implementing the zero trust have already emerged. For example, there has been provided a solution such as Endpoint Detection and Response (EDR) that enables quick detection and handling of a cyberattack by monitoring a client device and analyzing a log.

[0014] Under such circumstances, incident management using log information has been conventionally performed. For example, log information is analyzed to grasp the damage situation from information such as the source of the incident, the communication destination, and the authentication history.

[0015] However, the related technique has a problem of a difficulty in quickly handling an incident while suppressing cost. For example, when an incident occurs, there is a need to collect individual pieces of log information such as an occurrence source, a communication destination, and an authentication history stored in the upper NW device, the lower NW device, or the like, and accurately grasp a damage situation caused by the incident. However, it is necessary to perform analysis by matching pieces of log information in which information is not integrated by a device unit, an identification (ID) unit, or the like, which requires a lot of labor and time. In addition, there is a case of taking measures disregarding the cost in order to solve the problem at an early stage.

[0016] In view of this situation, an information processing apparatus 100 according to an embodiment includes: an acquirer 121 that acquires a security log including information regarding unauthorized communication (for example, malicious communication) stored in an upper NW device being a device constituting an overlay network, an authentication log stored in a cloud server, and a communication log stored in a lower NW device being a device constituting an underlay network; a specifier 123 that specifies information such that, when an

illustrating an outline of processing performed by the information processing apparatus 100.

[0039] The acquirer 121 acquires a security log being information regarding unauthorized communication stored in the upper NW device, an authentication log stored in the cloud server, and a communication log stored in the lower NW device. In the example of FIG. 3, the acquirer 121 acquires a security log, an authentication log (cloud log), and a communication log (NW log). Here, the security log is a log of information detected by a cloud proxy or the like of the upper NW device (for example, suspicious communication such as access to an external storage service from an unauthorized IP address), and includes information such as a detection date/time, a detection type, a connection destination IP: Port, and a connection source IP: Port. The authentication log is a log of authentication information, and includes information such as date/time, ID, connection source IP: Port, and an authentication result. The communication log is a communication log of the underlay NW, and includes information such as date/time, connection destination IP: Port, connection source IP: Port, a protocol, and the number of bytes transferred. In the example of FIG. 4, FIG. 4(1) corresponds to the communication log, FIG. 4(2) corresponds to the security log, and FIG. 4(3) corresponds to the cloud log.

[0040] Subsequently, the output part 122 performs matching of pieces of information regarding the cloud log, the security log, and the NW log acquired by the acquirer 121 and outputs the result. For example, the output part 122 displays the information regarding the cloud log, the security log, and the NW log that has undergone matching for each IP address or identification information.

CLAIMS

Claim 1. An information processing apparatus comprising:

an acquirer configured to acquire a security log including information regarding unauthorized communication stored in an upper NW device being a device constituting an overlay network, an authentication log stored in a cloud server, and a communication log stored in a lower NW device being a device constituting an underlay network;

a specifier configured to specify information such that, when the authentication log includes a connection source IP address that does not exist in the communication log acquired by the acquirer and the security log includes information regarding an access not permitted to be used from the connection source IP address, the specifier specifies the information regarding the access as unauthorized communication; and

a blocking instructor configured to give an instruction to block the unauthorized communication specified by the specifier.

Claim 2. The information processing apparatus according to claim 1,

wherein the specifier

compares a connection source IP address included in the security log with a connection source IP address included in the communication log, and determines whether the communication log includes log information in which a connection source IP address and the connection source IP address included in the security log are the same,

compares the connection source IP address included in the security log with a connection source IP address included in the authentication log, and determines whether the authentication log includes log information in which a

connection source IP address and the connection source IP address included in the security log are the same, and

specifies information such that, when having determined that the communication log includes no log information in which a connection source IP address and the connection source IP address included in the security log are the same, and having determined that the authentication log includes log information in which a connection source IP address and the connection source IP address included in the security log are the same, the specifier specifies the log information of the connection source IP address included in the security log as unauthorized communication.

Claim 3. The information processing apparatus according to claim 1, further including

an output part configured to output information obtained by matching logs acquired by the acquirer, the logs being the security log, the authentication log, and the communication log.

Claim 4. The information processing apparatus according to claim 1,

wherein the blocking instructor gives an instruction to block the unauthorized communication specified by the specifier by using identification information included in the unauthorized communication.

Claim 5. An information processing method to be executed by a computer, the information processing method comprising:

an acquisition process of acquiring a security log including information regarding unauthorized communication stored in an upper NW device being a device constituting an

overlay network, an authentication log stored in a cloud server, and a communication log stored in a lower NW device being a device constituting an underlay network;

a specifying process of specifying information such that, when the authentication log includes a connection source IP address that does not exist in the communication log acquired by the acquisition process and the security log includes information regarding an access not permitted to be used from the connection source IP address, the specifying process specifies the information regarding the access as unauthorized communication; and

a blocking instruction process of giving an instruction to block the unauthorized communication specified by the specifying process.

Claim 6. A computer-readable recording medium storing therein an information processing program that causes a computer to execute a process comprising:

an acquisition step of acquiring a security log including information regarding unauthorized communication stored in an upper NW device being a device constituting an overlay network, an authentication log stored in a cloud server, and a communication log stored in a lower NW device being a device constituting an underlay network;

a specifying step of specifying information such that, when the authentication log includes a connection source IP address that does not exist in the communication log acquired by the acquisition step and the security log includes information regarding an access not permitted to be used from the connection source IP address, the specifying step specifies the information regarding the access as unauthorized communication; and

a blocking instruction step of giving an instruction to block the unauthorized communication specified by the specifying

step.