McAfee Enterprise Security Manager

우선 순위를 결정하고, 조사 하고, 대응합니다.

가장 효과적인 보안은 시스템, 네트워크, 데이터베이스, 응용프로그램 및 클라우드의 모든 활동을 파악하는 데에서 시작됩니다. SIEM(보안 정보 및 이벤트 관리)은 효과적인 보안 프레임워크의 기초입니다. McAfee® Enterprise Security Manager는 McAfee SIEM 솔루션의 핵심으로, 보안 조직에 필요한 속도와 규모로 성능, 실행 가능한 인텔리전스 및 솔루션 통합을 제공합니다. 이로써 숨은 위협에 빠르게 우선 순위를 지정하고, 조사하고, 응답할 수 있으며, 컴플라이언스 요구 사항을 충족할 수 있습니다.

McAfee Enterprise Security Manager는 기업 내부의 시스템, 데이터, 위험 및 활동 보기뿐만 아니라 위협 데이터, 평판 피드 등 외부 세계에 대한 실시간 이해를 제공합니다. 이 보안 관리자는 신속한 위험 기반 의사 결정을 위해 필요한 콘텐츠와 컨텍스트에 대한 완벽하고 상호 연관된 액세스를 보안 팀에 제공하므로 역동적인 위협 및 운영 환경에서 최고의 효과를 내도록 리소스를 투자할 수 있습니다. 이는 또한 위험도가 낮고 느린 공격에 대해 조사하거나, 성능 저하 표시기(IoCs, indicators of compromise)를 검색하거나, 감사 결과를 교정하는 데 있어 매우 중요합니다. 위협 및 컴플라이언스 관리를 보안 작업의 핵심 요소로 만들기 위해 McAfee Enterprise Security Manager는 워크플로 및 보안 작업 팀의 효율성을 향상시키는 데 필요한 모든 것, 즉 구성 및 변경 관리, 사례 관리 및 중앙 관리식 정책 관리를 위한 통합된 도구를 제공합니다. 또한 McAfee Enterprise Security Manager에서 사용할 수 있는 콘텐츠 팩은 보안 작업을 단순화하는 데에 도움이 되는 고급 보안 사용 사례에 대해 미리 작성된 구성을 제공합니다.

몇 시간이 아닌 몇 분 만에 핵심 정보 파악

사고 조사, 진화된 공격의 증거 검색 또는 실패한 컴플라이언스 감사 시정을 위해서는 기록 데이터에 대한 가시성과 각 특정 이벤트의 모든 세부 정보에 대한 액세스가 필요하며 이벤트 데이터의 장기 스토리지에 신속하게 액세스하는 것이 중요합니다.

주요 이점

- **지능형:** 고급 분석 및 풍부한 컨텍스트를 통해 위협을 감지하고 우선 순위를 지정할 수 있습니다.
- **실행 가능:** 필요한 데이터는 중요한 경고 및 패턴을 조사, 포함, 교정 및 적용할 수 있도록 조치를 취할 옵션을 포함하는 동적 보기로 표시됩니다.
- **통합:** 이 솔루션은 광범위한 이기종 보안 인프라의 데이터를 모니터링 및 분석하고, 개방형 인터페이스를 통해 양방향 통합을 제공합니다. 또한 여러 초기 응답 작업을 자동화할 수 있습니다.
- **유연한 배포:** 사내 또는 클라우드에 배포하여 고유한 비즈니스 요구 사항 충족

McAfee에 문의

McAfee Enterprise Security Manager는 매우 정교하게 조정된 솔루션으로, 필요한 속도로 STIX 기반 위협 인텔리전스 피드를 포함하여 다른 데이터 스트림과 여러 해 동안의 로그 이벤트를 수집, 처리 및 상관관계를 구축할 수 있습니다. McAfee Enterprise Security Manager는 수십억 개의 이벤트와 흐름을 저장하므로 포렌식, 규칙 검증 및 컴플라이언스를 위해 장기적으로 데이터를 보존하면서 모든 정보를 즉각적인 임의 쿼리에 이용할 수 있습니다. 또한 데이터를 즉시 여러 저장 위치에 복제할 수 있으므로 비즈니스 연속성을 유지할 수 있습니다.

유연한 배포 옵션

McAfee Enterprise Security Manager를 고객의 데이터 센터에 사내 하드웨어 기반 솔루션으로 배포하거나 McAfee Enterprise Security Manager Cloud를 통해 클라우드로 배포할 수 있습니다.

사내 배포는 대량의 데이터 볼륨이 필요하거나 데이터 개인 정보 보호법을 준수함에 따라 회사 경계에 정보를 저장해야 하는 고객에게 가장 적합합니다. 또한, 이러한 고객은 일반적으로 솔루션을 배포, 운영 및 관리하는 인적 자원도 확보하고 있습니다.

더 소규모인 팀과 더 적은 규모의 데이터를 수집해야 하는 자원이 한정된 고객을 위해, McAfee Enterprise Security Manager Cloud는 운영 장벽을 제거하고, 자동 배포와 24시간 연중무휴 시스템 상태 모니터링, 정규 소프트 업데이트 및 패치를 제공하여 이러한 팀이 보안 업무에 역량을 집중할 수 있도록 합니다.

엔터프라이즈 규모에 맞게 제작됨

보안 작업 팀은 오늘날의 동적인 분산형 엔터프라이즈 아키텍처로부터 점점 더 많은 양의 원시 및 구문 분석한 데이터를 수집하고 빠르게 탐색하면서 더욱 뛰어난 효율성을 필요로 합니다. 이 과제를 극복하기 위해 McAfee Enterprise Security Manager는 대량 데이터 처리를 위해 특별히 구축된 확장 가능한 개방형 데이터 버스를 사용합니다. 또한, 확장성이 뛰어난 데이터 아키텍처는 데이터 수집, 검색 및 보관에 대한 성능 저하를 방지하기 위해 처리, 관리 및 분석을 지원합니다. 그러한 성능 저하는 중요한 데이터를 나중에 사용할 수 없는 경우, 쿼리 응답이 분석을 느리게 하는 경우 또는 성능으로 인해 부분 검색만 가능한 경우 조사를 약화시킬 수 있습니다.

컨텍스트 및 콘텐츠 인식

위협 데이터 및 평판 피드, ID 및 액세스 관리 시스템, 개인 정보 보호 솔루션 또는 기타 지원 시스템을 포함하여 컨텍스트 정보를 사용할 수 있는 경우 각 이벤트가 해당 컨텍스트로 강화됩니다. 이러한 강화를 통해 네트워크 및 보안 이벤트가 자산 특성 및 실제 비즈니스 프로세스와 정책과 상관되는 방식을 더 잘 이해하고 그러한 방식을 기반으로 하여 정확한 상담 분류를 제공합니다.

McAfee Enterprise Security Manager의 확장성 및 성능은 문서, 트랜잭션, 통신 등의 응용프로그램 콘텐츠를 포함하여 더 많은 소스로부터 더 많은 정보 수집을 지원함으로써 심층적인 포렌식 가치를 제공합니다. 이러한 정보는 광범위한 위험 및 위협을 감지할 수 있도록 매우 많은 양이 인덱싱, 정규화, 상호 연결되어 있습니다.

Advanced Threat Interpretation

네트워크 트래픽, 사용자 활동 또는 응용프로그램 사용이든 관계없이 정상적인 활동을 벗어나는 경우 위협이 임박한 상태이며 데이터 또는 인프라가 위험에 처해 있음을 표시하는 것일 수 있습니다. McAfee Enterprise Security Manager는 수집된 모든 정보와 관련하여 기준 활동을 계산하고 발생 전에 미리 잠재적인 위협을 탐색할 목적으로 우선순위 경보를 제공하는 동시에 더 큰 위협의 징후가 될 수 있는 패턴에 대한 데이터를 분석합니다. McAfee Enterprise Security Manager는 또한 컨텍스트 정보를 활용하고 각 보안 이벤트를 그러한 컨텍스트로 보충하여 보안 이벤트가 실제 비즈니스 과정에 영향을 미치는 방식을 더 잘 파악할 수 있습니다.

McAfee Enterprise Security Manager의 Cyber Threat Manager 대시보드는 새로 발생하는 위협의 향상된 실시간 모니터링 및 이해를 제공합니다. STIX/TAXII, McAfee® Advanced Threat Defense 및/또는 타사 웹 URL을 통해 보고된 의심스럽거나 확인된 위협 정보는 이벤트 데이터에 대해 거의 실시간으로 또는 (역추적 기능을 사용하여) 기록을 통해 집계하고 상호 연계함으로써 보안 팀에 환경 내에서 위협 전파에 대한 심층적인 이해를 제공합니다. 조직은 이러한 인텔리전스를 활용하여 올바른 데이터와 올바른 인력을 연계하여 거의 실시간으로 조치를 수행하고 더 스마트한 결정을 내릴 수 있습니다.

보안 운영 최적화

McAfee Enterprise Security Manager의 분석가 중심의 사용자 환경은 향상된 유연성, 간편한 사용자 지정 및 조사에 대한 빠른 응답을 제공합니다. 간소화된 워크플로를 통해 훨씬 시기적절하고 효율적인 사고 관리가 가능합니다. 위협 정보에 대한 빠르고 스마트한 액세스를 통해 초보자부터 전문가에 이르기까지 어떤 수준의 전문 지식을 가진 분석가 누구든지 진화하는 위협에 우선 순위를 두고, 조사하고, 응답하는 것이 훨씬 쉬워집니다.

McAfee Enterprise Security Manager의 유용성은 개봉 후 즉시 발휘되기 시작하는 데 수백 종류의 보고서, 보기, 규칙 및 경보를 바로 사용할 수 있으며 이 모두를 간편하게 사용자 지정할 수 있습니다. 일반적인 네트워크 사용량 파악을 위한 기준을 설정하거나 단순히 경보를 사용자 지정하든 관계없이, McAfee Enterprise Security Manager 대시보드를 통해 대부분의 관련된 보안 정보를 간편하게 시각화, 조사 및 보고할 수 있습니다. 이제 조직은 신속하고 지능에 기반한 의사결정에 필요한 데이터 및 컨텍스트에 종합적이고 상호 연결된 액세스를 갖게 됩니다.

또한 McAfee Enterprise Security Manager는 미리 구성된 "레디 투 고" 보안 사용 사례를 통해 보안 작업을 단순화하며 강화된 위협 또는 컴플라이언스 관리 기능에 대한 빠른 액세스를 제공하기 위한 콘텐츠 팩을 제공합니다. 콘텐츠 팩은 규칙, 경보, 보기, 보고서, 변수 및 관심 목록 집합을 제공하는 일반 보안 사용 사례에 대해 미리 작성된 구성입니다. 많은 콘텐츠 팩에서 추가 보안이나 자동 교정을 보장할 수 있는 활동에 대해 사전 패키지된 트리거를 제공합니다.

컴플라이언스 단순화

McAfee Enterprise Security Manager는 컴플라이언스 모니터링 및 보고 기능을 중앙에서 집중적으로 관리하고 자동화하여 시간이 많이 소모되는 수동 처리가 사라집니다. 또한 UCF (Unified Compliance Framework)와 통합되어 컴플라이언스 요구 사항을 충족하고 감사 관련 노력이나 비용을 최소한으로 유지하도록 '한 번의 데이터 수집으로 많은 컴플라이언스 달성'이 가능해집니다. UCF 지원으로 각 규제의 세부 사항을 정규화하여 수집된 단일 이벤트 세트를 개별적인 규제에 간편하게 매핑할 수 있게 되어 컴플라이언스 효율성이 증가합니다.

McAfee Enterprise Security Manager에는 수백 가지 유형의 사전 구축된 대시보드, 종합적 감사 추적 및 PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX를 포함한 240개 이상의 글로벌 규제 및 관리 프레임워크와 관련된 보고서가 포함되어 간편하고 신속하게 컴플라이언스를 관리할 수 있습니다. 즉시 사용 가능한 광범위한 지원 외에도 모든 McAfee Enterprise Security Manager 컴플라이언스 보고서, 규칙 및 대시보드를 완전히 사용자 지정할 수 있습니다.

IT 인프라 연결

보안 인프라 통합은 조직의 보안 상황에 대해 전무후무한 높은 수준의 실시간 가시성을 제공합니다. McAfee Enterprise Security Manager는 위협 인텔리전스 피드뿐만 아니라 수많은 타사 보안 공급업체 장치에서 중요한 데이터를 수집할 수 있습니다. McAfee® Global Threat Intelligence(McAfee® GTI)와의 통합은 1억 개가 넘는 McAfee® Labs의 글로벌 위협 센서에서 수집한 데이터를 가져와서 알려진 악성 IP 주소로부터 계속 업데이트되는 피드를 제공합니다. 또한 McAfee Enterprise Security Manager는 STIX/TAXII 및/또는 타사 웹 URL을 통해 보고된 위협 정보를 통합하고 분석을 기반으로 하여 조치를 취할 수 있습니다.

McAfee Enterprise Security Manager는 McAfee 솔루션 및 McAfee® Security Innovation Alliance 파트너 솔루션을 포함하여 수십 개의 보완 사고 관리 및 분석 솔루션과 능동적으로 통합됩니다.

예를 들어 엔드포인트 모니터링을 기반으로 하는 McAfee Threat Intelligence Exchange는 글로벌, 타사 및 로컬 위협 인텔리전스를 활용하여 확산성이 낮은 공격을 집계합니다. McAfee® Threat Intelligence Exchange는 또한 McAfee Advanced Threat Defense과 같은 통합된 다른 제품을 활용하여 파일을 추가로 분석하고 진단할 수 있습니다.

또한 수십억 가지의 보안 이벤트를 수백 가지의 이상으로 압축하여 우선 순위가 높은 소수의 위협 요소를 도출하고 분석가가 다른 솔루션으로는 식별하기 어려운 비정상적인 고위험 보안 위협을 감지할 수 있도록 지원하는 사용자 및 단체 행동 분석 전용 솔루션인 McAfee® Behavioral Analytics와의 통합으로 분석가들도 이점을 누릴 수 있습니다. 이와 유사하게, McAfee Enterprise Security Manager는 McAfee® Investigator와 통합해 분석가가 전문 조사자의 역할을 할 수 있도록 도우며 근본 원인을 규명했다는 확신을 갖고 더 많은 사례를 더 빨리 종결할 수 있도록 지원합니다.

사고 대응 팀과 관리자는 McAfee® Active Response를 사용하여 시스템에서 휴면 상태로 있거나 메모리에서 활성 프로세스로 있는 악성 제로 데이 파일을 찾을 수 있습니다.

또한, McAfee Active Response는 영구 수집기를 사용하여 특정 IOC에 대한 엔드포인트를 계속해서 모니터링함으로써 IOC가 환경에 나타나면 자동으로 알려줍니다. 이 결합은 표준적인 보안 접근 방법과 달리 탐색부터 억제 및 치료에 이르는 상세한 폐쇄형 루프 워크플로를 조직에 제공합니다.

McAfee는 새로운 위협을 방지하고 이에 대응할 수 있는 통합된 보안 시스템을 제공합니다. 더 적은 리소스로 많은 위협을 더 빠르게 해결할 수 있도록 돕습니다. 연결된 아키텍처와 중앙 집중식 관리는 보안 인프라 전반에서 복잡성을 줄이고 운영 효율성을 개선합니다. McAfee는 모든 통합 보완 기능을 제공함으로써 최고의 보안 파트너가 되기 위해 노력하고 있습니다.

자세히 알아보기

McAfee Enterprise Security Manager에 관한 자세한 내용은 www.mcafee.com/siem 및 www.mcafee.com/esm을 참조하십시오.

통합된 솔루션에 대한 자세한 내용은 www.mcafee.com/secops를 참조하십시오.

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

2020년 4월