(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0061463
(43) 공개일자 2014년05월21일

(51) 국제특허분류(Int. Cl.)
*G06F 21/00* (2006.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2014-7007384
(22) 출원일자(국제) 2012년09월14일
심사청구일자 2014년03월20일
(85) 번역문제출일자 2014년03월20일
(86) 국제출원번호 PCT/US2012/055630
(87) 국제공개번호 WO 2013/040496
국제공개일자 2013년03월21일
(30) 우선권주장
13/233,497 2011년09월15일 미국(US)

(71) 출원인
**맥아피 인코퍼레이티드**
미국 95054 캘리포니아 산타클라라 미션컬리지 블러바드 2821
(72) 발명자
**부, 젱**
미국 94539 캘리포니아주 프리몬트 세인트 필립 씨티. 216
**카쉬얍, 라훌 찬데르**
미국 94404 캘리포니아주 포스터 씨티 포레스탈 레인 1116
*(뒷면에 계속)*
(74) 대리인
**백만기, 양영준, 정은진**

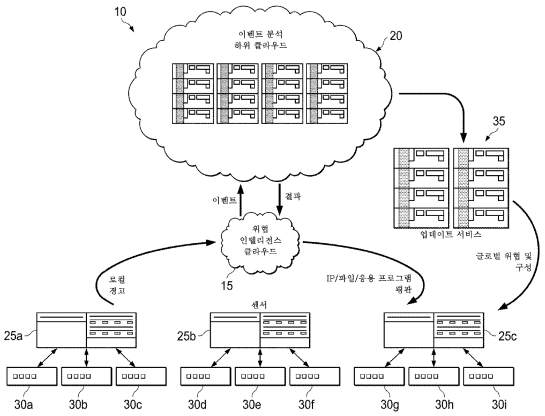
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **실시간 맞춤화된 위협 보호를 위한 시스템 및 방법**

## (57) 요 약

네트워크 환경 전반에 걸쳐 분산된 센서로부터의 리포트와 연관된 이벤트 정보를 수신하는 단계와, 위협을 식별하기 위해 이벤트 정보를 상호 연관시키는 단계를 포함하는 방법이 하나의 예시적인 실시 형태로 제공된다. 위협에 근거하여 맞춤화된 보안 정책은 센서에 전송될 수 있다.

## 대 표 도



(72) 발명자

**린, 이총**

미국 94538 캘리포니아주 프리몬트 베른 스트리트 40461

**마, 데니스 록 항**

미국 94043 캘리포니아주 마운틴 뷰 이시스 코트 183

## *특허청구의 범위*

**청구항 1**

네트워크 환경 전반에 걸쳐 분산된 센서들로부터의 리포트들과 연관된 이벤트 정보를 수신하는 단계;

위협을 식별하기 위해 상기 이벤트 정보를 상호 연관시키는 단계; 및

상기 위협에 근거하여 상기 센서들 중 적어도 하나의 센서에 맞춤화된 보안 정책(customized security policy)을 전송하는 단계

를 포함하는 방법.

**청구항 2**

제1항에 있어서, 상기 위협에 근거하여 평판 시스템에 평판 데이터를 전송하는 단계를 더 포함하는 방법.

**청구항 3**

제1항에 있어서, 상기 위협에 근거하여 위협 인텔리전스 클라우드(threat intelligence cloud)에 평판 데이터를 전송하는 단계를 더 포함하는 방법.

**청구항 4**

제1항에 있어서, 상기 센서들은 침입 방지 시스템들을 포함하는 방법.

**청구항 5**

제1항에 있어서, 상기 맞춤화된 보안 정책은 상기 위협으로 감염된 호스트를 검역하는 방법.

**청구항 6**

제1항에 있어서, 상기 이벤트 정보는 위협 인텔리전스 클라우드로부터 수신되는 방법.

**청구항 7**

제1항에 있어서, 새로운 위협에 근거하여 위협 인텔리전스 클라우드에 평판 데이터를 전송하는 단계를 더 포함하고, 상기 이벤트 정보는 위협 인텔리전스 클라우드로부터 수신되고, 상기 센서들은 침입 방지 시스템들을 포함하고, 상기 맞춤화된 보안 정책은 상기 새로운 위협에 감염된 호스트를 검역하는 방법.

**청구항 8**

실행을 위한 코드를 포함하고, 하나 이상의 프로세서에 의해 실행될 때 동작들을 수행하도록 동작가능한, 하나 이상의 비-일시적인 매체에 인코딩된 로직으로서,

상기 동작들은,

네트워크 환경 전반에 걸쳐 분산된 센서들로부터의 리포트들과 연관된 이벤트 정보를 수신하는 단계;

위협을 식별하기 위해 상기 이벤트 정보를 상호 연관시키는 단계; 및

상기 위협에 근거하여 상기 센서들 중 적어도 하나의 센서에 맞춤화된 보안 정책을 전송하는 단계

를 포함하는 로직.

**청구항 9**

제8항에 있어서, 상기 동작들은 상기 위협에 근거하여 평판 시스템에 평판 데이터를 전송하는 단계를 더 포함하는 로직.

**청구항 10**

제8항에 있어서, 상기 동작들은 상기 위협에 근거하여 위협 인텔리전스 클라우드에 평판 데이터를 전송하는 단

계를 더 포함하는 로직.

**청구항 11**

제8항에 있어서, 상기 센서들은 침입 방지 시스템들을 포함하는 로직.

**청구항 12**

제8항에 있어서, 상기 맞춤화된 보안 정책은 상기 위협으로 감염된 호스트를 검역하는 로직.

**청구항 13**

제8항에 있어서, 상기 이벤트 정보는 위협 인텔리전스 클라우드로부터 수신되는 로직.

**청구항 14**

장치로서,

상기 장치가,

네트워크 환경 전반에 걸쳐 분산된 센서들로부터의 리포트들과 연관된 이벤트 정보를 수신하고;

위협을 식별하기 위해 상기 이벤트 정보를 상호 연관시키고;

상기 위협에 근거하여 상기 센서들 중 적어도 하나의 센서에 맞춤화된 보안 정책을 전송하도록 구성되도록, 이벤트 분석 하위 클라우드와 연관된 명령어들을 실행하도록 동작가능한 하나 이상의 프로세서를 포함하는 장치.

**청구항 15**

제14항에 있어서, 상기 장치는 상기 위협에 근거하여 평판 시스템에 평판 데이터를 전송하도록 더 구성되는 장치.

**청구항 16**

제14항에 있어서, 상기 장치는 상기 위협에 근거하여 위협 인텔리전스 클라우드에 평판 데이터를 전송하도록 더 구성되는 장치.

**청구항 17**

제14항에 있어서, 상기 센서들은 침입 방지 시스템들을 포함하는 장치.

**청구항 18**

제14항에 있어서, 상기 맞춤화된 보안 정책은 상기 위협으로 감염된 호스트를 검역하는 장치.

**청구항 19**

제14항에 있어서, 상기 이벤트 정보는 위협 인텔리전스 클라우드로부터 수신되는 장치.

**청구항 20**

위협 인텔리전스 클라우드;

이벤트 분석 하위 클라우드; 및

상기 위협 인텔리전스 클라우드가 네트워크 환경 전반에 걸쳐 분산된 센서들로부터의 리포트들과 연관된 이벤트 정보를 수신하도록 구성되고;

상기 이벤트 분석 하위 클라우드가 위협을 식별하기 위해 상기 이벤트 정보를 상호 연관시키고, 상기 위협에 근거하여 상기 센서들 중 적어도 하나의 센서에 맞춤화된 보안 정책을 전송하도록 구성되도록,

상기 위협 인텔리전스 클라우드 및 상기 이벤트 분석 하위 클라우드와 연관된 명령어를 실행하도록 동작가능한 하나 이상의 프로세서

를 포함하는 장치.

# 명 세 서

## 기 술 분 야

[0001] 본 명세서는 일반적으로 네트워크 보안 분야에 관한 것이고, 보다 구체적으로는, 실시간 맞춤화된 위협 보호를 위한 시스템 및 방법에 관한 것이다.

## 배 경 기 술

[0002] 정보 시스템은 세계적인 규모로 사람과 기업의 일상 생활에 통합되어 있고, 정보 보안 분야도 마찬가지로 오늘날의 사회에서 점점 중요해지고 있다. 이러한 폭 넓은 통합은, 악의적 운영자가 이들 시스템을 악용하는 데에도 많은 기회를 제공하고 있다. 악성 소프트웨어가 호스트 컴퓨터를 감염시킬 경우, 이러한 호스트 컴퓨터로부터 스팸 또는 악성 이메일을 보내고, 호스트 컴퓨터와 연관된 기업 또는 개인으로부터 민감한 정보를 훔치며, 다른 호스트 컴퓨터에 전파하고, 및/또는 분산 서비스 거부 공격을 보조하는 등, 소정의 악성 동작을 수행할 수 있게 한다. 또한, 몇 가지 유형의 악성 코드(malware)에 대해서는, 악의적인 운영자는 다른 악의적인 운영자에게 판매하거나, 아니면 액세스를 제공할 수 있으므로, 호스트 컴퓨터의 악용을 확대시킬 수 있게 한다. 따라서, 안정적인 컴퓨터 및 시스템을 효율적으로 보호하고 유지 관리하기 위한 능력은, 부품 제조업체, 시스템 설계자 및 네트워크 운영자에 중요한 과제를 지속적으로 제시하고 있다.

## 도면의 간단한 설명

[0003] 본 발명과 그 특징 및 장점을 더 완전히 이해하기 위해서, 첨부된 도면을 참조하여, 이하의 설명에 대해 참조가 이루어지는데, 여기서 유사한 참조 번호는 유사한 부분을 나타낸다:

도 1은 본 명세서에 따른 실시간 맞춤화된 위협 보안을 위한 네트워크 환경의 예시적인 실시 형태를 도시하는 단순화된 블록도이다.

도 2는 네트워크 환경과 연관될 수 있는 잠재적인 동작의 단순화된 상호 작용 다이어그램이다.

도 3은 네트워크 환경과 연관될 수 있는 잠재적인 동작의 간략화된 흐름도이다.

## 발명을 실시하기 위한 구체적인 내용

[0004] 네트워크 환경 전반에 걸쳐 분산된 센서들로부터의 리포트와 연관된 이벤트 정보를 수신하는 단계와, 위협을 식별하기 위해 이벤트 정보를 상호 연관시키는 단계를 포함하는 방법이 하나의 예시적인 실시 형태로 제공된다. 위협에 근거하여 맞춤화된 보안 정책(customized security policy)은 센서에 전송될 수 있다. 좀 더 특별한 실시 형태에서, 이벤트 정보는 위협 인텔리전스 클라우드(threat intelligence cloud)로부터 수신될 수 있다. 또 다른 실시 형태에서, 평판 데이터는 위협에 근거하여 위협 인텔리전스 클라우드에 전송될 수도 있다.

[0005] 도 1을 참조하면, 도 1은 실시간 맞춤화된 위협 보안을 위한 시스템 및 방법이 구현될 수 있는 네트워크 환경(10)의 예시적인 실시 형태의 간략화된 블록도이다. 네트워크 환경(10)은 위협 인텔리전스 클라우드(15), 이벤트 분석 하위 클라우드(20), 센서(25a-25c) 및 호스트(30a-30i)를 포함한다. 센서(25a-25c)는, 예를 들어, 파일, 웹, 메시지 및 네트워크 위협 벡터를 포함하는, 위협 벡터에 걸쳐 호스트(30a-30i)로부터의 정보를 수집하기 위해, 네트워크 환경(10) 전반에 걸쳐 분산된 침입 방지 시스템, 게이트웨이 기기, 방화벽, 안티 바이러스 소프트웨어, 및/또는 다른 보안 시스템을 포함할 수 있다. 위협 인텔리전스 클라우드(15)는 일반적으로 센서(25a-25c)로부터 정보를 수신하고 그 정보에서 파생된 실시간 평판 기반 위협 인텔리전스를 제공하기 위한 인프라(infrastructure)를 나타낸다. 이벤트 분석 하위 클라우드는 위협 인텔리전스 클라우드(15)에 의해 수신된 정보를 분석하기 위한 인프라를 나타내며, 또한 센서(25a-25c) 및/또는 호스트(30a-30i)에 위협 정보 및 정책 구성 업데이트를 제공할 수 있는 업데이트 서비스(35)를 제공할 수도 있다.

[0006] 간단한 네트워크 인터페이스를 통해, 또는 네트워크 통신을 위한 가능한 경로를 제공하는 임의의 다른 적절한 접속(유선 또는 무선)을 통해, 도 1의 각 요소들은 서로 결합할 수 있다. 또한, 이러한 요소들 중 어느 하나 또는 그 이상은 조합되거나 특정 구성 요구에 따라 아키텍처로부터 제거될 수 있다. 네트워크 환경(10)은, 네트워크에서의 패킷의 송신 또는 수신을 위한 전송 제어 프로토콜/인터넷 프로토콜(TCP/IP) 통신이 가능한 구성을 포함할 수 있다. 네트워크 환경(10)은 또한, 적절한 경우 및 특정 필요에 따라, 사용자 데이터 그램 프로토

콜/IP (UDP/IP) 또는 임의의 다른 적절한 프로토콜과 함께 동작할 수 있다.

[0007] 도 1의 운영 및 인프라를 자세히 설명하기 전에, 특정 상황에 맞는 정보가, 네트워크 환경(10) 내에서 발생할 수 있는 몇 가지 운영의 개요를 제공하기 위해 제공된다. 이러한 정보는 진정으로 교육 목적으로만 제공되고, 따라서 본 발명의 광범위한 응용을 제한하는 방식으로 해석되어서는 안 된다.

[0008] 전형적인 네트워크 환경은, 예를 들어, 인터넷에 접속된 서버에 호스팅된 웹 페이지에 액세스하고, 전자 메일(즉, 이메일) 메시지를 전송 또는 수신하고, 또는 인터넷에 접속된 최종 사용자 또는 서버와 파일을 교환하기 위해, 인터넷을 이용하여, 다른 네트워크와 전자적으로 통신하는 기능을 포함한다. 사용자는, 일반적으로 네트워크 환경에 저장된 데이터가 용이하게 이용가능하지만, 인가되지 않은 액세스로부터 안전하기를 기대한다. 그들은 또한 일반적으로 통신이 신뢰할 수 있고 인증되지 않은 액세스로부터 안전하기를 기대한다. 그러나, 악의적인 사용자는 정상 작동을 방해하고 기밀 정보에 액세스하기 위한 새로운 전술을 지속적으로 개발하고 있다. 바이러스, 트로이 목마, 웜, 봇 및 기타 악성 코드는 네트워크 또는 시스템의 취약점을 악용하는데 사용된 비히클(vehicles)의 일반적인 예이지만, 데이터의 무단 액세스, 파괴, 노출, 변경, 및/또는 서비스의 거부를 통해 컴퓨터 또는 네트워크의 정상적인 작동을 방해하도록 설계된 임의의 활동은 "위협(threat)"이다.

[0009] 방화벽, 침입 방지 시스템, 네트워크 액세스 컨트롤 및 웹 필터링을 포함하는 광범위한 대책이 위협에 대해 전개될 수 있다. 또한, 예를 들어, 침입 탐지 및 방지 시스템(IDPS)으로도 알려진 침입 방지 시스템(IPS)은, 악의적이거나 잠재적으로 악의적인 활동에 대해 네트워크 및/또는 시스템 활동을 모니터링하여 경고를 보낼 수 있다. IPS의 경고는, 그러나, 항상 작동하지 않을 수도 있다. 대부분의 경고는, 하나의 이벤트가 적절한 정도의 신뢰를 갖고서 공격을 식별하기에는 충분하지 않을 수 있기 때문에, 관측된 이벤트가 악의적인 활동을 나타내는 경우에도, 단지 경계 정보나 지침만을 제공한다.

[0010] IPS는 일반적으로 인-라인 배치되어, 패킷을 드롭시키고, 접속을 재설정하고, 및/또는 소스로부터의 트래픽을 차단하는 등, 감지된 침입을 적극적으로 차단할 수 있다. IPS는 응용 프로그램과 프로토콜 이상, 쉘 코드 탐지 알고리즘 및 시그니처(signature)를 포함하는 다중 탐지 방법을 사용할 수 있다. 예를 들어, 시그니처 기반 탐지는 일반적으로 위협을 식별하기 위해 관측된 이벤트나 활동에 대해 시그니처(즉, 알려진 위협에 대응하는 임의의 패턴)을 비교하는 것을 포함하고 있다. 예시적 시그니처는 루트 사용자로서 원격 접속을 설정하기 위한 시도이다. 또 다른 예는 제목란과, 악성 코드의 알려진 형태의 특징인 첨부 파일을 이메일로 받는 것이다.

[0011] 시그니처 기반 탐지는 알려진 위협을 감지하기에 매우 효과적일 수 있지만, 알 수 없는 위협, 또는 알려진 위협의 약간의 변화를 감지하기에는 비효과적일 수 있다. 또한, IPS 시그니처는 보편적이나 일반적으로는 지역 환경에 맞게 사용자 정의되지는 않는 경향이 있다. 위협은 전역이 아닌, 지역적으로만 보여 질 수 있다. 전역적으로 전개된 센서로부터 수집된 지식은 일반적으로 로컬 보안 정책을 향상시키기에는 그 영향력을 끼칠 수 없다. 정책을 수동으로 조정하는 것 또한 종종 요구되는데, 이는 감염이 확산하는 것을 충분히 지연시킬 수 있다.

[0012] 본 명세서에 기재된 실시 형태에 따라, 네트워크 환경(10)은 글로벌 위협 인텔리전스와 로컬 위협 인텔리전스를 상호 관련시키는 시스템 및 방법을 제공하고, 맞춤화된 보안 정책을 제공함으로써, 이러한 단점(및 기타)을 극복할 수 있다.

[0013] 설명을 위해 도 1을 다시 참조하면, 호스트(30a-30i)는 네트워크 요소일 수 있는데, 이는 네트워크 장비, 서버, 라우터, 스위치, 게이트웨이, 브리지, 로드 밸런서(load-balancer), 방화벽, 프로세서, 모듈, 또는 네트워크 환경에서 정보를 교환하도록 동작가능한 임의의 다른 적절한 디바이스, 구성 요소, 요소, 또는 개체를 포괄하는 것을 의미한다. 네트워크 요소는 임의의 적절한 하드웨어, 소프트웨어, 구성 요소, 모듈, 인터페이스, 또는 이들의 조작을 용이하게 하는 개체를 포함할 수 있다. 이는, 데이터나 정보의 효과적인 교환을 허용하는 적절한 알고리즘 및 통신 프로토콜을 포함할 수 있게 한다. 호스트(30a-30i)는, 데스크탑 컴퓨터, 랩탑 컴퓨터, 또는 이동 통신 장치(예를 들어, 아이폰(iPhone), 아이패드(iPad), 안드로이드(Android) 장치 등) 등의 다른 유선 또는 무선 네트워크 노드를 대표할 수도 있다.

[0014] 위협 인텔리전스 클라우드(15)는 하나의 실시 형태에서의 평판 시스템인데, 이는 분산된 파일 시스템 클러스터로서 구현될 수 있다. 일반적으로, 평판 시스템은, 활동을 모니터링하고, 평판 값을 할당하거나 또는 과거의 동작을 근거로 엔터티에 점수를 매긴다. 평판 값은, 양성부터 악성까지, 스펙트럼에 대한 상이한 신뢰 수준을 표시할 수 있다. 예를 들어, 접속 평판 값(예를 들어, 최소 위험, 검증되지 않음, 높은 위험 등)은 어드레스 또는 어드레스로부터 발신되는 이메일로 만든 접속을 근거로 네트워크 어드레스에 대해 계산될 수 있다. 접속

평판 시스템은, 악의적인 활동으로 알려지거나 또는 악의적인 활동과 관련될 가능성이 있는 IP 어드레스를 갖는 이메일 또는 네트워크 접속을 거부하는데 사용될 수 있는 한편, 파일 평판 시스템은, 악의적인 활동으로 알려지거나 또는 악의적인 활동과 관련될 가능성이 있는 해시(hashes)를 갖는 파일(예를 들면, 응용 프로그램)의 활동을 차단할 수 있다. 위협 인텔리전스 클라우드(15)는, 일부가 별도의 엔터티에 의해 제어된 별도의 도메인 내에 있을 수 있는, 네트워크 전반에 걸쳐 분산된 센서(예를 들어, 센서(25a-25c))로부터의 리포트를 수신할 수 있다. 수집 모듈은 예를 들어, 센서에 요청하여, 위협 인텔리전스 클라우드(15)에 주기적으로 리포트를 전송할 수 있는데, 이는 민감한 정보를 보호하기 위해 익명으로 전송될 수 있다. 리포트는 접속의 소스 및 목적지 어드레스, 활동의 유형, 다운로드된 파일, 사용된 프로토콜 등의, 이벤트 정보를 포함할 수 있으며, 기소되거나(예를 들면, 다양한 심각성의 정도를 경고) 또는 권고(예를 들면, 그 자체로 기소될 수 없는 의심스러운 활동에 대한 정보를 제공)될 수 있다.

[0015] 이벤트 분석 하위 클라우드(20)는, 역사적으로 그리고 거의 실시간으로 이벤트를 저장하고, 처리하고, 마이닝하기 위한 클라우드 인프라를 나타낸다. 하위 클라우드(20)는 네트워크 전반에 걸쳐 분산된 센서(예를 들어, 센서(25a-25c))로부터의 정보를 상호 연관시키고 새로운 위협을 식별하기 위해 데이터-마이닝 경고에 대한 추론을 구현할 수 있다. 장단기 프로파일링 알고리즘은, 전 세계적으로 센서에 의해 감지된 널리 퍼져 있는 위협을 식별하고 응답을 자동화하기 위해 실행될 수 있다. 따라서, 하위 클라우드(20)는 실시간 경고 정보를 수집하고, 센서마다 사용자 정의될 수 있는 고급 분석 및 위협 상관 관계를 제공할 수 있는데, 이는 신속한 글로벌 위협 탐지를 용이하게 할 수 있다. 실시간 위협 정보는 위협이 발생할 때 센서로 다시 보내질 수 있다. 하위 클라우드(20)는, 위협 인텔리전스 클라우드(15)로부터의 이벤트(센서(25a-25c)로부터 이들을 경고로서 수신할 수 있음)를 검색할 수 있거나, 이들을 센서(25a-25c)로부터 직접 수신하고, 위협 인텔리전스 클라우드가 새로운 위협과 연관된 평판 데이터를 조정할 수 있게 하는 결과를 반환할 수 있다. 또한, 하위 클라우드(20)는, 원격으로 및 거의 실시간으로 센서(25a-25c) 및/또는 호스트(30a-30i)에 자동으로 업데이트 및 새로운 위협 정보를 제공할 수 있다. 그 다음, 고객은, 글로벌 위협 인텔리전스 뿐만 아니라, 하위 클라우드(20)의 처리 능력과 추론(heuristics)을 활용함으로써, 이러한 업데이트에 대해 신속하고 적극적으로 역할을 하여 자신의 시스템을 보호할 수 있다. 하위 클라우드(20)는 또한 정책 구성 제안을 가능하게 하고, 정책 또는 시그니처 세트 구성을 자동으로 조정하고, 및/또는 다른 대응 조치를 가능하게 하여, 새로운 글로벌 위협이 높은 수준의 신뢰를 갖고서(그리고 수동 구성없이) 식별되거나 차단될 수 있다.

[0016] 특정 실시 형태에서, 위협 인텔리전스 클라우드(15) 및 이벤트 분석 하위 클라우드(20)는 모두 클라우드 인프라로서 구현될 수 있다. 일반적으로 클라우드 인프라는, 최소한의 서비스 제공자의 상호 작용으로 빠르게 프로비전(및 해제)될 수 있는 컴퓨팅 자원의 공유 풀에 대해 온-디맨드(on-demand) 네트워크 액세스를 가능하게 하는 환경이다. 따라서, 계산, 소프트웨어, 데이터 액세스, 및 저장 서비스를 제공하는 시스템의 물리적 위치 및 구성의 최종 사용자에 대한 지식을 필요로 하지 않는 스토리지 서비스를 제공할 수 있다. 클라우드-컴퓨팅 인프라는 단일 액세스 포인트로 나타날 수 있는, 공유 데이터-센터를 통해 제공되는 서비스를 포함할 수 있다. 클라우드(15) 및 하위 클라우드(20) 등의 다중 클라우드 구성 요소는, 메시징 큐와 같은, 느슨한 결합 메커니즘을 통해 서로 통신할 수 있다. 따라서, 처리(및 관련 데이터)는, 특정되고, 공지된 또는 정적인 위치에 있을 필요가 없다. 클라우드(15)와 하위 클라우드(20)는, 실시간으로 기존의 기능을 확장할 수 있는 소정의 관리되고, 호스팅된 서비스를 포함할 수 있다.

[0017] 네트워크 환경(10)과 연관된 내부 구조와 관련하여, 위협 인텔리전스 클라우드(15), 이벤트 분석 하위 클라우드(20), 센서(25a-25c), 및 호스트(30a-30i)의 각각은, 여기에서 설명된 동작에 사용될 정보를 저장하기 위한 메모리 소자를 포함할 수 있다. 이들 소자는 또한, 소정의 적합한 메모리 소자(예를 들어, 랜덤 액세스 메모리(RAM), 판독 전용 메모리(ROM), 소거가능한 프로그램가능 ROM(EPROM), 전기적으로 소거가능한 프로그램가능 ROM(EEPROM), 응용 주문형 집적 회로(ASIC) 등), 소프트웨어, 하드웨어, 또는 적절한 경우 및 특정 필요에 따라, 임의의 다른 적절한 구성 요소, 디바이스, 요소, 또는 개체 내에 정보를 유지할 수 있다. 여기에서 논의된 임의의 메모리 아이템은, 광범위한 용어 "메모리 소자" 내에 포함되는 것으로 해석되어야 한다. 위협 인텔리전스 클라우드(15), 이벤트 분석 하위 클라우드(20), 센서(25a-25c), 또는 호스트(30a-30i)에 의해 추적되거나 전송되는 정보는, 임의의 데이터베이스, 레지스터, 테이블, 큐(queue), 제어 목록, 또는 스토리지 구조 내에 제공될 수 있는데, 이들 모두는 소정의 적절한 시간 프레임에 참조될 수 있다. 이러한 임의의 저장 옵션은 또한, 여기에서 사용된 광범위한 용어 "메모리 소자" 내에 포함될 수 있다.

[0018] 또한, 위협 인텔리전스 클라우드(15), 이벤트 분석 하위 클라우드(20), 센서(25a-25c) 및 호스트(30a-30i)는, 여기에서 논의된 활동을 수행하기 위해 소프트웨어 또는 알고리즘을 실행할 수 있는 다수의 프로세서를 포함할

수 있다. 프로세서는 여기에서 설명된 동작을 달성하기 위해 메모리 소자와 연관된 임의의 유형의 명령어를 실행할 수 있다. 하나의 예에서, 프로세서는 요소 또는 아티클(예를 들어, 데이터)를 하나의 상태 또는 일로부터 다른 상태 또는 일로 변환할 수 있다.

[0019] 특정한 예시적 구현에 있어서는, 여기에서 설명된 기능은, 비-일시적인 매체를 포함할 수 있는 하나 이상의 유형의(tangible) 매체 내에 인코딩된 로직(예를 들어, 프로세서, 또는 다른 유사 기기 등에 의해 실행될, ASIC 내에 제공된 임베디드 로직, 디지털 신호 프로세서(DSP) 명령어, 소프트웨어(개체 코드 및 소스 코드를 잠재적으로 포함))에 의해 구현될 수 있다는 점에 유의해야 한다. 이러한 경우의 일부에서, 메모리 소자는 여기에서 설명된 동작에 사용된 데이터를 저장할 수 있다. 이는 여기에서 설명된 활동을 수행하기 위해 실행되는 소프트웨어, 로직, 코드, 또는 프로세서 명령어를 저장할 수 있는 메모리 소자를 포함한다. 다른 예에서, 여기에서 설명된 활동은 고정된 로직 또는 프로그램 가능한 로직(예를 들어, 프로세서에 의해 실행된 소프트웨어/컴퓨터 명령어)으로 구현될 수 있으며, 여기에서 식별된 요소는 프로그램가능 프로세서, 프로그램가능 디지털 로직(예를 들면, 필드 프로그램가능 게이트 어레이(FPGA), EPROM, EEPROM), 또는 디지털 로직, 소프트웨어, 코드, 전자 명령어 또는 이들의 임의의 적절한 조합을 포함하는 ASIC 중의 일부 유형일 수 있다. 여기에서 설명된 임의의 잠재적인 처리 요소, 모듈 및 머신은 광범위한 용어 "프로세서" 내에 포함되는 것으로 해석되어야 한다.

[0020] 도 2는 하위 클라우드(20)가 IPS 센서로부터의 이벤트를 분석하는데 전용되는 네트워크 환경(10)의 예시적인 실시 형태들과 연관될 수 있는 잠재적인 동작의 단순화된 상호 작용 다이어그램이다. (200)에서, IPS 센서(예를 들어, 센서(25a))는 내장된 JAVASCRIPT 태그를 갖는 PDF 문서를 다운로드하는 호스트(30b)와 같이, 위협을 나타내는 활동을 관측할 수 있다. (205)에서, 로컬 IPS는 위협을 차단 및/또는 로컬 경고를 보낼 수 있다. (210)에서, 이벤트는 위협 인텔리전스 클라우드(15)에 보고될 수도 있다. (215)에서, 위협 인텔리전스 클라우드(15)는, 이벤트가 하위 클라우드(20) 내의 이벤트 분석에 관련되는지(예를 들어, 리포트가 IPS로부터 수신됨)를 판정할 수 있다. 이벤트가 하위 클라우드(20) 내의 분석에 관련된 경우, 위협 인텔리전스 클라우드(15)는 (220)에서 하위 클라우드(20)에 이벤트 정보를 보낼 수 있다. (225)에서, 다양한 분석 추론(예를 들면, 시간, 위치 정보, 평판 등에 근거)을 사용하여, 하위 클라우드(20)는 상기 이벤트를, 네트워크 환경(10) 전반에 걸쳐 분산된 다른 센서로부터 보고된 이벤트(또는, 대역외 트래픽에서의 예기치 않은 증가와 같은, 동일 센서로부터의 후속 이벤트)와 상호 연관시켜, 글로벌 위협을 식별할 수 있다.

[0021] 예를 들면, 낮은 심각성 경고는 JAVASCRIPT 태그를 갖는 PDF(Portable Document Format) 파일을 다운로드하기 위해 설정될 수 있다. 로컬 정책은, 낮은 심각성 경고이기 때문에 그러한 이벤트를 무시할 수 있다. 그러나, 이러한 PDF의 평판과 소스는, 네트워크를 통해 다중 센서로부터 수신된 리포트에 기초하여 결정될 수 있다. 분산된 센서로부터 보고된 이벤트를 데이터 마이닝함으로써, PDF 문서는 특정 국가, 지역 또는 산업에서 센서에 의해 보고된 이벤트를 상호 연관시킴으로써, 특정 국가, 지역 또는 산업을 대상으로 하는 위협으로 식별될 수 있다. 나쁜 평판을 가진 의심스러운 어드레스로부터 이러한 PDF 파일을 다운로드한 호스트 또한 식별될 수 있다. 그 다음, 제안, 지침 및 정책 변경 추천이 제공될 수 있다.

[0022] (230)에서, 하위 클라우드(20)는 글로벌 위협 정보를 생성할 수 있고, 네트워크 환경(10) 내의 또는 네트워크 환경(10)의 특정 세그먼트(예를 들면, 특정 국가와 관련된) 내의 모든 IPS를 알려줄 뿐만 아니라, 맞춤화된 보안 정책/구성 제안을 위협 상관 관계에 기반한 것에 제공할 수 있다. 맞춤화된 보안 정책은 관리자로부터의 개입 없이, 네트워크 환경(10)을 보호하기 위해 세부적인 대응 조치를 포함할 수 있다. 예를 들어, 업데이트 서비스(35)는 어드레스에 의해 감염된 호스트(예를 들면, 호스트(30b))를 식별하고, 데이터 손실(있는 경우)의 유형을 식별하고, 감염된 호스트를 검역하는 센서(25a)에는 맞춤화된 보안 정책을 제공할 수도 있고, 차단되어야 할 특정 어드레스를 식별할 수 있다. (235)에서, 하위 클라우드(20)는 다른 평판 데이터를 증가시키기 위해 위협 인텔리전스 클라우드(15)에 결과를 제공할 수도 있다.

[0023] 도 3은 네트워크 환경(10)의 특정 실시 형태와 연관될 수 있는 잠재적인 동작을 나타내는 간략화된 흐름도(300)이다. 특정 실시 형태에서, 이러한 동작은 예를 들어, 이벤트 분석 하위 클라우드(20)에 의해 실행될 수 있다. (305)에서, 이벤트 정보가 수신될 수 있다. 이벤트 정보는, 예를 들어, 위협 인텔리전스 클라우드(15)로부터 푸시 또는 풀될 수 있다. 일부 실시 형태에서, 이벤트 정보는 네트워크 환경(예를 들어, 네트워크 환경(10))을 통해 분산된 센서들에 의해 보고될 수 있다. (310)에서, 이벤트 정보는 상호 연관될 수 있다. (315)에서, 상관 관계가 위협을 드러내면, (320)에서, 맞춤화된 보안 정책은 센서들 중 적어도 하나에 전송될 수 있다. 맞춤화된 보안 정책은, (315)에서 식별된 위협에 부분적으로 또는 전체적으로 근거할 수 있다. 평판 데이터((315)에서 감지된 위협에 부분적으로 또는 전체적으로 근거할 수도 있음)는, (320)에서 전송될 수 있다. 예를 들어, 이벤트 정보의 상관 관계는 특정 네트워크 어드레스와 연관된 위협을 식별할 수 있고, 하위 클라우드

(20)는 네트워크 어드레스의 평판의 업데이트를 위협 인텔리전스 클라우드(15)에 보낼 수 있다.

[0024] 따라서, 네트워크 환경(10)은 일부 이미 설명된, 상당한 이점을 제공할 수 있다. 특히, 로컬 보안 대책은 로컬 네트워크의 요구에 따라 위협에 대한 보호를 제공하기 위해 로컬 조정 정책을 사용할 수 있고, 네트워크 환경(10)은 하나의 글로벌 위협 인텔리전스 네트워크 내에 각각의 로컬 센서(즉, 센서(25a-25c))를 접속할 수 있다. 네트워크 환경(10)에서, 로컬 보안 대책은 더 이상 최신 위협에 단순히 반응하지 않는다. 새로운 위협에 대한 인텔리전스는, 네트워크를 사전 보호 조치할 수 있도록 관리 시스템에 자동으로 푸시될 수 있다. 또한, 네트워크 환경(10)은 사전 조정을 위한 클라우드 기반의 인프라를 활용하여, 보안 대책에 대한 총 소유 비용을 상당히 줄일 수 있다.

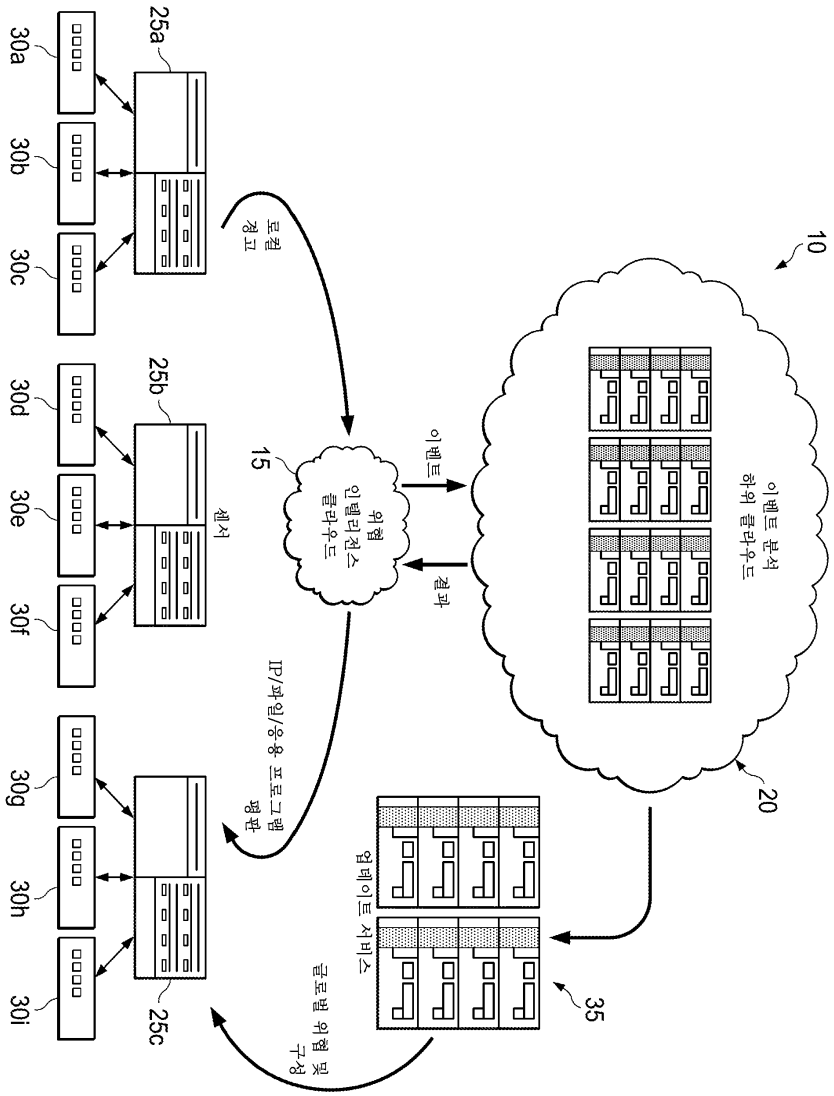
[0025] 상기 제공된 예를 이용하여, 상호 작용이 2개, 3개 또는 4개의 네트워크 요소의 관점에서 설명될 수도 있다는 것에 유의한다. 그러나, 이는 단지 명확성 및 예시적 목적으로만 행해졌다. 특정 경우에는, 제한된 수의 네트워크 요소를 참조하는 것만으로도, 주어진 세트의 플로우의 하나 이상의 기능을 설명하는 것이 더 쉬울 수 있다. 네트워크 환경(10)(및 그의 교시)이 용이하게 확장 가능하고 많은 수의 구성 요소뿐만 아니라, 더 복잡한/정교한 배치 및 구성을 수용할 수 있다는 것을 이해하여야 한다. 또한, IPS의 특정 문맥에 있어서는, 여기에서 설명한 원리가 게이트웨이, 방화벽 등의 다른 유형의 네트워크 요소로, 또는 안티바이러스 시스템 등의 호스트 시스템으로 용이하게 확장될 수 있다는 것을 이해하여야 한다. 따라서, 제공된 예들은 상기 범위를 제한하거나, 또는 많은 다른 아키텍처에 잠재적으로 적용된 네트워크 환경(10)의 광범위한 교시를 저해해서는 안 된다. 또한, 동작이 소정의 네트워크 요소와 연관될 수 있는 특정 시나리오를 참조하여 설명되었지만, 이러한 동작은 외부에서 구현될 수 있고, 또는 임의의 적절한 방식으로 통합 및/또는 조합될 수 있다. 어떤 경우에는, 특정 요소는 단일의 전용 모듈, 디바이스, 유닛 등의 형태로 제공될 수 있다.

[0026] 그러나, 첨부된 도면의 단계들이, 네트워크 환경(10)에 의해, 또는 그 내부에서 실행될 수 있는 가능한 시그널링 시나리오 및 패턴의 일부만을 예시한다는 점을 주의해야 하는 것도 중요하다. 이들 단계 중 일부는 적절한 경우에 삭제되거나 제거될 수 있고, 이들 단계는 여기에서 제공된 교시의 범위를 벗어나지 않는 한도에서 상당히 수정되거나 변경될 수 있다. 또한, 이러한 많은 동작들은 하나 이상의 추가 동작과 함께 또는 병렬로 동시에 실행되는 것으로 설명되었다. 그러나, 이들 동작의 타이밍은 상당히 변경될 수 있다. 선행 동작의 흐름은 예시와 토론의 목적을 위해 제공하였다. 임의의 적합한 배열, 연대, 구성 및 타이밍 메커니즘이 여기에서 제공된 교시를 벗어나지 않고 제공될 수 있다는 점에서, 네트워크 환경(10)에 의해 상당한 유연성이 제공된다.

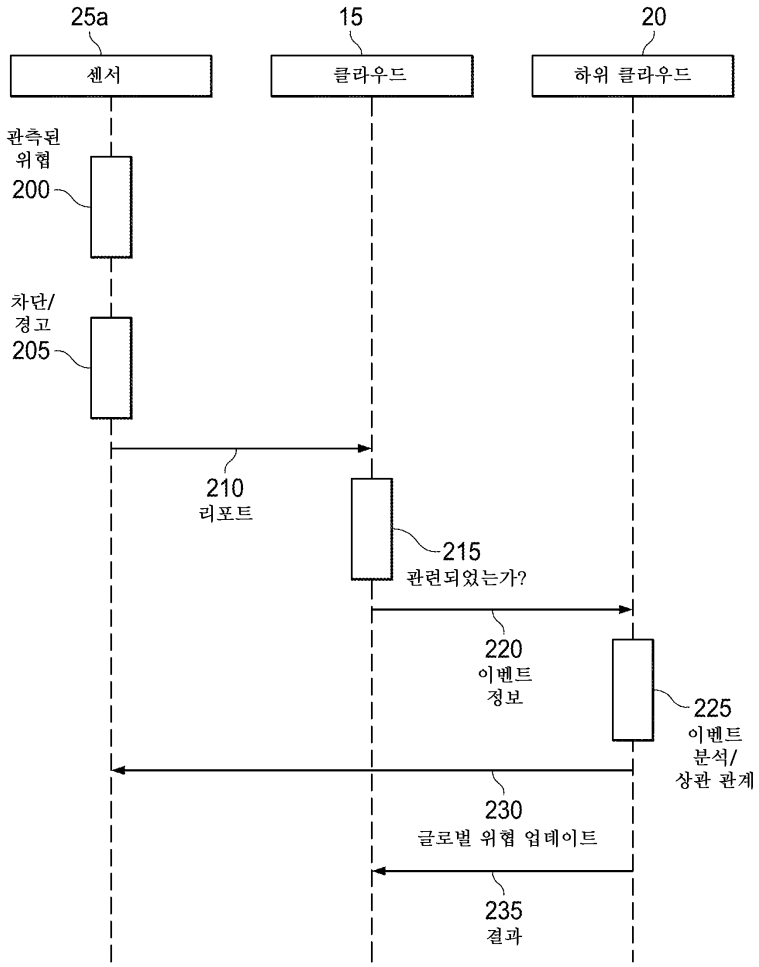
[0027] 많은 다른 변화, 대체, 변동, 변경, 및 변형은 당업자에게 확인될 수 있으며, 이는 본 발명이 첨부된 청구범위 내에 있는 한, 그러한 모든 변경, 대체, 변동, 변경 및 변형을 포함하도록 의도된다. 미국 특허 및 상표 사무소(USPTO), 및 추가로, 첨부된 청구항을 해석할 시에 이 출원에 대해 허여된 특허의 독자를 지원하기 위해서, 출원인은, (a) 소정의 첨부된 특허 청구 범위가, 단어 "수단" 또는 "단계"가 특정 특허 청구 범위에 특별하게 사용되지 않는 한, 이는 본 출원의 출원 일자에 존재하는 때문에, 35 U.S.C. 섹션 112의 단락 6을 근거로 하는 것을 의도하지 않고; (b) 명세서의 진술서에 의해, 첨부된 청구 범위에 달리 반영되지 않은 소정의 방식으로 본 발명을 제한하는 것을 의도하지 않는다는 것을 주지하기를 원한다.

## 도면

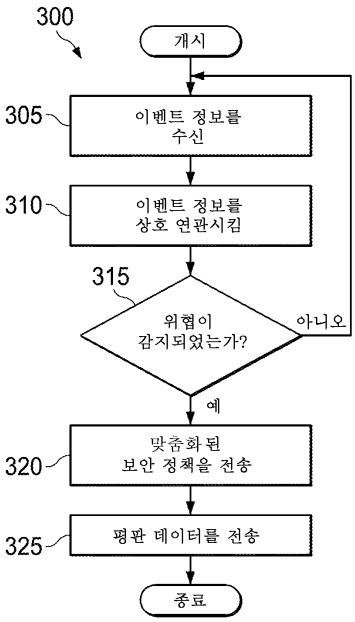
### 도면1


30a
30b
30c
25a
로컬 정보
30d
30e
30f
25b
센서
15
위협 인텔리전스 클라우드
이벤트
결과
10
이벤트 분석 하위 클라우드
20
IP/파일/응용 프로그램 평판
30g
30h
30i
25c
업데이트 서비스
35
글로벌 위협 및 구성

도면2


25a
15
20
센서
클라우드
하위 클라우드
관측된
위협
200
차단/
경고
205
210
리포트
215
관련되었는가?
220
이벤트
정보
225
이벤트
분석/
상관 관계
230
글로벌 위협 업데이트
235
결과

도면3


300
개시
305
이벤트 정보를
수신
310
이벤트 정보를
상호 연관시킴
315
위협이
감지되었는가?
아니오
예
320
맞춤화된
보안 정책을 전송
325
평판 데이터를 전송
종료