ABSTRACT

A method for network security joint defense includes: 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 the security device obtained by the security device in a network/system environment; 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; classifying and summarizing the intrusion event information included in the converted security log information according to preset intrusion event types; obtaining a security device identification corresponding to each preset intrusion event type; and pushing the intrusion event information corresponding to each preset intrusion event type to the security device corresponding to the security device identification, so that the security device adjusts its own defense policy according to the pushed intrusion event information.