alert. In one such exemplary embodiment, a predetermined group of computers are monitored to detect the occurrence of a predefined triggering event. Once a triggering event is detected, the method monitors the group of computers in order to detect a series of behaviors that are consistent with an ongoing cyber-attack.

[0005] In order to manage the amount of data monitored and recorded by an exemplary embodiment of the invention, likely targets of a cyber-attack are pre-identified based upon factors that would make the targets particularly attractive for such an attack. With likely targets having been identified, use cases are applied to detect computer system behaviors consistent with a probable cyber-attack. Once such behaviors are detected, an alert or other notification is provided to a party responsible for monitoring and investigating potential computer system threats.

[0005a] According to a first aspect of the present invention, there is provided 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.

[0005b] According to a second aspect of the present invention, there is provided 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.

[0005c] According to a third aspect of the present invention, there is provided 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.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] These and other features and advantages of the present invention will become better understood with regard to the following description and accompanying drawings in which:

[0007] Figure 1 represents an exemplary computer network;

[0008] Figure 2 illustrates a system for detecting cyber-attacks, according to an exemplary embodiment of the invention;

[0009] Figure 3 illustrates data flow within a system to implement a process of identifying a group of users for monitoring, according to an exemplary embodiment of the invention;

[0010] Figure 4 illustrates data flow within a system to implement a process to create baseline data according to an exemplary embodiment of the invention;

[0011] Figure 5 is a data flow diagram illustrating the delivery of an inventory feed to a baseline generator and correlation/alerting function, according to an exemplary embodiment of the invention;

[0012] Figure 6 is a diagram of an exemplary monitoring system detecting a cyber-attack; and

[0013] Figure 7 is a user interface of the system of Figure 6, according to an exemplary embodiment of the invention.