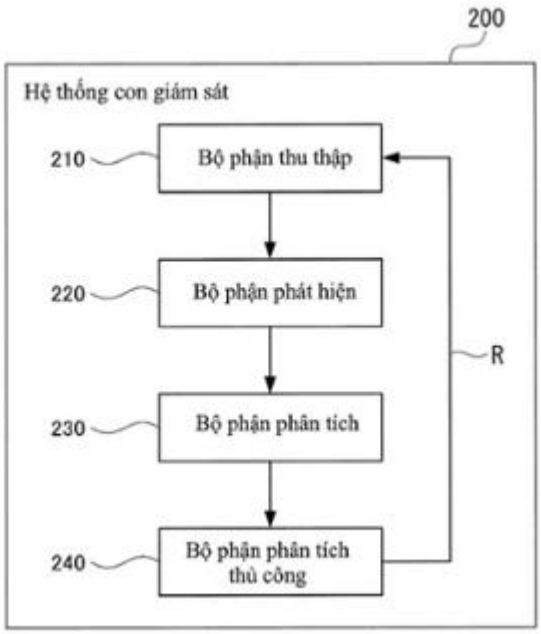
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0028233**
(51)[7] **G06F 13/00**; H04L 12/70; G06F 21/00 (13) **B**

(21) 1-2016-03446 (22) 26/02/2015
(86) PCT/JP2015/055618 26/02/2015 (87) WO 2015/151668 A1 08/10/2015
(30) 2014-074607 31/03/2014 JP
(45) 25/05/2021 398 (43) 26/12/2016 345A
(73) LAC Co., Ltd. (JP)
Hirakawacho Mori Tower, 2-16-1, Hirakawacho, Chiyoda-ku, Tokyo 102-0093 Japan
(72) FUJIMOTO Hiroshi (JP); NAKAMA Toshihide (JP).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) HỆ THỐNG PHÂN TÍCH NHẬT KÝ

(57) Sáng chế đề cập đến hệ thống phân tích nhật ký để phân tích nhật ký phát hiện được phát hiện trong hệ thống đích giám sát bao gồm thiết bị thu nhận để phát hiện các quy trình xử lý đích phát hiện được thực hiện trong hệ thống đích giám sát, và thu nhận nhật ký phát hiện của các quy trình xử lý đích phát hiện; và thiết bị xử lý để xử lý nhật ký phát hiện được thu nhận bởi bộ thu nhận. Thiết bị xử lý bao gồm các khối xử lý mà thực hiện quy trình xử lý trên nhật ký phát hiện theo trình tự. Thiết bị xử lý thực hiện xử lý trong khi gửi nhật ký phát hiện theo thứ tự từ khối xử lý phía trên cùng tới các khối xử lý phía dưới. Khối xử lý phía dưới cùng của thiết bị xử lý thông báo khối xử lý phía trên cùng của thiết bị xử lý rằng nhật ký phát hiện đã được thu. Đối với nhật ký phát hiện mà đang được xử lý mà không thể được xác nhận là đã tới khối xử lý phía dưới cùng trong thông báo thu được từ khối xử lý phía dưới cùng của thiết bị xử lý, khối xử lý phía trên cùng của thiết bị xử lý gửi lại nhật ký phát hiện tới khối xử lý phía dưới.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống phân tích nhật ký để thu nhận và phân tích các nhật ký được khởi tạo trong hệ thống đích.

Tình trạng kỹ thuật của sáng chế

Khối lượng truyền thông và xử lý dữ liệu lớn xuất hiện trong các loại hệ thống thông tin ứng dụng mạng truyền thông thông tin chẳng hạn như Internet (dưới đây được gọi đơn giản là "mạng"). Tuy nhiên, có thể có các vấn đề phát sinh chẳng hạn như truy cập không được phép của máy chủ hoặc thiết bị chẳng hạn như các thiết bị đầu cuối khác nhau hoạt động trên mạng, thông tin không được phép rò rỉ từ máy chủ, hoặc tương tự.

Chẳng hạn, có thể giám sát các truyền thông dữ liệu theo thời gian thực để ngăn ngừa sự hư hại do các truyền thông không được phép mà không cần điều tra khối lượng lớn truyền thông sau sự kiện. Các kỹ thuật thông thường để thực hiện điều này đã được bộc lộ. Ví dụ, đơn sáng chế Nhật Bản số 2007-536646 bộc lộ việc thu thập các sự kiện bảo vệ từ các thiết bị giám sát khác nhau, lưu trữ các sự kiện bảo vệ này, cung cấp tập hợp con của các sự kiện bảo vệ được lưu trữ tới bộ quản lý làm dòng sự kiện, và có bộ quản lý tìm kiếm một hoặc nhiều mẫu sự kiện chưa được biết đến trong dòng sự kiện.

Thông thường, sự xử lý tương ứng có thể được thực hiện bằng cách giám sát các truyền thông trên máy chủ trong mạng, và phát hiện truy cập không được phép hoặc gửi và thu dữ liệu. Việc giám sát có thể được thực hiện tại vị trí trung tâm khi nhiều máy chủ được lấy làm các đích cần được giám sát.

Tài liệu sáng chế 1: Đơn sáng chế Nhật Bản số 2007-536646

Khi phân tích lượng lớn các nhật ký và thực hiện xử lý thông tin để trích các quy trình xử lý có đặc tính riêng biệt (chẳng hạn như các truyền thông có vấn đề) để thực hiện giám sát truyền thông thông tin và tương tự trên mạng nêu trên, lượng dữ liệu trong các nhật ký được thu nhận làm các đích phân tích thường rất lớn. Tuy nhiên, có thể chỉ có số lượng nhỏ các quy trình xử lý có đặc tính riêng biệt mà cần được trích, và có thể chỉ có một vài nhật ký mà ở đó xử lý này có thể cần được thực hiện. Do đó, cần thu hẹp thích hợp các đích cần được phân tích và thực hiện phân tích với hiệu quả tốt trong nhiều loại vùng xử lý

thông tin mà không quan tâm đến việc các truyền thông có đang được kiểm soát hay không.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất hệ thống phân tích nhật ký có khả năng thu hẹp các nhật ký để phân tích và thực hiện phân tích nhật ký với hiệu quả tốt.

Để đạt được mục đích này, hệ thống phân tích nhật ký liên quan đến phương án của sáng chế có thể phân tích nhật ký phát hiện được phát hiện trong hệ thống đích giám sát. Hệ thống phân tích nhật ký có thể được bố trí với: thiết bị thu nhận để phát hiện các quy trình xử lý đích phát hiện được thực hiện trong hệ thống đích giám sát, và thu nhận nhật ký phát hiện của các quy trình xử lý đích phát hiện; và thiết bị xử lý để xử lý nhật ký phát hiện được thu nhận bởi bộ thu nhận. Thiết bị xử lý bao gồm nhiều khối xử lý mà thực hiện quy trình xử lý trên nhật ký phát hiện theo trình tự. Thiết bị xử lý thực hiện xử lý trong khi gửi nhật ký phát hiện theo thứ tự từ khối xử lý đầu tiên tới các khối xử lý phía dưới. Khối xử lý phía dưới cùng của thiết bị xử lý thông báo khối xử lý phía trên cùng của thiết bị xử lý rằng nhật ký phát hiện đã được thu. Đối với nhật ký phát hiện mà đang được xử lý mà không thể được xác nhận là đã tới khối xử lý phía dưới cùng trong thông báo thu được từ khối xử lý phía dưới cùng của thiết bị xử lý, khối xử lý phía trên cùng của thiết bị xử lý gửi lại nhật ký phát hiện tới khối xử lý phía dưới.

Trong hệ thống phân tích nhật ký nêu trên, khối xử lý phía trên cùng của thiết bị xử lý có thể dừng việc gửi nhật ký phát hiện đối với các trường hợp mà ở đó, sau khi đã gửi lặp lại nhật ký phát hiện với số lần định trước, không thể được xác nhận trong thông báo từ khối xử lý phía dưới cùng của thiết bị xử lý rằng nhật ký phát hiện đã tới khối xử lý phía dưới cùng.

Trong hệ thống phân tích nhật ký nêu trên, khối xử lý phía trên cùng của thiết bị xử lý có thể cũng bổ sung thông tin tới nhật ký phát hiện, thông tin có khả năng được sử dụng để nhận dạng xem nhật ký phát hiện đã được gửi lại hay chưa.

Trong hệ thống phân tích nhật ký nêu trên, khối xử lý phía trên cùng của thiết bị xử lý có thể cũng bổ sung thông tin tới nhật ký phát hiện, thông tin thể hiện nhật ký phát hiện đã được truyền bao nhiêu lần.

Các phương án của sáng chế có thể cũng đạt được bằng cách điều khiển máy tính để thực hiện các chức năng của thiết bị nêu trên nhờ chương trình. Chương trình có thể được bố trí nhờ được lưu trữ trên đĩa từ, đĩa quang, bộ nhớ bán dẫn, hoặc vật ghi khác, và có thể cũng được bố trí nhờ được phân phối thông qua mạng.

Theo sáng chế, các đích có thể được thu hẹp và phân tích có thể được thực hiện với hiệu quả tốt trong thời gian phân tích nhật ký.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ minh họa ví dụ về cấu hình của hệ thống giám sát bảo vệ theo phương án sáng chế.

Fig.2 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận thu thập mà tạo cấu hình hệ thống con giám sát được minh họa trên Fig.1.

Fig.3 là hình vẽ minh họa ví dụ về cấu hình của bộ phận thu thập được minh họa trên Fig.2 được tạo cấu hình bởi các khối bộ phận xử lý được cấu thành.

Fig.4 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận phát hiện mà tạo cấu hình hệ thống con giám sát được minh họa trên Fig.1.

Fig.5 là hình vẽ minh họa ví dụ về cấu hình của bộ phận phát hiện được minh họa trên Fig.4 được tạo cấu hình bởi các khối bộ phận xử lý được cấu thành.

Fig.6 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận phân tích mà tạo cấu hình hệ thống con giám sát được minh họa trên Fig.1

Fig.7 là hình vẽ minh họa mô hình phân tích tương quan theo phương án sáng chế.

Fig.8A là hình vẽ minh họa mô hình phân tích gia tăng theo phương án sáng chế, và là hình vẽ minh họa ví dụ về cấu hình của ứng viên sự cố được phát hiện mà trở thành đích phân tích tương quan đối với phân tích nhất định.

Fig.8B là hình vẽ minh họa mô hình phân tích gia tăng theo phương án sáng chế, và là hình vẽ minh họa ví dụ về cấu hình của cùng ứng viên sự cố được phát hiện đối với phân tích tiếp theo.

Fig.9 là hình vẽ minh họa ví dụ về cấu hình của bộ phận phân tích được minh họa trên Fig.6, được tạo cấu hình bởi các khối bộ phận xử lý được cấu thành bao gồm bộ xử lý phân tích riêng, bộ xử lý kết hợp sự kiện, bộ xử lý phân tích tương quan, và bộ xử lý phân tích gia tăng.

Fig.10 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận phân tích thủ công của hệ thống con giám sát được minh họa trên Fig.1.

Fig.11 là hình vẽ dùng để giải thích phương pháp chuyển tệp nhật ký truyền thông theo phương án sáng chế.

Fig.12 là hình vẽ minh họa ví dụ về truyền tệp nhật ký truyền thông theo phương án sáng chế.

Fig.13 là hình vẽ minh họa ví dụ khác về truyền tệp nhật ký truyền thông theo phương án sáng chế.

Fig.14 là hình vẽ minh họa ví dụ khác nữa về truyền tệp nhật ký truyền thông theo phương án sáng chế.

Fig.15 là hình vẽ minh họa ví dụ về cấu hình chức năng của thiết bị đầu cuối được minh họa trên Fig.1

Fig.16 là hình vẽ minh họa ví dụ về cấu hình của màn hình phân tích theo phương án sáng chế.

Fig.17 là hình vẽ minh họa ví dụ về cấu hình phần cứng ưu tiên dùng để tạo cấu hình mỗi máy chủ và thiết bị đầu cuối trong hệ thống con giám sát theo phương án sáng chế.

Mô tả chi tiết sáng chế

Các phương án của sáng chế được giải thích dưới đây dựa vào các hình vẽ.

Hệ thống phân tích nhật ký theo phương án sáng chế để thu nhận và phân tích nhật ký xử lý đích phát hiện ("nhật ký phát hiện") từ hệ thống đích điều tra được giải thích dưới đây dựa trên trường hợp áp dụng hệ thống phân tích nhật ký cho hệ thống giám sát bảo vệ mà giám sát các truyền thông trên mạng, và thu nhận và phân tích nhật ký truyền thông như nhật ký phát hiện. Hệ thống giám sát bảo vệ (Security Operation Center, "SOC") theo phương án sáng chế giám sát các truyền thông của thiết bị xử lý thông tin mà là thiết bị chịu sự giám sát, và

trích các truyền thông có vấn đề chẳng hạn như truy cập bên ngoài không được phép, các rò rỉ thông tin bên trong không được phép, hoặc tương tự như một đích của quy trình xử lý đích phát hiện có đặc tính riêng biệt cần trích.

Ví dụ về cấu hình hệ thống

Fig.1 là hình vẽ minh họa ví dụ về cấu hình của hệ thống giám sát bảo vệ theo phương án sáng chế.

Như được minh họa trên Fig.1, hệ thống giám sát bảo vệ theo phương án sáng chế bao gồm thiết bị phát hiện 110 làm thiết bị thu nhận dùng để giám sát các truyền thông trong thiết bị đích giám sát 100 và thu nhận nhật ký truyền thông, tác nhân thu nhận nhật ký 121, và hệ thống con quản lý nhật ký 120. Hệ thống giám sát bảo vệ theo phương án sáng chế cũng được bố trí với hệ thống con giám sát 200 làm thiết bị xử lý dùng để xử lý các nhật ký truyền thông đã được thu nhận và trích các truyền thông có vấn đề. Ngoài ra, hệ thống giám sát bảo vệ theo phương án sáng chế cũng được bố trí với thiết bị đầu cuối 300 làm thiết bị đầu ra dùng để đưa ra các kết quả xử lý bởi hệ thống con giám sát 200. Trong cấu hình được minh họa trên Fig.1, thiết bị phát hiện 110 và tác nhân thu nhận nhật ký 121 được cài đặt trong thiết bị đích giám sát 100 được tách từ hệ thống con quản lý nhật ký 120, hệ thống con giám sát 200, và thiết bị đầu cuối 300. Các phần tử cấu thành được lắp đặt trong thiết bị đích giám sát 100 có thể được gọi là hệ thống phía đích, trong khi hệ thống con quản lý nhật ký 120, hệ thống con giám sát 200, và thiết bị đầu cuối 300 có thể được gọi là hệ thống phía tâm. Lưu ý là mặc dù chỉ một thiết bị đích giám sát 100 được thể hiện trong ví dụ trên Fig.1, trong hệ thống thực, các truyền thông trong nhiều thiết bị đích giám sát 100 có thể được lấy làm đích để giám sát.

Thiết bị đích giám sát 100 là đích cần được giám sát bởi hệ thống giám sát bảo vệ theo phương án sáng chế, và là thiết bị mà tạo ra các nhật ký được thu nhận bởi thiết bị phát hiện 110 và hệ thống con quản lý nhật ký 120. Thiết bị đích giám sát 100 cụ thể là máy chủ hoặc tương tự mà chạy phần mềm được cài đặt chẳng hạn như hệ thống phát hiện xâm nhập (IDS- intrusion detection system), hệ thống ngăn ngừa xâm nhập (IPS- intrusion prevention system), hoặc hệ thống bảo vệ khác, hoặc phần mềm giống như tường lửa hoặc phần mềm chống virus.

Lưu ý là ví dụ được giải thích theo phương án sáng chế mà ở đó hệ thống phân tích nhật ký được lấy làm hệ thống giám sát bảo vệ, và hệ thống phân tích nhật ký thu nhận nhật ký truyền thông làm đích giám sát truyền thông mạng. Tuy nhiên, các ví dụ phù hợp theo phương án sáng chế không giới hạn ở ví dụ nêu trên. Cũng có thể ứng dụng hệ thống phân tích nhật ký theo phương án sáng chế để thu nhận và điều tra các loại nhật ký khác nhau được tạo ra bởi các quy trình xử lý khác nhau thay vì các truyền thông.

Thiết bị phát hiện 110 được tạo cấu hình bởi cảm biến 111 và bộ quản lý cảm biến 112. Cảm biến 111 là bộ phận đích giám sát của hệ thống giám sát bảo vệ theo phương án sáng chế. Cảm biến 111 có thể đạt được bằng cách sử dụng, chẳng hạn, chức năng phát hiện truyền thông trong thiết bị đích giám sát 100. Cảm biến 111 thu nhận dữ liệu liên quan đến các truyền thông theo thời gian thực. Bộ quản lý cảm biến 112 có thể đạt được bằng cách sử dụng, chẳng hạn, chức năng của thiết bị đích giám sát 100. Bộ quản lý cảm biến 112 quản lý cảm biến 111. Nghĩa là, cảm biến 111 và bộ quản lý cảm biến 112 có thể được bố trí theo nhiều dạng khác nhau chẳng hạn như phần mềm, dưới dạng kết hợp phần cứng và phần mềm, sử dụng các loại chức năng hệ thống bảo vệ chẳng hạn như IDS/IPS, tường lửa, phần mềm chống virus, và tương tự. Trong hệ thống thực, các loại cảm biến 111 và các bộ quản lý cảm biến 112 có thể được sử dụng tùy thuộc vào các đặc điểm kỹ thuật, sự sử dụng, và hoàn cảnh sử dụng của thiết bị đích giám sát 100 được thiết đặt làm đích cần được giám sát.

Tác nhân thu nhận nhật ký 121 gửi dữ liệu liên quan đến các truyền thông được thu nhận bởi cảm biến 111 được quản lý bởi bộ quản lý cảm biến 112 tới hệ thống con quản lý nhật ký 120 theo thời gian thực làm nhật ký truyền thông. Theo phương án sáng chế, nhật ký truyền thông được gửi bởi tác nhân thu nhận nhật ký 121 tới hệ thống con quản lý nhật ký 120 được gọi là "nhật ký chưa xử lý (raw log)". Tác nhân thu nhận nhật ký có thể được tạo ra dưới dạng, chẳng hạn, chương trình máy tính. Chức năng gửi nhật ký chưa xử lý tới hệ thống con quản lý nhật ký 120 có thể được thực hiện bằng cách cài đặt và chạy tác nhân thu nhận nhật ký 121 trong thiết bị đích giám sát 100. Các loại cảm biến và các bộ quản lý cảm biến khác nhau có thể được sử dụng cho cảm biến và bộ quản lý cảm biến 112 mà thu nhận nhật ký chưa xử lý, như được nêu trên. Do đó, nội dung và định dạng của thông tin được bao gồm trong nhật ký chưa xử lý

có thể khác nhau theo loại cảm biến 111 và bộ quản lý cảm biến 112 mà thu nhận nhật ký chưa xử lý.

Lưu ý rằng, với phương án được minh họa trên Fig.1, cấu hình được sử dụng trong đó tác nhân thu nhận nhật ký 121 được cài đặt trong thiết bị đích giám sát 100 làm hệ thống phía đích. Tuy nhiên, phương án sáng chế không giới hạn ở loại cấu hình này. Tác nhân thu nhận nhật ký 121 có thể cũng được tạo cấu hình làm hệ thống phía tâm mà không được cài đặt trong thiết bị đích giám sát 100. Trong trường hợp này, tác nhân thu nhận nhật ký 121 có thể được tạo cấu hình như máy chủ độc lập hoặc tương tự được kết nối với thiết bị đích giám sát 100 thông qua mạng, và tác nhân thu nhận nhật ký 121 có thể cũng đạt được như một chức năng của hệ thống con quản lý nhật ký 120.

Hệ thống con quản lý nhật ký 120 thu nhận nhật ký chưa xử lý từ tác nhân thu nhận nhật ký 121. Do đó, các nhật ký chưa xử lý được thu nhận đối với mỗi tác nhân thu nhận nhật ký 121 trong hệ thống con quản lý nhật ký 120. Ngoài ra, hệ thống con quản lý nhật ký 120 chia các nhật ký chưa xử lý đã được thu nhận thành các tệp nhật ký truyền thông đối với mỗi cảm biến, và gửi các tệp truyền thông tới hệ thống con giám sát 200 theo thời gian thực. Hệ thống con quản lý nhật ký có thể được thực hiện bằng cách sử dụng, chẳng hạn, máy tính. Nghĩa là, bằng cách sử dụng CPU (bộ xử lý trung tâm-center processing unit) để thực hiện chương trình được lưu trữ trong thiết bị lưu trữ của máy tính, chức năng nêu trên có thể được thực hiện. Các nhật ký chưa xử lý được thu nhận từ tác nhân thu nhận nhật ký 121 được chia thành các tệp nhật ký truyền thông, và được gửi tới hệ thống con giám sát 200.

Hệ thống con giám sát 200 là bộ phận xử lý dùng để thực hiện xử lý trên các tệp truyền thông được thu nhận từ tác nhân thu nhận nhật ký 120. Hệ thống con giám sát 200 bao gồm bộ phận thu thập 210, bộ phận phát hiện 220, bộ phận phân tích 230, và bộ phận phân tích thủ công 240. Hệ thống con giám sát 200 xử lý các tệp nhật ký truyền thông được thu nhận từ tác nhân thu nhận nhật ký 120 nhờ sử dụng các bộ phận xử lý 210, 220, 230, và 240, theo thứ tự đó, trích các truyền thông có vấn đề. Nói cách khác, hệ thống con giám sát 200 chia các truyền thông được thực hiện bởi thiết bị đích giám sát 100 được hiển thị trong tệp nhật ký truyền thông thành các truyền thông có vấn đề, và các truyền thông không có vấn đề.

Có thể tạo ra các bộ phận xử lý 210, 220, 230, và 240 trong hệ thống con giám sát 200 bằng cách sử dụng nhiều máy chủ (phần cứng- hardware). Nhiều máy chủ có thể thực hiện xử lý song song với nhau và không đồng bộ. Theo phương án sáng chế, việc truyền các tệp nhật ký truyền thông giữa các bộ phận xử lý 210, 220, 230, và 240 trong hệ thống con giám sát 200 có thể được thực hiện bằng cách sử dụng các truyền thông không đồng bộ dựa vào, chẳng hạn, dịch vụ thông báo Java (JMS- Java Message Service) hoặc tương tự. Hệ thống con giám sát 200 được thực hiện bằng cách sử dụng, chẳng hạn, máy tính. Nghĩa là, CPU có thể được bố trí để thực hiện chương trình được lưu trữ trong thiết bị lưu trữ của máy tính, nhờ đó đạt được các chức năng của mỗi bộ phận xử lý 210, 220, 230, và 240. Chi tiết về mỗi trong số các bộ phận xử lý 210, 220, 230, và 240, cũng như các truyền thông giữa các bộ phận xử lý, được đưa ra dưới đây.

Thiết bị đầu cuối 300 là thiết bị dùng để đưa ra các kết quả xử lý được tìm thấy bởi hệ thống con giám sát 200. Thiết bị đầu cuối 300 là thiết bị mà người dùng (người phân tích) sử dụng khi phân tích các truyền thông trong thiết bị đích giám sát 100. Các truyền thông trong thiết bị đích giám sát 100 được chia thành các truyền thông có vấn đề và các truyền thông không có vấn đề, và được đưa ra làm các kết quả xử lý bởi hệ thống con giám sát 200. Các truyền thông có vấn đề bao gồm vấn đề mà ở đó rõ ràng là sự truyền thông là không được phép, và vấn đề mà ở đó có khả năng là sự truyền thông là không được phép. Người dùng phân tích của thiết bị đầu cuối 300 có thể phân tích các truyền thông đó mà có thể là không được phép dựa vào các kết quả xử lý của hệ thống con giám sát 200 được đưa ra tới thiết bị đầu cuối 300, và sau đó có thể đánh giá xem các truyền thông có đúng là không được phép hay không.

Thiết bị đầu cuối 300 có thể được thực hiện bằng cách sử dụng, chẳng hạn, máy tính. Nghĩa là, CPU có thể được sử dụng để thực hiện chương trình được lưu trữ trong thiết bị lưu trữ của máy tính, nhờ đó đạt được mỗi chức năng của thiết bị đầu cuối 300. Các chức năng cụ thể của thiết bị đầu cuối 300, và chi tiết về nội dung và định dạng của thông tin được đưa ra trong thiết bị đầu cuối 300, được mô tả dưới đây.

Các chức năng của bộ phận thu thập

Fig.2 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận thu thập 210 mà tạo cấu hình hệ thống con giám sát 200 được minh họa trên Fig.1.

Bộ phận thu thập 210, mà là bộ phận xử lý thứ nhất, thực hiện quy trình thiết đặt cho tệp nhật ký truyền thông được thu nhận từ hệ thống con quản lý nhật ký 120 đối với mỗi loại thiết bị phát hiện 110 mà đã thu nhận nhật ký truyền thông cơ sở (nhật ký chưa xử lý) của tệp nhật ký truyền thông. Loại thiết bị phát hiện 110 như được sử dụng ở đây là loại sản phẩm chẳng hạn như IDS/IPS, tường lửa, phần mềm chống virus, hoặc tương tự mà tạo ra các chức năng của cảm biến 111 và bộ quản lý cảm biến 112 của thiết bị phát hiện 110. Lưu ý rằng thông tin mà định rõ loại thiết bị phát hiện 110 (chẳng hạn như ID, tên sản phẩm, hoặc tương tự) có thể được bao gồm trong, chẳng hạn, tệp nhật ký truyền thông.

Như được minh họa trên Fig.2, bộ phận thu thập 210 theo phương án sáng chế thực hiện xử lý sau đây trên tệp nhật ký truyền thông được thu nhận: xử lý để trích nhật ký đích phân tích, xử lý để chuẩn hóa nhật ký truyền thông, xử lý để phân phối nhật ký truyền thông, và lọc.

Trong suốt thời gian xử lý để trích nhật ký đích phân tích, bộ phận thu thập 210 trích nhật ký truyền thông mà trở thành đích để xử lý (phân tích) bởi hệ thống con giám sát 200 từ trong số các nhật ký truyền thông được bao gồm trong tệp nhật ký truyền thông được thu nhận từ hệ thống con quản lý nhật ký 120. Các nhật ký thao tác mà ở đó cảm biến 111 của thiết bị phát hiện đang hoạt động hoặc đã dừng hoạt động (các nhật ký mà không cần phải được phân tích) được bao gồm trong tệp nhật ký truyền thông (nhật ký chưa xử lý) được thu nhận từ hệ thống con quản lý nhật ký 120. Bộ phận thu thập 210 chỉ trích thông tin mà trở thành đích xử lý định trước (đích phân tích) cho hệ thống con giám sát 200, và loại bỏ thông tin khác.

Bộ phận thu thập 210 chuẩn hóa nhật ký truyền thông đích phân tích được trích dựa vào quy tắc định trước trong suốt thời gian xử lý để chuẩn hóa nhật ký truyền thông. Cụ thể là, bộ phận thu thập 210 lấy thông tin chẳng hạn như ngày tháng và thời gian, số giao thức, địa chỉ giao thức Internet người gửi (địa chỉ IP- Internet Protocol address), cổng người gửi, địa chỉ IP đích, cổng đích, và tương tự trong nhật ký truyền thông và tạo ra nó ở định dạng chung. Ví dụ, bộ phận thu thập 210 chuẩn hóa các tiêu chuẩn (kiểu phương tây, kiểu Nhật Bản, hoặc kiểu tương tự) và định dạng dùng để mô tả ngày tháng và thời gian, và chuẩn hóa hệ thống biểu diễn (hệ thống ký hiệu) đối với các địa chỉ IP.

Tùy thuộc vào loại thiết bị phát hiện 110, có thể có các lần mà ở đó một phần của thông tin trong nhật ký truyền thông được thu nhận trải qua xử lý chuẩn hóa không được bao gồm. Để xử lý các trường hợp như vậy, bộ phận thu thập 210 có thể thực hiện quy trình xử lý chẳng hạn như đưa vào giá trị ngầm định định trước như một sự thay thế, thay thế giá trị (giá trị rỗng) mà chỉ báo không có dữ liệu, thực hiện phân tích mà không bổ sung thông tin, hoặc tương tự. Cụ thể là, phương pháp được ứng dụng được xác định theo loại thông tin thiếu hụt. Lưu ý là đối với các trường hợp mà ở đó định dạng nhật ký truyền thông không trùng với các đặc điểm mô tả sản phẩm của thiết bị phát hiện 110 mà thu nhận nhật ký truyền thông, và đối với các trường hợp mà ở đó các giá trị trong nhật ký truyền thông được thu nhận là bất thường, bộ phận thu thập 210 xác định rằng nhật ký truyền thông được thu nhận là nhật ký truyền thông gây lỗi, loại bỏ nhật ký truyền thông từ các đích phân tích, và lưu trữ nhật ký truyền thông gây lỗi trong cơ sở dữ liệu lưu trữ. Các giá trị bất thường trong nhật ký truyền thông được thu nhận có thể là do, ví dụ, thông tin ngày tháng mà là ngày tháng trong tương lai.

Xử lý để phân phối nhật ký truyền thông là xử lý mà ở đó nhật ký truyền thông được chuẩn hóa được chia thành các nhật ký truyền thông trên mỗi đích giám sát được xác định bởi hợp đồng hoặc tương tự đối với các trường hợp mà ở đó thiết bị phát hiện 110 là mô hình trung tâm dữ liệu mà nó nhận các truyền thông trong nhiều thiết bị đích giám sát 100 làm các đích. Ví dụ, khi thực hiện dịch vụ được cung cấp bởi thiết bị phát hiện 110 được thiết lập trên mạng trong hoàn cảnh mà ở đó thiết bị đích giám sát được đăng ký 100 được ứng dụng, có thể là một thiết bị phát hiện 110 phát hiện các truyền thông từ nhiều thiết bị đích giám sát 100. Trong trường hợp này, các nhật ký truyền thông trong nhiều thiết bị đích giám sát 100 được bao gồm trong tệp nhật ký truyền thông được thu nhận bởi thiết bị phát hiện 110. Để thực hiện sự phân tích nhật ký truyền thông trên mỗi khách hàng riêng lẻ, theo phương án sáng chế bộ phận thu thập 210 chia nhật ký truyền thông bởi thiết bị đích giám sát 100. Do đó xử lý phân phối nhật ký truyền thông là không cần thiết đối với các trường hợp mà ở đó phương án về mô hình trung tâm dữ liệu không được ứng dụng và các thiết bị phát hiện riêng lẻ 110 được cung cấp cho mỗi đích giám sát. Điều này là do nhật ký truyền thông đã được phân phối trước.

Việc phân phối nhật ký truyền thông có thể được thực hiện dựa vào, chẳng hạn, thông tin dải địa chỉ IP. Cụ thể là, ví dụ có thể được giải thích dưới đây. Nghĩa là, dải địa chỉ IP được xử lý bởi thiết bị phát hiện 110 có thể là từ [x . x . x . 1] đến [x . x . x . 30], trong đó x là số từ 0 đến 255. Các địa chỉ IP được phân phối tới thiết bị đích giám sát của khách hàng có thể là từ [x . x . x . 1] đến [x . x . x . 10]. Các địa chỉ IP được phân phối tới thiết bị đích giám sát của khách hàng B có thể là từ [x . x . x . 11] đến [x . x . x . 12]. Các địa chỉ IP được phân phối tới thiết bị đích giám sát của khách hàng C có thể là từ [x . x . x . 13] đến [x . x . x . 30]. Bằng cách đăng ký các dải địa chỉ IP đối với mỗi trong số các thiết bị đích giám sát 100 trong bộ phận thu thập 210 trước đó với ví dụ này, bộ phận thu thập 210 có thể xác định thiết bị đích giám sát 100 nào mà nhật ký truyền thông cụ thể liên quan đến, và sau đó thực hiện việc phân phối.

Trong suốt thời gian xử lý lọc, bộ phận thu thập 210 xác định xem các nhật ký truyền thông được phân phối bởi quy trình phân phối nêu trên có là các đích phân tích hay không, dựa vào các điều kiện riêng lẻ và các quy tắc được thiết đặt theo các khách hàng riêng lẻ. Các mục cần được xác định trong suốt thời gian xử lý lọc bao gồm địa chỉ IP đích, cổng đích, địa chỉ IP người gửi, cổng người gửi, và tương tự. Nghĩa là, đối với các trường hợp mà ở đó địa chỉ IP đích trong nhật ký truyền thông nhất định là giá trị quy định, bộ phận thu thập 210 có thể thực hiện quy trình xử lý chẳng hạn như loại bỏ nhật ký truyền thông từ đích phân tích. Ngoài ra, khi ngày tháng và thời gian phát hiện được thiết đặt là mục xác định, bộ phận thu thập 210 có thể thực hiện quy trình xử lý sao cho chỉ các truyền thông mà được diễn ra tại hoặc sau ngày tháng và thời gian quy định được bao gồm làm các đích phân tích.

Bộ phận thu thập 210 nhờ đó trích các nhật ký truyền thông của các đích xử lý từ các tệp nhật ký truyền thông trong nhật ký chưa xử lý được thu nhận từ hệ thống con quản lý nhật ký 120, và thực hiện việc chuẩn hóa. Bộ phận thu thập 210 sau đó gửi các nhật ký truyền thông mà đã trải qua xử lý tới bộ phận phát hiện phía sau 220.

Theo phương án sáng chế, bộ phận thực hiện dùng để thực hiện xử lý nêu trên có thể được tạo cấu hình bởi các thành phần tách biệt đối với mỗi bộ phận xử lý nhỏ. Bằng cách kết hợp các khối của các bộ phận xử lý được cấu thành (trong bản mô tả này được gọi là "khối bộ phận xử lý"), việc cấu hình các

quy trình xử lý tương ứng với các thiết bị phát hiện khác nhau 110 có thể trở nên dễ dàng. Nội dung xử lý (các bộ phận xử lý) được thực hiện bởi các khối bộ phận xử lý riêng là không giới hạn. Nội dung có thể được thiết đặt để có thể xử lý các thiết bị phát hiện khác nhau 110 bằng cách tạo cấu hình lại các khối bộ phận xử lý.

Fig.3 là hình vẽ minh họa ví dụ về cấu hình của bộ phận thu thập được minh họa trên Fig.2 được tạo cấu hình bởi các khối bộ phận xử lý được cấu thành.

Như được minh họa trên Fig.3, các khối bộ phận xử lý 211 bao gồm khối thu thập thông tin ban đầu 211a, khối thu thập số đếm trường hợp thu được 211b, khối đăng ký tệp thu được 211c, khối biên soạn đề mục 211d, khối đăng ký thông tin nhật ký không phù hợp định dạng 211e, khối biên soạn đề mục chung các nhật ký 211f, và khối phân chia khách hàng 211d. Khối thu thập thông tin ban đầu 211a là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để thu nhận thông tin ban đầu. Khối thu thập số đếm trường hợp thu được 211b là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để thu nhận số lượng trường hợp thu được. Khối đăng ký tệp thu được 211c là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để đăng ký các tệp thu được. Khối biên soạn đề mục 211d là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để biên soạn các đề mục. Khối đăng ký thông tin nhật ký không phù hợp định dạng 211e là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để đăng ký thông tin nhật ký không phù hợp. Khối biên soạn đề mục nhật ký chung 211f là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để biên soạn các đề mục nhật ký chung. Khối phân chia khách hàng 211d là khối bộ phận xử lý dùng để thực hiện quy trình xử lý để phân chia khách hàng. Các khối bộ phận xử lý 211 được kết hợp để tạo cấu hình bộ phận thu thập 211. Lưu ý là chỉ một phần của các khối bộ phận xử lý 211 mà tạo cấu hình bộ phận thu thập 210 được minh họa trên Fig.3. Ví dụ, các khối bộ phận xử lý 211 chẳng hạn như khối thu thập thông tin ban đầu 211a, khối thu thập số đếm trường hợp thu được 211b, và khối đăng ký tệp thu được 211c xử lý quy trình trích đích phân tích nhật ký được minh họa trên Fig.2. Các khối bộ phận xử lý 211 chẳng hạn như khối biên soạn đề mục 211d, khối đăng ký thông tin nhật ký không phù hợp định dạng 211e, và khối biên soạn đề mục nhật ký chung 211f xử lý quy trình chuẩn hóa được minh họa trên Fig.2. Các khối bộ

phận xử lý 211 chẳng hạn như khối phân chia khách hàng 211g kiểm soát sự xử lý phân phối được minh họa trên Fig.2.

Theo phương án sáng chế, loại và trình tự của các khối bộ phận xử lý ứng dụng được 211 được thiết đặt theo loại thiết bị phát hiện 110 (các loại sản phẩm chẳng hạn như IDS/IPS, tường lửa, phần mềm chống virus, và tương tự). Nghĩa là, trình tự ứng dụng được của các khối bộ phận xử lý 211 được tạo ra đối với mỗi loại thiết bị phát hiện 110 của thiết bị đích giám sát 100 mà thiết đặt đích cần được giám sát. Sau đó xử lý được thực hiện bởi mỗi khối bộ phận xử lý 211 bằng cách ứng dụng trình tự được thiết đặt để thực hiện xử lý tệp nhật ký truyền thông theo loại thiết bị phát hiện 110 mà thu nhận tệp nhật ký truyền thông làm đích xử lý.

Các kết quả xử lý được thực hiện bởi mỗi trong số các khối bộ phận xử lý 211 của bộ phận thu thập 210 có thể được lưu trữ tạm thời trong, chẳng hạn, bộ nhớ máy tính mà tạo cấu hình bộ phận thu thập 210. Các kết quả sau đó được gửi tới bộ phận phát hiện phía sau 220 cùng với nhật ký truyền thông ngay khi sự xử lý bởi bộ phận thu thập 210 kết thúc.

Các chức năng của bộ phận phát hiện

Fig.4 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận phát hiện 220 mà tạo cấu hình hệ thống con giám sát 200.

Bộ phận phát hiện 220, mà là bộ phận xử lý thứ hai, thực hiện xử lý trên các nhật ký truyền thông được thu nhận từ bộ phận thu thập phía trước 210. Xử lý được thiết đặt theo loại thiết bị phát hiện 110 mà thu nhận nhật ký truyền thông cơ sở (nhật ký chưa xử lý) của tệp nhật ký truyền thông. Do được sử dụng trong bản mô tả này, nên loại dịch vụ bảo vệ bộ phận thiết bị phát hiện (IDS/IPS, tường lửa, hoặc tương tự) được dùng để cung cấp các chức năng của cảm biến 111 và bộ quản lý cảm biến 112 của thiết bị phát hiện 110. Lưu ý rằng thông tin mà định rõ loại thiết bị phát hiện (chẳng hạn như ID, tên thiết bị) có thể được bao gồm trong, chẳng hạn, tệp nhật ký truyền thông.

Như được minh họa trên Fig.4, bộ phận phát hiện 220 theo phương án sáng chế thực hiện xử lý bổ sung thông tin chung và xử lý tập hợp nhật ký (tạo các sự kiện) của nhật ký truyền thông được xử lý bởi bộ phận thu thập 210.

Bộ phận phát hiện 220 bổ sung thông tin chung được sử dụng trong phân tích nhật ký truyền thông trong suốt thời gian xử lý bổ sung thông tin chung. Thông tin chung là thông tin liên quan đến các đề mục chung trong mỗi nhật ký truyền thông. Theo phương án sáng chế, năm đề mục chung dưới đây được thiết đặt là thông tin chung: thông tin mẫu tấn công (ID ký hiệu gốc), phân loại hướng truyền thông, thông tin thực hành quy tắc, số hoặc tên giao thức, và mã quốc gia.

Thông tin mẫu tấn công là thông tin được bổ sung vào các nhật ký truyền thông bởi hệ thống con giám sát 200 để định rõ mẫu tấn công. Khi thiết bị phát hiện 110 phát hiện một vài loại tấn công trong nhật ký truyền thông (nhật ký chưa xử lý), thông tin mà định rõ sự tấn công được phát hiện (thông tin nhà sản xuất hoặc thông tin ký hiệu) được bổ sung vào nhật ký truyền thông. Tuy nhiên, định dạng của thông tin khác nhau tùy thuộc vào loại thiết bị đích giám sát 100 và loại thiết bị phát hiện 110. Do đó, bộ phận phát hiện 220 bổ sung thông tin gốc (thông tin mẫu tấn công) vào nhật ký truyền thông theo phương án sáng chế.

Phân loại hướng truyền thông là thông tin hiển thị xem truyền thông được thể hiện bởi nhật ký truyền thông là truyền thông được thực hiện theo hướng từ mạng ngoại vi hướng về mạng nội bộ mà được phân loại bởi thiết bị đích giám sát 100, hay là truyền thông được thực hiện theo hướng ngược lại từ mạng nội bộ, nhờ thiết bị đích giám sát 100, hướng về mạng ngoại vi. Trong lĩnh vực bảo vệ mạng, các sự liên quan và tầm quan trọng của các truyền thông khác biệt lớn bởi việc nguồn truyền thông là mạng nội bộ hay mạng ngoại vi. Trường hợp nhật ký truyền thông dùng cho các truyền thông được thực hiện bởi thiết bị xử lý thông tin gây ảnh hưởng xấu với virus máy tính được giải thích làm ví dụ cụ thể. Trong trường hợp này thông tin xử lý gây ảnh hưởng xấu với virus máy tính tồn tại trong mạng ngoại vi, vì vậy không có các vấn đề cụ thể được tạo ra mà truyền thông là từ mạng ngoại vi. Mặt khác khi truyền thông được gửi từ mạng nội bộ, khi thiết bị xử lý thông tin gây ảnh hưởng xấu với virus máy tính tồn tại trong mạng nội bộ mà là đích cần được bảo vệ của thiết bị đích giám sát 100, nó cần phải được xử lý. Theo phương án sáng chế, bộ phận phát hiện 220 bổ sung phân loại thông tin hướng truyền thông thể hiện hướng của các truyền thông trong nhật ký truyền thông. Sự phân loại thông tin hướng truyền thông có thể thu được, ví dụ, nhờ tham chiếu đến địa chỉ mạng và địa chỉ riêng lẻ của thiết bị đích giám sát 100 và xác định xem địa chỉ IP người gửi hoặc địa chỉ IP đích là mạng nội bộ của thiết bị đích giám sát 100 hay mạng ngoại vi.

Thông tin thực hành quy tắc là thông tin thể hiện hoạt động được thực hiện bởi thiết bị phát hiện 110 để đáp lại sự truyền thông khi truyền thông được phát hiện trong thiết bị đích giám sát 100. Đối với các trường hợp mà ở đó thiết bị bảo vệ chẳng hạn như IDS hoặc IPS được sử dụng làm thiết bị phát hiện 110, thiết bị thông báo rằng truyền thông nguy hiểm đã được phát hiện, hoặc dừng truyền thông bằng cách không cung cấp sự cho phép, dựa vào chức năng thiết bị. Thông tin thể hiện loại của hoạt động mà được thực hiện được bổ sung bởi bộ phận phát hiện 220. Có các trường hợp mà ở đó thông tin thực hành quy tắc được bổ sung vào nhật ký truyền thông tùy thuộc vào thiết bị bảo vệ được sử dụng cho thiết bị phát hiện 110. Tuy nhiên, ngay cả đối với các thao tác giống hệt nhau, tên được sử dụng cho hoạt động có thể khác nhau tùy thuộc vào loại thiết bị bảo vệ được sử dụng. Do đó, bộ phận phát hiện 220 của hệ thống con giám sát 200 bổ sung các tên được chuẩn hóa.

Số hoặc tên giao thức là thông tin thể hiện loại giao thức truyền thông được sử dụng trong các truyền thông được hiển thị trong nhật ký truyền thông. Một vài loại giao thức tồn tại, chẳng hạn như TCP UDT, và do đó bộ phận phát hiện 220 bổ sung thông tin để phân loại các giao thức. Theo phương án sáng chế, thông tin thể hiện các loại giao thức truyền thông có thể được thiết đặt dựa vào, chẳng hạn, các chỉ số của Tổ chức cấp phát số hiệu Internet (IANA- Internet Assigned Number Authority).

Mã quốc gia là thông tin thể hiện quốc gia người gửi và quốc gia đến dùng cho các truyền thông được hiển thị trong nhật ký truyền thông. Các quốc gia được xác định dựa vào địa chỉ IP người gửi và địa chỉ IP đích trong nhật ký truyền thông. Các mã quốc gia được sử dụng chủ yếu như thông tin tĩnh. Các mã quốc gia có thể cũng được sử dụng trong phân tích nhật ký truyền thông đối với các trường hợp khi xét đến các sự khác nhau về các mức nguy hiểm truyền thông dựa vào việc xem quốc gia người gửi hoặc quốc gia đến có là quốc gia có lượng tấn công cao bởi các truyền thông không được phép hay không, và xem các truyền thông không được phép có đến từ bên trong quốc gia mà ở đó bộ phận phát hiện 220 được xác định vị trí hay không.

Bộ phận phát hiện 220 nhờ đó bổ sung thông tin tới các nhật ký truyền thông làm thông tin định dạng chung. Thông tin có giá trị hữu ích cao để phân tích các nhật ký truyền thông.

Bộ phận phát hiện 220 xem xét các nhật ký truyền thông dựa vào nhu cầu, và tạo ra các sự kiện, mà là thông tin bộ phận phân tích, trong suốt thời gian xử lý tập hợp nhật ký. Độ chi tiết thông tin của các nhật ký truyền thông là khác nhau phụ thuộc vào loại thiết bị bảo vệ được sử dụng làm thiết bị phát hiện 110. Ví dụ, khi thiết bị phát hiện 110 là tường lửa và truyền thông mà được tiến hành việc phát hiện được tìm thấy, truyền thông được phát hiện ngay lập tức bởi cảm biến 111. Nếu thiết bị phát hiện 110 thay cho IDS hoặc tương tự, việc truyền thông có thể được đánh giá là nguy hiểm bởi cảm biến 111 theo quy tắc đánh giá định trước dựa vào nhiều sự kiện truyền thông nguy hiểm xảy ra. Đối với các trường hợp mà ở đó thiết bị phát hiện 110 là phần mềm chống virus, sự gây ảnh hưởng xấu được phát hiện bởi cảm biến 111 khi đích thiết bị xử lý thông tin bị gây ảnh hưởng xấu bởi virus máy tính. Khối lượng thông tin trong một nhật ký truyền thông do đó là khác nhau theo loại thiết bị phát hiện 110. Theo phương án sáng chế, bộ phận phát hiện 220 tập hợp nhiều nhật ký truyền thông và tạo các sự kiện, và đồng chỉnh độ chi tiết thông tin tùy thuộc vào loại thiết bị phát hiện. Nghĩa là, bộ phận phát hiện 220 tạo một sự kiện với số lượng rất nhỏ các nhật ký truyền thông khi các nhật ký truyền thông đơn được thu nhận bởi thiết bị phát hiện 110 chứa lượng lớn thông tin. Mặt khác, bộ phận phát hiện 220 tạo một sự kiện với số lượng khá lớn các nhật ký truyền thông khi các nhật ký truyền thông đơn được thu nhận bởi được phát hiện bởi thiết bị phát hiện 110 chứa lượng nhỏ thông tin.

Như một ví dụ, theo phương án sáng chế xử lý tạo sự kiện là khác nhau giữa các trường hợp mà ở đó thiết bị phát hiện 110 là tường lửa và đối với các trường hợp mà ở đó thiết bị phát hiện 110 là loại khác của thiết bị. Cụ thể là, nếu thiết bị phát hiện 110 là tường lửa, có lượng nhỏ thông tin trong các nhật ký truyền thông (một sự truyền thông được phát hiện bởi cảm biến 111), như được nêu trên. Do đó bộ phận phát hiện 220 tạo sự kiện bằng cách tập hợp các nhật ký truyền thông đã được thu nhận theo quy tắc định trước. Các nhật ký truyền thông được thu nhận khi thiết bị phát hiện là một thiết bị không phải là tường lửa chứa lượng thông tin tương đối lớn trên mỗi nhật ký truyền thông khi được so sánh với lượng thông tin của tường lửa (các truyền thông và tương tự được phát hiện bởi cảm biến 111 bao gồm nhiều truyền thông). Trong trường hợp này bộ phận phát hiện 220 nhờ đó tạo một sự kiện cho một nhật ký.

Xử lý tạo sự kiện khi thiết bị phát hiện 110 là tường lửa được thực hiện như sau đây. Đầu tiên, bộ phận phát hiện 220 tập hợp các nhật ký truyền thông tương ứng với quy tắc tập hợp định trước và tạo sự kiện, dựa vào thông tin được bao gồm trong các nhật ký truyền thông và dựa vào thông tin chung được bổ sung tới các nhật ký truyền thông bởi xử lý bổ sung thông tin chung nêu trên. Cụ thể là, bộ phận phát hiện 220 có thể lấy các nhật ký truyền thông làm các đích khi các đề mục đánh giá sau đây là chung: ID khách hàng, ngày tháng phát hiện, địa chỉ IP người gửi, số hiệu cổng người gửi, địa chỉ IP đích, hoặc số hiệu cổng đích được bao gồm trong các nhật ký truyền thông; và phân loại hướng truyền thông, sự thực hành quy tắc, và số giao thức (tên), mà là thông tin chung. Bộ phận phát hiện 220 tập hợp các nhật ký truyền thông ứng dụng được với nhau và tạo một sự kiện khi số lượng của các nhật ký truyền thông có các đề mục đánh giá chung là bằng hoặc vượt quá giá trị ngưỡng định trước.

Việc xác định bởi máy chủ và sự tập hợp quét được thực hiện tiếp theo trên các nhật ký truyền thông được xác định là không phù hợp dựa vào các quy tắc tập hợp nêu trên. Cụ thể là, bộ phận phát hiện 220 có thể lấy các nhật ký truyền thông làm các đích khi các đề mục đánh giá sau đây là chung: ID khách hàng, ngày tháng phát hiện, địa chỉ IP người gửi, số hiệu cổng người gửi, số hiệu cổng đích được bao gồm trong các nhật ký truyền thông; và thông tin chung bao gồm phân loại hướng truyền thông, sự thực hành quy tắc, và số giao thức (tên). Bộ phận phát hiện 220 tập hợp các nhật ký truyền thông ứng dụng được với nhau và tạo một sự kiện khi số lượng của các nhật ký truyền thông có địa chỉ IP đích nhất định, từ trong số các nhật ký truyền thông có các đề mục đánh giá chung, là bằng hoặc vượt quá giá trị ngưỡng định trước.

Tiếp theo, sự xác định được thực hiện bởi sự tập hợp quét cổng trên các nhật ký truyền thông được xác định là không phù hợp dựa vào sự tập hợp quét máy chủ nêu trên. Cụ thể là, bộ phận phát hiện 220 có thể lấy các nhật ký truyền thông làm các đích khi các đề mục đánh giá sau đây là chung: ID khách hàng, ngày tháng phát hiện, địa chỉ IP người gửi, số hiệu cổng người gửi, địa chỉ IP đích được bao gồm trong các nhật ký truyền thông; và thông tin chung bao gồm phân loại hướng truyền thông, sự thực hành quy tắc, và số giao thức (tên). Bộ phận phát hiện 220 tập hợp các nhật ký truyền thông ứng dụng được với nhau và tạo một sự kiện khi số lượng của các nhật ký truyền thông có số hiệu cổng đích

nhất định, từ trong số các nhật ký truyền thông có các đề mục đánh giá chung, là bằng hoặc vượt quá giá trị ngưỡng định trước.

Bộ phận phát hiện 220 tập hợp các nhật ký truyền thông ứng dụng được với nhau, và tạo một sự kiện từ số lượng định trước của các nhật ký truyền thông, đối với các nhật ký truyền thông không phù hợp được xác định bởi sự tập hợp quét cổng. Bộ phận phát hiện 220 nhờ đó tập hợp các nhật ký truyền thông được thu nhận bởi thiết bị phát hiện 110 của tường lửa có độ chi tiết thông tin nhỏ. Độ chi tiết thông tin gần như độ chi tiết thông tin của các nhật ký truyền thông (các sự kiện) được thu nhận bởi các thiết bị phát hiện 110 khác. Bộ phận phát hiện 220 sau đó gửi các sự kiện có độ chi tiết thông tin được đồng chỉnh tới bộ phận phân tích phía dưới 230.

Theo phương án sáng chế, bộ phận thực hiện dùng để thực hiện xử lý giống như các xử lý nêu trên được tạo cấu hình bằng cấu thành thành các bộ phận xử lý nhỏ. Bằng cách kết hợp các khối bộ phận xử lý được cấu thành (trong bản mô tả này được gọi là các khối bộ phận xử lý), nội dung xử lý được thực hiện bởi bộ phận phát hiện 220 (chẳng hạn như loại và trình tự của các bộ phận xử lý riêng) có thể được thiết kế. Việc tạo cấu hình xử lý tương ứng với các loại thiết bị đích giám sát 100 có thể trở nên dễ dàng. Không có giới hạn nào đối với nội dung xử lý (các bộ phận xử lý) được thực hiện bởi các khối bộ phận xử lý riêng. Nội dung được thiết đặt sao cho có thể điều khiển các thiết bị đích giám sát 100 bằng cách kết hợp các khối bộ phận xử lý.

Fig.5 là hình vẽ minh họa ví dụ về cấu hình của bộ phận phát hiện 220 được tạo cấu hình bởi các khối bộ phận xử lý được cấu thành.

Đối với ví dụ được minh họa trên Fig.5, các khối bộ phận xử lý 221 bao gồm khối bổ sung thông tin nhận dạng duy nhất 221a, khối bổ sung phân loại hướng truyền thông 221b, khối bổ sung thực hành quy tắc 221c, khối bổ sung số hiệu và tên giao thức 221d, khối bổ sung mã quốc gia 221e, khối xác định quy tắc tập hợp 221f, khối tập hợp quét máy chủ 221g, và khối tập hợp quét cổng 221h. Khối bổ sung thông tin nhận dạng duy nhất 221a là khối bộ phận xử lý để bổ sung thông tin nhận dạng duy nhất. Khối bổ sung phân loại hướng truyền thông 221b là khối bộ phận xử lý để bổ sung các phân loại hướng truyền thông. Khối bổ sung thực hành quy tắc 221c là khối bộ phận xử lý để bổ sung các sự thực hành quy tắc. Khối bổ sung số hiệu và tên giao thức 221d là khối bộ phận

xử lý để bổ sung các số hiệu và tên giao thức. Khối bổ sung mã quốc gia 221e là khối bộ phận xử lý để bổ sung các mã quốc gia. Khối xác định quy tắc tập hợp 221f là khối bộ phận xử lý để xác định các quy tắc tập hợp. Khối tập hợp quét máy chủ 221g là khối bộ phận xử lý để tập hợp sự quét máy chủ. Khối tập hợp quét cổng 221h là khối bộ phận xử lý để tập hợp các sự quét cổng. Sự kết hợp các khối bộ phận xử lý 221 tạo cấu hình bộ phận phát hiện 220. Lưu ý là chỉ một phần của các khối bộ phận xử lý 221 mà tạo cấu hình bộ phận phát hiện 220 được minh họa trên Fig.5. Ví dụ, các khối bộ phận xử lý 221 chẳng hạn như khối bổ sung thông tin nhận dạng duy nhất 221a, khối bổ sung phân loại hướng truyền thông 221b, khối bổ sung thực hành quy tắc 221c, khối bổ sung số hiệu và tên giao thức 221d, và khối bổ sung mã quốc gia 221e thực hiện xử lý bổ sung thông tin chung được minh họa trên Fig.4. Các khối bộ phận xử lý 221 chẳng hạn như khối xác định quy tắc tập hợp 221f, khối tập hợp quét máy chủ 221g, và khối tập hợp quét cổng 221h thực hiện xử lý tập hợp nhật ký (tạo sự kiện) được minh họa trên Fig.4

Theo phương án sáng chế, loại và trình tự của các khối bộ phận xử lý ứng dụng được 221 được thiết đặt tùy thuộc vào loại thiết bị đích giám sát 100 (sự phân loại thiết bị bảo vệ). Nghĩa là, trình tự ứng dụng được của các khối bộ phận xử lý 221 được tạo ra đối với mỗi loại thiết bị đích giám sát 100 mà được thiết đặt làm đích giám sát. Sau đó xử lý được thực hiện bởi mỗi khối bộ phận xử lý 221 bằng cách ứng dụng trình tự được thiết đặt để thực hiện xử lý tệp nhật ký truyền thông theo loại thiết bị đích giám sát 100 mà thu nhận tệp nhật ký truyền thông làm đích xử lý.

Các kết quả xử lý được thực hiện bởi mỗi trong số các khối bộ phận xử lý 221 của bộ phận thu thập 220 có thể được lưu trữ tạm thời trong bộ nhớ máy tính mà tạo cấu hình bộ phận thu thập 220 chẳng hạn. Các kết quả sau đó được gửi tới bộ phận phân tích phía dưới 230 cùng với nhật ký truyền thông ngay khi sự xử lý bởi bộ phận phát hiện 220 hoàn thành.

Các chức năng của bộ phận phân tích

Fig.6 là hình vẽ minh họa ví dụ về cấu hình chức năng của bộ phận phân tích 230 mà tạo cấu hình hệ thống con giám sát 200.

Trong ví dụ cấu hình được minh họa trên Fig.6, bộ phận phân tích 230, mà là bộ phận xử lý thứ ba, được tạo cấu hình bởi bộ xử lý phân tích riêng 230a,

bộ xử lý tập hợp sự kiện 230b, bộ xử lý phân tích tương quan 230c, và bộ xử lý phân tích gia tăng 230d.

Bộ xử lý phân tích riêng 230a xác định xem vấn đề tồn tại trong các sự kiện riêng lẻ có được tạo ra bởi bộ phận phát hiện 220 hay không. Cụ thể là, bộ xử lý phân tích riêng 230a kiểm tra các sự kiện (thực hiện sự so khớp) và các danh sách (các danh sách đen) liên quan đến các truyền thông không được phép, và xác định rằng việc truyền thông được hiển thị trong sự kiện cụ thể là truyền thông không được phép khi sự trùng khớp được phát hiện. Các địa chỉ IP liên quan đến các truyền thông có vấn đề có thể được ghi lại trong, chẳng hạn, danh sách truyền thông không được phép. Bộ xử lý phân tích riêng 23a sau đó xác định rằng truyền thông là truyền thông không được phép khi hoặc địa chỉ IP người gửi hoặc địa chỉ IP đích của truyền thông được hiển thị trong sự kiện trùng khớp địa chỉ IP được ghi trong danh sách.

Ngoài ra, bộ xử lý phân tích riêng 230a xác định xem có thực hiện quy trình xử lý hay không dựa vào sự tương quan giữa các sự kiện đối với các sự kiện mà ở đó đã được xác định rằng có truyền thông có vấn đề do trùng khớp với danh sách truyền thông có vấn đề. Nghĩa là, bộ xử lý phân tích riêng 230a có chức năng như bộ phận phân loại (bộ phân loại) dùng để phân loại các sự kiện làm các sự kiện mà ở đó phân tích được thực hiện dựa vào sự tương quan, và các sự kiện mà ở đó sự phân tích tương quan không được thực hiện dựa vào sự tương quan. Việc xác định xem sự kiện có là đích để phân tích hay không dựa vào sự tương quan có thể được thực hiện như sau đây, ví dụ: sự xác định có thể được thực hiện bởi thông tin chung (chẳng hạn như thông tin mẫu tấn công, thông tin hướng truyền thông, và tương tự) được bổ sung tới nhật ký truyền thông bởi bộ phận phát hiện 220 trong suốt thời gian xử lý bổ sung thông tin chung, dựa vào nội dung truyền thông cụ thể. Đối với các sự kiện mà đã được xác định là các đích mà ở đó xử lý phân tích là cần được thực hiện dựa vào sự tương quan, xử lý tập hợp được thực hiện tiếp theo bởi bộ xử lý tập hợp sự kiện 230b. Mặt khác, đối với các sự kiện mà ở đó đã được xác định rằng phân tích không cần được thực hiện dựa vào sự tương quan, bộ phận phân tích 230 gửi sự kiện tới bộ phận phân tích thủ công 240 mà không thực hiện phân tích sau đó (nghĩa là, do đích không được thực hiện phân tích tương quan hoặc phân tích gia tăng).

Bộ xử lý tập hợp sự kiện 230b tạo tập hợp các sự kiện mà được xác định bởi bộ xử lý phân tích riêng 230a là các đích phân tích dựa vào sự tương quan. Các sự kiện được tập hợp dựa vào quy tắc định trước. Bộ xử lý tập hợp sự kiện 230b cũng tạo danh sách sự kiện (chuỗi sự kiện) từ một hoặc nhiều sự kiện. Ngoài ra, bộ xử lý tập hợp sự kiện 230b tập hợp các chuỗi sự kiện dựa vào quy tắc định trước, và tạo ứng viên sự cố từ một hoặc nhiều chuỗi sự kiện. Ứng viên sự cố trở thành đích phát hiện bởi phân tích (được gọi là ứng viên sự cố được phát hiện). Nghĩa là, bộ tập hợp sự kiện 230b có chức năng làm bộ phận tập hợp (bộ tập hợp) để tập hợp các sự kiện và tạo các ứng viên sự cố được phát hiện. Cụ thể là, bộ xử lý tập hợp sự kiện 230b có thể thực hiện như sau đây đối với các sự tấn công do truy cập không được phép từ máy chủ hoặc tương tự hiện có trên mạng ngoại vi. Ví dụ bộ xử lý tập hợp sự kiện 230b có thể, ví dụ, trích các truyền thông được giả thiết là các sự tấn công từ cùng đối tượng tấn công (truy cập), sử dụng cùng bộ phận tấn công (phương pháp truy cập), có cùng đích tấn công, hoặc tương tự, và thu thập các truyền thông được trích làm các ứng viên sự cố được phát hiện. Việc trích các truyền thông được giả thiết là các sự tấn công bởi cùng đối tượng tấn công, sử dụng cùng bộ phận tấn công có cùng đích tấn công, hoặc tương tự có thể được thực hiện dựa vào thông tin chẳng hạn như địa chỉ IP người gửi, phân loại hướng truyền thông, ngày tháng phát hiện, hoặc tương tự chẳng hạn.

Sự thu nhận nhật ký truyền thông bởi thiết bị phát hiện 110 và hệ thống con quản lý nhật ký 120, và xử lý bởi bộ phận thu thập 210 và bộ phận phát hiện 220 của hệ thống con giám sát 200 xảy ra như mong muốn. Các sự kiện nhờ đó được tạo ra liên tiếp theo thời gian. Khi được xác định bởi bộ xử lý tập hợp sự kiện 230c là sự kiện đích được bao gồm trong ứng viên sự cố bộ phát hiện cụ thể, sự kiện mới được tạo ra được hợp nhất thành ứng viên sự cố bộ phát hiện. Ứng viên sự cố bộ phát hiện do đó trở thành đích để xử lý bởi bộ xử lý phân tích tương quan 230c và bởi bộ xử lý phân tích gia tăng 230d đối với mỗi sự kiện mới được bổ sung.

Bằng cách thực hiện sự xác định hợp nhất mẫu tấn công và xác định vượt ngưỡng số trường hợp, bộ xử lý phân tích tương quan (bộ phận phân tích, bộ phân tích) 230c xác định xem ứng viên sự cố có được phát hiện hay không, mà là sự kết hợp của nhiều sự kiện, là truyền thông có vấn đề.

Trong suốt thời gian xác định kết hợp mẫu tấn công, bộ xử lý phân tích tương quan 230c xác định xem truyền thông được định rõ bởi ứng viên sự cố được phát hiện có là truyền thông có vấn đề hay không. Sự xác định được thực hiện sử dụng loại truyền thông cụ thể dựa vào hướng truyền thông, người gửi và các địa chỉ IP đích (các khoảng), người gửi và đích, các sự thực hành quy tắc, người gửi và các mã quốc gia đích, dữ liệu phiên, và tương tự, và dựa vào thông tin mẫu tấn công (ID ký hiệu gốc). Nghĩa là, bộ xử lý phân tích tương quan 230c xác định xem nội dung truyền thông có được định rõ bởi ứng viên sự cố bộ phát hiện tương ứng với mẫu tấn công được định rõ bởi thông tin mẫu tấn công hay không. Lưu ý là bộ xử lý phân tích tương quan 230c xác định xem sự thực hiện tấn công thực tế (sự khai thác thông tin, xóa thông tin, hoặc tương tự) theo thông tin có khả năng cao hay không.

Trong suốt thời gian xác định vượt ngưỡng số trường hợp, bộ xử lý phân tích tương quan 230c xác định xem truyền thông được định rõ bởi ứng viên sự cố được phát hiện có là truyền thông có vấn đề hay không. Sự xác định được thực hiện dựa vào thông tin về số các trường hợp của hướng truyền thông, người gửi và các địa chỉ IP đích (các khoảng), người gửi và đích, các sự thực hành quy tắc, người gửi và các mã quốc gia đích, và tương tự trong các nhật ký truyền thông được bao gồm trong ứng viên sự cố được phát hiện. Bộ xử lý phân tích tương quan 230c xác định xem số lượng của các truyền thông được định rõ bởi ứng viên sự cố được phát hiện có tăng nhiều so với lượng thông thường hay không.

Fig.7 là hình vẽ minh họa mô hình phân tích tương quan.

Bộ xử lý tập hợp sự kiện 230b của bộ phận phân tích 230 tập hợp các sự kiện mà trở thành các đích xử lý tập hợp, tạo trình tự sự kiện và ngoài ra, tạo ứng viên sự cố được phát hiện từ trong số các sự kiện được thu nhận từ bộ phận phát hiện 220. Bộ xử lý tập hợp sự kiện 230b sau đó thực hiện xác định kết hợp mẫu tấn công và xác định vượt ngưỡng số trường hợp đối với mỗi ứng viên sự cố được phát hiện dựa trên trình tự sự kiện được bao gồm trong mỗi ứng viên sự cố bộ phát hiện và dựa trên sự tương quan giữa các sự kiện.

Bộ xử lý phân tích gia tăng 230d xác định xem ứng viên sự cố được phát hiện, mà là sự kết hợp của nhiều sự kiện, có là truyền thông có vấn đề hay không bằng cách thực hiện sự xác định thay đổi sự cố, sự xác định tăng bộ phận tấn

công, sự xác định tăng trường hợp tấn công, và sự xác định tăng đích tấn công. Ví dụ, đối với các sự tấn công từ máy chủ hoặc tương tự hiện có trong mạng ngoại vi, sự tấn công có thể không phải là sự cố đơn mà còn sự tấn công giống nhau có thể được lặp lại liên tiếp, nội dung tấn công có thể được thay đổi, hoặc các đích tấn công có thể tăng lên. Bộ xử lý phân tích gia tăng 230d xác định xem các truyền thông có vấn đề đã nghi ngờ các sự thay đổi sự cố dựa vào nhật ký truyền thông được bao gồm trong ứng viên sự cố được phát hiện hay chưa.

Sự giải thích tiếp theo liên quan đến các sự xác định như sau đây. Ví dụ, bộ xử lý phân tích gia tăng 230d có thể xác định các sự thay đổi ứng dụng được để phân tích các quy tắc (các quy tắc dùng để xác định kết hợp mẫu tấn công hoặc xác định vượt ngưỡng số trường hợp) được sử dụng trong phân tích mỗi ứng viên sự kiện phát hiện, dựa vào các kết quả phân tích trong khoảng thời gian cố định (ví dụ, một ngày) từ bộ xử lý phân tích tương quan 230c.

Sự xác định thay đổi ứng dụng có thể được sử dụng đối với các trường hợp mà ở đó các quy tắc khác với phân tích trước được ứng dụng (sự cố khác nhau). Bộ xử lý phân tích gia tăng 230c xác định rằng truyền thông được bao gồm trong ứng viên sự cố được phát hiện làm đích xác định là truyền thông có vấn đề.

Sự xác định tăng bộ phận tấn công có thể được sử dụng đối với các trường hợp mà ở đó các quy tắc giống với phân tích trước được ứng dụng, nhưng thông tin mẫu tấn công làm đích xác nhận đã tăng (bộ phận tấn công của đích xác nhận đã tăng). Bộ xử lý phân tích gia tăng 230d xác định rằng truyền thông được bao gồm trong ứng viên sự cố được phát hiện làm đích xác định là truyền thông có vấn đề.

Sự xác định tăng trường hợp tấn công có thể được sử dụng đối với các trường hợp mà ở đó các truyền thông có thông tin mẫu tấn công làm đích xác nhận giống nhau (bộ phận tấn công giống nhau), đối với các trường hợp mà ở đó các truyền thông được tiếp tục từ đối tượng tấn công giống nhau, và đối với các trường hợp mà ở đó số lượng của các sự kiện trên mỗi thời gian đơn vị do các truyền thông này đã tăng. Bộ xử lý phân tích gia tăng 230d xác định rằng truyền thông được bao gồm trong ứng viên sự cố được phát hiện làm đích xác định là truyền thông có vấn đề.

Sự xác định tăng đích tấn công có thể được sử dụng đối với các trường hợp các đích tấn công hoặc các đích kết nối đã tăng. Bộ xử lý phân tích gia tăng 230d xác định rằng truyền thông được bao gồm trong ứng viên sự cố được phát hiện làm đích xác định là truyền thông có vấn đề.

Fig.8A và Fig.8B là các hình vẽ minh họa mô hình phân tích gia tăng theo phương án sáng chế. Fig.8A minh họa ví dụ về cấu hình của một ứng viên sự cố được phát hiện mà trở thành đích phân tích tương quan đối với phân tích nhất định. Fig.8B minh họa ví dụ về cấu hình của cùng ứng viên sự cố được phát hiện đối với phân tích tiếp theo.

Cấu hình phân tích trước (xem Fig.8A) và cấu hình phân tích hiện thời (xem Fig.8B) liên quan đến cùng ứng viên sự cố bộ phát hiện được so sánh ở đây. Với cấu hình phân tích hiện thời, trình tự sự kiện (trình tự sự kiện được chia sẻ trên Fig.8B) không được bao gồm trong phân tích trước là hiện có trong cấu hình phân tích hiện thời. Do đó, ứng viên sự cố được phát hiện được xác định là truyền thông có vấn đề trong sự xác định bất kỳ trong số sự xác định thay đổi sự cố, sự xác định tăng bộ phận tấn công, sự xác định tăng trường hợp tấn công, hoặc sự xác định tăng đích tấn công, như được nêu trên.

Sau khi mỗi loại xác định được thực hiện, bộ phận phân tích 230 gửi các kết quả phân tích đối với mỗi ứng viên sự cố xác định tới bộ phận phân tích thủ công 240, với các ứng viên sự cố được phát hiện làm đích phân tích được kết hợp. Các kết quả phân tích từ bộ phận phân tích 230 thể hiện rằng mỗi ứng viên sự cố được phát hiện là truyền thông không được phép, truyền thông có vấn đề (truyền thông có khả năng là truyền thông không được phép), hoặc không phải là truyền thông không được phép.

Theo phương án sáng chế, bộ xử lý phân tích riêng 230a, bộ xử lý tập hợp sự kiện 230b, bộ xử lý phân tích tương quan 230c, và bộ xử lý phân tích gia tăng 230d mà thực hiện xử lý nêu trên được tạo cấu hình như được cấu thành thành các bộ phận xử lý nhỏ. Bằng cách kết hợp các khối bộ phận xử lý được cấu thành (trong bản mô tả này được gọi là các khối bộ phận xử lý), nội dung xử lý được thực hiện bởi mỗi bộ xử lý từ 230a đến 230d (chẳng hạn như loại và trình tự của các bộ phận xử lý riêng) có thể được thiết kế. Do đó việc đáp lại khi các sự tấn công bởi các phương pháp tấn công chưa được biết đến cho đến nay được phát hiện có thể trở nên dễ dàng. Điều này có thể đạt được bằng cách tăng

các khối bộ phận xử lý đối với xử lý ứng dụng được để xác định rằng truyền thông là từ sự tấn công đó.

Fig.9 là hình vẽ minh họa ví dụ về cấu hình của bộ phận phân tích 230, được tạo cấu hình bởi các khối bộ phận xử lý được cấu thành bao gồm bộ xử lý phân tích riêng 230a, bộ xử lý kết hợp sự kiện 230b, bộ xử lý phân tích tương quan 230c, và bộ xử lý phân tích gia tăng 230d.

Trong ví dụ được minh họa trên Fig.9, nhiều khối bộ phận xử lý 231 bao gồm khối truy vấn danh sách 231a, khối tập hợp sự kiện 231b, khối tập hợp trình tự sự kiện 231c, khối xác định kết hợp mẫu tấn công 231d, khối xác định vượt ngưỡng số trường hợp 231e, khối xác định thay đổi sự cố 231f, khối xác định tăng bộ phận tấn công 231g, khối xác định tốc độ tăng số trường hợp 231h, và khối xác định tăng địa chỉ IP đích 231i. Khối truy vấn danh sách 231a là khối bộ phận xử lý dùng để thực hiện các truy vấn danh sách. Khối tập hợp sự kiện 231b là khối bộ phận xử lý dùng để thực hiện sự tập hợp sự kiện. Khối tập hợp trình tự sự kiện 231c là khối bộ phận xử lý dùng để thực hiện sự tập hợp trình tự sự kiện. Khối xác định kết hợp mẫu tấn công 231d là khối bộ phận xử lý dùng để thực hiện xử lý xác định kết hợp mẫu tấn công. Khối xác định vượt ngưỡng số trường hợp 231e là khối bộ phận xử lý dùng để thực hiện sự xác định rằng số các trường hợp đã vượt quá ngưỡng. Khối xác định thay đổi sự cố 231f là khối bộ phận xử lý dùng để thực hiện sự xác định xem sự cố đã thay đổi hay chưa. Khối xác định tăng bộ phận tấn công 231g là khối bộ phận xử lý dùng để thực hiện xử lý để xác định rằng bộ phận tấn công tăng. Khối xác định tốc độ tăng số trường hợp 231h là khối bộ phận xử lý dùng để thực hiện sự xác định tốc độ tăng các trường hợp. Khối xác định tăng địa chỉ IP đích 231i là khối bộ phận xử lý dùng để thực hiện sự xác định xem các địa chỉ IP đích có tăng hay không. Sự kết hợp các khối bộ phận xử lý 231 tạo cấu hình mỗi bộ xử lý từ 230a đến 230d của bộ phận phân tích 230. Lưu ý là chỉ một phần của các khối bộ phận xử lý 231 mà tạo cấu hình bộ phận phân tích 230 được minh họa trên Fig.9. Ví dụ, các khối bộ phận xử lý 231, chẳng hạn như khối truy vấn danh sách 231a, thực hiện các truy vấn của danh sách truyền thông có vấn đề bởi bộ xử lý phân tích riêng 230a. Các khối bộ phận xử lý 231, chẳng hạn như khối tập hợp sự kiện 231b và khối tập hợp trình tự sự kiện 231c, thực hiện việc tạo các trình tự sự kiện và các ứng viên sự cố được phát hiện bởi bộ xử lý tập hợp sự kiện 230b. Các khối bộ phận xử lý 231, chẳng hạn như khối xác định kết hợp mẫu tấn công 231d và

khối xác định vượt ngưỡng số trường hợp 231e, thực hiện sự phân tích bởi bộ xử lý phân tích tương quan 230c. Các khối bộ phận xử lý 231, chẳng hạn như khối xác định thay đổi sự cố 231f, khối xác định tăng bộ phận tấn công 231g, khối xác định tốc độ tăng số trường hợp 231h, và khối xác định tăng địa chỉ IP đích 231i, thực hiện sự phân tích bởi bộ xử lý phân tích gia tăng 230d. Các ví dụ về các khối bộ phận xử lý 231 tạo cấu hình bộ xử lý phân tích riêng 230a, bộ xử lý tập hợp sự kiện 230b, bộ xử lý phân tích tương quan 230c, và bộ xử lý phân tích gia tăng 230d. Bộ xử lý phân tích riêng 230a, bộ xử lý tập hợp sự kiện 230b, bộ xử lý phân tích tương quan 230c, và bộ xử lý phân tích gia tăng 230d có thể được bố trí, và mỗi bộ xử lý có thể thực hiện quy trình xử lý song song hoặc không đồng bộ.

Các kết quả của xử lý phân tích riêng lẻ, xử lý tập hợp sự kiện, xử lý phân tích tương quan, và xử lý phân tích gia tăng được thực hiện bởi mỗi trong số các khối bộ phận xử lý 231 của bộ phận phân tích 230 có thể được lưu trữ tạm thời trong, chẳng hạn, bộ nhớ máy tính mà tạo cấu hình bộ phận phân tích 230. Các kết quả sau đó được gửi tới bộ phận phân tích phía dưới thủ công 240 cùng với các sự cố đích bộ phát hiện mà ở đó mỗi loại của xử lý phân tích được hoàn thành, và với các sự kiện không được lấy làm các đích tập hợp trong suốt thời gian xử lý phân tích riêng lẻ.

Các chức năng của bộ phận phân tích thủ công

Fig.10 là hình vẽ minh họa cấu hình chức năng của bộ phận phân tích thủ công 240 của hệ thống con giám sát 200.

Bộ phận phân tích thủ công 240, mà là bộ phận xử lý thứ tư, quản lý và lưu trữ các sự kiện, các trình tự sự kiện, và thông tin ứng viên sự cố được phát hiện thu được nhờ mỗi trong số xử lý nêu trên được thực hiện bởi bộ phận phát hiện 220 và bộ phận phân tích 230 trong thiết bị lưu trữ 241, cùng với các kết quả phân tích từ bộ phận phân tích 230. Ngoài ra, bộ phận phân tích thủ công 240 gửi các sự kiện, các trình tự sự kiện, thông tin ứng viên sự cố được phát hiện, và các kết quả phân tích từ bộ phận phân tích 230 được lưu trữ trong thiết bị lưu trữ 241 tới thiết bị đầu cuối 300 sử dụng bộ gửi và bộ thu 242 đáp lại yêu cầu từ thiết bị đầu cuối 300. Ngoài ra, bộ phận phân tích thủ công 240 thu được thông tin loại thiết bị đầu cuối 300 này từ bộ gửi và bộ thu 242, kết hợp thông tin được thu nhận với thông tin được lưu trữ, và quản lý thông tin được thu nhận.

Các truyền thông giữa các bộ phận xử lý hệ thống con giám sát

Hệ thống giám sát bảo vệ theo phương án sáng chế giám sát các truyền thông trong thiết bị đích giám sát 100, và phát hiện các truyền thông có vấn đề theo thời gian thực. Nghĩa là, hệ thống giám sát bảo vệ không phải là hệ thống mà phân tích các tệp nhật ký truyền thông được lưu trữ và tìm kiếm các truyền thông có vấn đề sau sự kiện. Do đó tốt hơn là truyền các tệp nhật ký giữa mỗi bộ phận xử lý trong hệ thống con giám sát 200, để phát hiện các truyền thông có vấn đề từ các nhật ký truyền thông, nhanh nhất có thể. Ví dụ, sự truyền thông không kết nối được thực hiện thay vì sử dụng sự truyền dạng kết nối chẳng hạn như giao thức điều khiển truyền vận (TCP-Transmission Control Protocol). Sự truyền thông không kết nối dựa vào JMS do đó được thực hiện theo phương án sáng chế.

Đối với các trường hợp mà ở đó sự truyền của các nhật ký truyền thông được thực hiện bởi sự truyền thông không kết nối, sự xác định xem mỗi truyền thông riêng lẻ giữa các bộ phận xử lý trong hệ thống con giám sát 200 đã được thực hiện một cách bình thường hay chưa không được thực hiện, không giống như các truyền thông dạng kết nối. Do đó thực tế là các truyền thông đã được thực hiện một cách bình thường không thể được xác nhận, ngay cả khi tệp nhật ký truyền thông làm đích xử lý bị mất trong suốt thời gian truyền thông giữa các bộ phận xử lý. Cần thiết phải sử dụng cơ cấu để phát hiện khi các truyền thông chưa được thực hiện một cách bình thường đối với các trường hợp mà ở đó tệp nhật ký truyền thông làm đích xử lý bị mất trong suốt thời gian xử lý bởi hệ thống con giám sát 200.

Fig.11 là hình vẽ dùng để giải thích phương pháp chuyển tệp nhật ký truyền thông theo phương án sáng chế.

Fig.11 minh họa các ví dụ của các bộ phận xử lý mà tạo cấu hình hệ thống con giám sát 200 (ví dụ tạo cấu hình hệ thống con giám sát 200 bởi bộ phận thu thập 210, bộ phận phát hiện 220, bộ phận phân tích 230, và bộ phận phân tích thủ công 240). Theo phương án sáng chế, cấu hình dùng để cung cấp sự phản hồi tới bộ phận xử lý đầu tiên được ứng dụng trong bộ phận xử lý ví dụ được minh họa trên Fig.11. Cấu hình phản hồi xác nhận rằng sự truyền của các nhật ký truyền thông từ bộ phận xử lý đầu tiên (bộ phận thu thập 210) tới bộ phận xử lý cuối cùng (bộ phận phân tích thủ công 240) đã xảy ra bình thường.

Nghĩa là, bộ phận phân tích thủ công 240, mà là bộ phận xử lý cuối cùng của hệ thống con giám sát 200, thu thông tin sự kiện hoặc ứng viên sự cố được phát hiện từ bộ phận phân tích 230, thông báo bộ phận thu thập 210, mà là bộ phận xử lý đầu tiên, rằng nhật ký truyền thông mà tạo cấu hình thông tin sự kiện hoặc ứng viên sự cố được phát hiện đã được thu. Bộ phận thu thập đầu tiên 210 nhờ đó xác nhận rằng tệp nhật ký truyền thông làm đích xử lý đã tới bộ phận xử lý cuối cùng (bộ phận phân tích thủ công 240), thông qua mỗi trong số các bộ phận xử lý, mà không bị mất. Sau khi gửi tệp nhật ký truyền thông tới bộ phận phát hiện 220, mà là bộ phận phía dưới, bộ phận thu thập 210 gửi lại cùng tệp nhật ký truyền thông ở các thời điểm cố định, ví dụ, đến khi điều kiện dừng việc gửi lại định trước được thỏa mãn.

Ví dụ về điều kiện dừng việc gửi lại có thể là sự thu nhận từ bộ phận phân tích thủ công 240 thông báo thể hiện rằng tệp nhật ký truyền thông đã được thu nhận trong thời gian cố định từ thời gian gửi trước. Đối với các trường hợp mà ở đó điều kiện dừng việc gửi lại được thiết đặt và tệp nhật ký truyền thông làm đích xử lý bị mất do một số lý do và không tới bộ phận phân tích thủ công 240, thông báo từ bộ phận phân tích thủ công 240 đến bộ phận thu thập 210 không được thực hiện (điều kiện dừng việc gửi lại không được thỏa mãn). Do đó tệp nhật ký truyền thông giống nhau được gửi lại từ bộ phận thu thập 210 sau khi khoảng thời gian cố định đã trôi qua.

Điều kiện mà ở đó cùng tệp nhật ký truyền thông được gửi với số lần định trước có thể cũng được thiết đặt như ví dụ khác về điều kiện dừng việc gửi lại. Ngoài ra, lượng thời gian định trước trôi qua từ sự truyền thứ nhất có thể cũng được thiết đặt làm điều kiện dừng việc gửi lại khác nữa. Do đó bằng cách thiết đặt điều kiện dừng việc gửi lại, lỗi xảy ra tại hệ thống con giám sát 200 có thể được xác định mà không có sự tổn hại do các đặc tính truyền không kết nối đối với các trường hợp mà ở đó tệp nhật ký truyền thông không được truyền bình thường khi việc truyền được lặp lại với số lần định trước. Trong trường hợp này người vận hành hệ thống được thông báo rằng việc gửi lại tệp truyền thông đã dừng, và lỗi tại hệ thống con giám sát 200 đã xảy ra. Lưu ý là việc đếm số lần mà cùng tệp truyền thông đã được gửi có thể đạt được bằng cách đếm số lần bộ phận thu thập 210 gửi tệp nhật ký truyền thông, ví dụ, và lưu trữ số lần được đếm.

Với phương pháp truyền được tạo cấu hình như được nêu trên, thực tế là tệp nhật ký truyền thông đã bị mất tại một vài giai đoạn trong suốt thời gian truyền tệp nhật ký truyền thông giữa mỗi bộ phận xử lý có thể được hiểu đối với các trường hợp mà ở đó tệp nhật ký truyền thông làm đích xử lý không tới bộ phận phân tích thủ công 240. Mặt khác, sự nhận dạng mà ở đó tệp nhật ký truyền thông bị mất là không khả thi. Tuy nhiên, theo phương án sáng chế xử lý (phân tích) trên tệp nhật ký truyền thông không được hoàn thành nếu tệp nhật ký truyền thông không tới bộ phận phân tích thủ công 240. Bộ phận phân tích thủ công 240, mà được định vị tại vị trí cuối của trình tự bộ phận xử lý của hệ thống con giám sát 200, được chọn làm vị trí tìm kiếm.

Với phương pháp truyền nêu trên, tệp nhật ký truyền thông được truyền lại từ bộ phận thu thập đầu tiên 210 tới bộ phận phân tích thủ công 240 cuối cùng, ngay cả khi tệp truyền thông bị mất ở đâu đó giữa các bộ phận xử lý trong suốt thời gian truyền tệp truyền thông. Do đó, nếu tệp nhật ký truyền thông bị mất giữa bộ phận phân tích 230 và bộ phận phân tích thủ công 240, ví dụ, cùng tệp nhật ký truyền thông được truyền lại ngay cả thông qua xử lý được thực hiện bởi bộ phận phát hiện 220 và bộ phận phân tích 230 tới tệp nhật ký truyền thông đã hoàn thành.

Tuy nhiên, với phương án sáng chế, nếu tệp nhật ký truyền thông không tới bộ phận phân tích thủ công 240, các kết quả xử lý từ mỗi trong số các bộ phận xử lý không được lưu trữ trong thiết bị lưu trữ 241 của bộ phận phân tích thủ công 240, và các kết quả bị mất cùng với tệp nhật ký truyền thông. Mỗi trong số các bộ phận xử lý do đó thực hiện xử lý của tệp nhật ký truyền thông được gửi lại, mà không quan tâm đến việc xem xử lý đã được thực hiện khi tệp nhật ký truyền thông được gửi trước đó hay không.

Fig.12 là hình vẽ minh họa ví dụ về truyền tệp nhật ký truyền thông theo phương án sáng chế.

Trên Fig.12, "×" biểu thị rằng tệp nhật ký truyền thông đã bị mất, trong khi "○" biểu thị rằng tệp nhật ký truyền thông đã tới bộ phận phân tích thủ công 240. Mũi tên Ta1 chỉ báo đang được gửi lần thứ nhất, mũi tên Ta2 chỉ báo đang được gửi lần thứ hai, và mũi tên Ta3 chỉ báo đang được gửi lần thứ ba.

Ở ví dụ được minh họa trên Fig.12, khi được gửi lần thứ nhất, tệp nhật ký truyền thông nhất định được gửi từ bộ phận thu thập 210 tới bộ phận phát

hiện 220. Sau khi xử lý bởi bộ phận phát hiện 220, tệp nhật ký truyền thông được gửi từ bộ phận phát hiện 220 tới bộ phận phân tích 230. Tệp nhật ký truyền thông không tới bộ phận phân tích, và bị mất (xem mũi tên Ta1). Trong trường hợp này bộ phận phân tích thủ công 240 không thông báo bộ phận thu thập 210 rằng tệp nhật ký truyền thông đã được thu nhận. Bộ phận thu thập 210 do đó gửi lại tệp nhật ký truyền thông. Nghĩa là, bộ phận thu thập 210 gửi tệp nhật ký truyền thông lần thứ hai.

Các kết quả xử lý từ bộ phận phát hiện 220 được thực hiện trên tệp nhật ký truyền thông khi được gửi lần thứ nhất bị mất, cùng với tệp nhật ký truyền thông được gửi đầu tiên. Do đó bộ phận phát hiện 220 thực hiện xử lý trên tệp nhật ký truyền thông được gửi lại.

Ở ví dụ được minh họa trên Fig.12, khi được gửi lần thứ hai, tệp nhật ký truyền thông được gửi từ bộ phận phân tích 230 tới bộ phận phân tích thủ công 240 sau khi trải qua xử lý bởi bộ phận phân tích 230. Tệp nhật ký truyền thông bị mất và không tới bộ phận phân tích thủ công 240 (xem mũi tên Ta2). Cũng trong trường hợp này, bộ phận phân tích thủ công 240 không thông báo bộ phận thu thập 210 rằng tệp nhật ký truyền thông đã được thu nhận. Bộ phận thu thập 210 do đó gửi lại tệp nhật ký truyền thông. Nghĩa là, bộ phận thu thập 210 gửi tệp nhật ký truyền thông lần thứ ba.

Các kết quả xử lý từ bộ phận phân tích 230 được thực hiện trên tệp nhật ký truyền thông khi được gửi lần thứ hai bị mất, cùng với tệp nhật ký truyền thông được gửi lần thứ hai. Bộ phận phát hiện 220 và bộ phận phân tích 230 do đó thực hiện quy trình xử lý trên tệp nhật ký truyền thông được gửi lại.

Ở ví dụ được minh họa trên Fig.12, khi được gửi lần thứ ba, tệp nhật ký truyền thông tới bộ phận phân tích thủ công 240, và được lưu trữ trong thiết bị lưu trữ 241 (xem mũi tên Ta3). Bộ phận phân tích thủ công 240 sau đó thông báo bộ phận thu thập 2 rằng tệp nhật ký truyền thông đã tới. Do đó việc gửi lại tệp nhật ký truyền thông được dừng lại.

Khi sử dụng phương pháp truyền như nêu trên, tệp nhật ký truyền thông có thể được gửi lại ngay cả khi nó không bị mất. Cụ thể là, có thể có các lần mà ở đó xử lý bởi các bộ phận xử lý trung gian yêu cầu lượng thời gian nhất định, và trước khi thông báo từ bộ phận phân tích thủ công 240 được thực hiện, thời gian chờ cho bộ phận thu thập 210 gửi lại tệp nhật ký truyền thông có thể trôi

qua. Trong trường hợp này, có khả năng là cùng tệp nhật ký truyền thông (ứng viên sự cố được phát hiện) và các kết quả xử lý của nó tới bộ phận phân tích thủ công 240 nhiều lần, và được lưu trữ trong thiết bị lưu trữ 241. Đối với các trường hợp này, tệp nhật ký truyền thông và các kết quả xử lý của nó được gửi sau cùng từ bộ phận thu thập 210 được sử dụng làm dữ liệu hợp lệ. Lưu ý là dữ liệu hợp lệ giới hạn được gửi tới thiết bị đầu cuối 300 và được hiển thị trên màn hình 330 (xem Fig.15), được bàn luận dưới đây.

Fig.13 là hình vẽ minh họa ví dụ khác về truyền tệp nhật ký truyền thông theo phương án sáng chế.

Trên Fig.13, "×" biểu thị rằng tệp nhật ký truyền thông đã bị mất, trong khi "○" biểu thị rằng tệp nhật ký truyền thông đã tới bộ phận phân tích thủ công 240. Mũi tên Tb1 chỉ báo đang được gửi lần thứ nhất, mũi tên Tb2 chỉ báo đang được gửi lần thứ hai, và mũi tên Tb3 chỉ báo đang được gửi lần thứ ba. Trong ví dụ được minh họa trên Fig.13, tệp nhật ký truyền thông được gửi lần thứ hai tới bộ phận phân tích 230 sau khi tệp nhật ký truyền thông được gửi lần thứ ba tới bộ phận phân tích 230, như được bàn luận dưới đây.

Trong ví dụ được minh họa trên Fig.13, khi được gửi lần thứ nhất, tệp nhật ký truyền thông không tới bộ phận phân tích 230 sau khi xử lý bởi bộ phận phát hiện 220, và bị mất (xem mũi tên Tb1). Khi được gửi lần thứ hai, tệp nhật ký truyền thông tới bộ phận phân tích thủ công 240 mà không bị mất (xem mũi tên Tb2). Tuy nhiên, thời gian được yêu cầu cho xử lý trung gian trong suốt thời gian tệp nhật ký truyền thông được gửi lần thứ hai. Do đó, trước khi thông báo của bộ phận thu thập 210 được thực hiện bởi bộ phận phân tích thủ công 240, tệp nhật ký truyền thông được gửi lần thứ ba (xem mũi tên Tb3). Ngoài ra, thời gian được yêu cầu để xử lý tệp nhật ký truyền thông liên quan đến việc được gửi lần thứ hai. Do đó, tệp nhật ký truyền thông được gửi lần thứ ba tới bộ phận phân tích thủ công 240 trước khi tệp nhật ký truyền thông được gửi lần thứ hai. Trong trường hợp này, các kết quả xử lý của tệp nhật ký truyền thông được gửi lần thứ ba (lần cuối cùng) được sử dụng làm dữ liệu hợp lệ, mà không quan tâm đến thứ tự mà ở đó các kết quả tới bộ phận phân tích thủ công 240.

Lưu ý rằng, đối với các trường hợp như nêu trên, dữ liệu lặp lại liên quan đến cùng tệp nhật ký truyền thông có thể tới bộ phận phân tích thủ công 240 và được lưu trữ trong thiết bị lưu trữ 241. Dữ liệu không phải là dữ liệu hợp lệ

(trong ví dụ được minh họa trên Fig.13, dữ liệu hợp lệ mà liên quan đến tệp nhật ký truyền thông được gửi lần thứ hai) có thể được xóa, hoặc được lưu trữ trong thiết bị lưu trữ 241.

Fig.14 là hình vẽ minh họa ví dụ khác nữa về truyền tệp nhật ký truyền thông theo phương án sáng chế.

Trên Fig.14, "×" biểu thị rằng tệp nhật ký truyền thông đã bị mất, trong khi "○" biểu thị rằng tệp nhật ký truyền thông đã tới bộ phận phân tích thủ công 240. Mũi tên Tc1 chỉ báo đang được gửi lần thứ nhất, mũi tên Tc2 chỉ báo đang được gửi lần thứ hai, và mũi tên Tc3 chỉ báo đang được gửi lần thứ ba.

Với ví dụ được minh họa trên Fig.13, có các lần khi tệp nhật ký truyền thông được gửi lại trước khi tệp nhật ký truyền thông được gửi trước đó tới bộ phận phân tích thủ công 240. Trong các trường hợp chẳng hạn như các trường hợp đó, tệp nhật ký truyền thông được gửi sau có thể bị mất trên đường truyền. Trong ví dụ được minh họa trên Fig.14, tệp nhật ký truyền thông được gửi lại (được gửi cho lần thứ ba) trước khi cùng tệp nhật ký truyền thông được gửi cho lần thứ hai tới bộ phận phân tích thủ công 240. Tuy nhiên, tệp nhật ký truyền thông được gửi cho lần thứ ba bị mất và không tới bộ phận phân tích thủ công 240. Trong trường hợp này, chỉ tệp nhật ký truyền thông được gửi cho lần thứ hai tới bộ phận phân tích thủ công 240 và được lưu trữ trong thiết bị lưu trữ 241. Dữ liệu liên quan đến tệp nhật ký truyền thông được gửi cho lần thứ hai do đó được sử dụng làm dữ liệu hợp lệ.

Lưu ý là các thao tác được thực hiện bởi các bộ phận xử lý nêu trên chỉ là các ví dụ về các thao tác được thực hiện trên tệp nhật ký truyền thông được gửi lại. Không có sự giới hạn nào về các thao tác mà có thể được thực hiện trên tệp nhật ký truyền thông. Ví dụ, theo phương án sáng chế các kết quả xử lý từ mỗi bộ phận xử lý được lưu trữ tạm thời trong bộ nhớ máy tính mà tạo cấu hình mỗi bộ phận xử lý. Tuy nhiên, phương án sáng chế không giới hạn ở loại cấu hình này. Cấu hình có thể cũng được ứng dụng mà ở đó các kết quả xử lý từ mỗi bộ xử lý mà được phân tách được lưu trữ trên cơ sở dữ liệu và từ đó được quản lý là ví dụ riêng lẻ về phương án theo sáng chế. Trong trường hợp này các kết quả xử lý duy trì trên cơ sở dữ liệu đối với xử lý đã hoàn thành, ngay cả khi tệp nhật ký truyền thông bị mất trong khi đang được chuyển giữa các bộ phận xử lý. Trong trường hợp này, nếu bộ phận xử lý thực hiện xử lý kép trên tệp nhật ký

truyền thông được gửi lại, thì độ chính xác dùng để phát hiện các truyền thông có vấn đề bị ảnh hưởng. Các kết quả xử lý kép được cho phép duy trì là cần thiết.

Khi tệp nhật ký truyền thông được gửi lại là tệp mà đã được xử lý trong bộ phận xử lý nhất định, thông tin về các kết quả xử lý hiện có có thể được trao đổi với thông tin về các kết quả xử lý hiện thời là một ví dụ. Nghĩa là, các kết quả xử lý trước đó liên quan đến tệp nhật ký truyền thông được loại bỏ. Ngoài ra, khi tệp nhật ký truyền thông được gửi lại là tệp mà đã được xử lý trong bộ phận xử lý nhất định, sự xử lý của cùng tệp nhật ký truyền thông khi được gửi lại có thể được bỏ qua, và tệp nhật ký truyền thông được gửi tới bộ phận xử lý phía dưới là ví dụ riêng lẻ.

Dữ liệu cờ hoặc tương tự mà thể hiện tệp nhật ký truyền thông đang được gửi lại có thể cũng được bổ sung tới tệp nhật ký truyền thông làm thông tin dùng để phân biệt các truyền thông được gửi lần thứ nhất và các truyền thông mà được gửi lại. Thông tin chỉ báo số lần tệp nhật ký truyền thông đã được gửi lại có thể cũng được bổ sung. Nếu thông tin được bổ sung chỉ báo số lần tệp nhật ký truyền thông đã được gửi được bao gồm cùng với thông báo khi được gửi từ bộ phận phân tích thủ công 240 đến bộ phận thu thập 210, thì số lần mà cùng tệp nhật ký truyền thông đã được gửi có thể được xác nhận dựa vào thông báo từ bộ phận phân tích thủ công 240, mà không đếm số lần mà cùng tệp nhật ký truyền thông đã được gửi bởi bộ phận thu thập 210.

Các chức năng của thiết bị đầu cuối

Fig.15 là hình vẽ minh họa ví dụ về cấu hình chức năng của thiết bị đầu cuối 300.

Trong ví dụ được minh họa trên Fig.15, thiết bị đầu cuối 300 bao gồm bộ gửi và bộ thu 310, và bộ xử lý dữ liệu 320. Ngoài ra, thiết bị đầu cuối 300 bao gồm màn hình 330 được làm từ màn hình tinh thể lỏng hoặc tương tự, và phần thao tác 340 được tạo ra bằng cách sử dụng thiết bị đầu vào chẳng hạn như bàn phím, chuột, hoặc tương tự.

Bộ gửi và bộ thu 310 là giao diện dùng để thực hiện sự truyền thông giữa chúng với bộ phận phân tích thủ công 240 của hệ thống con giám sát 200. Bộ gửi và bộ thu 310 thu sự kiện, trình tự sự kiện, và thông tin ứng viên sự cố được

phát hiện từ bộ phận phân tích thủ công 240. Thông tin thu được bởi xử lý được thực hiện bởi bộ phận phát hiện 220 và bộ phận phân tích 230. Bộ gửi và bộ thu 310 cũng thu các kết quả của phân tích được thực hiện bởi bộ phận phân tích 230. Ngoài ra, bộ gửi và bộ thu 310 gửi thông tin mà được nhập bởi các thao tác trên phần thao tác 340 tới bộ phận phân tích thủ công 240 của hệ thống con giám sát 200. Ngoài ra, khi truyền thông có vấn đề được phát hiện như kết quả phân tích của các truyền thông thiết bị đích giám sát 100, bộ gửi và bộ thu 310 gửi thông tin chỉ báo rằng truyền thông có vấn đề đã được phát hiện tới thiết bị đầu cuối (không được thể hiện) được thao tác bởi người thao tác thiết bị đích giám sát 100.

Bộ xử lý dữ liệu 320 tạo màn hình phân tích dựa vào sự kiện, trình tự sự kiện, và thông tin ứng viên sự cố được phát hiện được thu nhận bởi bộ gửi và bộ thu 310 từ bộ phận phân tích thủ công 240 của hệ thống con giám sát 200, và các kết quả phân tích từ bộ phận phân tích 230. Ngoài ra, bộ xử lý dữ liệu 320 hiển thị màn hình phân tích được tạo ra trên màn hình 330.

Fig.16 là hình vẽ minh họa ví dụ về cấu hình của màn hình phân tích theo phương án sáng chế.

Trong ví dụ được minh họa trên Fig.16, màn hình phân tích được hiển thị trên màn hình 330 được tạo cấu hình bởi sáu vùng hiển thị: vùng hiển thị điều kiện tìm kiếm 331, vùng hiển thị ứng viên sự cố được phát hiện 332, vùng hiển thị trình tự sự kiện 333, vùng hiển thị sự kiện 334, vùng hiển thị chú thích 335, và vùng hiển thị mức độ quan trọng 336.

Các ứng viên sự cố được phát hiện và tương tự được hiển thị trong vùng hiển thị ứng viên sự cố được phát hiện 332. Các điều kiện tìm kiếm của nó được hiển thị trong vùng hiển thị điều kiện tìm kiếm 331. Các điều kiện tìm kiếm có thể được thiết đặt ban đầu, ví dụ, là các điều kiện bất kỳ. Ngoài ra, các điều kiện tìm kiếm có thể cũng được thiết đặt bởi người phân tích mà nhập các điều kiện tìm kiếm mong muốn nhờ việc thao tác phần thao tác 340. Lưu ý là các ứng viên sự cố được phát hiện có một trình tự sự kiện hoặc chỉ có một sự kiện cũng được bao gồm làm các ứng viên sự cố được phát hiện mà trở thành các đích tìm kiếm. Ngoài ra, các sự kiện đơn được loại bỏ mà không thực hiện phân tích, dựa vào mối quan hệ điều kiện được tìm thấy bởi bộ xử lý phân tích riêng 230a của bộ

phận phân tích 230, có thể được thiết đặt làm các đích tìm kiếm. Cụ thể là, do các ứng viên sự cố được phát hiện được tạo ra từ một sự kiện.

Các ứng viên sự cố được phát hiện được tìm kiếm dưới các điều kiện tìm kiếm được hiển thị trong vùng hiển thị điều kiện tìm kiếm 331, và các kết quả xử lý của nó bởi bộ phận phân tích 230 của hệ thống con giám sát 200, được hiển thị trong vùng hiển thị ứng viên sự cố được phát hiện 332.

Các trình tự sự kiện được bao gồm trong các ứng viên sự cố được phát hiện được hiển thị trong vùng hiển thị ứng viên sự cố được phát hiện 332 (nghĩa là, các sự kiện được tìm kiếm dưới các điều kiện tìm kiếm được định rõ trong vùng hiển thị điều kiện tìm kiếm 331), và các kết quả xử lý của nó bởi bộ phận phân tích 230 của hệ thống con giám sát 200, được hiển thị trong vùng hiển thị trình tự sự kiện 333.

Các sự kiện được bao gồm trong các ứng viên sự cố được phát hiện được hiển thị trong vùng hiển thị ứng viên sự cố được phát hiện 332 (nghĩa là, các sự kiện được tìm kiếm dưới các điều kiện tìm kiếm được định rõ trong vùng hiển thị điều kiện tìm kiếm 331), và các kết quả xử lý của nó bởi bộ phận phân tích 230 của hệ thống con giám sát 200, được hiển thị trong vùng hiển thị sự kiện 334.

Các chú thích mà được nhập bởi người phân tích mà thao tác phần thao tác 340 được hiển thị trong vùng hiển thị chú thích 335. Cụ thể là, sự đánh giá phân tích hoặc chú thích khác liên quan đến, chẳng hạn, sự truyền thông của ba thiết bị đích giám sát 100 có thể được nhập.

Các mức đánh giá dùng để thực hiện sự đánh giá các ứng viên sự cố được phát hiện được hiển thị trong vùng hiển thị ứng viên sự cố được phát hiện 332 (nghĩa là, các sự kiện được tìm kiếm dưới các điều kiện tìm kiếm được định rõ trong vùng hiển thị điều kiện tìm kiếm 331) được hiển thị trong vùng hiển thị mức độ quan trọng 336. Giá trị đánh giá là giá trị quan trọng được phân mức trước tùy thuộc vào các hồi đáp cần thiết tới các truyền thông được định rõ bởi các ứng viên sự cố được phát hiện. Ví dụ, sự hồi đáp ngay lập tức có cần phải được đưa ra hay không, sự phát hiện và đánh giá liên tiếp của các truyền thông tương tự có cần thiết hay không, và tương tự. Vùng hiển thị mức độ quan trọng 336 trở thành giao diện đầu vào để thu sự lựa chọn mức độ quan trọng bởi người phân tích. Sự phân tích thực hiện sự đánh giá ứng viên sự cố được phát hiện

được tìm kiếm bằng cách chọn một mức quan trọng được hiển thị trong vùng hiển thị mức độ quan trọng 336.

Sự phân tích đánh giá (phân tích thủ công) các truyền thông của thiết bị đích giám sát 100 dựa vào các ứng viên sự cố được phát hiện, các trình tự sự kiện, và các sự kiện. Các ứng viên sự cố được phát hiện, các trình tự sự kiện, và các sự kiện được tìm kiếm dựa vào các điều kiện tìm kiếm ban đầu được hiển thị trong vùng hiển thị điều kiện tìm kiếm 331 của màn hình 330, hoặc dựa vào các điều kiện tìm kiếm mà được nhập bởi người phân tích mà thao tác phần thao tác 340. Khi truyền thông có vấn đề được phát hiện, người thao tác thao tác phần thao tác 340 để nhập chú thích và mức quan trọng tùy thuộc vào nội dung truyền thông (nội dung vấn đề). Người thao tác thiết bị đích giám sát 100 được thông báo nhờ bộ gửi và bộ thu 310.

Lưu ý là đối với các truyền thông được xác định là các truyền thông không được phép (chẳng hạn như các sự tấn công hoặc thông tin không được phép rò rỉ) bởi sự bố trí với danh sách trong bộ phận phân tích 230, và đối với các truyền thông được xác nhận là các truyền thông không được phép bởi người phân tích trong bộ phận phân tích 230, các truyền thông này có thể cũng là các đích thông báo cho người thao tác thiết bị đích giám sát 100. Sự đánh giá bởi người phân tích là không cần thiết.

Ví dụ cấu hình phần cứng

Fig.17 là hình vẽ minh họa ví dụ cấu hình phần cứng (máy tính) ứng dụng được dùng để tạo cấu hình mỗi bộ phận xử lý của hệ thống con giám sát 200 và thiết bị đầu cuối 300 theo phương án sáng chế.

Máy tính được minh họa trên Fig.17 bao gồm CPU (bộ phận xử lý trung tâm) 10a là bộ phận tính toán, và bộ nhớ 10c là bộ nhớ chính. Ngoài ra, máy tính được minh họa trên Fig.17 bao gồm thiết bị đĩa từ (ổ đĩa cứng, HDD) 10g, giao diện mạng 10f, cơ cấu hiển thị 10d chứa thiết bị màn hình, và thiết bị đầu vào 10i chẳng hạn như bàn phím, chuột, hoặc tương tự làm các thiết bị ngoại vi.

Trong ví dụ cấu hình được minh họa trên Fig.17, bộ nhớ 10c và cơ cấu hiển thị 10d được kết nối với CPU 10a nhờ bộ điều khiển hệ thống 10b. Ngoài ra, giao diện mạng 10f, thiết bị đĩa từ 10g, và thiết bị đầu vào 10k được kết nối với bộ điều khiển hệ thống 10b nhờ bộ điều khiển I/O 10e. Mỗi phần tử cấu thành

được kết nối bởi đường dẫn chẳng hạn như đường dẫn hệ thống, đường đầu tiên vào, hoặc tương tự.

Fig.17 chỉ là ví dụ minh họa về cấu hình phần cứng máy tính được ưu tiên dùng để ứng dụng phương án của sáng chế. Phương án sáng chế có thể được áp dụng rộng rãi cho các thiết bị xử lý thông tin có khả năng phát hiện các truyền thông không được phép hoặc các truyền thông có vấn đề bằng cách thu nhận và xử lý theo thời gian thực tệp nhật ký truyền thông từ thiết bị đích giám sát 100. Nghĩa là, các cấu hình để thực hiện phương án sáng chế không bị giới hạn ở cấu hình được minh họa trên Fig.17.

Chương trình OS (hệ điều hành- Operator System) và chương trình ứng dụng được lưu trữ trên thiết bị đĩa từ 10g trên Fig.17. Bằng cách đọc các chương trình trong bộ nhớ 10c và thực thi các chương trình trong CPU 10a, mỗi trong số các bộ phận xử lý từ 210 tới 240 của hệ thống con giám sát 200, và mỗi chức năng của thiết bị đầu cuối 300 theo phương án sáng chế, được thực hiện.

Khả năng ứng dụng trong công nghiệp

Sáng chế có thể được ứng dụng cho hệ thống phân tích nhật ký.

Danh mục số chỉ dẫn

100 Thiết bị đích giám sát

110 Thiết bị phát hiện

111 Cảm biến

112 Bộ quản lý cảm biến

120 Hệ thống con quản lý nhật ký

121 Tác nhân thu nhận nhật ký

200 Hệ thống con giám sát

210 Bộ phận thu thập

220 Bộ phận phát hiện

230 Bộ phận phân tích

240 Bộ phận phân tích thủ công

300 Thiết bị đầu cuối

YÊU CẦU BẢO HỘ

1. Hệ thống phân tích nhật ký được tạo cấu hình để phân tích các nhật ký phát hiện được phát hiện trong hệ thống đích giám sát, hệ thống phân tích nhật ký này bao gồm:

thiết bị thu nhận được tạo cấu hình để phát hiện các quy trình xử lý đích phát hiện được thực hiện trong hệ thống đích giám sát, và thu nhận các nhật ký phát hiện, mà ở đó các nhật ký phát hiện là các nhật ký được khởi tạo bởi các quy trình xử lý đích phát hiện; và

ít nhất một thiết bị xử lý được tạo cấu hình để xử lý các nhật ký phát hiện được thu nhận bởi thiết bị thu nhận,

trong đó ít nhất một thiết bị xử lý bao gồm các khối xử lý được tạo cấu hình để thực hiện quy trình xử lý của các nhật ký phát hiện theo thứ tự, các khối xử lý được tạo cấu hình để thực hiện quy trình xử lý trong khi gửi các nhật ký phát hiện theo thứ tự từ khối xử lý phía trên cùng tới các khối xử lý phía dưới của các khối xử lý;

trong đó khối xử lý phía dưới cùng của thiết bị xử lý được tạo cấu hình để thông báo cho khối xử lý phía trên cùng rằng khối xử lý phía trên này cùng thu được các nhật ký phát hiện, và

trong đó khối xử lý phía trên cùng gửi lại cho các khối xử lý phía dưới nhật ký phát hiện mà khối xử lý phía trên cùng được xác nhận rằng khối xử lý cuối cùng chưa thu được, dựa vào thông báo từ khối xử lý phía dưới cùng.

2. Hệ thống phân tích nhật ký theo điểm 1, trong đó khối xử lý phía trên cùng được tạo cấu hình để dừng việc gửi lại nhật ký phát hiện trong trường hợp mà sau khi đã gửi nhật ký phát hiện với số lần định trước, khối xử lý phía trên cùng được xác nhận rằng khối xử lý phía dưới cùng chưa thu được, dựa vào thông báo từ khối xử lý phía dưới cùng.

3. Hệ thống phân tích nhật ký theo điểm 1, trong đó khối xử lý phía trên cùng được tạo cấu hình để bổ sung vào nhật ký phát hiện thông tin nhận dạng để nhận dạng xem nhật ký phát hiện có cần được gửi lại hay không, trước khi gửi nhật ký phát hiện với thông tin nhận dạng tới các khối xử lý phía dưới.

4. Hệ thống phân tích nhật ký theo điểm 1, trong đó khối xử lý phía trên cùng được tạo cấu hình để bổ sung vào nhật ký phát hiện thông tin chỉ báo bao nhiêu

lần nhật ký phát hiện đã được gửi, trước khi gửi nhật ký phát hiện với thông tin tới các khối xử lý phía dưới.

FIG. 1

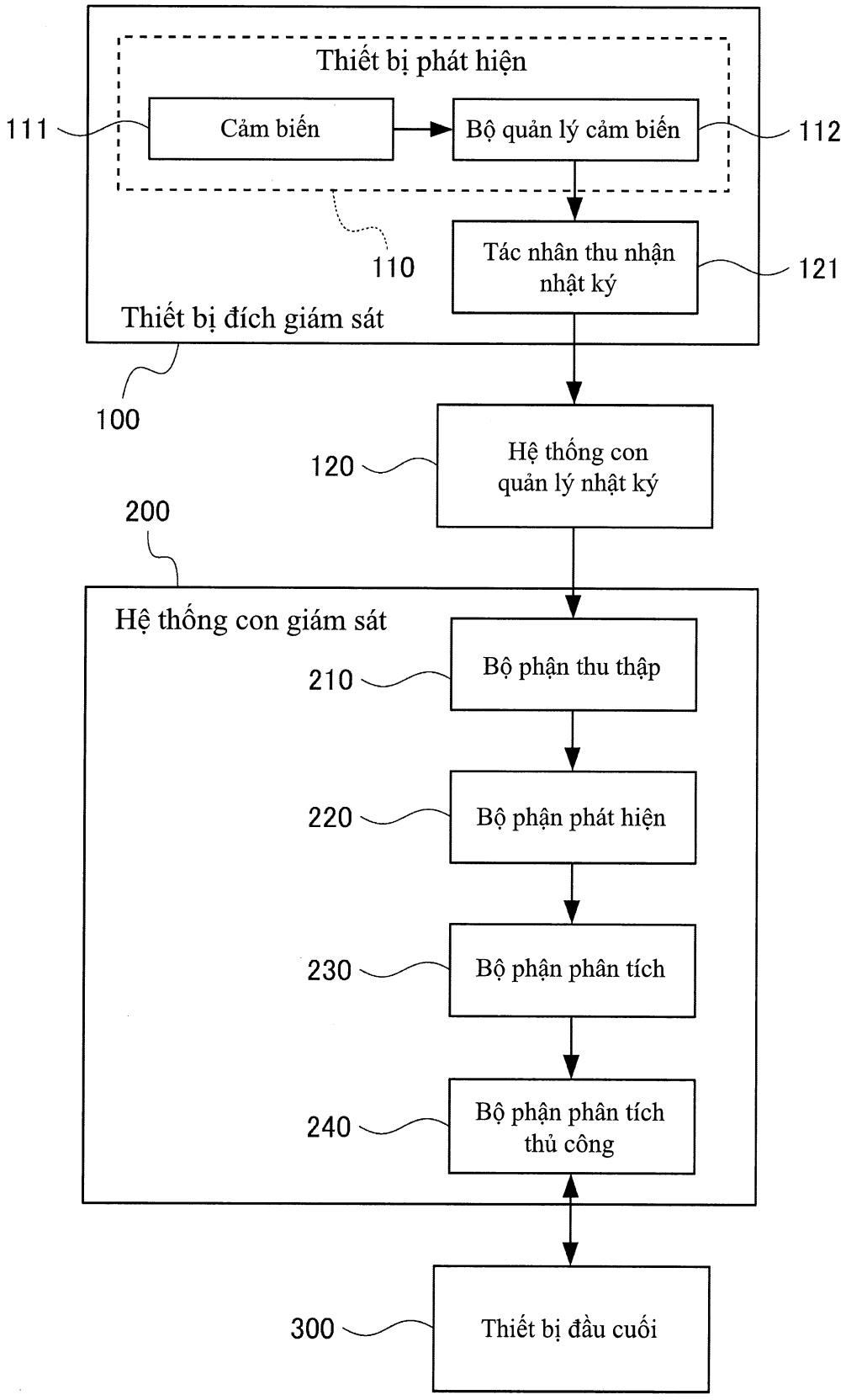

Thiết bị phát hiện
111
Cảm biến
Bộ quản lý cảm biến
112
110
Tác nhân thu nhận nhật ký
121
Thiết bị đích giám sát
100
120
Hệ thống con quản lý nhật ký
200
Hệ thống con giám sát
210
Bộ phận thu thập
220
Bộ phận phát hiện
230
Bộ phận phân tích
240
Bộ phận phân tích thủ công
300
Thiết bị đầu cuối

FIG. 2

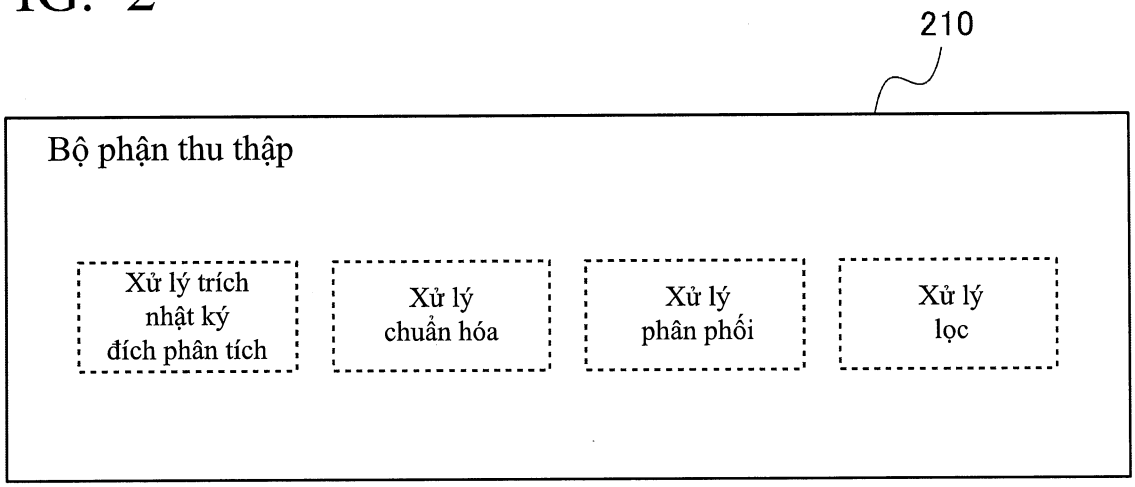

210
Bộ phận thu thập
Xử lý trích nhật ký đích phân tích
Xử lý chuẩn hóa
Xử lý phân phối
Xử lý lọc

FIG. 3

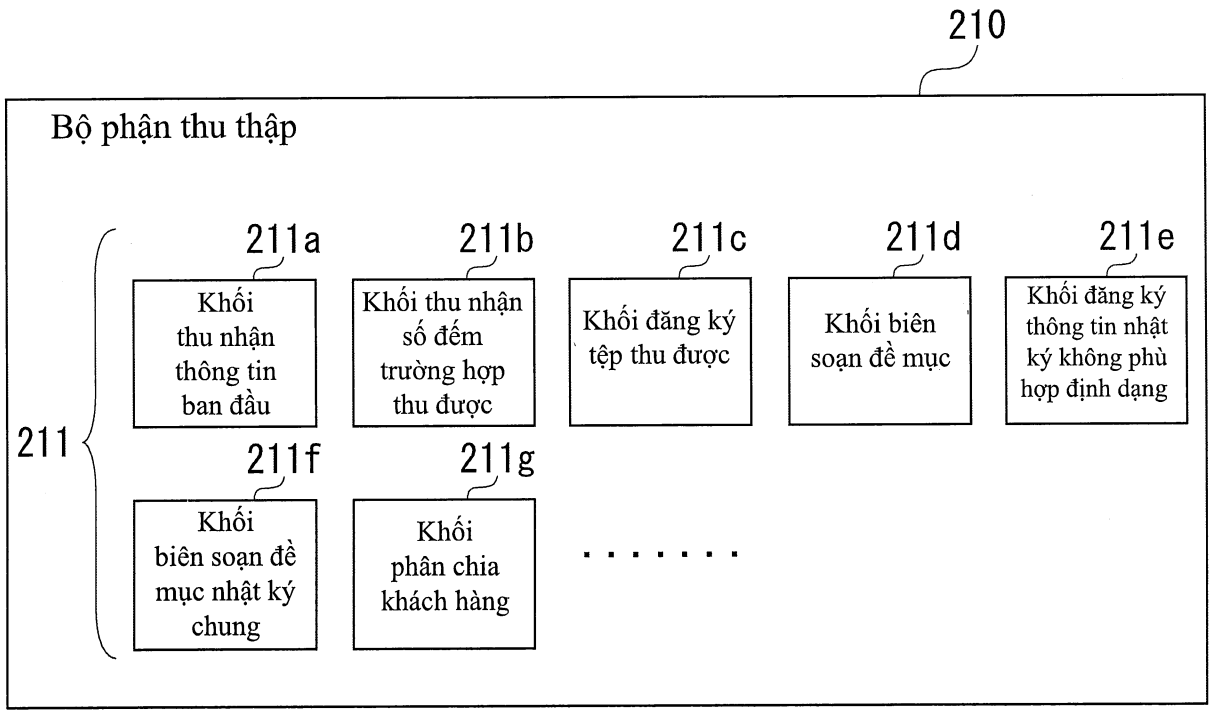

210
Bộ phận thu thập
211
211a
Khối thu nhận thông tin ban đầu
211b
Khối thu nhận số đếm trường hợp thu được
211c
Khối đăng ký tệp thu được
211d
Khối biên soạn đề mục
211e
Khối đăng ký thông tin nhật ký không phù hợp định dạng
211f
Khối biên soạn đề mục nhật ký chung
211g
Khối phân chia khách hàng
. . . . . .

FIG. 4

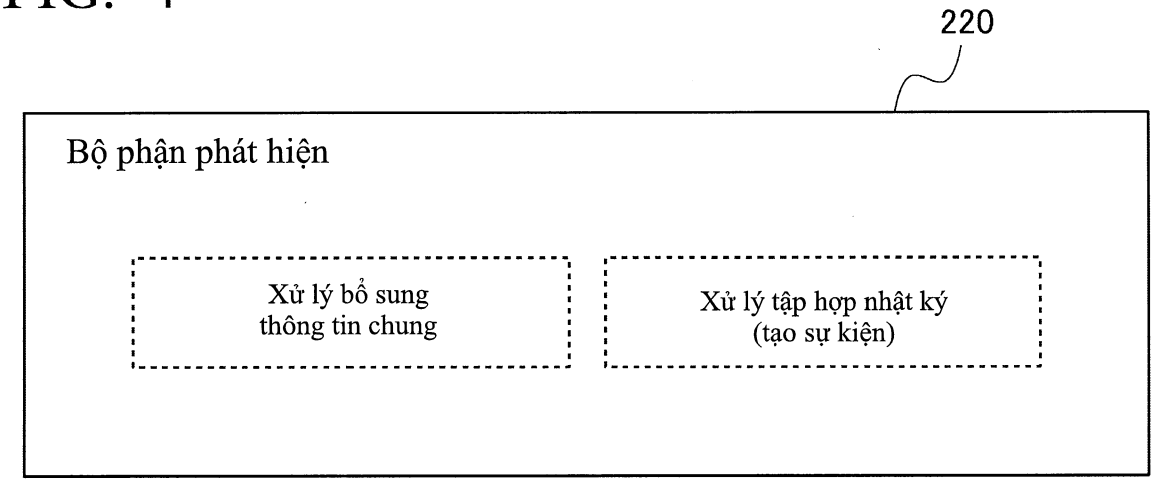

220
Bộ phận phát hiện
Xử lý bổ sung thông tin chung
Xử lý tập hợp nhật ký (tạo sự kiện)

FIG. 5

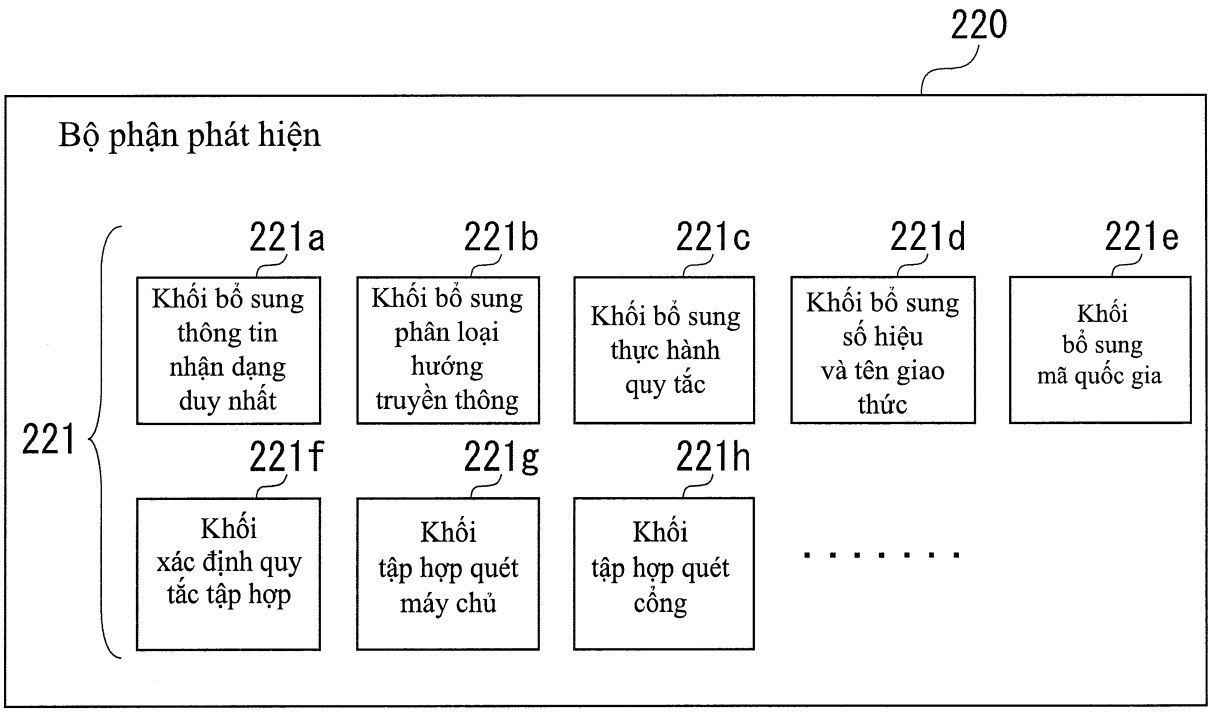

220
Bộ phận phát hiện
221
221a
Khối bổ sung thông tin nhận dạng duy nhất
221b
Khối bổ sung phân loại hướng truyền thông
221c
Khối bổ sung thực hành quy tắc
221d
Khối bổ sung số hiệu và tên giao thức
221e
Khối bổ sung mã quốc gia
221f
Khối xác định quy tắc tập hợp
221g
Khối tập hợp quét máy chủ
221h
Khối tập hợp quét cổng
. . . . . .

FIG. 6

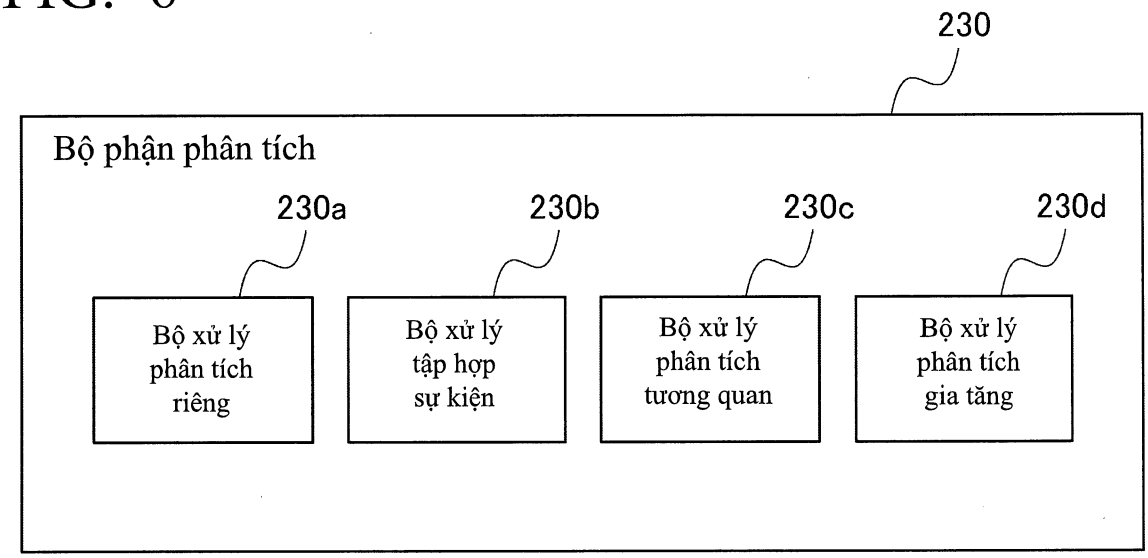

230
Bộ phận phân tích
230a
230b
230c
230d
Bộ xử lý phân tích riêng
Bộ xử lý tập hợp sự kiện
Bộ xử lý phân tích tương quan
Bộ xử lý phân tích gia tăng

FIG. 7

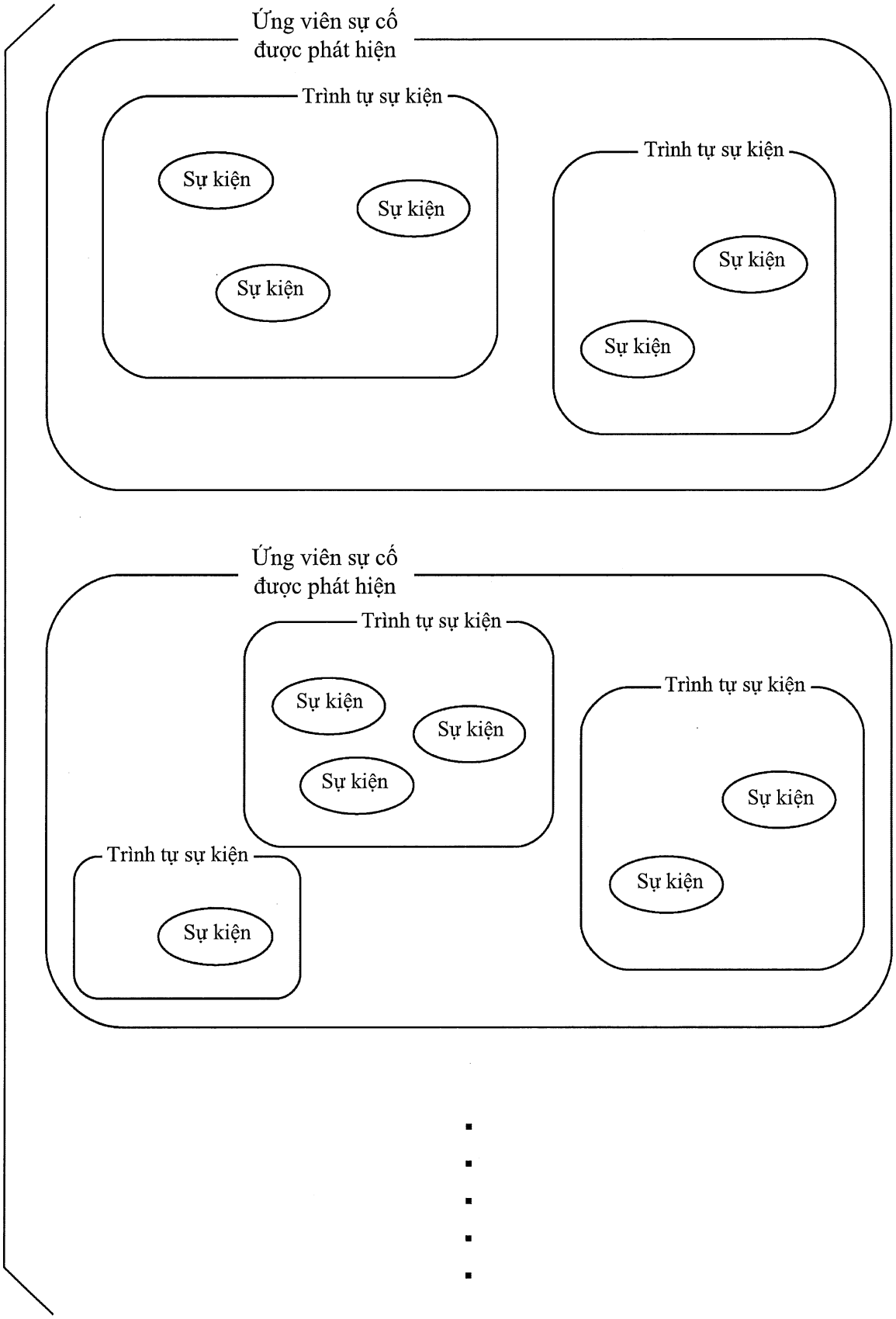

Ứng viên sự cố được phát hiện
Trình tự sự kiện
Sự kiện
Sự kiện
Sự kiện
Trình tự sự kiện
Sự kiện
Sự kiện
Ứng viên sự cố được phát hiện
Trình tự sự kiện
Sự kiện
Sự kiện
Sự kiện
Trình tự sự kiện
Sự kiện
Sự kiện
Trình tự sự kiện
Sự kiện

FIG. 8A

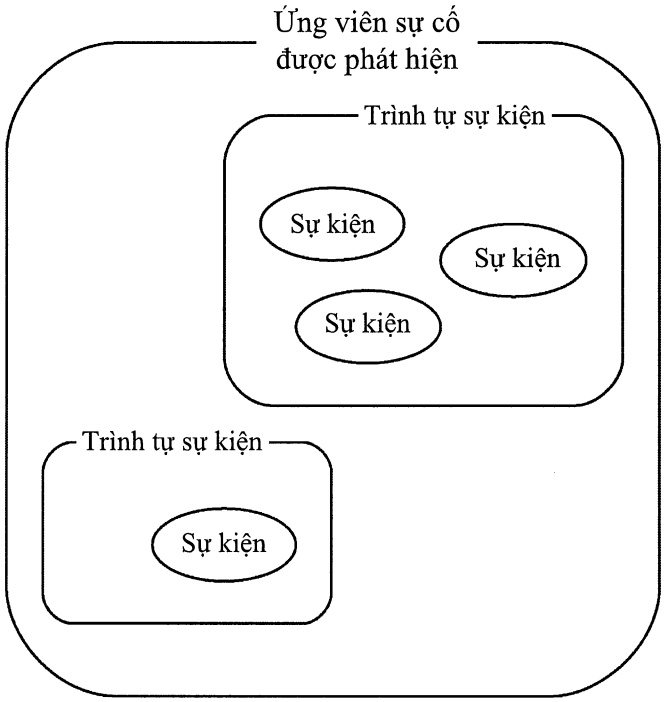

Ứng viên sự cố
được phát hiện
Trình tự sự kiện
Sự kiện
Sự kiện
Sự kiện
Trình tự sự kiện
Sự kiện

FIG. 8B

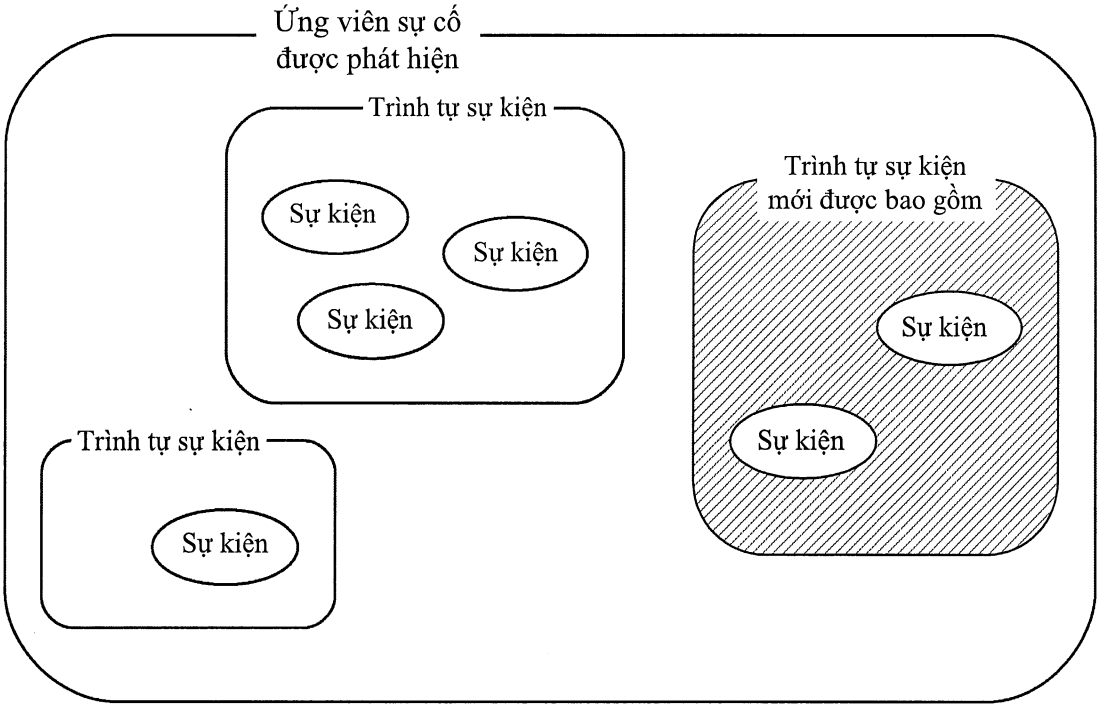

Ứng viên sự cố
được phát hiện
Trình tự sự kiện
Sự kiện
Sự kiện
Sự kiện
Trình tự sự kiện
mới được bao gồm
Sự kiện
Sự kiện
Trình tự sự kiện
Sự kiện

FIG. 9

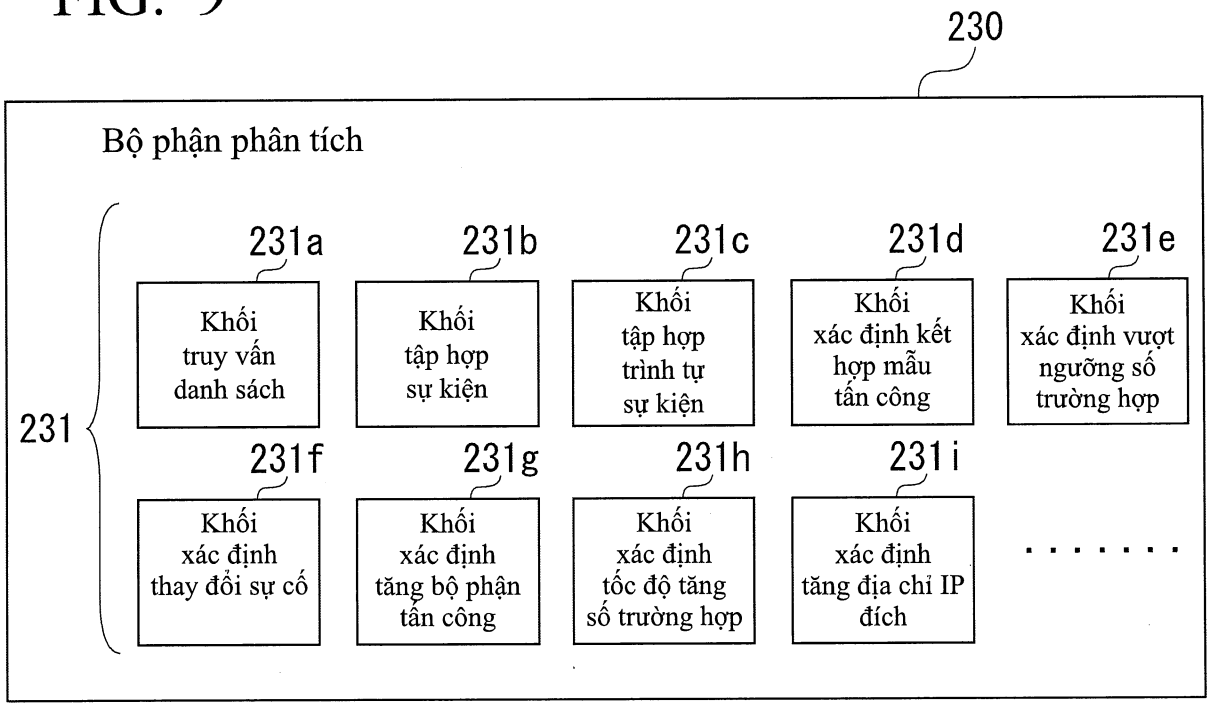

230
Bộ phận phân tích
231
231a
Khối truy vấn danh sách
231b
Khối tập hợp sự kiện
231c
Khối tập hợp trình tự sự kiện
231d
Khối xác định kết hợp mẫu tấn công
231e
Khối xác định vượt ngưỡng số trường hợp
231f
Khối xác định thay đổi sự cố
231g
Khối xác định tăng bộ phận tấn công
231h
Khối xác định tốc độ tăng số trường hợp
231i
Khối xác định tăng địa chỉ IP đích
. . . . . .

FIG. 10

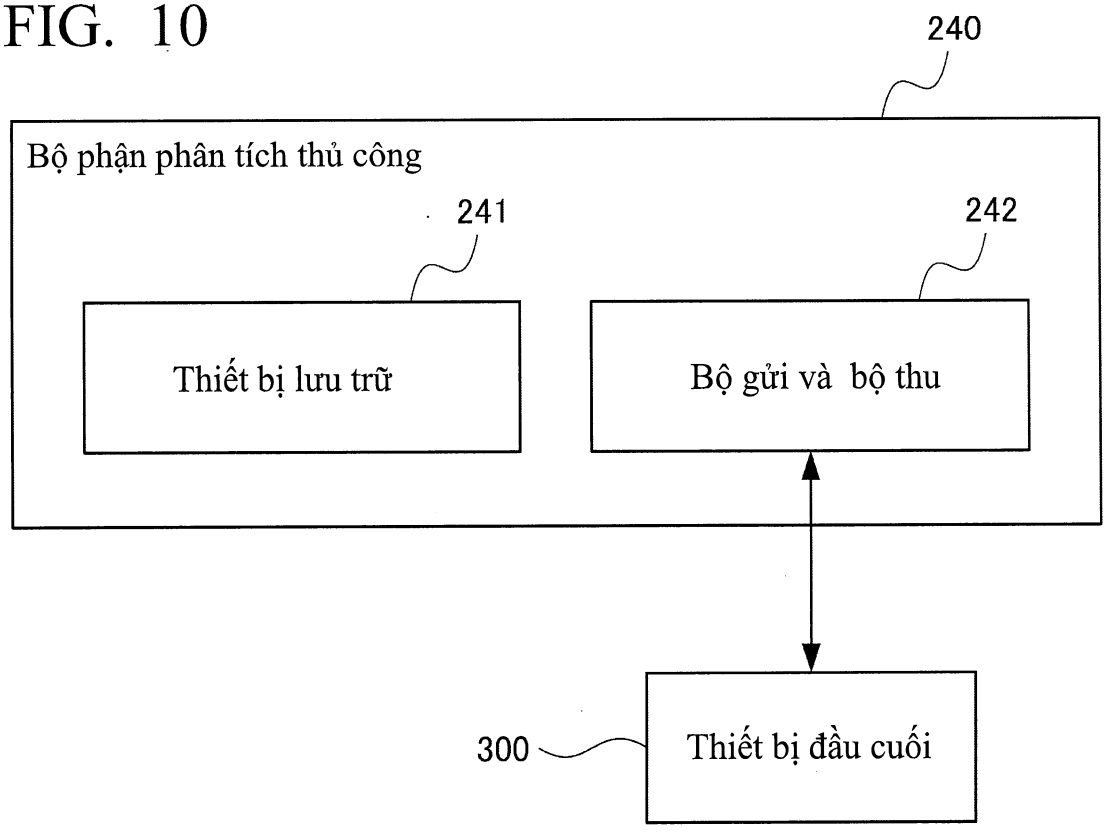

240
Bộ phận phân tích thủ công
241
Thiết bị lưu trữ
242
Bộ gửi và bộ thu
300
Thiết bị đầu cuối

FIG. 11

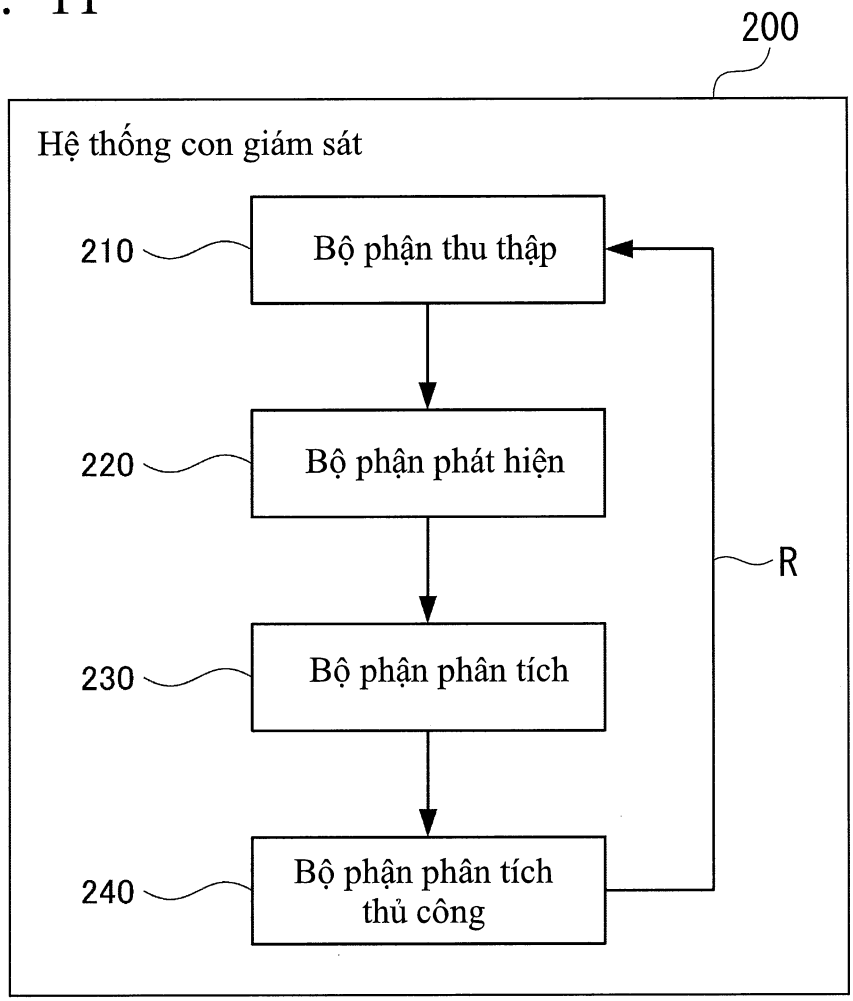

200
Hệ thống con giám sát
210
Bộ phận thu thập
220
Bộ phận phát hiện
230
Bộ phận phân tích
240
Bộ phận phân tích thủ công
R

FIG. 12

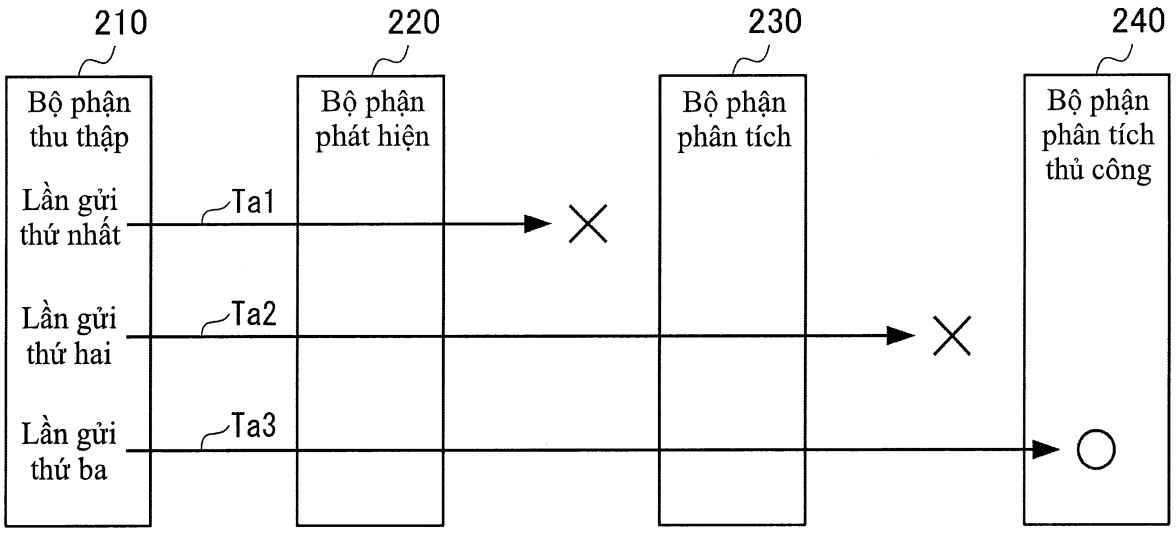

210
220
230
240
Bộ phận thu thập
Bộ phận phát hiện
Bộ phận phân tích
Bộ phận phân tích thủ công
Lần gửi thứ nhất
Ta1
Lần gửi thứ hai
Ta2
Lần gửi thứ ba
Ta3

FIG. 13

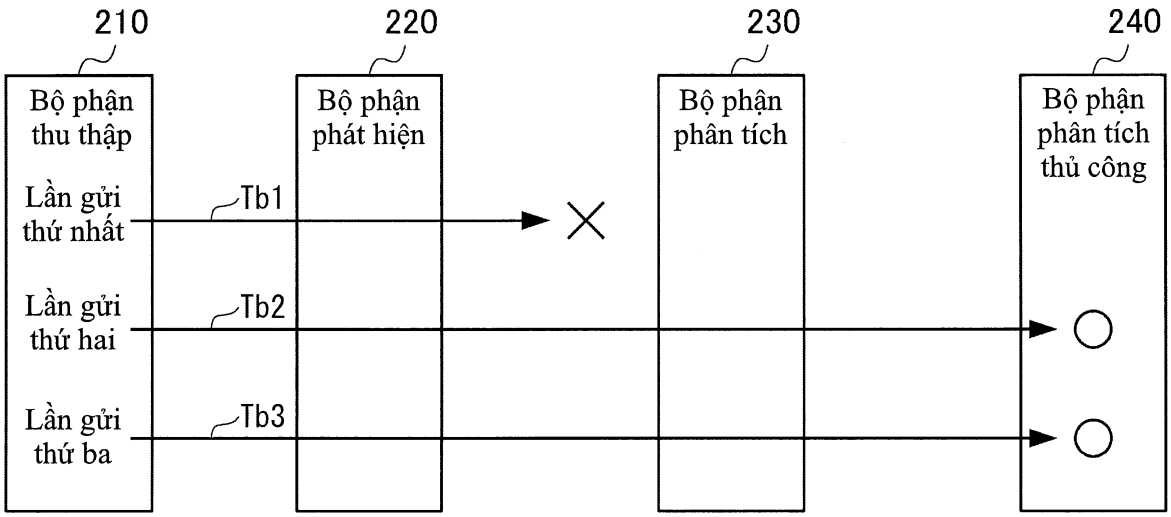

210
220
230
240
Bộ phận thu thập
Bộ phận phát hiện
Bộ phận phân tích
Bộ phận phân tích thủ công
Lần gửi thứ nhất
Lần gửi thứ hai
Lần gửi thứ ba
Tb1
Tb2
Tb3

FIG. 14

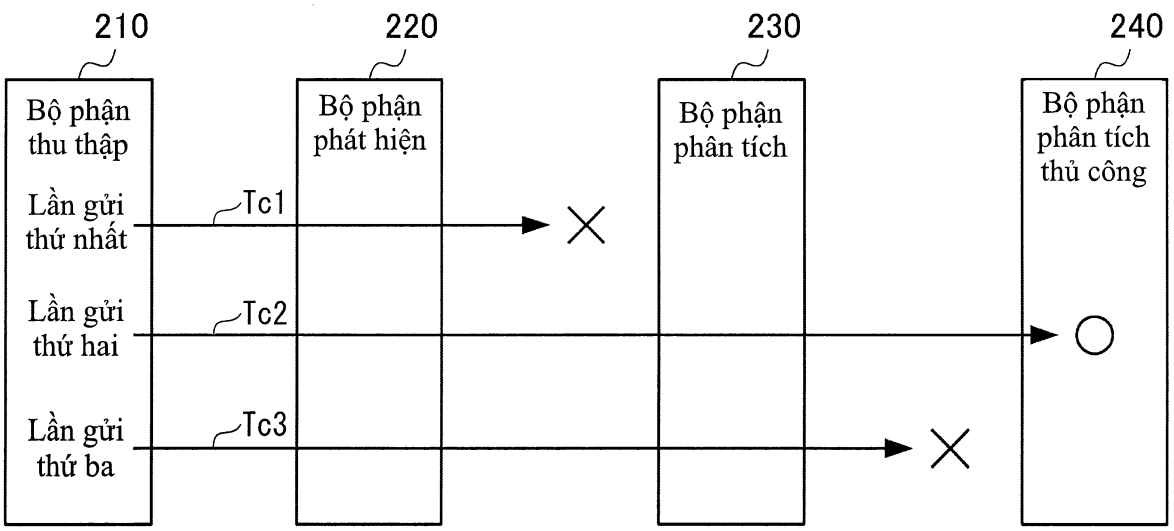

210
220
230
240
Bộ phận thu thập
Bộ phận phát hiện
Bộ phận phân tích
Bộ phận phân tích thủ công
Lần gửi thứ nhất
Lần gửi thứ hai
Lần gửi thứ ba
Tc1
Tc2
Tc3

FIG. 15

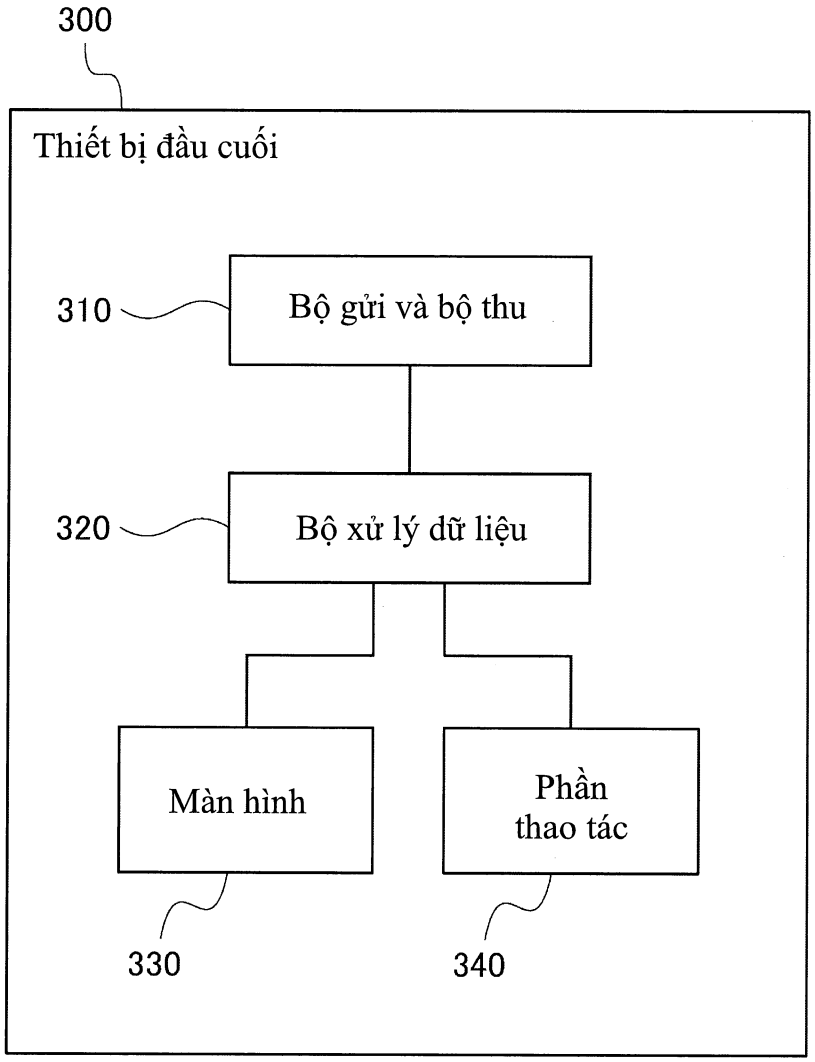

300
Thiết bị đầu cuối
310
Bộ gửi và bộ thu
320
Bộ xử lý dữ liệu
Màn hình
Phần
thao tác
330
340

FIG. 16

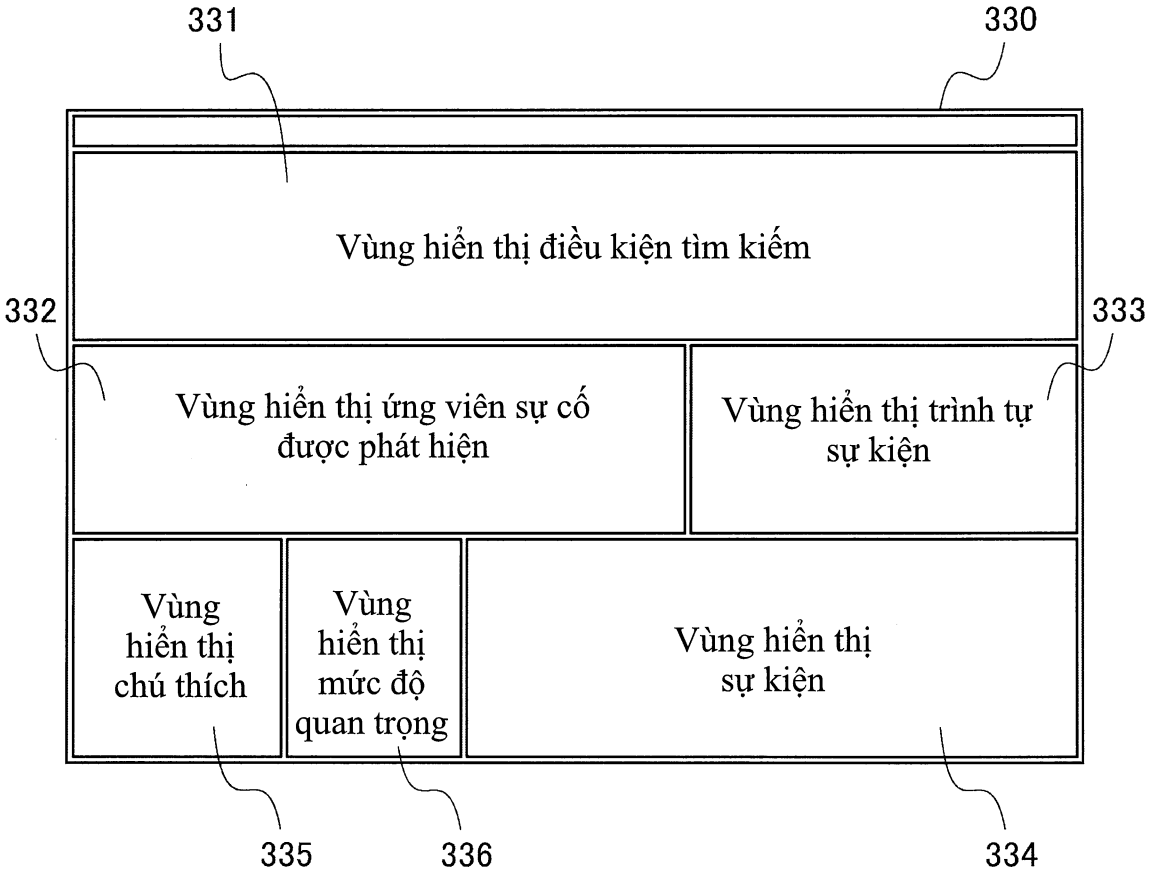
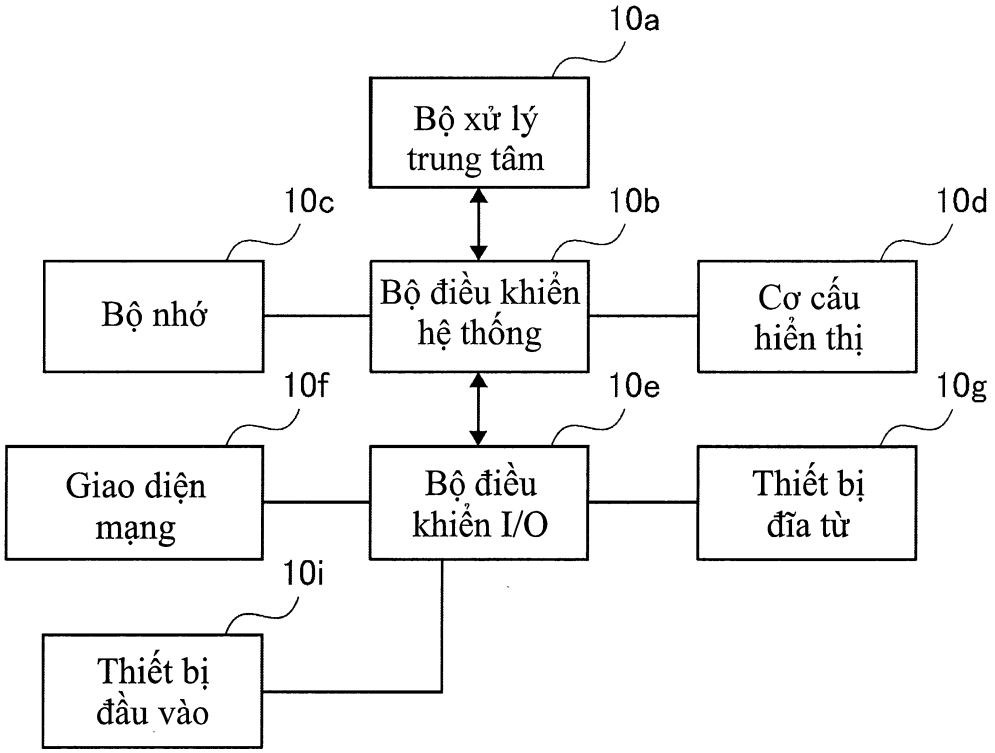

331
330
Vùng hiển thị điều kiện tìm kiếm
332
333
Vùng hiển thị ứng viên sự cố được phát hiện
Vùng hiển thị trình tự sự kiện
Vùng hiển thị chú thích
Vùng hiển thị mức độ quan trọng
Vùng hiển thị sự kiện
335
336
334

FIG. 17


10a
Bộ xử lý trung tâm
10c
10b
10d
Bộ nhớ
Bộ điều khiển hệ thống
Cơ cấu hiển thị
10f
10e
10g
Giao diện mạng
Bộ điều khiển I/O
Thiết bị đĩa từ
10i
Thiết bị đầu vào