Claims

What is claimed is:

1. A method for performing threat detection comprising:

at a first time, assigning, by a detection system, a first label of a set of labels to first unlabeled data using an unsupervised machine learning model;

at a second time, receiving, by the detection system and from a client device, second unlabeled data;

providing, by the detection system, the second unlabeled data to the unsupervised machine learning model to:

assign the first label of the set of labels to a first set of the second unlabeled data that is similar to the first unlabeled data based on a set of data characteristics,

generate a second label of the set of labels for a second set of the second unlabeled data that is not similar to the first unlabeled data based on the set of data characteristics, and

assign the second label of the set of labels to the second set of the second unlabeled data;

storing, by the detection system, the set of labels and the set of data characteristics with a label data store;

receiving, by the detection system, the set of labels from the label data store;

initiating, by the detection system, a first training process of a supervised machine learning model using the set of labels from the unsupervised machine learning model, wherein execution of the supervised machine learning model generates a set of clustered data;

initiating, by the detection system, an inference process of the supervised machine learning model, wherein output of the inference process generates the set of clustered data;

providing, by the detection system, the set of clustered data to a label audit process for relabeling the set of clustered data, wherein the label audit process generates a set of relabeled clustered data;

initiating, by the detection system, a second training process of the supervised machine learning model using the set of relabeled clustered data to update the supervised

machine learning model; and

updating, by the detection system, the supervised machine learning model in a model data store for future inference processes on new data.

2. The method of claim 1, wherein the label audit process is based on an automatically generated label determined by the unsupervised machine learning model using a data characteristic from the set of data characteristics of the second unlabeled data received from the client device.

3. The method of claim 1, wherein the label audit process is based on a human-generated label.

4. The method of claim 1, wherein the label audit process is a weighted combination of a human-generated label and an automatically generated label determined by the unsupervised machine learning model.

5. The method of claim 1, further comprising:

analyzing the first unlabeled data for balancing a distribution of values in the first unlabeled data;

initiating a random stratified sampling process to generate new second data; and

adding the new second data to the first unlabeled data.

6. The method of claim 1, wherein the supervised machine learning model is selected for the inference process based on a machine learning label corresponding with the second label of the set of labels to the second set of the second unlabeled data.

7. The method of claim 1, further comprising:

initiating an action based on the set of relabeled clustered data.

8. The method of claim 7, wherein the action comprises updating a display that identifies an inference associated with the second unlabeled data.

9. The method of claim 7, wherein the action comprises sending a notification to remove the client device from communicating with a detection system via a network.

10. The method of claim 7, wherein the action comprises adding a portion of the set of relabeled clustered data to an outlier queue for further review.

11. The method of claim 1, wherein the second label associated with the second unlabeled data is a data anomaly or outlier data.

12. The method of claim 1, wherein the first unlabeled data and the second unlabeled data comprise telemetry data.

13. A detection system comprising:

a memory; and

a processor configured to execute machine readable instructions stored in the memory for causing the processor to:

at a first time, assign a first label of a set of labels to first unlabeled data using an unsupervised machine learning model;

at a second time, receive, from a client device, second unlabeled data;

provide the second unlabeled data to the unsupervised machine learning model to:

assign the first label of the set of labels to a first set of the second unlabeled data that is similar to the first unlabeled data based on a set of data characteristics,

generate a second label of the set of labels to a second set of the second unlabeled data that is not similar to the first unlabeled data based on the set of data characteristics, and

assign the second label of the set of labels to the second set of the second labeled data;

store the set of labels and the set of data characteristics with a label data store;

receive the set of labels from the label data store;

initiate a first training process of a supervised machine learning model using the set of labels from the unsupervised machine learning model, wherein execution of the supervised machine learning model generates a set of clustered data;

initiate an inference process of the supervised machine learning model,

wherein output of the inference process generates the set of clustered data;

provide the set of clustered data to a label audit process for relabeling the set of clustered data, wherein the label audit process generates a set of relabeled clustered data;

initiate a second training process of the supervised machine learning model using the set of relabeled clustered data to update the supervised machine learning model; and

update the supervised machine learning model in a model data store for future inference processes on new data.

14. The detection system of claim 13, wherein the label audit process is based on an automatically generated label determined by the unsupervised machine learning model using a data characteristic from the set of data characteristics of the second unlabeled data received from the client device.

15. The detection system of claim 13, wherein the label audit process is based on a human-generated label.

16. The detection system of claim 13, wherein the label audit process is a weighted combination of a human-generated label and an automatically generated label determined by the unsupervised machine learning model.

17. The detection system of claim 13, wherein the processor is further caused to:

initiate an action based on the set of relabeled clustered data.

18. The detection system of claim 13, wherein the second label associated with the second unlabeled data is a data anomaly or outlier data.

19. The detection system of claim 13, wherein the first unlabeled data and the second unlabeled data comprise telemetry data.

20. A non-transitory computer-readable storage medium storing a plurality of instructions executable by one or more processors, the plurality of instructions when executed by the processor causes the processor to:

at a first time, assign a first label of a set of labels to first unlabeled data using an unsupervised machine learning model;

at a second time, receive, from a client device, second unlabeled data;

provide the second unlabeled data to the unsupervised machine learning model to:

assign the first label of the set of labels to a first set of the second unlabeled data that is similar to the first unlabeled data based on a set of data characteristics,

generate a second label of the set of labels for a second set of the second unlabeled data that is not similar to the first unlabeled data based on the set of data characteristics, and

assign the second label of the set of labels to the second set of the second unlabeled data;

store the set of labels and the set of data characteristics with a label data store;

receive the set of labels from the label data store;

initiate a first training process of a supervised machine learning model using the set of labels from the unsupervised machine learning model, wherein execution of the supervised machine learning model generates a set of clustered data;

initiate an inference process of the supervised machine learning model, wherein output of the inference process generates the set of clustered data;

provide the set of clustered data to a label audit process for relabeling the set of clustered data, wherein the label audit process generates a set of relabeled clustered data;

initiate a second training process of the supervised machine learning model using the set of relabeled clustered data to update the supervised machine learning model; and

update the supervised machine learning model in a model data store for future inference processes on new data.