

We claim:

1. A computer-readable medium comprising computer-executable instructions that when executed by a processor perform a method comprising:

transmitting electronic signals configured to display a ranking of plurality of user accounts that represent a threat to an organization, wherein the ranking is determined by monitoring values of at least four controls for each of the plurality of user accounts over a first time period, wherein the controls are selected from the group consisting of:

a quantity of bandwidth utilized by a user account over a first network;

blocked transmissions by a user account over the first network;

blocked communication through a targeted communication application;

non-blocked communication through the targeted communication application that violates at least one predefined criterion;

an association of at least one security application with the user account, wherein if a at least one software application is associated with the user account, then:

monitoring illegal storage attempts; and

recording a filename associated with illegal storage attempts; and

determining if communications through the first network are transmitted or received through an unauthorized protocol;

comparing the values of the at least four controls over the first time period with values of the at least four controls over a second time period; and

transmitting electronic signals configured to display a ranking of plurality of user accounts.

2. The computer-readable medium of claim 1, wherein the blocked transmissions by the user account over the first network are classified into a category selected from the group consisting of: a security threat, an ethics threat, and combinations thereof.

3. The computer-readable medium of claim 2, the computer-executable instructions further comprising:

receiving a user input selecting a graphical representation of the blocked communication through the first network; and

displaying whether the blocked communication was a security threat, an ethics threat or combinations thereof.

4. The computer-readable medium of claim 1, wherein an account weight has been applied to at least one user account displayed, wherein the account weight is assigned to the at least one user account, if the user account is within a category selected from the group consisting of:

granted access rights to a specific collection of data, exempt from having the at least one security application, the at least one security application is absent; access rights to at least one service has been deactivated, and combinations thereof.

5. The computer-readable medium of claim 4, wherein the at least one user account are weighted according to the values set forth in Table 2.

6. The computer-readable medium of claim 4, the instruction further comprising:

receiving a user input providing a new account weight to be applied to at least one of the plurality of user accounts; and

re-ranking a plurality of accounts using the new account weight.

7. The computer-readable medium of claim 2, the instruction further comprising:

receiving a user input requesting the re-ranking of the plurality of user accounts based upon one of the controls.

8. The computer-readable medium of claim 4, the instructions further comprising:

receiving a user input selecting a user account from the plurality of user accounts; and

displaying the user accounts ranking for a plurality of controls selected from the group consisting of:

the quantity of bandwidth utilized by the user account over the first network, denied access attempts by the user account over the first network, blocked communications through the targeted communication application, non-blocked communications through the targeted communication application that violates at least one predefined criterion, the presence of at least one security application with the user account, communications through the first network is transmitted or received through an unauthorized protocol, and combinations thereof.

9. The computer-readable medium of claim 1, wherein the first time period is less than about 3 days and the second time period is more than about 40 days.

10. The computer-readable medium of claim 1, wherein a control weight has been applied to at least one control utilized in determining the threat rating, wherein the weight is assigned to the at least one user account if the user account is within a group selected from the groups consisting of:

a security threat, an ethics threat, blocked communication through the targeted communication application, communication through the targeted communication application meeting the predefined criterion, accessing the centralized store, an attempted illegal storage attempt, and combinations thereof.

11. The computer-readable medium of claim 10, the instruction further comprising:

receiving a user input providing a new control weight to be applied to at least one of the plurality of controls; and

re-ranking a plurality of accounts using the new control weight.

12. The method of claim 10, further comprising:

determining that an activity of one of the controls occurred during a first time frame during either the first time period or the second time period; and

applying a second weight to the activity that occurred during the time frame.

13. The method of claim 10, further comprising:

further weighting a control if incidence of activity for that control is above a predetermined threshold.

14. The method of claim 13, wherein the predetermined threshold is based upon, the user account's average activity, average activity of other user accounts, or combinations thereof.

15. The method of claim 10, wherein the activities that occurred during the first time period are weighted differently than the activities that occurred during the second time period.

16. The method of claim 15, wherein the activities that occurred during the first time period and the second time period are weighted according to the values set forth in Table 2.

17. An apparatus comprising:

a communications module configured to receive data from a plurality of applications, the data relating to values of at least four controls for each of the plurality of user accounts over a first time period, wherein the controls are selected from the group consisting of:

- a quantity of bandwidth utilized by a user account over a first network;
- blocked transmissions by a user account over the first network;
- blocked communication through a targeted communication application;
- non-blocked communication through the targeted communication application that violates at least one predefined criterion;
- determining if any communications through the first network is transmitted or received through an unauthorized protocol;
- an application detection module configured to determine an association of at least one security application with each of the user accounts; and
- a processor configured to calculate a predictive threat score for a plurality of user accounts that compares the values of the at least four controls over the first time period with values of the at least four controls over a second time period; and
18. The apparatus of claim 17, wherein the processor is further configured to determine that an activity of one of the controls occurred during a first time frame during either the first time period or the second time period; and
- applying a second weight to the activity that occurred during the time frame.
19. The apparatus of claim 17, further comprising:
- further weighting a control if incidence of activity for that control is above a predetermined threshold.
20. The apparatus of claim 19, wherein the predetermined threshold is based upon, the user account's average activity, average activity of other user accounts, or combinations thereof.
21. The apparatus of claim 17, wherein the activities that occurred during the first time period are weighted differently than the activities that occurred during the second time period.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A non-transitory computer-readable medium storing computer-executable instructions that when executed by a processor cause the processor to perform:

calculating a ranking of a plurality of user accounts within an organization that represent a threat to the organization, wherein the ranking is determined by a predictive threat score for each user account of the plurality of user accounts, wherein the predictive threat score is based on a comparison of a first set of at least four values that are monitored over a first time period to a second set of at least four values that are monitored over a second time period, and wherein the values of the first set of values and the second set of values for each user account are selected from the group consisting of:

a value corresponding to a quantity of bandwidth utilized by the user account over a network;

a value corresponding to a number of blocked transmissions by the user account over the network;

a value corresponding to a number of blocked communications through a targeted communication application, the targeted communication application allowing a first user to communicate directly with another individual;

a value corresponding to a number of non-blocked communications through the targeted communication application that violates at least one predefined criterion;

a value indicating whether at least one security application is associated with the user account;

a value indicating an illegal storage attempt; and

a value indicating whether a communication has been transmitted or received through the network via an unauthorized protocol; and

transmitting electronic signals configured to display the ranking of the plurality of user accounts.

2. The computer-readable medium of claim 1, wherein the blocked transmissions by the user account over the network are classified into a category selected from the group consisting of: a security threat, an ethics threat, and combinations thereof.

3. The computer-readable medium of claim 2, the computer-executable instructions further comprising:

receiving a user input selecting a graphical representation of the blocked communication through the network; and

displaying whether the blocked communication was a security threat, an ethics threat or combinations thereof.

4. The computer-readable medium of claim 1, wherein an account weight has been applied to at least one user account displayed, wherein the account weight is assigned to the at least one user account, if the user account is within a category selected from the group consisting of:

granted access rights to a specific collection of data, exempt from having the at least one security application, the at least one security application is absent; access rights to at least one service has been deactivated, and combinations thereof.

5. The computer-readable medium of claim 4, wherein the at least one user account are weighted according to weights set forth in Table 2.

6. The computer-readable medium of claim 4, the instruction further comprising:

receiving a user input providing a new account weight to be applied to at least one of the plurality of user accounts; and

re-ranking a plurality of accounts using the new account weight.

7. The computer-readable medium of claim 2, the instruction further comprising:
receiving a user input requesting the re-ranking of the plurality of user accounts based upon one of the values the predictive threat score is based on.
8. The computer-readable medium of claim 4, the instructions further comprising:
receiving a user input selecting a user account from the plurality of user accounts;
and
displaying the ranking for a plurality of values selected from the group consisting of:

a value corresponding to the quantity of bandwidth utilized by the user account over the network, a value corresponding to a number of denied access attempts by the user account over the network, a value corresponding to a number of blocked communications through the targeted communication application, a value corresponding to a number of non-blocked communications through the targeted communication application that violate at least one predefined criterion, a value indicating whether at least one security application is associated with the user account, a value indicating whether communications through the network are transmitted or received via an unauthorized protocol, and combinations thereof.
9. The computer-readable medium of claim 1, wherein the first time period is less than about 3 days and the second time period is more than about 40 days.
10. The computer-readable medium of claim 1, wherein a value weight has been applied to at least one value utilized in determining the predictive threat score, wherein the weight is assigned to the at least one user account if the user account is within a group selected from the groups consisting of:

a security threat, an ethics threat, blocked communication through the targeted communication application, communication through the targeted communication

application meeting the predefined criterion, accessing the centralized store, an attempted illegal storage attempt, and combinations thereof.

11. The computer-readable medium of claim 10, the instruction further comprising:
receiving a user input providing a new value weight to be applied to at least one of the values; and
re-ranking a plurality of accounts using the new value weight.
12. The computer-readable medium of claim 10, further comprising:
determining that an activity associated with one of the values occurred during a time frame of either the first time period or the second time period; and
applying a second value weight to the activity that occurred during the time frame.
13. The computer-readable medium of claim 10, further comprising:
further weighting one of the values if incidence of activity associated with the value is above a predetermined threshold.
14. The computer-readable medium of claim 13, wherein the predetermined threshold is based upon an average activity of one of the user accounts of the plurality of user accounts, an average activity of at least one of the other user accounts of the plurality of user accounts, or combinations thereof.
15. The computer-readable medium of claim 10, wherein the activities that occurred during the first time period are weighted differently than the activities that occurred during the second time period.

16. The computer-readable medium of claim 15, wherein the activities that occurred during the first time period and the second time period are weighted according to weights set forth in Table 2.

17. An apparatus comprising:

a communications module configured to receive data from a plurality of applications, the data relating to a first set of at least four values and a second set of at least four values associated with each user account of a plurality of user accounts within an organization, wherein the first set of values are monitored over a first time period and the second set of values are monitored over a second time period, and wherein the values of the first set of values and the second set of values for each user account are selected from the group consisting of:

a value corresponding to a quantity of bandwidth utilized by the user account over a network;

a value corresponding to a number of blocked transmissions by the user account over the network;

a value corresponding to a number of blocked communications through a targeted communication application, the targeted communication application allowing a first user to communicate directly with another individual;

a value corresponding to a number of non-blocked communications through the targeted communication application that violate at least one predefined criterion; and

a value indicating whether a communication has been transmitted or received through first network via an unauthorized protocol;

an application detection module configured to determine whether at least one security application is associated with at least one of the user accounts; and

a processor configured to respectively calculate a predictive threat score for each user account of the plurality of user accounts based on a comparison of the first set of

values to the second of values that are respectively associated with each user account of the plurality of user accounts.

18. The apparatus of claim 17, wherein the processor is further configured to determine that an activity associated with one of the values occurred during a time frame of either the first time period or the second time period; and

applying a second value weight to the activity that occurred during the time frame.

19. The apparatus of claim 17, further comprising:

further weighting one of the values if incidence of activity associated with the value is above a predetermined threshold.

20. The apparatus of claim 19, wherein the predetermined threshold is based upon an average activity of one of the user accounts of the plurality of user accounts, an average activity of at least one of the other user accounts of the plurality of user accounts, or combinations thereof.

21. The apparatus of claim 17, wherein the activities that occurred during the first time period are weighted differently than the activities that occurred during the second time period.