Claims

1. A computer-implemented method of detecting potential cybersecurity threats from collected data pertaining to a monitored network, the collected data comprising at least one of network data and endpoint data, the method comprising:

structuring the collected data as at least one data matrix, each row of the data matrix being a datapoint and each column corresponding to a feature;

identifying at least one of the datapoints as anomalous, thereby detecting a potential cybersecurity threat, wherein the datapoint is identified as anomalous based on an anomaly score computed as:

a sum of squared components of a corresponding row of a residuals matrix, or

a sum of squared components of a second-pass coordinate vector for the datapoint; and

extracting causal information about the anomalous datapoint based on an angular relationship between the second-pass coordinate vector of the anomalous datapoint and a second-pass coordinate vector of at least one of the features,

the second-pass coordinate vectors determined by applying a second-pass singular value decomposition (SVD) to the residuals matrix,

the residuals matrix computed between the data matrix and an approximation of the data matrix, by applying a first-pass truncated SVD to the data matrix.

2. The method of claim 1, wherein the causal information is extracted based on (i) the angular relationship and (ii) magnitude information about the second-pass coordinate vector of the feature.

3. The method of claim 1, comprising applying an unsupervised classification process to an initial data matrix, the initial data matrix comprising rows corresponding to the datapoints, to classify each row of the initial data matrix in relation to a set of classes.

4. The method of claim 3, wherein the unsupervised classification process comprises:

applying an initial SVD to the initial data matrix, to determine an initial coordinate vector for each row of the initial data matrix, and

applying an unsupervised clustering algorithm to the initial coordinate vectors to determine a plurality of clusters of those initial coordinate vectors.

5. The method of claim 3, wherein the data matrix to which the first-pass SVD is applied has (i) at least one class column indicating classes to which the datapoints are assigned and (ii) feature columns corresponding to other features.

6. The method of claim 5, comprising applying an unsupervised classification process to an initial data matrix, the initial data matrix comprising rows corresponding to the datapoints, to classify each row of the initial data matrix in relation to a set of classes, wherein the initial data matrix to which the unsupervised classification process is applied comprises said feature columns, wherein the data points are classified based on said other features to determine the at least one class column for applying the first-pass SVD.

7. The method of claim 6, wherein the datapoints are re-clustered by applying an unsupervised clustering algorithm to first-pass coordinate vectors thereof, the first-pass coordinate vectors determined in the first-pass SVD.

8. The method of claim 3, wherein the data is partitioned into multiple partitions based on the results of the unsupervised classification, wherein the data matrix to which the first-pass SVD is applied corresponds to a single partition of the multiple partitions, whereby the residuals matrix is specific to that single partition.

9. The method of claim 8, wherein the collected data is structured into multiple data matrices, each corresponding to a different one of the partitions, and the identifying and extracting steps are applied separately to each of the multiple data matrices.

10. The method of claim 1, comprising the step of controlling a user interface to provide, to an analyst, the causal information about the anomalous datapoint.

11. The method of claim 10,

wherein the causal information is provided in response to determining that an escalation condition is met, the escalation condition dependent on the anomaly score.

12. The method of claim 11, wherein the collected data is used to create and populate a set of case records, each case record associated with a threat score, wherein at least one of the

cases pertains to the anomalous datapoint and the threat score of that case is dependent on the anomaly score, wherein the case is rendered available via the user interface when its threat score meets the escalation condition and the causal information is provided as part of the case record.

13. The method of claim 1, wherein each datapoint corresponds to a network endpoint, the method being applied to identify at least one anomalous network endpoint.

14. The method of claim 1, wherein the data matrix corresponds to a single process, each datapoint corresponding to an instance of that single process, the method being applied to identity at least one anomalous instance of that process.

15. The method of claim 1, wherein each datapoint corresponds to a network address, the method being applied to identify at least one anomalous network address.

16. A computer system comprising one or more hardware computers programmed or otherwise-configured to carry out a method of detecting potential cybersecurity threats from collected data pertaining to a monitored network, the collected data comprising at least one of network data and endpoint data, the method comprising:

structuring the collected data as at least one data matrix, each row of the data matrix being a datapoint and each column corresponding to a feature;

identifying at least one of the datapoints as anomalous, thereby detecting a potential cybersecurity threat, wherein the datapoint is identified as anomalous based on an anomaly score computed as:

a sum of squared components of a corresponding row of a residuals matrix, or

a sum of squared components of a second-pass coordinate vector for the datapoint; and

extracting causal information about the anomalous datapoint based on an angular relationship between the second-pass coordinate vector of the anomalous datapoint and a second-pass coordinate vector of at least one of the features,

the second-pass coordinate vectors determined by applying a second-pass singular value decomposition (SVD) to the residuals matrix,

the residuals matrix computed between the data matrix and an approximation of the data matrix, by applying a first-pass truncated SVD to the data matrix.

17. A non-transitory computer-readable medium comprising program instructions for programming a computer or a set of computers to carry out an anomaly detection method, the method comprising:

determining a data matrix from a set of collected data, each row of the data matrix being a datapoint and each column corresponding to a feature;

identifying at least one of the datapoints as anomalous, wherein the datapoint is identified as anomalous based on an anomaly score computed as:

a sum of squared components of a corresponding row of a residuals matrix, or

a sum of squared components of a second-pass coordinate vector for the datapoint; and

extracting causal information about the anomalous datapoint based on an angular relationship between the second-pass coordinate vector of the anomalous datapoint and a second-pass coordinate vector of at least one of the features,

the second-pass coordinate vectors determined by applying a second-pass singular value decomposition (SVD) to the residuals matrix,

the residuals matrix computed between the data matrix and an approximation of the data matrix, by applying a first-pass truncated SVD to the data matrix.