02_資安事件及異常紀錄 - 一般 #1222

Asia Cyber Security Service Portal (ACSSP) 【Reply in Jira】[INCGC-15458]-Low-Windows Bruteforce Attempt Detected

2025-12-31 08:52 - 益利 周

狀態:	Closed-關閉	**開始日期:**	2025-12-31
優先權:	Normal	**完成日期:**	
被分派者:	政益 楊	**完成百分比:**	100%
分類:		**預估工時:**	2:00 小時

概述

clipboard-202512310850-qt51k.png
Analysis: The alert indicates a brute-force style authentication attempt targeting user A40008 from workstation YILANA40008 via the domain controller YILAND-SRV.YILAND1.COM.TW, which was blocked by the security system. Since the action is BLOCK and the description shows a Status OK, there were no successful logins.

Recommendations:

1. Investigate the time-of-day restrictions configured for the user to confirm if the login attempt was legitimate and aligned with the user's allowed login times

2. Review the account activity of user to check for any successful logins or suspicious behavior.

3. Implement account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed

4. Review account policies to confirm and reinforce time-of-day restrictions.

歷史

#1 - 2025-12-31 16:59 - 益利 周

- 狀態 從 New-新增 變更為 Resolved-解決

- 被分派者 設定為 政益 楊

- 完成百分比 從 0 變更為 100

- 預估工時 設定為 2:00 小時

A40008為謝鈺晨組長的電腦，950668為林子堯組長電腦，今天因在AD要開通YILAND1.COM.TW網域的使用，故在Windows認證管理員寫入帳號及密碼，因為該兩員皆忘了這個密碼，故有各錯誤輸入的狀態，以上屬於正常。

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202512310850-qt51k.png	40.2 KB	2025-12-31	益利 周