(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년06월24일
(11) 등록번호 10-1991737
(24) 등록일자 2019년06월17일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/26* (2006.01)
(52) CPC특허분류
H04L 63/1408 (2013.01)
H04L 43/045 (2013.01)
(21) 출원번호 10-2017-0115074
(22) 출원일자 2017년09월08일
심사청구일자 2017년09월08일
(65) 공개번호 10-2019-0028076
(43) 공개일자 2019년03월18일
(56) 선행기술조사문헌
KR100992066 B1*
KR101689299 B1*
KR1020080050919 A*
KR1020110062561 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술정보연구원
대전광역시 유성구 대학로 245 (어은동)
(72) 발명자
송중석
세종특별자치시 남세종로 469, 412동 904호(보람동, 호려울마을4단지)
권태웅
대전광역시 유성구 농대로2번길 29-6, 베스트빌 306호(어은동)
(뒷면에 계속)
(74) 대리인
김용인, 지관영

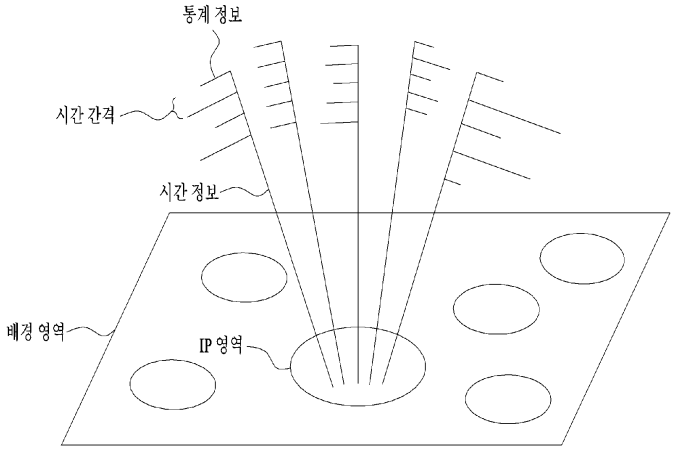
전체 청구항 수 : 총 15 항 심사관 : 오수정

(54) 발명의 명칭 **공격자 가시화 방법 및 장치**

(57) 요 약

본 발명은 공격자 가시화 방법 및 장치에 관한 것이다. 본 발명의 일 실시예에 따른 공격자 가시화 장치는 보안이벤트를 저장하는 스토리지로부터 상기 보안이벤트를 수신하고, 여기서 상기 전처리는 상기 보안이벤트에 대한 정보를 추출하고, 상기 보안이벤트에 대한 정보를 내부 공격자 영역 및 외부 공격자 영역으로 분류하는 통계정보 생성하고, 여기서 상기 통계정보 생성은 상기 내부 공격자 영역 및 상기 외부 공격자 영역에 대하여 상기 보안이벤트에 대한 통계정보를 추출하고, 상기 보안이벤트에 대한 정보를 기초로 상기 보안이벤트의 공격행위를 가시화하는 가시화하고, 여기서 상기 가시화는 배경영역, IP 주소 영역을 기초로 상기 보안이벤트에 대한 통계정보를 시간 순서에 따라서 가시화하는 장치를 포함한다.

대 표 도 - 도18



(52) CPC특허분류
H04L 63/0236 (2013.01)
(72) 발명자
박진학
서울특별시 성북구 오패산로3길 17, 105동 2102호 (하월곡동, 동신아파트)
최장원
대전광역시 서구 둔산북로 215, 7동 1408호(둔산동, 가람아파트)

명 세 서

청구범위

청구항 1

보안이벤트를 저장하는 스토리지로부터 상기 보안이벤트를 수신하는 전처리 모듈, 여기서 상기 전처리 모듈은 상기 보안이벤트에 대한 정보를 추출함;

상기 보안이벤트에 대한 정보를 내부 공격자 영역 및 외부 공격자 영역으로 분류하는 통계정보 모듈, 여기서 상기 통계정보 모듈은 상기 내부 공격자 영역 및 상기 외부 공격자 영역에 대하여 상기 보안이벤트에 대한 통계정보를 추출함;

상기 보안이벤트에 대한 정보를 기초로 상기 보안이벤트의 공격행위를 가시화하는 가시화 모듈을 포함하고,

상기 가시화 모듈은 상기 보안이벤트에 대한 통계정보를 IP 주소 영역에 표현하고, 상기 IP 주소 영역은 시간 간격에 따라 표현되고,

상기 내부 공격자 영역 또는 상기 외부 공격자 영역에 대응하는 지도를 표시하고,

상기 IP 주소 영역의 IP 주소 및 상기 IP 주소에 대응되는 상기 내부 공격자 영역 또는 상기 외부 공격자 영역 중 적어도 하나의 특정 영역을 연결시키는,

공격자 가시화 장치.

청구항 2

제 1 항에 있어서,

상기 보안이벤트에 대한 정보는 출발지 정보, 목적지 정보, 발생 시간, 명칭, 및 공격 유형을 포함하는,

공격자 가시화 장치.

청구항 3

제 2 항에 있어서,

상기 출발지 정보는 상기 보안이벤트에 대한 출발지 IP 주소 및 포트 번호를 포함하고,

상기 목적지 정보는 상기 보안이벤트에 대한 도착지 IP 주소 및 포트 번호를 포함하는,

공격자 가시화 장치.

청구항 4

제 1 항에 있어서,

상기 내부 공격자 영역은 대상기관의 내부 공격자 IP 주소이고,

상기 외부 공격자 영역은 상기 내부 공격자 영역에 포함되는 않는 외부 공격자 IP 주소인,

공격자 가시화 장치.

청구항 5

제 1 항에 있어서,

상기 통계정보 모듈은 상기 내부 공격자 영역 및 상기 외부 공격자 영역에 대하여 상기 보안이벤트에 대한 통계정보를 추출하여 통계정보 스토리지에 저장하는,

공격자 가시화 장치.

청구항 6

제 1 항에 있어서,

상기 IP 주소에 대한 보안이벤트의 공격행위가 발생한 경우, 상기 가시화 모듈은 상기 IP 주소 및 상기 IP 주소에 대응되는 특정 영역을 실시간으로 연결시키는,

공격자 가시화 장치.

청구항 7

삭제

청구항 8

제 1 항에 있어서,

상기 IP 주소 영역 내에 상기 보안이벤트에 대한 통계정보를 시간 순서에 따라서 선분 또는 곡선 중 적어도 하나의 형태로 가시화하는,

공격자 가시화 장치.

청구항 9

보안이벤트를 저장하는 스토리지로부터 상기 보안이벤트를 수신하는 전처리 단계, 여기서 상기 전처리 단계는 상기 보안이벤트에 대한 정보를 추출함;

상기 보안이벤트에 대한 정보를 내부 공격자 영역 및 외부 공격자 영역으로 분류하는 통계정보 생성 단계, 여기서 상기 통계정보 생성 단계는 상기 내부 공격자 영역 및 상기 외부 공격자 영역에 대하여 상기 보안이벤트에 대한 통계정보를 추출함;

상기 보안이벤트에 대한 정보를 기초로 상기 보안이벤트의 공격행위를 가시화하는 가시화 단계를 포함하고,

상기 가시화 단계는 상기 보안이벤트에 대한 통계정보를 IP 주소 영역에 표현하고, 상기 IP 주소 영역은 시간 간격에 따라 표현되고,

 상기 내부 공격자 영역 또는 상기 외부 공격자 영역에 대응하는 지도를 표시하고,

상기 IP 주소 영역의 IP 주소 및 상기 IP 주소에 대응되는 상기 내부 공격자 영역 또는 상기 외부 공격자 영역 중 적어도 하나의 특정 영역을 연결시키는,

 공격자 가시화 방법.

청구항 10

제 9 항에 있어서,

상기 보안이벤트에 대한 정보는 출발지 정보, 목적지 정보, 발생 시간, 명칭, 및 공격 유형을 포함하는,

공격자 가시화 방법.

청구항 11

제 10 항에 있어서,

상기 출발지 정보는 상기 보안이벤트에 대한 출발지 IP 주소 및 포트 번호를 포함하고,

상기 목적지 정보는 상기 보안이벤트에 대한 도착지 IP 주소 및 포트 번호를 포함하는,

공격자 가시화 방법.

청구항 12

제 9 항에 있어서,

상기 내부 공격자 영역은 대상기관의 내부 공격자 IP 주소이고,

상기 외부 공격자 영역은 상기 내부 공격자 영역에 포함되는 않는 외부 공격자 IP 주소인,

공격자 가시화 방법.

청구항 13

제 9 항에 있어서,

상기 통계정보 생성 단계는 상기 내부 공격자 영역 및 상기 외부 공격자 영역에 대하여 상기 보안이벤트에 대한 통계정보를 추출하여 통계정보 스토리지에 저장하는,

공격자 가시화 방법.

청구항 14

제 9 항에 있어서,

상기 IP 주소에 대한 보안이벤트의 공격행위가 발생한 경우, 상기 가시화 단계는 상기 IP 주소 및 상기 IP 주소에 대응되는 특정 영역을 실시간으로 연결시키는,

공격자 가시화 방법.

청구항 15

삭제

청구항 16

제 9 항에 있어서,

상기 IP 주소 영역 내에 상기 보안이벤트에 대한 통계정보를 시간 순서에 따라서 선분 또는 곡선 중 적어도 하나의 형태로 가시화하는,

공격자 가시화 방법.

청구항 17

보안이벤트를 저장하는 스토리지로부터 상기 보안이벤트를 수신하여 상기 보안이벤트에 대한 정보를 추출하고,

상기 보안이벤트에 대한 정보를 내부 공격자 영역 및 외부 공격자 영역으로 분류하여 상기 내부 공격자 영역 및 상기 외부 공격자 영역에 대하여 상기 보안이벤트에 대한 통계정보를 추출하고,

상기 보안이벤트에 대한 정보를 기초로 상기 보안이벤트의 공격행위를 가시화하기 위하여, 상기 보안이벤트에 대한 통계정보를 IP 주소 영역에 표현하고, 상기 IP 주소 영역은 시간 간격에 따라 표현되고, 상기 내부 공격자 영역 또는 상기 외부 공격자 영역에 대응하는 지도를 표시하고, 상기 IP 주소 영역의 IP 주소 및 상기 IP 주소에 대응되는 상기 내부 공격자 영역 또는 상기 외부 공격자 영역 중 적어도 하나의 특정 영역을 연결시키는,

프로그램을 저장하는 저장매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 공격자 가시화 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 기존의 보안이벤트 가시화 기술들은 보안이벤트에 포함된 기본정보(IP 주소, 포트, 프로토콜, 보안이벤트 명등)만을 이용하여 보안이벤트를 가시화하는 것에 초점을 맞추고 있다. 특히, 공격자 피해자 IP 발생 시간/순위, 공격자 피해자 국가 순위, 보안이벤트 발생 시간/순위 등 보안이벤트에 대한 전체적인 동향 분석 및 현황 파악은 가능하다.

[0003] 따라서, 개별 IP 주소의 공격행위에 대한 상세 분석 및 실제 공격을 유발한 IP 주소에 대한 직접적인 탐지 분석이 불가능하다.

[0004] 기존의 보안이벤트 가시화 기술들은 단시간에 발생한 보안이벤트에 대한 가시화에만 초점을 맞추고 있어 APT 공격과 같은 지속적 연속적으로 발생하는 사이버공격을 탐지할 수 없다.

[0005] 대부분의 사이버공격은 공격 시도부터 공격 성공까지 장기간에 걸쳐 지속적으로 발생하기 때문에 기존의 가시화 기술을 이용하여 보안이벤트에 대한 실제 공격여부를 판단하는 것은 매우 어렵다.

[0006] 기존의 보안이벤트 가시화 기술들은 보안이벤트에 포함된 기본정보(IP주소, 포트, 프로토콜, 보안이벤트 명등)만을 이용하여 보안이벤트를 가시화하는 것에 초점을 맞추고 있다. 특히, 공격자 피해자 IP 발생 시간/순위, 공격자 피해자 국가 순위, 보안이벤트 발생 시간/순위 등 보안이벤트에 대한 전체적인 동향 분석 및 현황 파악은 가능하다.

[0007] 기존의 보안이벤트 가시화 기술들은 보안이벤트 기반의 가시화에만 초점을 맞추고 있어, 공격에 직접적으로 가담하지 않는 IP등을 탐지하는 것은 불가능하다.

[0008] 다수의 악성 봇들을 이용하여 공격하는 DDoS공격들의 경우 공격자들을 탐지하는 것보다는 이들을 조종하는 C&C서버를 탐지·대응하여 근본적인 원인을 차단하는 것이 매우 중요하다.

[0009] 하지만, C&C서버는 피해 서버들과 직접적인 관계가 없으며, 주기적으로 변경되기 때문에 탐지하는 것이 매우 어렵다.

[0010] 또한, 기존의 IP상관관계 가시화 기술들은 IP간의 보안이벤트 발생량 기반의 분류알고리즘들을 사용하여 IP간의 관계성을 나타내기 때문에 보안이벤트 발생량이 적지만 위험도가 높은 IP들의 관계를 찾는 것이 매우 어렵다.

[0011] C&C서버는 좀비 PC들과 통신 시 다량의 데이터를 송·수신하지 않기 때문에 기존의 가시화 방법들로 C&C서버를 찾는 것이 매우 어렵다.

발명의 내용

해결하려는 과제

[0012] 본 발명이 이루고자 하는 과제는 IDS/IPS 등 탐지규칙 기반 보안장비가 탐지한 보안이벤트의 모든 IP 주소에 대한 이상행위를 가시화하는 방법을 제공하는 것이다.

[0013] 본 발명이 이루고자 하는 과제는 이상행위에 대한 실시간 및 통계적 가시화를 통해 모든 IP의 실제 공격 여부를 직관적으로 탐지 분석하는 방법을 제공하는 것이다.

[0014] 본 발명이 이루고자 하는 과제는 IDS/IPS등의 탐지규칙 기반 보안장비가 탐지한 대용량 보안이벤트의 모든 IP주소간 상관관계를 가시화하는 방법을 제공하는 것이다.

[0015] 본 발명이 이루고자 하는 과제는 장기간동안 보안이벤트를 발생시킨 모든 IP주소 간 상관관계를 장기적 및 대규모 관점에서 가시화함으로써 공격그룹 및 공격체계(공격근원지, 유포지, 감염경로 등)을 유추 및 탐지하는 방법을 제공하는 것이다.

과제의 해결 수단

[0016] 본 발명의 목적에 따라, 여기에 포함되고 대략적으로 기재된 바와 같이, 보안이벤트를 발생시킨 IP 주소에 대한

공격행위를 실시간 및 장기적 관점에서 가시화하는 방법을 제안한다.

[0017] 나아가, 본 발명은 IP 주소에 대한 공격행위를 다양한 통계정보로 추출하고 이를 실시간 및 장기적으로 가시화하는 방법을 제안한다.

[0018] 본 발명은 장기간 보안이벤트를 발생시킨 모든 IP들, IP들의 보안이벤트 발생량, IP간의 관계성을 가시화하는 방법을 제안한다.

발명의 효과

[0019] 본 발명의 일 실시예에 따른 IP 주소 기반 사이버공격 실시간 및 통계적 가시화 방법 및 장치는 IP 주소의 실제 공격 유발 여부를 직관적 효율적으로 탐지하는 효과를 제공한다.

[0020] 본 발명의 일 실시예에 따른 IP 주소 기반 사이버공격 실시간 및 통계적 가시화 방법 및 장치는 실제 해킹공격을 유발한 IP 주소를 직관적으로 탐지하여 보안관제 업무의 효율성을 극대화하는 효과를 제공한다.

[0021] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 별도의 알고리즘 없이도 악성 IP들의 직관적·효율적 탐지를 할 수 있는 효과를 제공한다.

[0022] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 추가적인 분류 알고리즘 없이 가시화하기 때문에 데이터를 일정하게 표현할 수 있으며 데이터에 대한 왜곡이 없어 분석결과의 신뢰성 향상시키는 효과를 제공한다.

[0023] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 다수의 IP와 통신하는 IP, 블랙리스트 IP와 통신하는 IP, 보안이벤트를 다량 발생시키는 IP등을 한눈에 파악할 수 있기 때문에 보안관제 업무의 효율성을 극대화하는 효과를 제공한다.

도면의 간단한 설명

[0024] 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 시스템 개념도를 나타낸 도면이다.

도 15는 본 발명의 일 실시예에 따른 전처리 시스템을 나타낸 도면이다.

도 16은 본 발명의 일 실시예에 따른 내부 공격자 가시화 시스템을 나타낸 도면이다.

도 17은 본 발명의 일 실시예에 따른 외부 공격자 가시화 시스템을 나타낸 도면이다.

도 18은 본 발명의 일 실시예에 따른 가시화 방법을 나타낸 도면이다.

도 19는 본 발명의 일 실시예에 따른 가시화 방법을 나타낸 도면이다.

도 20은 본 발명의 일 실시예에 따른 가시화 방법을 나타낸 도면이다.

도 21은 본 발명의 일 실시예에 따른 시스템 구성도를 나타낸 도면이다.

도 22는 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치의 시스템을 나타낸 도면이다.

도 23은 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 방법을 나타낸 도면이다.

도 24는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법을 나타낸 도면이다.

도 25는 본 발명의 일 실시예에 따른 공격자 가시화 방법을 나타낸 도면이다.

도 26은 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 방법을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0025] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 실시예를 상세하게 설명하지만, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다.

[0026] 본 명세서에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어를 선택하였으나, 이는 해당분야에 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.

[0027] 도 1은 본 발명의 일 실시예에 따른 종래 탐지 패턴 기반의 보안 관제를 나타낸 도면이다.

[0028] 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 분석해야 하기 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.

[0029] 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.

[0030] 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.

[0031] 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치는 차세대 보안 관제 기술을 통해 전주기적 침해 사고에 대응할 수 있는 역량을 강화할 뿐만 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.

[0032] 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.

[0033] 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-CSC (Science & Technology Cyber Security Center))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.

[0034] 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.

[0035] 도 2는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 장치의 대용량 보안이벤트 자동 검증 구조를 나타낸 도면이다.

[0036] 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.

[0037] 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.

[0038] 본 발명의 일 실시예에 따른 유형 분류 모듈은 보안이벤트들을 시그니처 기반 보안이벤트 또는 임계치 기반 보안이벤트로 분류할 수 있다.

[0039] 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.

[0040] 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.

[0041] 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.

[0042] 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.

[0043] 도 3은 본 발명의 일 실시예에 따른 기본 정보 (basic information)를 나타낸 도면이다.

[0044] 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.

[0045] 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.

[0046] 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.

[0047] 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 사용되는 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.

[0048] 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.

[0049] 도 4는 본 발명의 일 실시예에 따른 공격 유형 별 정탐에 해당하는 문자열 리스트를 나타낸 도면이다.

[0050] 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.

[0051] 도 5는 본 발명의 일 실시예에 따른 정적 요소 및 동적 요소에 대한 설명을 나타낸 도면이다.

[0052] 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.

[0053] 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 내

의 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 실시예에 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.

[0054] 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.

[0055] 도 6은 본 발명의 일 실시예에 따른 공격 유형의 특성을 나타낸 도면이다.

[0056] 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.

[0057] 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.

[0058] 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.

[0059] 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.

[0060] 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.

[0061] 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.

[0062] 파일 업로드 (File upload)에 따르면, 공격자는 보안상 취약점이 존재하는 웹사이트를 공격하여 해당 웹서버로부터 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.

[0063] 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.

[0064] 도 7은 본 발명의 일 실시예에 따른 자동 검증 방법의 전체 프로세스를 나타낸 도면이다.

[0065] 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.

[0066] 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.

[0067] 도 8은 본 발명의 일 실시예에 따른 악성 URL (malicious URL) 유형에 대한 자동 검증 알고리즘을 나타낸 도면

이다.

[0068] 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.

[0069] 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.

[0070] 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.

[0071] 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 모듈은 추가 검증을 위한 다음 단계를 수행할 수 있다.

[0072] 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.

[0073] 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 다운로드 하려고 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 미검증 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.

[0080] 도 10은 본 발명의 일 실시예에 따른 악성코드 감염 (Malware infection) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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 들어, 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.

[0086] 도 11은 본 발명의 일 실시예에 따른 정보 전송 (information transmission) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0087] 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.

[0088] 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.

[0089] 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.

[0090] 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.

[0091] 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.

[0092] 도 12는 본 발명의 일 실시예에 따른 파일 업로드 (File upload) 유형에 대한 자동 검증 알고리즘을 나타낸 도면이다.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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.

[0097] 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.

[0098] 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.

[0099] 도 13은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트 (Threshold based security event)에 대한 자

동 검증 알고리즘을 나타낸 도면이다.

[0100] 이 도면은 본 발명의 일 실시예에 따른 임계치 기반의 보안이벤트의 자동 검증 알고리즘을 나타낸다.

[0101] 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.

[0102] 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.

[0103] 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.

[0104] 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.

[0105] 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.

[0106] 본 발명은 상술한 바와 같이, 본 발명의 일 실시예에 따른 보안이벤트를 자동 검증하는 장치, 각 공격 유형의 특성, 자동 검증 절차, 및/또는 각 유형에 따른 알고리즘을 포함할 수 있다. 이하에서는, 보안이벤트에 대한 정보를 가시화하는 장치 및 방법에 대해 설명한다. 본 발명에 따른 일 실시예는 내부 및/또는 외부 공격자를 가시화하는 장치 및 방법을 포함할 수 있다. 나아가, 본 발명에 따른 일 실시예는 공격자 상관정보를 가시화하는 장치 및 방법을 포함할 수 있다.

[0107] 이하에서는, 본 발명의 일 실시예에 따른 내부 및/또는 외부 공격자를 가시화하는 장치 및 방법에 대해서 설명한다.

[0108] 도 14는 본 발명의 일 실시예에 따른 시스템 개념도를 도시한다.

[0109] 도 14에 도시된 바와 같이, 본 발명의 일 실시예에 따른 공격자 가시화 장치의 시스템 개념도는 보안이벤트 저장 스토리지, 내외부 가시화 시스템을 포함한다. 여기서, 내외부 가시화 시스템은 이하에서 가시화 시스템으로 명명될 수 있다.

[0110] 보안이벤트 저장 스토리지는 보안이벤트를 저장할 수 있다. 본 발명의 일 실시예에 따라 보안이벤트 저장 스토리지는 가시화 시스템에서 보안이벤트 요청을 수신하고, 보안이벤트 요청에 따라서 보안이벤트를 전송할 수 있다.

[0111] 가시화 시스템(또는 내외부 가시화 시스템)은 전처리 모듈, 통계정보 생성/관리 모듈, 가시화 모듈을 포함할 수 있고, 통계 정보 스토리지를 더 포함할 수 있다. 본 발명의 일 실시예에 따른 공격자 가시화 장치는, 전처리 모듈, 통계정보 생성/관리 모듈, 및/또는 가시화모듈로부터 통계정보를 수신하여 통계정보 스토리지에 저장할 수 있다. 본 발명의 일 실시예에 따른 공격자 가시화 장치는 통계정보 스토리지를 통해 통계정보를 요청하고 송수신할 수 있다.

[0112] 도 14에 도시된 본 발명의 일 실시예에 따른 공격자 가시화 장치의 시스템 개념도의 상세 시스템과 모듈을 이하에서 설명한다.

[0113] 도 14에 도시된 보안이벤트 저장 스토리지는 도 15의 침해위협관리 시스템에 위치한 보안이벤트를 저장하는 스토리지에 해당할 수 있다. 도 14에 도시된 가시화 시스템의 상세 시스템과 모듈은 도 15 내지 17에서 설명한다. 여기서, 가시화 시스템은 내외부 가시화 시스템을 의미한다. 도 14에 도시된 전처리 모듈은 도 15에 도시된 전처리 시스템에 해당할 수 있다. 도 14에 도시된 통계정보 생성/관리 모듈은 도 16에 도시된 가시화 데이터 생성 컴포넌트에 해당할 수 있다. 도 14에 도시된 가시화 모듈은 도 16에 도시된 가시화 엔진 컴포넌트에 해당할 수 있다. 도 14에 도시된 통계정보 스토리지는 도 16에 도시된 가시화 데이터 관리 컴포넌트 및/또는 가시화 데이터 생성 컴포넌트로부터 데이터 및/또는 가시화 데이터를 저장하는 스토리지에 해당할 수 있다. 또한, 도 16 및 도 17에 도시된 각각의 공격자 가시화 시스템은 공격자가 내부인지 외부인지에 따른 대상이 다를 수 있고, 도면에 도시된 각 모듈(또는 컴포넌트)의 기능 및 동작은 서로 유사할 수 있다. 따라서, 각 모듈의 명칭은 각 도면에 따라서 그 용어가 가지는 실질적인 의미와 본 명세서의 전반에 걸친 내용을 토대로 해석되어야 한다.

[0114] 도 14에 도시된 공격자 가시화 장치가 가시화하는 방법은 도 18에서 후술한다.

[0115] 도 15는 본 발명의 일 실시예에 따른 전처리 시스템을 도시한다.

[0116] 본 발명의 일 실시예에 따른 공격자 가시화 장치의 전처리 시스템은 보안이벤트 정보를 주기적으로 수집하고 사용자가 입력한 대상기관 정보를 토대로 Source IP가 내부 또는 외부인 보안이벤트를 분류하여 각 가시화 시스템으로 전송하기 위한 시스템이다.

[0117] 도 15에 도시된 바와 같이, 본 발명의 일 실시예에 따른 전처리 시스템은 보안이벤트 수집 컴포넌트, 대상기관 정보 입출력 GUI 컴포넌트, 대상기관 정보 설정 컴포넌트, 내부 공격자 IP 추출 컴포넌트, 외부 공격자 IP 추출 컴포넌트를 포함할 수 있다. 여기서, 컴포넌트는 시스템을 이루는 하나의 구성요소이고, 실시예에 따라서 모듈 등의 명칭으로 명명될 수 있다.

[0118] 본 발명의 일 실시예에 따른 전처리 시스템에 포함된 각 컴포넌트의 기능에 대해서 이하에서 설명한다.

[0119] 보안이벤트 수집 컴포넌트는 침해위협 관리 시스템으로부터 보안이벤트를 수집하는 컴포넌트다. 본 발명의 일 실시예에 따라, 침해위협 관리 시스템은 보안이벤트를 저장하는 스토리지를 포함할 수 있다. 여기서, 보안이벤트 수집 컴포넌트는 보안이벤트를 저장하는 스토리지로부터 보안이벤트를 전달받을 수 있다.

[0120] 대상기관 정보 입출력 GUI 컴포넌트는 관제 대상기관들의 정보를 입력·수정·삭제하기 위한 인터페이스 컴포넌트다.

[0121] 대상기관 정보 설정 컴포넌트는 관제 대상기관들의 정보를 입력·수정·삭제하는 컴포넌트다.

[0122] 내부 공격자 IP 추출 컴포넌트는 통계정보 생성을 위하여 Source IP가 대상기관인 IP와 보안이벤트를 추출하는 컴포넌트다.

[0123] 외부 공격자 IP 추출 컴포넌트는 통계정보 생성을 위하여 Source IP가 非대상기관인 IP와 보안이벤트를 추출하는 컴포넌트다.

[0124] 본 발명의 일 실시예에 따른 전처리 시스템에 포함된 컴포넌트의 구체적인 기능은 이하에서 설명한다.

[0125] 보안이벤트 수집 컴포넌트는 보안이벤트를 요청하고 수집하는 기능을 수행할 수 있다. 본 발명의 일 실시예에 따른 보안이벤트를 수집하는 방법은 다음과 같다. 旣 구축 운영 중인 침해위협 관리 시스템을 통해 보안이벤트를 수집할 수 있다. 본 발명의 일 실시예에 따라, 침해위협 관리 시스템은 보안이벤트를 저장하는 스토리지를 포함할 수 있다. 보안이벤트 수집 방법은 DB조회를 통한 수집방법이 가능할 수 있다. 데이터 수집 시 오류가 발생하는 경우 (예를 들어, query의 오류 또는 기타 이유로 query결과를 받지 못 하는 경우 등) 해당 오류를 GUI 컴포넌트를 가지는 시스템에 전송할 수 있다. 여기서, 오류 통보는 GUI 컴포넌트와 통계분석 컴포넌트 조회·출력 시 화면으로 제공할 수 있다.

[0126] 본 발명의 일 실시예에 따른 보안이벤트 수집항목은 탐지시간, 출발지 IP, 출발지 포트, 도착지 IP, 도착지 포트, 프로토콜, 페이로드, 탐지건수, 기관코드 등을 포함할 수 있다.

[0127] 대상기관정보 입출력 GUI 컴포넌트는 대상기관 정보 설정 기능을 수행할 수 있다. 본 발명의 일 실시예에 따라, 대상기관정보 입출력 GUI 컴포넌트는 대상기관의 IP, 기기타입(예를 들어, 보안장비, 일반서버, PC, 네트워크 장비, 기타 등등)을 입력할 수 있는 GUI화면이 있을 수 있다. 또한, 대상기관정보는 GUI를 통한 직접 입력 및/또는 수정이 가능하고, 대상기관 정보가 포함된 XML, JSON, CSV등의 파일을 통한 입력이 가능할 수 있다.

[0128] 대상기관정보 입출력 GUI 컴포넌트는 대상기관 정보 출력 기능을 수행할 수 있다. 본 발명의 일 실시예에 따라, 시스템에 저장된 대상기관 정보를 일정한 파일 포맷으로 원하는 경로에 출력하는 기능이 되는 GUI 버튼이 필요할 수 있다.

[0129] 대상기관정보 설정 컴포넌트는 대상기관 정보 설정 기능을 수행할 수 있다. 본 발명의 일 실시예에 따라, 파일 또는 GUI를 통해 입력된 대상기관 정보를 시스템에서 이용할 수 있도록 메모리에 저장할 수 있다.

[0130] 대상기관정보 설정 컴포넌트는 대상기관 정보 출력 기능을 수행할 수 있다. 본 발명의 일 실시예에 따라 시스템에 저장된 대상기관 정보를 일정한 파일 포맷으로 출력할 수 있다.

[0131] 내부 공격자 IP 추출 컴포넌트는 IP추출 기능을 수행할 수 있다. 본 발명의 일 실시예에 따라, 보안이벤트 수집 컴포넌트에서 수집한 이벤트의 Source IP와 대상기관정보설정컴포넌트에서 입력된 대상기관 정보를 비교하여 Source IP가 대상기관인 이벤트를 분류하고 분류된 이벤트에서 Source IP를 추출할 수 있다. 여기서, 이벤트 분류 시 Destination IP가 어느 대상기관 IP 또는 외부 IP인지 구분 필요할 수 있다.

[0132] 외부 공격자 IP 추출 컴포넌트는 IP추출 기능을 수행할 수 있다. 본 발명의 일 실시예에 따라, 보안이벤트 수집 컴포넌트에서 수집한 이벤트의 Source IP와 대상기관정보설정컴포넌트에서 입력된 대상기관 정보를 비교하여, Source IP가 非대상기관인 이벤트를 분류하고 분류된 이벤트에서 Source IP를 추출할 수 있다. 여기서, 이벤트 분류 시 Destination IP가 어느 대상기관 IP 또는 외부 IP인지 구분 필요할 수 있다.

[0133] 본 발명의 일 실시예에 따른 전처리 시스템은 내부 공격자 가시화 시스템, 외부 공격자 가시화 시스템, 공격자 상관정보 가시화 시스템과 각각 패키지화되어 동작할 수 있다.

[0134] 상술한 바와 같이, 보안이벤트 수집 컴포넌트는 보안이벤트를 침해위협관리 시스템에 요청하고, 침해위협관리 시스템으로부터 보안이벤트를 수집할 수 있다. 보안이벤트 수집 컴포넌트는 보안이벤트를 내부공격자 IP 추출 컴포넌트 또는 외부 공격자 IP 추출 컴포넌트에 전달할 수 있다.

[0135] 상술한 바와 같이, 대상기관 정보 입출력 GUI 컴포넌트는 대상기관 정보를 입력하고 출력할 수 있다. 또한, 대상기관 정보 입출력 GUI 컴포넌트는 파일을 통한 대상기관 정보를 입력할 수 있다. 게다가, 대상기관 정보 입출력 GUI 컴포넌트는 대상기관 정보를 대상기관 정보 설정 컴포넌트에 전달할 수 있다.

[0136] 상술한 바와 같이, 대상기관 정보 설정 컴포넌트는 대상기관 정보를 설정할 수 있다. 또한, 대상기관 정보 설정 컴포넌트는 대상기관 정보를 내부 공격자 IP 추출 컴포넌트 또는 외부 공격자 IP 추출 컴포넌트에 전달할 수 있다.

[0137] 상술한 바와 같이, 내부 공격자 IP 추출 컴포넌트는 보안이벤트 및/또는 대상기관 정보를 수신하여 내부 보안이벤트를 선별할 수 있다. 또한, 내부 공격자 IP 추출 컴포넌트는 보안이벤트 및/또는 대상기관 정보를 수신하여 대상기관, 즉, 내부 IP를 추출할 수 있다.

[0138] 상술한 바와 같이, 외부 공격자 IP 추출 컴포넌트는 보안이벤트 및/또는 대상기관 정보를 수신하여 외부 보안이벤트를 선별할 수 있다. 또한, 외부 공격자 IP 추출 컴포넌트는 보안이벤트 및/또는 대상기관 정보를 수신하여 대상기관이 아닌, 즉, 외부 IP를 추출할 수 있다.

[0139] 도 16은 본 발명의 일 실시예에 따른 내부 공격자 가시화 시스템을 도시한다.

[0140] 본 발명의 일 실시예에 따른 공격자 가시화 장치의 내부 공격자 가시화 시스템은 도 15에 도시된 전처리 시스템으로부터 수신한 전처리 정보를 활용하여 내부 공격자 IP에 대한 통계정보, 가시화 데이터 등을 추출하고 내부 공격자 IP의 행위를 실시간으로 가시화하기 위한 시스템이다.

[0141] 도 16에 도시된 바와 같이, 본 발명의 일 실시예에 따른 내부 공격자 가시화 시스템은 전처리 정보 수집 컴포넌트, 가시화 데이터 생성 컴포넌트, 가시화 데이터 관리 컴포넌트, 가시화 엔진 컴포넌트, 환경 설정 컴포넌트를 포함할 수 있다. 여기서, 컴포넌트는 시스템을 이루는 하나의 구성요소이고, 실시예에 따라서 모듈 등의 명칭으로 명명될 수 있다.

[0142] 본 발명의 일 실시예에 따른 내부 공격자 가시화 시스템에 포함된 각 컴포넌트의 기능에 대해서 이하에서 설명한다.

[0143] 전처리 정보 수집 컴포넌트는 전처리 시스템을 통하여 전처리가 완료된 보안이벤트 정보 및 내부 공격자 IP를 수집하여 가시화 데이터 생성 컴포넌트에 1분단위로 전송 및 검증하는 기능을 제공할 수 있다.

[0144] 가시화 데이터 생성 컴포넌트는 전처리 정보 수집 컴포넌트로부터 수집한 보안이벤트 정보 및 내부 공격자 IP와 가시화 데이터 관리 컴포넌트의 장기간 및 실시간 가시화 데이터를 활용하여 내부 공격자 IP에 대한 통계정보 및 가시화 데이터를 생성하고 가시화 엔진 컴포넌트에 전송 검증하는 기능을 제공할 수 있다.

[0145] 가시화 데이터 관리 컴포넌트는 가시화 데이터 생성 컴포넌트로부터 수신한 내부 공격자 IP에 대한 통계정보를 장기간 및 실시간으로 저장하는 기능을 제공할 수 있다. 또한, 가시화 데이터 관리 컴포넌트는 가시화 데이터 생성 컴포넌트 및 가시화 엔진 컴포넌트에서 요청하는 내부 공격자 IP에 대한 통계 정보를 제공하는 기능을 제공할 수 있다.

[0146] 가시화 엔진 컴포넌트는 가시화 데이터 생성 컴포넌트로부터 수신한 통계정보 및 가시화 데이터를 활용하여 내부 공격자 IP에 대한 공격 행위를 실시간으로 가사화하는 기능을 제공할 수 있다. 또한, 가시화 엔진 컴포넌트는 사용자의 환경 설정 및 인터랙션에 따라서 가시화 화면을 실시간으로 변경하고 내부 공격자 IP에 대한 상세 정보를 제공할 수 있다.

[0147] 환경 설정 컴포넌트는 가시화 IP 영역 설정, 스코어링 알고리즘 설정, 배경 프레임 설정, 통계정보 우선순위 설정 등 내부 공격자 IP에 대한 공격 행위를 실시간으로 가시화하기 위해 필요한 다양한 설정 기능 및 사용자 인터페이스 기능을 제공할 수 있다.

[0148] 본 발명의 일 실시예에 따른 내부 공격자 가시화 시스템에 포함된 각 컴포넌트의 구체적인 기능에 대해서 이하에서 설명한다.

[0149] 전처리 정보 수집 컴포넌트는 전처리 정보 수집 및 전송 기능을 수행할 수 있다. 전처리 정보 수집 컴포넌트는 전처리 시스템으로부터 모든 내부 공격자 IP에 대한 이벤트 정보를 수신할 수 있다. 또한, 전처리 정보 수집 컴포넌트는 이벤트정보를 1분 단위로 수신할 수 있고, 10만 건 이상의 내부 공격자 IP에 대해 지연 없이 처리할 수 있다. 전처리 정보 수집 컴포넌트는 모든 내부 공격자 IP에 대한 이벤트 정보를 가시화 데이터 생성 컴포넌트 및 가시화 데이터 관리 컴포넌트로 실시간 전송할 수 있다.

[0150] 또한, 본 발명의 일 실시예에 따른 전처리 정보 수집 컴포넌트는 전처리 정보 수집 검증 및 재전송 기능을 수행할 수 있다. 전처리 정보 수집 컴포넌트는 전처리 시스템으로부터 수신한 데이터가 원본 데이터와 상이한지 여부를 실시간으로 검증하고 다를 경우(예를 들어, 패킷 손실 등) 재전송이 가능할 수 있다.

[0151] 가시화 데이터 생성 컴포넌트는 통계정보를 생성할 수 있다. 전처리 정보 수집 컴포넌트로부터 전달 받은 Source IP가 대상기관인 IP(내부 공격자 IP)에서 발생한 보안이벤트를 활용하여 통계를 생성할 수 있다. 본 발명의 일 실시예에 따른 통계 정보는 다음과 같다. IP별 1분간 발생한 보안이벤트의 개수·종류, IP별 1분간 접근한 도착지 IP·Port의 개수, IP별 1분간 발생한 보안이벤트의 Source Port의 개수, IP별 보안이벤트 발생 간격의 평균·표준편차 등을 포함할 수 있다. 여기서, 최초로 통계 생성에 진입하는 IP의 경우 평균과 편차는 0일 수 있다. 통계를 유지해야 하는 IP목록은 가시화 데이터 관리 컴포넌트의 실시간 가시화 데이터 관리 기능을 참조할 수 있다. 발생 간격은 해당 분에서 가장 먼저 발생한 이벤트들 간의 차이를 의미할 수 있다. 프로그램 시작 시간의 -1분부터 통계를 생성할 수 있다.

[0152] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP별 지난 1분(현재-2분 ~ 현재-1분)간 발생한 보

안이벤트별 발생량과 현재(현재-1분~ 현재) 발생한 보안이벤트의 발생량 간의 비교하여 통계를 생성할 수 있다. 또한, IP별 White·Black IP list에 접근한 횟수를 통해 통계를 생성할 수 있다.

[0153] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 신규 가시화 IP 리스트를 추출할 수 있다. 구체적으로, 전처리 정보 수집 컴포넌트에서 수신한 모든 내부 공격자 IP와 가시화 데이터 관리 컴포넌트의 실시간 가시화 데이터를 비교하여 신규 IP 리스트를 추출할 수 있다.

[0154] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 IP에 대한 추가/삭제 대체/유지 기능을 수행할 수 있다. 본 발명의 일 실시예에 따른 추가, 삭제, 대체, 유지 기능을 이하에서 설명한다.

[0155] 추가는 3차원 구(球) 표면에 표시될 IP는 통계치 또는 스코어링 알고리즘에 따라 순차적으로 추가할 수 있고, 최대로 표시할 수 있는 IP 개수를 초과한 경우에는 후술할 '삭제 대체' 방법론을 따를 수 있다.

[0156] 삭제 대체는 3차원 구(球) 표면의 IP에서 1분간 발생한 모든 보안이벤트의 목적지 IP가 사용자가 사전에 등록한 'White IP 리스트'에 포함되면 해당 IP를 삭제하고 신규 IP를 추가할 수 있다. 추가 삭제가 필요할 경우 후술할 'a)' 또는 'b)' 또는 'c)'의 방법에 따라 기존 IP를 삭제하고 해당 부분에 신규 IP를 대체하여 표시할 수 있다. 본 발명의 일 실시예에 따른 'a)' 또는 'b)' 또는 'c)'의 방법을 이하에서 설명한다.

[0157] a) 각 IP에 대한 스코어링(각 IP의 통계정보에 대한 조합으로 점수 산출)을 통해서 가장 낮은 점수부터 삭제할 수 있다.

[0158] b) 표시 시간이 오래된 순서대로 삭제한다.

[0159] c) 통계정보의 각 항목에 대한 우선순위를 설정하고, 우선순위가 낮은 순서대로 삭제한다.

[0160] 유지는 보안이벤트의 목적지 IP가 사용자가 사전에 설정한 IP 리스트(예를 들어, 허니넷, 다크넷 등)에 포함될 경우 사용자가 사전에 설정한 기간(예를 들어, 1일, 1달 등) 동안 삭제하지 않고 유지할 수 있다.

[0161] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP 영역 내부 시간표시 정보 추출 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 시간정보에 대한 간격(예를 들어, 분/시간/일/월 단위), 길이(예를 들어, 시간/일/월 단위), 각도(예를 들어, 1도 단위) 값을 추출할 수 있다.

[0162] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP 영역 내부 통계표시 정보 추출 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 통계정보의 개수, 최대길이(센티미터 단위), 각도 값을 추출할 수 있다.

[0163] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 기본 가시화 정보 생성 기능을 수행할 수 있다. 구체적으로, 가시화 IP 리스트, 통계정보, 시간표시 정보, 통계표시 정보를 기반으로 가시화 엔진 컴포넌트에 제공할 가시화 데이터를 생성(파일, 바이너리, 스트링 등)할 수 있다.

[0164] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 데이터 전송 기능을 수행할 수 있다. 구체적으로, 생성된 가시화 데이터를 가시화 엔진 컴포넌트에 실시간으로 전송할 수 있다.

[0165] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 데이터 전송 검증 및 재전송 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 전송에 대한 성공 여부를 실시간으로 검증할 수 있고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0166] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 관리 기능을 수행할 수 있다. 나아가, 사용자가 설정한 최소기간(3개월) 이상의 기간 동안 발생한 모든 내부 공격자 IP에 대한 기본 정보 및 통계정보를 저장하고 가시화 엔진 컴포넌트와 연계하여 데이터를 제공할 수 있다.

[0167] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 송 수신 기능을 수행할 수 있다. 나아가, 가시화 엔진 컴포넌트에서 장기간 데이터에 대한 데이터를 요청할 경우 이에 대한 응답 데이터를 실시간으로 전송할 수 있다.

[0168] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 나아가, 장기간 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0169] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 실시간 가시화 데이터 관리 기능을 수행할 수 있다. 나아가, 현재 가시화 화면에 표시하고 있는 모든 IP에 대한 기본 정보 및 통계정보를 최소기간(3개월) 이

상 저장하고 가시화 엔진 컴포넌트와 연계하여 데이터를 제공할 수 있다.

[0170] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 실시간 가시화 데이터 송 수신 기능을 수행할 수 있다. 나아가, 가시화 엔진 컴포넌트에서 실시간 데이터에 대한 데이터를 요청할 경우 이에 대한 응답 데이터를 실시간으로 전송할 수 있다.

[0171] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 실시간 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 나아가, 실시간 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0172] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 가시화 데이터 송 수신 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 생성 컴포넌트에서 생성한 가시화 데이터(예를 들어, 상술한 장기 및 실시간 가시화 정보 포함)를 실시간으로 요청하고 수집할 수 있다.

[0173] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0174] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 배경 프레임(예를 들어, 물체) 가시화 기능을 수행할 수 있다. 구체적으로, 내부 공격자 IP를 표시하기 위한 배경 프레임(예를 들어, 물체)을 표시할 수 있다.

[0175] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 내부 공격자 IP 정보 가시화 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면에 표시하는 IP 정보는 총 3개 영역으로 구분하여 표시할 수 있다. 본 발명의 일 실시예에 따른 3개 영역은 IP 자체, 시간, 통계정보 값을 포함할 수 있고, 구체적 내용은 이하에서 설명한다.

[0176] ① IP 자체 : 분화구 모양(예를 들어, 배경은 검정, 내부는 주황색의 용암 꿈틀거리면서 움직이는 모습)을 원형에 가깝게 볼록 및 오목한 형태로 표시하며, 사용자가 설정한 IP 개수(예를 들어, 최소 100개 이상)만큼 3차원 구(球) 표면에 표시할 수 있다.

[0177] ② 시간 : 직선(예를 들어, 세로방향)에 가까운 곡선 모양이며 1분 단위로 구분할 수 있어야 하며, IP자체 모양 안에 사용자가 설정한 통계정보 개수(예를 들어, 최소 4개 이상)만큼 표시할 수 있다.

[0178] ③ 통계정보 값 : 해당 시간에 발생한 통계정보의 크기를 직선(예를 들어, 가로방향)에 가까운 곡선 모양으로 표시할 수 있다. 여기서, 비연속형(카테고리) 통계정보(예를 들어, 공격 유형, 종류 수 등)는 개수만큼 각도와 색깔을 달리하여 가로방향 직선을 표시할 수 있다.

[0179] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 3차원 구(球) 표면에 표시하는 IP의 '시간'과 '통계정보 값'의 방향은 사용자가 최대한 쉽게 구별할 수 있도록 자동재배치(예를 들어, 시간과 통계정보 값이 큰 부분을 뒤로 배치 등) 하는 기능을 수행할 수 있다.

[0180] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 세계지도 상에 보안이벤트 표시 기능을 수행할 수 있다.

[0181] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 3차원 구(球) 표면의 IP에서 발생한 보안이벤트를 세계지도(예를 들어, 도시 단위까지 구분)에 실시간으로 가시화해야 하며 해당 하는 'IP 자체'를 깜빡이도록 표시할 수 있다. 구체적으로, IP에 대한 도시정보를 추출하기 위해 GeoIP 등 오픈소스를 활용해야 하며, 주기적(예를 들어, 일 단위 또는 업데이트 발생 시)으로 업데이트할 수 있다. 또한, 본 발명의 일 실시예에 따라, 3차원 구(球) 표면의 IP와 세계지도를 연결하는 방법은 선, 점, 화살표 등 보안이벤트의 종류에 따라 표시할 수 있다. 여기서, 과학기술사이버안전센터의 K-Cube 가시화 시스템 방법론을 적용할 수 있다.

[0182] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 특정 보안이벤트를 표시하지 않는 기능을 수행할 수 있다. 구체적으로, 특정 목적지 IP로 발생하는 보안이벤트의 신규 송신자 IP 개수가 사용자가 사전에 설정한 개수(예를 들어, 100개)를 초과하는 경우에는 IP자체로 표시하지 않고 '세계지도 상에 보안이벤트 표시 기능' 방식에 따라서 표시할 수 있다. 구체적으로, 보안이벤트의 출발지 또는 목적지 IP가 사전에 사용자가 등록한 IP리스트에 포함될 경우에는 3차원 구(球)에 해당 출발지 IP를 표시하지 않을 수 있다.

[0183] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 3차원 구(球)에 표시된 IP의 지속 시간이 길어질수록 'IP 자체'에 대한 이미지를 변경(예를 들어, 용암이 흘러내림, 크기 증가, 색상 변화 등)할 수 있다.

[0184] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 특정 IP 리스트 및 상세정보를 표시하는 기능을 수행할 수

있다. 구체적으로, 특정 IP 리스트는 사용자 지정, 위험도(예를 들어, 스코어링 점수) 순서, 오래된 시간 순서 등으로 자동표시 되어야 하며, 각 IP에 대한 상세정보는 대상기관명, 시스템 종류, 위험도, 시간 등 사용자가 지정한 정보를 표시할 수 있다.

[0185] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 통계정보에 대한 범례 표시 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 영역에 표시하는 통계정보에 대한 범례를 화면의 상/하/좌/우 중 한 곳에 표시할 수 있다.

[0186] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 IP 영역 클릭 시 상세 정보 표시 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP영역을 클릭 시 해당 IP에 대한 상세정보를 가로축(예를 들어, 시간은 최대 1년까지 표시 가능)과 세로축(예를 들어, 통계정보, 기본정보 등)을 활용하여 현재 시점을 기준으로 과거 모든 정보를 3차원 형태(예를 들어, 막대그래프, 선 그래프 등)로 표시할 수 있다. 구체적으로, 해당 IP에 대한 상세정보 중 시간과 무관한 정보(예를 들어, 시스템 종류 등)는 그래프 상/하/좌/우/ 중 한 곳에 표시할 수 있다. 여기서, IP에 대한 상세정보는 보안이벤트 내 기본정보(예를 들어, IP, 발생 시간, 이벤트명 등) 및 통계정보(예를 들어, 발생횟수, 목적지 포트 개수 등), 시스템 종류(PC, 서버 등) 등 IP와 관련한 모든 정보일 수 있다.

[0187] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 3차원 구(球)가 자동으로 회전하는 기능을 수행할 수 있다. 구체적으로, 3차원 구(球)가 좌우 또는 상하로 자동으로 회전할 수 있다.

[0188] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 3차원 구(球)를 일시정지/재생하는 기능을 수행할 수 있다.

[0189] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 3차원 구(球)가 움직이는/정지된 상태에서 줌인/줌아웃 하는 기능을 수행할 수 있다. 여기서, 가시화 엔진 컴포넌트는 클라이언트 형태(예를 들어, 내부 공격자 가시화 시스템 또는 가시화 데이터 생성 컴포넌트와 서버/클라이언트 형태로 통신)로 개발해야 하며, 내부 공격자 가시화 시스템과 동일시스템에서 구동하는 패키지 및 별도의 전용시스템에 프로그램 형태로 설치 운용할 수 있다.

[0190] 본 발명의 일 실시예에 따른 가시화 엔진컴포넌트는 통계정보 우선순위 설정 기능을 수행할 수 있다. 구체적으로, 통계정보에 대한 우선순위를 설정할 수 있는 설정화면을 제공해야 하며 우선순위 정보에 따라 3차원 구(球) 표면의 IP를 삭제할 수 있다.

[0191] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 데이터 생성, 및/또는 가시화 엔진과 관련하여 각 기능 및/또는 컴포넌트에서 필요한 환경 설정을 할 수 있다. 가시화 데이터 생성과 관련된 환경 설정 컴포넌트의 구체적 기능 및 가시화 엔진과 관련된 환경 설정 컴포넌트의 구체적 기능을 이하에서 설명한다.

[0192] 본 발명의 일 실시예에 따른 가시화 데이터 생성과 관련된 환경 설정 컴포넌트의 구체적 기능은 다음과 같다.

[0193] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 전처리 시스템과 전처리 정보 수집 컴포넌트 간 연계를 위한 설정 기능을 수행할 수 있다. 구체적으로, 전처리 시스템으로부터 모든 내부 공격자 IP 및 보안이벤트 정보를 수신할 수 있도록 IP/PORT 번호, 통신 방법 등을 설정할 수 있다. 여기서, 본 발명의 일 실시예에 따라 패키지 구성 시 필요한 설정도 가능할 수 있다.

[0194] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 장기간 가시화 데이터 관리 기간 및 IP 개수 설정 기능을 수행할 수 있다. 구체적으로, 장기간 가시화 데이터를 관리하기 위한 기간(예를 들어, 일/월 단위) 및 IP 개수를 설정할 수 있다.

[0195] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 통계정보 생성을 위한 기간 설정 기능을 수행할 수 있다. 구체적으로, 각 IP에 대한 통계정보를 생성하기 위한 기간을 시간/일/월/년 단위로 설정할 수 있다.

[0196] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 내부 시간정보 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 시간정보에 대한 간격(예를 들어, 분/시간/일/월 단위), 길이(예를 들어, 시간/일/월 단위), 각도(예를 들어, 1도 단위)를 설정할 수 있다.

[0197] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 사용자 지정 White/Black IP 리스트 설정 기능을 수행할 수 있다. 구체적으로, 사용자가 White/Black IP 리스트를 입력할 수 있어야 하며, 입력 방법은 인터페이스를 통한 직접 입력, 파일 로딩(XML, JSON, CSV 등)을 통한 입력, 외부 URL 연동(API 등)을 통한 입력 기능을 제공할 수 있다.

[0198] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 외부정보 출력 기능을 수행할 수 있다. 구체적으로, 시스템에 입력된 White Black IP, 사고처리 이력을 일정한 파일 포맷으로 출력할 수 있다.

[0199] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 스코어링 알고리즘 설정 기능을 수행할 수 있다. 구체적으로, 통계정보에 대한 조합으로 스코어링 점수를 산출할 수 있는 설정화면을 제공해야 하며 각 통계정보에 대한 가중치를 설정할 수 있다.

[0200] 본 발명의 일 실시예에 따른 가시화 엔진과 관련된 환경 설정 컴포넌트의 구체적 기능은 다음과 같다.

[0201] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 전처리 시스템과 전처리 정보 수집 컴포넌트 간 연계를 위한 설정 기능을 수행할 수 있다. 구체적으로, 전처리 시스템으로부터 모든 내부 공격자 IP 및 보안이벤트 정보를 수신할 수 있도록 IP/PORT 번호, 통신 방법 등을 설정할 수 있다. 여기서, 본 발명의 일 실시예에 따라 패키지 구성 시 필요한 설정도 가능하다.

[0202] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 내부 공격자 가시화 시스템과 가시화 엔진 컴포넌트 간 연계를 위한 설정 기능을 포함할 수 있다. 구체적으로, 내부 공격자 가시화 시스템으로부터 가시화에 필요한 모든 정보(예를 들어, 가시화 데이터 생성 컴포넌트에서 생성한 데이터)를 수신할 수 있도록 IP/PORT 번호, 통신 방법 등을 설정할 수 있다. 여기서, 본 발명의 일 실시예에 따라 패키지 구성 시 필요한 설정도 가능하다.

[0203] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 IP 개수 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면에 표시할 IP 개수를 설정할 수 있다.

[0204] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 및 통계정보 색상 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면에 표시하는 IP 영역에 대한 배경색, 시간 색, 통계정보 색을 설정할 수 있다.

[0205] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역의 시스템 종류 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부 색을 표현하는 시스템 종류(예를 들어, PC, 서버, 네트워크 장비 등)를 설정할 수 있다.

[0206] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 볼록 및 오목 형태 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 영역을 볼록 및 오목으로 표시할 기준을 설정할 수 있다.

[0207] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 내부 통계정보 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 통계정보의 개수, 최대길이(예를 들어, 센티미터 단위), 각도를 설정할 수 있다.

[0208] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 하이라이트 속도 설정 기능을 포함할 수 있다. 구체적으로, 보안이벤트를 3차원 구(球) 표면과 세계지도 상에 표시할 경우, IP 자체가 하이라이트(예를 들어, 깜빡거리는) 하는 속도를 설정할 수 있다.

[0209] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역과 세계지도 연결 방법 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP와 세계지도를 연결하는 방법(예를 들어, 선, 점, 화살표 등)을 설정할 수 있다.

[0210] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 신규 IP 추가 방법 및 위치 설정 기능을 포함할 수 있다. 본 발명의 일 실시예에 따른 신규 IP 추가 방법 및 위치 설정 기능의 구체적 내용은 이하에서 설명한다.

[0211] IP 추가 방법 : IP 신규 발생부터 가시화 완료시점까지 보여지는 과정(날아오기, 깜빡거리기, 나타나기 등)을 설정할 수 있다.

[0212] IP 위치 : 신규로 추가하는 IP 위치를 랜덤 또는 아래→위 또는 위→아래 또는 좌→우 또는 우→좌 등으로 설정할 수 있다.

[0213] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 특정 IP 리스트 및 상세정보 설정 기능을 포함할 수 있다. 구체적으로, 사용자가 화면에 표시할 IP 리스트를 사용자 지정, 위험도 순서, 오래된 시간 순서 등으로 설정할 수 있다. 또한, 사용자 지정 IP 리스트에 대해 인터페이스를 통한 직접 입력, 파일 로딩(예를 들어, XML, JSON, CSV 등)을 통한 입력으로 설정할 수 있다. 나아가, 각 IP에 대해 표시할 상세정보(예를 들어, 대상기관명, 시스템 종류, 위험도, 시간 등)를 사용자가 직접 설정할 수 있다. 추가로, 사용자가 화면에 표시할 IP 리스트의 위치(예를 들어, 상/하/좌/우)를 설정할 수 있다.

[0214] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 통계정보에 대한 범례 설정 기능을 포함할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 영역에 표시하는 통계정보 범례의 위치(상/하/좌/우)를 설정할 수 있다.

[0215] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 클릭 시 상세 정보 표시 설정 기능을 포함할 수 있다. 구체적으로, 각 IP를 클릭했을 시 상세정보를 표시할 경우, 시간축의 단위(예를 들어, 분/시간/일/월)와 최대 길이(예를 들어, 분/시간/일/월 단위), 그래프 형태(예를 들어, 막대 그래프, 선 그래프 등), 시간과 무관한 정보(예를 들어, 시스템 종류 등)를 표시하는 위치(예를 들어, 상하좌우) 등을 설정할 수 있다. 여기서, 상세 표시 방법에 대해서는 본 발명의 일 실시예에 따라서 결정될 수 있다.

[0216] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 배경 모양과 을 설정하는 기능을 포함할 수 있다.

[0217] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 자동회전 유무를 설정하는 기능을 포함할 수 있다. 구체적으로, 3차원 구(球)가 좌우 또는 상하로 자동으로 회전시킬지 여부를 설정할 수 있다. 나아가, 3차원 구(球)의 회전 속도를 설정할 수 있다.

[0218] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 자동회전 유무를 설정하는 기능을 포함할 수 있다.

[0219] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 줌인/줌아웃 활성화 여부를 설정하는 기능을 포함할 수 있다. 여기서, 가시화 엔진 컴포넌트의 모든 기능을 키보드 단축키로 작동할 수 있도록 환경설정 컴포넌트에서 설정할 수 있다. 또한, 환경 설정 컴포넌트는 가시화 엔진 컴포넌트와 함께 별도의 가시화 전용 시스템에서 구동할 수 있다. 그리고, 환경 설정 컴포넌트는 클라이언트 형태(예를 들어, 내부 공격자 가시화 시스템 또는 가시화 데이터 생성 컴포넌트와 서버/클라이언트 형태로 통신)로 개발해야 하며, 내부 공격자 가시화 시스템과 동일시스템에서 구동하는 패키지 및 별도의 전용시스템에 프로그램 형태로 설치 운용할 수 있다. 예를 들어, 가시화 엔진 컴포넌트와 동일한 프로그램에서 구동 가능할 수 있다. 상술한 본 발명의 일 실시예에 따른 시스템의 가시화 구현은 모의 데이터를 통해 실제 표시해야 할 가시화 구현의 예를 후술한다.

[0220] 상술한 바와 같이, 내부 공격자 가시화 시스템(또는 장치)에 포함된 전처리 정보 수집 컴포넌트는 도 15에 도시된 전처리 시스템으로부터 전처리된 정보를 수신할 수 있다. 전처리 정보 수집 컴포넌트는 전처리 정보를 수집, 검증, 전송, 및/또는 재전송할 수 있다. 전처리 정보 수집 컴포넌트는 전처리 정보를 가시화 데이터 생성 컴포넌트에 전송할 수 있다.

[0221] 상술한 바와 같이, 내부 공격자 가시화 시스템(또는 장치)에 포함된 가시화 데이터 생성 컴포넌트는 통계정보 및/또는 가시화 데이터를 생성하고 전송할 수 있다. 가시화 데이터 생성 컴포넌트는 수신한 전처리 정보에 대하여 송/수신 검증 및 재전송을 수행할 수 있다. 가시화 데이터 생성 컴포넌트는 통계정보 및/또는 가시화 데이터를 가시화 엔진 컴포넌트에 요청 및/또는 전송할 수 있고, 가시화 데이터를 저장하는 스토리지에 가시화 데이터를 요청 및/또는 전송할 수 있다. 또한, 가시화 데이터 생성 컴포넌트는 환경 설정 컴포넌트로부터 환경 설정 정보를 요청하여 전달받을 수 있다.

[0222] 상술한 바와 같이, 내부 공격자 가시화 시스템(또는 장치)에 포함된 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 및/또는 실시간 가시화 데이터를 관리 및/또는 송수신 처리를 수행할 수 있다. 가시화 데이터 관리 컴포넌트는 가시화 엔진 컴포넌트로부터 정보를 요청하여 전달받을 수 있다. 또한, 가시화 데이터 관리 컴포넌트는 가시화 데이터를 저장하는 스토리지에 장기간 가시화 데이터 및/또는 실시간 가시화 데이터를 저장하거나, 스토리지로부터 가시화 데이터를 전달받을 수 있다.

[0223] 상술한 바와 같이, 내부 공격자 가시화 시스템(또는 장치)에 포함된 가시화 엔진 컴포넌트는 가시화 데이터를 수신하거나 송신하는 기능을 수행할 수 있다. 가시화 엔진 컴포넌트는 가시화 데이터를 송수신하는 과정에 있어서 이를 검증하고 재전송을 할 수 있다. 가시화 엔진 컴포넌트는 배경 프레임(물체), 내부 공격자 IP 정보, 내부 공격자 IP 실시간 정보를 가시화할 수 있다. 또한, 가시화 엔진 컴포넌트는 내부 공격자 IP 동적 재배치, 특정 내부 공격자 IP에 대한 상세정보 표시, 내부 공격자 IP를 선택하면 상세정보 표시 등을 제공할 수 있다. 가시화 엔진 컴포넌트는 환경 설정 컴포넌트로부터 환경 설정 정보를 요청하고 수신할 수 있다.

[0224] 상술한 바와 같이, 내부 공격자 가시화 시스템(또는 장치)에 포함된 환경 설정 컴포넌트는 상술한 컴포넌트 간의 연계를 설정할 수 있다. 구체적으로, 환경 설정 컴포넌트는 IP 영역 설정, 스코어링 알고리즘 설정, IP 선택 시 상세정보 설정, IP 관리 설정, 통계정보 관리, 특정 IP 상세정보 설정, 배경 프레임(물체) 설정 등을 할 수 있다.

[0225] 도 17은 본 발명의 일 실시예에 따른 외부 공격자 가시화 시스템을 도시한다.

[0226] 도 17에 도시된 본 발명의 일 실시예에 따른 공격자 가시화 장치의 외부 공격자 가시화 시스템은 전처리 시스템으로부터 수신한 전처리 정보를 활용하여 외부 공격자 IP에 대한 통계정보, 가시화 데이터 등을 추출하고 외부 공격자 IP의 행위를 실시간으로 가시화하기 위한 시스템이다.

[0227] 도 17에 도시된 바와 같이, 본 발명의 일 실시예에 따른 외부 공격자 가시화 시스템은 전처리 정보 수집 컴포넌트, 가시화 데이터 생성 컴포넌트, 가시화 데이터 관리 컴포넌트, 가시화 엔진 컴포넌트, 환경 설정 컴포넌트를 포함할 수 있다. 여기서, 컴포넌트는 시스템을 이루는 하나의 구성요소이고, 실시예에 따라서 모듈 등의 명칭으로 명명될 수 있다.

[0228] 본 발명의 일 실시예에 따른 외부 공격자 가시화 시스템에 포함된 각 컴포넌트의 기능을 이하에서 설명한다.

[0229] 전처리 정보 수집 컴포넌트는 전처리 시스템을 통하여 전처리가 완료된 보안이벤트 정보 및 외부 공격자 IP를 수집하여 가시화 데이터 생성 컴포넌트에 1분단위로 전송 및 검증하는 기능을 제공할 수 있다.

[0230] 가시화 데이터 생성 컴포넌트는 전처리 정보 수집 컴포넌트로부터 수집한 보안이벤트 정보 및 외부 공격자 IP와 가시화 데이터 관리 컴포넌트의 장기간 및 실시간 가시화 데이터를 활용하여 외부 공격자 IP에 대한 통계정보 및 가시화 데이터를 생성하고 가시화 엔진 컴포넌트에 전송 검증하는 기능을 제공할 수 있다.

[0231] 가시화 데이터 관리 컴포넌트는 가시화 데이터 생성 컴포넌트로부터 수신한 외부 공격자 IP에 대한 통계정보를 장기간 및 실시간으로 저장하는 기능을 제공할 수 있다. 나아가, 가시화 데이터 생성 컴포넌트 및 가시화 엔진 컴포넌트에서 요청하는 외부 공격자 IP에 대한 통계 정보를 제공하는 기능을 제공할 수 있다.

[0232] 가시화 엔진 컴포넌트 가시화 데이터 생성 컴포넌트로부터 수신한 통계정보 및 가시화 데이터를 활용하여 외부 공격자 IP에 대한 공격 행위를 실시간으로 가사화하는 기능을 제공할 수 있다. 나아가, 사용자의 환경 설정 및 인터랙션에 따라서 가시화 화면을 실시간으로 변경하고 외부 공격자 IP에 대한 상세정보를 제공할 수 있다.

[0233] 환경 설정 컴포넌트 가시화 IP 영역 설정, 스코어링 알고리즘 설정, 배경 프레임 설정, 통계정보 우선순위 설정 등 외부 공격자 IP에 대한 공격 행위를 실시간으로 가시화하기 위해 필요한 다양한 설정 기능 및 사용자 인터페이스 기능을 제공할 수 있다.

[0234] 본 발명의 일 실시예에 따른 외부 공격자 가시화 시스템에 포함된 각 컴포넌트의 구체적인 기능을 이하에서 설명한다

[0235] 본 발명의 일 실시예에 따른 전처리 정보 수집 컴포넌트는 전처리 정보 수집 및 전송 기능을 포함할 수 있다. 구체적으로, 전처리 시스템으로부터 모든 외부 공격자 IP에 대한 이벤트 정보를 수신할 수 있다. 나아가, 이벤트정보는 1분 단위로 수신해야 하며, 10만 건 이상의 외부 공격자 IP에 대해 지연 없이 처리할 수 있다. 또한, 모든 외부 공격자 IP에 대한 이벤트 정보를 가시화 데이터 생성 컴포넌트 및 가시화 데이터 관리 컴포넌트로 실시간 전송할 수 있다.

[0236] 본 발명의 일 실시예에 따른 전처리 정보 수집 컴포넌트는 전처리 정보 수집 검증 및 재전송 기능을 포함할 수 있다. 구체적으로, 전처리 시스템으로부터 수신한 데이터가 원본 데이터와 상이한지 여부를 실시간으로 검증하고 다를 경우(예를 들어, 패킷 손실 등) 재전송이 가능할 수 있다.

[0237] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 통계정보 생성 기능을 포함할 수 있다. 구체적으로, 전처리 정보 수집 컴포넌트로부터 전달 받은 source IP가 非대상기관인 IP(예를 들어, 외부 공격자 IP)에서 발생한 보안이벤트를 활용하여 통계를 생성할 수 있다. 여기서, 본 발명의 일 실시예에 따른 통계 정보는 다음의 정보를 포함할 수 있다. IP별 1분간 발생한 보안이벤트의 개수·종류, IP별 1분간 접근한 도착지 IP·Port의 개수, IP별 1분간 발생한 보안이벤트의 Source Port의 개수, 및/또는 IP별 보안이벤트 발생 간격의 평균·표준편차가 통계 정보에 포함될 수 있다. 여기서, 최초로 통계 생성에 진입하는 IP의 경우 평균과 편차는 0이다. 또한, 통계를 유지해야 하는 IP목록은 가시화 데이터 관리 컴포넌트의 실시간 가시화 데이터 관리 기능을 참조할 수 있다. 그리고, 발생 간격은 해당 분에서 가장 먼저 발생한 이벤트들 간의 차이를 의미할 수 있다. 추가로, 프로그램 시작 시간의 -1분부터 통계 생성할 수 있다.

[0238] 본 발명의 일 실시예에 따른 통계 정보로써, 상술한 정보 외에 다음의 정보를 더 포함할 수 있다. IP별 지난 1분(예를 들어, 현재-2분 ~ 현재-1분)간 발생한 보안이벤트별 발생량과 현재(예를 들어, 현재-1분~ 현재) 발생한 보안이벤트의 발생량 간의 비교, 및/또는 IP별 White·Black IP list에 접근한 횟수를 통계 정보로써 더 포함할 수 있다.

[0239] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 신규 가시화 IP 리스트 추출 기능을 수행할 수 있다. 구체적으로, 전처리 정보 수집 컴포넌트에서 수신한 모든 외부 공격자 IP와 가시화 데이터 관리 컴포넌트의 실시간 가시화 데이터를 비교하여 신규 IP 리스트를 추출할 수 있다.

[0240] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 IP에 대한 추가/삭제 대체/유지 기능을 수행할 수 있다. 본 발명의 일 실시예에 따른 각 기능은 이하에서 설명한다.

[0241] 추가 : 3차원 구(球) 표면에 표시될 IP는 통계치 또는 스코어링 알고리즘에 따라 순차적으로 추가해야 하며, 최대로 표시할 수 있는 IP 개수를 초과한 경우에는 '삭제 대체' 방법론을 따를 수 있다.

[0242] 삭제 대체 : 3차원 구(球) 표면의 IP에서 1분간 발생한 모든 보안이벤트의 목적지 IP가 사용자가 사전에 등록한 'White IP 리스트'에 포함되면 해당 IP를 삭제하고 신규 IP를 추가할 수 있다. 추가 삭제가 필요할 경우 후술할 'a)' 또는 'b)' 또는 'c)'의 방법에 따라 기존 IP를 삭제하고 해당 부분에 신규 IP를 대체하여 표시할 수 있다. 본 발명의 일 실시예에 따른 각 방법은 이하에서 설명한다.

[0243] a) 각 IP에 대한 스코어링(각 IP의 통계정보에 대한 조합으로 점수 산출)을 통해서 가장 낮은 점수부터 삭제할 수 있다.

[0244] b) 표시 시간이 오래된 순서대로 삭제할 수 있다.

[0245] c) 통계정보의 각 항목에 대한 우선순위를 설정하고, 우선순위가 낮은 순서대로 삭제할 수 있다.

[0246] 유지 : 보안이벤트의 목적지 IP가 사용자가 사전에 설정한 IP 리스트(허니넷, 다크넷 등)에 포함될 경우 사용자가 사전에 설정한 기간(1일, 1달 등) 동안 삭제하지 않고 유지할 수 있다.

[0247] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP 영역 내부 시간표시 정보 추출 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 시간정보에 대한 간격(예를 들어, 분/시간/일/월 단위), 길이(예를 들어, 시간/일/월 단위), 각도(예를 들어, 1도 단위) 값을 추출할 수 있다.

[0248] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP 영역 내부 통계표시 정보 추출 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 통계정보의 개수, 최대길이(예를 들어, 센티미터 단위), 각도 값을 추출할 수 있다.

[0249] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 기본 가시화 정보 생성 기능을 수행할 수 있다. 구체적으로, 가시화 IP 리스트, 통계정보, 시간표시 정보, 통계표시 정보를 기반으로 가시화 엔진 컴포넌트에 제공할 가시화 데이터를 생성(예를 들어, 파일, 바이너리, 스트링 등)할 수 있다.

[0250] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 데이터 전송 기능을 수행할 수 있다. 구체적으로, 생성된 가시화 데이터를 가시화 엔진 컴포넌트에 실시간으로 전송할 수 있다.

[0251] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 데이터 전송 검증 및 재전송 기능을 수행할 수 있다. 구체적으로, 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 가시화 데이터 전송에 대한 성공 여부를 실시간으로 검증할 수 있어야 하고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0252] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 관리 기능을 수행할 수 있다. 구체적으로, 사용자가 설정한 최소기간(예를 들어, 3개월) 이상의 기간 동안 발생한 모든 외부 공격자 IP에 대한 기본 정보 및 통계정보를 저장하고 가시화 엔진 컴포넌트와 연계하여 데이터를 제공할 수 있다.

[0253] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 송 수신 기능을 수행할 수 있다. 구체적으로, 가시화 엔진 컴포넌트에서 장기간 데이터에 대한 데이터를 요청할 경우 이에 대한 응답 데이터를 실시간으로 전송할 수 있다.

[0254] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 장기간 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 구체적으로, 장기간 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있어야 하고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0255] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 실시간 가시화 데이터 관리 기능을 수행할 수 있다. 구체적으로, 현재 가시화 화면에 표시하고 있는 모든 IP에 대한 기본 정보 및 통계정보를 최소기간(예를 들어, 3개월) 이상 저장하고 가시화 엔진 컴포넌트와 연계하여 데이터를 제공할 수 있다.

[0256] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 실시간 가시화 데이터 송 수신 기능을 수행할 수 있다. 구체적으로, 가시화 엔진 컴포넌트에서 실시간 데이터에 대한 데이터를 요청할 경우 이에 대한 응답 데이터를 실시간으로 전송할 수 있다.

[0257] 본 발명의 일 실시예에 따른 가시화 데이터 관리 컴포넌트는 실시간 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 실시간 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있어야 하고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0258] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 데이터 송 수신 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 생성 컴포넌트에서 생성한 가시화 데이터(예를 들어, 장기 및 실시간 가시화 정보 포함)를 실시간으로 요청하고 수집할 수 있다.

[0259] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있어야 하고 데이터 전송 실패 시 재전송이 가능할 수 있다.

[0260] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 배경 프레임(예를 들어, 물체) 가시화 기능을 수행할 수 있다. 구체적으로, 외부 공격자 IP를 표시하기 위한 배경 프레임(물체)을 표시할 수 있다.

[0261] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 외부 공격자 IP 정보 가시화 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면에 표시하는 IP 정보는 총 3개 영역으로 구분하여 표시할 수 있다. 본 발명의 일 실시예에 따른 3개의 영역은 이하에서 설명한다.

[0262] ① IP 자체 : 분화구 모양(예를 들어, 배경은 검정, 내부는 주황색의 용암 꿈틀거리면서 움직이는 모습)을 원형에 가깝게 볼록 및 오목한 형태로 표시하며, 사용자가 설정한 IP 개수(예를 들어, 최소 100개 이상)만큼 3차원 구(球) 표면에 표시할 수 있다.

[0263] ② 시간 : 직선(예를 들어, 세로방향)에 가까운 곡선 모양이며 1분 단위로 구분할 수 있어야 하며, IP자체 모양 안에 사용자가 설정한 통계정보 개수(예를 들어, 최소 4개 이상)만큼 표시할 수 있다.

[0264] ③ 통계정보 값 : 해당 시간에 발생한 통계정보의 크기를 직선(예를 들어, 가로방향)에 가까운 곡선 모양으로 표시할 수 있다. 여기서, 비연속형(카테고리) 통계정보(예를 들어, 공격 유형, 종류 수 등)는 개수만큼 각도와 색깔을 달리하여 가로방향 직선을 표시할 수 있다.

[0265] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 외부 공격자 IP 정보 가시화 기능을 수행하는데 있어서, 3차원 구(球) 표면에 표시하는 IP의 '시간'과 '통계정보 값'의 방향은 사용자가 최대한 쉽게 구별할 수 있도록 자동재배치(예를 들어, 시간과 통계정보 값이 큰 부분을 뒤로 배치 등) 하는 기능을 포함할 수 있다.

[0266] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 대상기관에 대한 보안이벤트 표시 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP에서 발생한 보안이벤트를 대상기관 지도(예를 들어, 사용자가 사전에 설정한 대상기관명 및 개수에 따라서 자동으로 표시)에 실시간으로 가시화해야 하며 해당 하는 'IP 자체'를 깜빡이도록 표시할 수 있다. 또한, 3차원 구(球) 표면의 IP와 대상기관 지도를 연결하는 방법은 선, 점, 화살표 등 보안이벤트의 종류에 따라 표시할 수 있다. 여기서, 과학기술사이버안전센터의 K-Cube 가시화 시스템 방법론을 적용할 수 있다.

[0267] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 특정 보안이벤트를 표시하지 않는 기능을 수행할 수 있다. 구체적으로, 특정 목적지 IP로 발생하는 보안이벤트의 신규 송신자 IP 개수가 사용자가 사전에 설정한 개수(예를 들어, 100개)를 초과하는 경우에는 IP자체로 표시하지 않고 ‘세계지도 상에 보안이벤트 표시 기능’ 방식에 따라서 표시할 수 있다. 나아가, 보안이벤트의 출발지 또는 목적지 IP가 사전에 사용자가 등록한 IP리스트에 포함될 경우에는 3차원 구(球)에 해당 출발지 IP를 표시하지 않을 수 있다.

[0268] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 3차원 구(球)에 표시된 IP의 지속 시간이 길어질수록 'IP 자체'에 대한 이미지를 변경(예를 들어, 용암이 흘러내림, 크기 증가, 색상 변화 등)할 수 있다.

[0269] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 특정 IP 리스트 및 상세정보를 표시하는 기능을 수행할 수 있다. 구체적으로, 특정 IP 리스트는 사용자 지정, 위험도(예를 들어, 스코어링 점수) 순서, 오래된 시간 순서 등으로 자동표시 되어야 하며, 각 IP에 대한 상세정보는 대상기관명, 시스템 종류, 위험도, 시간 등 사용자가 지정한 정보를 표시할 수 있다.

[0270] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 통계정보에 대한 범례 표시 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 영역에 표시하는 통계정보에 대한 범례를 화면의 상/하/좌/우 중 한 곳에 표시할 수 있다.

[0271] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 IP 영역 클릭 시 상세 정보 표시 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP영역을 클릭 시 해당 IP에 대한 상세정보를 가로축(예를 들어, 시간 : 최대 1년까지 표시 가능)과 세로축(예를 들어, 통계정보, 기본정보 등)을 활용하여 현재 시점을 기준으로 과거 모든 정보를 3차원 형태(예를 들어, 막대그래프, 선 그래프 등)로 표시할 수 있다. 나아가, 해당 IP에 대한 상세정보 중 시간과 무관한 정보(예를 들어, 시스템 종류 등)는 그래프 상/하/좌/우/ 중 한 곳에 표시할 수 있다. 또한, IP에 대한 상세정보는 보안이벤트 내 기본정보(예를 들어, IP, 발생 시간, 이벤트명 등) 및 통계정보(예를 들어, 발생횟수, 목적지 포트 개수 등), 시스템 종류(예를 들어, PC, 서버 등) 등 IP와 관련한 모든 정보일 수 있다.

[0272] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 3차원 구(球)가 자동으로 회전하는 기능을 수행할 수 있다. 구체적으로, 3차원 구(球)가 좌우 또는 상하로 자동으로 회전할 수 있다.

[0273] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 3차원 구(球)를 일시정지/재생하는 기능을 수행할 수 있다.

[0274] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 3차원 구(球)가 움직이는/정지된 상태에서 줌인/줌아웃 하는 기능을 수행할 수 있다. 여기서, 가시화 엔진 컴포넌트는 클라이언트 형태(예를 들어, 외부 공격자 가시화 시스템 또는 가시화 데이터 생성 컴포넌트와 서버/클라이언트 형태로 통신)로 개발해야 하며, 외부 공격자 가시화 시스템과 동일시스템에서 구동하는 패키지 및 별도의 전용시스템에 프로그램 형태로 설치 운용할 수 있다.

[0275] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 통계정보 우선순위 설정 기능을 수행할 수 있다. 구체적으로, 통계정보에 대한 우선순위를 설정할 수 있는 설정화면을 제공해야 하며 우선순위 정보에 따라 3차원 구(球) 표면의 IP를 삭제할 수 있다.

[0276] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 데이터 생성 및/또는 가시화 엔진에 대하여 환경을 설정할 수 있다. 본 발명의 일 실시예에 따른 각 환경 설정 컴포넌트의 기능을 이하에서 설명한다.

[0277] 본 발명의 일 실시예에 따른 가시화 데이터 생성에 대한 환경 설정 컴포넌트의 구체적 내용을 이하에서 설명한다.

[0278] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 전처리 시스템과 전처리 정보 수집 컴포넌트 간 연계를 위한 설정 기능을 수행할 수 있다. 구체적으로, 전처리 시스템으로부터 모든 외부 공격자 IP 및 보안이벤트 정보를 수신할 수 있도록 IP/PORT 번호, 통신 방법 등을 설정할 수 있다. 여기서, 본 발명의 일 실시예에 따라 패키지 구성 시 필요한 설정도 가능할 수 있다.

[0279] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 장기간 가시화 데이터 관리 기간 및 IP 개수 설정 기능을 수행할 수 있다. 구체적으로, 장기간 가시화 데이터를 관리하기 위한 기간(일/월 단위) 및 IP 개수를 설정할 수 있다.

[0280] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 통계정보 생성을 위한 기간 설정 기능을 수행할 수 있다. 구체적으로, 각 IP에 대한 통계정보를 생성하기 위한 기간을 시간/일/월/년 단위로 설정할 수 있다.

[0281] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 내부 시간정보 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 시간정보에 대한 간격(예를 들어, 분/시간/일/월 단위), 길이(예를 들어, 시간/일/월 단위), 각도(예를 들어, 1도 단위)를 설정할 수 있다.

[0282] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 사용자 지정 White/Black IP 리스트 설정 기능을 수행할 수 있다. 구체적으로, 사용자가 White/Black IP 리스트를 입력할 수 있어야 하며, 입력 방법은 인터페이스를 통한 직접 입력, 파일 로딩(예를 들어, XML, JSON, CSV 등)을 통한 입력, 외부 URL 연동(예를 들어, API 등)을 통한 입력 기능을 제공할 수 있다.

[0283] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 외부정보 출력 기능을 수행할 수 있다. 구체적으로, 시스템에 입력된 White Black IP, 사고처리 이력을 일정한 파일 포맷으로 출력할 수 있다.

[0284] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 스코어링 알고리즘 설정 기능을 수행할 수 있다.

구체적으로, 통계정보에 대한 조합으로 스코어링 점수를 산출할 수 있는 설정화면을 제공해야 하며 각 통계정보에 대한 가중치를 설정할 수 있다.

[0285] 본 발명의 일 실시예에 따른 가시화 엔진에 대한 환경 설정 컴포넌트의 구체적 내용을 이하에서 설명한다.

[0286] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 전처리 시스템과 전처리 정보 수집 컴포넌트 간 연계를 위한 설정 기능을 수행할 수 있다. 구체적으로, 전처리 시스템으로부터 모든 외부 공격자 IP 및 보안이벤트 정보를 수신할 수 있도록 IP/PORT 번호, 통신 방법 등을 설정할 수 있다. 여기서, 본 발명의 일 실시예에 따라 패키지 구성 시 필요한 설정도 가능하다.

[0287] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 외부 공격자 가시화 시스템과 가시화 엔진 컴포넌트 간 연계를 위한 설정 기능을 수행할 수 있다. 구체적으로, 외부 공격자 가시화 시스템으로부터 가시화에 필요한 모든 정보(예를 들어, 가시화 데이터 생성 컴포넌트에서 생성한 데이터)를 수신할 수 있도록 IP/PORT 번호, 통신 방법 등을 설정할 수 있다. 여기서, 본 발명의 일 실시예에 따라 패키지 구성 시 필요한 설정도 가능하다.

[0288] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 IP 개수 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면에 표시할 IP 개수를 설정할 수 있다.

[0289] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 및 통계정보 색상 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면에 표시하는 IP 영역에 대한 배경색, 시간 색, 통계정보 색을 설정할 수 있다.

[0290] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역의 시스템 종류 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부 색을 표현하는 시스템 종류(PC, 서버, 네트워크 장비 등)를 설정할 수 있다.

[0291] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 볼록 및 오목 형태 설정 기능을 수행할 수 있다.

[0292] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 내부 통계정보 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP 내부에 표시할 통계정보의 개수, 최대길이(예를 들어, 센티미터 단위), 각도를 설정할 수 있다.

[0293] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 대상기관 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP와 대상기관 지도를 연결하는 대상기관 정보(예를 들어, 이름, 개수 등)을 설정할 수 있는 기능을 수행한다.

[0294] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 하이라이트 속도 설정 기능을 수행할 수 있다. 구체적으로, 보안이벤트를 3차원 구(球) 표면과 대상기관 지도 상에 표시할 경우, IP 자체가 하이라이트(예를 들어, 깜빡거리는) 하는 속도를 설정할 수 있다.

[0295] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역과 대상기관 지도 연결 방법 설정 기능을 수행할 수 있다. 구체적으로, 3차원 구(球) 표면의 IP와 대상기관 지도를 연결하는 방법(예를 들어, 선, 점, 화살표 등)을 설정할 수 있다.

[0296] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 신규 IP 추가 방법 및 위치 설정 기능을 수행할 수 있다. 본 발명의 일 실시예에 따른 신규 IP 추가 방법 및 위치 설정 기능은 이하에서 설명한다.

[0297] IP 추가 방법 : IP 신규 발생부터 가시화 완료시점까지 보여지는 과정(날아오기, 깜빡거리기, 나타나기 등)을 설정할 수 있다.

[0298] IP 위치 : 신규로 추가하는 IP 위치를 랜덤 또는 아래→위 또는 위→아래 또는 좌→우 또는 우→좌 등으로 설정할 수 있다.

[0299] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 특정 IP 리스트 및 상세정보 설정 기능을 수행할 수 있다. 구체적으로, 사용자가 화면에 표시할 IP 리스트를 사용자 지정, 위험도 순서, 오래된 시간 순서 등으로 설정할 수 있다. 나아가, 사용자 지정 IP 리스트에 대해 인터페이스를 통한 직접 입력, 파일 로딩(예를 들어, XML, JSON, CSV 등)을 통한 입력으로 설정할 수 있다. 또한, 각 IP에 대해 표시할 상세정보(예를 들어, 대상기관명, 시스템 종류, 위험도, 시간 등)를 사용자가 직접 설정할 수 있다. 그리고, 사용자가 화면에 표시할 IP 리스트의 위치(예를 들어, 상/하/좌/우)를 설정할 수 있다.

[0300] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 통계정보에 대한 범례 설정 기능을 수행할 수 있다. 구체적

으로, 3차원 구(球) 표면의 IP 영역에 표시하는 통계정보 범례의 위치(예를 들어, 상/하/좌/우)를 설정할 수 있다.

[0301] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 영역 클릭 시 상세 정보 표시 설정 기능을 수행할 수 있다. 구체적으로, 각 IP를 클릭했을 시 상세정보를 표시할 경우, 시간축의 단위(예를 들어, 분/시간/일/월)와 최대 길이(예를 들어, 분/시간/일/월 단위), 그래프 형태(예를 들어, 막대 그래프, 선 그래프 등), 시간과 무관한 정보(예를 들어, 시스템 종류 등)를 표시하는 위치(예를 들어, 상하좌우) 등을 설정할 수 있다. 여기서, 상세 표시 방법에 대해서는 본 발명의 일 실시예에 따라서 결정될 수 있다.

[0302] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 배경 모양과 을 설정하는 기능을 수행할 수 있다.

[0303] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 자동회전 유무를 설정하는 기능을 수행할 수 있다. 구체적으로, 3차원 구(球)가 좌우 또는 상하로 자동으로 회전시킬지 여부를 설정할 수 있다. 나아가, 3차원 구(球)의 회전 속도를 설정할 수 있다.

[0304] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 자동회전 유무를 설정하는 기능을 수행할 수 있다.

[0305] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 3차원 구(球)의 줌인/줌아웃 활성화 여부를 설정하는 기능을 수행할 수 있다. 여기서, 가시화 엔진 컴포넌트의 모든 기능을 키보드 단축키로 작동할 수 있도록 환경설정 컴포넌트에서 설정할 수 있다. 또한, 환경 설정 컴포넌트는 가시화 엔진 컴포넌트와 함께 별도의 가시화 전용 시스템에서 구동할 수 있다. 그리고, 환경 설정 컴포넌트는 클라이언트 형태(예를 들어, 외부 공격자 가시화 시스템 또는 가시화 데이터 생성 컴포넌트와 서버/클라이언트 형태로 통신)로 개발해야 하며, 외부 공격자 가시화 시스템과 동일시스템에서 구동하는 패키지 및 별도의 전용시스템에 프로그램 형태로 설치 운용할 수 있다. 예들 들어, 가시화 엔진 컴포넌트와 동일한 프로그램에서 구동 가능하다. 상술한 본 발명의 일 실시예에 따른 시스템의 가시화 구현은 모의 데이터를 통해 실제 표시해야 할 가시화 구현의 예를 후술한다.

[0306] 상술한 바와 같이, 외부 공격자 가시화 시스템(또는 장치)는 내부 공격자 가시화 시스템(또는 장치)와 컴포넌트 및 컴포넌트의 기능이 유사하되, 가시화 데이터의 종류가 상이하다. 즉, 내부 공격자 가시화 시스템은 내부 공격자 IP 가시화 데이터를 처리한다면, 외부 공격자 가시화 시스템은 외부 공격자 IP 가시화 데이터를 처리한다. 또한, 내부 공격자 가시화 시스템이 세계지도 상에 보안이벤트를 표시한다면, 외부 공격자 가시화 시스템은 대상기관 지도 상에 보안이벤트를 표시할 수 있다.

[0307] 도 18은 본 발명의 일 실시예에 따른 가시화 방법을 도시한다.

[0308] 본 발명의 일 실시예에 따른 공격자 가시화 장치는 도 14에 도시된 보안이벤트 저장 스토리지, 및 가시화 시스템에 포함된 전처리 컴포넌트, 통계정보 생성/관리 컴포넌트, 가시화 컴포넌트, 및 통계 정보 스토리지에 따라서 도 18에 도시된 바와 같이 가시화할 수 있다.

[0309] 본 발명의 일 실시예에 따른 공격자 가시화 장치는 도 16 내지 17에 도시된 가시화 엔진 컴포넌트에서 도 18에 도시된 바와 같이 가시화를 할 수 있다.

[0310] 본 발명의 일 실시예에 따른 공격자 가시화 장치의 가시화 방법은 다음과 같다.

[0311] 1. 본 발명의 일 실시예에 따른 공격자 가시화 장치의 전처리 컴포넌트는 사용자가 지정한 시간(예를 들어, 1분) 단위로 보안이벤트 저장 스토리지에서 보안이벤트를 수집 저장할 수 있다.

[0312] 2. 본 발명의 일 실시예에 따른 공격자 가시화 장치의 전처리 컴포넌트는 ‘1’에 따라 수집한 전체 보안이벤트에 대해서 아래와 같은 항목들을 추출하고 이를 통계정보 생성/관리 컴포넌트로 전송할 수 있다. 본 발명의 일 실시예에 따른 항목들은 다음 정보를 포함할 수 있다.

[0313] 가. 출발지 IP 주소 및 포트번호

[0314] 나. 도착지 IP 주소 및 포트번호

[0315] 다. 보안이벤트 발생 시간

[0316] 라. 보안이벤트 명

[0317] 마. 보안이벤트 공격 유형

[0318] 3. 통계정보 생성/관리 컴포넌트는 '2' 에 따라 추출한 출발지 IP주소에 대해 아래와 같은 2개 영역으로 분류할 수 있다. 본 발명의 일 실시예에 따른 2개의 영역은 다음과 같다.

[0319] 가. 내부 공격자 IP 주소 : 보안관제 대상기관 내부 시스템

[0320] 나. 외부 공격자 IP 주소 : 내부 공격자 IP 주소에 포함되지 않는 모든 IP 주소

[0321] 4. 통계정보 생성/관리 컴포넌트는 '3' 에 따라 추출한 내부 및 외부 공격자 IP 주소에 대하여 '2' 에서 추출한 항목을 기반으로 사용자가 정의한 다양한 통계정보(예를 들어, 내부 공격자 IP 주소에서 발생한 보안이벤트 건수)를 추출하고 이를 통계정보 저장 스토리지에 전송 저장할 수 있다.

[0322] 5. 가시화 컴포넌트는 아래와 같은 절차에 따라 내부 및 외부 공격자 IP 주소에 대해 가시화할 수 있다.

[0323] 가. 화면상에 각 IP 주소에 대한 공격행위를 가시화하기 위한 배경 영역(예를 들어, 3차원 구, 평면 등)을 표시할 수 있다. 도 18에 도시된 바와 같이, 배경영역이 표시될 수 있다.

[0324] 나. '가' 에서 표시한 배경 영역에 각 IP 주소에 대한 영역(예를 들어, 원, 삼각형 등)을 표시할 수 있다. 도 18에 도시된 바와 같이, 각 IP 영역이 표시될 수 있다.

[0325] 다. '나' 에서 표시한 IP 주소 영역 내에 '4' 에서 추출한 통계정보를 시간 순서에 따라서 표시하며 통계정보의 개수는 사용자가 사전에 정의할 수 있다. 도 18에 도시된 바와 같이, 통계정보가 포함될 수 있다. 여기서, 본 발명의 일 실시예에 따른 통계정보는 상술한 바와 같다.

[0326] 라. '다' 에서 통계 정보 및 시간 순서는 선분 또는 곡선의 길이로 표시하며, 통계 정보의 종류는 서로 다른 색깔로 표시할 수 있다. 도 18에 도시된 바와 같이, 각 통계정보가 시간 간격 및 시간 정보에 따라서 표시될 수 있다.

[0327] 상술한 바와 같이, 본 발명의 일 실시예에 따른 가시화 방법은 공격자가 내부 공격자 또는 외부 공격자인 경우 가시화하는 방법을 나타낸다.

[0328] 본 발명의 일 실시예에 따라 공격자가 내부 공격자인 경우, 도 18에 도시된 바와 같이, 내부 공격자에 대한 통계정보를 가시화할 수 있다. 배경영역은 상술한 3차원 구의 일부 표면일 수 있다. 여기서, 3차원 구는 본 발명의 일 실시예로써, 3차원 구 또는 평면 등을 포함할 수 있다. 배경영역 상에 적어도 하나 이상의 IP 영역이 있고, 내부 공격자 IP 주소에 해당하는 통계정보가 도 18과 같이 가시화될 수 있다. 여기서, 배경영역은 원의 형태를 가지고 있지만, 본 발명의 일 실시예에 따라 원 또는 삼각형 등 평면도형의 모형을 포함할 수 있다. 통계정보는 시간 정보에 기초하여 가시화될 수 있다.

[0329] 본 발명의 일 실시예에 따라 공격자가 외부 공격자인 경우, 외부 공격자 IP 주소에 해당하는 통계정보가 도 18과 같이 가시화될 수 있다. 외부 공격자에 해당하는 IP 영역 상에서 외부 공격자에 대한 통계정보를 시간 간격 순으로 가시화할 수 있다.

[0330] 상술한 바와 같이, 내부 또는 외부 공격자에 대한 통계정보를 가시화함으로써, 통계정보의 종류 및 통계정보에 대한 시간 정보, 통계정보의 기초가 된 IP 정보를 실시간 또는 장기간으로 가시화하는 것이 가능하고, 대용량 보안정보를 효율적으로 파악할 수 있는 효과를 본 발명이 제공할 수 있다.

[0331] 또한, 도 18에 도시된 본 발명의 일 실시예에 따른 가시화 방법 또는 장치는 내부 또는 외부 공격자에 대한 보안 이벤트를 통해서 통계정보를 추출하고 이를 가시화할 수 있다. 내부 공격자에 대한 통계정보가 도 18과 같이 가시화된 경우, 상술한 바와 같이, 내부 공격자 IP의 목적지에 해당하는 영역을 세계지도 상에 연결 또는 표시할 수 있다. 외부 공격자에 대한 통계정보가 도 18과 같이 가시화된 경우, 외부 공격자 IP의 목적지에 해당하는 영역을 대상기관 지도 상에 연결 또는 표시할 수 있다. 내부 또는 외부 공격자 IP에서 발생한 보안이벤트를 세계지도 또는 대상기관 지도에 표시하는 방법은 상술한 바와 같이, 선, 점, 화살표 등을 포함할 수 있고, 보안이벤트의 종류에 따라서 표시방법은 달라질 수 있다.

[0332] 도 19는 본 발명의 일 실시예에 따른 가시화 방법을 나타낸 도면이다.

[0333] 도 19는 도 18에 도시된 가시화 방법의 일 실시예를 나타낸다. 도 19는 본 발명의 일 실시예에 따른 공격자 가시화 방법을 나타내고, 구체적으로, 공격자가 내부 공격자인 경우 보안이벤트에 대한 통계정보를 가시화하는 방법을 나타낸다. 적어도 하나 이상의 내부 공격자 IP (예를 들어, IP A, B, C, D, E, F, G, H) 에 대한 영역이

타원 궤도 모형 상에 표시될 수 있다. 여기서, IP 영역은 도 18에 도시된 IP 영역이 확장된 형태일 수 있다. 타원 궤도 모형의 중앙에는 내부 공격자 IP 에 대해 발생한 보안 이벤트로부터 추출된 통계정보와 연결될 세계지도가 위치할 수 있다. 세계지도로부터 바깥으로 멀어지는 방향은 IP 별 시간 축을 의미할 수 있고, 타원 궤도 안에 줄 간격은 시간 간격을 나타낼 수 있다. 또한, 내부 공격자 가시화 데이터가 실시간 또는 장기간 가시화 데이터인 경우에 따라서 실시간 가시화 데이터인 경우 세계지도와 선의 형태로 연결될 수 있다. 여기서, 세계지도와 연결되는 통계정보는 실시간 가시화 데이터에 한정되는 것은 아니고, 가시화 데이터의 확인 필요성에 따라서 연결되는 정보는 본 발명의 일 실시예에 따라서 다양할 수 있다. 본 발명의 실시예에 따라, 도 19에 도시된 바와 같이 적어도 하나 이상의 내부 공격자 IP에 대한 통계치 (예를 들어, 통계치 1 내지 5) 정보가 타원 궤도 모형 상에서 표시될 수 있다. 여기서, IP 별 시간 축을 따라서 시간 간격에 해당하는 통계치 정보가 면 또는 선 상에서 표시될 수 있다. 그리고, 통계치 정보가 표시되는 영역은 본 발명의 일 실시예에 따라서 다양하게 설정될 수 있다. 또한, 표시되는 통계치 정보는 색을 달리하여 구분될 수 있게 표시될 수 있다.

[0334] 도 20은 본 발명의 일 실시예에 따른 가시화 방법을 나타낸 도면이다.

[0335] 도 20은 도 18에 도시된 가시화 방법의 일 실시예를 나타낸다. 도 20은 본 발명의 일 실시예에 따른 공격자 가시화 방법을 나타내고, 구체적으로, 공격자가 외부 공격자인 경우 보안이벤트에 대한 통계정보를 가시화하는 방법을 나타낸다. 적어도 하나 이상의 외부 공격자 IP (예를 들어, 예를 들어, IP A, B, C, D, E, F, G, H) 에 대한 영역이 타원 궤도 모형 상에 표시될 수 있다. 여기서, IP 영역은 도 18에 도시된 IP 영역이 확장된 형태일 수 있다. 타원 궤도 모형의 중앙에는 외부 공격자 IP 에 대해 발생한 보안 이벤트로부터 추출된 통계정보와 연결될 대상기관 지도가 위치할 수 있다. 대상기관 지도로부터 바깥으로 멀어지는 방향은 IP 별 시간 축을 의미할 수 있고, 타원 궤도 안에 줄 간격은 시간 간격을 나타낼 수 있다. 또한, 외부 공격자 가시화 데이터가 실시간 또는 장기간 가시화 데이터인 경우에 따라서 실시간 가시화 데이터인 경우 대상기관 지도와 선의 형태로 연결될 수 있다. 여기서, 대상기관 지도와 연결되는 통계정보는 실시간 가시화 데이터에 한정되는 것은 아니고, 가시화 데이터의 확인 필요성에 따라서 연결되는 정보는 본 발명의 일 실시예에 따라서 다양할 수 있다. 본 발명의 실시예에 따라, 도 20에 도시된 바와 같이 적어도 하나 이상의 내부 공격자 IP에 대한 통계치 (예를 들어, 통계치 1 내지 5) 정보가 타원 궤도 모형 상에서 표시될 수 있다. 여기서, IP 별 시간 축을 따라서 시간 간격에 해당하는 통계치 정보가 면 또는 선 상에서 표시될 수 있다. 그리고, 통계치 정보가 표시되는 영역은 본 발명의 일 실시예에 따라서 다양하게 설정될 수 있다. 또한, 표시되는 통계치 정보는 색을 달리하여 구분될 수 있게 표시될 수 있다.

[0336] 이하에서는, 본 발명에 따른 일 실시예는 공격자 상관정보를 가시화하는 장치 및 방법을 설명한다.

[0337] 도 21은 본 발명의 일 실시예에 따른 시스템 구성도를 도시한다.

[0338] 도 21에 도시된 바와 같이, 본 발명의 공격자 상관정보 가시화 장치는 보안이벤트 저장 스토리지 및/또는 IP주소 기반 공격자 상관정보 가시화 시스템을 포함할 수 있다. 여기서, IP 주소 기반 공격자 상관정보 가시화 시스템은 본 명세서에서 가시화 시스템, 가시화 장치, 공격자 상관정보 가시화 장치, 공격자 상관정보 가시화 시스템 등으로 명명될 수 있다.

[0339] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 도 21에 도시된 시스템에 따라서 도 23에 도시된 바와 같이 공격자 상관정보 가시화를 수행할 수 있다.

[0340] 보안이벤트 저장 스토리지는 보안이벤트를 저장할 수 있다. 본 발명의 일 실시예에 따른 보안이벤트 저장 스토리지는 공격자 상관정보 가시화 장치로부터 보안이벤트를 요청 받고, 공격자 상관정보 가시화 장치로 보안이벤트를 전송할 수 있다.

[0341] IP주소 기반 공격자 상관정보 가시화 시스템은 도 21에 도시된 바와 같이, 전처리 컴포넌트, 통계정보 생성/관리 컴포넌트, 및/또는 가시화 컴포넌트를 포함할 수 있다.

[0342] 도 21에 도시된 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치에 포함된 컴포넌트의 구체적 기능은 이하에서 설명한다.

[0343] 도 21에 도시된 전처리 컴포넌트는 도 22의 전처리 시스템에 해당할 수 있다. 도 21에 도시된 통계정보 생성/관리 컴포넌트는 도 22에 도시된 가시화 데이터 생성 컴포넌트에 해당할 수 있다. 도 21에 도시된 가시화 컴포넌트는 도 22에 도시된 가시화 엔진 컴포넌트에 해당할 수 있다. 도 22에 도시된 공격자 상관정보 가시화 장치는 도 21에 도시된 시스템 구성도를 상세히 나타낸 도면이다. 따라서, 각 컴포넌트의 명칭은 각 도면에 따라서 그

용어가 가지는 실질적인 의미와 본 명세서의 전반에 걸친 내용을 토대로 해석되어야 한다.

[0344] 도 21에 도시된 공격자 상관정보 가시화 장치가 가시화하는 방법은 도 23에서 후술한다.

[0345] 도 22는 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치의 시스템을 도시한다.

[0346] 도 22에 도시된 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 과학기술사이버안전센터에서 운용중인 침해위협수집시스템(TMS) 보안이벤트를 중심으로 악성(Malicious) 및 의심(Suspicious) IP정보를 직관적이고 신속하게 파악할 수 있는 가시화 시스템에 해당한다.

[0347] 도 22에 도시된 바와 같이 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 이벤트 분류 컴포넌트, 가시화 데이터 생성 컴포넌트, IP 상관관계 판단 컴포넌트, 가시화 엔진 컴포넌트, 이상행위 알림 컴포넌트, 및/또는 환경 설정 컴포넌트를 포함할 수 있다. 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치에 포함된 각 컴포넌트의 기능은 이하에서 설명한다. 여기서, 컴포넌트는 시스템을 이루는 하나의 구성요소이고, 실시예에 따라서 모듈 등의 명칭으로 명명될 수 있다.

[0348] 이벤트 분류 컴포넌트는 이벤트 분류(예를 들어, 사고처리 유 무, 블랙리스트)에 따른 가시화 데이터를 분류할 수 있다.

[0349] 가시화 데이터 생성 컴포넌트는 IP별 보안이벤트 발생 횟수 및 연결된 상대 IP 개수를 산출할 수 있다.

[0350] IP 상관관계 판단 컴포넌트는 IP 상관관계에 따른 가시화 데이터를 분류할 수 있다.

[0351] 가시화 엔진 컴포넌트는 가시화 데이터 송 수신 및 상관정보를 실시간 가시화할 수 있다.

[0352] 이상행위 알림 컴포넌트는 블랙 IP 관리 및 이상행위를 보안관제요원에게 알림을 제공할 수 있다.

[0353] 환경 설정 컴포넌트는 공격자 상관정보 가시화 시스템에 필요한 정보들을 설정할 수 있다.

[0354] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치에 포함된 각 컴포넌트의 구체적인 기능을 이하에서 설명한다.

[0355] 본 발명의 일 실시예에 따른 이벤트 분류 컴포넌트는 전처리 시스템으로부터 데이터 수신할 수 있다. 여기서, 데이터 수신 항목은 탐지시간, 출발지 IP, 출발지 포트, 도착지 IP, 도착지 포트, 탐지건수, 기관코드 등을 포함할 수 있다.

[0356] 본 발명의 일 실시예에 따른 이벤트 분류 컴포넌트는 외부정보 수집 기능을 수행할 수 있다. 여기서, White Black IP, 사고 처리 이력은 GUI를 통한 직접 입력 수정과 대상기관 정보가 포함된 XML, JSON, CSV 등의 파일을 통한 입력이 가능해야 한다. 본 발명의 일 실시예에 따른 이벤트 분류 컴포넌트는 외부정보 출력 기능을 수행할 수 있다. 구체적으로, 시스템에 입력된 White Black IP, 사고처리 이력을 일정한 파일 포맷으로 출력할 수 있다.

[0357] 본 발명의 일 실시예에 따른 이벤트 분류 컴포넌트는 수신된 데이터를 기반으로 보안이벤트를 다음과 같이 분류할 수 있다. 본 발명의 일 실시예에 따라 분류되는 보안이벤트는 단순 보안이벤트, 사고처리 有 이벤트, 블랙리스트 이벤트 등을 포함할 수 있다.

[0358] 단순 보안이벤트는 사고처리 有 이벤트와 블랙리스트 이벤트에 모두 해당사항이 없는 경우이다.

[0359] 사고처리 有 이벤트는 전처리 시스템으로부터 받은 사고처리 이력이 있는 IP일 경우이다.

[0360] 블랙리스트 이벤트는 외부정보 수집 기능을 과 이상행위 알림 컴포넌트로부터 전송받은 블랙리스트에 해당할 경우이다.

[0361] 본 발명의 일 실시예에 따른 이벤트 분류 컴포넌트는 전처리 정보 수집 검증 및 재전송 기능을 수행할 수 있다. 특히, 전처리 시스템으로부터 수신한 데이터가 원본 데이터와 상이한지 여부를 실시간으로 검증하고 다를 경우 재전송이 가능해야 한다.

[0362] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP간의 보안이벤트 발생 횟수를 카운트하는 기능을 수행할 수 있다. 구체적으로, 내외부 공격자 IP 추출 컴포넌트에서 추출된 IP들 사이에 발생한 보안 이벤트를 카운트할 수 있다.

[0363] 본 발명의 일 실시예에 따른 가시화 데이터 생성 컴포넌트는 IP별 보안이벤트를 발생시킨 상대 IP 개수를 카운

트하는 기능을 수행할 수 있다. 구체적으로, 각 IP별로 보안이벤트를 발생시킨 IP의 개수도 함께 카운트 한다. 즉, IP별 보안이벤트 발생횟수와 연결된 상대 IP 개수에 대한 카운트가 가능해야 한다. 예를 들어, A→B, B→A, C→A 3건의 보안이벤트 발생 시 A↔B는 2건, A↔C는 1건, A는 2개의 IP와 연결, B와 C는 각각 1개의 IP와 연결이 발생한 것으로 볼 수 있다. 여기서, 가시화 업데이트 주기에 따라 IP 주소 공간 배치 가시화에 필요한 IP별 보안이벤트 발생횟수와 연결된 상대 IP 개수를 실시간 카운트할 수 있다.

[0364] 본 발명의 일 실시예에 따른 IP 상관 관계 판단 컴포넌트는 가시화 데이터 생성 컴포넌트로부터 분류된 데이터 수신하여 IP 상관관계를 판단할 수 있다. 본 발명의 일 실시예에 따른 IP 상관관계는 출발지/목적지 연결 및 임계치 이상 보안이벤트 발생을 포함할 수 있고, 그 구체적 내용은 다음과 같다.

[0365] 출발지/목적지 연결 : IP주소들 간에 출발지와 목적지로 분류

[0366] 임계치 이상 보안이벤트 발생 : IP주소들 간에 설정된 임계치 이상의 보안이벤트가 발생하는 경우

[0367] 여기서, 본 발명의 일 실시예에 따라 기본적으로 출발지/목적지 연결로 분류되지만, 환경 설정 컴포넌트로부터 전송받은 조건인 보안이벤트 횟수 이상이 발생될 경우 임계치 이상 보안이벤트 발생으로 판단될 수 있다.

[0368] 본 발명의 일 실시예에 따른 IP 상관 관계 판단 컴포넌트는 환경 설정 컴포넌트로부터 임계치 이상 보안이벤트 횟수 설정 정보를 수신할 수 있다.

[0369] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 데이터 송 수신 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 생성 컴포넌트에서 생성한 모든 가시화 정보(예를 들어, 장기 및 실시간 가시화 정보 포함)를 실시간으로 요청하고 수집할 수 있다. 여기서, 가시화 엔진 컴포넌트를 상관정보 공격자 상관정보 가시화 시스템 내부가 아닌 별도 가시화 전용 시스템 형태로 구축하므로, 내부 공격자 가시화 시스템과의 연계(예를 들어, 데이터 송 수신 등)가 가능해야 한다.

[0370] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 데이터 송 수신 검증 및 재전송 기능을 수행할 수 있다. 구체적으로, 가시화 데이터 송 수신에 대한 성공 여부를 실시간으로 검증할 수 있어야 하고 데이터 전송 실패 시 재전송이 가능해야 한다.

[0371] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화에 필요한 IP 주소 공간 배치를 할 수 있다. 가시화 엔진 컴포넌트는 2D 및/또는 3D로 모든 IP 공간 배치를 할 수 있다. 본 발명의 일 실시예에 따라 2D 극좌표계(예를 들어, 원 모양)를 사용하는 경우 다음과 같다.

[0372] $$(r,\theta)\rightarrow(x=r\cos\theta,\ y=r\sin\theta)$$

[0373] $$r=R\times\frac{Count}{Max\,Count}\ \text{or}\ R\times\frac{IPAddress}{2^{32}}$$
($R=$ 반지름, $Count=$ 각 IP에서 발생된 이벤트 수)

[0374] $$\theta=\frac{IPAddress}{2^{32}}\times 2\pi$$

[0375] 좌표계에 따른 가시화는 도 23과 같이 나타날 수 있다. 여기서, 좌표계를 구성하는 r은 반지름, Θ는 각도를 의미한다. IP address는 공간 배치를 통해 가시화되는 IP 주소를 나타낸다. 그리고, R은 공간 배치를 통해 가시화되는 IP 주소를 나타내는 점 또는 2D 원형 형태의 반지름을 의미한다. R 반지름은 좌표계를 구성하는 r 반지름과는 구분된다. 또한, R은 본 발명의 일 실시예에 따라 최대값으로 설정될 수 있으며, 최대값은 보안이벤트를 관제하는 기관의 통계 데이터에 기초하여 결정될 수 있다.

[0376] 여기서, r은 IP 주소에 count 값에 기초하여 계산될 수 있고, 본 발명의 일 실시예에 따라서, IP 주소에 기초하여 계산될 수도 있다.

[0377] 여기서, 카운트(count) 값은 각 IP에서 발생된 이벤트의 수를 의미한다. 또한, 커넥트(connect) IP는 해당 IP와 연결된 IP의 수를 의미한다. 즉, r, h의 값이 커질수록 원점에서 멀어지고 해당 IP에서 발생된 이벤트 수와 해당 IP와 연결된 IP의 수가 많음을 나타낸다.

[0378] 한편, 본 발명의 일 실시예에 따라 3D 원기둥좌표계(예를 들어, 원통모양)을 사용하는 경우 다음과 같다.

[0379] $$(r,\theta,h)\rightarrow(x=r\cos\theta, y=r\sin\theta, z=h)$$

[0380] $$r=R\times\frac{Count}{Max\,Count}\ \text{or}\ R\times\frac{(A,B\,Class)}{2^{16}}$$
(R= 반지름, $Count$= 각 IP에서 발생된 이벤트 수)

[0381] $$\theta=\frac{IP\,Address}{2^{32}}\times 2\pi\ \text{or}\ \frac{IP\,Address \bmod 360}{360}\times 2\pi$$

[0382] $$h=R\times\frac{Connect\,IP}{Max\,Connect\,IP}\ \text{or}\ R\times\frac{(C,D\,Class)}{2^{16}}$$
(R= 반지름, $Connect\,IP$= 해당 IP와 연결된 IP 수)

[0383] 좌표계에 따른 가시화는 도 23과 같이 나타날 수 있다. 여기서, 좌표계를 구성하는 r은 반지름, Θ는 각도를 의미한다. IP address는 공간 배치를 통해 가시화되는 IP 주소를 나타낸다. 그리고, R은 공간 배치를 통해 가시화되는 IP 주소를 나타내는 점 또는 3D 원형 형태의 반지름을 의미한다. R 반지름은 좌표계를 구성하는 r 반지름과는 구분된다. 또한, R은 본 발명의 일 실시예에 따라 최대값으로 설정될 수 있으며, 최대값은 보안이벤트를 관제하는 기관의 통계 데이터에 기초하여 결정될 수 있다.

[0384] 여기서, r은 count 값에 기초하여 계산될 수 있고, 본 발명의 일 실시예에 따라서 IP 주소에 기초하여 계산될 수 있다. 구체적으로, IP 주소를 이용하는 경우 IP 주소를 구성하는 클래스 A, B 값을 이용하여 r을 계산하는 실시예를 상기 수식에서 기재하고 있다.

[0385] 또한, h는 connect IP 값에 기초하여 계산 될 수 있고, 본 발명의 일 실시예에 따라서 IP 주소에 기초하여 계산될 수 있다. 구체적으로, IP 주소를 이용하는 경우 IP 주소를 구성하는 클래스 C, D 값을 이용하여 h를 계산하는 실시예를 상기 수식에서 기재하고 있다.

[0386] 여기서, 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 외부 IP의 경우, 높이는 양수로 대상기관 IP의 경우, 높이는 음수로 가시화 표현(예를 들어, 원기둥의 위쪽 : 외부 IP들, 원기둥의 아래쪽 : 대상기관 IP들)할 수 있다. 반대로, 외부 IP의 경우, 높이는 음수로, 대상기관 IP의 경우, 높이는 양수로 가시화 표현될 수 있다.

[0387] 또한, 가시화에 필요한 IP 주소 공간 배치의 경우 본 발명의 일 실시예에 따라서 배치될 수 있다.

[0388] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 IP 이벤트 발생 시간에 따른 투명도 설정을 수행할 수 있다. 구체적으로, 최대 누적 가시화 데이터 주기에 따른 시간별 투명도를 적용할 수 있다. 예를 들어, 0~6시간인 경우 투명도 0%, 6~12시간인 경우 투명도 25%, 12~18시간인 경우 투명도 50%, 18~24시간인 경우 투명도 75%로 설정할 수 있다.

[0389] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 이벤트 분류 컴포넌트와 IP 상관관계 판단 컴포넌트를 통해 분류된 데이터를 가시화할 수 있다. 구체적으로, 분류 이벤트 가시화를 다음과 같이 할 수 있다. 단순 보안이벤트인 경우, 예를 들어, 백색, 사고처리 有 이벤트인 경우, 예를 들어, 황색, 블랙리스트 이벤트인 경우, 적색, 블랙 IP 판단 이벤트인 경우, 예를 들어, 주황색으로 표시할 수 있다. 여기서, 가시화할 각 데이터들에 대한 크기 및 모양 설정 기능을 수행할 수 있다. 또한, 환경 설정 컴포넌트로부터 분류 이벤트 가시화할 색 정보를 수신할 수 있다. 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 상관관계 가시화를 할 수 있다. 구체적으로, 상관관계에 따라서, 출발지/목적지 연결인 경우, 예를 들어, 점선, 임계치 이상 보안이벤트 발생인 경우, 예를 들어, 실선으로 가시화할 수 있다. 여기서, 출발지/목적지 연결 데이터에서 설정된 보안이벤트 횟수 이상이 되어 실선으로 바뀔 경우 확인 가능한 강조 표시를 할 수 있다. 예를 들어, 깜박임, 및/또는 색바뀜을 통해서 표시할 수 있다. 그리고, 환경 설정 컴포넌트로부터 강조 표시(깜박임, 색바뀜) 정보를 수신할 수 있다. 나아가, 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 임계치 이상의 IP들과 연결된 IP의 경우 크기를 증가시켜 표현할 수 있다.

[0390] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 크기가 증가된 IP의 경우 블랙 IP로 판단하는 기능을 제공할 수 있다. 구체적으로, 임계치 이상의 IP들과 연결된 IP의 가시화 크기 증가 설정에 따른 블랙 IP 판단 기능을 제공할 수 있다.

[0391] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화된 IP 클릭 시 세부정보를 제공할 수 있다. 구체적으로, 해당 IP, 연결된 IP 목록, 각 연결 간 발생 이벤트 수, 기관명, 및/또는 지역명 관련한 세부정보를 제공할 수 있다.

[0392] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 이상행위 알림 컴포넌트로부터 블랙 IP를 수신할 수 있다. 여기서, 이벤트 분류 컴포넌트에서 분류된 블랙리스트 이벤트와 다른 색 또는 다른 모양으로 가시화할 수 있다.

[0393] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 화면 좌측에 IP Rank 표시 기능을 제공할 수 있다. 여기서, 일정 수준이상의 보안이벤트 발생 IP to IP 리스트, 일정 수준이상의 IP와 연결된 IP 리스트를 선택할 수 있다.

[0394] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 화면 하단에 범례 표시 기능을 제공할 수 있다. 본 발명에 따른 가시화 정보 표시는 다음과 같다. 단순 보안이벤트인 경우, 예를 들어, 백색, 사고처리 有 이벤트인 경우, 예를 들어, 황색, 블랙리스트 이벤트인 경우, 예를 들어, 적색, 블랙 IP 판단 이벤트인 경우, 예를 들어, 주황색, 출발지/목적지 연결인 경우, 예를 들어, 점선, 임계치 이상 보안이벤트 발생인 경우, 예를 들어, 실선으로 표시할 수 있다.

[0395] 본 발명의 일 실시예에 따른 가시화 엔진 컴포넌트는 가시화 화면 회전 및 줌인/줌아웃 하는 기능을 제공할 수 있다.

[0396] 본 발명의 일 실시예에 따른 이상 행위 알림 컴포넌트는 블랙리스트로 판단된 IP에 대한 메일 자동 발송 기능을 제공할 수 있다. 구체적으로, 자동메일 발송 시 메일 제목, 블랙 IP, 시간, 연결된 IP 목록 포함할 수 있고, 보안관제요원이 블랙 IP로 판단된 IP들에 대해 가시화 뷰어 컴포넌트에서 표시할 블랙 IP 선택이 가능하다.

[0397] 본 발명의 일 실시예에 따른 이상 행위 알림 컴포넌트는 자동 메일 발송 활성 비활성화 설정 기능을 제공할 수 있다. 나아가, 메일 발송 기능 ON/OFF 설정 기능을 더 제공할 수 있다.

[0398] 본 발명의 일 실시예에 따른 이상 행위 알림 컴포넌트는 가시화 뷰어 컴포넌트로부터 전송받은 블랙 IP 관리 기능을 제공할 수 있다. 나아가, 가시화 통합저장 시스템으로 블랙 IP 전송을 수행할 수 있다.

[0399] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 엔진 설정 컴포넌트 및/또는 가시화 뷰어 설정 컴포넌트에 대한 기능을 설정할 수 있다. 이하에서 각 컴포넌트별 설정 기능을 설명한다.

[0400] 본 발명의 일 실시예에 따른 가시화 엔진 설정 컴포넌트에 대한 환경 설정 컴포넌트의 구체적 기능은 다음과 같다.

[0401] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화에 필요한 IP 주소 공간 배치 선택(예를 들어, 2D, 3D) 기능을 제공할 수 있다.

[0402] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 분류 이벤트 가시화 설정 기능을 제공할 수 있다. 나아가, 임계치 이상의 IP들과 연결된 IP의 가시화 크기 증가 기준(예를 들어, 1~n개 점점 커지게 하는 유형과 5개, 10개, 20개 등 일정 개수 이상이면 커지게 되는 유형)을 설정할 수 있다. 또한, 가시화 데이터 크기의 경우 본 발명의 일 실시예에 따라 변경될 수 있다. 예를 들어, 임계치 이상의 IP들과 연결된 IP의 크기 증가 표현하는 경우, 또는 최초 표시될 가시화 데이터 위치는 본 발명의 일 실시예에 따라서 결정될 수 있다.

[0403] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 IP 상관관계 판단 컴포넌트로 보안이벤트 임계치 설정 횟수를 전송할 수 있다. 구체적으로, 보안이벤트 횟수 설정을 예를 들어, 1~n회, 5회, 10회, 20회 등으로 설정할 수 있다.

[0404] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 주기 설정 기능을 제공할 수 있다. 구체적으로, 가시화 누적 데이터에 대한 주기 설정을 제공할 수 있다. 여기서, 시간(예를 들어, 일단위, 월단위), IP 개수(예를 들어, 최대 15만개)를 설정할 수 있고, 가시화 업데이트 주기 설정(예를 들어, 시간단위)을 제공할 수 있다. 또한, 가시화 주기 설정 기준은 본 발명의 일 실시예에 따라 결정할 수 있다.

[0405] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 이상행위 알림 설정 기능을 제공할 수 있다. 구체적으로, 메일 발송 시 송신자 및 수신자 지정 변경 등을 위한 기능, 또는 메일 자동 발송 기능을 제어(ON/OFF)하기 위한 기능을 제공할 수 있다.

[0406] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 블랙리스트 관리 설정 기능을 제공할 수 있다. 구체적으로, 블랙리스트에 등록된 IP 삭제/출력 기능이 가능할 수 있다.

[0407] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 환경 설정 컴포넌트의 기능은 키보드 단축키를 통한 입력을 제공할 수 있다.

[0408] 본 발명의 일 실시예에 따른 가시화 뷰어 설정 컴포넌트에 대한 환경 설정 컴포넌트의 구체적 기능은 다음과 같다.

[0409] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 분류 이벤트 가시화 설정 기능을 제공할 수 있다. 구체적으로, 가시화할 데이터에 대한 크기, 모양, 색 설정이 가능하다. 예를 들어, 모양은 원, 네모, 세모, 별 등을 포함할 수 있고, 색은 백색, 황색, 주황색, 적색 등을 포함할 수 있다.

[0410] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 상관관계 가시화 설정 기능을 제공할 수 있다. 구체적으로, 출발지/목적지 연결, 보안이벤트 발생을 실선 또는 점선, 색, 굵기, 밝기 선택을 제공할 수 있다. 여기서, 가시화 업데이트 시 강조 표시 선택을 할 수 있다. 예를 들어, 발지/목적지 연결 → 보안이벤트 발생인 경우 깜박임, 색바뀜 등으로 표시 선택을 할 수 있다.

[0411] 본 발명의 일 실시예에 따른 환경 설정 컴포넌트는 가시화 화면 좌측에 IP Rank 정보 선택 기능을 제공할 수 있다. 구체적으로, 일정 수준이상의 보안이벤트 발생 IP to IP 리스트, 일정 수준이상의 IP와 연결된 IP 리스트를 선택할 수 있다.

[0412] 본 발명의 일 실시예에 따른 상술한 내용은 모의 데이터를 통해 실제 표시해야 할 가시화 구현의 예를 후술한다.

[0413] 상술한 바와 같이, 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 도 22와 같이 통계정보 수집 컴포넌트, 가시화 데이터 생성 컴포넌트, 가시화 엔진 컴포넌트, 환경 설정 컴포넌트, 대상기관에 대한 정보를 저장하는 스토리지를 포함할 수 있고, 각 컴포넌트 간의 정보를 요청 및 전달하여 공격자 상관정보 가시화를 수행할 수 있다.

[0414] 도 23은 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 방법을 도시한다.

[0415] 도 23에 도시된 공격자 가시화 방법은 도 21에 도시된, 보안이벤트 저장 스토리지, 공격자 상관정보 가시화 시스템에 의해 가시화할 수 있다. 여기서, 공격자 상관정보 가시화 시스템은 전처리 컴포넌트, 통계정보 생성/관리 컴포넌트, 가시화 컴포넌트를 포함할 수 있다. 여기서, 컴포넌트는 시스템을 이루는 하나의 구성요소이고, 실시예에 따라서 모듈 등의 명칭으로 명명될 수 있다.

[0416] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 도 23에 도시된 바와 같이, 공격자 상관정보를 가시화할 수 있다.

[0417] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치의 가시화 방법은 다음의 과정을 따른다.

[0418] 1. 전처리 컴포넌트는 사용자가 요청 시(또는, 가시화 하고자 하는 기간 선택 시) 사용자가 지정한 기간(예를 들어, 1개월)동안 발생한 전체 보안이벤트를 보안이벤트 저장 스토리지에 요청하여 수집할 수 있다.

[0419] 2. '1' 에 따라 수집된 전체 보안이벤트들에 대해서 아래와 같은 통계 정보들을 추출한다.

[0420] 가. 출발지 · 도착지 IP

[0421] 나. IP별 보안이벤트 발생횟수(C)

[0422] 다. 출발지 · 도착지 IP쌍별 보안이벤트 발생횟수(EC)

[0423] 라. IP별 유니크한 IP쌍의 개수(IC)

[0424] 3. 추출된 IP들을 가시화하기 위해서 아래와 같은 절차에 따른다.

[0425] 가. 3차원 극좌표계(r, θ, h)를 사용하여 점으로 표현

[0426] 나. 제안한 극좌표계(r, θ, h)는 사용자 정의 반지름(R), '2-나', '2-라', IP를 이용하여 좌표를 결정한다.

[0427] 다. 외부 IP와 대상기관 IP는 h부호를 서로 다르게 표현한다.

[0428] 4. IP 이력(예를 들어, 단순 보안이벤트, 사고처리, 블랙리스트)에 따라 점의 색, 형태, 크기를 다르게 표현한다.

[0429] 5. c에 따라 IP간 연결선을 점선, 실선, 겹선, 쇄선, 파선 등의 다양한 형태로 표현한다.

[0430] 6. ic에 따라 점의 색, 형태, 크기를 다르게 표현한다.

[0432] 상술한 바와 같이, 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 도 23에 도시된 바와 같이 공격자 상관정보를 가시화할 수 있다. 공격자 상관정보 가시화 장치는 보안이벤트를 저장하는 스토리지로부터 보안이벤트를 수신할 수 있다. 공격자 상관정보 가시화 장치는 수신한 보안이벤트로부터 보안이벤트에 대한 통계정보를 생성 또는 추출할 수 있다. 여기서, 통계정보는 상술한 바와 같이 출발지/도착지(또는 목적지) IP, IP별 보안이벤트 발생횟수, 출발지/도착지 IP쌍별 보안이벤트 발생횟수, IP별 유니크한 IP쌍 개수 등을 포함할 수 있다. 보안이벤트에 대한 IP는 3차원 극좌표계를 사용하여 점으로 표현될 수 있다. 극좌표계의 좌표값은 도 22에서 상술한 바와 같다. 공격자 상관정보 가시화 장치는 보안이벤트에 대한 정보를 수신하여 보안이벤트에 대한 IP를 단순 보안이벤트, 사고처리 이벤트, 블랙리스트 이벤트로 분류할 수 있다. 여기서, 블랙리스트 이벤트란 별로도 블랙리스트로써 관리 대상이 되는 IP에 해당하는 경우, 해당 IP를 의미한다. 블랙리스트는 별도로 저장 및 관리될 수 있다. IP의 이력 분류를 마친 뒤, 공격자 상관정보 가시화 장치는 점의 형태로써 IP를 가시화할 수 있고, 이때, 점의 색, 형태, 크기를 다양하게 표현할 수 있다. 점으로 표현된 IP들 사이에 점선의 형태로 상관정보가 표시된 경우, 출발지/목적지를 의미하며, 보안이벤트 발생횟수가 임계치 이상이 되면, 실선의 형태로 표시될 수 있다. 예를 들어, IP A와 IP B 간에 A에서 B로 화살표가 생긴 경우, 출발지는 A이고, 목적지는 B가 될 수 있다. 또한, 상술한 바와 같이 A 및 B 사이에 점선의 형태로 상관정보가 가시화될 수 있다. 공격자 상관정보 가시화 장치는 상관정보를 가시화하는데 있어서, 출발지/목적지를 화살표를 사용하여 가시화하진 않고, 해당 IP를 선택하면 상세정보로써 출발지/목적지 정보를 제공할 수 있다. 도 23에 도시된 바와 같이, 공격자 상관정보 가시화 장치는 보안이벤트에 대한 IP를 파악할 수 있고, 각 IP별로 보안이벤트 발생 횟수 및 해당 IP와 연결된 IP의 수를 가시적으로 파악할 수 있는 효과를 제공할 수 있다.

[0433] 상술한 바와 같이, 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 장치는 보안이벤트에 대해서 출발지 IP 주소 정보, 목적지 IP 주소 정보를 통계정보로써 추출할 수 있다. 나아가, IP 주소 별로 보안이벤트 발생횟수, 출발지 IP 주소, 목적지 IP 주소 쌍 간에 발생한 보안이벤트 발생횟수, IP 주소 쌍의 개수를 통계정보로써 추출할 수 있다. 예를 들어, IP 주소 A와 연결된 IP 주소가 B, C 가 있는 경우, IP 주소 쌍의 개수는 2개가 되고, A에서 발생한 보안이벤트 발생횟수, A-B 쌍 및 A-C 쌍 각각에서 발생한 보안이벤트 발생횟수가 통계정보로써 추출될 수 있다.

[0434] 도 24는 본 발명의 일 실시예에 따른 보안이벤트 자동 검증 방법을 나타낸 도면이다.

[0435] 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.

[0436] 보안이벤트 및 보안이벤트와 관련된 정보를 입력받는 단계 (S22010)에 대한 상세한 설명은 도 2, 3, 7에서 전술하였다.

[0437] 보안이벤트의 특성을 추출하는 단계 (S22020)에 대한 상세한 설명은 도 2, 5, 7에서 전술하였다.

[0438] 보안이벤트를 분류하는 단계 (S22030)에 대한 상세한 설명은 도 2, 6, 7에서 전술하였다.

[0439] 보안이벤트를 검증하는 단계 (S22040)에 대한 상세한 설명은 도 2, 4, 7, 8, 9, 10, 11, 12, 13에서 전술하였다.

[0440] 도 25는 본 발명의 일 실시예에 따른 공격자 가시화 방법을 나타낸 도면이다.

[0441] 본 발명의 일 실시예에 따른 공격자 가시화 방법은 보안이벤트를 수신하는 단계(S23010), 보안이벤트에 대한 통계정보 및 가시화 데이터 생성하는 단계(S23020), 및/도는 통계정보 및 가시화 데이터를 가시화하는 단계(S23030)를 포함할 수 있다.

[0442] 보안이벤트를 수신하는 단계(S23010)에 대한 상세한 설명은 도 14, 15에서 전술하였다.

[0443] 보안이벤트에 대한 통계정보 및 가시화 데이터 생성하는 단계(S23020)에 대한 상세한 설명은 도 16, 17에서 전술하였다.

[0444] 통계정보 및 가시화 데이터를 가시화하는 단계(S23030)에 대한 상세한 설명은 도 18 내지 20에서 전술하였다.

[0445] 도 26은 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 방법을 나타낸 도면이다.

[0446] 본 발명의 일 실시예에 따른 공격자 상관정보 가시화 방법은 보안이벤트를 수신하는 단계(S24010), 보안이벤트에 대한 통계정보를 추출하는 단계(S24020), 및/또는 보안이벤트에 대한 통계정보를 가시화하는 단계(S24030)를 포함할 수 있다.

[0447] 보안이벤트를 수신하는 단계(S24010)에 대한 상세한 설명은 도 21에서 전술하였다.

[0448] 보안이벤트에 대한 통계정보를 추출하는 단계(S24020)에 대한 상세한 설명은 도 22에서 전술하였다.

[0449] 보안이벤트에 대한 통계정보를 가시화하는 단계(S24030)에 대한 상세한 설명은 도 23에서 전술하였다.

[0450] 본 발명의 실시예들에 따른 컴포넌트, 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.

[0451] 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.

[0452] 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.

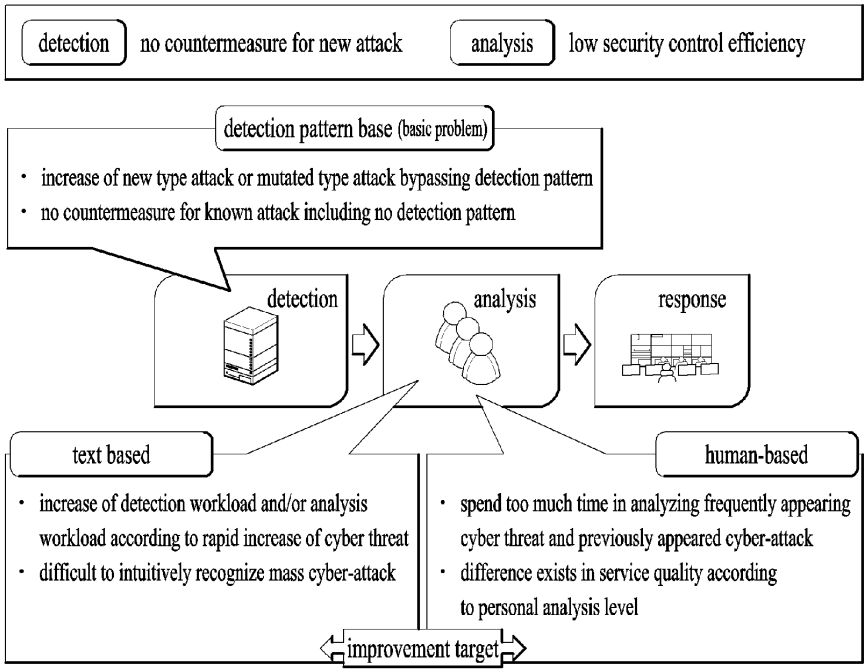
[0453] 한편, 본 발명의 영상 처리 방법은 네트워크 디바이스에 구비된 프로세서가 읽을 수 있는 기록매체에 프로세서가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 프로세서가 읽을 수 있는 기록매체는 프로세서에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 프로세서가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한, 프로세서가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 프로세서가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0454] 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.

[0455] 그리고, 당해 명세서에서는 물건 발명과 방법 발명이 모두 설명되고 있으며, 필요에 따라 양 발명의 설명은 보충적으로 적용될 수가 있다.

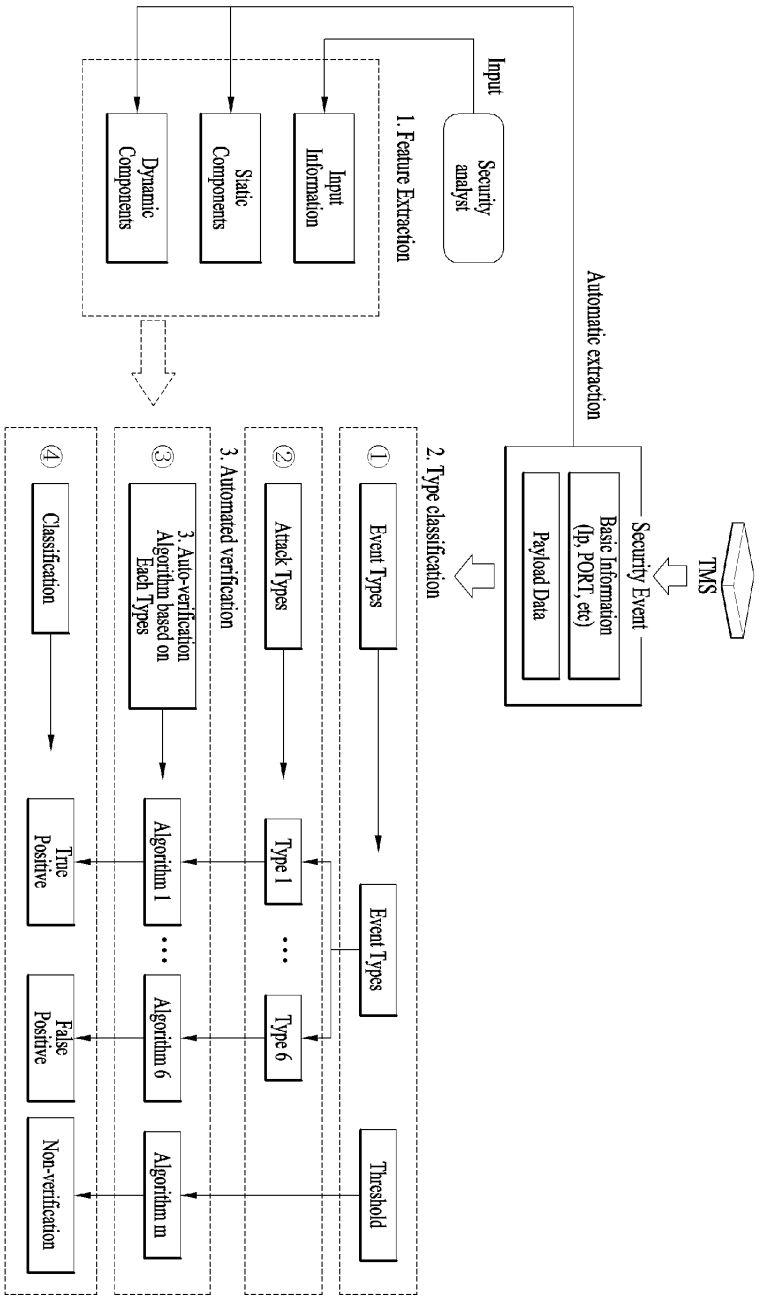
도면

도면1



※ based on information collected in the year 2012 of Science-technology cyber security center, about 7 million security events occur a day.

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

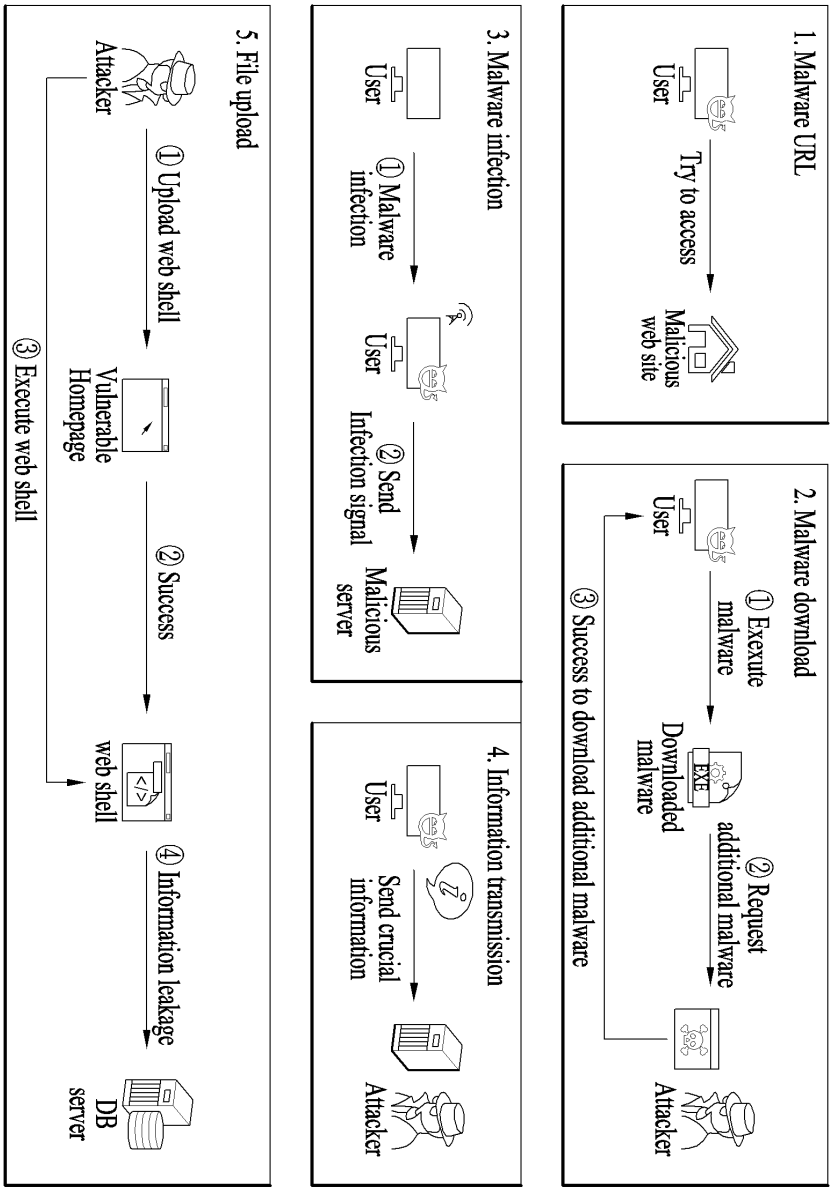
도면4

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	

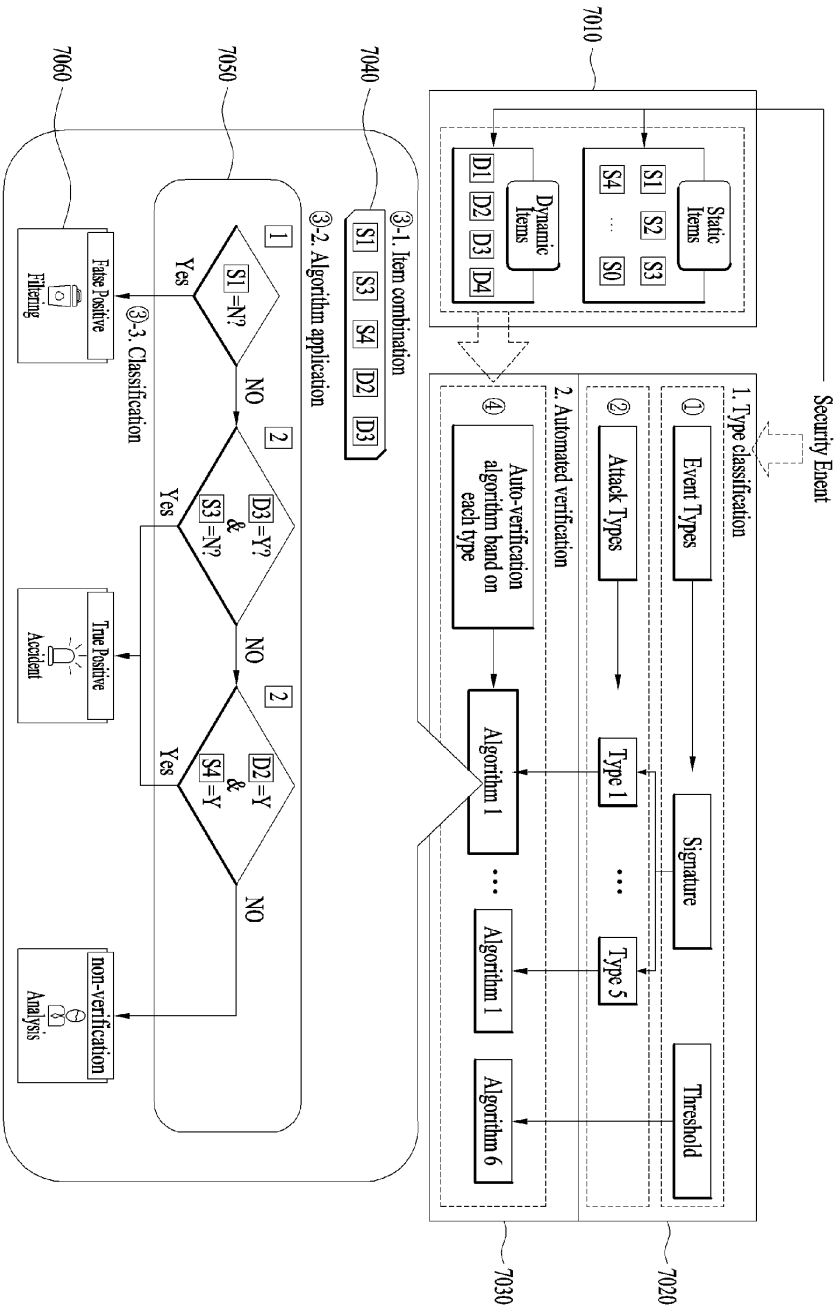
도면5

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

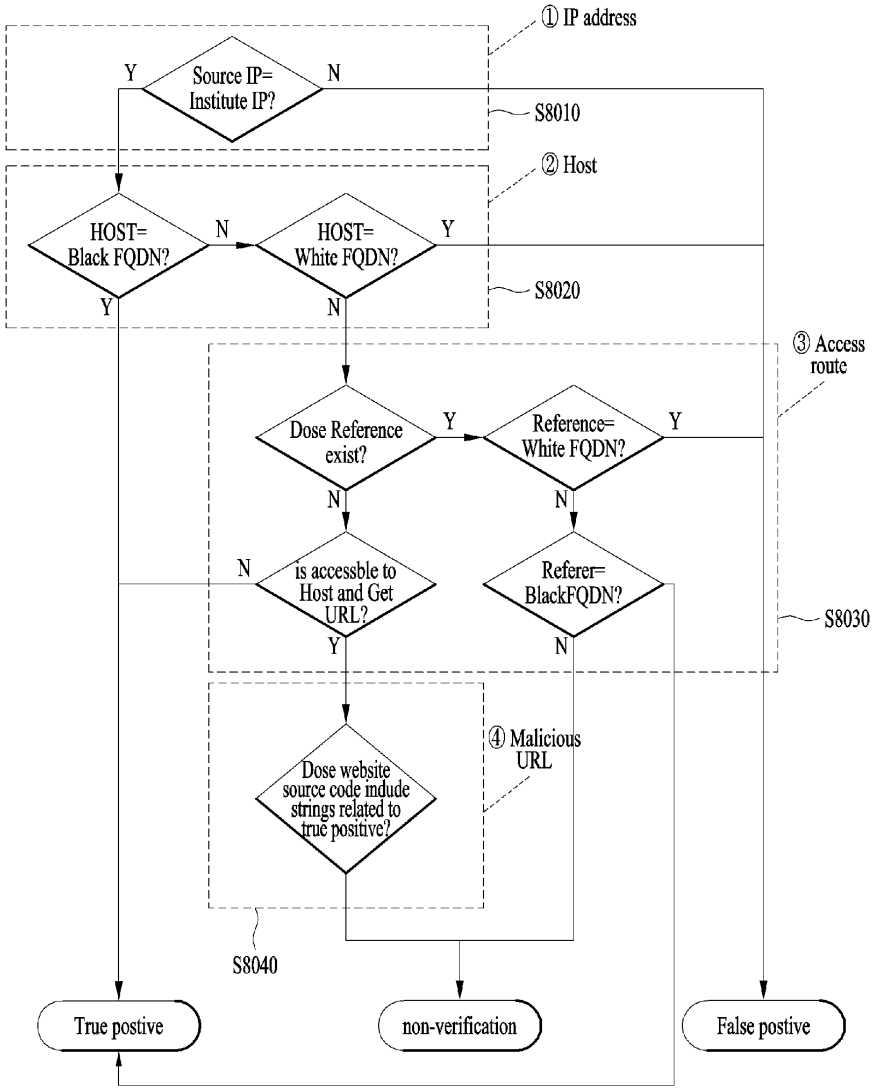
도면6


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
④ Information leakage
DB server
③ Execute web shell

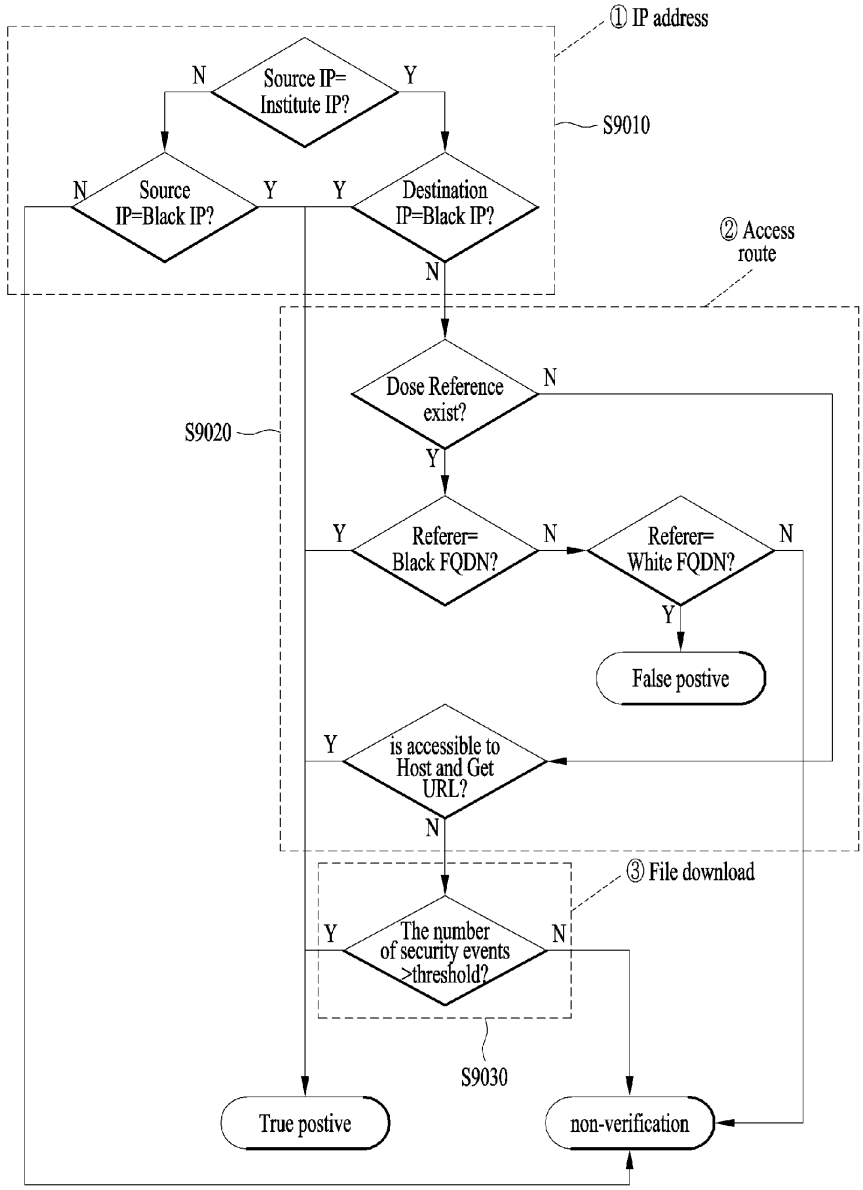
도면7


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

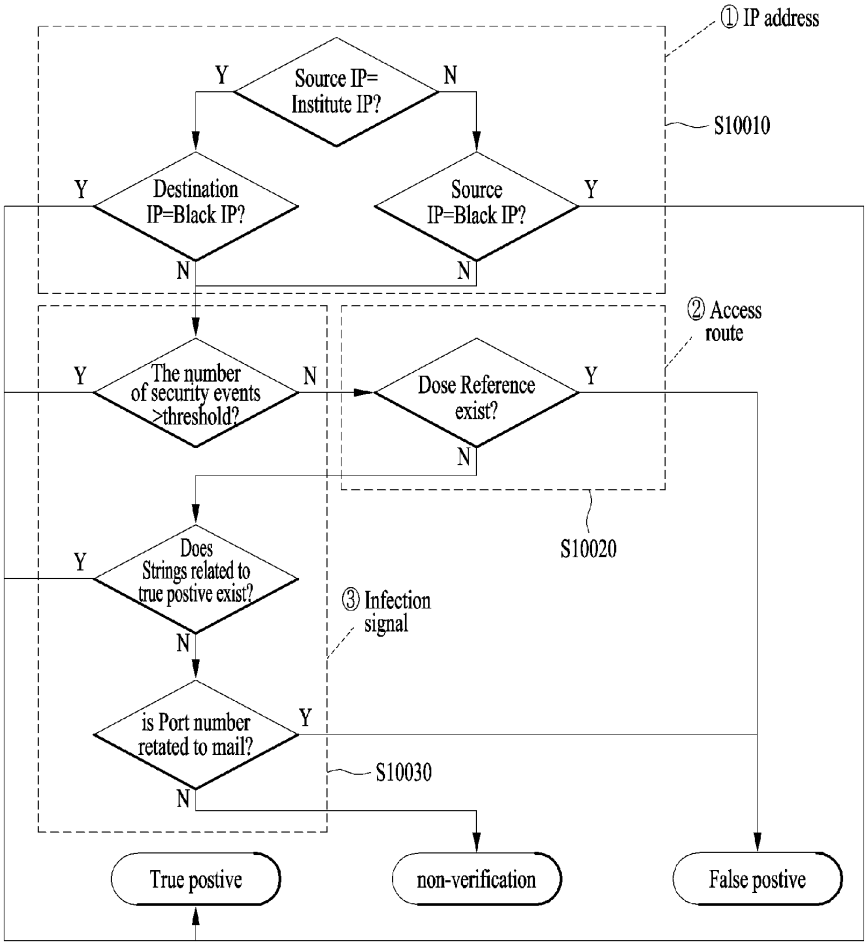
도면8


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

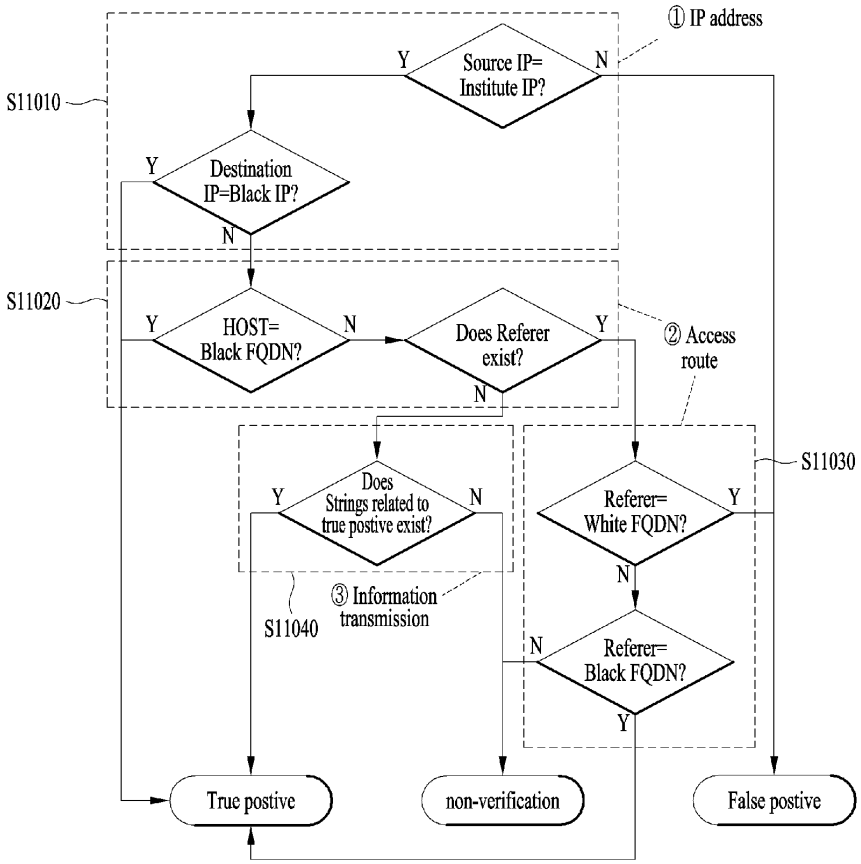
도면9


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

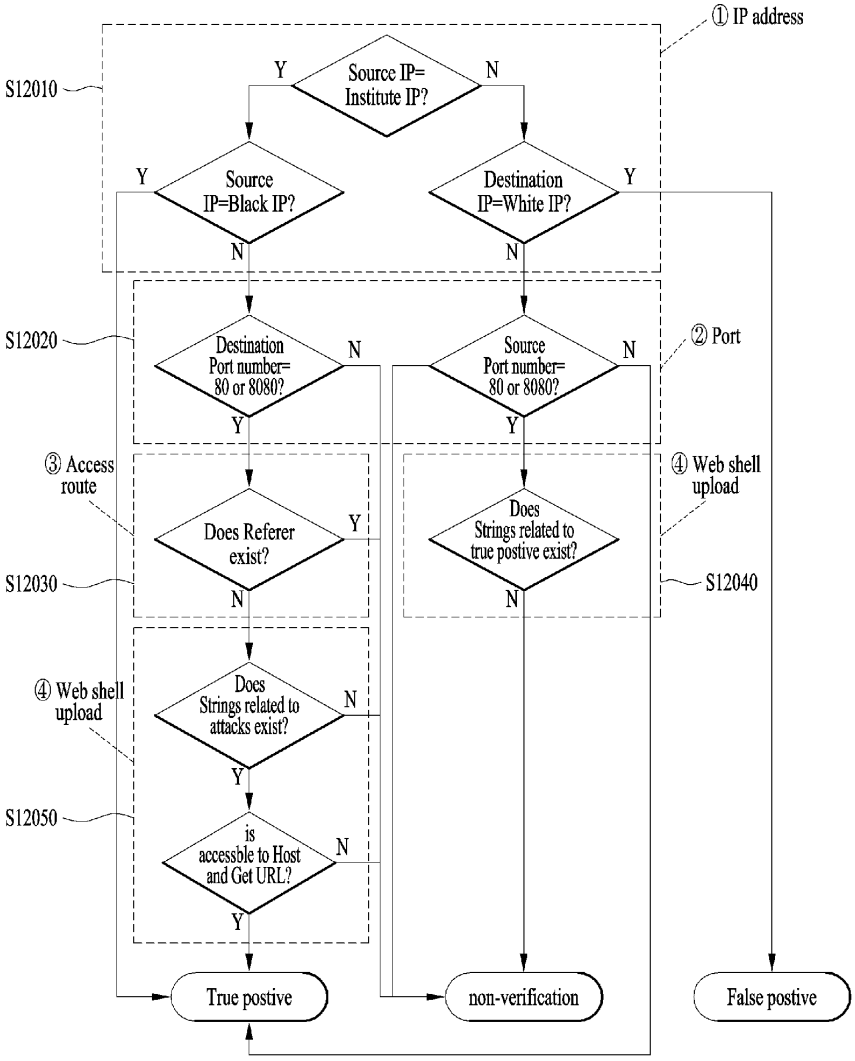
도면10


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

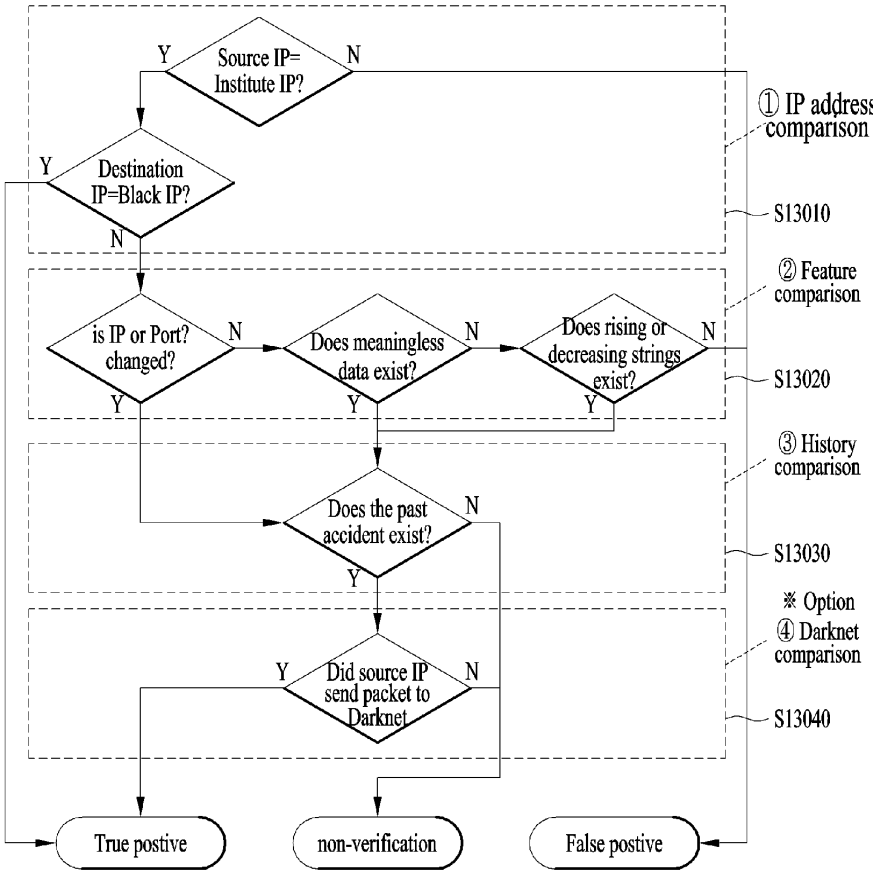
도면11


① IP address
S11010
Source IP= Institute IP?
Y
N
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
S11040
③ Information transmission
Referer= White FQDN?
Y
N
Referer= Black FQDN?
N
Y
True postive
non-verification
False postive

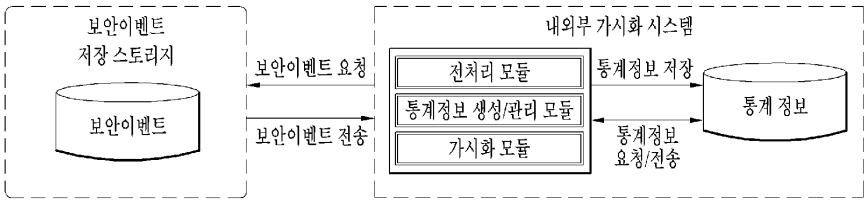
도면12


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

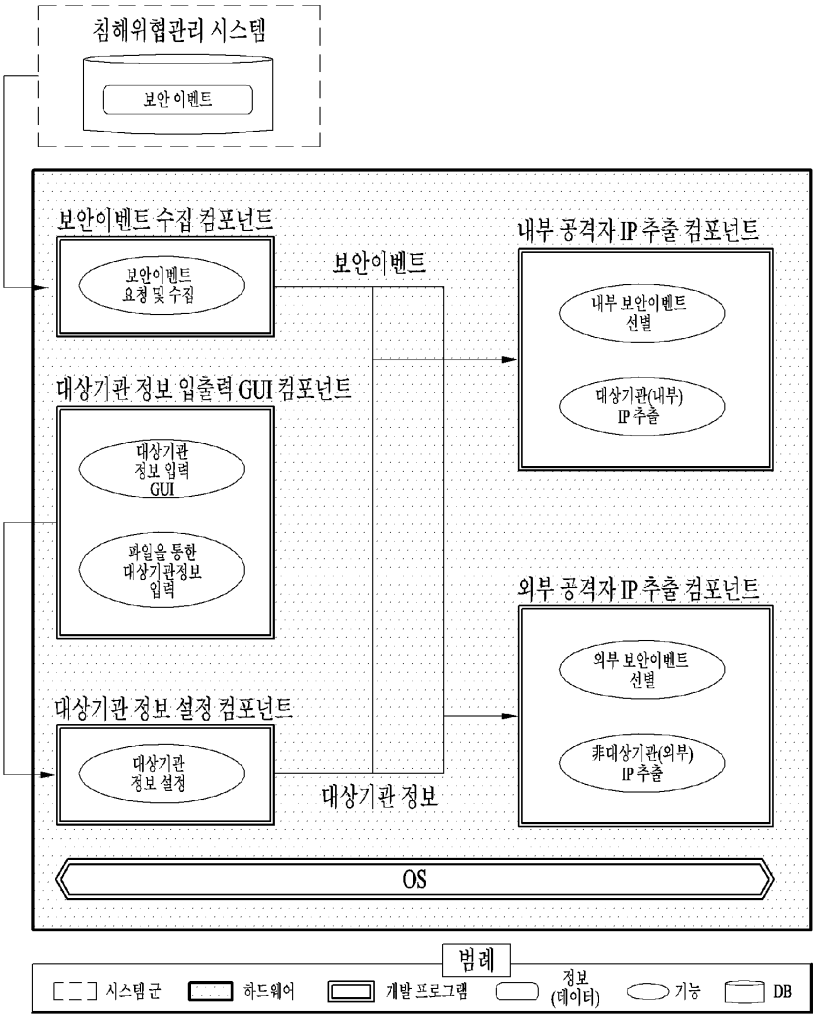
도면13


Source IP= Institute IP?
Y
N
① IP address comparison
Destination IP=Black IP?
S13010
② Feature comparison
is IP or Port? changed?
Does meaningless data exist?
Does rising or decreasing strings exist?
S13020
③ History comparison
Does the past accident exist?
S13030
※ Option
④ Darknet comparison
Did source IP send packet to Darknet
S13040
True postive
non-verification
False postive

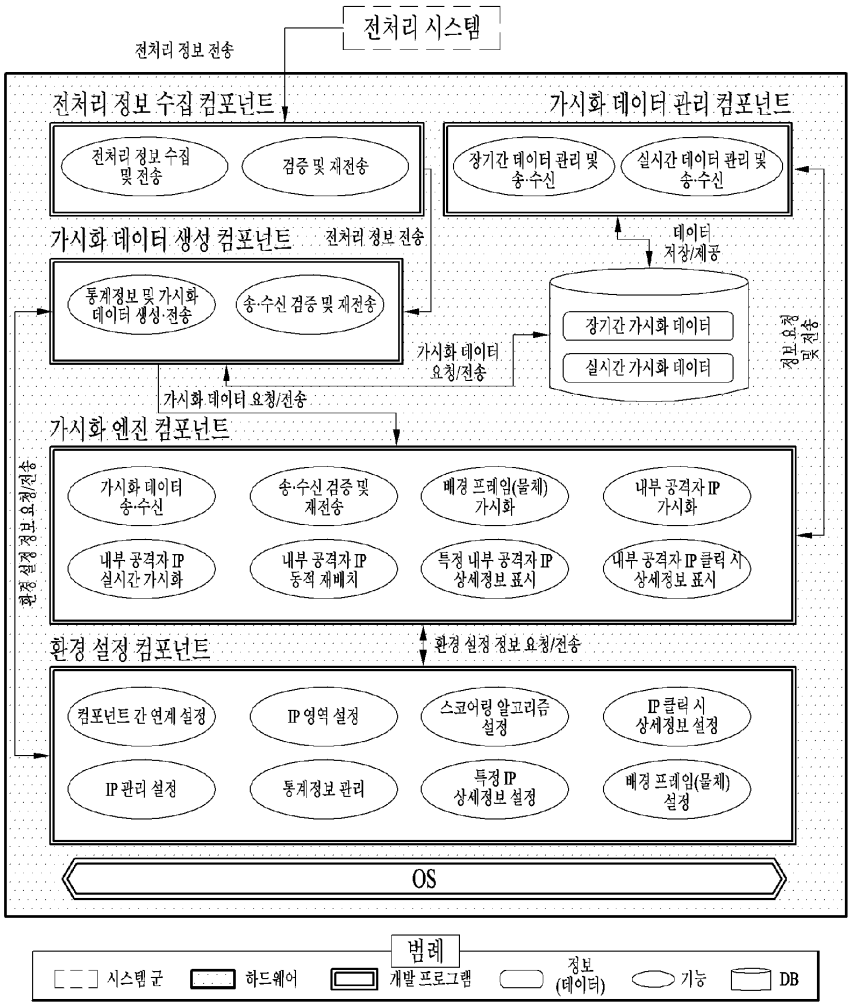
도면14


보안이벤트 저장 스토리지
보안이벤트
보안이벤트 요청
보안이벤트 전송
내외부 가시화 시스템
전처리 모듈
통계정보 생성/관리 모듈
가시화 모듈
통계정보 저장
통계정보 요청/전송
통계 정보

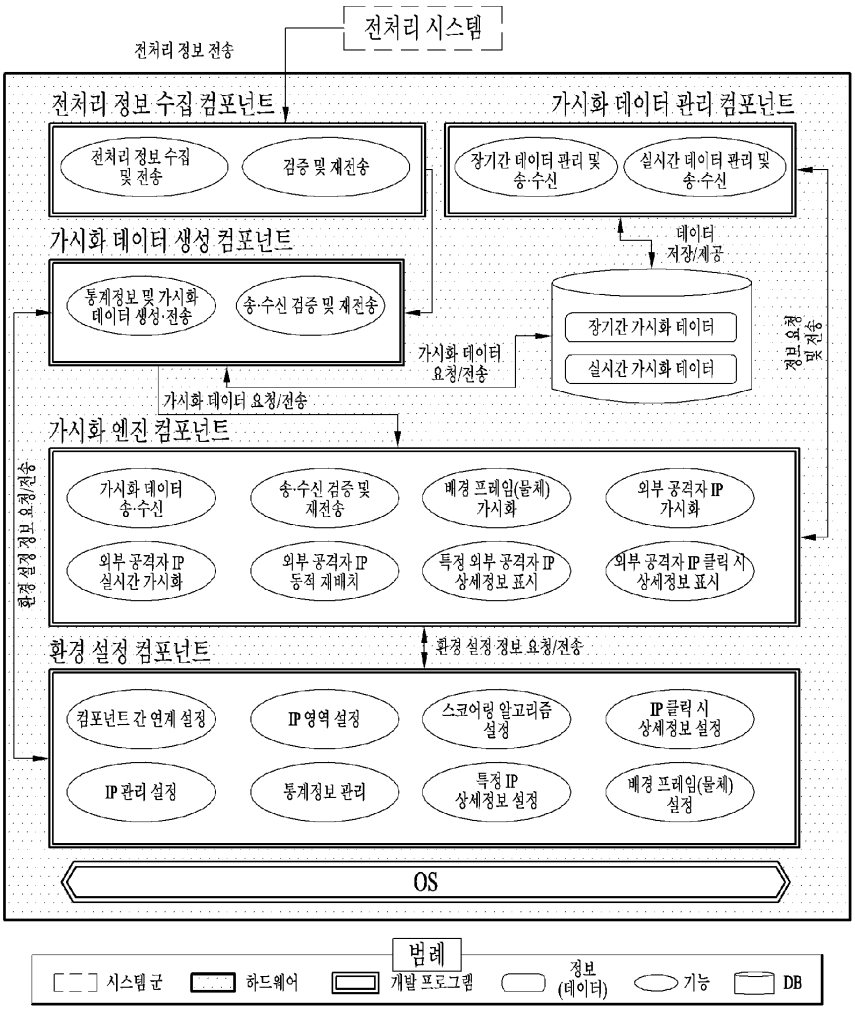
도면15


침해위협관리 시스템
보안 이벤트
보안이벤트 수집 컴포넌트
보안이벤트 요청 및 수집
보안이벤트
내부 공격자 IP 추출 컴포넌트
내부 보안이벤트 선별
대상기관(내부) IP 추출
대상기관 정보 입출력 GUI 컴포넌트
대상기관 정보 입력 GUI
파일을 통한 대상기관정보 입력
외부 공격자 IP 추출 컴포넌트
외부 보안이벤트 선별
非대상기관(외부) IP 추출
대상기관 정보 설정 컴포넌트
대상기관 정보 설정
대상기관 정보
OS
범례
시스템군
하드웨어
개발 프로그램
정보 (데이터)
기능
DB

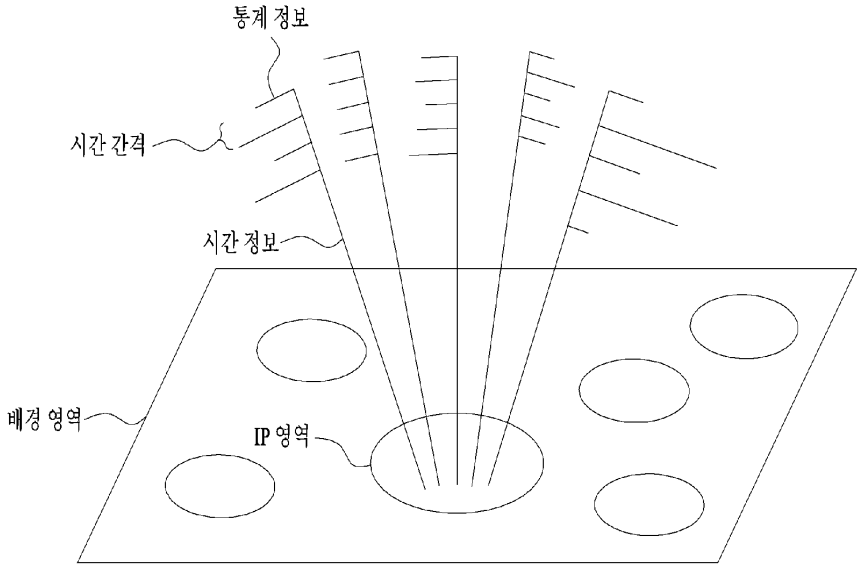
도면16


전처리 시스템
전처리 정보 전송
전처리 정보 수집 컴포넌트
전처리 정보 수집 및 전송
검증 및 재전송
가시화 데이터 관리 컴포넌트
장기간 데이터 관리 및 송·수신
실시간 데이터 관리 및 송·수신
데이터 저장/제공
가시화 데이터 생성 컴포넌트
전처리 정보 전송
통계정보 및 가시화 데이터 생성·전송
송·수신 검증 및 재전송
장기간 가시화 데이터
실시간 가시화 데이터
정보 요청 및 전송
가시화 데이터 요청/전송
가시화 데이터 요청/전송
가시화 엔진 컴포넌트
가시화 데이터 송·수신
송·수신 검증 및 재전송
배경 프레임(물체) 가시화
내부 공격자 IP 가시화
내부 공격자 IP 실시간 가시화
내부 공격자 IP 동적 재배치
특정 내부 공격자 IP 상세정보 표시
내부 공격자 IP 클릭 시 상세정보 표시
환경 설정 정보 요청/전송
환경 설정 정보 요청/전송
환경 설정 컴포넌트
컴포넌트 간 연계 설정
IP 영역 설정
스코어링 알고리즘 설정
IP 클릭 시 상세정보 설정
IP 관리 설정
통계정보 관리
특정 IP 상세정보 설정
배경 프레임(물체) 설정
OS
범례
시스템 군
하드웨어
개발 프로그램
정보 (데이터)
기능
DB

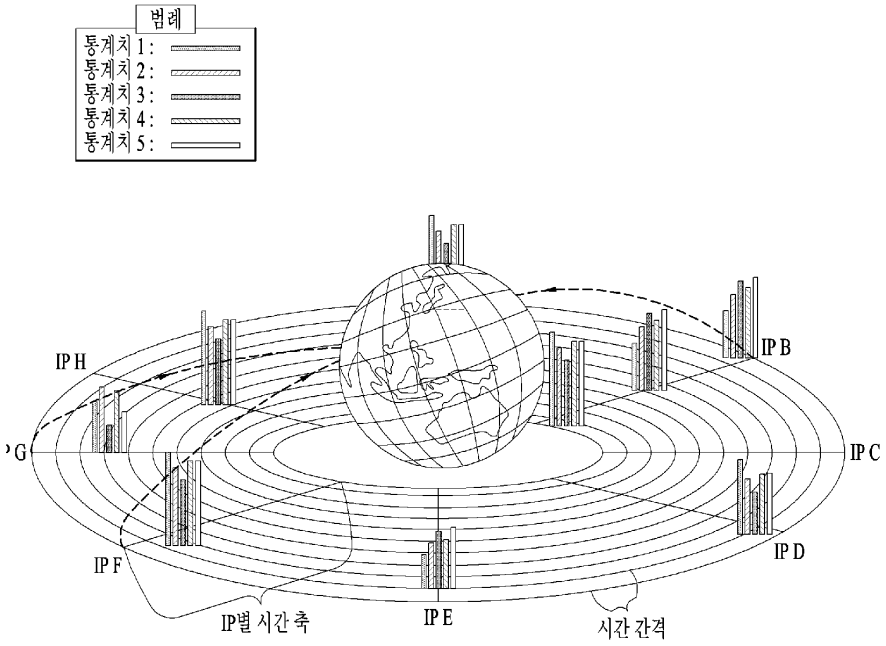
도면17


전처리 시스템
전처리 정보 전송
전처리 정보 수집 컴포넌트
전처리 정보 수집 및 전송
검증 및 재전송
가시화 데이터 관리 컴포넌트
장기간 데이터 관리 및 송·수신
실시간 데이터 관리 및 송·수신
데이터 저장/제공
가시화 데이터 생성 컴포넌트
통계정보 및 가시화 데이터 생성·전송
송·수신 검증 및 재전송
장기간 가시화 데이터
실시간 가시화 데이터
가시화 데이터 요청/전송
가시화 데이터 요청/전송
정보 요청 및 전송
가시화 엔진 컴포넌트
가시화 데이터 송·수신
송·수신 검증 및 재전송
배경 프레임(물체) 가시화
외부 공격자 IP 가시화
외부 공격자 IP 실시간 가시화
외부 공격자 IP 동적 재배치
특정 외부 공격자 IP 상세정보 표시
외부 공격자 IP 클릭 시 상세정보 표시
환경 설정 정보 요청/전송
환경 설정 정보 요청/전송
환경 설정 컴포넌트
컴포넌트 간 연계 설정
IP 영역 설정
스코어링 알고리즘 설정
IP 클릭 시 상세정보 설정
IP 관리 설정
통계정보 관리
특정 IP 상세정보 설정
배경 프레임(물체) 설정
OS
범례
시스템 군
하드웨어
개발 프로그램
정보 (데이터)
기능
DB

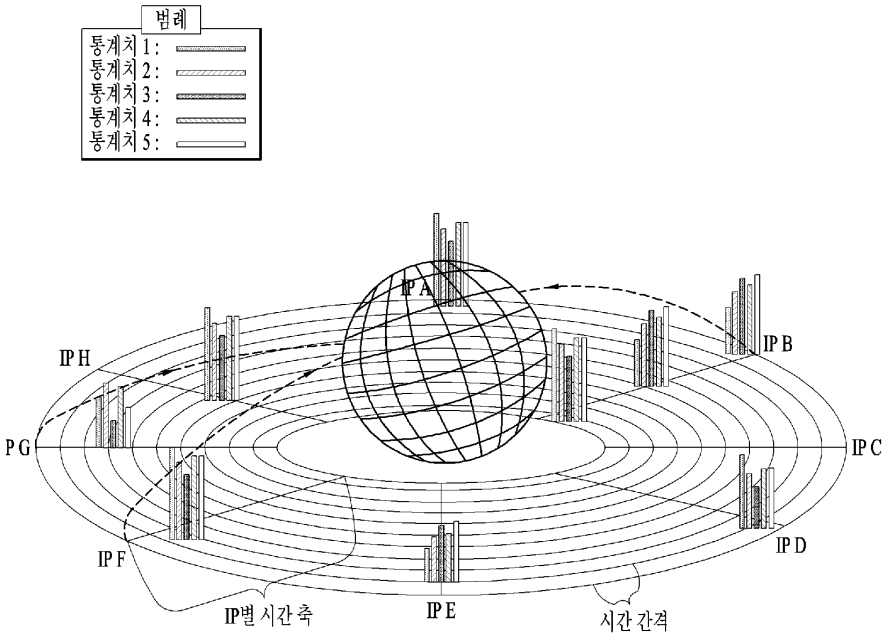
도면18


통계 정보
시간 간격
시간 정보
배경 영역
IP 영역

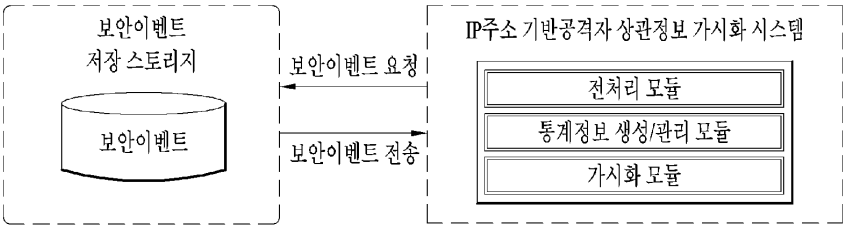
도면19


범례
통계치 1 :
통계치 2 :
통계치 3 :
통계치 4 :
통계치 5 :
IP H
IP B
PG
IP C
IP D
IP F
IP별 시간 축
IP E
시간 간격

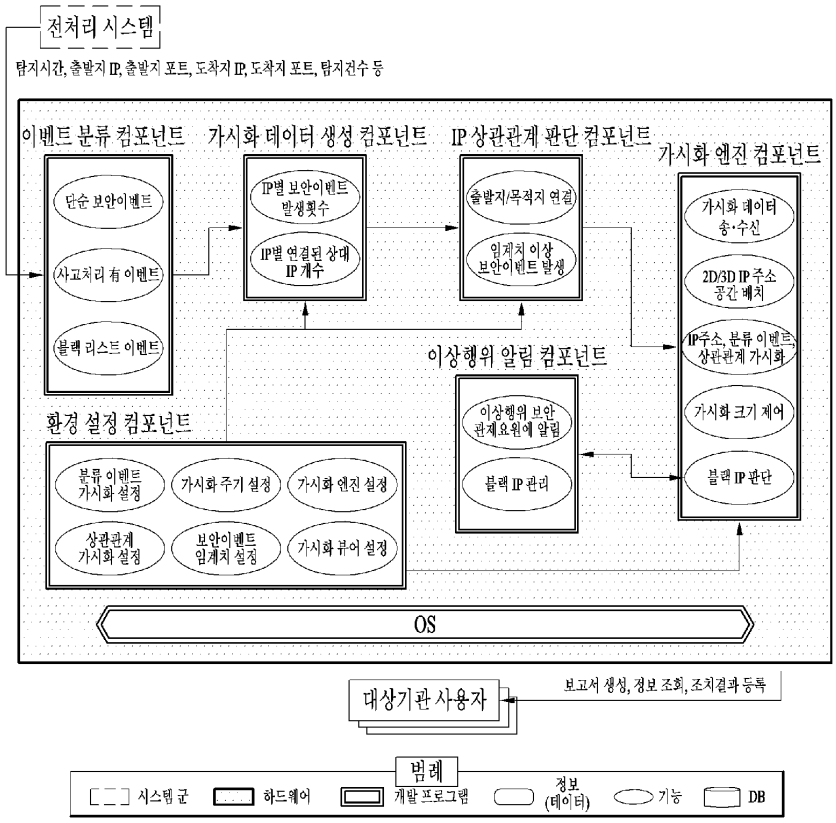
도면20


범례
통계치 1 :
통계치 2 :
통계치 3 :
통계치 4 :
통계치 5 :
IP A
IP H
IP B
PG
IP C
IP D
IP F
IP별 시간 축
IP E
시간 간격

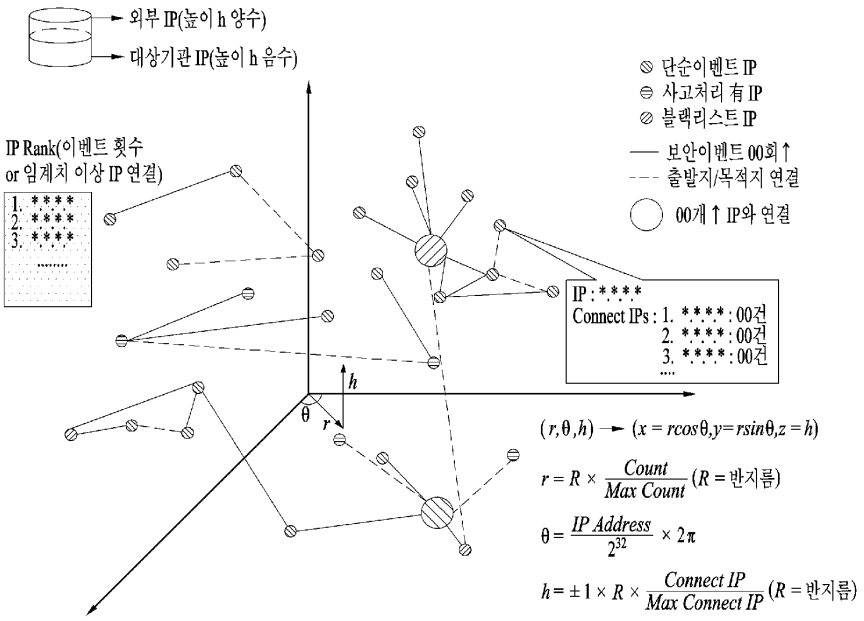
도면21


보안이벤트
저장 스토리지
보안이벤트
보안이벤트 요청
보안이벤트 전송
IP주소 기반공격자 상관정보 가시화 시스템
전처리 모듈
통계정보 생성/관리 모듈
가시화 모듈

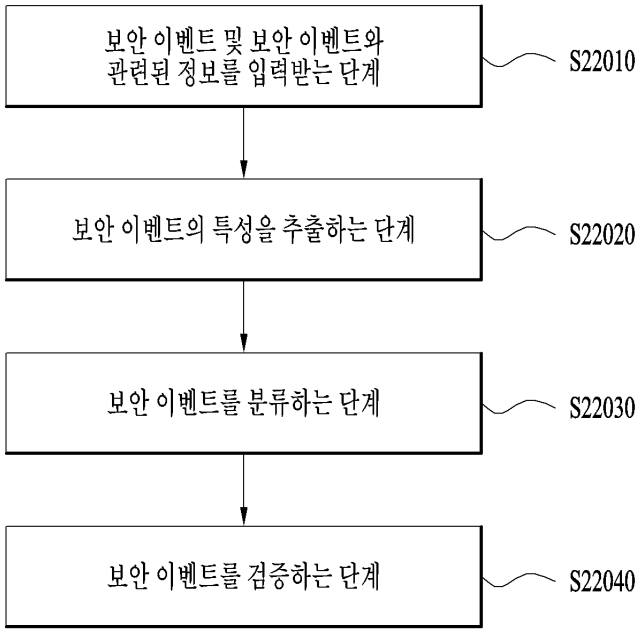
도면22


전처리 시스템
탐지시간, 출발지 IP, 출발지 포트, 도착지 IP, 도착지 포트, 탐지건수 등
이벤트 분류 컴포넌트
단순 보안이벤트
사고처리 有 이벤트
블랙 리스트 이벤트
가시화 데이터 생성 컴포넌트
IP별 보안이벤트 발생횟수
IP별 연결된 상대 IP 개수
IP 상관관계 판단 컴포넌트
출발지/목적지 연결
임계치 이상 보안이벤트 발생
가시화 엔진 컴포넌트
가시화 데이터 송·수신
2D/3D IP 주소 공간 배치
IP주소, 분류 이벤트 상관관계 가시화
가시화 크기 제어
블랙 IP 판단
이상행위 알림 컴포넌트
이상행위 보안 관제요원에 알림
블랙 IP 관리
환경 설정 컴포넌트
분류 이벤트 가시화 설정
가시화 주기 설정
가시화 엔진 설정
상관관계 가시화 설정
보안이벤트 임계치 설정
가시화 뷰어 설정
OS
대상기관 사용자
보고서 생성, 정보 조회, 조치결과 등록
범례
시스템 군
하드웨어
개발 프로그램
정보 (데이터)
기능
DB

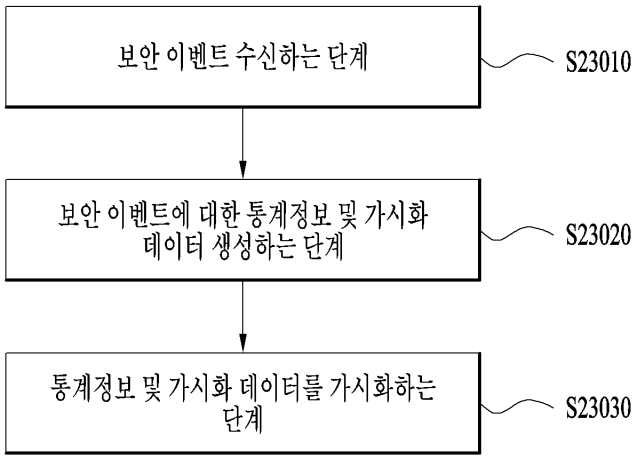
도면23


외부 IP(높이 h 양수)
대상기관 IP(높이 h 음수)
IP Rank(이벤트 횟수
or 임계치 이상 IP 연결)
1. *.*.*.*
2. *.*.*.*
3. *.*.*.*
.....
단순이벤트 IP
사고처리 有 IP
블랙리스트 IP
보안이벤트 00회↑
출발지/목적지 연결
00개↑ IP와 연결
IP : *.*.*.*
Connect IPs : 1. *.*.*.* : 00건
2. *.*.*.* : 00건
3. *.*.*.* : 00건
....
h
θ
r
$(r,\theta,h) \rightarrow (x = r\cos\theta, y = r\sin\theta, z = h)$
$r = R \times \frac{Count}{Max\ Count}$ (R = 반지름)
$\theta = \frac{IP\ Address}{2^{32}} \times 2\pi$
$h = \pm 1 \times R \times \frac{Connect\ IP}{Max\ Connect\ IP}$ (R = 반지름)

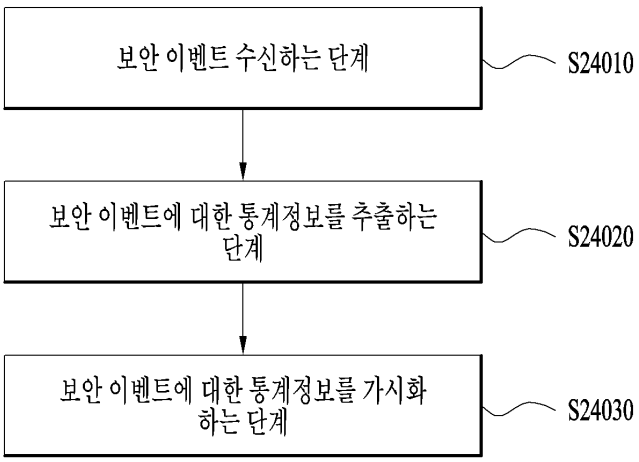
도면24


보안 이벤트 및 보안 이벤트와
관련된 정보를 입력받는 단계
S22010
보안 이벤트의 특성을 추출하는 단계
S22020
보안 이벤트를 분류하는 단계
S22030
보안 이벤트를 검증하는 단계
S22040

도면25


보안 이벤트 수신하는 단계
S23010
보안 이벤트에 대한 통계정보 및 가시화 데이터 생성하는 단계
S23020
통계정보 및 가시화 데이터를 가시화하는 단계
S23030

도면26


보안 이벤트 수신하는 단계
S24010
보안 이벤트에 대한 통계정보를 추출하는 단계
S24020
보안 이벤트에 대한 통계정보를 가시화 하는 단계
S24030