【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I941162
【45】公告日： 中華民國 115 (2026) 年 10 月 01 日
【51】Int. Cl.：　*G06F21/57　(2013.01)*　*G06F21/50　(2013.01)*
發明　全 4 頁

【54】名　稱：資安綜合風險評估方法及系統
【21】申請案號：114113851　【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：

CN	106790186A	CN	119071049A
US	11552974B1	US	2016/0226905A1
US	2018/0336353A1	US	2019/0034641A1

審查人員：徐瑞甫

【57】申請專利範圍

1. 一種資安綜合風險評估方法，由一系統執行，該系統儲存多筆歷史異常事件資訊，每一筆歷史異常事件資訊包括一風險分數、一來源資源、一目標資源，及一攻擊特徵，該方法包含以下步驟：
(A)收集多筆日誌資料，並根據該等日誌資料，獲得一當前異常事件資訊，該當前異常事件資訊包括一風險分數、一來源資源、一目標資源，及一攻擊特徵；
(B)根據該當前異常事件資訊，從該等歷史異常事件資訊獲得至少一相關該當前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來源資源、目標資源，及攻擊特徵之至少一者與該當前異常事件資訊的來源資源、目標資源，及攻擊特徵相同；及
(C)將該當前異常事件資訊及該至少一目標歷史異常事件資訊作為多筆關聯異常事件資訊，並根據該等關聯異常事件資訊算出一綜合風險分數；
其中，在步驟(C)中，對於每一筆關聯異常事件資訊，根據該關聯異常事件資訊的來源資源獲得一信譽等級，並根據該信譽等級獲得一信譽權重；根據該關聯異常事件資訊的攻擊特徵獲得一相關攻擊階段的跨越數，並根據該跨越數獲得一跨越階段權重；再將該關聯異常事件資訊的風險分數、該信譽權重，及該跨越階段權重相乘，以獲得一加權風險分數，該綜合風險分數為所有加權風險分數的總和。
2. 如請求項 1 所述的資安綜合風險評估方法，其中，步驟(A)包括以下子步驟：
(A-1)收集該等日誌資料；
(A-2)利用一關聯規則演算法及一用以辨識出異常事件的機器學習模型之其中至少一者，產生一告警資料；
(A-3)根據該告警資料進行關鍵元數據萃取，以獲得一關鍵元數據；及
(A-4)將該關鍵元數據轉換成一預設數據格式，以獲得該當前異常事件資訊。
3. 如請求項 1 所述的資安綜合風險評估方法，每一筆歷史異常事件資訊還包括一觸發時間，其中，在步驟(A)中，該當前異常事件資訊還包括一觸發時間，在步驟(C)中，對於每一筆關聯異常事件資訊，根據該關聯異常事件資訊的觸發時間及一當前時間獲得一時

間權重，再將該關聯異常事件資訊的風險分數、該信譽權重、該跨越階段權重，及該時間權重相乘，以獲得該加權風險分數，該綜合風險分數為所有加權風險分數的總和。

4. 如請求項 1 所述的資安綜合風險評估方法，每一筆歷史異常事件資訊還包括一觸發時間，其中，在步驟(A)中，該當前異常事件資訊還包括一觸發時間，在步驟(C)中，對於每一筆關聯異常事件資訊，根據該關聯異常事件資訊的觸發時間、來源資源，及目標資源之其中一者獲得一觸發頻率權重，再將該關聯異常事件資訊的風險分數、該信譽權重、該跨越階段權重，及該觸發頻率權重相乘，以獲得該加權風險分數，該綜合風險分數為所有加權風險分數的總和。

5. 如請求項 1 所述的資安綜合風險評估方法，其中，在步驟(C)中，對於每一筆關聯異常事件資訊，將該關聯異常事件資訊的風險分數、該信譽權重、該跨越階段權重，及一近期入侵權重相乘，以獲得該加權風險分數，該綜合風險分數為所有加權風險分數的總和。

6. 如請求項 1 所述的資安綜合風險評估方法，其中，在步驟(C)中，根據該等關聯異常事件資訊的攻擊特徵獲得一不重複事件種類權重，並對於每一筆關聯異常事件資訊，將該關聯異常事件資訊的風險分數、該信譽權重、該跨越階段權重，及該不重複事件種類權重相乘，以獲得該加權風險分數，該綜合風險分數為所有加權風險分數的總和。

7. 如請求項 1 所述的資安綜合風險評估方法，每一筆歷史異常事件資訊的該目標資源具有一受害主機資訊，其中，在步驟(C)中，對於每一關聯異常事件資訊，根據該關聯異常事件資訊的目標資源之受害主機資訊獲得一相關於受害主機的機敏性之機敏性權重，再將該關聯異常事件資訊的風險分數、該信譽權重，及該跨越階段權重相乘，並與該機敏性權重相加，以獲得該加權風險分數，該綜合風險分數為所有加權風險分數的總和。

8. 如請求項 1 所述的資安綜合風險評估方法，其中，在步驟(C)中，對於每一筆關聯異常事件資訊，根據該關聯異常事件資訊的攻擊特徵獲得一高危害權重，再將該關聯異常事件資訊的風險分數、該信譽權重，及該跨越階段權重相乘，並與該高危害權重相加，以獲得該加權風險分數，該綜合風險分數為所有加權風險分數的總和。

9. 一種資安綜合風險評估系統，包含：

一儲存單元，儲存多筆歷史異常事件資訊，每一筆歷史異常事件資訊包括一風險分數、一來源資源、一目標資源，及一攻擊特徵；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 至 8 其中任一項所述的資安綜合風險評估方法。

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，說明本發明資安綜合風險評估系統的一實施例；

圖 2 是一流程圖，說明本發明資安綜合風險評估方法的一實施例；及

圖 3 是一流程圖，輔助說明圖 2 的步驟 21 的子步驟。

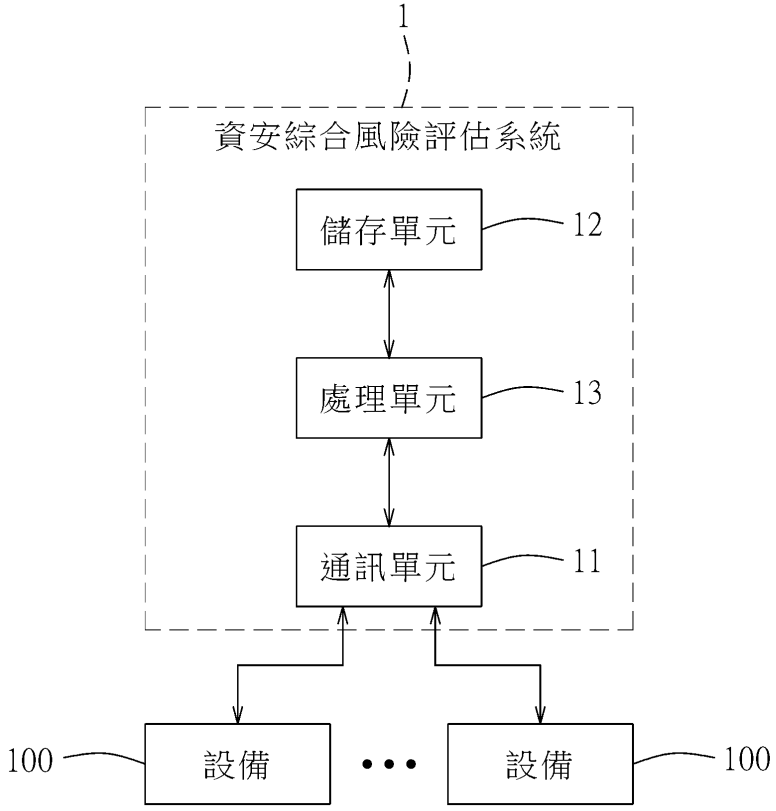


圖 1

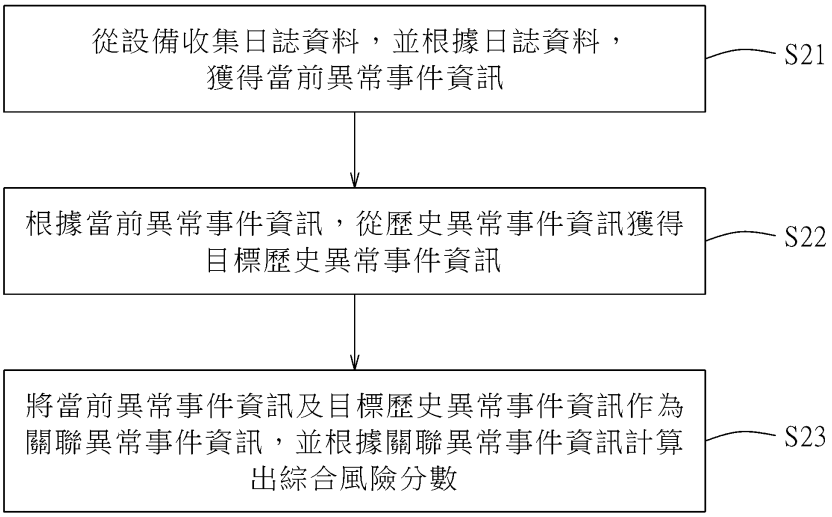

從設備收集日誌資料，並根據日誌資料，
獲得當前異常事件資訊
S21
根據當前異常事件資訊，從歷史異常事件資訊獲得
目標歷史異常事件資訊
S22
將當前異常事件資訊及目標歷史異常事件資訊作為
關聯異常事件資訊，並根據關聯異常事件資訊計算
出綜合風險分數
S23

圖 2

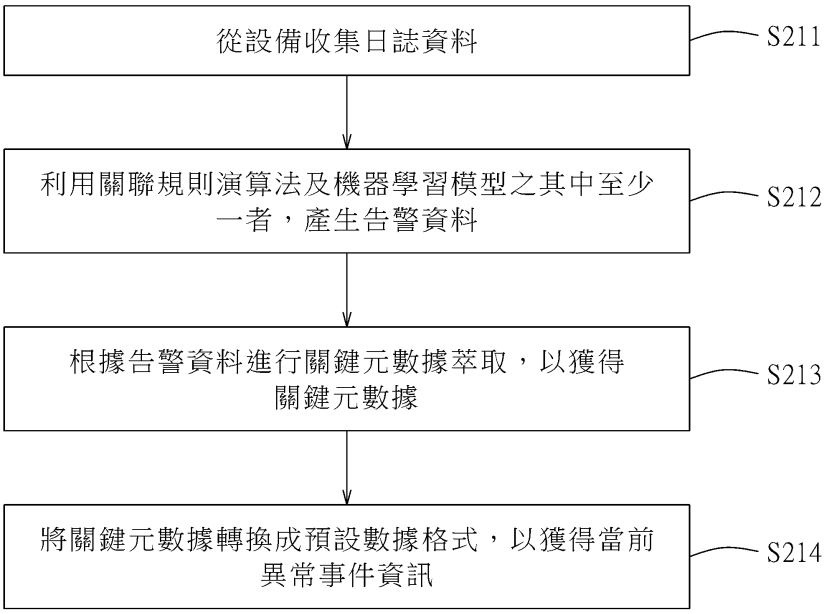

從設備收集日誌資料
S211
利用關聯規則演算法及機器學習模型之其中至少
一者，產生告警資料
S212
根據告警資料進行關鍵元數據萃取，以獲得
關鍵元數據
S213
將關鍵元數據轉換成預設數據格式，以獲得當前
異常事件資訊
S214

圖 3