

CLAIMS

1. A non-transitory recording medium recording a cyber-attack analysis supporting program that causes a computer to execute a process, the process comprising:

accepting registration of pieces of information each including one or more items regarding respective cyber-attack events in response to detection of malware in an information processing system of a monitoring target;

displaying each of the pieces of the information registered regarding the respective cyber-attack events in a state in which each of the one or more items is coupled as a subordinate node to a representative node of the cyber-attack event;

displaying pieces of data of the respective one or more items in a state in which each of the pieces of data is coupled as a sub-subordinate node to the subordinate node of the respective one or more items; and

displaying a coupling state between a first sub-subordinate node of the representative node of one of the cyber-attack events and a second sub-subordinate node of the representative node of the other of the cyber-attack events when the first sub-subordinate node is associated with the second sub-subordinate node to recognize a relation between the one of the cyber-attack events and the other of the cyber-attack events.

2. The non-transitory recording medium according to claim 1, wherein the one or more items include an attacker, an attack method, a detection index, an observation event, an incident, a corrective measure, or an attack target.

3. The non-transitory recording medium according to claim 2, wherein the information of the attacker includes information regarding at least one of a transmission source mail address of the cyber-attack event and an account of a social network service.

4. The non-transitory recording medium according to claim 2, wherein the information of the attack method includes information of a pattern of an attack, a resource used by the attacker, an attack base of the attacker, or an attack target.

5. The non-transitory recording medium according to claim 2, wherein the information of the detection index includes information indicative of an index that characterizes the cyber-attack event.

6. The non-transitory recording medium according to claim 2, wherein the information of the observation event includes information indicative of an event relating to an operation observed in the cyber-attack event.

7. The non-transitory recording medium according to claim 2, wherein the information of the incident includes information regarding at least one of an owner or a manager of an asset damaged by the attacker and a place of the asset.

8. The non-transitory recording medium according to claim 2, wherein the information of the corrective measure includes information indicative of a measure to cope with a threat by the cyber-attack event.

9. The non-transitory recording medium according to claim 2, wherein the information of the attack target includes information indicative of a weak point of an asset that becomes a target of an attack in the cyber-attack event.

10. A cyber-attack analysis supporting method, comprising:
accepting, by a computer, registration of pieces of information each including one or more items regarding respective cyber-attack events in response

to detection of malware in an information processing system of a monitoring target;

displaying the pieces of information registered regarding the respective cyber-attack events in a state in which each of the one or more items is coupled as a subordinate node to a representative node of the cyber-attack event;

displaying pieces of data of the respective one or more items in a state in which each of the pieces of data is coupled as a sub-subordinate node to the subordinate node of the respective one or more items; and

displaying a coupling state between a first sub-subordinate node of the representative node of one of the cyber-attack events and a second sub-subordinate node of the representative node of the other of the cyber-attack events when the first sub-subordinate node is associated with the second sub-subordinate node to recognize a relation between the one of the cyber-attack events and the other of the cyber-attack events.

11. The cyber-attack analysis supporting method according to claim 10, wherein the one or more items include an attacker, an attack method, a detection index, an observation event, an incident, a corrective measure, or an attack target.

12. A cyber-attack analysis supporting apparatus, comprising:
a memory that stores a cyber-attack analysis supporting program; and
a processor that executes a process based on the cyber-attack analysis supporting program,

wherein the process includes:

accepting registration of pieces of information each including one or more items regarding respective cyber-attack events in response to detection of malware in an information processing system of a monitoring target;

displaying the information registered regarding the cyber-attack event in a state in which each of the one or more items is coupled as a subordinate node to a representative node of the cyber-attack event;

displaying pieces of data of the respective one or more items in a state in which each of the pieces of data is coupled as a sub-subordinate node to the subordinate node of the respective one or more items; and

displaying a coupling state between a first sub-subordinate node of the representative node of one of the cyber-attack events and a second sub-subordinate node of the representative node of the other of the cyber-attack events when the first sub-subordinate node is associated with the second sub-subordinate node to recognize a relation between the one of the cyber-attack events and the other of the cyber-attack events.

13. The cyber-attack analysis supporting apparatus according to claim 12, wherein the one or more items include an attacker, an attack method, a detection index, an observation event, an incident, a corrective measure, or an attack target.