02_資安事件及異常紀錄 - 一般 #1119

INCGC-13232-Multiple Fortinet Firewall Configuration Change Detected In 30 Mins

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 16:10 - 益利 周

- 檔案 clipboard-202511281609-5dcbz.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: 2025-10-17 20:48:00 TST
End Time: 2025-10-17 21:18:00 TST
Customer Name: Veolia
Rule Name: Multiple_Fortinet_Firewall_Configuration_Change_Detected_in_30_Mins
Rule Description: This rule detects if more than 5 firewall configuration change is detected within 30 minutes from the same user
Priority: Low
Risk Score: 20
Log Type: FORTINET_FIREWALL
Event Type: USER_UNCATEGORIZED
Description: Configuration changed
Vendor Name: Fortinet
Product Name: Fortigate
Product Event Type: event - system
Product Log ID: 0100032102
Device: ULPU_LiuDu
Principal IP: 210.61.66.31
Principal Location State: Taipei City
Principal Country/Region: Taiwan
Principal Network ASN: 3462
Principal Network Carrier Name: data communication business group
Principal Organization Name: chunghwa telecom co. ltd.
Principal DNS Domain: hinet.net
Principal Administrative Domain: root
Principal User ID: barrytsai

30分鐘內 連線進 5台設備 -協力廠商進行維護保養

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

- 狀態 從 Resolved-解決 變更為 Closed-關閉

檔案

clipboard-202511281609-5dcbz.png	48 KB	2025-11-28	益利 周