

What is claimed is:

1. A system for detecting behavior associated with a potential security breach of an enterprise, the system comprising:

a computing device;

a network in communication with the computer device;

a baseline generation and monitoring system in communication with the network;

a correlation/alert generator in communication with the network; and

a memory storing instructions that when executed, cause the baseline generation and monitoring system to:

identify an employee of the enterprise that represents an elevated risk of contributing to the potential security breach where the computing device is associated with the employee;

store a list of predetermined behaviors indicative of the potential security breach;

determine a baseline of the computing device behaviors;

monitor the computing device associated with the identified employee for occurrence of a behavior that exceeds the baseline;

monitor the behavior of the computing device for an occurrence of a second behavior that is related to the first behavior; and

generate an alert using the correlation and alert generator if both the first behavior and second behavior occurs.

2. The system of claim 1, wherein the elevated security risk is determined based on at least one of: criticality of an employee, extra-organizational threat intelligence, or input from an organization of which the employee is a member.

3. The system of claim 1, further comprising an event log which stores a history of computing device activity.

4. The system of claim 3, further comprising instructions that when executed, cause the baseline generation and monitoring system to:

normalize the computing device activity stored in the event log; and
generate a whitelist of activities from the normalized computing device activity.

5. The system of claim 4, further comprising instructions that cause the baseline generation and monitoring system to:

analyze a data feed comprising asset inventory information to identify new assets; and

add activities related to deploying these new assets to the whitelist of activities.

6. The system of claim 1, wherein the baseline of user activity is determined for at least one of: email activity, process activity, installations, register modifications, new proxy connections, new user agents, new user connections, new source authorizations, new attempted accesses, or new outbound data connections.

7. A method of detecting behavior associated with a potential security breach of an enterprise, the method comprising:

identifying an employee of the enterprise that represents an elevated risk of contributing to the potential security breach;

providing a list of predetermined behaviors indicative of the potential security breach;

determining a baseline of the behaviors;

monitoring a network for activity associated with the employee for occurrence of any of the behaviors that exceeds the baseline; and

generating an alert if at least one of the behaviors is detected from the network activity.

8. The method of claim 7, further comprising storing network activity associated with the employee in an event log.

9. The method of claim 8, further comprising the steps of:

normalizing the network activity stored in the event log that is related to behaviors indicative of the potential security breach; and

generating a whitelist of network activities from the normalized network activity.

10. The method of claim 9, wherein the step of monitoring network activity associated with the employee for occurrence of any of the behaviors comprises;

monitoring the network activity; and

detecting an activity related to behaviors indicative of the potential security breach that is not included on the whitelist of activities.

11. The method of claim 9, wherein a data feed comprised of asset inventory information is analyzed to identify new assets and predicted network activities related to deploying these new assets are added to the whitelist of activities.

12. The method of claim 7, wherein the employee is identified based on at least one of: criticality of the employee, extra-organizational threat intelligence, or input from an organization of which the employee is a member.

13. The method of claim 7, wherein the baseline of the behaviors indicative of the potential security breach is determined for at least one of: email activity, process activity, installations, register modifications, new proxy connections, new user agents, new user connections, new source authorizations, new attempted accesses, or new outbound data connections.

14. A method of detecting behavior associated with a potential security breach of an enterprise, the method comprising:

identifying an employee of the enterprise that represents an elevated risk of contributing to the potential security breach;

providing a list of predetermined behaviors indicative of the potential security breach;

storing network activity of the employee in an event log;

determining a baseline of the behaviors indicative of the potential security breach comprising at least one of: email activity, process activity, installations, register modifications, new proxy connections, new user agents, new user connections, new source authorizations, new attempted accesses, or new outbound data connections;

generating a whitelist of network activities from the network activity

developing use cases based on cyber-attack methodology;

monitoring the network activity;

detecting a network activity that is not included on the whitelist of activities;

comparing the detected activity to the use cases;

upon detection of network activity that satisfies a use case, monitoring the network activity for activity that satisfies a second use case that is related to the first use case; and

generating an alert if network activity compares to at least one second use case.

15. The method of claim 14, wherein identifying an employee that represents an elevated risk of contributing to a potential security breach is determined based on at least one of: criticality of the employee, extra-organizational threat intelligence, or input from an organization of which the employee is a member.
16. The method of claim 14, further comprising the step of normalizing the network activity stored in the event log.
17. The method of claim 16, wherein the step of generating a whitelist of network activities uses the normalized network activity.
18. The method of claim 14, further comprising the steps of:

analyzing a data feed comprised of asset inventory information to identify new assets; and

adding predicted activities on a network related to deploying these new assets to the whitelist of network activities.