

## CLAIMS

1. A computer system comprising at least one hardware processor configured to:
- in response to receiving a cluster membership indicator indicating a grouping of a plurality of client systems into a plurality of client clusters, select a client cluster from the plurality of client clusters, the selected client cluster comprising multiple client systems;
- in response to selecting the client cluster, select a training corpus of events from an event collection according to whether the selected events have occurred on members of the selected client cluster;
- in response to selecting the training corpus of events, train a behavior model to encode a collective behavior of members of the selected client cluster according to the training corpus of events, the behavior model having a set of adjustable parameters; and
- in response to training the behavior model, transmit a set of values of the adjustable parameters to an anomaly detector configured to determine whether a target event occurring on a target client system is indicative of a computer security threat;
- wherein:
- the behavior model is configured to input a selected event of an event sequence and in response, to determine a prediction indicator indicative of a likelihood that another event of the event sequence is of a selected event type;
- the event sequence comprises a plurality of events of the training corpus, the plurality of events ordered according to a time of occurrence of each event of the plurality of events; and
- training the behavior model comprises adjusting the set of configurable parameters according to the prediction indicator.
2. The computer system of claim 1, wherein training the behavior model comprises:

2 determining a predicted event according to the prediction indicator;  
3 comparing the predicted event to the another event of the event sequence; and  
4 adjusting the set of configurable parameters according to a result of the  
5 comparison.  
6

1 3. The computer system of claim 1, wherein:

2 the event sequence comprises a central event and an event context, the event  
3 context comprising a first subset of the events occurring prior to the  
4 central event and a second subset of events occurring later than the central  
5 event;  
6 the selected event is the central event; and  
7 the another event is a member of the event context.  
8

1 4. The computer system of claim 1, wherein:

2 the event sequence comprises a central event and an event context, the event  
3 context comprising a first subset of the events occurring prior to the  
4 central event and a second subset of events occurring later than the central  
5 event;  
6 the selected event is a member of the event context; and  
7 the another event is the central event.  
8

1 5. The computer system of claim 1, wherein the behavior model comprises an event  
2 encoder configured to input the selected event and in response, to determine a set  
3 of coordinates indicative of a position of the selected event in an event embedding  
4 space, the coordinates determined according to whether the selected event occurs  
5 in a selected context of other events of the training corpus.  
6

1 6. The computer system of claim 1, wherein:

2 the event collection is divided into a plurality of event categories according to  
3 whether an event of the event collection occurs in a selected context of  
4 other events of the event collection; and

5 the plurality of client systems are grouped into clusters according to an event  
6 profile of each client system, the event profile determined according to a  
7 count of events occurring on the each client system and belonging to a  
8 selected category of the plurality of event categories.

9  
1 7. The computer system of claim 6, wherein the event profile of the each client  
2 system comprises a plurality of components, each component determined  
3 according to a proportion of events belonging to each event category of the  
4 plurality of event categories, the proportion calculated out of a total count  
5 of events of the event collection occurring on the each client system.

6  
1 8. The computer system of claim 6, wherein grouping the plurality of client  
2 systems into clusters comprises assigning client systems having similar  
3 event profiles to the same client cluster.

4  
1 9. The computer system of claim 1, wherein the training corpus is selected to include  
2 only events that have occurred on members of the selected client cluster.

3  
1 10. The computer system of claim 1, wherein the selected event comprises a launch of a  
2 selected process on a client system of the plurality of client systems.

3  
1 11. A computer-implemented method comprising:  
2 employing at least one hardware processor of a computer system, in response to receiving  
3 a cluster membership indicator indicating a grouping of a plurality of client  
4 systems into a plurality of client clusters, to select a client cluster from the

5 plurality of client clusters, the selected client cluster comprising multiple client  
6 systems;

7 in response to selecting the client cluster, employing at least one hardware processor of  
8 the computer system to select a training corpus of events from an event collection  
9 according to whether the selected events have occurred on members of the  
10 selected client cluster;

11 in response to selecting the training corpus of events, employing at least one hardware  
12 processor of the computer system to train a behavior model to encode a collective  
13 behavior of members of the selected client cluster according to the training corpus  
14 of events, the behavior model having a set of adjustable parameters; and

15 in response to training the behavior model, employing at least one hardware processor of  
16 the computer system to transmit a set of values of the adjustable parameters to an  
17 anomaly detector configured to determine whether a target event occurring on a  
18 target client system is indicative of a computer security threat;

19 wherein:

20 the behavior model is configured to input a selected event of an event sequence  
21 and in response, to determine a prediction indicator indicative of a  
22 likelihood that another event of the event sequence is of a selected event  
23 type;

24 the event sequence comprises a plurality of events of the training corpus, the  
25 plurality of events ordered according to a time of occurrence of each event  
26 of the plurality of events; and

27 training the behavior model comprises adjusting the set of configurable  
28 parameters according to the prediction indicator.

29  
1 12. The method of claim 11, wherein training the behavior model comprises:

2 determining a predicted event according to the prediction indicator;

3 comparing the predicted event to the another event of the event sequence; and

4 adjusting the set of configurable parameters according to a result of the  
5 comparison.  
6

1 13. The method of claim 11, wherein:

2 the event sequence comprises a central event and an event context, the event  
3 context comprising a first subset of the events occurring prior to the  
4 central event and a second subset of events occurring later than the central  
5 event;

6 the selected event is the central event; and

7 the another event is a member of the event context.  
8

1 14. The method of claim 11, wherein:

2 the event sequence comprises a central event and an event context, the event  
3 context comprising a first subset of the events occurring prior to the  
4 central event and a second subset of events occurring later than the central  
5 event;

6 the selected event is a member of the event context; and

7 the another event is the central event.  
8

1 15. The method of claim 11, wherein the behavior model comprises an event encoder  
2 configured to input the selected event and in response, to determine a set of  
3 coordinates indicative of a position of the selected event in an event embedding  
4 space, the coordinates determined according to whether the selected event occurs  
5 in a selected context of other events of the training corpus.  
6

1 16. The method of claim 11, wherein:

2 the event collection is divided into a plurality of event categories according to  
3 whether an event of the event collection occurs in a selected context of  
4 other events of the event collection; and

5 the plurality of client systems are grouped into clusters according to an event  
6 profile of each client system, the event profile determined according to a  
7 count of events occurring on the each client system and belonging to a  
8 selected category of the plurality of event categories.

1 17. The method of claim 16, wherein the event profile of the each client system  
2 comprises a plurality of components, each component determined  
3 according to a proportion of events belonging to each event category of the  
4 plurality of event categories, the proportion calculated out of a total count  
5 of events of the event collection occurring on the each client system.

1 18. The method of claim 16, wherein grouping the plurality of client systems into  
2 clusters comprises assigning client systems having similar event profiles to  
3 the same client cluster.

1 19. The method of claim 11, wherein the training corpus is selected to include only  
2 events that have occurred on members of the selected client cluster.

1 20. The method of claim 11, wherein the selected event comprises a launch of a selected  
2 process on a client system of the plurality of client systems.

1 21. A non-transitory computer-readable medium storing instructions which, when executed  
2 by at least one hardware processor of a computer system, cause the computer system to:  
3 in response to receiving a cluster membership indicator indicating a grouping of a  
4 plurality of client systems into a plurality of client clusters, select a client cluster  
5 from the plurality of client clusters, the selected client cluster comprising multiple  
6 client systems;

7 in response to selecting the client cluster, select a training corpus of events from an event  
8 collection according to whether the selected events have occurred on members of  
9 the selected client cluster;

10 in response to selecting the training corpus of events, train a behavior model to encode a  
11 collective behavior of members of the selected client cluster according to the  
12 training corpus of events, the behavior model having a set of adjustable  
13 parameters; and

14 in response to training the behavior model, transmit a set of values of the adjustable  
15 parameters to an anomaly detector configured to determine whether a target event  
16 occurring on a target client system is indicative of a computer security threat;

17 wherein:

18 the behavior model is configured to input a selected event of an event sequence  
19 and in response, to determine a prediction indicator indicative of a  
20 likelihood that another event of the event sequence is of a selected event  
21 type;

22 the event sequence comprises a plurality of events of the training corpus, the  
23 plurality of events ordered according to a time of occurrence of each event  
24 of the plurality of events; and

25 training the behavior model comprises adjusting the set of configurable  
26 parameters according to the prediction indicator.  
27

## CLAIMS

1. A computer system comprising at least one hardware processor configured to:

in response to receiving a cluster membership indicator indicating a grouping of a plurality of client systems into a plurality of client clusters, select a client cluster from the plurality of client clusters,

wherein the grouping is determined by analyzing a collection of events having occurred on members of the plurality of client systems to identify client systems having similar behavior;

in response to selecting the client cluster, train a behavior model to encode a baseline behavior collectively characterizing members of the selected client cluster, wherein:

the behavior model comprises an event encoder configured to determine an embedding vector of a selected event of a sequence of events according to a position of the selected event within the sequence of events and further according to at least another event of the sequence of events,

the sequence of events is composed exclusively of events having occurred on members of the selected client cluster and is ordered according to a time of occurrence of each event, and

wherein training the behavior model comprises predicting yet another event of the sequence of events according to the embedding vector and adjusting a parameter of the event encoder according to the prediction; and

in response to training the behavior model, transmit an adjusted value of the parameter to an anomaly detector configured to employ the trained behavior model to determine whether a target event occurring on a target client system is indicative of a computer security threat.

2. The computer system of claim 1, wherein:

the sequence of events comprises a central event and an event context, the event context comprising a first subset of events occurring prior to the central event and a second subset of events occurring later than the central event;

the selected event is the central event; and

the yet another event is a member of the event context.

3. The computer system of claim 1, wherein:

the sequence of events comprises a central event and an event context, the event context comprising a first subset of events occurring prior to the central event and a second subset of events occurring later than the central event;

the selected event is a member of the event context; and

the yet another event is the central event.

4. The computer system of claim 1, wherein:

the collection of events is divided into a plurality of event categories according to an event context of each event of the collection of events; and

grouping the plurality of client systems into clusters comprises determining whether a selected client system belongs to the selected client cluster according to a count of events having occurred on the selected client system and belonging to a selected category of the plurality of event categories.

5. The computer system of claim 4, wherein grouping the plurality of client systems into clusters comprises determining whether a selected client system belongs to the selected client cluster further according to another count of events having occurred on the selected client system and belonging to another category of the plurality of event categories.

6. The computer system of claim 1, wherein the selected event comprises a launch of a selected process on a client system of the plurality of client systems.

7. The computer system of claim 1, wherein predicting the yet another event comprises determining a prediction indicator indicative of a likelihood that the yet another event belongs to the sequence of events.

8. A computer-implemented method comprising:

employing at least one hardware processor of a computer system, in response to receiving a cluster membership indicator indicating a grouping of a plurality of client systems into a plurality of client clusters, to select a client cluster from the plurality of client clusters,

wherein the grouping is determined by analyzing a collection of events having occurred on members of the plurality of client systems to identify client systems having similar behavior;

in response to selecting the client cluster, employing at least one hardware processor of the computer system to train a behavior model to encode a baseline behavior collectively characterizing members of the selected client cluster, wherein:

the behavior model comprises an event encoder configured to determine an embedding vector of a selected event of a sequence of events according to a position of the selected event within the sequence of events and further according to at least another event of the sequence of events,

the sequence of events is composed exclusively of events having occurred on members of the selected client cluster and is ordered according to a time of occurrence of each event, and

wherein training the behavior model comprises predicting yet another event of the sequence of events according to the embedding vector and adjusting a parameter of the event encoder according to the prediction; and

in response to training the behavior model, employing at least one hardware processor of the computer system to transmit an adjusted value of the parameters to an anomaly detector configured to employ the trained behavior model to determine whether a target event occurring on a target client system is indicative of a computer security threat.

9. The method of claim 8, wherein:

the sequence of events comprises a central event and an event context, the event context comprising a first subset of events occurring prior to the central event and a second subset of events occurring later than the central event;

the selected event is the central event; and

the yet another event is a member of the event context.

10. The method of claim 8, wherein:

the sequence of events comprises a central event and an event context, the event context comprising a first subset of events occurring prior to the central event and a second subset of events occurring later than the central event;

the selected event is a member of the event context; and

the yet another event is the central event.

11. The method of claim 8, wherein:

the collection of events is divided into a plurality of event categories according to an event context of each event of the collection of events; and

grouping the plurality of client systems into clusters comprises determining whether a selected client system belongs to the selected client cluster according to a count of events having occurred on the selected client system and belonging to a selected category of the plurality of event categories.

12. The method of claim 11, wherein grouping the plurality of client systems into clusters comprises determining whether a selected client system belongs to the selected client cluster further according to another count of events having occurred on the selected client system and belonging to another category of the plurality of event categories.

13. The method of claim 8, wherein the selected event comprises a launch of a selected process on a client system of the plurality of client systems.

14. The method of claim 8, wherein predicting the yet another event comprises determining a prediction indicator indicative of a likelihood that the yet another event belongs to the sequence of events.

15. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a computer system, cause the computer system to:

in response to receiving a cluster membership indicator indicating a grouping of a plurality of client systems into a plurality of client clusters, select a client cluster from the plurality of client clusters,

wherein the grouping is determined by analyzing a collection of events having occurred on members of the plurality of client systems to identify client systems having similar behavior;

in response to selecting the client cluster, train a behavior model to encode a baseline behavior collectively characterizing members of the selected client cluster, wherein:

the behavior model comprises an event encoder configured to determine an embedding vector of a selected event of a sequence of events according to a position of the selected event within the sequence of events and further according to at least another event of the sequence of events,

the sequence of events is composed exclusively of events having occurred on members of the selected client cluster and is ordered according to a time of occurrence of each event, and

wherein training the behavior model comprises predicting yet another event of the sequence of events according to the embedding vector and adjusting a parameter of the event encoder according to the prediction; and

in response to training the behavior model, transmit an adjusted value of the parameter to an anomaly detector configured to employ the trained behavior model to determine whether a target event occurring on a target client system is indicative of a computer security threat.