02_資安事件及異常紀錄 - 一般 #1092

INCGC-5376-Windows Brute Force Attempt Detected Logon Type 3

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 18:25 - 益利 周

- 檔案 clipboard-202511281824-h9buz.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

View the request and select *Get notifications* to follow along.

Basic information

Alert Name: Alerts Notification_Taiwan from CrowdStrike ["SensorGroupingTags/Taiwan_TAHO"] - TAHOTN-002

Alert time: 2025-08-25T17:12:31.000+0800

Priority: Low

Key fields

RawAlert_command : "C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --control

RawAlert_filename : AnyDesk.exe

RawAlert_hostip : 192.168.0.102

RawAlert_hostname : TAHOTN-002

RawAlert_username : 990044

Check Items and Results

Check Items	Suspicious	Comment
		command:"C:\Program Files (x86)\AnyDesk\AnyDesk.exe" --control
*//		Actions taken:Process blocked
*Analyze the excution elementscommand/action/result	No	AnyDesk remote software was detected on the host. The software itself poses no threat. Please confirm whether its use is for business or IT operations, and whether the usage of this software is compliant.
*		filepath:\Device\HarddiskVolume4\Program Files (x86)\AnyDesk\AnyDesk.exe
*Check the File Hash (Threat Intelligence)	No	sha256:052c14c713fcb8ef5473763e9c07dcf55a957869b5fcb0f72d448ecdd09c601d No security vendors flagged this file as malicious
*		
*Check the File Sample (Sandbox)	No	No security vendors flagged this file as malicious
7		
Check if there are alerts on related hosts (within the last 7 days)	No	No

使用者990044 操作電腦 TAHOTN-002 使用AnyDesk 軟體 被偵測到

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281824-h9buz.png	63.2 KB	2025-11-28	益利 周