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.