데이터시트

McAfee Database Event Monitor for SIEM

성능 저하 없이 데이터베이스 트랜잭션에 대한 가시성 확보

컴플라이언스를 위해서는 데이터베이스 트랜잭션에 대한 믿을 수 있는 감사가 필수적이지만 일반적인 기본 데이터베이스 감사 솔루션은 데이터베이스 성능과 데이터베이스 관리자 생산성을 저해할 수 있습니다. McAfee® Database Event Monitor for SIEM의 비침입 설계는 확장하는 컴플라이언스 감사 및 보고 요구 사항을 지원하고 보안 작업을 향상시킵니다.

McAfee Database Event Monitor for SIEM은 데이터베이스 및 응용프로그램에 대한 비침입 상세 보안 로깅을 제공하여 중요한 기업 및 고객 데이터에 대한 모든 액세스를 모니터링합니다. 최소한의 배포 노력으로 누가 왜 데이터를 액세스하는지를 포함하여 데이터베이스 트랜잭션, 이벤트, 특정 데이터베이스 쿼리 및 응답에 대한 가시성을 얻을 수 있습니다.

McAfee Database Event Monitor for SIEM은 데이터베이스 활동을 중앙 감사 저장소로 통합하고 정규화, 상관 관계, 분석, 해당 활동의 보고를 제공하는 유일한 제품입니다.

사전 정의된 규칙 및 보고서와 개인정보 친화적인 로깅 기능은 쉽게 컴플라이언스를 달성하고 전반적인 보안 상태를 강화합니다.

컨텍스트의 데이터베이스 액세스

McAfee Database Event Monitor for SIEM은 단순한 로깅에 그치지 않고 데이터를 정규화하고 데이터베이스 트랜잭션을 다른 정보와 상호 연결함으로써 실시간 분석 수행을 돕습니다.

McAfee Database Event Monitor for SIEM은 사용자 정보, 응용프로그램 콘텐츠, 운영 체제 작업, 취약성은 물론 네트워크 위치에 대한 가시성까지 제공함으로써 다음이 가능합니다.

- 응용프로그램 전반에서 사용자 추적
- 로그인에서 로그오프까지 전체 세션 활동을 검사
- 중요 데이터를 감지하고 정책 위반을 파악
- 허가된 채널을 통해 데이터 손실 감지
- 보안 이벤트에 대한 데이터베이스 활동 상관 관계 파악
- 모든 데이터베이스 활동에 대한 감사 추적 생성
- PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX 등에 대한 상세한 보고서 생성

주요 이점

- 데이터베이스 성능에 전혀 영향을 주지 않는 수동 네트워크 기반 모니터링 사용
- 무단 또는 위험한 데이터베이스를 포함한 모든 데이터베이스 인스턴스를 검색
- 조정된 정보를 통해 데이터베이스에 대한 액세스의 모니터링 및 로깅 가능
- 감사 지원을 위해 로그인에서 로그오프까지 모든 데이터베이스 트랜잭션의 세부 정보를 보존
- 원클릭 세션 복원을 통해 분석 간소화
- McAfee Enterprise Security Manager와 완전히 통합되어 상관 관계 및 기타 고급 SIEM 작업 시 데이터베이스 트랜잭션 사용 가능
- 유연한 혼합 배달 옵션에는 물적 및 가상 어플라이언스가 포함됩니다.

intel Security

각 트랜잭션에 대한 완전한 가시성

McAfee Database Event Monitor for SIEM은 모든 데이터베이스 트랜잭션을 모니터링하고 쿼리, 결과, 인증 활동, 권한 상승을 포함한 모든 데이터베이스 활동에 대한 완전한 감사 추적을 제공합니다. McAfee Database Event Monitor for SIEM은 모든 트랜잭션에 대한 전체 세션 세부 정보를 유지하므로 로그인에서 로그아웃까지 특정 트랜잭션 전후로 어떤 일이 있었는지 쉽게 알 수 있습니다.

자동화된 컴플라이언스 프로세스

미리 구성된 정책 기반 감지 규칙과 컴플라이언스 보고서는 PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX 등에서 요구하는 데이터 액세스 정보를 생성할 수 있도록 보장합니다. 또한 McAfee Database Event Monitor for SIEM은 McAfee Enterprise Security Manager 및 McAfee Enterprise Log Manager와 완전히 통합되어 전례 없는 이벤트 분석 및 상관 관계를 제공하고 활동 로그에 민감한 데이터를 적절히 저장하고 마스킹합니다.

예외 목록은 모니터링하고 있지 않은 데이터베이스 서버는 물론 데이터베이스의 데이터를 액세스하기 위해 개방된 부적절한 포트를 표시합니다.

사용자 및 계정 추적

McAfee 보안 관리 제품군의 고급 기능을 활용하여 여러 응용프로그램과 계정에 대해 사용자와 관리자를 쉽게 추적할 수 있고 데이터베이스 액세스 방법에 관계 없이 모든 사용자 활동에 대한 종단 간 책임 소재 추적을 제공합니다.

사용자 활동 프로파일링

McAfee Database Event Monitor는 모든 SQL 쿼리를 대상 데이터베이스 서버에서 액세스되는 개체(테이블, 보기, 저장 프로시저)인 명령으로 토큰화하여 새로운 활동과 비정상적 활동을 모두 드러냅니다.

SQL 주입

모든 SQL 쿼리 응답 패킷은 쿼리 성공 또는 실패에 대해 모니터링됩니다. SQL 주입 공격의 증상인 구문 오류와 같은 심각도가 낮은 오류가 연속으로 발생하는 경우 이를 추적하고 상관 관계를 파악합니다. 이는 SQL 주입 시도를 미리 감지하는 확실한 방법입니다.

위험 및 위협 감지

McAfee Database Event Monitor for SIEM은 모든 모니터링된 활동을 사용자 지정 가능한 정책 규칙 모음에 대해 분석하고 모든 의심스러운 활동을 감지하고 경고합니다. 또한 이상 기반 탐지는 비정상적인 사용자 활동, 쿼리, 응답 및 기타 부적절한 동작을 알려줍니다.

오버헤드가 없는 강력한 기능

고성능 데이터 캡처 엔진을 가진 McAfee Database Event Monitor for SIEM 어플라이언스는 네트워크를 통해 데이터베이스를 모니터링하므로 데이터베이스 자체에 오버헤드를 부과하지 않고 필요한 감사 데이터의 보존을 보장합니다.

McAfee Enterprise Security Manager는 관리를 제공하고 데이터베이스 모니터링을 나머지 보안 및 컴플라이언스 에코 시스템과 연결합니다. 로컬 터미널 활동에 대한 가시성을 높이려면 경쟁업체나 기본 감사에 비해 성능 영향이 적은 호스트 에이전트 옵션을 사용하십시오.

데이터베이스 모니터링 기능

- 모든 데이터베이스 활동을 모니터링 및 기록
- 컴플라이언스 노력 지원
- 데이터 도청
- 책임 소재 추적 향상
- 개체, 작업, 정책 위반 경고
- 데이터베이스 서비스 수준/성능 관리를 위한 귀중한 메트릭 확보
- 다음을 포함하여 데이터에 대한 모든 경로 모니터링:
  - 응용프로그램
  - 사용자
  - 악성 프로그램
  - 유틸리티
  - 백도어
  - 쿼리
  - LAMP 스크립팅
  - ODBC(Open Database Connectivity)

사용 사례

컴플라이언스

McAfee Database Event Monitor for SIEM은 컴플라이언스 보장을 돕기 위해 사용 중인 중요 데이터를 검색할 수 있습니다. 이러한 데이터베이스를 모니터링하고 보호된 데이터 액세스, 사용자 계정 활동, 변경 사항에 대한 감사 추적을 설정할 수 있습니다. 엄격한 통제를 위해 보안 업무를 데이터베이스 관리로부터 분리하고 중요 데이터를 로깅으로부터 마스킹할 수 있습니다. 보고서를 통해 보호된 레코드를 가장 많이 사용하는 사용자를 알 수 있습니다. 언제든지 다양한 규제를 위해 미리 구성된 보고서를 생성할 수 있습니다.

데이터베이스 감지 및 분류

McAfee Database Event Monitor for SIEM은 데이터베이스 명령에 대한 네트워크를 모니터링함으로써 알 수 없는 데이터베이스 또는 위험한 데이터베이스를 포함하여 모든 데이터베이스 인스턴스를 감지할 수 잇습니다. 또한 McAfee Database Event Monitor for SIEM은 쿼리 결과를 포함한 모든 트랜잭션을 모니터링하고 이를 정책 규칙과 사전에 대해 분석함으로써 신용 카드, 주민 번호 또는 기타 중요 데이터가 저장된 데이터베이스가 무엇인지 감지할 수 있습니다.

보안 모니터링

McAfee Database Event Monitor for SIEM은 데이터베이스를 직접 모니터링하고 실시간으로 브루트 포스 로그인, SQL 주입 공격, 비정상적인 액세스 패턴과 그 외 서버 보안 침해 가능성을 감지하고 경고합니다. 백엔드 응용프로그램 활동을 모니터링하고 사기 데이터 검색 및 위험한 사용자 계정을 포함하여 의심스러운 활동을 감지할 수 있습니다.

공격이 네트워크 내부에서 시작된 경우 사용자 활동을 추적하고 네트워크 흐름 데이터에 대해 상관 관계를 규명하여 공격자를 식별하고 찾아낼 수 있습니다. 외부 공격의 경우 다른 아웃바운드 네트워크 및 응용프로그램 활동에 대한 상관 관계를 추적하여 데이터 손실, 비밀 통신 채널, 기타 손실 벡터를 발견할 수 있습니다.

61321ds_db-event-monitor_0914

McAfee. Part of Intel Security.
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.intelsecurity.com