【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I938940
【45】公告日： 中華民國 115 (2026) 年 09 月 11 日
【51】Int. Cl.：　*G06F21/57　(2013.01)*　*G06F21/50　(2013.01)*
發明　全 3 頁

【54】名　稱：主動式資安監控方法及系統
【21】申請案號：114113850　【22】申請日： 中華民國 114 (2025) 年 04 月 11 日
【72】發 明 人： 李茂義 (TW) ；謝昌益 (TW) ；簡君曄 (TW) ；廖羿婷 (TW)
【71】申 請 人： 數聯資安股份有限公司　INFORMATION SECURITY SERVICE DIGITAL UNITED INC.
臺北市內湖區港墘路 220 號 6 樓
【74】代 理 人： 楊祺雄；吳俊彥
【56】參考文獻：
TW　M661374U　TW　202312710A
US　11106789B2
網路文獻 Maria Poltavtseva “Key Concepts of Systemological Approach to CPS Adaptive Information Security Monitoring” Symmetry 15 December 2021
審查人員：陳奕昌

【57】申請專利範圍

1. 一種主動式資安監控方法，由一系統執行，該系統儲存多筆歷史異常事件資訊及多筆群組資料，每一筆歷史異常事件資訊包括一觸發時間及一具有一目標 IP、一目標帳號及一受害主機資訊之其中至少一者的目標資源，每一筆群組資料包括多筆相互關聯的群組異常事件資訊，該方法包含以下步驟：
(A)對於每一筆群組資料，判斷該等歷史異常事件資訊中的多筆候選歷史異常事件資訊之其中至少一者是否與該群組資料的群組異常事件資訊相關，其中比對該等候選歷史異常事件資訊之目標資源與該群組資料中至少一群組異常事件資訊之目標資源是否相同，以判斷該等候選歷史異常事件資訊之其中至少一者是否與該群組資料相關，且每一筆候選歷史異常事件資訊的觸發時間與一當前時間的時間差小於一第一時間區間；
(B)對於每一筆群組資料，當判斷出該等候選歷史異常事件資訊皆與該群組資料的群組異常事件資訊不相關時，判斷一當前時間與前次更新該群組資料的時間之差是否大於一大於該第一時間區間的第二時間區間，並當判斷出該當前時間與前次更新該群組資料的時間之差小於等於該第二時間區間時，等待該第一時間區間後重複步驟(A)，當判斷出該當前時間與前次更新該群組資料的時間之差大於該第二時間區間時，則結束；
(C)對於每一筆群組資料，當判斷出該等候選歷史異常事件資訊之其中至少一者與該群組資料的群組異常事件資訊相關時，從該等候選歷史異常事件資訊獲得至少一相關該群組資料的群組異常事件資訊的目標歷史異常事件資訊，其中，每一筆目標歷史異常事件資訊的目標資源與該群組資料的群組異常事件資訊之目標資源相同；
(D)對於每一筆群組資料，將該至少一目標歷史異常事件資訊作為群組異常事件資訊加入該群組資料，以更新該群組資料；
(E)對於每一筆群組資料，根據該群組資料的群組異常事件資訊更新該群組資料對應的風險分數；及

(F)對於每一筆群組資料，根據該群組資料對應的風險分數，調整該第一時間區間及該第二時間區間之其中至少一者，其中，當更新後的該風險分數高於更新之前的該風險分數時，縮短該第一時間區間以增加監控頻率，且增加該第二時間區間以延長監控時間。

2. 一種主動式資安監控系統，包含：

一儲存單元，儲存多筆歷史異常事件資訊及多筆群組資料，每一筆歷史異常事件資訊包括一觸發時間及一目標資源，每一筆群組資料包括多筆相互關聯的群組異常事件資訊；及

一處理單元，電連接該儲存單元；

該處理單元執行如請求項 1 所述的主動式資安監控方法。

圖式簡單說明

本發明的其他的特徵及功效，將於參照圖式的實施方式中清楚地呈現，其中：

圖 1 是一方塊圖，說明本發明資安監測系統的一實施例；及

圖 2 是一流程圖，說明本發明資安監測方法的一實施例。

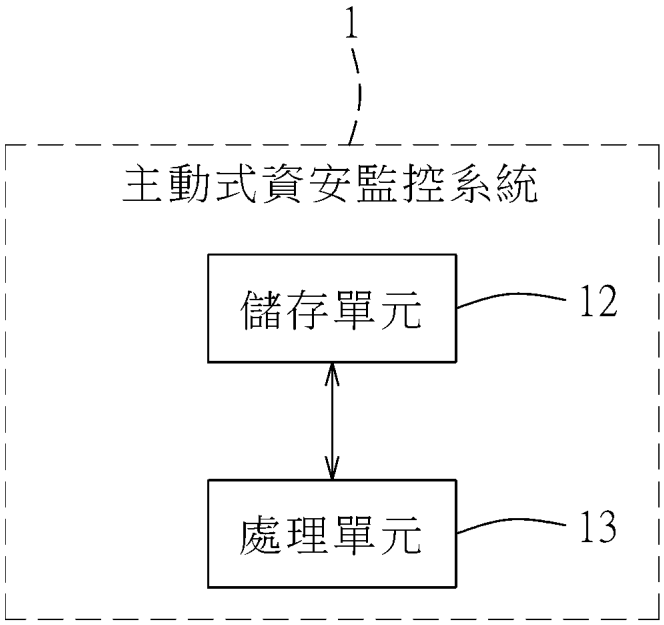

圖 1

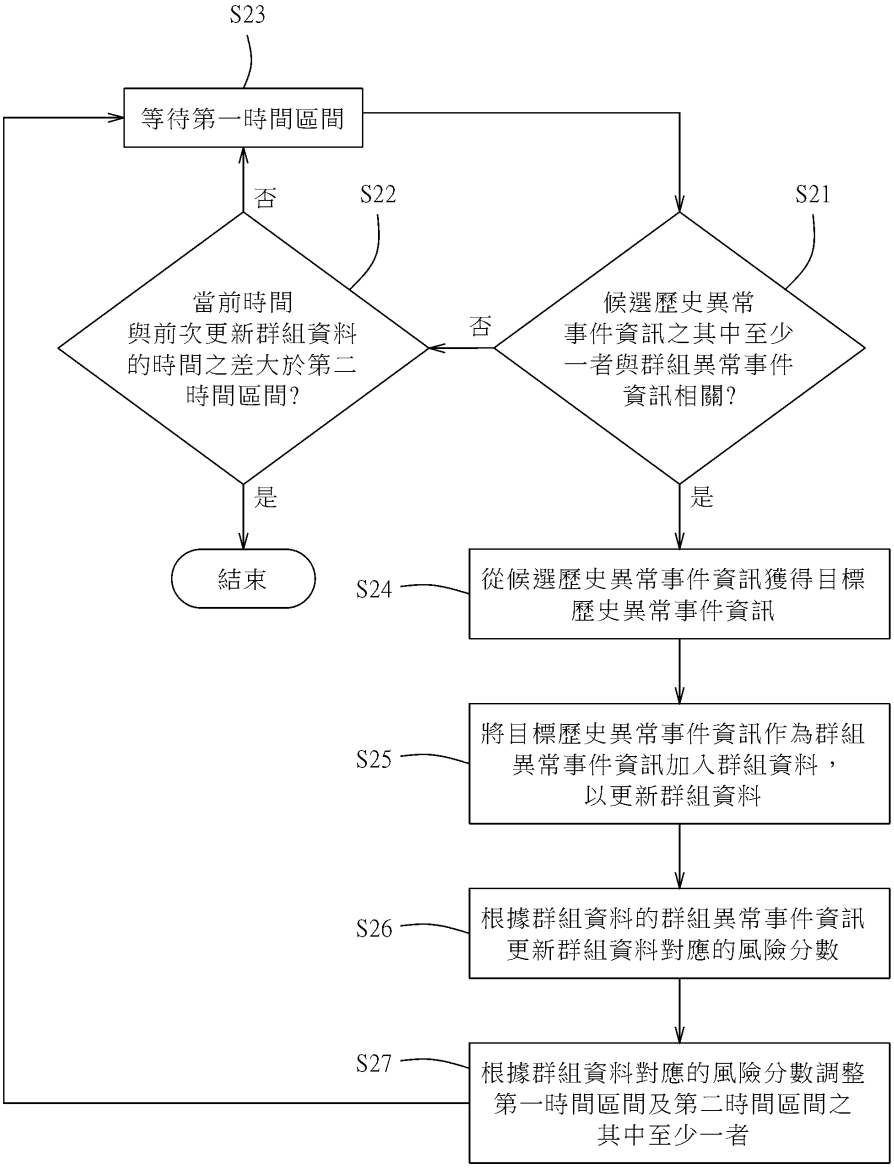
S23
等待第一時間區間
否
S22
當前時間
與前次更新群組資料
的時間之差大於第二
時間區間?
否
S21
候選歷史異常
事件資訊之其中至少
一者與群組異常事件
資訊相關?
是
是
結束
S24
從候選歷史異常事件資訊獲得目標
歷史異常事件資訊
S25
將目標歷史異常事件資訊作為群組
異常事件資訊加入群組資料，
以更新群組資料
S26
根據群組資料的群組異常事件資訊
更新群組資料對應的風險分數
S27
根據群組資料對應的風險分數調整
第一時間區間及第二時間區間之
其中至少一者

圖 2