(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년12월23일
(11) 등록번호 10-1689295
(24) 등록일자 2016년12월19일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/22* (2006.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 63/30 (2013.01)
H04L 12/22 (2013.01)
(21) 출원번호 10-2016-0017257
(22) 출원일자 2016년02월15일
심사청구일자 2016년02월15일
(30) 우선권주장
62/243,143 2015년10월19일 미국(US)
(56) 선행기술조사문헌
논문(Automated Verification Methodology of Security Events Based on Heuristic Analysis", 2015.09.27.)*
논문(효율적인 보안관제 수행을 위한 다크넷 트래픽 기반 악성 URL 수집 및 분석방법 연구, 2014.12.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
송중석
대전광역시 유성구 온천북로 41, 1005호(봉명동, 모나빌)
최장원
대전광역시 서구 둔산북로 215, 7동 1408호(둔산동, 가람아파트)
(뒷면에 계속)
(74) 대리인
김용인, 지관영

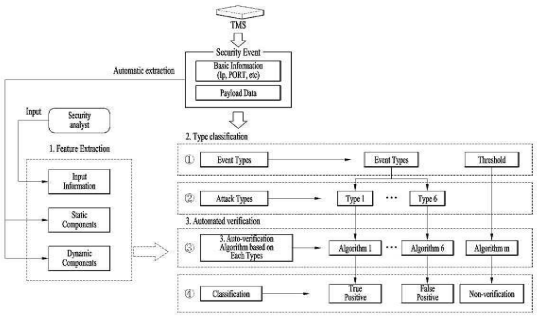
전체 청구항 수 : 총 13 항 심사관 : 김상인

(54) 발명의 명칭 **보안이벤트 자동 검증 방법 및 장치**

(57) 요 약

본 발명은 보안이벤트 자동 검증 방법 및 장치에 관한 것이다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법은 보안이벤트 및 보안이벤트와 관련된 정보를 입력받는 단계, 보안이벤트의 특성을 추출하는 단계, 보안이벤트를 분류하는 단계 및 보안이벤트를 검증하는 단계 포함한다.

대 표 도 - 도2



(52) CPC특허분류
H04L 63/1408 (2013.01)
H04L 63/1441 (2013.01)
H04L 67/02 (2013.01)
(72) 발명자
최상수
대전광역시 유성구 노은로 353, 303동 1507호(하기동, 송림마을3단지아파트)
김희석
대전광역시 유성구 지족북로 33, 107동 1301호(지족동, 한화꿈에그린 1블럭)
최지연
대전광역시 유성구 송강로42번길 61, 309동 802호(송강동, 송강청솔아파트)
이윤수
대전광역시 유성구 동서대로 725, 1202동 1003호(원신흥동, 어울림하트)

명 세 서

청구범위

청구항 1

탐지규칙 기반 보안장비에 의해 공격으로 탐지된 보안이벤트 및 상기 보안이벤트와 관련된 정보를 입력받는 단계;

상기 입력된 보안이벤트의 특성을 추출하는 단계;

상기 보안이벤트가 시그니처 기반의 보안이벤트인 경우, 상기 보안이벤트의 공격 유형에 따라 분류하는 단계; 및

상기 분류된 보안이벤트가 악성 URL 유형인 경우, 상기 악성 URL 유형에 대한 자동 검증 알고리즘에 따라 상기 추출된 보안이벤트의 특성과 상기 입력된 보안이벤트와 관련된 정보를 비교하여 상기 탐지된 보안이벤트가 정탐인지 여부를 검증하는 단계;

를 포함하는 보안이벤트 자동 검증 방법으로서,

상기 보안이벤트의 특성은 상기 보안이벤트의 검증을 위해 필수적인 정적 요소 및 상기 보안이벤트의 검증을 위해 부수적인 동적 요소를 포함하고,

상기 정적 요소는 출발지 IP (source IP) 정보, 목적지 IP (destination IP) 정보, 출발지 포트 (source port) 정보, 목적지 포트 (destination port) 정보, 호스트 (host) 정보, 페이로드 (payload) 정보, HTTP 레퍼러 (hypertext transfer protocol referer) 정보 및 보안이벤트의 개수 정보 중 적어도 하나를 포함하고, 상기 동적 요소는 호스트 및 GET URL 정보, 웹사이트 소스 코드 (Website source code) 정보 및 목적지 포트 (Destination port) 정보 중 적어도 하나를 포함하고,

상기 입력된 보안이벤트와 관련된 정보는 상기 보안이벤트의 검증을 위해 필수적인 필수 요소 및 상기 보안이벤트의 검증을 위해 부수적인 보조 요소를 포함하고,

상기 필수 요소는 공격의 대상이 되는 기관의 IP 주소의 목록을 나타내는 기관 IP 리스트 (Institute IP list) 정보를 포함하고, 상기 보조 요소는 공격에 사용되는 악성 IP 주소인 블랙 IP 주소의 목록을 나타내는 블랙 IP 리스트 (Black IP list) 정보, 정상적인 통신에 사용되는 IP 주소인 화이트 IP 주소의 목록을 나타내는 화이트 IP 리스트 (White IP list) 정보, 공격에 사용되는 호스트의 도메인 네임인 블랙 FQDN (Fully Qualified Domain Name)의 목록을 나타내는 블랙 FQDN 리스트 (Black FQDN list) 정보, 정상적인 통신에 사용되는 호스트의 도메인 네임인 화이트 FQDN의 목록을 나타내는 화이트 FQDN 리스트 (White FQDN list) 정보 및 특정 문자열 리스트 정보 중 적어도 하나를 포함하고,

상기 특정 문자열 리스트 정보는 올바로 탐지된 보안이벤트임을 나타내는 특정 문자열 정보를 포함하고,

상기 자동 검증 알고리즘은 상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있는지 여부를 확인하는 단계, 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있는지 여부를 확인하는 단계 및 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있는지 여부를 확인하는 단계를 포함하는 보안이벤트 자동 검증 방법.

청구항 2

제 1 항에 있어서, 상기 자동 검증 알고리즘은

상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있는지 여부를 확인하는 단계;

상기 레퍼러 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있는지 여부를 확인하는 단계;

상기 레퍼러 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있는지 여부를 확인하는 단계; 및

상기 보안이벤트의 출발지 IP에 의해 요청되는 호스트 및 GET URL이 존재하고 상기 호스트 및 GET URL에 접근이 가능한지 여부를 확인하는 단계;

를 포함하는 보안이벤트 자동 검증 방법.

청구항 3

제 2 항에 있어서, 상기 자동 검증 알고리즘은

상기 웹사이트 소스 코드가 상기 올바로 탐지된 보안이벤트임을 나타내는 특정 문자열 정보를 포함하는지 여부를 확인하는 단계를 포함하는 보안이벤트 자동 검증 방법.

청구항 4

제 1 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있지 않으면, 상기 탐지된 보안이벤트는 오탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 5

제 1 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있으면, 상기 탐지된 보안이벤트는 정탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 6

제 1 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있으면, 상기 탐지된 보안이벤트는 오탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 7

제 2 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있고 상기 레퍼러 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있으면, 상기 탐지된 보안이벤트는 오탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 8

제 2 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있고 상기 레퍼러 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 레퍼러 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있으면, 상기 탐지된 보안이벤트는 정탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 9

제 2 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있고 상기 레퍼러 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 레퍼러 정보가 상기 블랙

FQDN 리스트 정보에 포함되어 있지 않으면, 상기 탐지된 보안이벤트는 추가 분석이 필요한 것으로 판별되는 보안이벤트 자동 검증 방법.

청구항 10

제 2 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있지 않고 상기 보안이벤트의 출발지 IP 정보에 의해 요청되는 호스트 및 GET URL이 존재하지 않거나 상기 호스트 및 GET URL에 접근이 불가능하면, 상기 탐지된 보안이벤트는 정탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 11

제 3 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있지 않고 상기 보안이벤트의 출발지 IP 정보에 의해 요청되는 호스트 및 GET URL이 존재하고 상기 호스트 및 GET URL에 접근이 가능하고 상기 웹사이트 소스 코드가 상기 올바로 탐지된 보안이벤트임을 나타내는 특정 문자열 정보를 포함하면, 상기 탐지된 보안이벤트는 정탐으로 판별되는 보안이벤트 자동 검증 방법.

청구항 12

제 3 항에 있어서, 상기 자동 검증 알고리즘에 따라,

상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있고 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있지 않고 상기 보안이벤트 내에 상기 보안이벤트가 참조하는 레퍼러 정보가 포함되어 있지 않고 상기 보안이벤트의 출발지 IP 정보에 의해 요청되는 호스트 및 GET URL이 존재하고 상기 호스트 및 GET URL에 접근이 가능하고 상기 웹사이트 소스 코드가 상기 올바로 탐지된 보안이벤트임을 나타내는 특정 문자열 정보를 포함하지 않으면, 상기 탐지된 보안이벤트는 추가 분석이 필요한 것으로 판별되는 보안이벤트 자동 검증 방법.

청구항 13

탐지규칙 기반 보안장비에 의해 공격으로 탐지된 보안이벤트 및 상기 보안이벤트와 관련된 정보를 입력받는 입력 모듈;

상기 입력된 보안이벤트의 특성을 추출하는 특성 추출 모듈;

상기 보안이벤트가 시그니처 기반의 보안이벤트인 경우, 상기 보안이벤트의 공격 유형에 따라 분류하는 유형 분류 모듈; 및

상기 분류된 보안이벤트가 악성 URL 유형인 경우, 상기 악성 URL 유형에 대한 자동 검증 알고리즘에 따라 상기 추출된 보안이벤트의 특성과 상기 입력된 보안이벤트와 관련된 정보를 비교하여 상기 탐지된 보안이벤트가 정탐인지 여부를 검증하는 자동 검증 모듈;

를 포함하는 보안이벤트 자동 검증 장치로서,

상기 보안이벤트의 특성은 상기 보안이벤트의 검증을 위해 필수적인 정적 요소 및 상기 보안이벤트의 검증을 위해 부수적인 동적 요소를 포함하고,

상기 정적 요소는 출발지 IP (source IP) 정보, 목적지 IP (destination IP) 정보, 출발지 포트 (source port) 정보, 목적지 포트 (destination port) 정보, 호스트 (host) 정보, 페이로드 (payload) 정보, HTTP 레퍼러 (hypertext transfer protocol referer) 정보 및 보안이벤트의 개수 정보 중 적어도 하나를 포함하고, 상기 동적 요소는 호스트 및 GET URL 정보, 웹사이트 소스 코드 (Website source code) 정보 및 목적지 포트

(Destination port) 정보 중 적어도 하나를 포함하고,

상기 입력된 보안이벤트와 관련된 정보는 상기 보안이벤트의 검증을 위해 필수적인 필수 요소 및 상기 보안이벤트의 검증을 위해 부수적인 보조 요소를 포함하고,

상기 필수 요소는 공격의 대상이 되는 기관의 IP 주소의 목록을 나타내는 기관 IP 리스트 (Institute IP list) 정보를 포함하고, 상기 보조 요소는 공격에 사용되는 악성 IP 주소인 블랙 IP 주소의 목록을 나타내는 블랙 IP 리스트 (Black IP list) 정보, 정상적인 통신에 사용되는 IP 주소인 화이트 IP 주소의 목록을 나타내는 화이트 IP 리스트 (White IP list) 정보, 공격에 사용되는 호스트의 도메인 네임인 블랙 FQDN (Fully Qualified Domain Name)의 목록을 나타내는 블랙 FQDN 리스트 (Black FQDN list) 정보, 정상적인 통신에 사용되는 호스트의 도메인 네임인 화이트 FQDN의 목록을 나타내는 화이트 FQDN 리스트 (White FQDN list) 정보 및 특정 문자열 리스트 정보 중 적어도 하나를 포함하고,

상기 특정 문자열 리스트 정보는 올바로 탐지된 보안이벤트임을 나타내는 특정 문자열 정보를 포함하고,

상기 자동 검증 알고리즘은 상기 보안이벤트의 출발지 IP 정보가 상기 기관 IP 리스트 정보에 포함되어 있는지 여부를 확인하는 단계, 상기 보안이벤트의 호스트 정보가 상기 블랙 FQDN 리스트 정보에 포함되어 있는지 여부를 확인하는 단계 및 상기 보안이벤트의 호스트 정보가 상기 화이트 FQDN 리스트 정보에 포함되어 있는지 여부를 확인하는 단계를 포함하는 보안이벤트 자동 검증 장치.

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 보안이벤트를 자동 검증하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 기존에 대용량 보안이벤트에 대한 탐지 및 분석 업무의 효율성을 향상시키기 위한 다양한 연구가 국내/외에서 진행되어 왔으나, 이들 연구의 대부분은 보안이벤트에 대한 기본정보 (IP, 포트, 프로토콜, 이벤트 명 등)만을 이용하여 사이버 위협 동향 파악 및 분석 대상 보안이벤트 수를 감소시키기 위한 간접적 접근 (통계분석, 가시화 등)에 초점을 맞추고 있었다. 따라서, 보안이벤트에 대한 실제 해킹공격 발생여부를 판단하기 어렵기 때문에 보안 관제 업무 수행 시 추가적인 분석이 필요하였다.

[0003] 기존 연구는 대용량 보안이벤트에 대한 자동 분석을 위해 주로 데이터 마이닝 및 기계 학습 기술을 적용하고 있으나, 이러한 접근 방법은 근본적으로 정확도가 떨어지는 문제점이 존재한다. 하지만, 사이버 해킹 공격의 경우 탐지 및 분석 정확도가 매우 중요하기 때문에, 해당 기술을 사이버 안전 센터에 실제로 적용하기는 어려움이 존재하였다.

[0004] 현재 지속적인 사이버 위협 시도 증가에 따라 대량의 보안이벤트가 발생하는 상황이고, 국내 보안 관제 체계에서는 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)에서 발생하는 보안이벤트를 보안 관제 요원에 의한 수동 분석 및 경험에 의존하는 상황이다. 나아가, 보안 관제 결과 도출 시 특정 유형에 분석이 편중되는 현상 발생하고 있다.

[0005] 나아가, 현재 정부 주도형 중앙 집중식 보안 관제 체계는 사이버 해킹 공격을 탐지하기 위한 탐지 패턴을 공유하고, 이를 토대로 신속한 침해공격 탐지 및 대응을 수행하는 범국가 차원의 일원화된 해킹사고 공조체계 구축하는데 초점이 맞춰져 있다. 하지만, 이러한 패턴 기반의 보안 관제 체계는 이 도면에 도시된 바와 같은 한계점을 가질 수 있다. 현재 사이버 위협 급증에 따라 탐지 패턴에 의해 발생하는 보안이벤트는 폭발적이고 지속적으로 증가하고 있다. 하지만, 보안관제 요원이 해당 보안이벤트에 대한 실제 공격 여부를 판단하기 위하여 모든 보안이벤트를 분석하는 것은 현실적으로 불가능하다. 예를 들면, 보안 관제 요원은 1분당 수백에서 수천 건의 보안이벤트를 분석해야하기 때문에 보안 관제의 신속성 및 정확성이 저하되고 있다. 또한, 현재의 보안 관제 업무는 보안 관제 요원이 보유한 전문 지식 및/또는 경험에 전적으로 의존하고 있기 때문에, 특정 보안이벤트에 대한 분석에만 집중되는 업무 편중 현상이 발생할 수 있다. 이에 따라, 기존에 알려지지 않은 새로운 해킹 공격 기술에 대한 대응 능력이 부족한 실정이다.

[0006] 기존의 탐지 패턴 기반의 보안 관제에서, 탐지 패턴을 기반으로 함으로써 탐지 패턴을 우회하는 신종 또는 변종 공격이 증가하고, 탐지 패턴이 없는 알려진 공격에도 대응할 수 없는 문제점이 있다. 나아가, 텍스트를 기반으로 함으로써 사이버 위협 급증에 따른 탐지 및/또는 분석 업무량이 증가하고, 대용량 사이버 공격에 대해 직관적으로 인지하기가 어렵다는 문제점이 있다. 나아가, 인간이 보안 관제를 함으로써 출현 빈도가 높고 이력이 있는 분석에만 많은 시간을 소비하고, 개인별 분석 수준에 따른 서비스 질의 차이가 발생하는 문제점이 있다.

발명의 내용

해결하려는 과제

[0007] 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)보안이벤트본 발명이 이루고자 하는 과제는, 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)에서 공격으로 탐지된 보안이벤트의 특성을 추출하는 방법을 제공하는 것이다.

[0008] 본 발명이 이루고자 하는 과제는, 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)에서 공격으로 탐지된 보안이벤트를 공격 유형에 따라 분류하는 방법을 제공하는 것이다.

[0009] 본 발명이 이루고자 하는 과제는, 각 공격 유형에 따른 알고리즘을 적용하여 보안이벤트를 자동 검증하는 방법을 제공하는 것이다.

과제의 해결 수단

[0010] 본 발명의 목적에 따라, 여기에 포함되고 대략적으로 기재된 바와 같이, 본 발명은 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)에 의해 공격으로 탐지된 보안이벤트들이 정탐(실제 공격에 의해 발생한 보안이벤트)인지 여부를 자동적으로 검증하는 방안을 제안한다.

발명의 효과

[0011] 보안장비탐지규칙 기반 보안장비(IDS/IPS, TMS 등)가 탐지한 보안이벤트를 자동으로 검증하여 정탐(실제 공격에 의해 발생한 보안이벤트)과 오탐(정상 통신에 의해 발생한 보안이벤트)으로 판별함으로써 해당 보안장비의 효율성을 극대화할 수 있는 효과가 있다.

[0012] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법 및 장치에 따르면, 탐지 패턴을 우회하는 신종 또는 변종 공격이 증가하고, 탐지 패턴이 없는 알려진 공격에도 대응할 수 있는 효과가 있다.

[0013] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법 및 장치에 따르면, 대용량 사이버 공격에 대해 직관적으로 인지할 수 있는 효과가 있다.

[0014] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법 및 장치에 따르면, 각 공격 유형에 따른 알고리즘을 적용하여 높은 수준의 자동 검증 결과를 제공할 수 있는 효과가 있다.

도면의 간단한 설명

[0015] 본 발명에 대해 더욱 이해하기 위해 포함되며 본 출원에 포함되고 그 일부를 구성하는 첨부된 도면은 본 발명의 원리를 설명하는 상세한 설명과 함께 본 발명의 실시예를 나타낸다.

도 1은 본 발명의 일 실시예에 따른 종래 탐지 패턴 기반의 보안 관제를 나타낸 도면이다.

도 2는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치의 대용량 보안이벤트 자동 검증 구조를 나타낸 도면이다.

도 3은 본 발명의 일 실시예에 따른 기본 정보 (basic information)를 나타낸 도면이다.

도 4는 본 발명의 일 실시예에 따른 공격 유형 별 정탐에 해당하는 문자열 리스트를 나타낸 도면이다.

도 5는 본 발명의 일 실시예에 따른 정적 요소 및 동적 요소에 대한 설명을 나타낸 도면이다.

도 6은 본 발명의 일 실시예에 따른 공격 유형의 특성을 나타낸 도면이다.

도 7은 본 발명의 일 실시예에 따른 자동 검증 방법의 전체 프로세스를 나타낸 도면이다.

도 8은 본 발명의 일 실시예에 따른 악성 URL (malicious URL) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

도 9는 본 발명의 일 실시예에 따른 악성 코드 다운로드 (malware download) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

도 10은 본 발명의 일 실시예에 따른 악성코드 감염 (Malware infection) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

도 11은 본 발명의 일 실시예에 따른 정보 전송 (information transmission) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

도 12는 본 발명의 일 실시예에 따른 파일 업로드 (File upload) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

도 13은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트 (Threshold based security event)에 대한 자동 검증 알고리즘을 나타낸 도면이다.

도 14는 본 발명의 일 실시예에 따른 탐지 규칙 (signature rules)의 통계를 나타낸 도면이다.

도 15는 본 발명의 일 실시예에 따른 악성 URL (malicious URL) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

도 16은 본 발명의 일 실시예에 따른 악성 코드 다운로드 (malware download) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

도 17은 본 발명의 일 실시예에 따른 악성코드 감염 (Malware infection) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

도 18은 본 발명의 일 실시예에 따른 정보 전송 (information transmission) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

도 19는 본 발명의 일 실시예에 따른 파일 업로드 (File upload) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

도 20은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트 (threshold based security event)에 대한 자동 검증 방법의 정확도를 나타낸 도면이다.

도 21은 본 발명의 일 실시예에 따른 보안이벤트의 유형을 분류하는 과정을 나타낸 도면이다.

도 22는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 실시예를 상세하게 설명하지만, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다.

[0017] 본 명세서에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어를 선택하였으나, 이는 당분야에 종사하는 기술자의 의도 또는 관례 또는 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 그 의미를 기재할 것이다. 따라서 본 명세서에서 사용되는 용어는, 단순한 용어의 명칭이 아닌 그 용어가 가지는 실질적인 의미와 본 명세서의 전반에 걸친 내용을 토대로 해석되어야 함을 밝혀두고자 한다.

[0019] 도 1은 본 발명의 일 실시예에 따른 종래 탐지 패턴 기반의 보안 관제를 나타낸 도면이다.

[0020] 본 발명의 일 실시예에 따르면, 정부 주도형 중앙집중식 보안관제체계는 사이버 해킹공격을 탐지하기 위한 탐지 패턴을 공유하고, 이를 토대로 신속한 침해공격 탐지 및 대응을 수행하는 범국가 차원의 일원화된 해킹사고 공조체계 구축하는데 초점이 맞춰져 있다. 하지만, 이러한 패턴 기반의 보안 관제 체계는 이 도면에 도시된 바와 같은 한계점을 가질 수 있다. 본 발명의 일 실시예에 따르면, 현재 사이버 위협 급증에 따라 탐지 패턴에 의해 발생하는 보안이벤트는 폭발적이고 지속적으로 증가하고 있다. 하지만, 보안관제 요원이 해당 보안이벤트에 대한 실제 공격 여부를 판단하기 위하여 모든 보안이벤트를 분석하는 것은 현실적으로 불가능하다. 예를 들면, 보안 관제 요원은 1분당 수백에서 수천 건의 보안이벤트를 분석해야하기 때문에 보안 관제의 신속성 및 정확성이 저하되고 있다. 또한, 현재의 보안 관제 업무는 보안 관제 요원이 보유한 전문 지식 및/또는 경험에 전적으로 의존하고 있기 때문에, 특정 보안이벤트에 대한 분석에만 집중되는 업무 편중 현상이 발생할 수 있다. 이에 따라, 기존에 알려지지 않은 새로운 해킹 공격 기술에 대한 대응 능력이 부족한 실정이다.

[0021] 하지만 종래의 탐지 패턴 기반의 보안 관제에서, 탐지 패턴을 기반으로 함으로써 탐지 패턴을 우회하는 신종 또는 변종 공격이 증가하고, 탐지 패턴이 없는 알려진 공격에도 대응할 수 없는 문제점이 있다. 나아가, 텍스트를 기반으로 함으로써 사이버 위협 급증에 따른 탐지 및/또는 분석 업무량이 증가하고, 대용량 사이버 공격에 대해 직관적으로 인지하기가 어렵다는 문제점이 있다. 나아가, 인간이 보안 관제를 함으로써 출현 빈도가 높고 이력이 있는 분석에만 많은 시간을 소비하고, 개인별 분석 수준에 따른 서비스 질의 차이가 발생하는 문제점이 있다.

[0022] 따라서 본 발명에서는 대용량 보안 이벤트에 대한 자동 분석을 통해 실제 공격 및/또는 피해 여부를 신속하고 정확하게 판단하고 차세대 보안 관제 및 침해 대응을 수행하기 위한 정적 및/또는 동적 분석 기반의 보안 이벤트 자동 검증을 수행할 수 있는 보안 이벤트 자동 검증 장치를 제안한다.

[0023] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 차세대 보안 관제 기술을 통해 전주기적 침해 사고에 대응할 수 있는 역량을 강화할뿐만 아니라 핵심적인 연구 정보 자원을 이용하는 이용자가 안전하게 연구할 수 있는 환경을 제공할 수 있다. 나아가, 선진 보안 관제 인프라 구축 및/또는 운용에 대한 핵심 기술 및 노하우를 타 부문 관제 센터에 전파함으로써 공공의 이익에 공헌할 수 있다. 또한, 신종 해킹 공격, 변종 해킹 공격 및/또는 대용량 해킹 공격의 탐지를 위한 원천 기술을 이용하여 핵심적인 연구 자료의 유출을 원천 봉쇄할 수 있다. 이로써, 경제적 손실 최소화 및/또는 국가 경쟁력 향상에 기여할 수 있다.

[0024] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 기존의 인적 기반에서 시스템 기반의 보안 관제로 전환하기 위한 보안 관제 요원의 해킹 공격 탐지 및/또는 분석 노하우를 정형화 및/또는 자동화함으로써 국가 차원의 보안 관제 및/또는 침해 대응 체계를 수행할 수 있다.

[0025] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 임계치 기반의 보안이벤트 자동 검증 기술을 제공할 수 있다. 보다 구체적으로, 과학 기술 사이버 안전 센터 (S&T-SEC)에서 구축 및/또는 운용 중인 침해 위협 관리 시스템 (TMS)을 활용하여 임계치 기반으로 사고 처리한 보안이벤트의 특성을 통계적으로 분석하고 분류하여 보안이벤트 탐지 결과가 정탐인지 오탐인지 판별하고 이로써 보안이벤트를 자동 검증할 수 있다.

[0026] 본 발명의 다른 일 실시예에 따른 보안이벤트 자동 검증 장치는 공격 유형별 보안 이벤트 자동 검증 기술을 제공할 수 있다. 보다 구체적으로, 사이버 공격의 유형 예시(악성 URL, 악성코드 다운로드, 악성코드 감염, 정보 전송, 파일 업로드) 및 동적 특징 정보를 활용하여 보안이벤트를 자동 검증할 수 있다.

[0028] 도 2는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치의 대용량 보안이벤트 자동 검증 구조를 나타낸

도면이다.

[0029] 본 도면은 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치의 대용량 보안이벤트 자동 검증 방법의 전체 구조를 나타낸다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 대용량 보안이벤트의 자동 검증을 수행하기 위하여 특성 추출 (feature extraction) 모듈, 유형 분류 (type classification) 모듈 및/또는 자동 검증 (automated verification) 모듈을 포함할 수 있다.

[0030] 본 발명의 일 실시예에 따른 특성 추출 모듈은 자동 검증 단계에서 이루어지는 보안이벤트의 자동 검증을 위한 특성들을 추출할 수 있다. 본 발명의 일 실시예에 따라 이 단계에서 추출되는 특성들은 기본 정보 (basic information), 정적 요소 (static item) 및/또는 동적 요소 (dynamic item)를 포함할 수 있다. 본 발명의 일 실시예에 따른 기본 정보는 보안 관제 요원(사용자)에 의해 입력되는 정보를 나타낼 수 있다. 본 발명의 일 실시예에 따른 정적 요소는 보안이벤트에 포함된 정보와 비교를 수행하는 정적 검증을 위해 사용되는 요소를 나타낼 수 있다. 본 발명의 일 실시예에 따른 동적 요소는 외부 시스템으로 접근의 확인 결과를 수행하는 동적 검증을 위해 사용되는 요소를 나타낼 수 있다. 여기서, 기본 정보 (basic information)는 입력 정보 (input information)와 동일한 의미를 가질 수 있다.

[0031] 본 발명의 일 실시예에 따른 유형 분류 모듈은 보안이벤트들을 시그니처 기반 보안이벤트 또는 임계치 기반 보안이벤트로 분류할 수 있다.

[0032] 본 발명의 일 실시예에 따른 시그니처 기반 보안이벤트는 사전에 정의한 문자열 패턴(영문자/숫자/특수기호의 조합 또는 정규표현식)과 동일한 문자열을 포함한 패킷에 의해 발생한 보안이벤트라고 정의할 수 있으며, 임계치 기반 보안이벤트는 특정 패킷이 사전에 정의한 임계치(단위시간 당 발생 빈도)를 초과하여 발생한 보안이벤트를 의미한다.

[0033] 그리고, 유형 분류 모듈은 자동 검증 단계에서 각 공격 유형에 따른 보안이벤트들을 검증하기 위하여 공격 특성들을 기반으로 하여 시그니처 기반 보안이벤트를 5개의 공격 유형들로 분류할 수 있다.

[0034] 본 발명의 일 실시예에 따른 자동 검증 모듈은 특성 추출 단계에서 추출된 특성들을 입력받고, 각 공격 유형을 기반으로 설정된 자동 검증 알고리즘을 이용하여, 공격 유형별로 분류된 시그니처 기반 보안이벤트 및 임계치 기반 보안이벤트들을 검증할 수 있다. 도면에 도시된 바와 같이 검증 결과는 정탐 (true positive), 오탐 (false positive), 미검증 (non-verification) 중 어느 하나에 해당할 수 있다.

[0035] 본 발명의 일 실시예에 따르면, 상술한 특성 추출 모듈, 유형 분류 모듈 및/또는 자동 검증 모듈은 각각 독립적인 기능을 수행하는 하드웨어인 프로세서에 해당할 수 있다.

[0037] 도 3은 본 발명의 일 실시예에 따른 기본 정보 (basic information)를 나타낸 도면이다.

[0038] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 보안이벤트들의 자동 검증을 위하여 먼저 기본 정보, 정적 요소 및/또는 동적 요소를 추출할 수 있다.

[0039] 본 발명의 일 실시예에 따른 기본 정보는 사용자가 입력한 자동검증에 필요한 정보로서, 보안이벤트와 관련된 기관에 대한 정보 또는 도메인 정보등을 포함할 수 있다. 상술한 바와 같이 본 발명의 일 실시예에 따른 자동 검증 모듈은 보안이벤트를 검증할 때, 기본 정보를 정적 요소 및/또는 동적 요소와 비교할 수 있다. 본 도면은 본 발명의 일 실시예에 따른 기본 정보에 포함되는 항목들 및 그 설명을 나타내는 테이블이다. 이하 각 항목을 설명한다.

[0040] 본 발명의 일 실시예에 따르면, 기본 정보는 필수 요소 (essential items) 및/또는 보조 요소 (additional items)를 포함할 수 있다. 필수 요소는 자동 검증을 위해 필수적인 요소를 나타낸다. 보조 요소는 자동 검증의 정확도를 향상시키는데 도움이 되는 요소를 나타낸다. 필수 요소는 기관 IP 리스트 (Institute IP list)를 포함할 수 있다. 보조 요소는 블랙 IP 리스트 (Black IP list), 화이트 IP 리스트 (White IP list), 블랙 FQDN 리스트 (Black Fully Qualified Domain Name list), 화이트 FQDN 리스트 (White FQDN list) 및/또는 5가지 공격 유형을 위한 문자열 리스트 (String lists for the five attack types)를 포함할 수 있다.

[0041] 본 발명의 일 실시예에 따른 기관 IP 리스트는 보안 모니터링 서비스를 수신하는 기관들의 IP 주소를 포함한다. 본 발명의 일 실시예에 따르면, 기관 IP 리스트가 존재하지 않으면, 자동 검증은 수행되지 않을 수 있다. 블랙 IP 리스트는 보통 공격에 사용되는 악성 IP 주소를 포함한다. 화이트 IP 리스트는 주요 포탈 사이트들 또는 클라우드 서비스와 같은 신뢰할 만한 IP 주소를 포함한다. 본 발명의 일 실시예에 따르면, 블랙 FQDN 리스트 및 화이트 FQDN 리스트는 인터넷 사용자에 의해 요청되는 도메인 이름을 포함한다. 블랙 FQDN 리스트는 공격에 사

용되는 호스트 이름을 포함하고, 화이트 FQDN 리스트는 신뢰할 만한 호스트 이름을 포함한다. 5가지 공격 유형을 위한 문자열 리스트은 피해자가 공격을 당했을 때, 공격자에게 보내는 패킷의 페이로드에 포함된 값을 포함한다. 예를 들어, 피해자가 공격자 시스템 정보를 보내는 경우, 문자열은 맥 주소 (mac address), OS정보 등과 관련된 값일 수 있다. 본 발명의 일 실시예에 따르면, 정탐인 공격과 관련된 문자열은 보안이벤트의 유형에 따라 분류될 수 있다.

[0042] 본 발명의 일 실시예에 따르면, 상술한 기본 정보는 사용자 기본 정보로 명명될 수 있고, 필수 요소는 필수 정보로 보조 요소는 보조 정보로 명명될 수 있다.

[0044] 도 4는 본 발명의 일 실시예에 따른 공격 유형 별 정탐에 해당하는 문자열 리스트를 나타낸 도면이다.

[0045] 이 도면을 참조하면, 본 발명의 일 실시예에 따르면, 공격 유형이 정보 전송 (information transmission)인 경우, mac=, os=, register, avs=, ver=, pwd=, ie=, MB, provider, machine, npki, uid=, cpuname=, username=, WolfDDos, #information, prj=, logdata=, Windows, ADDNEW, MHz, uin=, nickname, ip, name, mobile 등의 문자열은 정탐에 해당한다. 공격 유형이 악성 URL (malicious URL)인 경우, USER, PORT, CWD, PASS, NICK, /ttt/sty.htm, user-agent : wget 등의 문자열은 정탐에 해당한다. 공격 유형이 악성코드 감염 (Malware infection)인 경우, GhOst, X.C…, x.Kc”…., o.b.j.e.c.t, t.a.b.l.e, &&&&&, filepath=, filename=, RooKIE 등의 문자열은 정탐에 해당한다. 공격 유형이 파일 업로드 (File upload)인 경우, EasyPhpWebShell, zecmd, idssvc, iesvc, Action=MainMenu, Action=ScanPort, JspSpy Ver, Not Found Shell, .asp.jpg, .php.jpg, 200 OK 등의 문자열은 정탐에 해당한다.

[0047] 도 5는 본 발명의 일 실시예에 따른 정적 요소 및 동적 요소에 대한 설명을 나타낸 도면이다.

[0048] 본 발명의 일 실시예에 따른 자동 검증 단계에서 정적 검증을 위한 정적 요소에 대하여 이하 설명한다. 본 발명의 일 실시예에 따른 정적 요소는 보안이벤트로부터 추출될 수 있는 기본 정보를 나타낸다. 정적 요소는 정탐을 찾기 위해 그리고, 보안이벤트의 오탐을 필터링하기 위해 TMS에 의해 탐지된 보안이벤트의 정적 검증을 위해 사용될 수 있다. 이 도면은 정적 요소 및 동적 요소를 설명한다. 정적 요소는 출발지 IP (source IP), 목적지 IP (destination IP), 출발지 포트 (source port), 목적지 포트 (destination port), 호스트 (host), 페이로드 (payload), HTTP 레퍼러 (HTTP Referer) 및/또는 보안이벤트의 수 (The number of security events)를 포함할 수 있다. 정적 검증을 수행할 때, 대부분의 정적 요소들은 몇몇 항목들을 제외하고는 기본 정보와 비교하는데 사용될 수 있다.

[0049] 본 발명의 일 실시예에 따른 출발지 IP (출발지 IP) 및 목적지 IP는 보안이벤트를 검증하가 위한 매우 기본적인 정보이다. 본 발명의 일 실시예에 따르면, 출발지 IP 및/또는 목적지 IP는 기본 정보 중 기관 IP 리스트, 블랙 IP 리스트 및/또는 화이트 IP 리스트와 비교함으로써 분석될 수 있다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 출발지 IP 및/또는 목적지 IP가 보안 관제 요원에 의해 입력되는 상술한 3개의 IP 리스트 내의 IP 주소에 속하는지 여부를 확인할 수 있다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 공격자 및 피해자를 식별하기 위하여 기관 IP 리스트에 해당하는 보안이벤트의 출발지 IP 및/또는 목적지 IP를 찾을 수 있다. 나아가, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 출발지 IP 및/또는 목적지 IP가 블랙 IP 또는 화이트 IP와 일치하는지 여부를 확인할 수 있다. 본 발명의 일 실시예에 따르면, 출발지 IP 또는 목적지 IP가 블랙 IP와 일치하는 경우, 해당 보안이벤트는 의심스러운 시스템으로 인식될 수 있다. 반면, 출발지 IP 또는 목적지 IP가 화이트 IP와 일치하는 경우, 해당 보안이벤트는 정상적인 서비스 (예를 들어, 인터넷 포탈, 주요 클라우드 시스템 등)를 제공하기 위한 IP 주소를 갖는 것으로 인식될 수 있다. 나아가, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 출발지 IP 및/또는 목적지 IP를 미사용 IP 주소들의 집합인 다크넷 IP (darknet IP)와 비교할 수 있다. 이는 다크넷으로 패킷을 보내는 것은 정상적인 활동을 위한 것이 아니기 때문이다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 실제 공격과 IDS 알림의 오탐을 구별하기 위해 사용될 수 있는 정적 요소의 일부로서 출발지 포트 및 목적지 포트를 정의한다. 이는 공격의 대상에 연결할 때, 공격자들은 보통 잘 알려진 포트 넘버를 사용하기 때문이다. 본 발명의 일 실시예에 따른 호스트는 인터넷 사용자에 의해 요청된 도메인 이름을 나타낸다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 탐지된 보안이벤트가 블랙 FQDN 또는 화이트 FQDN으로의 연결을 요청하는지 여부를 검증함으로써 호스트 정보를 이용하여 정상 연결과 악성 연결을 식별할 수 있다. 본 발명의 일 실시예에 따른 페이로드는 보안이벤트의 패킷 내의 데이터를 나타낸다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 보안이벤트 내의 패킷의 페이로드에 포함된 문자열을 실제 공격 또는 정상 신호와 연관된 문자열과 비교하기 위하여, 보안이벤트 내의 패킷의 페이로드에 포함된 문자열을 확인할 수 있다. 문자열에 대한 상세한 설명은 전술하였다. 본 발명의 일 실

시예에 따른 HTTP 레퍼러는 사용자가 목적지 웹페이지를 위한 하이퍼링크 (hyperlink)를 클릭하기 직전의 마지막 페이지를 나타낸다. 본 발명의 일 실시예에 따른 자동 검증 장치는 보안이벤트의 패킷 내에 HTTP 레퍼러가 존재하는지 여부를 식별할 수 있다. 이로써, 자동 검증 장치는 어디서 HTTP 트래픽 (traffic)이 요청되었는지를 확인할 수 있다. 본 발명의 일 실시예에 따르면, 특정 출발지 IP 주소에 의해 야기된 보안이벤트의 수는 악성코드 다운로드 및 악성코드 감염의 분석 시, 임계 값과 비교를 위해 사용될 수 있다. 본 발명의 일 실시예에 따르면, 동일한 출발지 IP 및 목적지 IP를 갖는 보안이벤트의 수는 실시간 정보를 나타낸다. 이는, 본 발명의 일 실시예에 따른 자동 검증 장치가 보안이벤트를 실시간으로 처리하기 때문이다. 따라서, 악성코드 다운로드 유형의 경우, 1 내지 5분의 시간 안에 탐지된, 동일한 출발지 IP 및 목적지 IP를 갖는 보안이벤트의 수가 임계치보다 크면, 자동 검증 장치는 파일 다운로드 관련한 활동은 반복적으로 실패하는 것으로 간주하고, 해당 보안이벤트를 악성 파일 관련한 접근으로 간주할 수 있다. 나아가, 악성코드 감염 유형의 경우, 24시간 안에 탐지된, 동일한 출발지 IP 및 목적지 IP를 갖는 보안이벤트의 수가 임계치보다 크면, 자동 검증 장치는 악성코드 감염 PC가 반복적으로 감염 신호를 커맨드 서버 또는 악성 서버로 전송하고 있는 것으로 간주할 수 있다.

[0050] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 동적 검증을 위하여 외부 시스템으로 접근에 대한 확인이 필요한 동적 요소를 추출할 수 있다. 본 발명의 일 실시예에 따른 동적 요소는 호스트 및 GET URL (Host URL), Get URL, 웹사이트 소스 코드 (Website source code) 및/또는 목적지 포트 (Destination port)를 포함할 수 있다. 정적 요소는 보안이벤트로부터 추출된 기본 정보인 반면에, 동적 요소는 외부 시스템 또는 서비스와 연관된 실제 정보이다. 따라서, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 실제 공격을 발견하기 위하여 추출된 URL에 접근하거나 동적 활동들을 수행함으로써 보안이벤트로부터 추출된 동적 요소의 각 항목을 분석할 수 있다. 본 발명의 일 실시예에 따른 호스트 및 GET URL 및/또는 Get URL은 보안이벤트의 페이로드로부터 추출될 수 있다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 해당 URL에 접근함으로써 보안이벤트의 실제 공격들을 식별할 수 있기 때문에 호스트 및 GET URL 및/또는 Get URL은 검증 요소로 사용될 수 있다. 본 발명의 일 실시예에 따른 웹사이트 소스 코드는 사용자에 의해 요청된 웹사이트 안의 소스 코드를 나타낸다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 웹사이트 소스 코드를 보안 관제 요원에 의해 입력된 문자열 (문자열)과 비교할 수 있다. 여기서, 상술한 문자열은 보안 관제 요원에 의해 입력된 실제 공격 및 정상 신호와 연관된 문자열을 나타낸다. 본 발명의 일 실시예에 따르면, 웹사이트 소스 코드는 공격에 대한 명령 (command)을 포함할 수 있다. 따라서, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 웹사이트 소스 코드와 보안 관제 요원에 의해 입력된 문자열을 비교하여 해당 보안이벤트가 실제 공격인지 아닌지를 판단할 수 있다. 본 발명의 일 실시예에 따른 목적지 포트는 목적지 IP와 일치하는 피해자로의 공격이 성공했는지 실패했는지를 확인하기 위하여, 목적지 포트가 오픈되어 있는지 여부를 확인하기 위한 것이다. 목적지 포트가 오픈되어 있으면, 오픈된 포트를 통한 공격이 가능하므로 해당 공격이 성공했을 가능성이 크다.

[0052] 도 6은 본 발명의 일 실시예에 따른 공격 유형의 특성을 나타낸 도면이다.

[0053] 본 발명의 일 실시예에 따른 유형 분류 모듈은 공격 특성을 기반으로 하여 시그니처 기반의 보안이벤트를 5가지 공격 유형들로 구분할 수 있다. 이 도면은 공격 유형들의 각 특성을 나타낸다.

[0054] 본 발명의 일 실시예에 따른 공격 유형은 악성 URL (malicious URL), 악성코드 다운로드 (malware download), 악성코드 감염 (Malware infection), 정보 전송 (information transmission) 및/또는 파일 업로드 (File upload)을 포함할 수 있다.

[0055] 악성 URL (malicious URL)에 따르면, 웜, 바이러스 등 악성코드에 감염된 시스템은 공격자가 구축해 놓은 악성 웹사이트(URL)에 접속하여 추가적인 악성 행위를 시도할 수 있다.

[0056] 악성코드 다운로드 (malware download)에 따르면, 웜, 바이러스 등 악성코드에 감염된 시스템은 공격자가 구축해 놓은 배포서버로부터 추가적으로 악성파일(.exe, .txt 등)에 대한 다운로드를 시도할 수 있다.

[0057] 악성코드 감염 (Malware infection)에 따르면, 웜, 바이러스 등 악성코드에 감염된 시스템은 해당 시스템이 악성코드에 감염된 사실을 알리기 위해 커맨드 서버, 경유지 서버 등 공격자가 구축해 놓은 시스템으로 감염신호를 송신할 수 있다.

[0058] 정보 전송 (information transmission)에 따르면, 웜, 바이러스 등 악성코드에 감염된 시스템은 해당 시스템의 정보(예를 들어, OS정보, MAC주소, PC name 등), 개인정보(예를 들어, 메일 계정, 주소록 등)등 중요 정보를 커맨드 서버, 경유지 서버 등 공격자가 구축해 놓은 시스템으로 송신할 수 있다.

[0059] 파일 업로드 (File upload)에 따르면, 공격자는 보안상 취약점이 존재하는 웹사이트를 공격하여 해당 웹서버로

부터 중요 정보 유출, 접근권한 탈취 등 악성행위를 수행하기 위한 악성코드(웹 쉘: web shell)를 업로드할 수 있다. 또한, 공격자는 이러한 악성코드(웹 쉘: web shell)를 실행할 수 있다.

[0060] 본 발명의 일 실시예에 따르면, 악성 URL 유형은 특정 URL 접속 유형으로 명명될 수 있고, 악성코드 다운로드 유형은 정보 유출 유형으로 명명될 수 있고, 악성코드 감염 유형은 DDoS 공격 유형 또는 좀비 PC 유형 또는 감염신호 전송 유형으로 명명될 수 있고, 파일 업로드 유형은 홈페이지 공격 유형 또는 접근권한 탈취 유형으로 명명될 수 있다. 나아가, 본 발명의 일 실시예에 따른 보안이벤트는 상술한 공격 유형 외에, 신호 송수신 특성 유형 및/또는 해킹 경유지 유형의 공격 유형을 가질 수 있다.

[0062] 도 7은 본 발명의 일 실시예에 따른 자동 검증 방법의 전체 프로세스를 나타낸 도면이다.

[0063] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 보안이벤트의 자동 검증 방법을 제공할 수 있다. 이 도면은 본 발명에서 제안하는 자동 검증 방법의 전체 프로세스를 나타낸다. 전술한 바와 같이, 본 발명의 일 실시예에 따른 보안이벤트는 시그니처 기반의 보안이벤트 및 임계치 기반의 보안이벤트로 분류될 수 있다. 시그니처 기반의 보안이벤트들은 5 가지의 공격 유형들로 분류될 수 있고, 보안이벤트들의 자동 검증은 공격 유형들을 기반으로 한 각 검증 알고리즘을 적용함으로써 수행될 수 있다. 본 발명의 일 실시예에 따른 자동 검증 방법은 특성 추출 단계 (7010), 유형 분류 단계 (7020) 및/또는 자동 검증 단계 (7030)를 포함할 수 있다. 그리고, 본 발명의 일 실시예에 따른 자동 검증 단계 (7030)는 요소 조합 단계 (items combination, 7040), 알고리즘 적용 단계 (algorithm application, 7050) 및/또는 분류 단계 (classification, 7060)를 포함할 수 있다. 요소 조합 단계에서, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 알고리즘의 각 단계를 수행하기 위하여, 보안이벤트로부터 추출된 정적 요소 및 동적 요소를 조합할 수 있다. 알고리즘 적용 단계에서, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 보안이벤트의 공격 유형에 속하는 알고리즘을 적용한 이후에, 알고리즘의 각 단계를 검증할 수 있다. 분류 단계에서, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 적용된 알고리즘의 검증 결과에 따라 보안이벤트를 분류할 수 있다. 분류 결과는 정탐 (true positive), 오탐 (false positive) 및/또는 미검증 (non-verification)를 포함할 수 있다. 정탐은 실제 공격을 의미하고, 오탐은 해당 보안이벤트가 정상적인 통신에 의해 야기된 것임을 의미할 수 있다. 본 발명의 일 실시예에 따르면, 정탐 또는 오탐으로 분류된 보안이벤트들은 추가적인 분석 없이, 자동적으로 사고 처리되거나 필터링될 수 있다. 하지만, 미검증으로 분류된 경우, 보안 관제 요원은 정탐인지 오탐인지를 식별하기 위하여 보안이벤트에 대해 추가적인 분석을 수행할 수 있다.

[0064] 본 발명의 일 실시예에 따르면, 공격 유형 기반의 자동 검증을 위하여, 보안 관제 요원의 노하우, 지난 사고 처리 히스토리 및/또는 관련 자료를 이용하여 5 가지의 공격 유형들이 분석되었다. 그 결과, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 각 공격 유형에 대한 정적 요소 및 동적 요소의 조합으로 이뤄진 특성들을 추출하고, 각 유형에 대한 자동 검증 알고리즘을 설계하여 제공한다.

[0066] 도 8은 본 발명의 일 실시예에 따른 악성 URL (malicious URL) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0067] 본 발명의 일 실시예에 따른 악성 URL 유형의 보안이벤트는 웜 또는 바이러스에 의해 감염된 시스템이 악성 URL에 접속하려할 때 탐지될 수 있다. 이 도면은 악성 URL 유형에 속하는 보안이벤트의 자동 검증 알고리즘을 나타낸다.

[0068] 본 발명의 일 실시예에 따르면, 악성 URL 유형에 대한 자동 검증 방법은 IP 주소 (IP address) 검증 단계 (S8010), 호스트 (HOST) 검증 단계 (S8020), 접근 경로 (access route) 검증 단계 (S8030) 및/또는 악성 URL 검증 단계 (S8040)를 포함할 수 있다.

[0069] IP 주소 검증 단계 (S8010)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 기관 IP의 PC 또는 시스템이 악성 URL에 접속하는 활동을 발견하기 위하여 출발지 IP와 기관 IP 리스트를 비교할 수 있다. 출발지 IP가 기관 IP 리스트와 일치하지 않는 경우, 해당 보안이벤트는 오탐으로 간주될 수 있다. 출발지 IP가 기관 IP 리스트와 일치하는 경우 자동 검증 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0070] 호스트 검증 단계 (S8020)에서, 자동 검증 모듈은 사용자에 의해 요청된 해당 호스트의 신뢰성을 검증하기 위하여 해당 호스트가 블랙 FQDN 리스트 또는 화이트 FQDN 리스트에 해당하는지 여부를 식별할 수 있다. 해당 보안이벤트의 호스트가 블랙 FQDN 리스트에 포함되는 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 해당 보안이벤트의 호스트가 화이트 FQDN 리스트에 포함되는 경우, 해당 보안이벤트는 오탐 그룹으로 분류될 수 있다. 호스트가 블랙 FQDN 리스트에 포함되지 않고, 화이트 FQDN 리스트에도 포함되지 않는 경우, 자동 검증 모

듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0071] 접근 경로 검증 단계 (S8030)에서, 자동 검증 모듈은 피해자가 정말로 악성 URL에 접근하려고 한건지 아닌지 여부를 확인하기 위하여 외부의 접근 경로를 검증할 수 있다. 자동 검증 모듈은 해당 보안이벤트 내에 레퍼러가 존재하는지 여부를 식별할 수 있다. 레퍼러가 존재하는 경우, 자동 검증 모듈은 레퍼러가 화이트 FQDN 리스트 및/또는 블랙 FQDN 리스트에 속하는지 여부를 확인할 수 있다. 레퍼러가 화이트 FQDN 리스트에 속하는 경우, 해당 보안이벤트는 오탐 그룹으로 분류될 수 있다. 왜냐하면, 해당 보안이벤트는 단지 정상적인 웹사이트 사용할 때 탐지된 것으로 간주될 수 있기 때문이다. 레퍼러가 블랙 FQDN 리스트에 속하는 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 레퍼러가 화이트 FQDN 리스트에 속하지 않고, 블랙 FQDN 리스트에도 속하지 않는 경우 해당 보안이벤트는 미검증 그룹으로 분류될 수 있다. 자동 검증 모듈은 레퍼러가 존재하지 않는 경우, 출발지 IP에 의해 요청된 호스트 및 GET URL에 접속이 가능한지 여부를 식별할 수 있다. 호스트 및 GET URL이 존재하고 해당 호스트 및 GET URL에 접근이 가능한 경우, 피해자가 악성 URL로 추정되는 웹페이지에 접속하였는지를 확인하기 위하여 자동 검증 모듈은 다음 단계를 수행할 수 있다. 하지만, 호스트 및 GET URL로의 접근이 실패하는 경우, 해당 보안이벤트는 정탐으로 간주될 수 있다. 왜냐하면, 레퍼러 없이 정상적인 서비스를 제공하지 못하는 호스트 및 GET URL로의 접근은 악성 활동을 의미할 수 있기 때문이다.

[0072] 악성 URL 검증 단계 (S8040)에서, 자동 검증 모듈은 호스트 및 GET URL의 웹사이트 내의 소스 코드가 정탐과 관련된 특정 문자열을 포함하고 있는지 여부를 식별할 수 있다. 본 발명의 일 실시예에 따르면, HTML 코드들은 웹사이트들를 생성하기 위하여 사용될 수 있고, 웹사이트들을 구성하는 이미지 및 오브젝트들을 삽입 (embed)하기 위해 사용될 수 있다. 방문자들이 악성 웹사이트로 향하도록 하기 위하여, 공격자들은 iframe 또는 frame과 같은 HTML 코드들을 웹사이트의 소스 코드에 삽입할 수 있다. 공격자들은 보이지 않는 iframe을 웹사이트에 삽입하기 위하여, iframe의 높이, 너비 및 경계 (border) 값을 0 또는 작은 값으로 설정할 수 있다. 따라서, 자동 검증 모듈은 웹사이트의 소스 코드 내의 문자열들을 보안 관제 요원에 의해 입력된 문자열들과 비교함으로써 해당 보안이벤트의 정탐 여부를 확인할 수 있다.

[0074] 도 9는 본 발명의 일 실시예에 따른 악성 코드 다운로드 (malware download) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0075] 이 도면은 악성 코드 다운로드에 속하는 보안이벤트의 검증 알고리즘을 나타낸다. 악성 코드 다운 로드 유형의 보안이벤트는 웜 또는 바이러스에 의해 감염된 시스템이 악성 웹사이트에 접속함으로써 악성 코드 파일들을 다운로드하려고 시도할 때, 탐지될 수 있다.

[0076] 본 발명의 일 실시예에 따르면, 악성 코드 다운로드 유형에 대한 자동 검증 방법은 IP 주소 (IP address) 검증 단계 (S9010), 접근 경로 (access route) 검증 단계 (S9020) 및/또는 파일 다운로드 (file download) 검증 단계 (S9030)를 포함할 수 있다.

[0077] IP 주소 검증 단계 (S9010)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 기관의 시스템 또는 컴퓨터가 악성 코드 파일의 다운로드를 시도하는 것을 막기 위하여 보안이벤트의 출발지 IP와 기관 IP 주소를 비교할 수 있다. 먼저, 자동 검증 모듈은 출발지 IP가 기관 IP 리스트에 포함되는지 여부를 확인할 수 있다. 그리고 나서, 출발지 IP가 기관 IP 리스트에 포함되어 있으면, 자동 검증 모듈은 보안이벤트의 목적지 IP와 블랙 IP 리스트를 비교할 수 있다. 목적지 IP가 블랙 IP가 아닌 경우, 자동 검증 모듈은 추가적인 분석을 위한 다음 단계를 수행할 수 있다. 목적지 IP가 블랙 IP로 식별되는 경우, 해당 보안이벤트는 정탐 (실제 공격)으로 분류될 수 있다. 자동 검증 모듈은 목적지 IP가 기관 IP 리스트에 포함되는 경우, 출발지 IP와 블랙 IP 리스트를 비교할 수 있다. 출발지 IP가 블랙 IP에 속하는 경우, 해당 보안이벤트는 정탐으로 간주될 수 있다. 그리고, 출발지 IP가 블랙 IP가 아닌 경우, 해당 보안이벤트는 보안 관제 요원에 의해 추가 분석이 필요한 미검증 그룹으로 분류될 수 있다.

[0078] 접근 경로 검증 단계 (S9020)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 피해자가 정말로 악성 코드 파일을 다운로드하려고 했는지 아니면 단지 정상적인 파일을 다운로드하려 했는지를 확인하기 위하여 외부의 접근 경로를 검증할 수 있다. 자동 검증 모듈은 먼저 해당 보안이벤트의 패킷 내의 레퍼러 (reference)를 식별할 수 있다. 레퍼러가 존재하는 경우, 자동 검증 모듈은 레퍼러가 화이트 FQDN 리스트 및/또는 블랙 FQDN 리스트에 속하는지 여부를 확인할 수 있다. 레퍼러가 블랙 FQDN 리스트에 속하는 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 레퍼러가 화이트 FQDN 리스트에 속하는 경우, 해당 보안이벤트는 오탐 그룹으로 분류될 수 있다. 왜냐하면, 해당 보안이벤트는 단지 정상적인 웹사이트 사용할 때 탐지된 것으로 간주될 수 있기 때문이다. 레퍼러가 화이트 FQDN 리스트에 속하지 않고, 블랙 FQDN 리스트에도 속하지 않는 경우 해당 보안이벤트는 미검

증 그룹으로 분류될 수 있다. 반면, 레퍼러가 존재하지 않는 경우, 자동 검증 모듈은 출발지 IP에 의해 요청된 호스트 및 GET URL로의 접속이 가능한지 여부를 식별할 수 있다. 호스트 및 GET URL이 존재하고 호스트 및 GET URL에 접속이 되는 경우, 피해자가 악성 웹사이트에 접속함으로써 악성 코드 파일을 다운로드한 것으로 간주될 수 있다. 즉, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 하지만, 호스트 및 GET URL이 존재하지 않거나 호스트 및 GET URL에 접속되지 않는 경우, 자동 검증 모듈은 다음 단계를 수행할 수 있다. 여기서, 상술한 레퍼러는 보안이벤트에서 추출한 HTTP 레퍼러 정보를 나타낼 수 있다.

[0079] 파일 다운로드 (file download) 검증 단계 (S9030)에서, 자동 검증 모듈은 파일 다운로드와 관련된 활동을 검증할 수 있다. 자동 검증 모듈은 대상 기관의 IP와 동일한 출발지 IP 주소 및 목적지 IP 주소를 갖는 보안이벤트들의 수가 임계치보다 큰지 작은지 여부를 식별할 수 있다. 이 단계에서 자동 검증 모듈은 상술한 보안이벤트의 개수 정보를 이용할 수 있다. 1 내지 5분 동안 탐지된 보안이벤트의 수가 임계치보다 큰 경우, 접근 불가능한 웹사이트임에도 불구하고 감염된 시스템 또는 PC가 계속적으로 그리고 자동적으로 웹사이트 안에서 악성코드 파일을 다운로드하려고 시도하고 있음을 나타낸다. 따라서, 이 경우 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 1 내지 5분 동안 탐지된 보안이벤트의 수가 임계치보다 크지 않는 경우, 보안 관제 요원은 해당 보안이벤트가 접근 불가능한 웹사이트에 접근하려고 한 이유를 분석해야 한다. 따라서, 이 경우, 보안 관제 요원에 의한 추가 분석을 위하여 해당 보안이벤트는 미검증 그룹으로 분류될 수 있다.

[0081] 도 10은 본 발명의 일 실시예에 따른 악성코드 감염 (Malware infection) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0082] 이 도면은 악성코드 감염에 속하는 보안이벤트의 자동 검증 알고리즘을 나타낸 도면이다. 악성코드 감염 유형의 보안이벤트는 웜 또는 바이러스에 의해 감염된 시스템이 악성코드에 감염된 사실을 알리기 위해 커맨드 서버, 경유지 서버 등 공격자가 구축해 놓은 시스템으로 감염신호를 송신할 때, 탐지될 수 있다.

[0083] 본 발명의 일 실시예에 따르면, 악성코드 감염 유형에 대한 자동 검증 방법은 IP 주소 (IP address) 검증 단계 (S10010), 접근 경로 (access route) 검증 단계 (S10020) 및/또는 감염 신호 (infection signal) 검증 단계 (S10030)를 포함할 수 있다.

[0084] IP 주소 검증 단계 (S10010)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 보안이벤트의 출발지 IP가 대상 기관인지 여부를 확인한 후에, 출발지 IP 및 목적지 IP를 블랙 IP 리스트와 비교할 수 있다. 왜냐하면, 웜 또는 바이러스에 의해 감염된 대상 기관의 IP 주소가 외부의 서버로 감염 신호를 송신하거나 외부로부터 감염 신호를 수신하는 커맨드 서버로 악용될 수 있기 때문이다. 출발지 IP 또는 목적지 IP가 블랙 IP 리스트에 포함된 경우, 해당 보안이벤트는 실제 공격으로 간주되고, 정탐 그룹으로 분류될 수 있다. 출발지 IP 및 목적지 IP가 블랙 IP 리스트에 포함되지 않는 경우, 자동 검증 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0085] 접근 경로 검증 단계 (S10020)에서, 레퍼러를 검증하는 것은 중요할 수 있다. 왜냐하면, 악성코드 감염 신호 송신은 악성코드에 의하여 자동적으로 발생하기 때문이다. 이 단계에서, 자동 검증 모듈은 해당 보안이벤트 내에 레퍼러가 존재하는지 여부를 식별할 수 있다. 레퍼러가 존재하는 경우, 해당 보안이벤트는 오탐 그룹으로 분류될 수 있다. 왜냐하면, 이 경우, 해당 보안이벤트는 단지 정상적인 웹페이지를 사용할 때, 감염 신호와 동일한 문자열 때문에 탐지된 것으로 간주될 수 있기 때문이다. 레퍼러가 존재하지 않는 경우, 자동 검증 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0086] 감염 신호 검증 단계 (S10030)에서, 자동 검증 모듈은 감염 신호의 전송과 관련된 활동을 검증할 수 있다. 이를 위하여, 자동 검증 모듈은 동일한 출발지 IP 주소 및 목적지 IP 주소를 갖는 보안이벤트들의 수가 임계치보다 큰지 작은지 여부를 식별할 수 있다. 24시간 안에 탐지된, 동일한 출발지 IP 및 목적지 IP를 갖는 보안이벤트의 수가 임계치보다 크면, 자동 검증 모듈은 악성코드 감염 PC가 반복적으로 감염 신호를 커맨드 서버 또는 악성 서버로 전송하고 있는 것으로 간주할 수 있다. 따라서, 이 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 24시간 안에 탐지된, 동일한 출발지 IP 및 목적지 IP를 갖는 보안이벤트의 수가 임계치보다 작으면, 자동 검증 모듈은 보다 정확한 검증을 위한 다음 검증을 수행할 수 있다. 왜냐하면, 악성코드 감염 유형의 보안이벤트는 정상적인 연결임에도 불구하고 패킷의 페이로드 내의 단순한 문자열들이 시그니처 규칙들과 일치하는 경우에 탐지될 수 있기 때문이다. 다음 과정으로, 자동 검증 모듈은 보안 관제 요원에 의해 입력된 문자열을 해당 보안이벤트의 페이로드 내의 문자열과 비교할 수 있다. 악성코드 감염 유형의 경우, 정탐과 연관된 문자열은 감염 신호에 대하여 무의미한 값일 수 있다. 해당 보안이벤트의 문자열이 감염 신호와 연관된 문자열인 경우, 해당 보안이벤트는 정탐으로 간주될 수 있다. 반면, 해당 보안이벤트의 문자열이 감염 신호와 연관된 문자열이 아닌 경우, 자동 검증 모듈은 해당 보안이벤트의 포트 넘버가 해당 보안이벤트의 메일 포트 (mail port, 예를 들

어, SMPT(TCP/25), POP(TCP/109, 110, 143))와 관련이 있는지 여부를 확인할 수 있다. 메일을 전송할 때, 메일 내의 데이터는 base 64의 인코딩 방법으로 인코딩될 수 있다. 악성코드 감염 유형의 보안이벤트는 메일 전송의 경우로 탐지될 수 있다. 왜냐하면, 해당 보안이벤트는 감염 신호와 연관된 문자열과 함께, 메일의 인코딩된 데이터와 우연적으로 일치할 수 있기 때문이다. 따라서, 해당 보안이벤트의 포트 넘버가 메일 포트와 연관이 있는 경우, 해당 보안이벤트는 오탐으로 간주될 수 있다. 해당 보안이벤트의 포트 넘버가 메일 포트와 연관이 없는 경우, 해당 보안이벤트는 보안 관제 요원에 의해 추가 분석이 필요한 미검증 그룹으로 분류될 수 있다.

[0088] 도 11은 본 발명의 일 실시예에 따른 정보 전송 (information transmission) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0089] 이 도면은 정보 전송 유형에 속하는 보안이벤트의 자동 검증 알고리즘을 나타낸다. 정보 전송 유형의 보안이벤트는 웜 또는 바이러스에 의해 감염된 시스템이 자신의 시스템 정보를 공격자에 송신할 때 탐지될 수 있다.

[0090] 본 발명의 일 실시예에 따르면, 정보 전송 유형에 대한 자동 검증 방법은 IP 주소 (IP address) 검증 단계 (S11010), 접근 경로 (access route) 검증 단계 (S11020, S11030) 및/또는 정보 전송 (information transmission) 검증 단계 (S11040)를 포함할 수 있다.

[0091] IP 주소 검증 단계 (S11010)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 보안이벤트의 출발지 IP와 기관 IP 리스트를 비교할 수 있다. 출발지 IP와 기관 IP 리스트에 포함되면, 자동 검증 모듈은 목적지 IP와 블랙 IP 리스트를 비교할 수 있다. 출발지 IP가 기관 IP 리스트에 포함되지 않으면, 해당 보안이벤트는 오탐으로 간주될 수 있다. 왜냐하면, 본 발명의 일 실시예에 따른 자동 검증 모듈은 기관 IP의 PC 또는 시스템이 시스템 정보를 전송하는 활동을 찾는 것을 우선으로 하기 때문이다. 목적지 IP가 블랙 IP 리스트에 포함되는 경우, 해당 보안이벤트는 실제 공격으로 간주되고 정탐 그룹으로 분류될 수 있다. 하지만, 목적지 IP가 블랙 IP에 포함되지 않는 경우, 자동 검증 모듈은 추가적인 분석을 위한 다음 단계를 수행할 수 있다.

[0092] 접근 경로 검증 단계 (S11020, S11030)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 피해자가 정말로 중요 정보를 공격자에게 전송하였는지 아니면 단지 정상적인 서비스의 제공을 수신하기 위하여 정보를 전송하였는지 여부를 확인하기 위하여 외부 접근 경로를 검증할 수 있다. 자동 검증 모듈은 사용자에 의해 요청된 호스트가 블랙 FQDN 리스트에 포함되어 있는지 아닌지를 식별할 수 있다. 해당 호스트가 블랙 FQDN에 포함되는 경우, 해당 보안이벤트는 실제 공격으로 간주되고 정탐 그룹으로 분류될 수 있다. 해당 호스트가 블랙 FQDN에 포함되지 않는 경우, 자동 검증 모듈은 해당 보안이벤트의 패킷 내의 레퍼러를 식별할 수 있다. 레퍼러가 존재하는 경우, 자동 검증 모듈은 레퍼러가 블랙 FQDN 리스트 및/또는 화이트 FQDN 리스트에 포함되는지 여부를 식별할 수 있다. 레퍼러가 화이트 FQDN 리스트에 포함되는 경우, 해당 보안이벤트는 오탐 그룹으로 분류될 수 있다. 왜냐하면, 이 경우, 해당 보안이벤트는 정상적인 웹사이트를 사용할 때 탐지된 것으로 간주될 수 있기 때문이다. 레퍼러가 블랙 FQDN 리스트에 포함되는 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 레퍼러가 화이트 FQDN 리스트에 포함되지 않고, 블랙 FQDN 리스트에도 포함되지 않는 경우, 자동 검증 모듈은 추가적인 분석을 위해 다음 단계를 수행할 수 있다.

[0093] 정보 전송 검증 단계 (S11040)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 보안 관제 요원에 의해 입력된 문자열 (string)을 해당 보안이벤트의 페이로드 내의 문자열과 비교할 수 있다. 정보 전송 유형의 경우, 정탐과 연관된 문자열은 시스템 또는 개인 정보에 대한 것일 수 있다. 해당 보안이벤트의 문자열이 시스템 정보와 연관된 문자열과 동일한 경우, 해당 보안이벤트는 정탐으로 간주될 수 있다. 하지만, 해당 보안이벤트의 문자열이 시스템 정보와 연관된 문자열과 동일하지 않은 경우, 해당 보안이벤트는 보안 관제 요원에 의한 추가 분석을 위한 미검증 그룹으로 분류될 수 있다.

[0095] 도 12는 본 발명의 일 실시예에 따른 파일 업로드 (File upload) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0096] 본 발명의 일 실시예에 따른 파일 업로드 유형의 보안이벤트는 보안상 취약점이 존재하는 웹사이트를 공격하여 해당 웹서버로부터 중요 정보 유출, 접근권한 탈취 등 악성행위를 수행하기 위한 악성코드(웹 쉘: web shell)를 업로드할 때 탐지될 수 있다. 이 도면은 파일 업로드 유형에 속하는 보안이벤트의 자동 검증 알고리즘을 나타낸다.

[0097] 본 발명의 일 실시예에 따르면, 파일 업로드 유형에 대한 자동 검증 방법은 IP 주소 (IP address) 검증 단계 (S12010), 포트 (port) 검증 단계 (S12020), 접근 경로 (access route) 검증 단계 (S12030) 및/또는 웹 쉘 업로드 (web shell upload) 검증 단계 (S12040, S12050)를 포함할 수 있다.

[0098] IP 주소 검증 단계 (S12010)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 보안이벤트의 출발지 IP가 대상 기관인지 여부를 확인한 후에, 출발지 IP 및 목적지 IP를 블랙 IP 리스트와 비교할 수 있다. 왜냐하면, 기관의 취약한 홈페이지에 웹 쉘이 업로드될 수 있고, 웹 쉘을 통해 기관의 중요 정보가 외부 공격자에게 전송될 수 있기 때문이다. 출발지 IP 또는 목적지 IP가 블랙 IP인 경우, 해당 보안이벤트는 실제 공격으로 간주되고, 정탐 그룹으로 분류될 수 있다. 출발지 IP 및 목적지 IP가 블랙 IP가 아닌 경우, 자동 검증 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0099] 포트 검증 단계 (S12020)에서, 자동 검증 모듈은 목적지 포트 넘버가 해당 보안이벤트의 HTTP에 사용되는 포트 (즉, 80 또는 8080)와 연관이 있는지 여부를 확인할 수 있다. 왜냐하면, 공격자들은 해당 웹사이트에 웹 쉘을 업로드하기 위하여 상술한 목적지 포트와 통신하려고 하기 때문이다. 자동 검증 모듈은 보안이벤트의 출발지 IP가 기관 IP 리스트에 포함되는 경우, 출발지 포트 넘버가 해당 보안이벤트의 HTTP 또는 Web 포트 (즉, 80 또는 8080)와 연관이 있는지 여부를 확인할 수 있다. 왜냐하면, HTTP 또는 Web 포트와 연관된 출발지 포트의 넘버가 웹페이지 요청에 대한 응답 값을 전송하기 위해 사용되기 때문이다. 따라서, 출발지 포트 넘버가 해당 보안이벤트의 HTTP 또는 Web 포트와 연관이 있는 경우, 해당 보안이벤트는 보안 관제 요원에 의한 추가 분석이 필요한 미검증 그룹으로 분류될 수 있다. 반면, 출발지 포트 넘버가 해당 보안이벤트의 HTTP 또는 Web 포트와 연관이 없는 경우, 자동 검증 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0100] 접근 경로 검증 단계 (S12030)에서, 자동 검증 모듈은 보안이벤트의 페이로드 내에 레퍼러가 존재하는지 여부를 식별할 수 있다. 레퍼러가 존재하는 경우, 해당 보안이벤트는 추가 검증을 위한 미검증 그룹으로 분류될 수 있다. 레퍼러가 존재하지 않는 경우, 자동 검증 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0101] 웹 쉘 업로드 검증 단계 (S12040, S12050)에서, 자동 검증 모듈은 보안 관제 요원에 의해 입력된 문자열을 해당 보안이벤트의 페이로드 내의 문자열과 비교할 수 있다. 파일 업로드 유형의 경우, 정탐과 관련된 문자열은 파일 이름 확장자 (file name extension, 예를 들어, .php.jpg, .asp.jpg 등)에 대한 것일 수 있다. 왜냐하면, 공격자들은 업로드 페이지에서 스크립트 파일 (script files, .asp, .php 등)을 필터링하는 기능이 없는 취약한 시스템의 약점을 이용하기 때문이다. 나아가, 중요 정보가 공격자에게 유출 되는 경우에, 정탐과 관련된 문자열은 시스템 커멘드에 관한 것일 수 있다. 보안이벤트의 페이로드 내에 상술한 문자열이 존재하지 않는 경우, 해당 보안이벤트는 추가 검증을 위한 미검증 그룹으로 분류될 수 있다. 보안이벤트의 페이로드 내에 상술한 문자열이 존재하는 경우, 자동 검증 모듈은 출발지 IP에 의해 요청된 호스트 및 Get URL에 접근이 가능한지 여부를 식별할 수 있다. 호스트 및 Get URL이 존재하고 접근이 가능한 경우, 피해자는 홈페이지에 웹 쉘을 업로드한 것으로 간주될 수 있고, 이 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다. 반면, 호스트 및 Get URL이 존재하지 않거나 접근이 불가능한 경우, 해당 보안이벤트는 미검증 그룹으로 간주될 수 있다. 본 발명의 일 실시예에 따르면, 정탐과 관련된 문자열은 실제 공격과 관련된 문자열을 나타낼 수 있다.

[0103] 도 13은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트 (Threshold based security event)에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0104] 이 도면은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트의 자동 검증 알고리즘을 나타낸다.

[0105] 본 발명의 일 실시예에 따르면, 임계치 기반의 보안이벤트의 자동 검증 방법은 IP 주소 비교 (IP address comparison) 단계 (S13010), 특성 비교 (feature comparision) 단계 (S13020), 히스토리 비교 (history comparision) 단계 (S13030) 및/또는 다크넷 비교 (darknet comparison) 단계 (S13040)를 포함할 수 있다.

[0106] IP 주소 비교 단계 (S13010)에서, 본 발명의 일 실시예에 따른 자동 검증 모듈은 해당 보안이벤트의 출발지 IP가 기관 IP 리스트에 포함되는지 여부를 확인하고, 해당 보안이벤트의 목적지 IP가 블랙 IP 리스트에 포함되는지 여부를 확인할 수 있다. 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트의 주요 목적은 피해자가 그들의 정상적인 서비스 또는 업무를 더 이상 제공할 수 없도록 하기 위하여 짧은 시간 내에 수많은 패킷들을 목표 호스트 또는 네트워크에 전송하는 것이다. 따라서, 출발지 IP와 기관 IP 리스트를 비교하는 것은 웜 또는 바이러스에 의해 감염되어 외부 피해자를 공격하는 기관 시스템과 관련된 IP 주소를 찾기 위한 것이다. 출발지 IP와 기관 IP 리스트에 포함되고, 목적지 IP가 블랙 IP가 아닌 경우, 자동 검증 모듈은 다음 단계를 수행하고, 출발지 IP와 기관 IP 리스트에 포함되지 않는 경우 해당 보안이벤트는 오탐 그룹으로 분류될 수 있고, 목적지 IP가 블랙 IP인 경우, 해당 보안이벤트는 정탐 그룹으로 분류될 수 있다.

[0107] 특성 비교 단계 (S13020)에서, 자동 검증 모듈은 추출된 특성들에 대한 비교를 수행할 수 있다. 임계치 기반의 보안이벤트의 경우, 자동 검증 모듈은 목적지 IP 또는 포트가 변경되었는지 여부를 확인할 수 있다. 왜냐하면,

공격자들은 공격을 플러딩 (flooding) 또는 스캐닝 (scanning)하기 위하여 대체로 목적지 IP 또는 포트 넘버를 변경하기 때문이다. 자동 검증 모듈은 해당 보안이벤트의 패킷이 반복되는 문자열 (무의미한 문자열)을 포함하고 있는지 여부를 식별할 수 있다. 본 발명의 일 실시예에 따르면, 임계치 기반의 보안이벤트의 패킷들은 페이로드 데이터를 대체로 포함하지 않지만, 임계치 기반의 보안이벤트의 패킷들은 쓸모없는 형식의 값 (예를 들어, “XXXXX”, “AAAAA” 등)을 나타내는 무의미한 데이터를 포함한다. 나아가, 임계치 기반의 보안이벤트의 몇몇 패킷은 오름차순 또는 내림차순의 특정 문자열 (예를 들어, “abcde” 등)을 포함할 수 있다. 자동 검증 모듈은 임계치 기반의 보안이벤트의 자동 검증을 위하여 상술한 문자열을 특성으로서 사용할 수 있다. 해당 보안이벤트의 목적지 IP 및 포트가 변경되지 않았고, 해당 보안이벤트 내의 문자열이 반복되지 않고, 해당 보안 인벤트가 특정 문자열을 포함하지 않는 경우, 해당 보안이벤트는 오탐 그룹으로 분류될 수 있다. 반면, 해당 보안이벤트의 목적지 IP 및 포트가 변경되었거나, 해당 보안이벤트 내의 문자열이 반복되거나, 해당 보안 인벤트가 특정 문자열을 포함하는 경우, 자동 검증 모듈은 다음 단계로서 히스토리 비교를 수행한다.

[0108] 히스토리 비교 단계 (S13030)에서, 자동 검증 모듈은 해당 보안이벤트의 출발지 IP가 해당 보안이벤트와 동일한 출발지 IP를 갖는 다른 보안이벤트가 최근 실제 공격으로 밝혀진 과거의 히스토리를 갖고 있는지 여부를 식별할 수 있다. 해당 보안이벤트가 상술한 과거의 히스토리가 있는 보안이벤트인 경우, 자동 검증 모듈은 다음 단계를 수행할 수 있다. 반면, 해당 보안이벤트가 상술한 과거의 히스토리가 있는 보안이벤트가 아닌 경우, 해당 보안이벤트는 추가 분석이 필요한 미검증 그룹으로 분류될 수 있다.

[0109] 다크넷 비교 단계 (S13040)에서, 자동 검증 모듈은 해당 보안이벤트의 출발지 IP와 다크넷에 대한 IP를 비교할 수 있다. 본 발명의 일 실시예에 따르면, 다크넷 상에서 발견된 패킷들은 악성 활동들로 간주될 수 있다. 왜냐하면, 다크넷은 미사용 IP 주소의 집합이고, 실제 서버 또는 시스템이 아님을 의미하기 때문이다. 해당 보안이벤트의 출발지 IP가 이전에 다크넷 IP로 패킷을 전송한 적이 있다면, 해당 보안이벤트는 정탐으로 분류될 수 있다. 반면, 해당 보안이벤트의 출발지 IP가 이전에 다크넷 IP로 패킷을 전송한 적이 없다면, 해당 보안이벤트는 추가 분석이 필요한 미검증 그룹으로 분류될 수 있다. 본 발명의 일 실시예에 따르면, 이 단계는 생략될 수 있다.

[0111] 도 14는 본 발명의 일 실시예에 따른 탐지 규칙 (signature rules)의 통계를 나타낸 도면이다.

[0112] 본 발명의 일 실시예에 따르면, 본 발명에서 제안하는 자동 검증 방법의 효율성을 증명하기 위하여, 보안 관제 요원에 의하여 3년 동안 하나 이상의 실제 공격으로 식별된 보안이벤트들이 표본으로 준비되었다. 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 먼저, 보안이벤트들을 임계치 기반의 보안이벤트 및 5 가지 공격 유형의 시그니처 기반의 보안이벤트로 분류하였다. 이 도면은 분류된 탐지 규칙의 결과를 나타낸다. 이 도면을 참조하면, 2013, 2014 및 2015년에 하나 이상의 실제 공격으로 식별된 탐지 규칙은 각각 96, 70 및 38 개로 나타났다. 나아가, 중복된 것을 제외한 값인 유일한 탐지 규칙의 수는 134개로 나타났고, 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 이러한 탐지 규칙들을 실험에 사용하였다. 134 개의 탐지 규칙들의 실제 공격에 대한 보안이벤트의 총 개수는 3074 개로 나타났다.

[0114] 도 15는 본 발명의 일 실시예에 따른 악성 URL (malicious URL) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

[0115] 본 발명의 일 실시예에 따르면, 본 발명에서 제안하는 각 공격 유형에 따른 자동 검증 방법의 정확도가 측정되었다. 이 측정을 위하여, 각 유형의 보안이벤트에 본 발명의 일 실시예에 따른 자동 검증 방법이 적용되었고, 4517 개의 패킷이 실제 공격으로 증명되었다. 이 도면은 악성 URL (malicious URL) 유형에 대한 정확도 측정 결과를 나타낸 그림이다. 이 그림을 참조하면, 악성 URL 유형 중에 36개의 유일한 보안이벤트 (unique security event)에 대하여 정탐 (즉, 실제 공격)을 확인하였다. 그 결과, 36개의 유일한 보안이벤트에 대하여 2704674 (2013년), 942475 (2014년) 및 797023 (2015년)건이 탐지되었다. 나아가, 36개의 유일한 보안이벤트의 138 (2013년), 111 (2014년) 및 221 (2015년)건의 실제 공격이 정탐으로 올바르게 분류되었음을 확인할 수 있었고, 2704536 (2013년), 942364 (2014년) 및 796802 (2015년)건이 오탐으로 올바르게 분류되었음을 확인할 수 있었다. 나아가, 악성 URL 유형에 대한 본 발명이 제안하는 자동 검증 방법의 정확도는 100 퍼센트임이 확인되었다.

[0117] 도 16은 본 발명의 일 실시예에 따른 악성 코드 다운로드 (malware download) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

[0118] 이 도면은 악성 코드 다운로드 (malware download) 유형에 대한 정확도 측정 결과를 나타낸 그림이다. 이 그림을 참조하면, 악성 코드 다운로드 유형 중에 5개의 유일한 보안이벤트 (unique security event)에 대하여 정탐

(즉, 실제 공격)을 확인하였다. 그 결과, 5개의 유일한 보안이벤트에 대하여 7285 (2013년), 36384 (2014년) 및 9651 (2015년)건이 탐지되었다. 나아가, 5개의 유일한 보안이벤트의 206 (2013년), 219 (2014년) 및 545 (2015년)건의 실제 공격이 정탐으로 올바르게 분류되었음을 확인할 수 있었고, 7079 (2013년), 63165 (2014년) 및 9106 (2015년)건이 오탐으로 올바르게 분류되었음을 확인할 수 있었다. 나아가, 악성 코드 다운로드 유형에 대한 본 발명이 제안하는 자동 검증 방법의 정확도는 100 퍼센트임이 확인되었다.

[0120] 도 17은 본 발명의 일 실시예에 따른 악성코드 감염 (Malware infection) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

[0121] 이 도면은 악성코드 감염 (Malware infection) 유형에 대한 정확도 측정 결과를 나타낸 그림이다. 이 그림을 참조하면, 악성코드 감염 유형 중에 52개의 유일한 보안이벤트 (unique security event)에 대하여 정탐 (즉, 실제 공격)을 확인하였다. 그 결과, 52개의 유일한 보안이벤트에 대하여 1411259 (2013년), 18492488 (2014년) 및 14810746 (2015년)건이 탐지되었다. 나아가, 52개의 유일한 보안이벤트의 504 (2013년), 131 (2014년) 및 337 (2015년)건의 실제 공격이 정탐으로 올바르게 분류되었음을 확인할 수 있었고, 1410755 (2013년), 18492357 (2014년) 및 14810409 (2015년)건이 오탐으로 올바르게 분류되었음을 확인할 수 있었다. 나아가, 악성코드 감염 유형에 대한 본 발명이 제안하는 자동 검증 방법의 정확도는 100 퍼센트임이 확인되었다.

[0123] 도 18은 본 발명의 일 실시예에 따른 정보 전송 (information transmission) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

[0124] 이 도면은 정보 전송 (information transmission) 유형에 대한 정확도 측정 결과를 나타낸 그림이다. 이 그림을 참조하면, 정보 전송 유형 중에 14개의 유일한 보안이벤트 (unique security event)에 대하여 정탐 (즉, 실제 공격)을 확인하였다. 그 결과, 14개의 유일한 보안이벤트에 대하여 42543 (2013년), 7356 (2014년) 및 16756 (2015년)건이 탐지되었다. 나아가, 14개의 유일한 보안이벤트의 1277 (2013년), 471 (2014년) 및 29 (2015년)건의 실제 공격이 정탐으로 올바르게 분류되었음을 확인할 수 있었고, 41266 (2013년), 6885 (2014년) 및 16727 (2015년)건이 오탐으로 올바르게 분류되었음을 확인할 수 있었다. 나아가, 정보 전송 유형에 대한 본 발명이 제안하는 자동 검증 방법의 정확도는 100 퍼센트임이 확인되었다.

[0126] 도 19는 본 발명의 일 실시예에 따른 파일 업로드 (File upload) 유형에 따른 자동 검증 방법의 정확도를 나타낸 도면이다.

[0127] 이 도면은 파일 업로드 (File upload) 유형에 대한 정확도 측정 결과를 나타낸 그림이다. 이 그림을 참조하면, 파일 업로드 유형 중에 21개의 유일한 보안이벤트 (unique security event)에 대하여 정탐 (즉, 실제 공격)을 확인하였다. 그 결과, 21개의 유일한 보안이벤트에 대하여 88414 (2013년), 1222146 (2014년) 및 28795133 (2015년)건이 탐지되었다. 나아가, 그 결과, 21개의 유일한 보안이벤트의 22 (2013년), 37 (2014년) 및 54 (2015년)건의 실제 공격이 정탐으로 올바르게 분류되었음을 확인할 수 있었고, 88392 (2013년), 1222109 (2014년) 및 28795079 (2015년)건이 오탐으로 올바르게 분류되었음을 확인할 수 있었다. 나아가, 파일 업로드 유형에 대한 본 발명이 제안하는 자동 검증 방법의 정확도는 100 퍼센트임이 확인되었다.

[0129] 도 20은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트 (threshold based security event)에 대한 자동 검증 방법의 정확도를 나타낸 도면이다.

[0130] 이 도면은 임계치 기반의 보안이벤트 (threshold based security event)에 대한 자동 검증의 정확도 측정 결과를 나타낸 그림이다. 본 발명의 일 실시예에 따르면, 임계치 기반의 보안이벤트의 경우, 2014년에 한 번 이상 실제 공격으로 식별된 6개의 보안이벤트가 수집되었다. 하지만, TCP null scan 및 UDP port scan에 대한 검증은 2009년부터 2011년까지 수집된 데이터를 이용하여 수행되었다. 왜냐하면, 2011년 이후에 TCP null scan 및 UDP port scan에 대한 데이터는 없기 때문이다. 따라서, 이 그림을 참조하면, 6개의 임계치 기반의 보안이벤트에 대하여 215 건의 정탐 (즉, 실제 공격)을 확인하였다. 그 결과, 6개의 임계치 기반의 보안이벤트에 대하여 215 건의 실제 공격이 정탐으로 올바르게 분류되었음을 확인할 수 있었다. 나아가, 임계치 기반의 보안이벤트에 대한 본 발명이 제안하는 자동 검증 방법의 정확도는 100 퍼센트임이 확인되었다.본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 공격 유형 기반의 보안이벤트의 자동 검증 방법을 제공한다. 본 발명의 일 실시예의 주목적은 보안 관제 요원이 효율적으로 보안 모니터링 및 응답을 수행할 수 있도록 수많은 보안이벤트들로부터 실제 공격을 식별하는 것이고, 오탐을 필터링해 내는 것이다. 본 발명의 일 실시예에 따른 공격 유형 기반의 보안이벤트에 대한 자동 검증 방법은 특성 추출 (feature extraction) 단계, 유형 분류 (type classification) 단계 및/또는 자동 검증 (automated verification) 단계를 포함할 수 있다. 본 발명이 제안하는 자동 검증 방법의

효율성을 측정하기 위하여, 134개의 탐지 규칙들이 사용되었고, 134개의 탐지 규칙들에 의해 탐지된 4517 건의 보안이벤트가 추출되었다. 따라서, 본 발명의 일 실시예에 따라, 4517 건의 보안이벤트가 공격 유형에 따라 6개의 그룹으로 분류되었고, 각 유형에 따른 검증 방법의 정확성이 측정되었다. 그 결과, 모든 유형의 총 정확도는 낮은 오탐률을 유지하면서 대략 100 퍼센트를 나타내는 것이 실험적으로 증명되었다.

[0132] 도 21은 본 발명의 일 실시예에 따른 보안이벤트의 유형을 분류하는 과정을 나타낸 도면이다.

[0133] 본 발명의 일 실시예에 따른 유형 분류 단계는 이벤트 유형 및/또는 공격 유형을 분류할 수 있다. 먼저, 이벤트 유형에 대해 설명하면, TMS는 탐지 메커니즘을 기반으로 하여 두가지 유형의 보안이벤트를 탐지하고 기록할 수 있다. 여기서, 두가지 유형은 시그니처 (signature) 기반 및 임계치 (threshold) 기반를 나타낸다. 본 발명의 일 실시예에 따른 유형 분류 모듈은 자동 검증 단계에서 각 유형에 따른 보안이벤트를 검증하기 위하여 보안이벤트들을 시그니처 기반의 보안이벤트 및 임계치 기반의 보안이벤트로 분류할 수 있다. 본 발명의 일 실시예에 따른 시그니처 기반의 보안이벤트는 공격 유형에 따라 재분류될 수 있다. 여기서, 본 발명의 일 실시예에 따른 시그니처 기반 보안이벤트는 사전에 정의된 문자열 패턴 (영문자, 숫자 및 특수기호의 조합 또는 정규 표현식)과 동일한 문자열을 포함한 패킷에 의해 발생하는 보안이벤트를 나타낸다. 본 발명의 일 실시예에 따른 임계치 기반 보안이벤트는 특정 패킷이 사전에 정의된 임계치 (단위 시간당 발생 빈도)를 초과하여 발생한 보안이벤트를 나타낸다. 본 발명의 일 실시예에 따르면, 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)의 탐지 방법에 따라 시그니처 기반 보안이벤트 및/또는 임계치 기반 보안이벤트가 탐지될 수 있다. 예를 들어, 탐지규칙 기반 보안장비(IDS/IPS, TMS 등)이 사전에 정의된 발생 빈도 (임계치)를 초과하여 발생한 보안이벤트를 탐지하는 시스템일 수 있고, 사전에 정의된 문자열 패턴을 포함하는 모든 보안이벤트를 탐지하는 시스템일 수 있다.

[0135] 도 22는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법을 나타낸 도면이다.

[0136] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법은 보안이벤트 및 보안이벤트와 관련된 정보를 입력받는 단계 (S22010), 보안이벤트의 특성을 추출하는 단계 (S22020), 보안이벤트를 분류하는 단계 (S22030) 및/또는 보안이벤트를 검증하는 단계 (S22040)를 포함할 수 있다.

[0137] 보안이벤트 및 보안이벤트와 관련된 정보를 입력받는 단계 (S22010)에 대한 상세한 설명은 도 2, 3, 7에서 전술하였다.

[0138] 보안이벤트의 특성을 추출하는 단계 (S22020)에 대한 상세한 설명은 도 2, 5, 7에서 전술하였다.

[0139] 보안이벤트를 분류하는 단계 (S22030)에 대한 상세한 설명은 도 2, 6, 7에서 전술하였다.

[0140] 보안이벤트를 검증하는 단계 (S22040)에 대한 상세한 설명은 도 2, 4, 7, 8, 9, 10, 11, 12, 13에서 전술하였다.

[0142] 본 발명의 실시예들에 따른 모듈, 유닛 또는 블락은 메모리(또는 저장 유닛)에 저장된 연속된 수행과정들을 실행하는 프로세서/하드웨어일 수 있다. 전술한 실시예에 기술된 각 단계 또는 방법들은 하드웨어/프로세서들에 의해 수행될 수 있다. 또한, 본 발명이 제시하는 방법들은 코드로서 실행될 수 있다. 이 코드는 프로세서가 읽을 수 있는 저장매체에 쓰여질 수 있고, 따라서 본 발명의 실시예들에 따른 장치(apparatus)가 제공하는 프로세서에 의해 읽혀질 수 있다.

[0143] 설명의 편의를 위하여 각 도면을 나누어 설명하였으나, 각 도면에 서술되어 있는 실시 예들을 병합하여 새로운 실시 예를 구현하도록 설계하는 것도 가능하다. 그리고, 당업자의 필요에 따라, 이전에 설명된 실시 예들을 실행하기 위한 프로그램이 기록되어 있는 컴퓨터에서 판독 가능한 기록 매체를 설계하는 것도 본 발명의 권리범위에 속한다.

[0144] 본 발명에 따른 장치 및 방법은 상술한 바와 같이 설명된 실시 예들의 구성과 방법이 한정되게 적용될 수 있는 것이 아니라, 상술한 실시 예들은 다양한 변형이 이루어질 수 있도록 각 실시 예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.

[0145] 한편, 본 발명의 영상 처리 방법은 네트워크 디바이스에 구비된 프로세서가 읽을 수 있는 기록매체에 프로세서가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 프로세서가 읽을 수 있는 기록매체는 프로세서에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 프로세서가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한, 인터넷을 통한 전송 등과 같은 캐리어 웨이브의 형태로 구현되는 것도 포함한다. 또한, 프로세서가 읽을 수 있는 기록매체는 네트워크

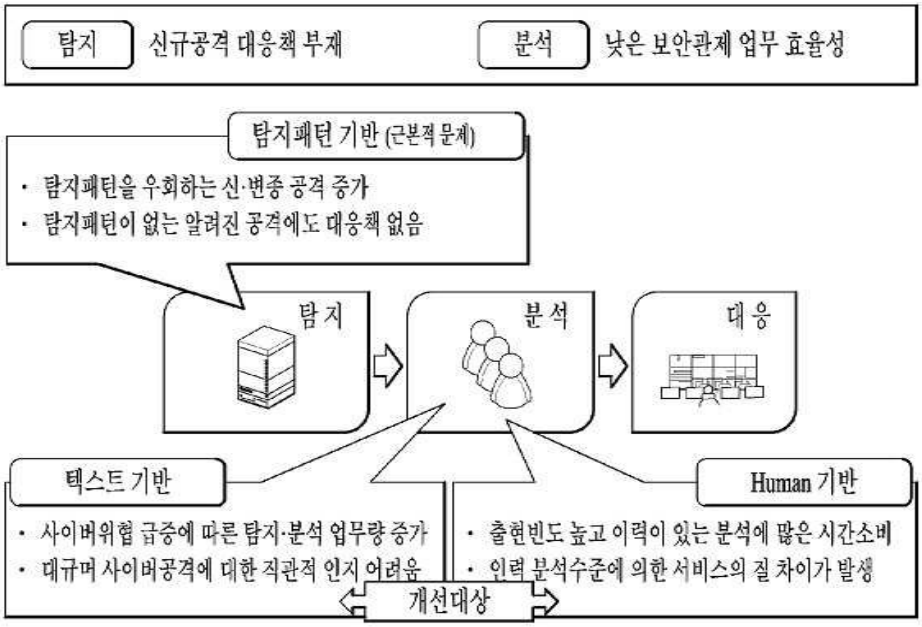
로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 프로세서가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0146] 또한, 이상에서는 본 발명의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해돼서는 안 될 것이다.

[0147] 그리고, 당해 명세서에서는 물건 발명과 방법 발명이 모두 설명되고 있으며, 필요에 따라 양 발명의 설명은 보충적으로 적용될 수가 있다.

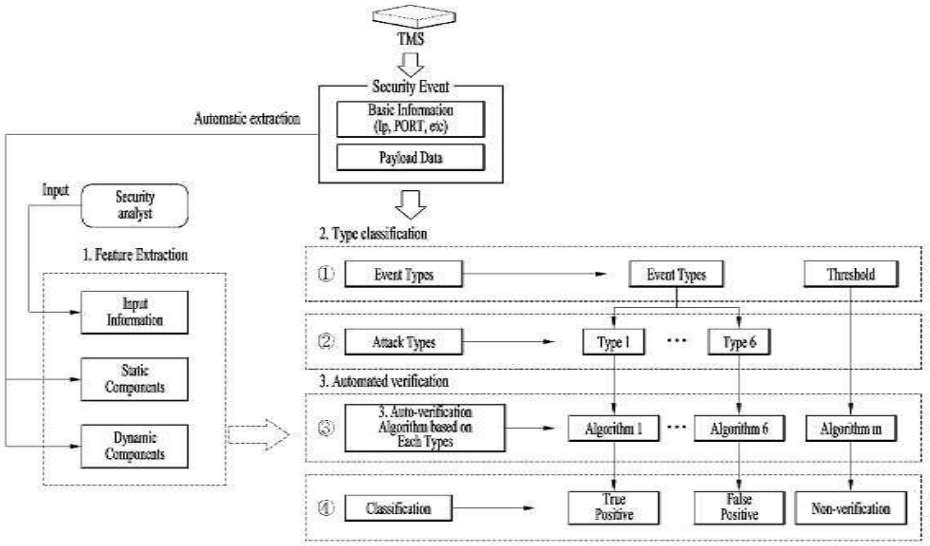
도면

도면1



※ 과학기술사이버안전센터의 2012년 수집정보 기준, 1일 약 7백만 건의 보안이벤트 발생

도면2



도면3

Essential item	Institute IP list
Additional item	Black IP list
	White IP list
	Black FQDN list
	White FQDN list
	String lists for the five attack types

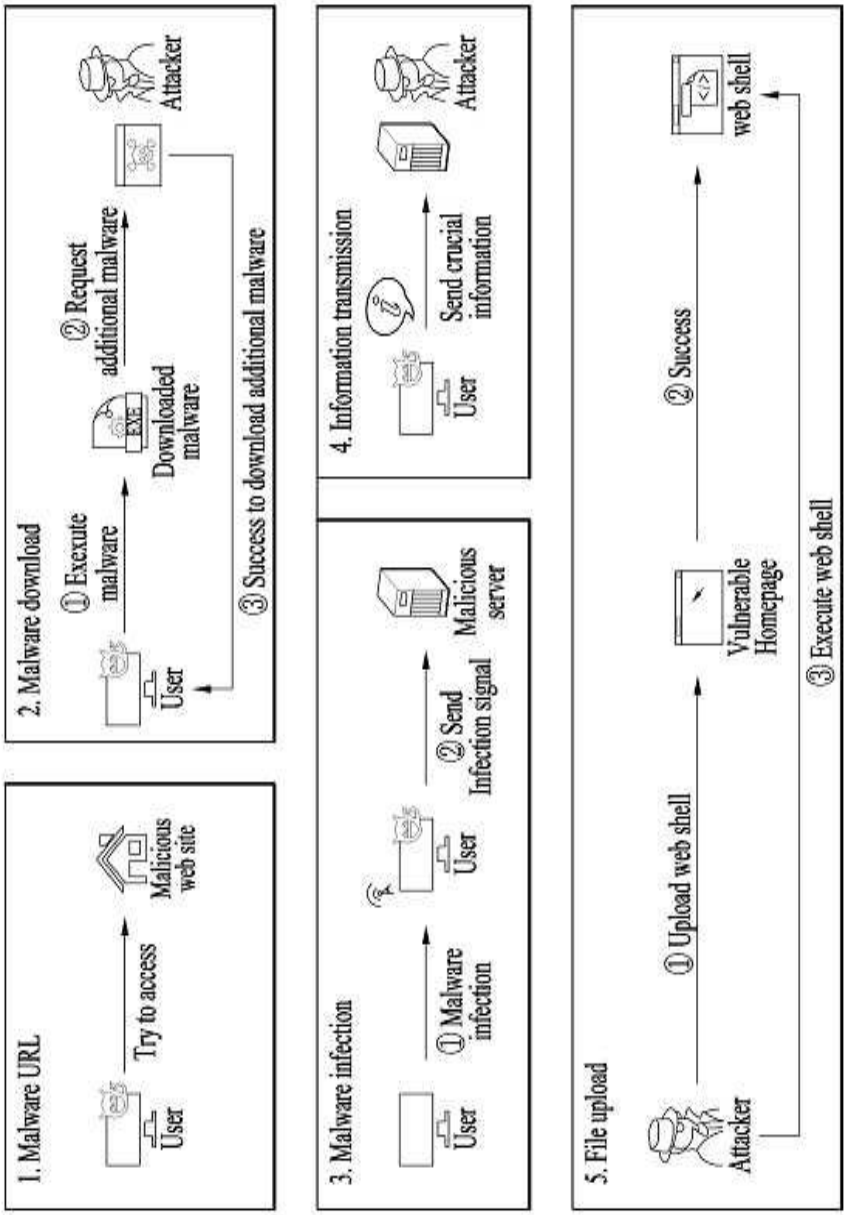
도면4

Attack TYpe	Strings for true positives	
Malicious URL	USER	POST
	CWD	PASS
	/ttt/sty.htm	user-agent : wget
	NICK	
Malware download	-	
Malware infection	GhOst	X.C...
	x.Kc"...	o.b.j.e.c.t
	t.a.b.l.e	&&&&&
	filepath=	filename=
	RooKIE	
Information transmission	mac=	username=
	os=	WolfDDos
	register	#information
	avs=	prj=
	ver=	logdata=
	pwd=	Windows
	ie=	ADDNEW
	MB	MHz
	provider	uin=
	machine	nickname
	npki	ip
	uid=	name
	cpuname=	mobile
File upload	EasyPhpWebShell	zecmd
	idssvc	iesvc
	Action=MainMenu	Action=ScanPort
	JspSpy Ver	Not Found Shell
	.asp.jpg	.php.jpg
	200 OK	

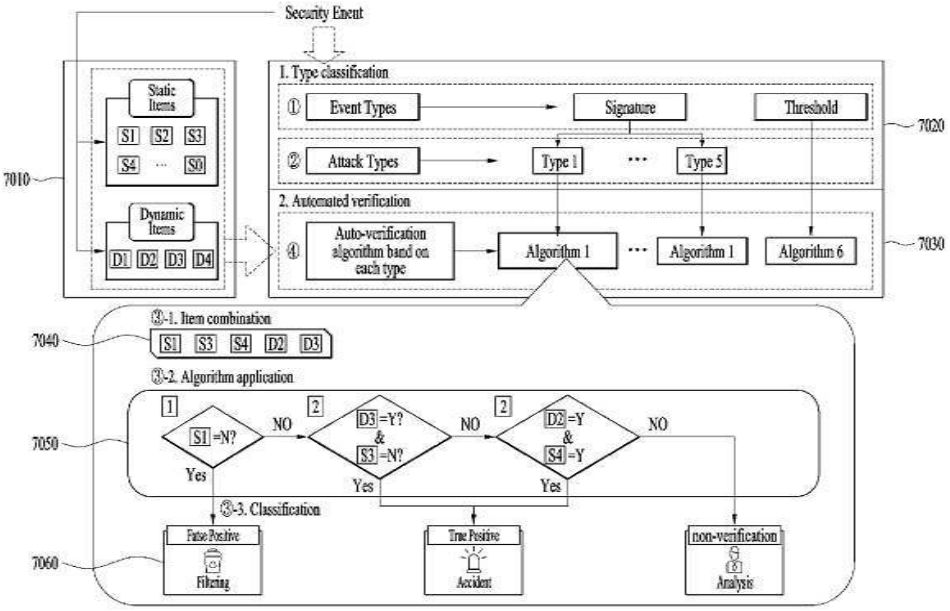
도면5

Static components	Source IP
	Destination
	Source Port
	Destination Port
	Host
	Payload
	HTTP Referer
	The number of security events
Dynamic components	Host URL
	Get URL
	Website source code
	Destination Port

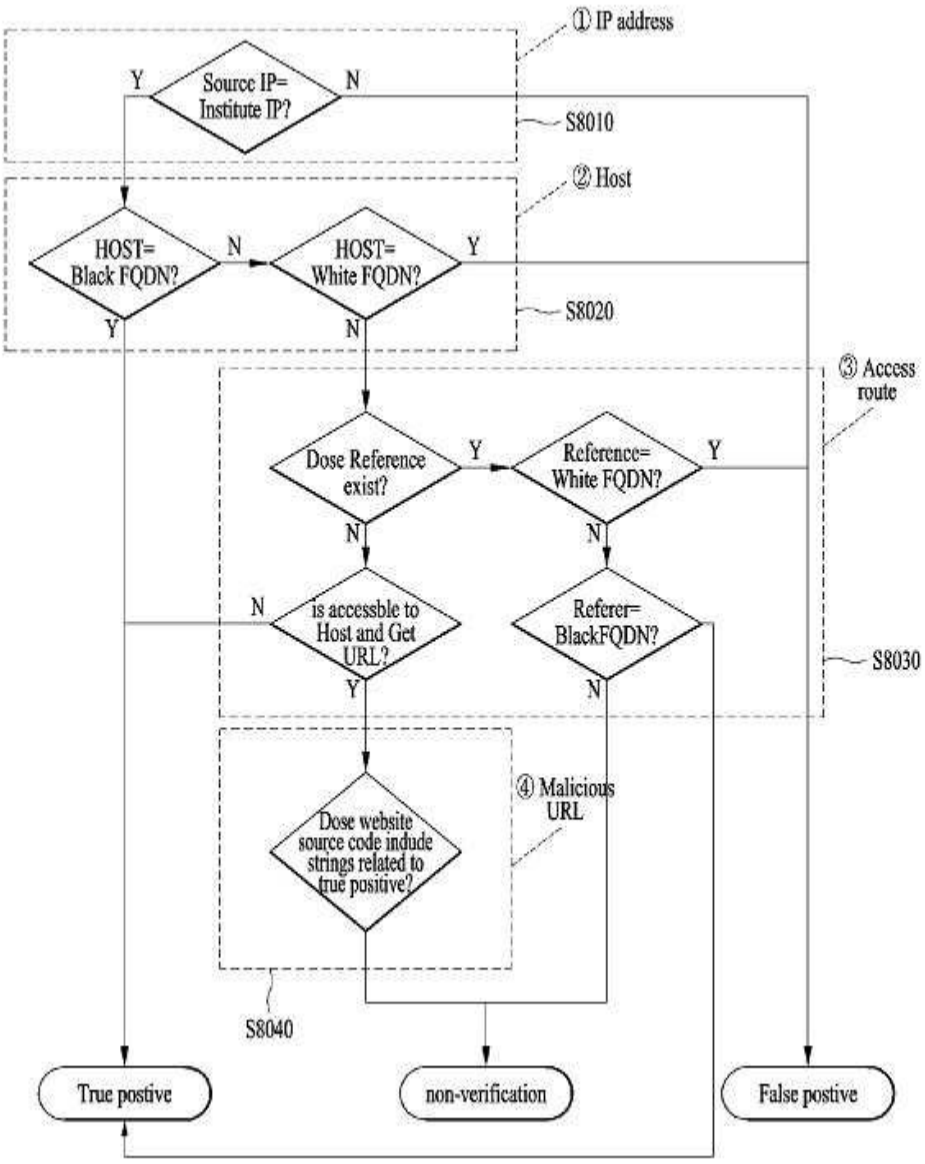
도면6


1. Malware URL
User
Try to access
Malicious web site
2. Malware download
User
① Exexute malware
Downloaded malware
② Request additional malware
Attacker
③ Success to download additional malware
3. Malware infection
User
① Malware infection
User
② Send Infection signal
Malicious server
4. Information transmission
User
Send crucial information
Attacker
5. File upload
Attacker
① Upload web shell
Vulnerable Homepage
② Success
web shell
③ Execute web shell

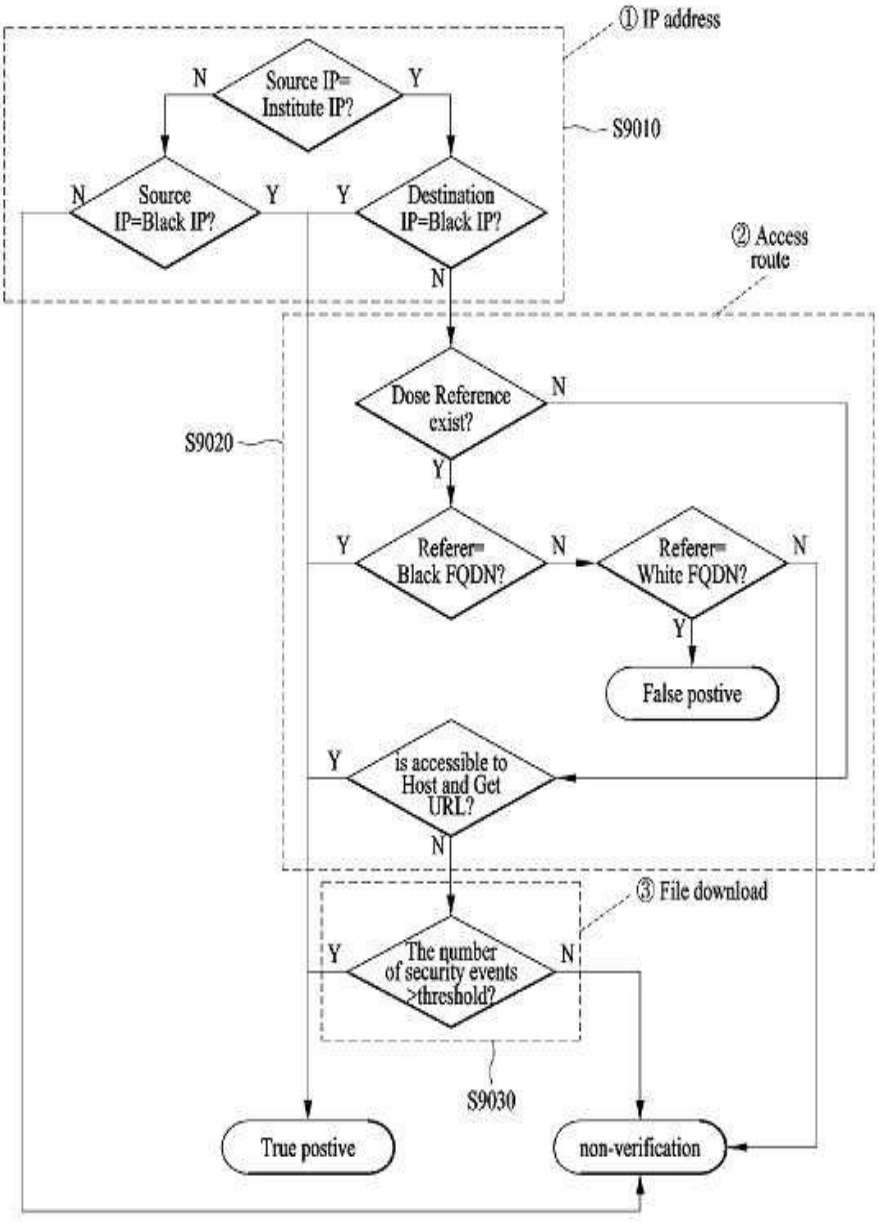
도면7


Security Event
7010
Static Items
S1 S2 S3
S4 ... S0
Dynamic Items
D1 D2 D3 D4
1. Type classification
① Event Types
Signature
Threshold
7020
② Attack Types
Type 1
Type 5
2. Automated verification
④ Auto-verification algorithm based on each type
Algorithm 1
Algorithm 1
Algorithm 6
7030
③-1. Item combination
7040
S1 S3 S4 D2 D3
③-2. Algorithm application
7050
1
S1 =N?
NO
2
D3 =Y?
&
S3 =N?
NO
2
D2 =Y
&
S4 =Y
NO
Yes
Yes
Yes
③-3. Classification
7060
False Positive
Filtering
True Positive
Accident
non-verification
Analysis

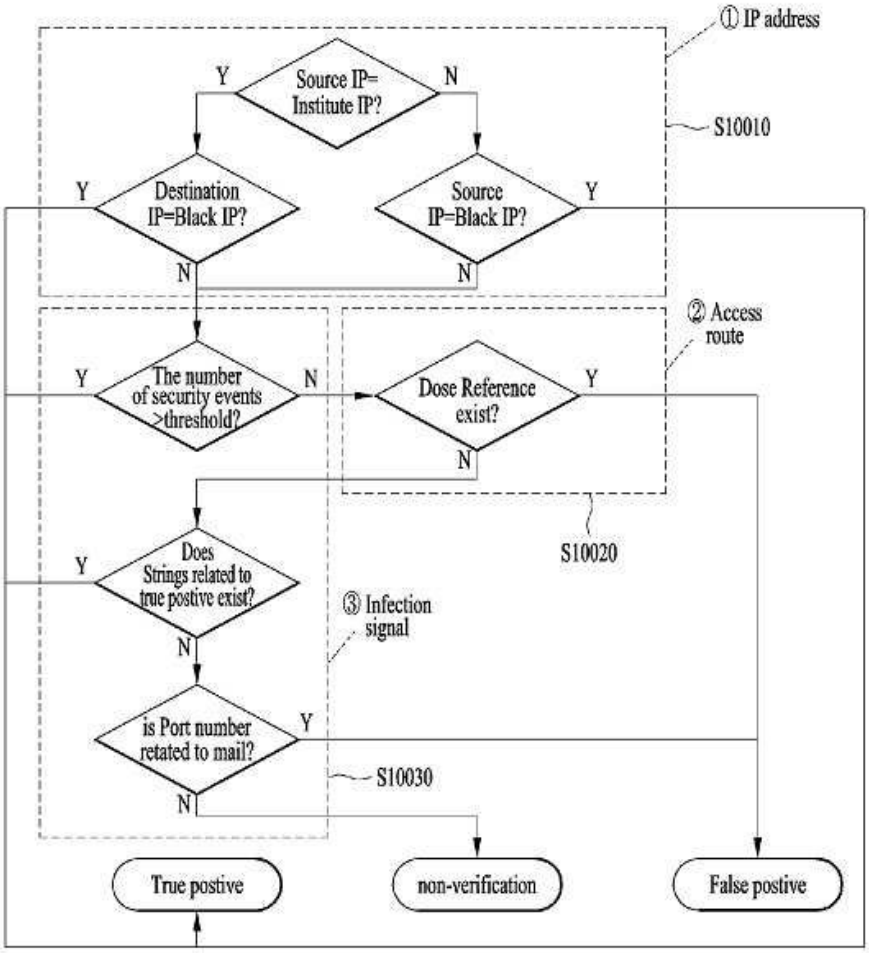
도면8


① IP address
Source IP= Institute IP?
Y
N
S8010
② Host
HOST= Black FQDN?
HOST= White FQDN?
S8020
③ Access route
Dose Reference exist?
Reference= White FQDN?
is accessble to Host and Get URL?
Referer= BlackFQDN?
S8030
④ Malicious URL
Dose website source code indude strings related to true positive?
S8040
True postive
non-verification
False postive

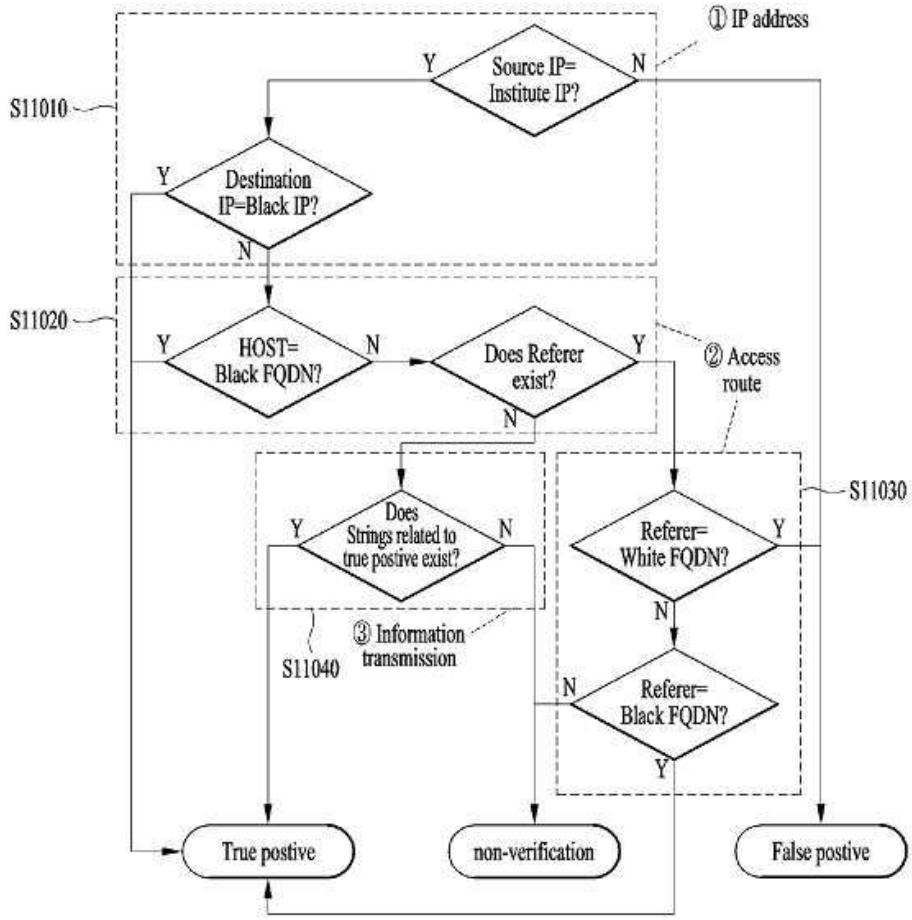
도면9


① IP address
Source IP= Institute IP?
N
Y
S9010
Source IP=Black IP?
N
Y
Y
Destination IP=Black IP?
N
② Access route
S9020
Dose Reference exist?
N
Y
Y
Referer= Black FQDN?
N
Referer= White FQDN?
N
Y
False postive
Y
is accessible to Host and Get URL?
N
③ File download
Y
The number of security events >threshold?
N
S9030
True postive
non-verification

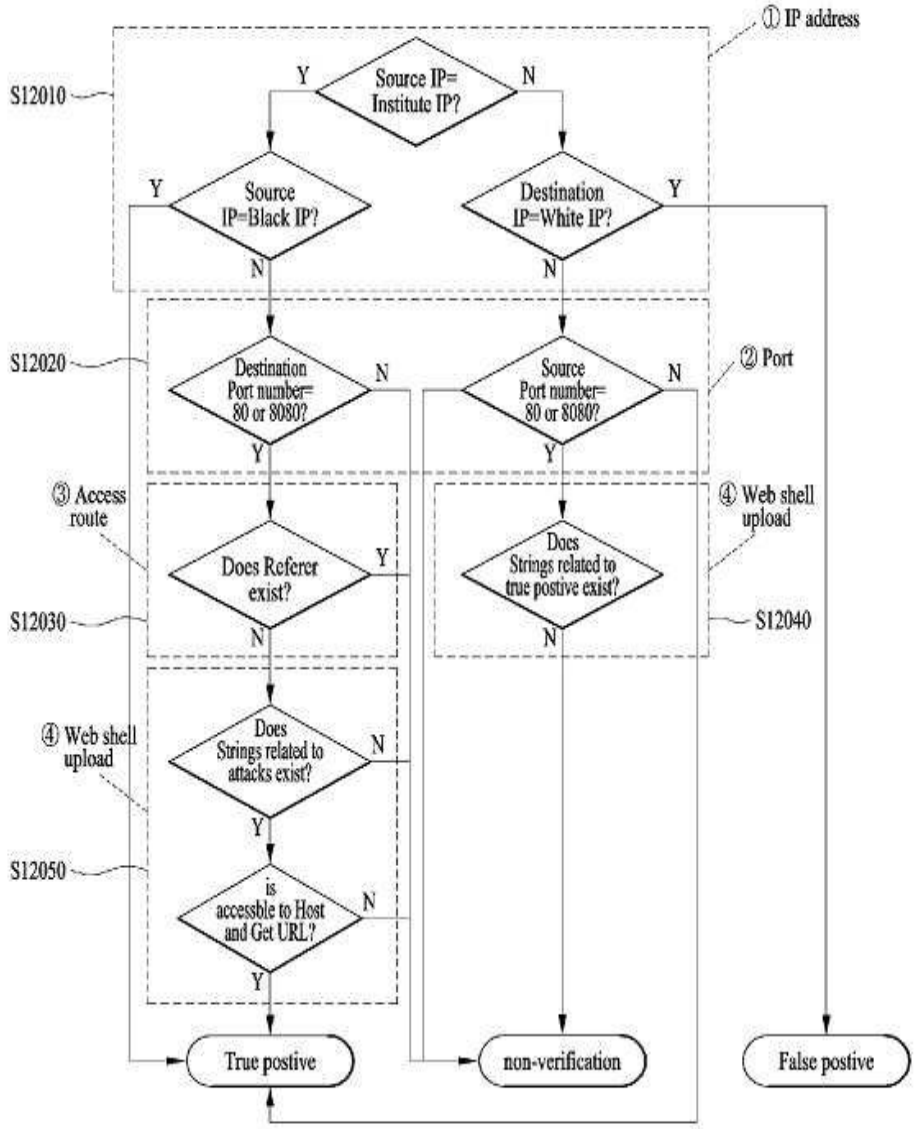
도면10


① IP address
Source IP= Institute IP?
Y
N
S10010
Destination IP=Black IP?
Source IP=Black IP?
② Access route
The number of security events >threshold?
Dose Reference exist?
S10020
Does Strings related to true postive exist?
③ Infection signal
is Port number retated to mail?
S10030
True postive
non-verification
False postive

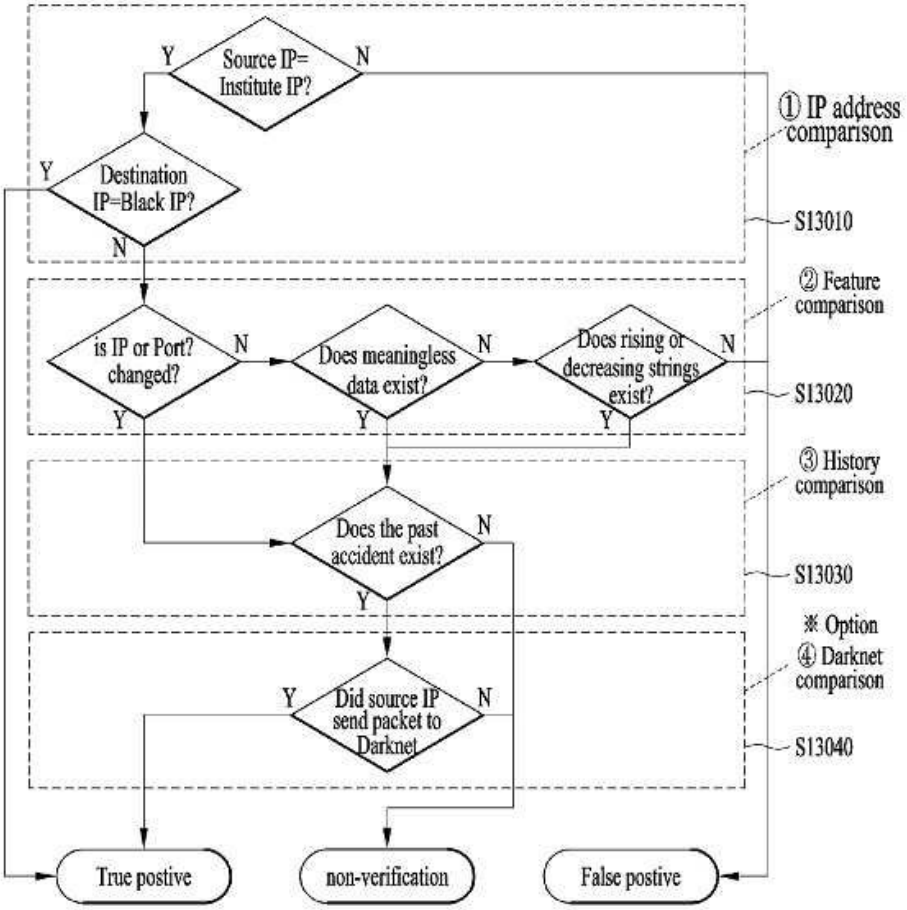
도면11


① IP address
Source IP= Institute IP?
Y
N
S11010
Destination IP=Black IP?
Y
N
S11020
HOST= Black FQDN?
Y
N
Does Referer exist?
Y
N
② Access route
S11030
Does Strings related to true postive exist?
Y
N
Referer= White FQDN?
Y
N
③ Information transmission
S11040
Referer= Black FQDN?
N
Y
True postive
non-verification
False postive

도면12


① IP address
S12010
Source IP= Institute IP?
Y
N
Source IP=Black IP?
Destination IP=White IP?
S12020
Destination Port number= 80 or 8080?
Source Port number= 80 or 8080?
② Port
③ Access route
④ Web shell upload
Does Referer exist?
Does Strings related to true postive exist?
S12030
S12040
④ Web shell upload
Does Strings related to attacks exist?
S12050
is accessble to Host and Get URL?
True postive
non-verification
False postive

도면13



도면14

Attack Type	The number of signature rules			
	2013	2014	2015	Unique signature rules
Malicious URL	27	13	5	36
Malware download	4	2	1	5
Malware infection	43	26	19	52
Information transmission	10	8	3	14
File upload	12	15	10	21
Threshold	-	6	-	6
Total	96	70	38	134

도면15

	Event name	Number of total security events			Number of total security events			Number of total security events			Accuracy
		2013	2014	2015	2013	2014	2015	2013	2014	2015	
1	cn*****er	443,032	157,594	89,182	66	17	18	442,966	157,577	89,164	100%
2	bl**.****.com.cn	3,150	6,882	59,861	13	0	0	3,137	6,882	59,861	100%
3	qaz***.***.org	260,712	47,526	36,608	11	6	0	260,701	475,254	36,608	100%
4	R***ng	35,792	13,173	35	10	2	1	35,782	13,171	34	100%
5	us******nt:ly**	33	0	0	6	0	0	27	0	0	100%
6	http-****	34,111	10,807	0	4	0	0	34,107	10,807	0	100%
7	www.sa****.ru	44	0	0	3	0	0	41	0	0	100%
					...						
36	K***n C** ***.**.***.***	6,432	14	124	1	0	0	6,431	0	0	100%
	Total	2,704,674	942,475	797,023	138	111	221	2,704,536	942,364	796,802	100%

도면16

	Event name	Number of total security events			Number of total security events			Number of total security events			Accuracy
		2013	2014	2015	2013	2014	2015	2013	2014	2015	
1	ma**-***	5,232	6,612	3,553	201	216	545	5,031	6,396	3,008	100%
2	iframe(**7890)	19	2	2	3	0	0	16	2	2	100%
3	pi*****(MZ)	1	0	0	1	0	0	0	0	0	100%
4	t******(exe)	2,033	1,846	1,223	1	0	0	2,032	1,846	1,223	100%
5	RAT(t******)	0	27,924	4,873	0	3	0	0	27,921	4,873	100%
	Total	7,285	36,381	9,631	206	219	545	7,079	36,165	9,106	100%

도면17

	Event name	Number of total security events			Number of total security events			Number of total security events			Accuracy
		2013	2014	2015	2013	2014	2015	2013	2014	2015	
1	g***t-sub***e	54,790	3,886	603	96	19	0	54,694	3,867	603	100%
2	G***t3.7	2,747	141	8	17	3	0	2,730	138	0	100%
3	ddos-tool(su******us)	3,339	16,787	840	59	0	1	3,280	16,787	839	100%
4	tro***-cn-g***t	46,922	33,673	7,136	56	12	5	46,866	33,661	7,131	100%
5	h***th	19,947	473,905	11,951,096	25	10	2	19,922	473,895	11,951,091	100%
6	Da*****et 5.3.1	187	265	41	11	13	1	176	252	40	100%
7	Gu***ot(A**)	1,676	831	264	9	6	6	1,667	825	258	100%
					...						
51	Bit******ner	0	17,061,447	1,897,895	0	10	12	0	17,061,437	1,897,883	100%
52	PA****T	0	14	0	0	4	0	0	10	0	100%
	Total	1,411,259	18,492,488	14,810,746	504	131	337	1,410,755	18,492,357	14,810,409	100%

도면18

	Event name	Number of total security events			Number of total security events			Number of total security events			Accuracy
		2013	2014	2015	2013	2014	2015	2013	2014	2015	
1	D*5	22,528	4,304	8,479	1,030	446	23	21,498	3,858	8,456	100%
2	F****w	3,090	770	445	151	5	2	2,939	765	443	100%
3	A***info()	1,483	661	125	74	12	0	1,409	649	125	100%
4	RTA(ca******1.2)	167	237	6,993	8	0	0	159	237	6,993	100%
5	do****t	556	24	3	4	0	0	552	24	3	100%
6	su******us-net***	1,146	358	216	3	0	0	1,143	358	216	100%
7	u****d(**file)	225	193	83	3	2	0	222	191	83	100%
8	URL(www.g*****a.co.kr)	246	0	0	2	0	0	244	0	0	100%
9	da******.bot	1	0	24	1	0	0	0	0	24	100%
10	fta.go*****n	13,101	153	0	1	0	0	13,100	153	0	100%
11	port(5****))	0	19	0	0	3	0	0	16	0	100%
12	do*****,co.kr	0	61	0	0	1	0	0	60	0	100%
13	port(1**3))	0	93	365	0	1	4	0	92	361	100%
14	z***.k***f.com	0	483	23	0	1	0	0	482	23	100%
	Total	42,543	7,356	16,756	1,277	471	29	41,266	6,885	16,727	100%

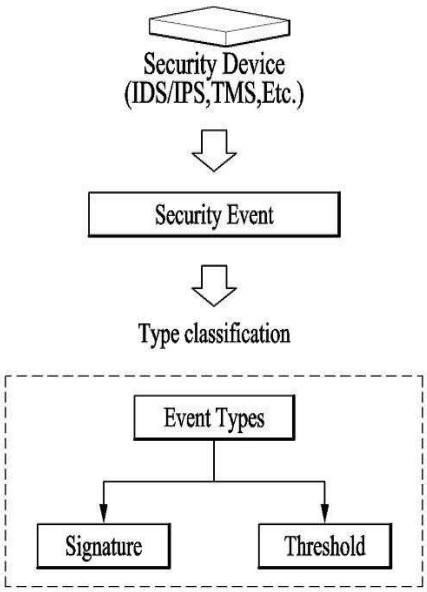
도면19

	Event name	Number of total security events			Number of total security events			Number of total security events			Accuracy
		2013	2014	2015	2013	2014	2015	2013	2014	2015	
1	file(up****)	79,186	571,698	676,223	5	3	3	79,181	571,695	676,220	100%
2	Su******us(D****)	4	509,765	8,450,237	4	4	1	0	509,761	8,450,236	100%
3	po**-net****	15	24	22	2	1	0	13	23	22	100%
4	j** FiLE Br*****)	157	433	969	2	5	4	155	428	965	100%
5	Da****(file*****)	0	326	632	0	12	34	0	314	598	100%
6	web*****(top****t)	27	1	11	1	1	0	26	0	11	100%
7	web*****(php_***)	492	28,251	53,516	0	1	2	492	28,250	53,514	100%
					...						
20	web*****(W**2.1)	0	5	0	0	1	0	0	4	0	100%
21	attack(u****)	0	1,307	0	0	1	0	0	1,306	0	100%
	Total	88,414	1,222,146	28,795,133	22	37	54	88,392	1,222,109	28,795,079	100%

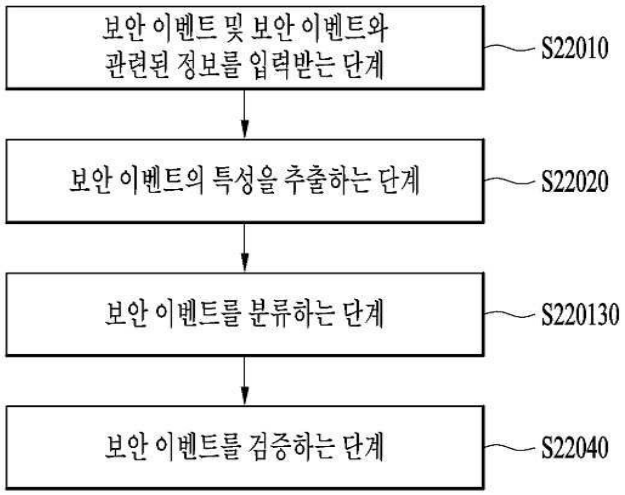
도면20

	Event name	Number of true positives	period	Accuracy
1	TCP syn flooding	13	2014.01.01~2014.10.20	99%
2	TCP service scan	3	2014.01.01~2014.10.20	100%
3	UDP flooding fragmented	4	2014.01.01~2014.10.20	99%
4	TCP null scan	11	2009.01.01~2011.12.31	100%
5	UDP port scan	182	2009.01.01~2011.12.31	100%
6	UDP flooding same IP	2	2014.01.01~2014.10.20	100%
	Total	215		

도면21


Security Device
(IDS/IPS,TMS,Etc.)
Security Event
Type classification
Event Types
Signature
Threshold

도면22


보안 이벤트 및 보안 이벤트와 관련된 정보를 입력받는 단계
S22010
보안 이벤트의 특성을 추출하는 단계
S22020
보안 이벤트를 분류하는 단계
S220130
보안 이벤트를 검증하는 단계
S22040