(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2018 년 5 월 31 일 (31.05.2018)

WIPO | PCT

(10) 국제공개번호
WO 2018/097344 A1

(51) 국제특허분류:
H04L 29/06 (2006.01) *H04L 12/26* (2006.01)

(21) 국제출원번호: PCT/KR2016/013526

(22) 국제출원일: 2016 년 11 월 23 일 (23.11.2016)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(71) 출원인: 라인 가부시키가이샤 **(LINE CORPORATION)** [JP/JP]; 160-0022 도쿄 신주쿠쿠 신주쿠 4-1-6, Tokyo (JP).

(72) 발명자: **윤주호 (YUN, Juho)**; 13591 경기도 성남시 분당구 황새울로360번길 42,11층, Gyeonggi-do (KR). **가성호 (KA, Seongho)**; 13591 경기도 성남시 분당구 황새울로360번길 42,11층, Gyeonggi-do (KR).

(74) 대리인: **양성보 (YANG, Sungbo)**; 06099 서울시 강남구 선릉로125길 14 삼성빌딩 2층 피앤티특허법률사무소, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

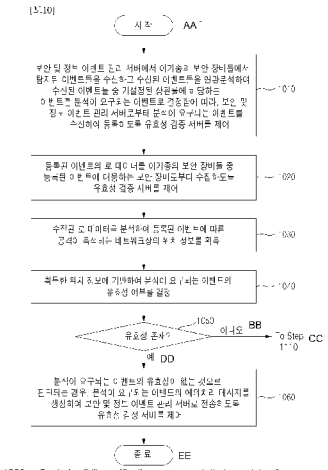
공개:

— 국제조사보고서와 함께 (조약 제21조(3))

WO 2018/097344 A1

(54) **Title:** METHOD AND SYSTEM FOR VERIFYING VALIDITY OF DETECTION RESULT

(54) **발명의 명칭:** 탐지 결과의 유효성을 검증하는 방법 및 시스템



(57) **Abstract:** Provided are a method and a system for verifying validity of a detection result. A method for verifying validity can comprise the steps of: receiving events, which are detected from heterogeneous security devices, from a security information and event management (SIEM) server, correlatively analyzing the received events, and determining an event which corresponds to a preset correlation rule among the received events as an event requiring analysis, and thus receiving the event requiring analysis from the security information and event management server, and registering same; collecting raw data of the registered event from a security device corresponding to the registered event among the heterogeneous security devices; analyzing the collected raw data and obtaining location information on a network targeted by an attack with respect to the registered event; determining whether or not there is validity in the event requiring analysis on the basis of the obtained location information; and, if it is determined that there is no validity in the event requiring analysis, generating an exception processing message of the event requiring analysis and transmitting same to the security information and event management server.

(57) **요약서:** 탐지 결과의 유효성을 검증하는 방법 및 시스템을 제공한다. 유효성 검증 방법은, 보안 및 정보 이벤트 관리(Security Information & Event Management, SIEM) 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고 상기 수신된 이벤트들을 연관분석하여 상기 수신된 이벤트들 중 기설정된 상관룰에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 상기 보안 및 정보 이벤트 관리 서버로부터 상기 분석이 요구되는 이벤트를 수신하여 등록하는 단계, 상기 등록된 이벤트의 로 데이터를 상기 이기종의 보안 장비들 중 상기 등록된 이벤트에 대응하는 보안 장비로부터 수집하는 단계, 상기 수집된 로 데이터를 분석하여 상기 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득하는 단계, 상기 획득한 위치 정보에 기반하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 단계 및 상기 분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우, 상기 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 상기 보안 및 정보 이벤트 관리 서버로 전송하는 단계를 포함할 수 있다.

명세서

발명의 명칭: 탐지 결과의 유효성을 검증하는 방법 및 시스템

기술분야

[1] 아래의 설명은 탐지 결과의 유효성을 검증하는 방법 및 시스템에 관한 것이다.

배경기술

[2] 침입 탐지 시스템(Intrusion Detection System, IDS)/침입 차단 시스템(Intrusion Prevention System, IPS)은 네트워크에서 백신과 유사한 역할을 하는 것으로, 네트워크를 통한 공격을 탐지/차단하기 위한 장비이다. 이러한 IDS/IPS는 보호하고자 하는 시스템에 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 불법행위를 구분하여 실시간으로 침입을 차단하는 기능을 가진다. 또한 내부 네트워크의 행동들을 탐지하고 기록하여 이상 상황 발생 시 즉시 이를 파악하고, 불법행위를 일으킨 패킷을 차단하여 내부 시스템의 보안을 실현한다. 이러한 IDS/IPS는 일례로 여러 개의 컴포넌트들로 구성된다. 센서는 보안 이벤트를 발생시키며, 콘솔은 발생된 이벤트를 모니터하고 센서를 제어하거나 경계하며(alert), 중앙 엔진은 센서에 의해 기록된 이벤트를 데이터베이스에 기록하거나 시스템 규칙을 사용하여 수신된 보안 이벤트로부터 경고를 생성한다. 예를 들어, 한국공개특허 제10-2009-0076612호는 상호 협력적인 다중 서버를 통한 침입 탐지 시스템 및 방법 그리고 침입 탐지 통제 시스템 및 방법에 대해 개시하고 있다.

[3] 한편, 이러한 침입 탐지 시스템을 포함하는 다양한 이기종의 보안 장비들을 통해 탐지되어 데이터베이스에 기록된 탐지 결과의 유효성은 보호하고자 하는 시스템을 위해 배치된 관제 인력과 같이 사람이 직접 검증해야 한다. 예를 들어, 관제센터의 담당자가 동일한 형태의 탐지 결과에 대한 응답 내용을 확인하는 유효성 검증을 수행한다. 그러나 대부분의 탐지 결과는 영향력이 없는 탐지 결과를 포함하고 있다. 예를 들어, 특정 페이지에 대해 실제로 공격은 시도가 되었으나 해당 서버가 요청된 페이지를 찾지 못하여 404 에러 메시지를 리턴하는 경우와 같이 실제로 영향력이 없는 사이트에 대한 공격에 대해서도 탐지 결과가 생성 및 기록된다. 이 경우 관제 인력은 이러한 영향력이 없을 뿐만 아니라 전체 탐지 결과에서 대다수를 차지하는 탐지 결과들에 대해서도 직접 불필요한 검증 작업을 처리해야 한다. 다시 말해, 모든 탐지 결과들에 대해 사람이 직접 유효성을 검증하는 것은 매우 비효율적이라는 문제점이 있다.

발명의 상세한 설명

기술적 과제

[4] 보안 동작과 관련하여 탐지되는 이벤트들의 영향력에 따라 유효성 검증의 필요성이 낮은 탐지 결과들에 대한 유효성 확인을 자동화함으로써, 불필요한 자원 낭비를 막을 수 있고 네트워크를 통한 공격에 대한 대응의 효율성을 높일

수 있는 유효성 검증 방법 및 시스템을 제공한다.

과제 해결 수단

[5] 보안 및 정보 이벤트 관리(Security Information & Event Management, SIEM) 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고 상기 수신된 이벤트들을 연관분석하여 상기 수신된 이벤트들 중 기설정된 상관룰에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 상기 보안 및 정보 이벤트 관리 서버로부터 상기 분석이 요구되는 이벤트를 수신하여 등록하는 단계; 상기 등록된 이벤트의 로 데이터를 상기 이기종의 보안 장비들 중 상기 등록된 이벤트에 대응하는 보안 장비로부터 수집하는 단계; 상기 수집된 로 데이터를 분석하여 상기 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득하는 단계; 상기 획득한 위치 정보에 기반하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 단계; 및 상기 분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우, 상기 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 상기 보안 및 정보 이벤트 관리 서버로 전송하는 단계를 포함하는 것을 특징으로 하는 유효성 검증 방법을 제공한다.

[6] 유효성 검증 서버에 있어서, 컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 보안 및 정보 이벤트 관리 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고 상기 수신된 이벤트들을 연관분석하여 상기 수신된 이벤트들 중 기설정된 상관룰에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 상기 보안 및 정보 이벤트 관리 서버로부터 상기 분석이 요구되는 이벤트를 수신하여 등록하도록 상기 유효성 검증 서버를 제어하고, 상기 등록된 이벤트의 로 데이터를 상기 이기종의 보안 장비들 중 상기 등록된 이벤트에 대응하는 보안 장비로부터 수집하도록 상기 유효성 검증 서버를 제어하고, 상기 수집된 로 데이터를 분석하여 상기 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득하고, 상기 획득한 위치 정보에 기반하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하고, 상기 분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우, 상기 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 상기 보안 및 정보 이벤트 관리 서버로 전송하도록 상기 유효성 검증 서버를 제어하는 것을 특징으로 하는 유효성 검증 서버를 제공한다.

발명의 효과

[7] 보안 동작과 관련하여 탐지되는 이벤트들의 영향력에 따라 유효성 검증의 필요성이 낮은 탐지 결과들에 대한 유효성 확인을 자동화함으로써, 불필요한 자원 낭비를 막을 수 있고 네트워크를 통한 공격에 대한 대응의 효율성을 높일 수 있다.

도면의 간단한 설명

[8] 도 1은 본 발명의 일실시예에 있어서, 유효성 검증 시스템의 전체 구조의 예를 도시한 도면이다.

[9] 도 2는 본 발명의 일실시예에 있어서, IDS 관리 콘솔에서 탐지된 이벤트 리스트의 예를 도시한 도면이다.

[10] 도 3은 본 발명의 일실시예에 있어서, IDS 관리 콘솔에서 탐지된 이벤트에 대한 세부 정보의 예를 나타낸 도면이다.

[11] 도 4는 본 발명의 일실시예에 있어서, IDS 관리 콘솔에서 탐지된 이벤트에 대한 실제 네트워크 패킷 정보의 예를 나타낸 도면이다.

[12] 도 5는 본 발명의 일실시예에 있어서, 보안 및 정보 이벤트 관리 서버에서 발생되는 경고의 예를 도시한 도면이다.

[13] 도 6은 본 발명의 일실시예에 있어서, 등록된 이벤트의 대기목록의 예를 도시한 도면이다.

[14] 도 7은 본 발명의 일실시예에 있어서, 탐지된 이벤트의 영향력을 확인하는 예를 도시한 도면이다.

[15] 도 8은 본 발명의 일실시예에 있어서, 유효성 검증 서버의 내부 구성을 설명하기 위한 블록도이다.

[16] 도 9는 본 발명의 일실시예에 있어서, 유효성 검증 서버의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이다.

[17] 도 10은 본 발명의 일실시예에 따른 유효성 검증 서버가 수행할 수 있는 유효성 검증 방법의 예를 도시한 흐름도이다.

[18] 도 11 및 도 12는 본 발명의 일실시예에 따른 유효성 검증 방법이 더 포함할 수 있는 단계들의 예를 도시한 도면이다.

발명의 실시를 위한 최선의 형태

[19] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.

[20] 도 1은 본 발명의 일실시예에 있어서, 유효성 검증 시스템의 전체 구조의 예를 도시한 도면이다.

[21] 도 1에서 점선박스(110)는, 침입 탐지/방지 시스템(Intrusion Detection/Prevention System, IDS/IPS), 클라우드 보안 솔루션인 딥시큐리티(Deepsecurity) 및 SEPM(Symantec Endpoint Protection Manager) 등과 같은 보안 장비들을 나타내고 있다. 이러한 보안 장비들에 대해서는 이미 잘 알려져 있다. 따라서, 도 1에 도시된 보안 장비들 이외에도 HIDS(Host-based Intrusion Detection System, HIDS) 등과 같이 역시 잘 알려진 다양한 보안 장비들 중 하나 이상이 본 발명의 실시예들을 위해 활용될 수 있음에 대해, 그리고 이러한 보안 장비들이 네트워크를 통한 공격을 탐지하기 위해 어떻게 동작하는가에 대해서는 당업자라면 용이하게 이해할 수 있을 것이다.

[22] 이러한 보안 장비들에서 탐지된 이벤트들은 보안 및 정보 이벤트 관리(Security Information & Event Management, SIEM) 서버(120)로 발송될 수 있다. 도 1에

나타난 ①의 과정은 보안 장비들에서 탐지된 이벤트들이 보안 및 정보 이벤트 관리 서버(120)로 전송되는 과정의 예를 나타낸다.

[23] 또한, 보안 및 정보 이벤트 관리 서버(120)는 이기종의 이벤트들을 연관분석하여 기설정된 상관룰에 맞는 이벤트를 결정할 수 있다. 예를 들어, 둘 이상의 보안 장비들에서 제1 이벤트와 제2 이벤트가 기설정된 시간 간격 이내(일례로, 1분 이내의 간격)로 발생되어 보안 및 정보 이벤트 관리 서버(120)로 전송되는 경우, 보안 및 정보 이벤트 관리 서버(120)는 제1, 2 이벤트들을 상관룰에 맞는 이벤트들로 결정할 수 있다. 이러한 상관룰은 이미 잘 알려져 있는 보안 및 정보 이벤트 관리에 대한 기술을 통해 당업자가 쉽게 이해할 수 있을 것이다. 이 경우, 보안 및 정보 이벤트 관리 서버(120)는 결정된 이벤트들을 보안관제 업무 관리 서버(130)로 전송하여 업무로서 등록되도록 할 수 있다. 도 1에 나타난 ②의 과정이 이러한 이벤트를 보안 및 정보 이벤트 관리 서버(120)에서 보안관제 업무 관리 서버(130)로 전송하여 등록하는 과정의 예를 나타낼 수 있다. 예를 들어, 보안 및 정보 이벤트 관리 서버(120)는 결정된 이벤트들에 대한 보안 및 정보 이벤트 관리 티켓을 생성하여 보안관제 업무 관리 서버(130)로 전송할 수 있고, 보안관제 업무 관리 서버(130)는 수신된 보안 및 정보 이벤트 관리 티켓을 등록함으로써 특정 공격에 대한 이벤트(분석이 요구되는 이벤트)를 등록할 수 있다.

[24] 보안관제 업무 관리 서버(130)는 업무로서 등록되는 공격에 대한 이벤트들의 정보를 관제 인력들에게 제공하고, 관제 인력들이 등록된 이벤트들을 처리할 수 있는 기능을 제공할 수 있다. 예를 들어, 보안관제 업무 관리 서버(130)는 관제 인력들이 개별 이벤트들에 대한 상세 정보를 살펴보고 이러한 개별 이벤트들의 공격 유효성을 검증하여 유효성 여부를 지정할 수 있는 사용자 인터페이스를 관제 인력들에게 제공할 수 있다. 이러한 보안관제 업무 관리 서버(130)는 일례로, 위험 관리 시스템(Threat Management System, TMS)과 같은 기술을 통해 당업자가 용이하게 이해할 수 있다.

[25] 한편, 이미 설명한 바와 같이 등록되는 모든 이벤트들의 유효성을 사람이 직접 검증하는 것은 매우 비효율적이다. 이러한 문제점을 해결하기 위해, 본 발실시예들에 따른 유효성 검증 시스템은 도 1에 도시된 바와 같이 이벤트 분석 서버(140)와 로그 확인 서버(150)를 포함할 수 있다. 도 1의 실시예에 따른 유효성 검증 시스템은 보안관제 업무 관리 서버(130), 이벤트 분석 서버(140) 및 로그 확인 서버(150)를 개별 장치로서 포함하고 있으나, 실시예에 따라 이벤트 분석 서버(140)와 로그 확인 서버(150)는 보안관제 업무 관리 서버(130)와 결합된 하나의 시스템으로 구성될 수도 있다. 예를 들어, 하나의 서버 장치에서 보안관제 업무 관리 서버(130), 이벤트 분석 서버(140) 및 로그 확인 서버(150)를 통해 제공하고자 하는 모든 기능을 제공할 수도 있다.

[26] 이벤트 분석 서버(140)는 보안관제 업무 관리 서버(130)에 등록된 이벤트를 수집할 수 있다. 예를 들어, 이벤트 분석 서버(140)는 기설정된 시간 간격(일례로,

1분)마다 보안관제 업무 관리 서버(130)에 등록된 이벤트들을 수집할 수 있다. 도 1에 도시된 ③의 과정이 이벤트 분석 서버(140)가 등록된 이벤트들을 수집하는 과정의 예를 나타낼 수 있다.

[27] 또한, 이벤트 분석 서버(140)는 수집된 이벤트를 로그 확인 서버(150)로 전달할 수 있다. 예를 들어, 도 1에 도시된 ④의 과정은 이벤트 분석 서버(140)가 수집된 이벤트를 로그 호가인 서버(150)로 삽입(insert)하는 과정의 예를 나타낼 수 있다.

[28] 로그 확인 서버(150)는 수신된 이벤트에 대응하는 로(raw) 데이터를 해당 이벤트를 생성한 보안 장비의 데이터베이스(160)로부터 수집할 수 있다. 예를 들어, 로그 확인 서버(150)는 수신된 이벤트의 이름과 소스의 IP 주소/포트 넘버, 그리고 목적지의 IP 주소/포트 넘버 등의 정보를 이용하여 해당 이벤트를 생성한 보안 장비의 데이터베이스(160)를 조회할 수 있고, 조회 결과로서 해당 이벤트에 대응하는 로 데이터를 얻을 수 있다. 도 1에 도시된 ⑤의 과정이 로 데이터를 수집하는 과정의 예를 나타낼 수 있다.

[29] 로그 확인 서버(150)는 수집된 로 데이터를 파싱할 수 있다. 도 1에 도시된 ⑥의 과정이 수집된 로 데이터를 파싱하는 과정의 예를 나타낼 수 있다. 예를 들어, 로 데이터의 파싱은 해당 이벤트에 대응하는 공격이 목적한 페이지의 URI(Uniform Resource Identifier)를 추출하기 위해 이루어질 수 있다.

[30] 또한, 로그 확인 서버(150)는 파싱된 정보를 이용하여 이벤트에 대응하는공격과 동일한 공격을 실시하여 응답 결과를 확인할 수 있다. 예를 들어, 로그 확인 서버(150)는 추출된 URI를 이용하여 확인되는 페이지로 네트워크(170)를 실제 공격과 동일한 공격을 실행함으로써, 해당 페이지에서의 응답 결과를 확인할 수 있다. 도 1에 도시된 ⑦의 과정이 이러한 응답 결과의 확인을 위한 과정의 예를 나타낼 수 있다.

[31] 로그 확인 서버(510)는 확인된 응답 결과를 이벤트 분석 서버(140)로 전달할 수 있다. 도 1에 도시된 ⑧의 과정이 이러한 응답 결과의 전달을 위한 과정의 예를 나타낼 수 있다.

[32] 이벤트 분석 서버(140)는 전달된 응답 결과를 분석하여 이벤트의 리스크 정도를 결정할 수 있다. 예를 들어, 상술한 ⑦의 과정에서 URI를 통해 실행된 공격에 따라 해당 페이지를 찾을 수 없다는 HTTP 404 메시지가 수신된다면, 해당 공격은 영향력이 없는 공격으로 판단될 수 있고, 해당 이벤트는 리스크가 낮은 이벤트로 결정될 수 있다. 이때, 이벤트 분석 서버(140)는 리스크가 큰 이벤트(일례로, 리스크가 기설정된 정도 이상인 이벤트)에 대해서는 보안 및 정보 이벤트 관리 이벤트를 보안 및 정보 이벤트 관리 서버(120)로 전송할 수 있다. 또한, 이벤트 분석 서버(140)는 리스크가 낮은 이벤트(일례로, 리스크가 기설정된 정도 미만인 이벤트)에 대해서는 예외처리 메시지를 보안 및 정보 이벤트 관리 서버(120)로 전송될 수 있다. 도 1에 도시된 ⑨의 과정이 이러한 보안 및 정보 이벤트 관리 이벤트 및/또는 예외처리 메시지를 발송하는 과정의 예를 나타낼 수 있다.

[33] 이때, 보안 및 정보 이벤트 관리 서버(120)는 예외처리 메시지에 따라 예외처리 메시지에 대응하는 이벤트를 보안 및 정보 이벤트 관리 필터에 추가할 수 있다. 이 경우, 향후에 동일한 URI에 대해 발생하는 공격에 따른 이벤트는 보안 및 정보 이벤트 관리 서버(120)에서 추가적으로 필터링될 수 있다. 따라서, 이러한 예외처리되는 이벤트들은 보안관제 업무 관리 서버(130)로 전달되지 않게 되고, 동일한 공격을 위한 다수의 패킷들이 존재하기 때문에 이러한 예외처리가 증가할수록 보안관제 업무 관리 서버(130)에서 관제 인력이 유효성을 검증해야 할 이벤트의 수가 급격히 감소하게 된다. 다시 말해, 본 실시예에 따른 유효성 검증 시스템을 통해 영향력이 없는 이벤트에 대한 유효성이 자동적으로 검증될 수 있기 때문에 불필요한 자원 낭비를 막을 수 있고 네트워크를 통한 공격에 대한 대응의 효율성을 높일 수 있다.

[34] 도 2는 본 발명의 일실시예에 있어서, IDS 관리 콘솔에서 탐지된 이벤트 리스트의 예를 도시한 도면이다. 보안 장비로서 IDS는 네트워크 트래픽(일례로, 수신되는 패킷들)에서 보안 공격으로 판단되는 문자열에 대해, 사전에 등록된 패턴과 일치하는 트래픽을 탐지할 수 있다. 도 2의 이벤트 리스트는 IDS에서 탐지된 이벤트들의 리스트를 의미할 수 있고, 도 2에 도시된 바와 같이 공격 유형(Attack Type), 서명 그룹(Signature Group), 심각도(Severity), 탐지된 시각(Time detected), 소스 IP 주소(Source IP), 공격자 포트(Attacker port), 목적지 IP 주소(Destination IP), 목적지 포트(Destination Port)와 같은 정보들을 포함할 수 있다.

[35] 도 3은 본 발명의 일실시예에 있어서, IDS 관리 콘솔에서 탐지된 이벤트에 대한 세부 정보의 예를 나타낸 도면이고, 도 4는 본 발명의 일실시예에 있어서, IDS 관리 콘솔에서 탐지된 이벤트에 대한 실제 네트워크 패킷 정보의 예를 나타낸 도면이다. 도 3은 하나의 이벤트가 이벤트 이름, 소스 IP 주소, 소스 포트, 목적지 IP 주소, 목적지 포트, 탐지된 시각 등을 이용하여 식별될 수 있음을 간접적으로 보여준다. 또한, 도 4는 하나의 이벤트에 대해 실제 네트워크 패킷 정보가 관리됨을 보여주고 있다.

[36] 또한, IDS와 같은 보안 장비에서 탐지된 이벤트는 보안 및 정보 이벤트 관리 서버(120)로 전송될 수 있고, 보안 및 정보 이벤트 관리 서버(120)에서는 수신되는 이벤트에 대해 상관룰에 따른 조건을 체크하여 경고(Alert)를 발생할지 여부를 판단할 수 있고, 추가 분석이 필요한 이벤트에 대해서는 경고를 발생할 수 있다.

[37] 도 5는 본 발명의 일실시예에 있어서, 보안 및 정보 이벤트 관리 서버에서 발생되는 경고의 예를 도시한 도면이다. 도 5는 경고가 발생한 이벤트에 대한 정보와 관련 데이터의 예를 나타내고 있다. 이러한 정보들은 보안 및 정보 이벤트 관리 서버(120)에서 보안관제 업무 관리 서버(130)으로 발송되어 보안관제 업무 관리 서버(130)에 등록될 수 있다.

[38] 도 6은 본 발명의 일실시예에 있어서, 등록된 이벤트의 대기목록의 예를 도시한

도면이다. 도 6은 보안관제 업무 관리 서버(130)이 관제 인력에게 제공하는 사용자 인터페이스 화면 중 일부의 화면(600)으로서, 보안관제 업무 관리 서버(130)에 등록되어 유효성 검증을 위해 대기 중인 이벤트들의 리스를 나타내고 있다. 이때, 관제 인력은 화면(600)에 나타난 이벤트들을 선택하여 각 이벤트들의 상세 정보를 확인할 수 있고, 선택된 이벤트들의 유효성을 검증할 수 있다. 예를 들어, 도 6의 '정탐' 버튼(610)은 선택된 이벤트가 유효성이 있는 탐지임을, '오탐' 버튼(620)은 선택된 이벤트가 유효성이 없는 탐지임을 각각 지정하기 위해 이용될 수 있다.

[39] 이처럼, 보안관제 업무 관리 서버(130)에 등록되는 이벤트들에 대해서는 관제 인력이 매번 수동으로 유효성을 검증할 필요가 있다. 본 발명의 실시예들에서는 이미 설명한 바와 같이 이벤트 분석 서버(140)와 로그 확인 서버(150)를 통해 영향력이 없는 이벤트에 대한 예외처리를 보안 및 정보 이벤트 관리 서버(120)에 등록하여 보안 및 정보 이벤트 관리 서버(120)가 영향력 없는 이벤트를 필터링하여 보안관제 업무 관리 서버(130)에 등록하지 않음으로써 관제 인력이 수동으로 유효성을 검증해야 할 이벤트의 수를 줄일 수 있다.

[40] 도 7은 본 발명의 일실시예에 있어서, 탐지된 이벤트의 영향력을 확인하는 예를 도시한 도면이다.

[41] 제1 점선박스(710)는 도 1에 도시된 ⑤의 과정을 통해 로그 확인 서버(150)가 수신된 이벤트를 생성한 보안 장비의 데이터베이스(160)로부터 수집한 로 데이터의 예를 나타내고 있다.

[42] 또한, 제2 점선박스(720)는 도 1에 도시된 ⑥의 과정을 통해 로그 확인 서버(150)가 로 데이터를 파싱하여 추출한 URL(Uniform Resource Locator)의 예를 나타내고 있다.

[43] 또한, 제3 점선박스(730)는 도 1에 도시된 ⑦의 과정을 통해 로그 확인 서버(150)가 추출한 URL을 통해 접근함에 따라 해당 서버로부터 수신한 응답 결과(URL에 대응하는 페이지의 소스 코드)의 예를 나타내고 있다.

[44] 이미 설명한 바와 같이 로그 확인 서버(150)는 수신한 응답 결과를 이벤트 분석 서버(140)로 전송할 수 있고, 이벤트 분석 서버(140)는 응답 결과에서 404 응답 코드를 확인함에 따라 해당 이벤트가 영향력이 없음을 확인할 수 있다.

[45] 제4 점선박스(740)는 해당 공격에 대한 식별자(USD_316_Eval_One_Line_PHP_WebShell_090803)와 대상 IP 주소(125.6.190.6), 그리고 대상 포트 넘버(80)를 나타내고 있다. 보안 및 정보 이벤트 관리 서버(120)는 이러한 공격, 대상 IP 주소 및 대상 포트 넘버를 예외처리함으로써 이후에는 해당 공격이나 대상에 대해 이벤트가 발생하지 않도록 조치할 수 있다.

[46] 도 7은 영향력이 없는 이벤트에 대한 예외처리의 실시예를 설명하였으나, 실시예에 따라 영향력이 높은 이벤트에 대해서는 이벤트의 등록뿐만 아니라, 보안 및 정보 이벤트 관리 서버(120)에서 보안관제 업무 관리 서버(130)으로

별도의 경고(Alert) 메시지를 발송함으로써, 관제 인력이 영향력이 높은 이벤트를 놓치지 않도록 할 수 있다.

[47] 도 8은 본 발명의 일실시예에 있어서, 유효성 검증 서버의 내부 구성을 설명하기 위한 블록도이다. 본 실시예에서는 보안관제 업무 관리 서버(130), 이벤트 분석 서버(140) 및 로그 확인 서버(150)가 하나의 장치인 유효성 검증 서버(800)로서 구현되는 예를 설명한다. 유효성 검증 서버(800)는 도 8에 도시된 바와 같이 메모리(810), 프로세서(820), 통신 모듈(830) 그리고 입출력 인터페이스(840)를 포함할 수 있다. 메모리(810)는 컴퓨터에서 판독 가능한 기록매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 여기서 ROM과 비소멸성 대용량 기록장치는 메모리(810)와 분리되어 별도의 영구 저장 장치로서 포함될 수도 있다. 또한, 메모리(810)에는 운영체제와 적어도 하나의 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 메모리(810)와는 별도의 컴퓨터에서 판독 가능한 기록매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록매체를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록매체가 아닌 통신 모듈(830)을 통해 메모리(810)에 로딩될 수도 있다.

[48] 프로세서(820)는 기본적인 산술, 로직 및 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(810) 또는 통신 모듈(830)에 의해 프로세서(820)로 제공될 수 있다. 예를 들어 프로세서(820)는 메모리(810)에 로딩된 프로그램 코드에 따라 수신되는 명령을 실행하도록 구성될 수 있다.

[49] 통신 모듈(830)은 실제 컴퓨터 네트워크를 통해 다른 물리적인 기기들과 서로 통신하기 위한 기능을 제공할 수 있다. 일례로, 통신 모듈(830)은 보안 및 정보 이벤트 관리 서버(120)나 보안 장비들과의 네트워크를 통해 데이터를 송수신 하기 위한 기능을 제공할 수 있다.

[50] 입출력 인터페이스(840)는 입출력 장치(850)와의 인터페이스를 위한 수단일 수 있다. 예를 들어, 입출력 장치(850)에서 입력 장치는 키보드 또는 마우스 등의 장치를, 그리고 출력 장치는 디스플레이나 스피커와 같은 장치를 포함할 수 있다. 도 8에서 입출력 장치(850)는 유효성 검증 서버(800)와 별도의 장치로 표현되었으나, 실시예에 따라 입출력 장치(850)가 유효성 검증 서버(800)에 포함되도록 유효성 검증 서버(800)가 구현될 수도 있다.

[51] 또한, 다른 실시예들에서 유효성 검증 서버(800)는 도 8의 구성요소들보다 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 유효성 검증 서버(800)는 각종 물리적인 버튼이나 터치패널, 또는 광출력 장치 등의 다양한

구성요소들을 더 포함하도록 구현될 수도 있다.

[52] 도 9는 본 발명의 일실시예에 있어서, 유효성 검증 서버의 프로세서가 포함할 수 있는 구성요소의 예를 도시한 블록도이고, 도 10은 본 발명의 일실시예에 따른 유효성 검증 서버가 수행할 수 있는 유효성 검증 방법의 예를 도시한 흐름도이다. 또한, 도 11 및 도 12는 본 발명의 일실시예에 따른 유효성 검증 방법이 더 포함할 수 있는 단계들의 예를 도시한 도면이다.

[53] 도 9는 앞서 설명한 유효성 검증 서버(800)의 프로세서(820)가 포함할 수 있는 구성요소들로서 이벤트 등록부(910), 로 데이터 수집부(920), 위치 정보 획득부(930), 유효성 결정부(940) 및 예외처리 메시지 전송부(950)를 나타내고 있다. 또한, 프로세서(820)는 도 9에 도시된 바와 같이 실시예에 따라, 유효성 메시지 전송부(960), 경고 메시지 수신부(970) 및 사용자 인터페이스 제공부(980) 중 적어도 하나를 더 포함할 수 있다. 이러한 프로세서(820) 및 프로세서(820)의 구성요소들은 도 10의 유효성 검증 방법이 포함하는 단계들(1010 내지 1060), 그리고 도 11 및 도 12에 도시된 단계들(1110, 1120 및 1210)을 수행할 수 있다. 이때, 프로세서(820) 및 프로세서(820)의 구성요소들은 메모리(810)가 포함하는 운영체제의 코드 및/또는 적어도 하나의 컴퓨터 프로그램의 코드에 따른 명령(instruction)을 실행하도록 구현될 수 있다. 여기서, 프로세서(820)의 구성요소들은 유효성 검증 서버(800)에 저장된 컴퓨터 프로그램의 코드가 제공하는 제어 명령에 따라 프로세서(820)에 의해 수행되는 프로세서(820)의 서로 다른 기능들(different functions)의 표현들일 수 있다. 예를 들어, 프로세서(820)는 유효성 검증 서버(800)의 제어와 관련된 명령이 로딩된 메모리(810)로부터 필요한 제어 명령을 읽어드릴 수 있으며, 읽어들인 제어 명령에 따라 이후 설명될 단계들(1010 내지 1060, 1110, 1120 및 1210)을 수행하도록 유효성 검증 서버(800)를 제어할 수 있다.

[54] 단계(1010)에서 이벤트 등록부(910)는 보안 및 정보 이벤트 관리(Security Information & Event Management, SIEM) 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고 수신된 이벤트들을 연관분석하여 수신된 이벤트들 중 기설정된 상관률에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 보안 및 정보 이벤트 관리 서버로부터 분석이 요구되는 이벤트를 수신하여 등록하도록 유효성 검증 서버(800)를 제어할 수 있다. 여기서, 보안 및 정보 이벤트 관리 서버는 도 1을 통해 설명한 보안 및 정보 이벤트 관리 서버(120)에 대응할 수 있다. 다시 말해, 보안 및 정보 이벤트 관리 서버는 도 1의 점선박스(110)에 나타난 바와 같은 이기종의 보안 장비들에서 탐지되는 이벤트들을 수신할 수 있으며, 수신된 이벤트들을 연관분석하여 이러한 이벤트들 중 기설정된 상관률에 맞는 이벤트를 유효성 검증 서버(800)로 전송하여 등록되도록 할 수 있다. 이때, 이벤트 등록부(910)는 보안 및 정보 이벤트 관리 서버로부터 수신되는 이벤트를 등록하도록 유효성 검증 서버(800)를 제어할 수 있다.

[55] 상술한 단계(1010) 이후에는 도 12에 도시된 단계(1210)이 수행될 수 있다.

[56] 단계(1210)에서 사용자 인터페이스 제공부(980)는 등록된 이벤트에 대한 유효성 여부를 지정할 수 있는 사용자 인터페이스를 제공할 수 있다. 예를 들어, 앞서 설명한 도 6에서와 같이 유효성 검증 서버(800)를 통해 등록된 이벤트의 대기목록과 이러한 대기목록상의 이벤트에 대한 유효성 여부를 지정할 수 있는 사용자 인터페이스가 관제 인력들에게 제공될 수 있다. 이러한 사용자 인터페이스는 유효성 검증 서버(800)와 직접 연결된 디스플레이 또는 유효성 검증 서버(800)와 통신하는 관제 인력들의 단말기들의 디스플레이를 통해 관제 인력들에게 표시될 수 있다.

[57] 단계(1020)에서 로 데이터 수집부(920)는 등록된 이벤트의 로 데이터를 이기종의 보안 장비들 중 등록된 이벤트에 대응하는 보안 장비로부터 수집하도록 유효성 검증 서버(800)를 제어할 수 있다. 예를 들어, 상기 등록된 이벤트가 도 1에서 제1 점선박스(110)에 나타난 IDS/IPS 보안 장비에서 생성된 이벤트인 경우, 유효성 검증 서버(800)는 로 데이터 수집부(920)의 제어에 따라 IDS/IPS 보안 장비에 접근하여 IDS/IPS 보안 장비가 포함하는 데이터베이스로부터 등록된 이벤트의 로 데이터를 수집할 수 있다. 로 데이터의 예는 도 7을 통해 설명한 바 있다.

[58] 단계(1030)에서 위치 정보 획득부(930)는 수집된 로 데이터를 분석하여 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득할 수 있다. 이러한 네트워크상의 위치 정보는 URL을 포함하는 URI일 수 있다. 앞서 실시예들은 네트워크상의 특정 페이지로 한정하여 설명하였으나, 네트워크상의 공격이 페이지로 한정되지는 않는다. 다시 말해, 본 실시예에서 네트워크상의 위치 정보는 공격자의 패킷이 목적하는 네트워크상의 자원에 대한 위치 정보를 의미할 수 있다.

[59] 단계(1040)에서 유효성 결정부(940)는 획득한 위치 정보에 기반하여 분석이 요구되는 이벤트의 유효성 여부를 결정할 수 있다. 예를 들어, 유효성 결정부(940)는 획득한 위치 정보에 기반하여 상기 공격과 동일한 공격을 실시하고, 획득한 위치 정보에 대응하는 시스템으로부터의 응답 결과를 확인 및 분석하여 분석이 요구되는 이벤트의 유효성 여부를 결정할 수 있다. 보다 구체적인 예로, 획득한 위치 정보는 네트워크상의 페이지에 대한 URI를 포함할 수 있다. 이 경우, 유효성 결정부(940)는 상기 URI를 통해 페이지에 접속을 시도하여 페이지의 상태에 대한 응답 코드를 수신하고, 수신된 응답 코드를 분석하여 분석이 요구되는 이벤트의 유효성 여부를 결정할 수 있다. 이미 HTTP 404 코드와 같이 찾을 수 없는 페이지에 대한 공격은 영향력이 없기 때문에 이벤트의 유효성이 없음을 설명한 바 있다.

[60] 단계(1050)은 유효성 여부에 따라 유효성이 존재하는 경우 단계(1060)이 수행되고, 유효성이 존재하지 않는 경우 도 11의 단계(1110)이 수행될 수 있음을 나타내고 있다.

[61] 단계(1060)에서 예외처리 메시지 전송부(950)는 분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우, 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 보안 및 정보 이벤트 관리 서버로 전송하도록 유효성 검증 서버(800)를 제어할 수 있다. 이 경우, 보안 및 정보 이벤트 관리 서버는 예외처리 메시지에 대응하는 이벤트가 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 재탐색되어 수신된 이벤트를 예외처리하도록 기설정된 상관룰을 갱신할 수 있다. 즉, 예외처리 메시지에 대응하는 이벤트는 보안 및 정보 이벤트 관리 서버에서 필터링되어 유효성 검증 서버(800)에 등록되지 않게 되며, 따라서 관제 인력들이 유효성을 검증해야 할 이벤트들의 수가 줄어들게 된다.

[62] 단계(1110)에서 유효성 메시지 전송부(960)는 분석이 요구되는 이벤트의 유효성이 있는 것으로 판단되는 경우, 분석이 요구되는 이벤트에 대한 유효성 메시지를 보안 및 정보 이벤트 관리 서버로 전송하도록 유효성 검증 서버(800)를 제어할 수 있다. 예를 들어, 특정 이벤트에 대해 리스크가 높다고 결정되면, 유효성 검증 서버(800)는 보안 및 정보 이벤트 관리 서버로 해당 이벤트에 대한 유효성 메시지를 전송할 수 있다.

[63] 단계(1120)에서 경고 메시지 수신부(970)는 보안 및 정보 이벤트 관리 서버에서 유효성 메시지에 대응하는 이벤트가 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 보안 및 정보 이벤트 관리 서버가 재탐색되어 수신된 이벤트에 대해 생성하는 경고 메시지를 보안 및 정보 이벤트 관리 서버로부터 수신하도록 유효성 검증 서버(800)를 제어할 수 있다. 다시 말해, 보안 및 정보 이벤트 관리 서버는 유효성 메시지에 대응하는 이벤트가 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 단계(1010)에서 설명한 바와 같이 해당 이벤트를 유효성 검증 서버(800)에 등록할 뿐만 아니라, 별도의 경고 메시지를 유효성 검증 서버(800)로 더 전송할 수 있다. 이 경우, 유효성 검증 서버(800)는 경고 메시지에 따른 이벤트와 관련하여 추가적인 정보나 경고를 관제 인력들에게 제공함으로써, 관제 인력들이 해당 이벤트에 대한 분석을 놓치지 않도록 할 수 있다.

[64] 이상에서와 같이, 본 발명의 실시예들에 따르면, 보안 동작과 관련하여 탐지되는 이벤트들의 영향력에 따라 유효성 검증의 필요성이 낮은 탐지 결과들에 대한 유효성 확인을 자동화함으로써, 불필요한 자원 낭비를 막을 수 있고 네트워크를 통한 공격에 대한 대응의 효율성을 높일 수 있다.

[65] 이상에서 설명된 시스템 또는 장치는 하드웨어 구성요소, 소프트웨어 구성요소 또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터

또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[66] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[67] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

발명의 실시를 위한 형태

[68] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정

및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[69] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

청구범위

[청구항 1] 보안 및 정보 이벤트 관리(Security Information & Event Management, SIEM) 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고
상기 수신된 이벤트들을 연관분석하여 상기 수신된 이벤트들 중 기설정된 상관룰에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 상기 보안 및 정보 이벤트 관리 서버로부터 상기 분석이 요구되는 이벤트를 수신하여 등록하는 단계;
상기 등록된 이벤트의 로 데이터를 상기 이기종의 보안 장비들 중 상기 등록된 이벤트에 대응하는 보안 장비로부터 수집하는 단계;
상기 수집된 로 데이터를 분석하여 상기 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득하는 단계;
상기 획득한 위치 정보에 기반하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 단계; 및
상기 분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우, 상기 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 상기 보안 및 정보 이벤트 관리 서버로 전송하는 단계
를 포함하는 것을 특징으로 하는 유효성 검증 방법.

[청구항 2] 제1항에 있어서,
상기 보안 및 정보 이벤트 관리 서버는 상기 예외처리 메시지에 대응하는 이벤트가 상기 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 재탐색되어 수신된 이벤트를 예외처리하도록 상기 기설정된 상관룰을 갱신하는 것을 특징으로 하는 유효성 검증 방법.

[청구항 3] 제1항에 있어서,
상기 분석이 요구되는 이벤트의 유효성이 있는 것으로 판단되는 경우, 상기 분석이 요구되는 이벤트에 대한 유효성 메시지를 상기 보안 및 정보 이벤트 관리 서버로 전송하는 단계; 및
상기 보안 및 정보 이벤트 관리 서버에서 상기 유효성 메시지에 대응하는 이벤트가 상기 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 상기 보안 및 정보 이벤트 관리 서버가 상기 재탐색되어 수신된 이벤트에 대해 생성하는 경고 메시지를 상기 보안 및 정보 이벤트 관리 서버로부터 수신하는 단계
를 더 포함하는 것을 특징으로 하는 유효성 검증 방법.

[청구항 4] 제1항에 있어서,
상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 단계는,
상기 획득한 위치 정보에 기반하여 상기 공격과 동일한 공격을 실시하고, 상기 획득한 위치 정보에 대응하는 시스템으로부터의 응답 결과를 확인 및 분석하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는

것을 특징으로 하는 유효성 검증 방법.

[청구항 5] 제1항에 있어서,
상기 획득한 위치 정보는 네트워크상의 페이지에 대한 URI(Uniform Resource Identifier)를 포함하고,
상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 단계는,
상기 URI를 통해 상기 페이지에 접속을 시도하여 상기 페이지의 상태에 대한 응답 코드를 수신하고, 상기 수신된 응답 코드를 분석하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 것을 특징으로 하는 유효성 검증 방법.

[청구항 6] 제1항에 있어서,
상기 등록된 이벤트에 대한 유효성 여부를 지정할 수 있는 사용자 인터페이스를 제공하는 단계
를 더 포함하는 것을 특징으로 하는 유효성 검증 방법.

[청구항 7] 제1항 내지 제6항 중 어느 한 항의 방법을 컴퓨터에 실행시키기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록매체.

[청구항 8] 유효성 검증 서버에 있어서,
컴퓨터에서 판독 가능한 명령을 실행하도록 구현되는 적어도 하나의 프로세서
를 포함하고,
상기 적어도 하나의 프로세서는,
보안 및 정보 이벤트 관리(Security Information & Event Management, SIEM) 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고
상기 수신된 이벤트들을 연관분석하여 상기 수신된 이벤트들 중 기설정된 상관룰에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 상기 보안 및 정보 이벤트 관리 서버로부터 상기 분석이 요구되는 이벤트를 수신하여 등록하도록 상기 유효성 검증 서버를 제어하고,
상기 등록된 이벤트의 로 데이터를 상기 이기종의 보안 장비들 중 상기 등록된 이벤트에 대응하는 보안 장비로부터 수집하도록 상기 유효성 검증 서버를 제어하고,
상기 수집된 로 데이터를 분석하여 상기 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득하고,
상기 획득한 위치 정보에 기반하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하고,
상기 분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우,
상기 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 상기 보안 및 정보 이벤트 관리 서버로 전송하도록 상기 유효성 검증 서버를

제어하는 것
을 특징으로 하는 유효성 검증 서버.

[청구항 9] 제8항에 있어서,
상기 보안 및 정보 이벤트 관리 서버는 상기 예외처리 메시지에 대응하는 이벤트가 상기 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 재탐색되어 수신된 이벤트를 예외처리하도록 상기 기설정된 상관룰을 갱신하는 것을 특징으로 하는 유효성 검증 서버.

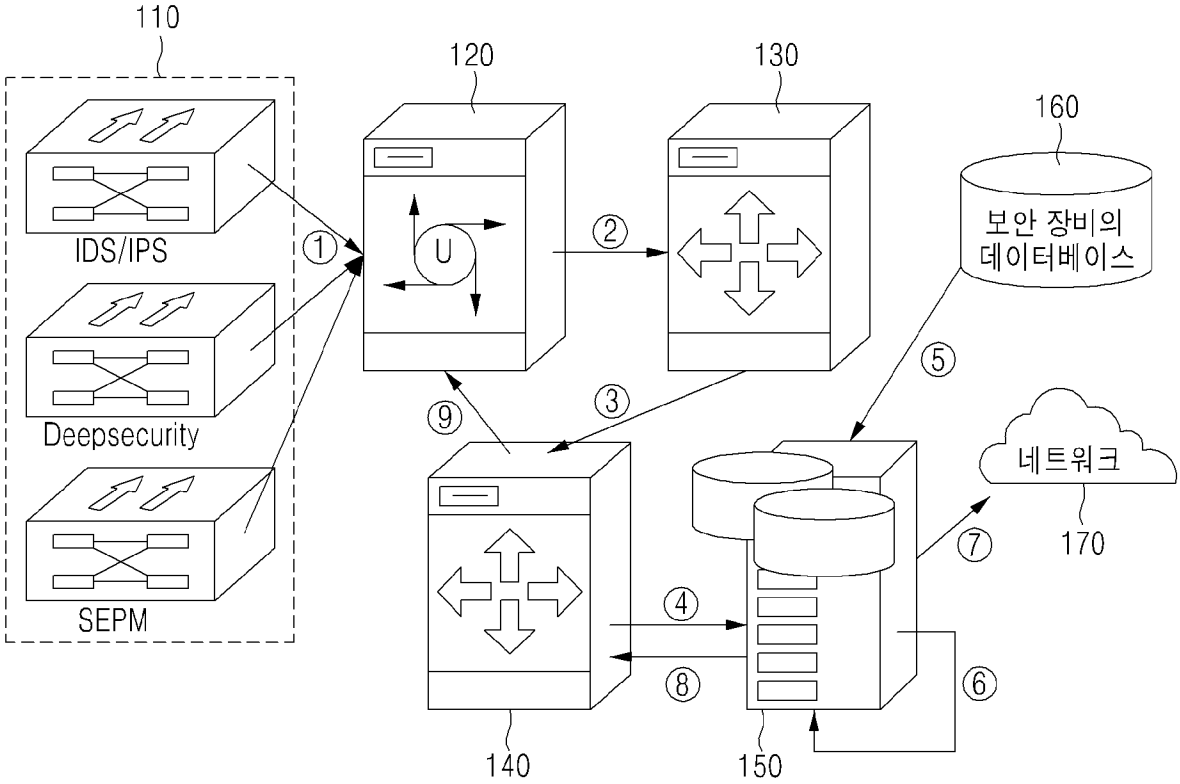
[청구항 10] 제8항에 있어서,
상기 적어도 하나의 프로세서는,
상기 분석이 요구되는 이벤트의 유효성이 있는 것으로 판단되는 경우, 상기 분석이 요구되는 이벤트에 대한 유효성 메시지를 상기 보안 및 정보 이벤트 관리 서버로 전송하도록 상기 유효성 검증 서버를 제어하고,
상기 보안 및 정보 이벤트 관리 서버에서 상기 유효성 메시지에 대응하는 이벤트가 상기 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 상기 보안 및 정보 이벤트 관리 서버가 상기 재탐색되어 수신된 이벤트에 대해 생성하는 경고 메시지를 상기 보안 및 정보 이벤트 관리 서버로부터 수신하도록 상기 유효성 검증 서버를 제어하는 것
을 특징으로 하는 유효성 검증 서버.

[청구항 11] 제8항에 있어서,
상기 적어도 하나의 프로세서는,
상기 분석이 요구되는 이벤트의 유효성 여부를 결정하기 위해, 상기 획득한 위치 정보에 기반하여 상기 공격과 동일한 공격을 실시하고, 상기 획득한 위치 정보에 대응하는 시스템으로부터의 응답 결과를 확인 및 분석하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 것을 특징으로 하는 유효성 검증 서버.

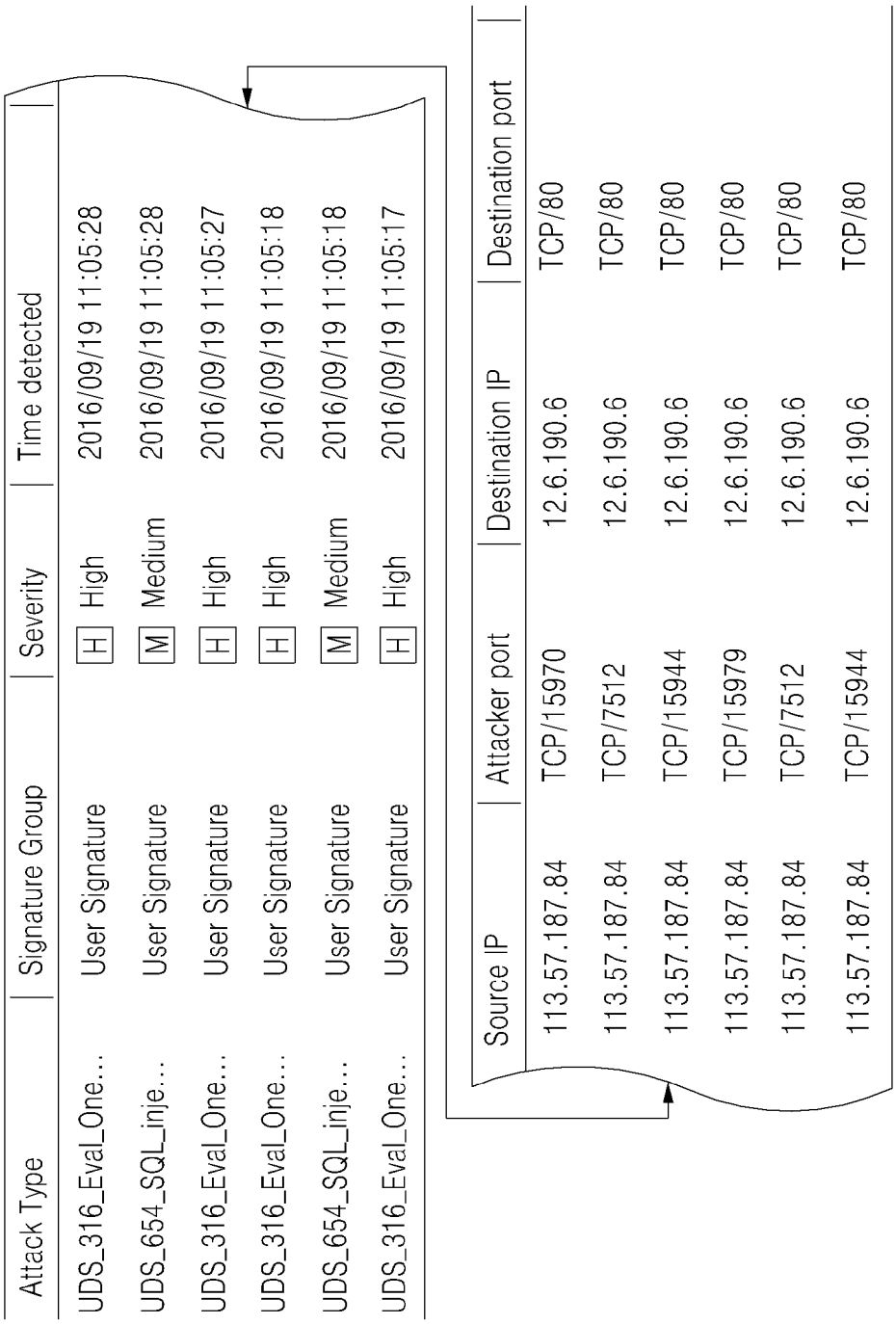
[청구항 12] 제8항에 있어서,
상기 획득한 위치 정보는 네트워크상의 페이지에 대한 URI를 포함하고,
상기 적어도 하나의 프로세서는,
상기 분석이 요구되는 이벤트의 유효성 여부를 결정하기 위해, 상기 URI를 통해 상기 페이지에 접속을 시도하여 상기 페이지의 상태에 대한 응답 코드를 수신하고, 상기 수신된 응답 코드를 분석하여 상기 분석이 요구되는 이벤트의 유효성 여부를 결정하는 것을 특징으로 하는 유효성 검증 서버.

[청구항 13] 제8항에 있어서,
상기 적어도 하나의 프로세서는,
상기 등록된 이벤트에 대한 유효성 여부를 지정할 수 있는 사용자 인터페이스를 제공하는 것
을 특징으로 하는 유효성 검증 서버.

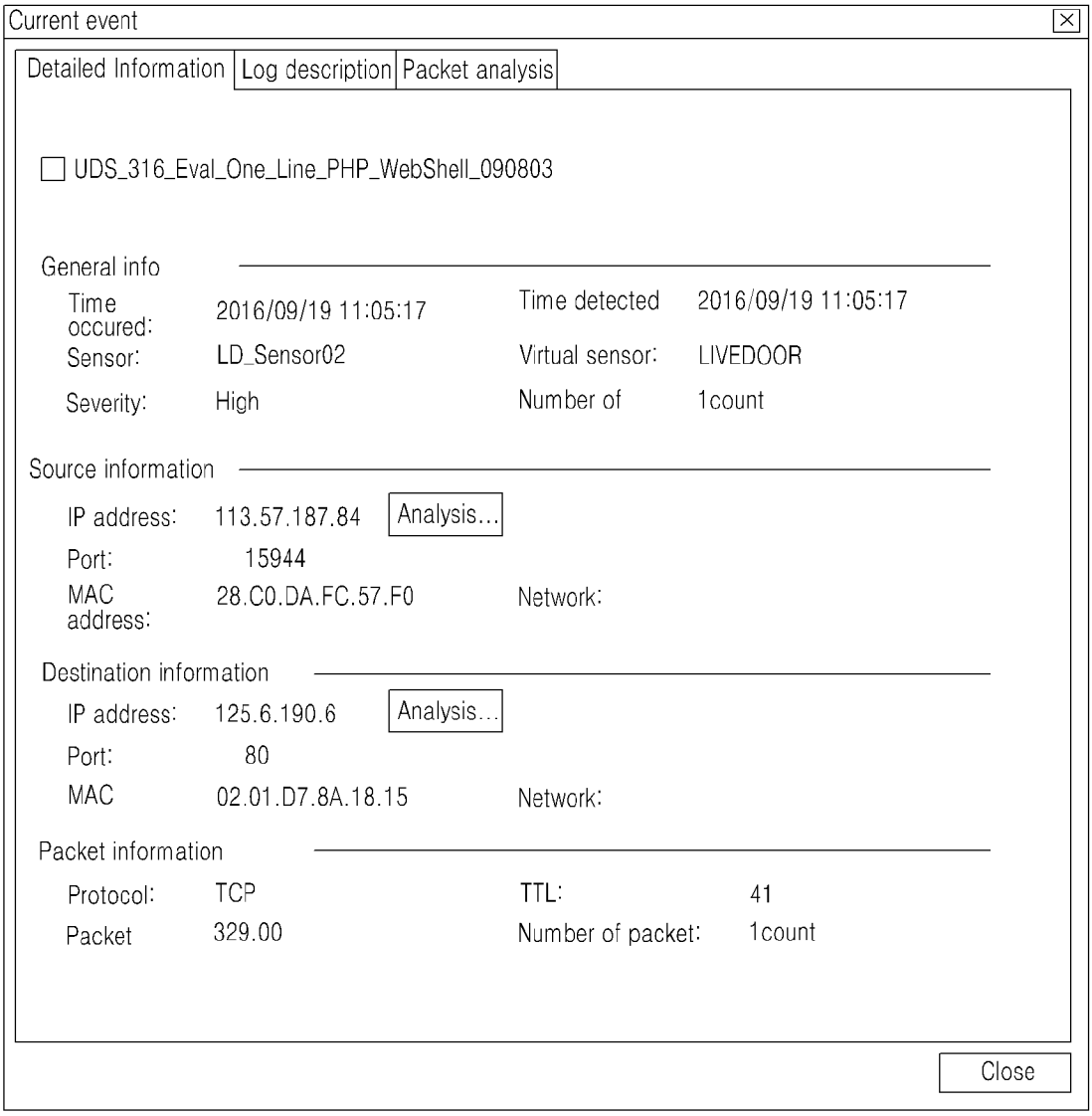
[도1]


110
120
130
160
IDS/IPS
Deepsecurity
SEPM
U
보안 장비의
데이터베이스
네트워크
170
140
150
①
②
③
④
⑤
⑥
⑦
⑧
⑨

[도2]


Attack Type
Signature Group
Severity
Time detected
UDS_316_Eval_One...
User Signature
H High
2016/09/19 11:05:28
UDS_654_SQL_inje...
User Signature
M Medium
2016/09/19 11:05:28
UDS_316_Eval_One...
User Signature
H High
2016/09/19 11:05:27
UDS_316_Eval_One...
User Signature
H High
2016/09/19 11:05:18
UDS_654_SQL_inje...
User Signature
M Medium
2016/09/19 11:05:18
UDS_316_Eval_One...
User Signature
H High
2016/09/19 11:05:17
Source IP
Attacker port
Destination IP
Destination port
113.57.187.84
TCP/15970
12.6.190.6
TCP/80
113.57.187.84
TCP/7512
12.6.190.6
TCP/80
113.57.187.84
TCP/15944
12.6.190.6
TCP/80
113.57.187.84
TCP/15979
12.6.190.6
TCP/80
113.57.187.84
TCP/7512
12.6.190.6
TCP/80
113.57.187.84
TCP/15944
12.6.190.6
TCP/80

[도3]


Current event
Detailed Information
Log description
Packet analysis
UDS_316_Eval_One_Line_PHP_WebShell_090803
General info
Time occured:
2016/09/19 11:05:17
Time detected
2016/09/19 11:05:17
Sensor:
LD_Sensor02
Virtual sensor:
LIVEDOOR
Severity:
High
Number of
1count
Source information
IP address:
113.57.187.84
Analysis...
Port:
15944
MAC address:
28.C0.DA.FC.57.F0
Network:
Destination information
IP address:
125.6.190.6
Analysis...
Port:
80
MAC
02.01.D7.8A.18.15
Network:
Packet information
Protocol:
TCP
TTL:
41
Packet
329.00
Number of packet:
1count
Close

[도4]

[도5]

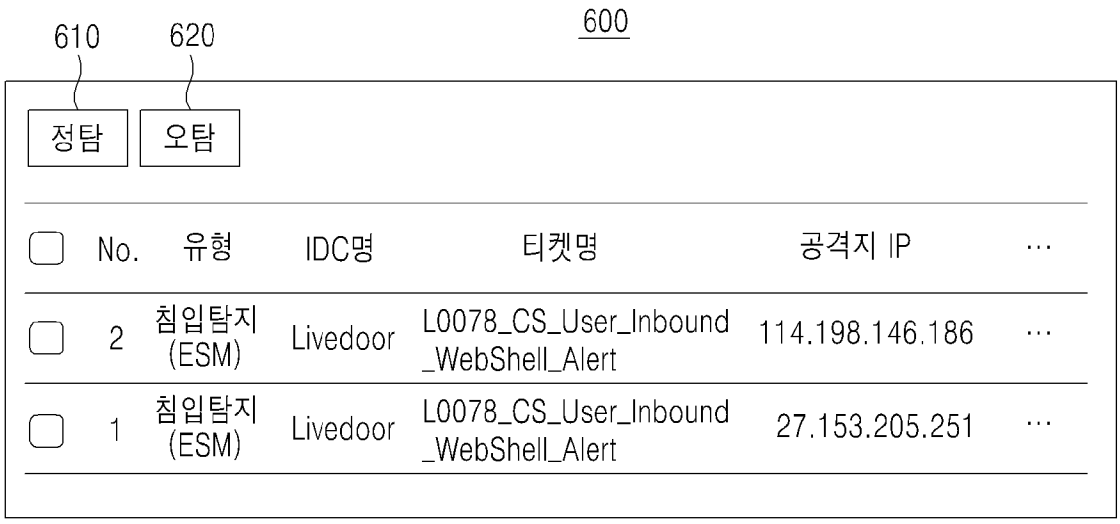
Events

	endTime	name	sourceAddress	···
	2016/09/19 11:05:17	L0078_CS_User_Inb...	113.57.187.84	···

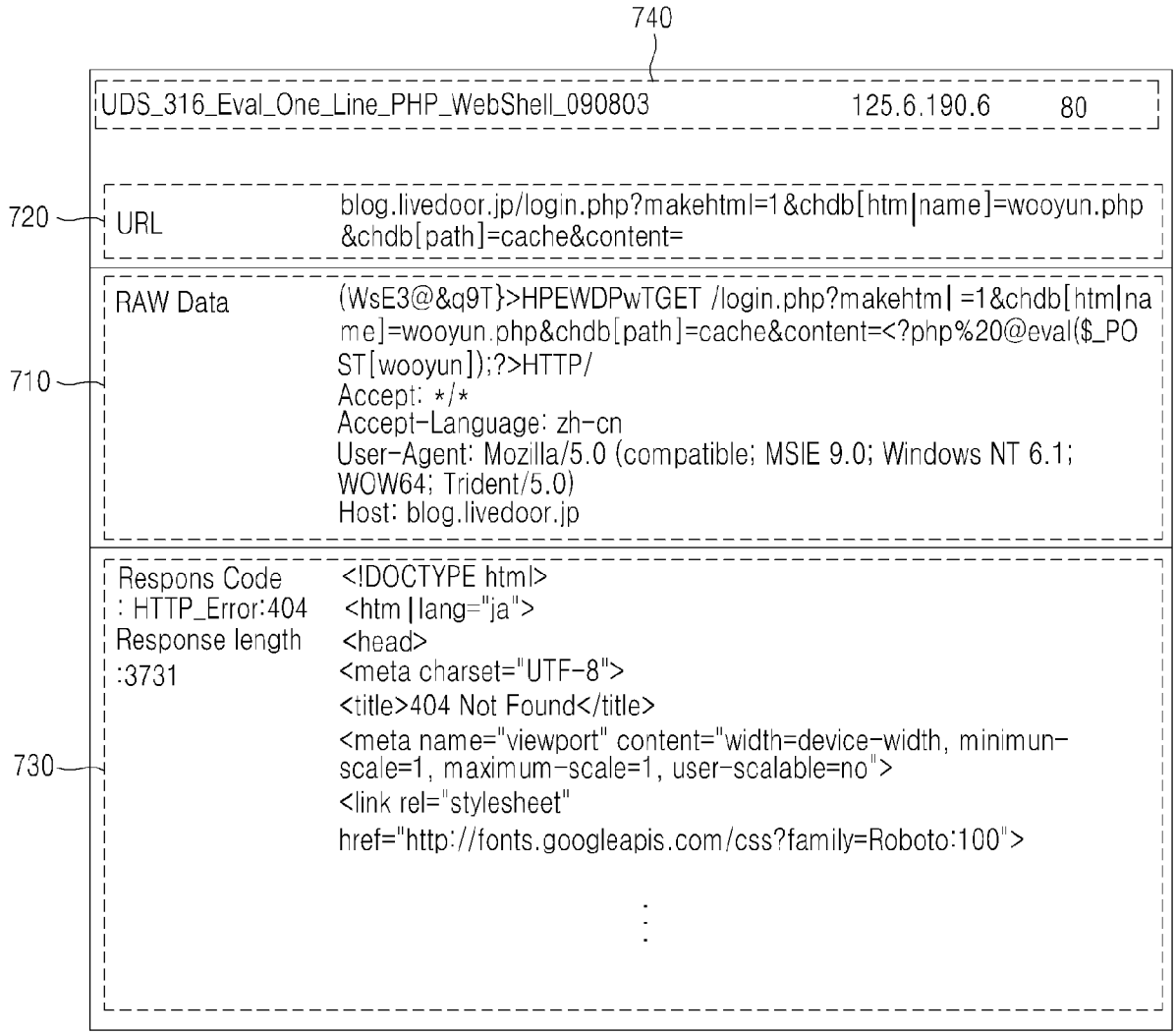
RAW CEF : 0|ArcSight|ArcSight|6.5.1.2083.2|rule : 102|L0078_CS_User_In BounD_WebShel_Alert|High|eventID=26993438503 end=1474250717000 mrt=1474250738196 cnt=1 dpt=980 type=2 generAtor=3300076020 priority =7 sRc=113.57.187.84 start=147250717000 sessionID=0 modelConfience =0 severity=0 relevance=10 locality=Local asetCriticality=0 cat=/Rule/Fire

:

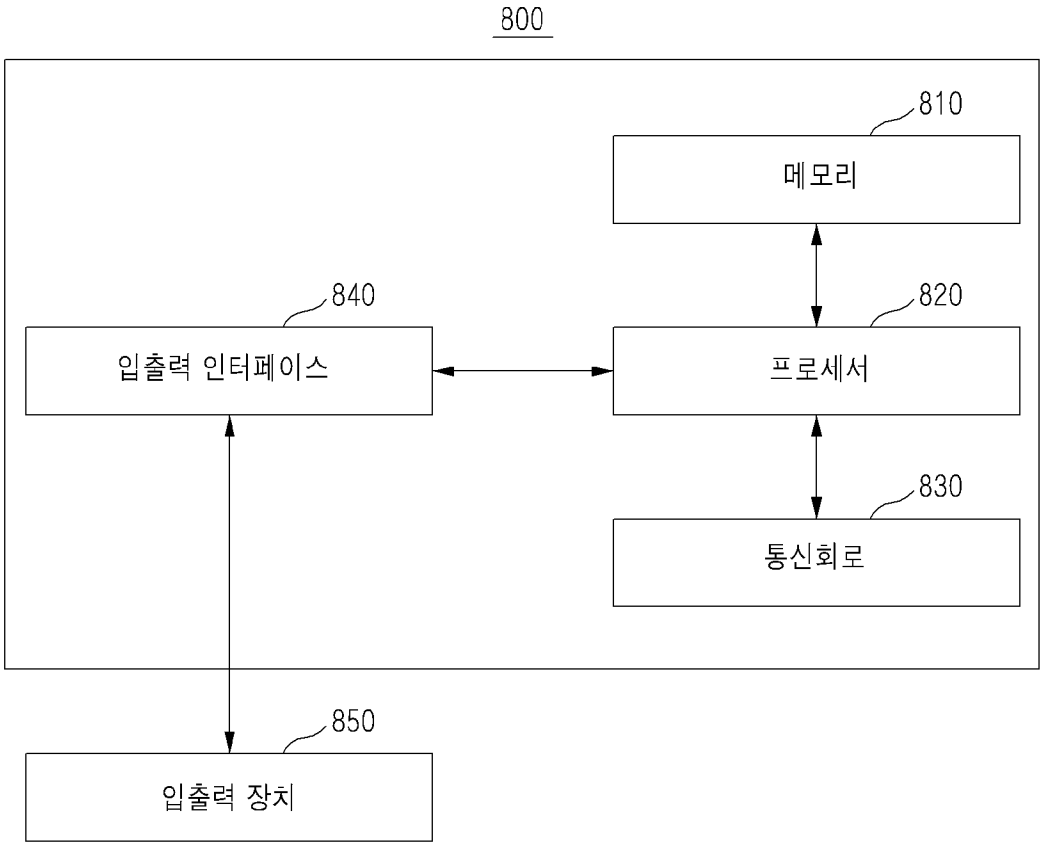
[도6]


600
610
620
정탐
오탐
No.
유형
IDC명
티켓명
공격지 IP
…
2
침입탐지 (ESM)
Livedoor
L0078_CS_User_Inbound _WebShell_Alert
114.198.146.186
…
1
침입탐지 (ESM)
Livedoor
L0078_CS_User_Inbound _WebShell_Alert
27.153.205.251
…

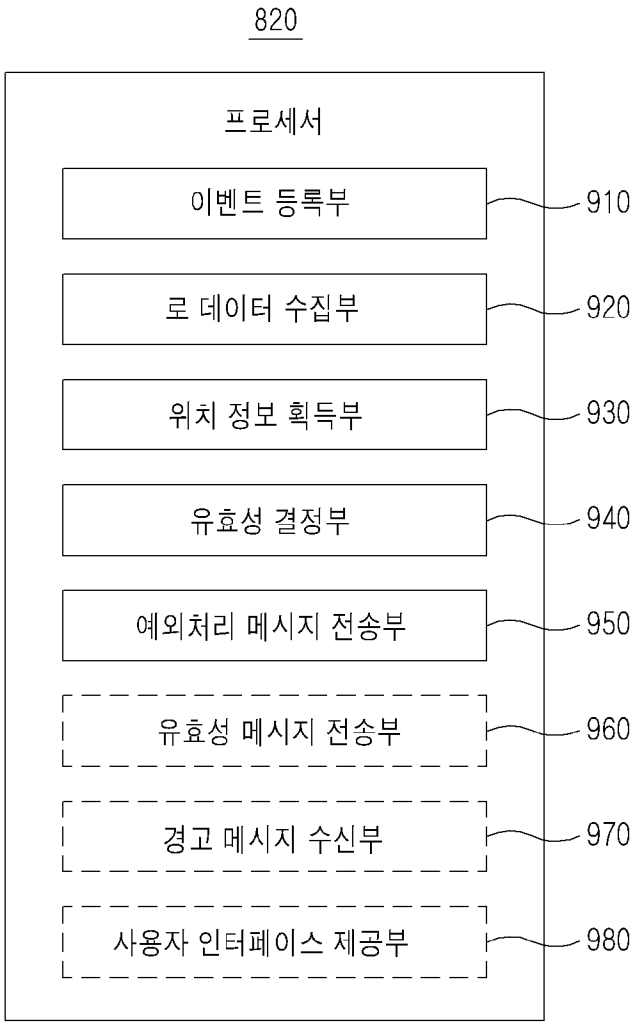
[도7]


740
UDS_316_Eval_One_Line_PHP_WebShell_090803
125.6.190.6
80
720
URL
blog.livedoor.jp/login.php?makehtml=1&chdb[htm|name]=wooyun.php &chdb[path]=cache&content=
710
RAW Data
(WsE3@&q9T}>HPEWDPwTGET /login.php?makehtm| =1&chdb[htm|name]=wooyun.php&chdb[path]=cache&content=<?php%20@eval($_POST[wooyun]);?>HTTP/
Accept: */*
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: blog.livedoor.jp
730
Respons Code : HTTP_Error:404
Response length :3731
<!DOCTYPE html>
<htm |lang="ja">
<head>
<meta charset="UTF-8">
<title>404 Not Found</title>
<meta name="viewport" content="width=device-width, minimun-scale=1, maximum-scale=1, user-scalable=no">
<link rel="stylesheet"
href="http://fonts.googleapis.com/css?family=Roboto:100">
⋮

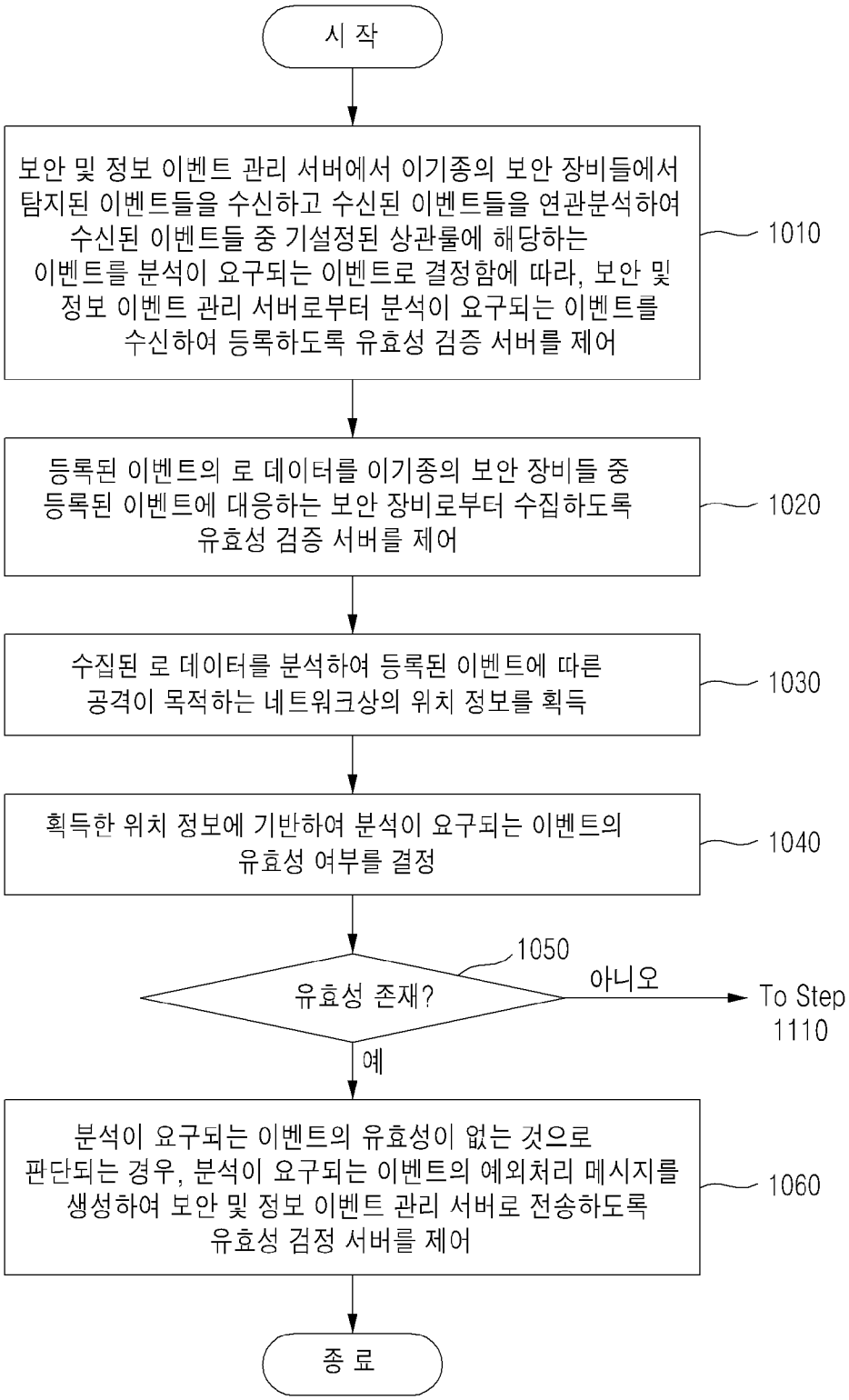
[도8]



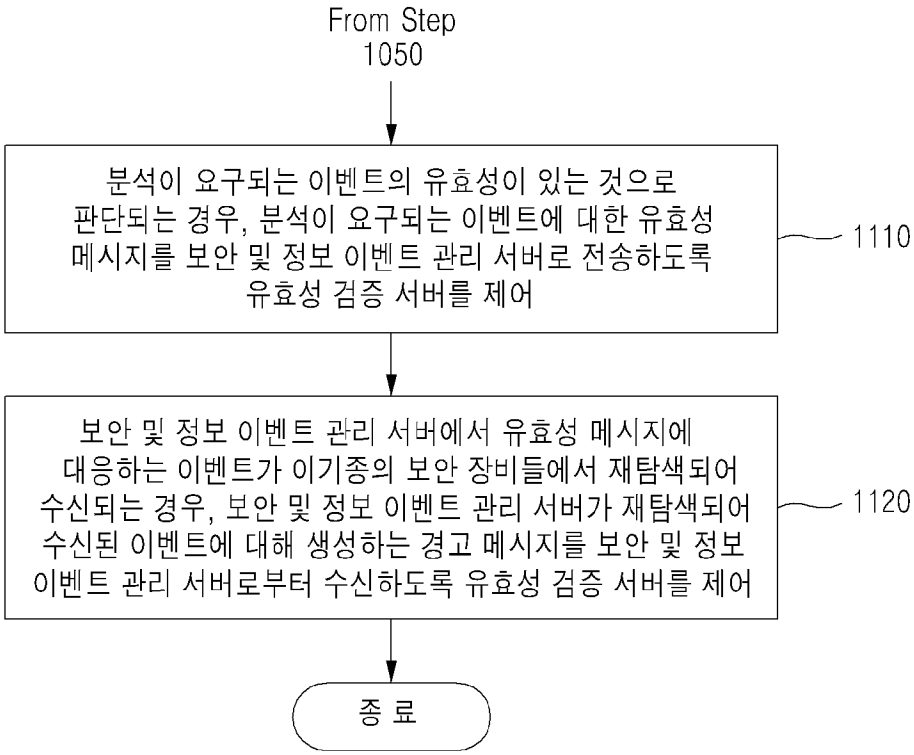
[도9]


820
프로세서
이벤트 등록부
910
로 데이터 수집부
920
위치 정보 획득부
930
유효성 결정부
940
예외처리 메시지 전송부
950
유효성 메시지 전송부
960
경고 메시지 수신부
970
사용자 인터페이스 제공부
980

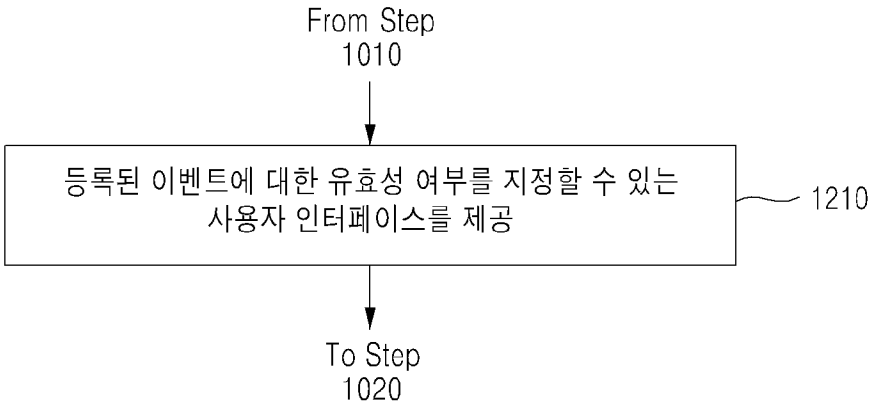
[도10]


시 작
보안 및 정보 이벤트 관리 서버에서 이기종의 보안 장비들에서 탐지된 이벤트들을 수신하고 수신된 이벤트들을 연관분석하여 수신된 이벤트들 중 기설정된 상관룰에 해당하는 이벤트를 분석이 요구되는 이벤트로 결정함에 따라, 보안 및 정보 이벤트 관리 서버로부터 분석이 요구되는 이벤트를 수신하여 등록하도록 유효성 검증 서버를 제어
1010
등록된 이벤트의 로 데이터를 이기종의 보안 장비들 중 등록된 이벤트에 대응하는 보안 장비로부터 수집하도록 유효성 검증 서버를 제어
1020
수집된 로 데이터를 분석하여 등록된 이벤트에 따른 공격이 목적하는 네트워크상의 위치 정보를 획득
1030
획득한 위치 정보에 기반하여 분석이 요구되는 이벤트의 유효성 여부를 결정
1040
1050
유효성 존재?
아니오
To Step 1110
예
분석이 요구되는 이벤트의 유효성이 없는 것으로 판단되는 경우, 분석이 요구되는 이벤트의 예외처리 메시지를 생성하여 보안 및 정보 이벤트 관리 서버로 전송하도록 유효성 검정 서버를 제어
1060
종 료

[도11]


From Step
1050
분석이 요구되는 이벤트의 유효성이 있는 것으로 판단되는 경우, 분석이 요구되는 이벤트에 대한 유효성 메시지를 보안 및 정보 이벤트 관리 서버로 전송하도록 유효성 검증 서버를 제어
1110
보안 및 정보 이벤트 관리 서버에서 유효성 메시지에 대응하는 이벤트가 이기종의 보안 장비들에서 재탐색되어 수신되는 경우, 보안 및 정보 이벤트 관리 서버가 재탐색되어 수신된 이벤트에 대해 생성하는 경고 메시지를 보안 및 정보 이벤트 관리 서버로부터 수신하도록 유효성 검증 서버를 제어
1120
종 료

[도12]


From Step
1010
등록된 이벤트에 대한 유효성 여부를 지정할 수 있는 사용자 인터페이스를 제공
1210
To Step
1020

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2016/013526

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, H04L 12/26(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/06; H04W 12/12; H04L 12/28; H04L 12/22; H04L 12/56; G06F 21/00; G06F 11/00; H04L 12/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: event, detection, security, location, validation, exception handling

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2011-0006175 A (AGENCY FOR DEFENSE DEVELOPMENT) 20 January 2011 See paragraphs [0013], [0026]-[0029]; and figures 1, 3-4.	1-13
A	KR 10-2004-0042397 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 20 May 2004 See pages 2-3; and figure 1.	1-13
A	KR 10-2011-0022141 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 07 March 2011 See paragraphs [0112]-[0124]; and figures 6a-6b.	1-13
A	KR 10-2001-0079361 A (KIM, Sang Wook) 22 August 2001 See page 4; and figures 4-5.	1-13
A	US 2013-0160122 A1 (CHOI, Young-Han et al.) 20 June 2013 See paragraphs [0049]-[0066]; and figure 3.	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 JULY 2017 (20.07.2017)	**24 JULY 2017 (24.07.2017)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. +82-42-481-8578	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2016/013526

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2011-0006175 A	20/01/2011	NONE	
KR 10-2004-0042397 A	20/05/2004	KR 10-0456635 B1	10/11/2004
		US 2004-0098618 A1	20/05/2004
		US 7200866 B2	03/04/2007
KR 10-2011-0022141 A	07/03/2011	KR 10-1250899 B1	04/04/2013
KR 10-2001-0079361 A	22/08/2001	NONE	
US 2013-0160122 A1	20/06/2013	KR 10-1280910 B1	02/07/2013
		KR 10-2013-0068631 A	26/06/2013
		US 8732833 B2	20/05/2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2016/013526

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i, H04L 12/26(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; H04W 12/12; H04L 12/28; H04L 12/22; H04L 12/56; G06F 21/00; G06F 11/00; H04L 12/26

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 이벤트, 탐지, 보안, 위치, 유효성, 예외처리

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2011-0006175 A (국방과학연구소) 2011.01.20 단락 [0013], [0026]-[0029]; 및 도면 1, 3-4 참조.	1-13
A	KR 10-2004-0042397 A (한국전자통신연구원) 2004.05.20 페이지 2-3; 및 도면 1 참조.	1-13
A	KR 10-2011-0022141 A (한국전자통신연구원) 2011.03.07 단락 [0112]-[0124]; 및 도면 6a-6b 참조.	1-13
A	KR 10-2001-0079361 A (김상욱) 2001.08.22 페이지 4; 및 도면 4-5 참조.	1-13
A	US 2013-0160122 A1 (YOUNG-HAN CHOI 등) 2013.06.20 단락 [0049]-[0066]; 및 도면 3 참조.	1-13

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2017년 07월 20일 (20.07.2017)	2017년 07월 24일 (24.07.2017)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
이은규
전화번호 +82-42-481-3580

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2016/013526

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2011-0006175 A	2011/01/20	없음	
KR 10-2004-0042397 A	2004/05/20	KR 10-0456635 B1	2004/11/10
		US 2004-0098618 A1	2004/05/20
		US 7200866 B2	2007/04/03
KR 10-2011-0022141 A	2011/03/07	KR 10-1250899 B1	2013/04/04
KR 10-2001-0079361 A	2001/08/22	없음	
US 2013-0160122 A1	2013/06/20	KR 10-1280910 B1	2013/07/02
		KR 10-2013-0068631 A	2013/06/26
		US 8732833 B2	2014/05/20