

CLAIMS

1. A method for network security joint defense, comprising:

obtaining security log information of a plurality of security devices, wherein the security log information includes intrusion event information violating an own defense policy of each security device of the plurality of security devices, the intrusion event information being obtained by each security device in a network/system environment;

classifying and summarizing the intrusion event information included in the security log information according to preset intrusion event types;

obtaining a corresponding relationship between each preset intrusion event type and a security device identification; and

pushing the intrusion event information which is summarized according to the intrusion event types to at least one security device of the plurality of security devices directed to by the security device identification having a corresponding relationship, so that the at least one security device adjusts its own defense policy according to the pushed intrusion event information.

2. The method according to claim 1, wherein after obtaining security log information of the plurality of security devices, the method further comprises:

converting log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

3. The method according to claim 1 or 2, wherein the plurality of security devices comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

the pushing the intrusion event information which is summarized according to the intrusion event types to the at least one security device directed to by the security device identification having a corresponding relationship, so that the at least one security device adjusts its own defense policy according to the pushed intrusion event information further comprises:

pushing fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

4. The method according to claim 3, wherein the security device further comprises an attack defense device, and the attack source information is associated with an attack defense device identification;

the pushing the intrusion event information which is summarized according to the intrusion event types to the at least one security device directed to by the security device identification having a corresponding relationship, so that the at least one security device adjusts its own defense policy according to the pushed intrusion event information further comprises:

40 pushing the attack source information to the attack defense device, so that the attack defense device generates a joint defense policy according to the attack source information.

5. A method for network security joint defense, comprising:

detecting network/system state information and user behavior information in a network/system environment according to an own defense policy to generate security log information;

45 uploading the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log information, to generate a plurality of event types of intrusion event information, and to push the plurality of event types of intrusion event information according to a preset rule;

receiving at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and

50 generating a joint defense policy by taking the received intrusion event information as clue information.

6. The method according to claim 5, wherein the generating a joint defense policy by taking the received intrusion event information as clue information comprises:

55 associating the security log information generated by a security device itself with the received intrusion event information to generate joint security log information; and

generating a joint defense policy according to the joint security log information, and implementing the joint defense policy to perform intrusion event detection and intrusion event defense.

60 7. An apparatus for network security joint defense, comprising:

a security log information obtaining module, configured to obtain security log information of a plurality of security devices, wherein the security log information includes intrusion event information violating an own defense policy of each security device of the plurality of security devices, the intrusion event information being obtained by each security device in a network/system environment;

a log information classifying module, configured to classify and summarize the intrusion event information included in the security log information according to preset intrusion event types;

an associated information obtaining module, configured to obtain a corresponding relationship between each preset intrusion event type and a security device identification; and

70 a log information pushing module, configured to push the intrusion event information which is

summarized according to the intrusion event types to at least one security device of the plurality of security devices directed to by the security device identification having a corresponding relationship, so that the at least one security device adjusts its own defense policy according to the pushed intrusion event information.

75 8. The apparatus according to claim 7, wherein further comprising:

a format converting module, configured to convert log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

80 9. The apparatus according to claim 7 or 8, wherein the plurality of security devices comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

85 the log information pushing module is further configured to push fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

10. An apparatus for network security joint defense, comprising:

90 a security log information generating module, configured to detect network/system state information and user behavior information in a network/system environment according to an own defense policy to generate security log information;

95 a security information sharing module, configured to upload the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log information to generate a plurality of event types of intrusion event information, and to push the plurality of event types of intrusion event information according to a preset rule;

an event information receiving module, configured to receive at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and

100 a joint policy generating module, configured to generate a joint defense policy by taking the received intrusion event information as clue information.

11. A server, comprising a memory and a processor, wherein the memory stores computer executable instructions, which, when executed by the processor, cause the processor to perform following steps, comprising:

105 obtaining security log information of a plurality of security devices, wherein the security log

information includes intrusion event information violating an own defense policy of each security device of the plurality of security devices, the intrusion event information being obtained by each security device in a network/system environment;

classifying and summarizing the intrusion event information included in the security log information according to preset intrusion event types;

obtaining a corresponding relationship between each preset intrusion event type and a security device identification; and

pushing the intrusion event information which is summarized according to the intrusion event types to at least one security device of the plurality of security devices directed to by the security device identification having a corresponding relationship, so that the at least one security device adjusts its own defense policy according to the pushed intrusion event information.

12. The server according to claim 11, wherein the processor further performs a following step, comprising: converting log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

13. The server according to claim 11 or 12, wherein the plurality of security devices comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

the processor further performs a following step, comprising:

pushing fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

14. The server according to claim 13, wherein the plurality of security devices further comprises an attack defense device, and the attack source information is associated with an attack defense device identification; and wherein

the processor further performs a following step, comprising:

pushing the attack source information to the attack defense device, so that the attack defense device generates a joint defense policy according to the attack source information.

15. One or more non-volatile readable storage medium storing computer executable instructions, which, when executed by one or more processors, cause the one or more processors to perform following steps, comprising:

obtaining security log information of a plurality of security devices, wherein the security log

information includes intrusion event information violating an own defense policy of each security device of the plurality of security devices, the intrusion event information being obtained by each security device in a network/system environment;

classifying and summarizing the intrusion event information included in the security log
 145 information according to preset intrusion event types;

obtaining a corresponding relationship between each preset intrusion event type and a security device identification; and

pushing the intrusion event information which is summarized according to the intrusion event types to at least one security device of the plurality of security devices directed to by the security
 150 device identification having a corresponding relationship, so that the at least one security device adjusts its own defense policy according to the pushed intrusion event information.

16. The non-volatile readable storage medium according to claim 15, wherein the one or more processors further performs a following step, comprising: converting log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log
 155 format that is identifiable by the plurality of the security devices.

17. The non-volatile readable storage medium according to claim 15 or 16, wherein the plurality of security devices comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated
 160 with an attack detection device identification; and wherein

the one or more processors further perform a following step, comprising:

pushing fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to
 165 the attack source joint detection policy.

18. The non-volatile readable storage medium according to claim 17, wherein the plurality of security devices further comprises an attack defense device, and the attack source information is associated with an attack defense device identification;

the one or more processors further perform a following step, comprising:

pushing the attack source information to the attack defense device, so that the attack defense device generates a joint defense policy according to the attack source information.
 170

19. One or more non-volatile readable storage medium storing computer executable instructions, which, when executed by one or more processors, cause the one or more processors to perform following steps, comprising:

175 detecting network/system state information and user behavior information in a network/system

environment according to an own defense policy to generate security log information;

uploading the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log information, to generate a plurality of event types of intrusion event information, and to push the

180 plurality of event types of intrusion event information according to a preset rule;

receiving at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and

generating a joint defense policy by taking the received intrusion event information as clue information.

185 20. The non-volatile readable storage medium according to claim 19, wherein the generating a joint defense policy by taking the received intrusion event information as clue information performing by the one or more processors, comprises:

associating the security log information generated by a security device itself with the received intrusion event information to generate joint security log information; and

190 generating a joint defense policy according to the joint security log information, and implementing the joint defense policy to perform intrusion event detection and intrusion event defense.