

the most appropriate countermeasure when there is a security risk in a terminal. However, because effects on the terminal and the system caused by applying the proposed countermeasure are unknown, a security administrator has not been able to determine whether to apply the proposed countermeasure immediately and, when a plurality of countermeasures are proposed, which of them is the most appropriate. Therefore, it has been difficult for a security administrator to develop countermeasures against security risks.

[0007]

Embodiments of the present invention provide a technique to solve the above problem.

Solution to Problem

[0008]

According to one exemplary aspect of the present invention, an information processing device includes a selection receiving unit configured to receive an input indicating selection of at least one countermeasure among a plurality of countermeasures applicable to a terminal with a security risk, an operating information specifying unit configured to specify a type of operating information corresponding to a countermeasure applicable to the terminal by using terminal-specific countermeasure information indicating a countermeasure applicable to each terminal against the security risk and definition information defining correspondence between a type of operating information of the terminal and a countermeasure against the security risk, an operating information acquisition unit configured to acquire operating information of the type specified by the operating information specifying unit among the operating information of the terminal, a remaining terminal specifying unit configured to specify remaining terminals where the security risk remains when the countermeasure received by the selection receiving unit is applied based on the terminal-specific countermeasure information, a prediction unit configured to predict the number of the remaining terminals at a future time based on the operating information acquired by the operating information acquisition unit, and a presentation unit configured to present prediction results predicted by the prediction unit.

[0009]

According to another exemplary aspect of the present invention, an information processing method is an information processing method performed by

an information processing device, the method including a step of receiving an input indicating selection of at least one countermeasure among a plurality of countermeasures applicable to a terminal with a security risk, a step of specifying a type of operating information corresponding to a countermeasure applicable to the terminal by using terminal-specific countermeasure information indicating a countermeasure applicable to each terminal against the security risk and definition information defining correspondence between a type of operating information of the terminal and a countermeasure against the security risk, a step of acquiring operating information of the specified type among the operating information of the terminal, a step of specifying remaining terminals where the security risk remains when the received countermeasure is applied based on the terminal-specific countermeasure information, a step of predicting the number of the remaining terminals at a future time based on the acquired operating information, and a step of presenting the predicted results.

[0010]

According to another exemplary aspect of the present invention, a non-transitory computer readable medium stores a program causing a computer to execute a step of receiving an input indicating selection of at least one countermeasure among a plurality of countermeasures applicable to a terminal with a security risk, a step of specifying a type of operating information corresponding to a countermeasure applicable to the terminal by using terminal-specific countermeasure information indicating a countermeasure applicable to each terminal against the security risk and definition information defining correspondence between a type of operating information of the terminal and a countermeasure against the security risk, a step of acquiring operating information of the specified type among the operating information of the terminal, a step of specifying remaining terminals where the security risk remains when the received countermeasure is applied based on the terminal-specific countermeasure information, a step of predicting the number of the remaining terminals at a future time based on the acquired operating information, and a step of presenting the predicted results.

Advantageous Effects of Invention

[0011]

According to the exemplary aspects of the present invention, a security

terminals to be managed in which the security risk remains (remaining terminals).
[0019]

The operating information specifying unit 120 specifies the type of operating information corresponding to countermeasures applicable to terminals to be managed by using the above-described terminal-specific countermeasure information and definition information that defines the correspondence between the type of operating information of a terminal to be managed and a countermeasure against a security risk. The operating information is information containing at least one of information indicating a history of operations and processing actually performed in a terminal to be managed (operating history information) and information indicating operations and processing scheduled to be performed in a terminal to be managed (operating schedule information). Such operating information is generated in each terminal to be managed in response to input of an execution of a specified operation or processing or input of an execution schedule of a specified operation or processing in each terminal to be managed, and stored into a storage unit of this terminal to be managed. Further, "type of operating information" means a category to which each operating information belongs. Specific examples of "type of operating history information" include "patch application history", "restart history", "continuous operating time", "port usage history", "process operating history", "application usage history" and the like. Further, specific examples of "type of operating schedule information" include "scheduled patch application date and time", "scheduled restart date and time", "scheduled application start date and time" and the like. Note that, however, the type of operating information is not limited to those examples.

[0020]

The definition information is stored in a specified storage unit (not shown) in the format as shown in Fig. 4, for example. Fig. 4 is a view showing an example of the definition information. Note that Fig. 4 is an example of the definition information in the case where the security risk is the vulnerability A. In Fig. 4, a countermeasure against the vulnerability A ("countermeasure (1)", "countermeasure (2)", "countermeasure (3)") and the type of operating information of a terminal to be managed, which is used as a reference to determine whether or not to apply this countermeasure, are stored in association with each other. In the

example of Fig. 4, "countermeasure (1)" is a countermeasure that applies a patch AAAA and restarts. "Countermeasure (2)" is a countermeasure that stops a process ZZZZ. "Countermeasure (3)" is a countermeasure that blocks a port 1027. Further, "type of operating information" corresponding to "countermeasure (1)" is "patch application history", "restart history" and "continuous operating time". "Type of operating information" corresponding to "countermeasure (2)" is "operating history of process ZZZZ". "Type of operating information" corresponding to "countermeasure (3)" is "usage history of port 1027". A storage unit to store the definition information as shown in Fig. 4 may be included in the information processing device 10, or may be included in another device that is connected for communication with the information processing device 10.

[0021]

The operating information specifying unit 120 specifies an applicable countermeasure and the type of operating information corresponding to this countermeasure for each terminal to be managed based on the terminal-specific countermeasure information in Fig. 3 and the definition information in Fig. 4, for example. To be specific, based on the terminal-specific countermeasure information in Fig. 3, the operating information specifying unit 120 specifies that, against the vulnerability A, "countermeasure (1)" and "countermeasure (3)" are applicable to the terminal A. Then, based on the definition information in Fig. 4, the operating information specifying unit 120 specifies "type of operating information" corresponding to "countermeasure (1)" as "patch application history", "restart history" and "continuous operating time". Further, based on the definition information in Fig. 4, the operating information specifying unit 120 specifies "type of operating information" corresponding to "countermeasure (3)" as "usage history of port 1027". Regarding the terminal B also, just like in the case of the terminal A, the operating information specifying unit 120 specifies an applicable countermeasure (only "countermeasure (2)") and the type of operating information corresponding to it ("operating history of process ZZZZ").

[0022]

The operating information acquisition unit 130 acquires the operating information of the type specified by the operating information specifying unit 120. The operating information acquisition unit 130 acquires the operating information of the type specified by the operating information specifying unit 120 from the

history", "restart history" and "continuous operating time" from the terminal A for "countermeasure (1)", which is applicable to the terminal A, based on the type of the operating information specified by the operating information specifying unit 120. Further, the operating information acquisition unit 130 acquires the
5 operating information of "usage history of port 1027" from the terminal A for "countermeasure (3)", which is applicable to the terminal A, based on the type of the operating information specified by the operating information specifying unit 120. Regarding the terminal B, just like in the case of the terminal A, the operating information acquisition unit 130 also acquires the operating information
10 of "operating history of process ZZZZ" from the terminal B for "countermeasure (2)", which is applicable to the terminal B. When the operating information relates to the past operating history, the date of the operating information is in the past. When, on the other hand, the operating information relates to the future operating schedule, the date of the operating information is in the future.

15 [0025]

The prediction unit 150 predicts the number of terminals to be managed in which the security risk remains (remaining terminals) at future times based on the operating information acquired by the operating information acquisition unit 130. For example, according to the operating information shown in Fig. 5, the
20 prediction unit 150 can make the following predictions about the terminal A (it is assumed in this example that the prediction unit 150 checks the operating information of in Fig. 5 on Wednesday, May 27, 2015). The prediction unit 150 can determine the periodic restart timing by referring to "restart history" associated with "countermeasure (1)". In the case where the field of "restart
25 schedule" is placed together with the field of "restart history" or instead of the field of "restart history", and information about a schedule of future restart is stored in the field of "restart schedule", the restart timing can be determined by referring to "restart schedule". For example, the prediction unit 150 may predict or determine the restart schedule with the closest scheduled date and time as the
30 restart timing. Further, the prediction unit 150 can determine the periodic patch application timing by referring to "patch application history" associated with "countermeasure (1)". To be specific, in the terminal A, a patch was applied and the terminal A was restarted periodically in the morning every Thursday. Based on this information, the prediction unit 150 can predict the timing to apply

graph representing "remaining risk predicted value" for each category at each future time in chronological order as shown in Fig. 17, instead of the screen of Fig. 16. Fig. 17 is a view showing another example of a screen presented by the presentation unit 160. Fig. 17 is an example of a screen in the case where the security risk is the vulnerability A. Further, although Fig. 17 displays the number of remaining risks (terminals to be managed in which the vulnerability A remains) at the present time also, whether or not to display the number of remaining risks at the present time is not particularly limited.

[0051]

10 Note that the screen of Fig. 16 or 17 presented by the presentation unit 160 is output to the administrator terminal 20 and displayed on a display unit (not shown) of the administrator terminal 20 by the display processing unit 190.

[0052]

15 The definition information storage unit 196 stores definition information that defines the correspondence between the type of operating information of the terminal 30 to be managed and countermeasures against security risks (e.g., the definition information in Fig. 4). The definition information may be delivered from a server device (not shown) to the information processing device 10. The operating information specifying unit 120 specifies the type of operating
20 information by using the definition information stored in the definition information storage unit 196.

[0053]

[Hardware Configuration]

The information processing device 10 according to the second embodiment
25 has the same hardware configuration as in the first embodiment. The storage 103 further stores a program for implementing the function of each processing unit (the information acquisition unit 170, the risk investigation unit 180 and the display processing unit 190) according to the second embodiment, and the processor 101 executes each program and thereby implements each processing unit according to
30 the second embodiment. Further, the memory 102 and the storage 103 serve also as the risk information storage unit 192, the classification information storage unit 194 and the definition information storage unit 196.

[0054]

wherein

the prediction step predicts the number of the remaining terminals at future times in chronological order, and

the presentation step presents a graph showing the number of the
5 remaining terminals at future times in chronological order.