
End Time: 2025-09-08 10:50:06 TST
Customer Name: Veolia
Rule Name: Windows_multiple_failed_login_attempts_then_success
Rule Description: Detects multiple failed login attempts followed by successful login
Priority: High
Risk Score: 70
Log Type: WINEVTLOG
Event Type: USER_LOGIN
Vendor Name: Microsoft
Product Name: Microsoft-Windows-Security-Auditing
Product Event Type: 4624
Product Log ID: 889034681
Opcode: 0
Channel: Security
Device: GSVR.tahoho.com.tw
Device Action: ALLOW
Principal Hostname: GSVR.tahoho.com.tw
Principal Windows SID: S-1-0-0
Principal Subject Logon ID: 0x0
Principal Process PID: 0x0
Target Administrative Domain: ULPU.LOCAL
Target User ID: klmaster
Target Windows SID: S-1-5-21-962174734-806159982-315997048-1635
Target Process File Full Path: Kerberos
Mitre Tactic: Credential Access
Mitre Technique: Brute Force: Password Guessing

上水網域帳號連線測試調整

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281755-trzjk.png	44.9 KB	2025-11-28	益利 周