WHAT IS CLAIMED IS:

1. A method comprising:

receiving, with at least one processor, data associated with a plurality of entities, wherein the data comprises a static characteristic of each entity of the plurality of entities, a dynamic characteristic of each entity of the plurality of entities, and a risk score of each entity of the plurality of entities, and wherein the risk score of each entity of the plurality of entities indicates a probability of an anomaly occurring with regard to a behavior of that entity;

generating, with the at least one processor, a relational graph based on the static characteristic of each entity of the plurality of entities, the relational graph comprising a plurality of nodes and a plurality of edges, wherein each node represents an entity of the plurality of entities, and wherein each edge is associated with a static characteristic that is shared between two nodes of the plurality of nodes connected by that edge;

selecting, with the at least one processor, a target entity from the plurality of entities by selecting a target node from the plurality of nodes on the relational graph, wherein the target node represents the target entity, and wherein the target entity comprises a first static characteristic;

determining, with the at least one processor, a peer group of the target entity based on the relational graph and the first static characteristic, wherein the peer group comprises a subset of the plurality of nodes, and wherein the subset of the plurality of nodes represents a subset of the plurality of entities that share the first static characteristic with the target entity;

calculating, with the at least one processor, an average of the risk scores of the peer group and a standard deviation of the risk scores of the peer group;

determining, with the at least one processor, whether a systematic change in the behavior in the peer group has occurred based on the average of the risk scores of the peer group and the standard deviation of the risk scores of the peer group, wherein determining whether a systematic change in the behavior in the peer group has occurred comprises:

generating a ratio of the average of the risk scores of the peer group to the standard deviation of the risk scores of the peer group;

determining whether the ratio satisfies a threshold value; and

determining that a systematic change in the behavior in the peer group has occurred based on the ratio satisfying the threshold value;

determining, with the at least one processor, whether a change in behavior of the target entity is a false anomaly or a true anomaly based on determining that a systematic change in the behavior in the peer group has occurred; and

performing, with the at least one processor, an action based on determining whether the change in behavior of the target entity is a false anomaly or a true anomaly.

2. The method of claim 1, further comprising:

determining a temporal sequence of a value of the dynamic characteristic over a period of time for each entity of the plurality of entities; and

determining a length of an edge connecting a first node associated with a first entity and a second node associated with a second entity based on the temporal sequences of the first and second entities represented by the first and second nodes, wherein the length of the edge connecting the two nodes comprises an indication of a degree of similarity with regard to the dynamic characteristic between the temporal sequence of the first entity and the temporal sequence of the second entity; and

wherein generating the relational graph comprises:

generating the relational graph based on the length of the edge connecting the first node associated with the first entity and the second node associated with the second entity.

3. The method of claim 1, wherein the plurality of nodes is a first plurality of nodes, and wherein determining the peer group of the target entity comprises:

selecting a target node from the first plurality of nodes, wherein the target node represents the target entity;

sorting a second plurality of nodes, wherein the second plurality of nodes is a subset of nodes of the first plurality of nodes, and wherein sorting the second plurality of nodes comprises:

sorting the second plurality of nodes based on a length of an edge connecting the target node to each of the second plurality of nodes to provide a sorted second plurality of nodes; and

determining the peer group of the target entity based on the sorted second plurality of nodes.

4. The method of claim 1, wherein determining whether a systematic change in the behavior in the peer group has occurred comprises:

determining that a systematic change in the behavior in the peer group has not occurred based on the ratio not satisfying the threshold value.

5. The method of claim 1, wherein determining whether the change in behavior of the target entity is a false anomaly or a true anomaly comprises:

determining that the change in the behavior of the target entity is a false anomaly based on determining that a systematic change in the behavior of the peer group has occurred; and

wherein performing the action comprises:

performing the action based on determining that the change in behavior of the target entity is a false anomaly.

6. The method of claim 5, wherein performing the action based on determining that the change in behavior of the target entity is a false anomaly comprises:

modifying an anomaly detection alert associated with the target entity based on determining that the change in the behavior of the target entity is a false anomaly; or

transmitting an anomaly detection alert associated with the target entity based on determining that the change in the behavior of the target entity is a false anomaly.

7. A system comprising at least one processor programmed or configured to:

receive data associated with a plurality of entities, wherein the data comprises a static characteristic of each entity of the plurality of entities, a dynamic characteristic of each entity of the plurality of entities, and a risk score of each entity

of the plurality of entities, and wherein the risk score of each entity of the plurality of entities indicates a probability of an anomaly occurring with regard to a behavior of that entity;

generate a relational graph based on the static characteristic of each entity of the plurality of entities, the relational graph comprising a plurality of nodes and a plurality of edges, wherein each node represents an entity of the plurality of entities, and wherein each edge is associated with a static characteristic that is shared between two nodes of the plurality of nodes connected by that edge;

select a target entity from the plurality of entities by selecting a target node from the plurality of nodes on the relational graph, wherein the target node represents the target entity, and wherein the target entity comprises a first static characteristic;

determine a peer group of the target entity based on the relational graph and the first static characteristic, wherein the peer group comprises a subset of the plurality of nodes, and wherein the subset of the plurality of nodes represent a subset of the plurality of entities that share the first static characteristic with the target entity;

calculate an average of the risk scores of the peer group and a standard deviation of the risk scores of the peer group;

determine whether a systematic change in the behavior in the peer group has occurred based on the average of the risk scores of the peer group and the standard deviation of the risk scores of the peer group, wherein, when determining whether a systematic change in the behavior in the peer group has occurred, the at least one processor is programmed or configured to:

generate a ratio of the average of the risk scores of the peer group to the standard deviation of the risk scores of the peer group;

determine whether the ratio satisfies a threshold value; and

determine that a systematic change in the behavior in the peer group has occurred based on the ratio satisfying the threshold value;

determine whether a change in behavior of the target entity is a false anomaly or a true anomaly based on determining that a systematic change in the behavior in the peer group has occurred; and

perform an action based on determining whether the change in behavior of the target entity is a false anomaly or a true anomaly.

8. The system of claim 7, wherein the at least one processor is further programmed or configured to:

determine a temporal sequence of a value of the dynamic characteristic over a period of time for each entity of the plurality of entities; and

determine a length of an edge connecting a first node associated with a first entity and a second node associated with a second entity based on the temporal sequences of the first and second entities represented by the first and second nodes, wherein the length of the edge connecting the two nodes comprises an indication of a degree of similarity with regard to the dynamic characteristic between the temporal sequence of the first entity and the temporal sequence of the second entity; and

wherein, when generating the relational graph, the at least one processor is further programmed or configured to:

generate the relational graph based on the length of the edge connecting the first node associated with the first entity and the second node associated with the second entity.

9. The system of claim 7, wherein the plurality of nodes is a first plurality of nodes, and wherein, when determining the peer group of the target entity, the at least one processor is programmed or configured to:

select a target node from the first plurality of nodes, wherein the target node represents the target entity;

sort a second plurality of nodes, wherein the second plurality of nodes is a subset of nodes of the first plurality of nodes, and wherein, when sorting the second plurality of nodes, the at least one processor is programmed or configured to:

sort the second plurality of nodes based on a length of an edge connecting the target node to each of the second plurality of nodes to provide a sorted second plurality of nodes; and

determine the peer group of the target entity based on the sorted second plurality of nodes.

10. The system of claim 7, wherein, when determining whether a systematic change in the behavior in the peer group has occurred, the at least one processor is programmed or configured to:

determine that a systematic change in the behavior in the peer group has not occurred based on the ratio not satisfying the threshold value.

11. The system of claim 7, wherein, when determining whether the change in behavior of the target entity is a false anomaly or a true anomaly, the at least one processor is programmed or configured to:

determine that the change in the behavior of the target entity is a false anomaly based on determining that a systematic change in the behavior of the peer group has occurred; and

wherein, when performing the action, the at least one processor is programmed or configured to:

perform the action based on determining that the change in behavior of the target entity is a false anomaly.

12. The system of claim 11, wherein, when performing the action based on determining that the change in behavior of the target entity is a false anomaly, the at least one processor is programmed or configured to:

modify an anomaly detection alert associated with the target entity based on determining that the change in the behavior of the target entity is a false anomaly; or

transmit an anomaly detection alert associated with the target entity based on determining that the change in the behavior of the target entity is a false anomaly.

13. A computer program product comprising at least one non-transitory computer-readable medium including one or more instructions that, when executed by at least one processor, cause the at least one processor to:

receive data associated with a plurality of entities, wherein the data comprises a static characteristic of each entity of the plurality of entities, a dynamic characteristic of each entity of the plurality of entities, and a risk score of each entity of the plurality of entities, and wherein the risk score of each entity of the plurality of

entities indicates a probability of an anomaly occurring with regard to a behavior of that entity;

generate a relational graph based on the static characteristic of each entity of the plurality of entities, the relational graph comprising a plurality of nodes and a plurality of edges, wherein each node represents an entity of the plurality of entities, and wherein each edge is associated with a static characteristic that is shared between two nodes of the plurality of nodes connected by that edge;

select a target entity from the plurality of entities by selecting a target node from the plurality of nodes on the relational graph, wherein the target node represents the target entity, and wherein the target entity comprises a first static characteristic;

determine a peer group of the target entity based on the relational graph and the first static characteristic, wherein the peer group comprises a subset of the plurality of nodes, and wherein the subset of the plurality of nodes represent a subset of the plurality of entities that share the first static characteristic with the target entity;

calculate an average of the risk scores of the peer group and a standard deviation of the risk scores of the peer group;

determine whether a systematic change in the behavior in the peer group has occurred based on the average of the risk scores of the peer group and the standard deviation of the risk scores of the peer group, wherein the instructions that cause the at least one processor to determine whether a systematic change in the behavior in the peer group has occurred cause the at least one processor to:

generate a ratio of the average of the risk scores of the peer group to the standard deviation of the risk scores of the peer group;

determine whether the ratio satisfies a threshold value; and

determine that a systematic change in the behavior in the peer group has occurred based on the ratio satisfying the threshold value;

determine whether a change in behavior of the target entity is a false anomaly or a true anomaly based on determining that a systematic change in the behavior in the peer group has occurred; and

perform an action based on determining whether the change in behavior of the target entity is a false anomaly or a true anomaly.

14. The computer program product of claim 13, wherein the one or more instructions further cause the at least one processor to:

determine a temporal sequence of a value of the dynamic characteristic over a period of time for each entity of the plurality of entities; and

determine a length of an edge connecting a first node associated with a first entity and a second node associated with a second entity based on the temporal sequences of the first and second entities represented by the first and second nodes, wherein the length of the edge connecting the two nodes comprises an indication of a degree of similarity with regard to the dynamic characteristic between the temporal sequence of the first entity and the temporal sequence of the second entity; and

wherein, the one or more instructions that cause the at least one processor to generate the relational graph, further cause the at least one processor to:

generate the relational graph based on the length of the edge connecting the first node associated with the first entity and the second node associated with the second entity.

15. The computer program product of claim 13, wherein the plurality of nodes is a first plurality of nodes, and wherein, when determining the peer group of the target entity, the one or more instructions cause the at least one processor to:

select a target node from the first plurality of nodes, wherein the target node represents the target entity;

sort a second plurality of nodes, wherein the second plurality of nodes is a subset of nodes of the first plurality of nodes, and wherein, the one or more instructions that cause the at least one processor to sort the second plurality of nodes, further cause the at least one processor to:

sort the second plurality of nodes based on a length of an edge connecting the target node to each of the second plurality of nodes to provide a sorted second plurality of nodes; and

determine the peer group of the target entity based on the sorted second plurality of nodes.

16. The computer program product of claim 13, wherein, the one or more instructions that cause the at least one processor to determine whether a

systematic change in the behavior in the peer group has occurred, further cause the at least one processor to:

determine that a systematic change in the behavior in the peer group has not occurred based on the ratio not satisfying the threshold value.

17. The computer program product of claim 13, wherein the one or more instructions that cause the at least one processor to determine whether the change in behavior of the target entity is a false anomaly or a true anomaly, further cause the at least one processor to:

determine that the change in the behavior of the target entity is a false anomaly based on determining that a systematic change in the behavior of the peer group has occurred; and

wherein, the one or more instructions that cause the at least one processor to perform the action, further cause the at least one processor to:

perform the action based on determining that the change in behavior of the target entity is a false anomaly.

18. The computer program product of claim 17, wherein, the one or more instructions that cause the at least one processor to perform the action based on determining that the change in behavior of the target entity is a false anomaly further cause the at least one processor to:

modify an anomaly detection alert associated with the target entity based on determining that the change in the behavior of the target entity is a false anomaly; or

transmit an anomaly detection alert associated with the target entity based on determining that the change in the behavior of the target entity is a false anomaly.