Symantec Security Analytics

지능형 보안 위협을 탐지하고 파악하여 신속하게 대응

오늘날의 최신 지능형 악성 코드와 제로데이 공격은 기존 보안 기술의 감시망을 피해 활동하고 있습니다. 이에 따라 기업은 네트워크의 모든 지점에서 데이터 유출이 발생할 수 있다는 사실을 인정해야 합니다. 그 결과 보다 효율적인 전략, 즉 지능형 보안 위협과 표적 공격을 탐지하여 파악 및 대응하고 이를 차단할 수 있도록 네트워크를 강화하는 데 필요한 인텔리전스 및 실시간 분석 기능을 제공하는 통합적인 접근 방식이 확산되고 있습니다. Symantec Security Analytics는 보안 가시성, 보안 분석, 실시간 인텔리전스를 통합하여 즉각적인 탐지 및 효과적인 침해 사고 대응을 지원하면서 빈틈 없이 완벽한 보안을 실현합니다. 또한 지능형 네트워크 포렌식 분석 및 신속한 침해 사고 대응을 지원하고 보안 팀이 신종 보안 위협에 대한 두려움과 우려를 극복하고 비즈니스에 필요한 새로운 가능성을 발굴할 수 있도록 지원합니다.

진화하는 보안 위협 환경에 적응

보안 공격의 횟수, 다양성, 출처가 모두 증가하고 있습니다. 매일 수천 개의 신종 악성 코드 샘플이 등장하고, 외부 소스를 비롯하여 내부 직원들로 인해 발생하는 지능형 제로데이 보안 위협, 정교한 악성 코드, 표적 공격과 그 규모 역시 계속해서 증가하는 추세입니다.

기존의 차단 전략으로는 이러한 지능형 공격에 올바르게 대처할 수 없습니다. 보안 환경이 계속 진화함에 따라 보안 팀과 침해 사고 대응 팀에게 적응력을 갖춘 맞춤형 솔루션이 필요합니다. 즉 기존 시그니처 기반 툴의 허점을 극복하는 동시에 빠르게 증가하는 방대한 규모의 모든 네트워크 트래픽을 철저히 모니터링할 수 있는 솔루션입니다. 또한 보안 프레임워크의 틈새가 커지는 것을 효율적으로 해결하기 위해서는 간단하고 유연하며 비용 효율적인 보안 솔루션도 필요합니다.

시만텍 침해 사고 대응(Symantec Incident Response) 솔루션의 핵심 요소인 Security Analytics는 완벽한 보안을 실현하면서 알려지지 않은 위험에 대비하고 현재 진행 중인 공격으로부터 보호하기 위해 아래와 같은 주요 과제를 해결합니다.

- 복잡한 에코시스템, 프로세스, 워크플로우 수용
- 가장 통합적인 실시간 보안 위협 인텔리전스 소스를 활용하여 공격 전후 및 공격 진행 단계의 모든 활동을 빠짐없이 기록
- 조직의 성장, 중앙 보안 관리의 필요성, 늘어나는 네트워크 성능 요구 사항 충족을 위해 확장

명확한 인텔리전스 즉시 이용

보안 전문가는 Symantec Security Analytics를 통해 보안 사고 이후에 반드시 해야 할 보안 질문, 이를테면 누가 어떻게 언제 침투했으며 무엇에 액세스했는지 간단명료하게 답할 수 있습니다. 업계 최고의 이 플랫폼은 고객이 소유한 업계 표준 하드웨어에서 사전 구성된 어플라이언스 형태 또는 가상 어플라이언스 형태로 구축하여 레이어 2부터 레이어 7까지 모든 네트워크 트래픽 패킷을 기록하고 분류할 뿐 아니라 데이터를 인덱싱, 분류, 강화, 저장하여 모든 보안 이벤트를 꼼꼼히 확인하는 통합 보안 위협 인텔리전스 및 사후 분석 기능을 제공합니다.

4백만 달러
데이터 유출 사고 평균 총 비용

158달러
유출된 기록당 평균 비용

48%
데이터 유출 사고 중 악성 공격의 비율

출처: Ponemon Institute, 2016년

그 결과, 실용성 있는 증거를 확보하여 침해 사고 대응 및 포렌식 분석 속도를 높이고 실시간으로 상황을 파악하며 지속적인 모니터링, IT 거버넌스, 리스크 관리 및 컴플라이언스, 보안 보증을 실현합니다.

주요 기능 및 혜택

Security Analytics는 유연하고 비용 효율적이며 잘 알려진 여러 보안 위협 인텔리전스 소스 및 차세대 샌드박싱 기술과의 통합을 통해 통합적인 실시간 모니터링 및 소급적 포렌식 분석을 지원하는 유일한 솔루션입니다. 이 솔루션은 아래와 같은 기능을 제공합니다.

애플리케이션 분류

Security Analytics는 은밀하게 네트워크에 침투하려는 모든 애플리케이션의 실체를 밝힙니다. 통합 심층 패킷 검사(Deep Packet Inspection, DPI)는 2,500여 개의 애플리케이션과 수천 개의 기술적 메타데이터 세부 정보를 분류합니다. 이 기능은 애플리케이션을 효율적으로 식별할 뿐 아니라 네트워크 세션에 대한 기술적 정보, 즉 애플리케이션, 사용자 페르소나, 의도한 행동, 컨텐트 유형, 파일 이름 등을 제공합니다.

Symantec

실시간 보안 위협 인텔리전스

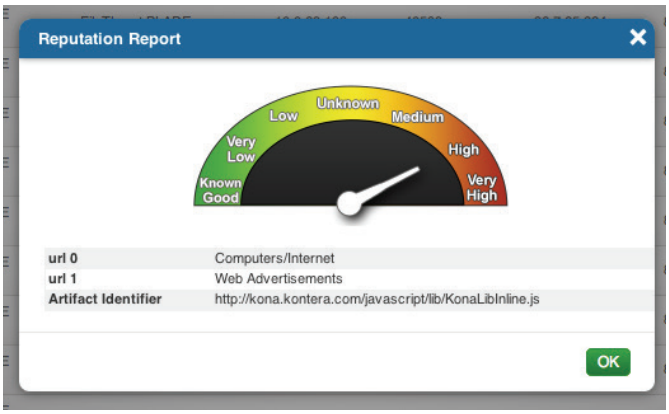
이 플랫폼은 Symantec Intelligence Services와의 직접 통합을 지원하면서 진정한 보안 혁신을 주도합니다. Symantec Intelligence Services는 Symantec Global Intelligence Network를 기반으로 15,000여 고객사와 수백만 사용자의 "네트워크 효과"를 활용하면서 웹, 이메일 또는 파일 기반 보안 위협에 대해 즉각적이고 실용적인 인텔리전스를 제공합니다. 또한 Security Analytics는 실시간 파일 추출 기능을 통해 자동으로 파일을 추출하고 검사하여 알려진 보안 위협을 자동으로 즉시 식별하고, 알려진 보안 위협이 불필요하게 탐지되지 않도록 악성 코드 샌드박싱을 최적화합니다.

레이어 2 ~ 레이어 7 보안 분석

Security Analytics는 다양한 첨단 분석 기능을 제공하며 이를 통해 통합적이고 결정적인 분석을 연계하면서 효과적으로 보안 침해 사고에 대응할 수 있도록 지원합니다. 전체 세션 재구성, 실시간 평판 조회, 인스턴트 메시징(IM), 이메일 및 이미지 재구성, 근본 원인 탐색, 패킷뿐 아니라 전체 아티팩트 전송 등 여러 핵심 기능을 갖추었습니다.

컨텍스트 인식 보안

이 솔루션을 최고의 네트워크 및 엔드포인트 보안 기술과 통합하면 원하는 알림 또는 로그에서 곧바로 전환하여 알림 전후 및 알림 단계에서 이벤트의 전체 페이로드 세부 정보를 수집할 수 있습니다. 개방형 웹 서비스 REST API를 통해 원하는 보안 툴에 전체 컨텍스트를 추가할 수 있으며 Carbon Black, Cisco, Countertack, Dell SonicWALL, FireEye, Guidance Software, HP ArcSight, Sourcefire, Splunk, Tripwire, 기타 여러 보안 애플리케이션의 대표적인 기술을 활용할 수 있습니다.



실시간 보안 위협 분석

완벽한 보안 가시성

Security Analytics와 Symantec SSL Visibility 솔루션의 강력한 통합을 통해 수천 개의 애플리케이션, 수십 개의 파일 전송, 모든 플로우 및 패킷(암호화된 트래픽 포함)에 대한 인사이트를 확보할 수 있습니다.

Root Cause Explorer

Root Cause Explorer는 침해 사고 대응을 간소화합니다. 추출된 네트워크 개체를 사용하여 의심스러운 웹 세션, 이메일, 채팅 대화의 타임라인을 재구성합니다. Root Cause Explorer에서 이러한 이벤트의 타임라인을 자동으로 생성하므로 보안 분석가가 신속하게 감염 또는 침투의 원인을 밝혀내고 해결할 수 있습니다.

유연한 구축

Security Analytics는 여러 구축 옵션을 통해 총소유비용(TCO)을 최적화하고 설비 투자 지출(CapEx)을 최소화하면서 다른 모든 솔루션을 능가하는 차원의 유연성을 실현합니다. 업계 표준 하드웨어에서 사전 구성된 어플라이언스 또는 가상 어플라이언스로 손쉽게 구축하여 지점 및 지사부터 엔터프라이즈 데이터 센터 전반에서 통합적인 보안을 제공합니다.

시각화. 분석. 해결

Symantec Security Analytics는 침해 사고에 신속하게 대응하고 첨단 기술로 네트워크 포렌식 분석을 수행하는 업계 최고의 통합 솔루션입니다. 실용적인 인텔리전스로 보안 위협의 모든 출처와 범위를 규명하면서 네트워크 트래픽에 대한 완벽한 가시성을 제공하므로 고객이 신속하게 허점을 해결하고 현재 진행 중인 리스크를 최소화하면서 온전한 기업으로 회복시킬 수 있습니다.

자세한 내용을 알아보거나 데모를 요청하려면 해당 지역의 시만텍 담당자에게 문의하십시오. 귀사의 보안 방어 및 침해 사고 대응 체계를 새로운 차원으로 발전시키고 비즈니스 역량을 강화할 수 있는 새로운 기회를 마련하십시오.

시만텍 소개

시만텍코리아

서울시 강남구 테헤란로 152 강남파이낸스센터 28층 TEL: 02-3468-2000 | FAX: 02-3468-2001 | www.symantec.com/ko/kr