Claims

What is claimed is:

1. A method for performing threat detection comprising:

receiving, by a detection system, a set of labels that are generated using an unsupervised machine learning model, the set of labels received from a label data store;

initiating, by the detection system, a training process of a supervised machine learning model using the set of labels from the unsupervised machine learning model;

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

storing, 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 generating the set of labels comprises:

executing the unsupervised machine learning model to identify clusters in unlabeled data; and

automatically assigning, by the unsupervised machine learning model, labels that encode cluster membership for the unlabeled data without human labeling intervention.

3. The method of claim 1, wherein generating the set of labels comprises: executing the unsupervised machine learning model to reduce a number of input variables or features from unlabeled data and transform the unlabeled data into a low-dimensional space to produce a transformed representation; and

Automatically assigning , by the unsupervised machine learning model, labels for the unlabeled data based on the transformed representation.

4. The method of claim 1, wherein generating the set of labels comprises: executing the unsupervised machine learning model to automatically assign binary labels to indicate whether unlabeled data is outlier data or normal data.

5. The method of claim 1, wherein the set of labels that was determined from the unsupervised machine learning model is provided as input to the supervised machine learning model, and the training process iteratively adjusts parameters of the supervised machine learning model to minimize a difference between predictions and true labels.

6. The method of claim 1, further comprising:

generating a confidence score associated with the inference process of the supervised machine learning model, wherein the confidence score is a likelihood that unlabeled data received by the unsupervised machine learning model is to be grouped in the set of clustered data.

7. The method of claim 6, wherein the confidence score is determined for each cluster in the set of clustered data and a greatest confidence score associated with a particular cluster determines which cluster data are assigned.

8. The method of claim 6, wherein the confidence score is determined for each cluster in the set of clustered data and the confidence score is a thresholding for classification.

9. The method of claim 6, wherein the confidence score corresponds with a determination that the unlabeled data is outlier data when it is not similar to existing data.

10. The method of claim 1, further comprising:

initiating an action based on the inference process of the supervised machine learning model.

11. The method of claim 10, wherein the action comprises updating a display that identifies an inference associated with the set of clustered data.

12. The method of claim 10, wherein the action comprises sending a notification to remove a device from communicating with a detection system via a network.

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

14. A detection system comprising:

a memory; and

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

receive a set of labels that are generated using an unsupervised machine learning model, the set of labels received from a label data store;

initiate a training process of a supervised machine learning model using the set of labels from the unsupervised machine learning model;

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

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

15. The detection system of claim 14, wherein generating the set of labels comprises: executing the unsupervised machine learning model to identify clusters in unlabeled data; and

automatically assigning, by the unsupervised machine learning model, labels that encode cluster membership for the unlabeled data without human labeling intervention.

16. The detection system of claim 14, wherein generating the set of labels comprises:

executing the unsupervised machine learning model to a number of input variables or features from unlabeled data and transform the unlabeled data into a low-dimensional space; and

automatically assigning, by the unsupervised machine learning model, labels for the unlabeled data based on the transformed representation.

17. The detection system of claim 14, wherein generating the set of labels comprises :

executing the unsupervised machine learning model to automatically assign binary labels to indicate whether unlabeled data is outlier data or normal data.

18. The detection system of claim 14, wherein the set of labels that was determined from the unsupervised machine learning model is provided as input to the supervised machine learning model, and the training process iteratively adjusts parameters of the supervised machine learning model to minimize a difference between predictions and true labels.

19. The detection system of claim 14, wherein the processor is further caused to:

initiate an action based on the inference process of the supervised machine learning model.

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:

receive a set of labels that are generated using an unsupervised machine learning model, the set of labels received from a label data store;

initiate a training process of a supervised machine learning model using the set of labels from the unsupervised machine learning model;

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

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