05

초연결네트워크

사이버공격 실시간 추적 가시화 시스템

- 특허명 : 공격자 가시화 방법 및 장치 (10-2017-0115074)
- 보유기관 : 한국과학기술정보연구원
- 상태정보 : 출원 `17.09.08 → 공개 `19.03.18 → 등록 `19.06.17
- 기타정보 : 관련특허 포트폴리오 구축(총 4건)

특허원문보기

기술개요

· 보안이벤트를 발생시킨 IP 주소에 대한 공격행위를 실시간 및 장기적 관점에서 가시화하는 방법에 관한 기술임

· 네트워크 보안 솔루션 개발사, 보안관제센터 및 전문업체, 인터넷서비스 사업자 등 통신사, 은행, 증권사 등 금융기관

기존 문제점

· 기존의 보안이벤트 가시화 기술들은 보안이벤트에 포함된 기본정보(IP 주소, 포트, 프로토콜, 보안이벤트 명 등)만을 이용하여 보안이벤트를 가시화함

기술 차별점

· 보안이벤트를 발생시킨 IP 주소에 대한 공격행위를 다양한 통계정보로 추출하고, 실시간 및 장기적 관점에서 가시화하는 방법을 이용

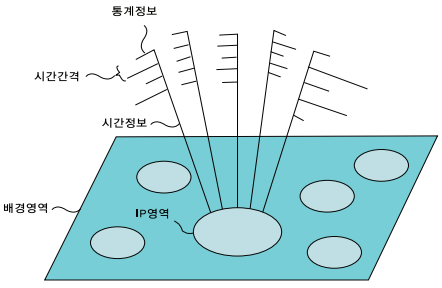
세부내용

· IDS/IPS 등 탐지규칙 기반 보안장비가 탐지한 보안이벤트의 모든 IP 주소에 대한 이상행위를 가시화하는 방법

· 이상행위에 대한 실시간 및 통계적 가시화를 통해 모든 IP의 실제 공격 여부를 직관적으로 탐지 분석하는 방법

· IDS/IPS등의 탐지규칙 기반 보안장비가 탐지한 대용량 보안이벤트의 모든 IP주소간 상관관계를 가시화하는 방법

· 장기간 동안 보안이벤트를 발생시킨 모든 IP주소 간 상관관계를 장기적 및 대규모 관점에서 가시화함으로써 공격그룹 및 공격체계를 유추 및 탐지하는 방법



기술이전 문의

· 한국과학기술정보연구원 윤신혜 (042-869-1832, shyoon@kisti.re.kr)

· 공동마케팅사무국 이가영(042-862-6985, gylee@wips.co.kr)