【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】令和5年4月14日(2023.4.14)

【国際公開番号】WO2020/214585
【公表番号】特表2022-529467(P2022-529467A)
【公表日】令和4年6月22日(2022.6.22)
【年通号数】公開公報(特許)2022-112
【出願番号】特願2021-561816(P2021-561816)
【国際特許分類】
G06F 21/55(2013.01)
【ＦＩ】
Ｇ０６Ｆ 21/55 ３４０
Ｇ０６Ｆ 21/55 ３２０

【手続補正書】
【提出日】令和5年4月6日(2023.4.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
クラウド環境における異常行動を検出する方法であって、
前記クラウド環境において複数の前の時間間隔中に取られたアクションを表わす第１のベクトルを算出するステップと、
前記第１のベクトルと、現在の時間間隔中に取られたアクションのカウントを含む第２のベクトルとの間の類似度を算出するステップと、
１つ以上の異常アクションが発生したかどうかを判断するために、前記類似度をベースライン閾値と比較するステップと、
前記１つ以上の異常アクションが前記クラウド環境において発生したという判断に少なくとも部分的に基づいてアラートを生成するステップとを含む、方法。
【請求項２】
前記類似度はコサイン類似度を用いて算出される、請求項１に記載の方法。
【請求項３】
前記第１のベクトルにおける各エントリは前記複数の前の時間間隔中の平均イベントスコアを含む、請求項１または２に記載の方法。
【請求項４】
前記複数の前の時間間隔の各々は１日を含む、請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記複数の前の時間間隔は少なくとも６０日の窓を含む、請求項１～４のいずれか１項に記載の方法。
【請求項６】
前記複数の前の時間間隔は複数の日のスライディング窓を含み、前記複数の日のスライディング窓は、各時間間隔の後に、前記現在の時間間隔を前記複数の日のスライディング窓に追加し、前記複数の日のスライディング窓から最も古い時間間隔を除去する、請求項１～５のいずれか１項に記載の方法。
【請求項７】

前記第１のベクトルは、前記複数の前の時間間隔の各々に関するイベントカウントのヒストグラムを格納することによって、前記複数の前の時間間隔中に取られたアクションを表わす、請求項１～６のいずれか１項に記載の方法。
【請求項８】
１つ以上のプロセッサによって実行されると前記１つ以上のプロセッサに動作を実行させる命令を備えるコンピュータプログラムであって、前記動作は、
クラウド環境において複数の前の時間間隔中に取られたアクションを表わす第１のベクトルを算出する動作と、
前記第１のベクトルと、現在の時間間隔中に取られたアクションのカウントを含む第２のベクトルとの間の類似度を算出する動作と、
１つ以上の異常アクションが発生したかどうかを判断するために、前記類似度をベースライン閾値と比較する動作と、
前記１つ以上の異常アクションが前記クラウド環境において発生したという判断に少なくとも部分的に基づいてアラートを生成する動作とを含む、コンピュータプログラム。
【請求項９】
前記動作はさらに、
前記類似度を上限閾値と比較して、１つ以上の異常アクションが発生したかどうかをさらに判断する、請求項８に記載のコンピュータプログラム。
【請求項１０】
前記ベースライン閾値は、前記類似度を疑わしいものであると特徴付け、前記上限閾値は、前記類似度を脅威を表わすものとして特徴付ける、請求項９に記載のコンピュータプログラム。
【請求項１１】
前記上限閾値は、前記第１のベクトルにおいて算出される平均値についての予め定められた数の標準偏差に基づいて決定される、請求項９または１０に記載のコンピュータプログラム。
【請求項１２】
前記上限閾値は、前記類似度を入力として受取るニューラルネットワークによって表わされる、請求項９または１０に記載のコンピュータプログラム。
【請求項１３】
前記ベースライン閾値は、前記類似度を入力として受取るニューラルネットワークによって表わされる、請求項８～１２のいずれか１項に記載のコンピュータプログラム。
【請求項１４】
前記ベースライン閾値は、現在のユーザと同様の複数のユーザに関するピアグループ分析を用いて決定される、請求項８～１２のいずれか１項に記載のコンピュータプログラム。
【請求項１５】
システムであって、
１つ以上のプロセッサと、
前記１つ以上のプロセッサによって実行されると前記１つ以上のプロセッサに動作を実行させる命令を備える１つ以上のメモリデバイスとを含み、前記動作は、
クラウド環境において複数の前の時間間隔中に取られたアクションを表わす第１のベクトルを算出する動作と、
前記第１のベクトルと、現在の時間間隔中に取られたアクションのカウントを含む第２のベクトルとの間の類似度を算出する動作と、
１つ以上の異常アクションが発生したかどうかを判断するために、前記類似度をベースライン閾値と比較する動作と、
前記１つ以上の異常アクションが前記クラウド環境において発生したという判断に少なくとも部分的に基づいてアラートを生成する動作とを含む、システム。
【請求項１６】

前記動作はさらに、
前記第２のベクトルにおける１つ以上の値を、前記１つ以上の値に関連付けられた１つ以上のアクションスコアと比較する動作を含む、請求項１５に記載のシステム。
【請求項１７】
前記１つ以上のアクションスコアの各々は、前記アクションが脅威を表わす悪意あるアクションである可能性を表わす、請求項１６に記載のシステム。
【請求項１８】
前記第２のベクトルは、特定のリソースに対して取られたアクションのカウントを含む、請求項１５～１７のいずれか１項に記載のシステム。
【請求項１９】
前記第１のベクトルにおける複数の値は、アクションが発生した週の日に応じて重み付けされる、請求項１５～１８のいずれか１項に記載のシステム。
【請求項２０】
前記第２のベクトルは、特定のユーザに対して取られたアクションのカウントを含む、請求項１５～１９のいずれか１項に記載のシステム。