

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:

4 select a third routine for evaluating the third security predicate from the plurality of
5 routines; and
6 add a third text message to the security alert in preparation for transmission to the
7 administration device, the third text message determined according to a third
8 message template selected according to the third routine.
9

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

1 4. The method of claim 1, further comprising employing at least one hardware processor
2 of the server computer system to:
3 determine a verdict indicating whether the client system is subject to the computer
4 security threat, the verdict determined according to the result of executing the
5 first routine and to another result of executing the second routine; and
6 add an indicator of the verdict to the security alert in preparation for transmission to
7 the administration device.
8

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

1 6. The method of claim 1, wherein the first text message comprises an item selected
2 from a group consisting of an indicator of a device type of the client system, an
3 indicator of a geographical location of the another party, and an indicator of a time of
4 occurrence of the electronic communication.
5

- 1 7. The method of claim 1, wherein the plurality of metadata elements comprises a
2 tagged element computed according to another element of the plurality of metadata
3 elements.
4
- 1 8. The method of claim 1, wherein the first text message comprises an identifier
2 enabling the human operator to identify the first routine among the plurality of
3 routines.
4
- 1 9. The method of claim 1, wherein the first text message comprises a hyperlink which,
2 when activated, causes a display of a value of the first security predicate.
3
- 1 10. A server computer system configured to protect a plurality of client systems against
2 computer security threats, the server computer system comprising at least one hardware
3 processor configured to execute a forensic analyzer and an alert manager connected to the
4 forensic analyzer, wherein:
5 the forensic analyzer is configured to:
6 in response to receiving a forensic indicator, select a first routine for evaluating a
7 first security predicate from a plurality of routines, the first routine
8 selected according to the forensic indicator, wherein the forensic indicator
9 comprises a plurality of metadata elements characterizing a network flow
10 between a client system of the plurality of client systems and another
11 party, and
12 select a second routine for evaluating a second security predicate from the
13 plurality of routines, the second routine selected according to a result of
14 executing the first routine; and
15 the alert manager is configured to:
16 in response to the forensic analyzer selecting the first routine, add a first text
17 message to a security alert indicating whether the client system is subject

18 to a computer security threat, the first text message determined according
19 to a first message template selected according to the first routine,
20 in response to the forensic analyzer selecting the second security algorithm, add a
21 second text message to the security alert, the second text message
22 determined according to a second message template selected according to
23 the second routine, and
24 transmit the security alert to an administration device configured to display the
25 security alert to a human operator.
26

1 11. The server computer system of claim 10, wherein evaluating the first security
2 predicate comprises evaluating a third security predicate, and wherein:
3 the forensic analyzer is further configured to select a third routine for evaluating the
4 third security predicate from the plurality of routines; and
5 the alert manager is further configured to add a third text message to the security alert
6 in preparation for transmission to the administration device, the third text
7 message determined according to a third message template selected according
8 to the third routine.

9
1 12. The server computer system of claim 11, wherein the first text message
2 comprises a hyperlink which, when activated, causes a display of the third text
3 message.
4

1 13. The server computer system of claim 10, wherein:
2 the forensic analyzer is further configured to determine a verdict indicating whether
3 the client system is subject to the computer security threat, the verdict
4 determined according to the result of executing the first routine and to another
5 result of executing the second routine; and
6 the alert manager is further configured to add an indicator of the verdict to the
7 security alert in preparation for transmission to the administration device.

8

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

5

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

5

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

4

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

4

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

4

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

7 in response to receiving a forensic indicator, select a first routine for evaluating a
8 first security predicate from a plurality of routines, the first routine
9 selected according to the forensic indicator, wherein the forensic indicator
10 comprises a plurality of metadata elements characterizing a network flow
11 between a client system of the plurality of client systems and another
12 party, and
13 select a second routine for evaluating a second security predicate from the
14 plurality of routines, the second routine selected according to a result of
15 executing the first routine; and

16 the alert manager is configured to:

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

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

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

27
1 20. The computer-readable medium of claim 19, further storing a second set of
2 instructions, the second set of instructions causing the at least one hardware processor
3 to execute the first routine.
4