02_資安事件及異常紀錄 - 阻斷服務 #1124

INCGC-13693-Outbound Communication Detected To Malicious Domain Detected On Firewall

2025-11-10 17:46 - Joy Liao

狀態:	Resolved-解決	**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
版本:			

概述

歷史

#1 - 2025-11-28 15:56 - 益利 周

- 檔案 clipboard-202511281550-yscup.png 已新增

- 追蹤標籤 從 一般 變更為 阻斷服務

- 狀態 從 New-新增 變更為 Resolved-解決

- 完成百分比 從 0 變更為 100

Description:

Start Time: 2025-10-27 10:11:00 TST
End Time: 2025-10-27 10:21:00 TST
Customer Name: Veolia
Rule Name: Outbound_Communication_Detected_To_Malicious_Domain_Detected_On_Firewall
Rule Description: Rule to check for any traffic is outgoin to any malicious/suspicious domain
Priority: Medium
Risk Score: 20
Log Type: FORTINET_FIREWALL
Event Type: NETWORK_CONNECTION
Description: Network.Service: SSL_TLSv1.2
Vendor Name: Fortinet
Product Name: Fortigate
Product Event Type: utm - app-ctrl
Product Log ID: 1059028704
Device: TAHO_DAFA
Device Action: pass
Principal IP: 192.168.7.3
Principal Port: 50957
Principal Hostname: dafawks01
Principal Administrative Domain: root
Target IP: 134.70.80.3
Target Port: 443
Target Country/Region: Japan
Target ASN: 31898
Target Network Carrier Name: oracle corporation
Target Organization Name: oracle public cloud
Target Hostname: objectstorage.ap-tokyo-1.oraclecloud.com
Mitre Tactic: Defense Evasion, Persistence, Command and Control
Mitre Technique: Traffic Signaling: Port Knocking

已禁止 對 objectstorage.ap-tokyo-1.oraclecloud.com 134.70.80.3 連線

檔案

clipboard-202511281550-yscup.png	51.9 KB	2025-11-28	益利 周