CLAIMS

What is claimed is:

1. A method comprising employing at least one hardware processor of a server computer system configured to protect a plurality of client systems against computer security threats to:

in response to receiving a forensic indicator, select a first routine for evaluating a first security predicate from a plurality of routines, the first routine selected according to the forensic indicator, wherein the forensic indicator comprises a plurality of metadata elements characterizing a network flow between a client system of the plurality of client systems and another party;

select a second routine for evaluating a second security predicate from the plurality of routines, the second routine selected according to a result of executing the first routine;

in response to selecting the first routine, add a first text message to a security alert indicating whether the client system is subject to a computer security threat, the first text message determined according to a first message template selected according to the first routine;

in response to selecting the second routine, add a second text message to the security alert, the second text message determined according to a second message template selected according to the second routine; and

transmit the security alert to an administration device configured to display the security alert to a human operator.

2. The method of claim 1, wherein evaluating the first security predicate comprises evaluating a third security predicate, and wherein the method further comprises employing at least one hardware processor of the server computer system to:

select a third routine for evaluating the third security predicate from the plurality of routines; and

add a third text message to the security alert in preparation for transmission to the administration device, the third text message determined according to a third message template selected according to the third routine.

3. The method of claim 2, wherein the first text message comprises a hyperlink which, when activated, causes a display of the third text message.

4. The method of claim 1, further comprising employing at least one hardware processor of the server computer system to:

determine a verdict indicating whether the client system is subject to the computer security threat, the verdict determined according to the result of executing the first routine and to another result of executing the second routine; and

add an indicator of the verdict to the security alert in preparation for transmission to the administration device.

5. The method of claim 1, wherein the first message template comprises a placeholder, and wherein determining the first text message comprises replacing the placeholder with a value of the first security predicate determined according to the result of executing the first routine.

6. The method of claim 1, wherein the first text message comprises an item selected from a group consisting of an indicator of a device type of the client system, an indicator of a geographical location of the another party, and an indicator of a time of occurrence of the electronic communication.

7. The method of claim 1, wherein the plurality of metadata elements comprises a tagged element computed according to another element of the plurality of metadata elements.

8. The method of claim 1, wherein the first text message comprises an identifier enabling the human operator to identify the first routine among the plurality of routines.

9. The method of claim 1, wherein the first text message comprises a hyperlink which, when activated, causes a display of a value of the first security predicate.

10. A server computer system configured to protect a plurality of client systems against computer security threats, the server computer system comprising at least one hardware processor configured to execute a forensic analyzer and an alert manager connected to the forensic analyzer, wherein:

the forensic analyzer is configured to:

in response to receiving a forensic indicator, select a first routine for evaluating a first security predicate from a plurality of routines, the first routine selected according to the forensic indicator, wherein the forensic indicator comprises a plurality of metadata elements characterizing a network flow between a client system of the plurality of client systems and another party, and

select a second routine for evaluating a second security predicate from the plurality of routines, the second routine selected according to a result of executing the first routine; and

the alert manager is configured to:

in response to the forensic analyzer selecting the first routine, add a first text message to a security alert indicating whether the client system is subject

to a computer security threat, the first text message determined according to a first message template selected according to the first routine,

in response to the forensic analyzer selecting the second security algorithm, add a second text message to the security alert, the second text message determined according to a second message template selected according to the second routine, and

transmit the security alert to an administration device configured to display the security alert to a human operator.

11. The server computer system of claim 10, wherein evaluating the first security predicate comprises evaluating a third security predicate, and wherein:

the forensic analyzer is further configured to select a third routine for evaluating the third security predicate from the plurality of routines; and

the alert manager is further configured to add a third text message to the security alert in preparation for transmission to the administration device, the third text message determined according to a third message template selected according to the third routine.

12. The server computer system of claim 11, wherein the first text message comprises a hyperlink which, when activated, causes a display of the third text message.

13. The server computer system of claim 10, wherein:

the forensic analyzer is further configured to determine a verdict indicating whether the client system is subject to the computer security threat, the verdict determined according to the result of executing the first routine and to another result of executing the second routine; and

the alert manager is further configured to add an indicator of the verdict to the security alert in preparation for transmission to the administration device.

14. The server computer system of claim 10, wherein the first message template comprises a placeholder, and wherein determining the first text message comprises replacing the placeholder with a value of the first security predicate determined according to the result of executing the first routine.

15. The server computer system of claim 10, wherein the first text message comprises an item selected from a group consisting of an indicator of a device type of the client system, an indicator of a geographical location of the another party, and an indicator of a time of occurrence of the electronic communication.

16. The server computer system of claim 10, wherein the plurality of metadata elements comprises a tagged element computed according to another element of the plurality of metadata elements.

17. The server computer system of claim 10, wherein the first text message comprises an identifier enabling the human operator to identify the first routine among the plurality of routines.

18. The server computer system of claim 10, wherein the first text message comprises a hyperlink which, when activated, causes a display of a value of the first security predicate.

19. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a server computer system configured to protect a plurality of client systems against computer security threats, causes the server computer system to execute a forensic analyzer and an alert manager connected to the forensic analyzer, wherein:

the forensic analyzer is configured to:

in response to receiving a forensic indicator, select a first routine for evaluating a first security predicate from a plurality of routines, the first routine selected according to the forensic indicator, wherein the forensic indicator comprises a plurality of metadata elements characterizing a network flow between a client system of the plurality of client systems and another party, and

select a second routine for evaluating a second security predicate from the plurality of routines, the second routine selected according to a result of executing the first routine; and

the alert manager is configured to:

in response to the forensic analyzer selecting the first routine, add a first text message to a security alert indicating whether the client system is subject to a computer security threat, the first text message determined according to a first message template selected according to the first routine,

in response to the forensic analyzer selecting the second security algorithm, add a second text message to the security alert, the second text message determined according to a second message template selected according to the second routine, and

transmit the security alert to an administration device configured to display the security alert to a human operator.

20. The computer-readable medium of claim 19, further storing a second set of instructions, the second set of instructions causing the at least one hardware processor to execute the first routine.

Claims

1. A method comprising employing at least one hardware processor of a server computer system configured to protect a plurality of client systems against computer security threats to:

in response to receiving a forensic indicator, select a first routine for evaluating a first security predicate from a plurality of routines, the first routine selected according to the forensic indicator, wherein the forensic indicator comprises a plurality of metadata elements characterizing a network flow between a client system of the plurality of client systems and another party, wherein the plurality of routines form a decision tree, and wherein each node of the decision tree represents a different security predicate to be evaluated;

select a second routine for evaluating a second security predicate from the plurality of routines, the second routine selected according to a result of executing the first routine;

in response to selecting the first routine, add a first text message to a security alert indicating whether the client system is subject to a computer security threat, the first text message determined according to a first message template selected according to the first routine;

in response to selecting the second routine, add a second text message to the security alert, the second text message determined according to a second message template selected according to the second routine; and

transmit the security alert to an administration device configured to display the security alert to a human operator.

2. The method of claim 1, wherein evaluating the first security predicate comprises evaluating a third security predicate, and wherein the method further comprises employing at least one hardware processor of the server computer system to:

select a third routine for evaluating the third security predicate from the plurality of routines; and

add a third text message to the security alert in preparation for transmission to the administration device, the third text message determined according to a third message template selected according to the third routine.

3. The method of claim 2, wherein the first text message comprises a hyperlink which, when activated, causes a display of the third text message.

4. The method of claim 1, further comprising employing at least one hardware processor of the server computer system to:

determine a verdict indicating whether the client system is subject to the computer security threat, the verdict determined according to the result of executing the first routine and to another result of executing the second routine; and

add an indicator of the verdict to the security alert in preparation for transmission to the administration device.

5. The method of claim 1, wherein the first message template comprises a placeholder, and wherein determining the first text message comprises replacing the placeholder with a value of the first security predicate determined according to the result of executing the first routine.

6. The method of claim 1, wherein the first text message comprises an item selected from a group consisting of an indicator of a device type of the client system, an indicator of a geographical location of the another party, and an indicator of a time of occurrence of the electronic communication.

7. The method of claim 1, wherein the plurality of metadata elements comprises a tagged element computed according to another element of the plurality of metadata elements.

8. The method of claim 1, wherein the first text message comprises an identifier enabling the human operator to identify the first routine among the plurality of routines.

9. The method of claim 1, wherein the first text message comprises a hyperlink which, when activated, causes a display of a value of the first security predicate.

10. A server computer system configured to protect a plurality of client systems against computer security threats, the server computer system comprising at least one hardware processor configured to execute a forensic analyzer and an alert manager connected to the forensic analyzer, wherein:

the forensic analyzer is configured to:

in response to receiving a forensic indicator, select a first routine for evaluating a first security predicate from a plurality of routines, the first routine selected according to the forensic indicator, wherein the forensic indicator comprises a plurality of metadata elements characterizing a network flow between a client system of the plurality of client systems and another party, wherein the plurality of routines form a decision tree, and wherein each node of the decision tree represents a different security predicate to be evaluated, and

select a second routine for evaluating a second security predicate from the plurality of routines, the second routine selected according to a result of executing the first routine; and

the alert manager is configured to:

in response to the forensic analyzer selecting the first routine, add a first text message to a security alert indicating whether the client system is subject to a computer security threat, the first text message determined according to a first message template selected according to the first routine,

in response to the forensic analyzer selecting the second routine, add a second text message to the security alert, the second text message determined

according to a second message template selected according to the second routine, and

transmit the security alert to an administration device configured to display the security alert to a human operator.

11. The server computer system of claim 10, wherein evaluating the first security predicate comprises evaluating a third security predicate, and wherein:

the forensic analyzer is further configured to select a third routine for evaluating the third security predicate from the plurality of routines; and

the alert manager is further configured to add a third text message to the security alert in preparation for transmission to the administration device, the third text message determined according to a third message template selected according to the third routine.

12. The server computer system of claim 11, wherein the first text message comprises a hyperlink which, when activated, causes a display of the third text message.

13. The server computer system of claim 10, wherein:

the forensic analyzer is further configured to determine a verdict indicating whether the client system is subject to the computer security threat, the verdict determined according to the result of executing the first routine and to another result of executing the second routine; and

the alert manager is further configured to add an indicator of the verdict to the security alert in preparation for transmission to the administration device.

14. The server computer system of claim 10, wherein the first message template comprises a placeholder, and wherein determining the first text message comprises replacing the placeholder with a value of the first security predicate determined according to the result of executing the first routine.

15. The server computer system of claim 10, wherein the first text message comprises an item selected from a group consisting of an indicator of a device type of the client system, an indicator of a geographical location of the another party, and an indicator of a time of occurrence of the electronic communication.

16. The server computer system of claim 10, wherein the plurality of metadata elements comprises a tagged element computed according to another element of the plurality of metadata elements.

17. The server computer system of claim 10, wherein the first text message comprises an identifier enabling the human operator to identify the first routine among the plurality of routines.

18. The server computer system of claim 10, wherein the first text message comprises a hyperlink which, when activated, causes a display of a value of the first security predicate.

19. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a server computer system configured to protect a plurality of client systems against computer security threats, causes the server computer system to execute a forensic analyzer and an alert manager connected to the forensic analyzer, wherein:

the forensic analyzer is configured to:

in response to receiving a forensic indicator, select a first routine for evaluating a first security predicate from a plurality of routines, the first routine selected according to the forensic indicator, wherein the forensic indicator comprises a plurality of metadata elements characterizing a network flow between a client system of the plurality of client systems and another party, wherein the plurality of routines form a decision tree, and wherein each node of the decision tree represents a different security predicate to be evaluated, and

select a second routine for evaluating a second security predicate from the plurality of routines, the second routine selected according to a result of executing the first routine; and

the alert manager is configured to:

in response to the forensic analyzer selecting the first routine, add a first text message to a security alert indicating whether the client system is subject to a computer security threat, the first text message determined according to a first message template selected according to the first routine,

in response to the forensic analyzer selecting the second routine, add a second text message to the security alert, the second text message determined according to a second message template selected according to the second routine, and

transmit the security alert to an administration device configured to display the security alert to a human operator.

20. The computer-readable medium of claim 19, further storing a second set of instructions, the second set of instructions causing the at least one hardware processor to execute the first routine.