데이터시트

McAfee Global Threat Intelligence for Enterprise Security Manager

McAfee® Labs의 강력한 역량을 상황 인식에 적용해 보십시오.

McAfee® Global Threat Intelligence for Enterprise Security Manager는 엔터프라이즈 보안 모니터링에 McAfee Labs의 강력한 역량을 적용합니다. McAfee Labs가 전 세계 1억 개 이상의 위협 센서에서 수집한 IP 평판을 처음으로 보안 정보 및 이벤트 관리(SIEM) 솔루션에 제공할 수 있게 되었습니다. 지속적으로 업데이트되면서 McAfee Enterprise Security Manager에 제공되는 풍부한 피드는 의심스럽거나 악의적인 IP와의 통신과 관련된 이벤트를 빠르게 발견할 수 있게 함으로써 상황 인식을 개선합니다. 이를 통해 보안 관리자는 어떤 호스트가 불량 요소와 통신을 했는지 또는 현재 통신 중에 있는지 파악하고 파악된 불량 요소가 위협 활동의 소스인 상황을 신속하게 인지할 수 있습니다.

외부 컨텍스트에 대한 필요성

보안 이벤트는 현재를 기준으로 보안 관련 활동에 관한 정보를 제공합니다. 이러한 이벤트의 상관 관계를 파악할 수 있는 기능이 SIEM에 탑재되어 있지만 아직 작업자가 해결해야 할 여러 가지 문제가 남아 있습니다. 이 활동은 수용 가능한가? 어떤 것이 가장 긴급한지 어떻게 알 수 있는가? 뚜렷한 증상을 나타내지 않는 정교한 공격을 탐지하는 방법은 무엇인가? 이러한 문제에 기업의 일반적인 일상 이벤트(2.5억 건 이상)가 가중되면 기존의 SIEM이 중점을 두는 알려진 패턴의 감지는 보안 모니터링의 극히 일부에 지나지 않는다는 것이 분명해집니다. 알려지지 않은 보안 모니터링의 이면에 있는 가장 중요한 컨텍스트 요소 중 하나는 외부 시스템의 평판을 이해하는 것입니다. 지금까지는 보안 이벤트를 이처럼 분명하게 이해하는 것이 불가능했습니다.

McAfee Labs의 강력한 기능을 SIEM에 적용

McAfee Global Threat Intelligence for Enterprise Security Manager는 보안 빅데이터를 위해 구축된 매우 지능적인 고속 McAfee SIEM을 통해 McAfee Labs의 강력한 기능을 보안 모니터링 흐름에 직접 적용합니다. 이 제품 서비스 옵션은 1억 4천만 개 이상의 IP 주소에 대한 소스 평판을 지속적으로 제공 및 조정하여 외부 시스템 평판의 컨텍스트를 보안 이벤트 스트림에 직접 적용하고 알려진 불량 요소와의 현재 및 과거의 상호 작용을 빠르게 식별합니다. McAfee Global Threat Intelligence(GTI) IP 평판은 1억 개 이상의 전 세계 센서와 500명 이상의 조사자들을 통해 모든 주요 위협 벡터에서 수집한 위협 인텔리전스의 상관 관계로부터 파생됩니다.

주요 이점

- McAfee Labs의 강력한 역량을 SIEM에 적용
- 이벤트와 관련된 위험을 정확하게 파악합니다.
- 성능에 영향을 미치지 않고 McAfee GTI의 방대한 위협 피드를 활용합니다.
- McAfee Enterprise Security Manager에서 새로운 소스 평판을 자동으로 받아 처리합니다.
- 응답 시간을 단축하면서 위협 탐지 정확도를 높입니다.
- 봇네트/분산 서비스 거부(DDoS), 네트워크 프로브를 호스팅하는 메일/스팸 전송 악성 프로그램, 악성 프로그램 존재, DNS 호스팅, 침입 공격에 의해 생성되는 활동 등과 연관된 알려진 불량 요소와의 이전 상호 작용 및 공격 경로를 빠르게 식별합니다.

McAfee Global Threat Intelligence for Enterprise Security Manager의 이점

- **전체 네트워크에 대한 보호 향상:** McAfee Global Threat Intelligence for Enterprise Security Manager는 네트워크에 의심스러운 요소 또는 알려진 불량 요소와 통신하는 노드가 있는 경우 이를 즉시 탐지하고 위협 경로를 신속히 파악합니다.
- **위험 기반 우선 순위 지정:** IP 평판은 자동으로 McAfee Enterprise Security Manager 무규칙 위험 점수 알고리즘에 통합되어 자동으로 대응 필요성을 정확히 파악합니다.
- **24/7 위협 모니터링:** McAfee Labs는 새롭게 등장한 감염된 시스템과 악의적인 시스템을 탐지하기 위해 지속적으로 위협 정보를 채점하며 그러한 시스템이 깨끗해진 후에는 글로벌 위협 환경에 대한 정확한 최신 이해를 조직에 제공합니다.

악의적인 활동을 실시간으로 파악

이제 조직은 McAfee Global Threat Intelligence for Enterprise Security Manager를 통해 이기종 방화벽, 침입 방지 시스템, 라우터 및 엔드포인트를 포함한 모든 이벤트에 대한 IP 평판을 이해할 수 있는 역량을 갖추게 되었습니다. McAfee Enterprise Security Manager의 동적 감시 목록 기능을 활용하면 이벤트가 자동으로 소스 평판 점수와 연관되며 위험이 조정됩니다. 글로벌 위협 환경이 변화함에 따라 McAfee GTI는 McAfee Enterprise Security Manager를 최신 상태로 유지하여 서버와 시스템이 지속적으로 정확한 평판 점수를 보유할 수 있도록 보장합니다. 이는 조직이 위험을 이해하는 데 도움이 될 뿐만 아니라 실시간으로 긴급한 문제를 지목하여 사고 대응 시간을 단축하고 정확한 위험 분석을 제공할 수 있습니다.

알지 못하는 요소 파악

McAfee Enterprise Security Manager의 핵심적인 강점은 수년 간의 데이터에 대한 역사적 상관 관계를 보관, 검색 및 활용할 수 있는 기능입니다. 이제 McAfee GTI를 통해 보안 분석가들은 시간을 거슬러 올라가 수년 간의 데이터를 참조하여 과거 불량 요소와의 상호 작용을 이해할 수 있습니다. 이는 '적고 느린' 공격, 봇네트의 반복적인 활동, 교차 사이트 스크립팅, SQL 주입 시도를 탐지하는 데 대단히 중요합니다.

응답 시간 감소

McAfee GTI는 McAfee Enterprise Security Manager 경보 및 경고 메커니즘과 원활하게 통합되어 알려진 악성 시스템과 상호 작용하여 그에 합당한 주의를 기울일 수 있게 합니다.

보안 빅 데이터를 위해 구축된 McAfee Database 지원 제공

데이터 증가에 대해 수많은 논의가 있었는데, McAfee Labs의 풍부한 보안 관련 지식을 SIEM에 적용하는 논의도 그중 하나입니다. McAfee Enterprise Security Manager는 성능에 큰 영향을 주지 않으면서 방대한 McAfee GTI IP 평판 데이터 스토어를 저장, 상관 관계 파악, 업데이트할 수 있는 고유한 기능을 갖추고 있습니다. McAfee Enterprise Security Manager는 SIEM에서 시간이 많이 걸리는 데이터베이스 관리를 없애고 매우 빠른 속도로 유입되는 이벤트 및 관계 데이터를 처리할 수 있도록 특별히 구축되었습니다. McAfee Global Threat Intelligence for Enterprise Security Manager를 통해 고객은 McAfee GTI 지식이 실시간으로 제공될 것이라는 확신을 가질 수 있습니다.

사양

지원되는 버전

McAfee Enterprise Security Manager 9.4 및 McAfee Event Reporter Appliance 9.4

- McAfee Labs 위협 인텔리전스 네트워크: 120여 개 국가에서 1억 개 이상의 노드를 활용
- 평균 IP 평판: 위협 환경에 따라 다름

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr

2014년 9월