

We claim:

1. A computer-implemented method comprising:

calculating a first threat score corresponding to a first time period for a plurality of user accounts, each user account having access to a first network and at least a portion of the user accounts having access to a second network that comprises a centralized store of electronic data, the calculations of the first threat score for each user account comprising:

receiving at least one of an indication of activity through the first network for the presence of a security threat, an ethics threat, or combinations thereof;

receiving an indication indicative of any blocked transmissions and non-blocked transmissions through a targeted communication application associated with the user account that meet a predefined criterion; and

determining if a transmission through the first network is transmitted or received through an unauthorized protocol; and

comparing the first threat score with a second threat score corresponding to a second time period to create an overall threat score.

2. The method of claim 1, further comprising:

applying a weight to at least one user account of the plurality of user accounts, wherein the weight is assigned to the at least one user account if the user account is in the group consisting of: granted access rights to a specific collection of data, exempt from having at least one software application, the at least one software application is absent; access rights to at least one service has been deactivated, and combinations thereof.

3. The method of claim 2, further comprising:

receiving an indication whether at least one security application is associated with the user account, wherein if the 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

if the at least one security application is not associated with the user account, then applying a first weight to the user account; and

wherein if the at least one security application is disabled for the user account, then applying a second weight to the user account.

4. The method claim 1, wherein the first time period is less than about 3 days and the second time period is more than about 40 days.

5. The method of claim 1, further comprising:
applying an activity weight to at least one activity selected from the group consisting of: a security threat, an ethics threat, blocked transmission of the targeted communication application, transmission through the targeted communication application meeting the predefined criterion, attempted access to the centralized store, an attempted illegal storage attempt, and combinations thereof.

6. The method of claim 5, further comprising:
applying a second activity weight to at least one activity if the at least one activity occurred during a first time frame within either the first or second time period.

7. The method of claim 6, wherein the first time frame is selected from a predefined quantity of time before a user associated with the user account is scheduled to utilize a network, a predefined quantity of time before or after an average time frame the user account is active on a network, a specific date, and combinations thereof.

8. The method of claim 5, further comprising:
applying a second activity weight to at least one activity if an incidence of activity is above a predetermined threshold.

9. The method of claim 8, wherein the predetermined threshold is based upon, the user account's average activity, average activity of other user accounts, or combinations thereof.

10. The method of claim 7, wherein the activities that occurred during the first time period are weighted differently than the activities that occurred during the second time period.

11. The method of claim 10, 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 1.

12. The method of claim 9, further comprising:

assigning a weight to at least one user account of the plurality of user accounts, wherein a weight is assigned to the at least one user account if classified in the group consisting of:

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

13. The method of claim 12, wherein the user accounts are weighted according to the values set forth in Table 2.

14. The method of claim 1, wherein a software application from the at least one software application is configured to perform an action selected from the group consisting of:

preventing unauthorized writing of data to a specific location, monitor a transfer of data through the first network, monitor a transfer of data using the communication protocol.

15. A computer-implemented method comprising:

calculating a threat score for a plurality of user accounts having access to a first network and at least a portion of the user accounts having access to a second network that comprises a centralized store of electronic data, comprising, for each user account determining an overall

threat score (f_{overall}), where $f_{\text{overall}} = \frac{(f_{\text{live}} + f_{\text{analytic}}) * f_{\text{weight}}}{2}$, wherein f_{live} includes the calculation of data from a first time period and is calculated for a plurality of activities, wherein for each activity:

$$f_{\text{live}} = \sum_{i=1}^n x_{\text{predefined}} \left(\frac{f_{\text{live}}}{n} \right) + \left(\frac{f_{\text{live}}}{n} \right) \left(\frac{f_{\text{live}}}{n} \right),$$

where x specifies a predefined activity selected from a plurality of activities, and

$$x_{\text{predefined}} = \begin{cases} 1, & \text{if } f_{\text{live}} > 0 \\ 0, & \text{if } f_{\text{live}} = 0 \end{cases}$$

wherein f_{analytic} includes the calculation of data from a second time period and is calculated for the plurality of activities of f_{live} , wherein:

$$f_{activity} = (spike_x + aboveavg_x + offHours_x) * (weight_{activity})$$

wherein $spike_x$ is assigned a zero value unless the user account comprises an activity level during the first time period that is over a first threshold level above an average of the same user account during the second time period;

wherein $aboveavg_x$ is assigned a zero unless the user account comprises an activity level that is over a first threshold level above an average of a plurality of user accounts for the same time period;

wherein $offhours_x$ is assigned a zero unless the user account comprises an activity level during a time frame during the first time period before or after the average start or end time for that user account; and

wherein f_{person} considers one or more weights given to the user account.

16. The method of claim 15, wherein $spike_x$ is assigned a first integer if the first threshold level of $spike_x$ is about 40% great than the average of the same user account during the second time period.

17. The method of claim 15, wherein the $aboveavg_x$ is assigned a first integer if the first threshold level of $aboveavg_x$ is above about 30% greater than the activity of the plurality of user accounts for the same time period.

18. The method of claim 15, wherein the $offhours_x$ is assigned a first integer if the activity level is detected about 6 hours before or after the average start or end time for that user account.

19. The method of claim 15, wherein an activity is selected from the group consisting of: a security threat, an ethics threat, blocked transmission through the targeted communication application, transmission through the targeted communication application meeting the predefined criterion, attempted access of the centralized store, an attempted illegal storage attempt, and combinations thereof.

20. The method of claim 15, wherein f_{person} is calculated according to:

$$f_{\text{person}} = 1 + \sum_{\text{category}} (\text{weight}_{\text{category}}).$$

We claim:

1. A computer-implemented method comprising:

determining, by a system having at least one computing device, a first threat score corresponding to a first time period for a plurality of user accounts comprising at least a first user account, each user account having access to a first network and at least a portion of the user accounts having access to a second network that comprises a centralized store of electronic data, the determined first threat score for each user account being based at least in part on:

receiving, by the system, at least one of an indication of activity through the first network for the presence of a security threat, an ethics threat, or combinations thereof;

receiving, by the system, an indication indicative of any blocked transmissions and non-blocked transmissions through a targeted communication application associated with the user account that meet a predefined criterion, wherein the targeted communication application is selected from the group consisting of: electronic mail (e-mail), instant messaging (IM), chatting, and combinations thereof; and

determining, by the system, if a transmission through the first network is transmitted or received through an unauthorized protocol;

comparing, by the system, the determined first threat score of the first user account with a second threat score of the same first user account corresponding to a second time period to identify an overall threat score for the first user account and a ranking of the first user account; and

displaying the ranking on a graphical user interface.

2. The method of claim 1, further comprising:

applying a weight to at least one user account of the plurality of user accounts, wherein the weight is assigned to the at least one user account if the user account is in the group consisting of: granted access rights to a specific collection of data, exempt from having at least one software application, the at least one software application is absent; access rights to at least one service has been deactivated, and combinations thereof.

3. The method of claim 2, further comprising:

receiving an indication whether at least one security application is associated with the user account, wherein if the at least one security application is associated with the user account, then:

monitoring illegal storage attempts; and

recording a filename associated with illegal storage attempts; and

if the at least one security application is not associated with the user account, then applying a first weight to the user account wherein the first weight is utilized in the calculation of the overall threat score; and

wherein if the at least one security application is disabled for the user account, then applying a second weight to the user account, wherein the second weight is utilized in the calculation of the overall threat score.

4. The method claim 1, wherein the first time period is less than 3 days and the second time period is more than 40 days.

5. The method of claim 1, further comprising:

applying an activity weight to at least one activity selected from the group consisting of: a security threat, an ethics threat, blocked transmission of the targeted communication application, transmission through the targeted communication application meeting the predefined criterion, attempted access to the centralized store, an attempted illegal storage attempt, and combinations thereof.

6. The method of claim 5, further comprising:

applying a second activity weight to at least one activity if the at least one activity occurred during a first time frame within either the first or second time period.

7. The method of claim 6, wherein the first time frame is selected from a predefined quantity of time before a user associated with the user account is scheduled to utilize a network, a predefined quantity of time before or after an average time frame the user account is active on a network, a specific date, and combinations thereof.

8. The method of claim 7, wherein the activities that occurred during the first time period are weighted differently than the activities that occurred during the second time period.

9. The method of claim 8, wherein individual instances of the activities of a security threat, an ethics threat, blocked transmission of the targeted communication application, transmission through the targeted communication application meeting the predefined criterion, attempted access to the centralized store, and an attempted illegal storage attempt that occurred during the first time period are assigned weights of 3.5, 1.5, 3.5, 5, 5, 3.5 and 4, respectively; and individual instances of the activities that occurred during the second time period are assigned weights of 2, 1, 2, 3, 3, 2 and 3, respectively.

10. The method of claim 5, further comprising:

applying a second activity weight to at least one activity if an incidence of activity is above a predetermined threshold.

11. The method of claim 10, wherein the predetermined threshold is based upon, the user account's average activity, average activity of other user accounts, or combinations thereof.

12. The method of claim 11, further comprising:

assigning a weight to at least one user account of the plurality of user accounts, wherein a weight is assigned to the at least one user account if classified in the group consisting of: access rights to a specific collection of data, exempt from having the at least one software application, the at least one software application is absent; access rights to at least one service has been deactivated, and combinations thereof.

13. The method of claim 12, wherein the user accounts classified by: access rights to a specific collection of data, exempt from having the at least one software application, the at least one software application is absent; access rights to at least one service has been deactivated are assigned weights of 2, 1.5, 1.5, 1, 1, and 2, respectively.

14. The method of claim 1, wherein a software application from the at least one software application is configured to perform an action selected from the group consisting of:

preventing unauthorized writing of data to a specific location, monitor a transfer of data through the first network, monitor a transfer of data using the communication protocol.

15. A computer-implemented method comprising:

determining, by a system having at least one computing device, a first threat score corresponding to a first time period for a plurality of user accounts within a first domain, the plurality of user accounts including a first user account assigned to a first individual, wherein each user account is assigned to a particular individual, and only a portion of the user accounts have access to a second network that comprises a centralized store of electronic data internal to the domain, the determined first threat score for each user account is based at least in part on:

receiving, by the system, at least one of an indication of activity by the user account through the first network for the presence of a security threat, an ethics threat, or combinations thereof;

receiving, by the system, an indication indicative by the user account of any blocked transmissions and non-blocked transmissions through a targeted communication application associated with the user account that meet a predefined criterion, wherein the targeted communication application is configured to permit the first individual to transmit and/or receive electronic information directly with a second account of the plurality of accounts that is associated with a second individual; and

determining, by the system, if a transmission by the user account through the first network is transmitted or received through an unauthorized protocol;

comparing, by the system, the first threat score of the first user account with a second threat score from the same first user account corresponding to a second time period to create an overall threat score for the first user account and a ranking for the first user account; and displaying the ranking on a graphical user interface.

16. The method of claim 15, wherein the targeted communication application is configured to transmit communications from the first user account assigned to the first individual to a second user account within the first domain assigned to a second individual.

17. The method of claim 15, wherein the targeted communication application is configured to transmit communications from the first user account assigned to the first individual to a second user account assigned to a second individual.