國家資通安全會報 技術服務中心

聯防監控資訊回傳數據欄位與格式規範

編號	Field Name	參考中文描述(勿以此為回傳名稱)	格式	欄位必須性(M 必填 O 選擇)	說明
1	Organization	發送單位	String(max 40)	M	發送事件單之單位或組織代號，如中華電信、ACER 等
2	Event_ID	事件單(Incident)ID	String(max 40)	M	事件單(Incident)編號，此為發送事件單之單位的事件單編號，該欄位亦為檔案名稱(如補充說明 4)。
3	Customer_Name	機關名稱	String(max 255)	M	監控機關完整名稱(中央政府機關名稱請參照 http://www.gov.tw/OrgInfo/ORPF-GOV-01.aspx)
4	Customer_ID	機關代碼	中央政府機關之 OID	M	監控機關之 OID 編號
5	Subject	事件單主旨	String(max 255)	M	事件單簡述主旨(Subject)
6	Base_Event_ID	事件(Event)ID	String(max 40)	O	發送事件單之單位關聯事件單之編號
7	Event_Name	事件名稱	String(max 255)	M	事件單名稱(暫依各單位之定義)
8	Start_Time	事件發生時間	String(max 25) YYYY-MM-DD HH:MM:SS.X	M	事件觸發之時間(原始第一筆時間)
9	End_Time	事件結束時間	String(max 25) YYYY-MM-DD HH:MM:SS.X	M	事件結束時間(發送機關時間)
10	Connector_Translated_Zone_Reference_ID	事件來源	String(max 40)	O	被監控機關觸發事件單之原始事件搜集器 ID 與名稱
11	Source_Address	來源 IP	String(max 40)	M	事件單來源位址
12	Target_Address	目標 IP	String(max 40)	M	事件單目標位址

編號	Field Name	參考中文描述(勿以此為回傳名稱)	格式	欄位必須性(M 必填 O 選擇)	說明
13	Source_Port	來源 PORT	String(max 40)	O	事件單來源使用埠
14	Target_Port	目標 PORT	String(max 40)	O	事件單目標使用埠
15	Source_ Geo_Descriptor	來源 IP 經緯度	String(max 40) 格式(xxx,xxx)	O	事件單來源經緯度
16	Target_ Geo_Descriptor	目標 IP 經緯度	String(max 40) 格式(xxx,xxx)	O	事件單目標經緯度
17	Event_ Attacking_ Technical	手法研判	String(max 255)	O	事件單中註明之攻擊手法
18	Events_ Description	事件描述	String(max 255)	M	事件單中註明之事件過程
19	Event_Message	處理說明	String(max 255)	M	事件單中發送單位之處理建議
20	Event_ Vulnerability	弱點資訊	String(max 255)	O	本事件單之弱點補充資訊如:弱點類別, 弱點名稱, CVE-ID 等
21	Event_Severity	影響等級	String(max 20)	M	本事件單之風險嚴重度，預設分 10 等級
22	Device_ Translated_Zone Reference_ID	觸發設備	String(max 255)	O	本事件單之來源 Log 設備名稱(型號為補充內容)
23	Triggered_Rule Name	觸發規則	String(max 255)	O	本事件單之來源 Log 設備規則名稱
24	Correlated_Rule Name	關聯規則名稱	String(max 255)	O	觸發關聯規則名稱
25	Correlated_Rule ID	關聯規則 ID	String(max 255)	O	觸發關聯規則編號(關聯規則編碼)
26	Correlated_Raw Event_ID	關聯事件 ID	String(max 255)	O	觸發關聯規則之紀錄編號
27	Aggregated_ Count	關聯事件數	String(max 40)	M	觸發關聯規則之彙總記錄數量
28	Attachment	附件(如補充說明 6)	UTF-8 編碼	O	觸發關聯規則之附檔說明

補充說明:

1. 資訊回傳欄位應至少包含上述欄位內容，實際輸出時依狀況不同會額外增加其他欄 位內容，但以不影響 CSV/XML 資訊結構為主。
2. XML 編碼語言請設定為 UTF-8。
3. 回傳數據欄位 Field Name 要求與二線 SOC Field Name 一致(勿以中文欄位回傳)，Field Name 中間請加底線，勿留空格。
4. 回傳檔名命名方式: Event_ID.xml(如格式欄位編號 2)。
5. 必填欄位若無回傳值，內容請回傳 NULL 值。
6. 上傳檔案放置於 incident 目錄，附件放置於 attachment 目錄。