McAfee Advanced Correlation Engine

중요 자산에 대한 위협 탐지

오늘날의 미묘한 위협은 표준 규칙 기반 위협 탐지로는 부족합니다. McAfee® Advanced Correlation Engine 솔루션과 McAfee Enterprise Security Manager를 배포하고 규칙 기반 및 위험 기반 로직을 모두 사용하여 실시간으로 위협 이벤트를 식별하고 점수를 매기십시오. McAfee Advanced Correlation Engine 솔루션에서 사용자 또는 그룹, 응용프로그램, 특정 서버 또는 서브넷 등 중요한 사항을 설정하면 그에 대한 위협이 있을 때 경고합니다. 감사 추적 및 기록 재생을 통해 포렌식, 컴플라이언스, 규칙 조정을 지원합니다.

주요 이점

- 시작 간소화: 규칙 업데이트, 시그니처 조정 또는 다른 문제가 없음
- 우선 사용자, 자산, 응용프로그램 및 활동에 대한 위협을 경고
- 동시적인 규칙 기반 및 규칙 없는 상관관계를 통한 정확한 점수
- 기록에 대한 새로운 공격 및 취약성 검사를 통해 지난 이벤트 탐지
- McAfee Enterprise Security Manager에 대한 특수 상관관계 및 처리 리소스 추가
- 어플라이언스 및 가상 배포 형태로 모두 사용 가능

McAfee Advanced Correlation Engine 솔루션은 두 개의 전용 상관관계 엔진과 맞춤형 성능을 통해 McAfee Enterprise Security Manager 이벤트 상관관계를 보완합니다.

- 규칙 없는 점수 상관관계를 사용하여 위험 점수를 산정하는 위험 탐지 엔진
- 일반 규칙 기반 이벤트 상관관계를 사용하여 위협을 탐지하는 위협 탐지 엔진

독립형 McAfee Advanced Correlation Engine 솔루션은 기업 전체에서 이처럼 풍부한 이벤트 상관관계를 지원하는 데 필요한 처리 능력을 제공합니다. 이 데이터 엔진은 가장 큰 네트워크까지도 수용할 수 있도록 확장합니다.

실시간 및 기록 위협 탐지

McAfee Advanced Correlation Engine 솔루션은 실시간 또는 기록 모드로 배포할 수 있습니다. 실시간 모드에서 McAfee Advanced Correlation Engine 솔루션은 즉각적인 위협 및 위험 탐지를 위해 이벤트를 수집과 동시에 분석합니다.

- 즉각적인 위협 탐지를 위한 실시간 이벤트 데이터의 규칙 기반 상관관계 분석
- 위협 진행에 따른 탐지를 위한 실시간 이벤트 데이터의 규칙 없는 상관관계 분석

기록 모드에서는 반복되는 위협 및 위험 탐지를 위해 두 상관 분석 엔진 모두를 통해 수집한 모든 데이터를 재생할 수 있습니다. 제로 데이 공격이 감지되면 McAfee Advanced Correlation Engine 솔루션은 하위 제로 데이 위협 탐지를 위해 기록을 검토하여 과거에 조직이 해당 공격에 노출된 적이 있는지 파악합니다.

필요한 곳에 성능을 집중

McAfee Advanced Correlation Engine 솔루션은 자급형 어플라이언스 또는 가상 솔루션으로서 이벤트 수집 및 관리에 있어 McAfee Enterprise Security Manager의 성능에 영향을 끼치지 않습니다. McAfee Advanced Correlation Engine 응용프로그램의 모든 기능을 성능 저하 없이 활용하고 McAfee Enterprise Security Manager 유틸리티를 최대화할 수 있습니다.

intel Security

규칙 기반 이벤트 상관관계

규칙 기반 상관관계는 기존의 상관관계 로직을 사용하여 수집한 정보를 실시간으로 분석합니다. 모든 로그, 이벤트 및 네트워크 흐름의 상관관계를 ID, 역할, 취약성 등의 컨텍스트에 맞는 정보와 함께 분석하여 대규모 위협을 나타내는 패턴을 감지합니다. 네트워크 전체에 대한 규칙 기반 상관관계가 이미 모든 McAfee Enterprise Security Manager 솔루션에서 지원되지만 McAfee Advanced Correlation Engine 솔루션은 기존 상관관계 작업을 보완하거나 완전히 오프로드함으로써 더 큰 데이터 볼륨의 상관관계 분석을 위한 전용 처리 리소스를 제공합니다.

규칙 없는 위험 점수 상관관계

규칙 기반 상관관계는 모든 기존 SIEM(security information and event management)의 필수적이고 중요한 기능이지만 이러한 시스템은 알려진 패턴만 탐지할 수 있으며 효과적인 작동을 위해서는 지속적인 시그니처 조정과 업데이트가 필요합니다. 해답은 "규칙 없는" 상관관계 기술을 통해 기존의 이벤트 상관관계를 보강하는 것입니다. 규칙 없는 상관관계 시스템에서 탐지 시그니처는 단순한 일회성 구성으로 대체됩니다. McAfee Advanced Correlation Engine 솔루션에서 귀사에 중요한 항목이 무엇인지 설정하기만 하면 됩니다. 그 항목은 특정 서비스 또는 응용프로그램, 사용자 그룹 또는 특정 데이터 유형이 될 수 있습니다.

실시간 추적 및 경고

McAfee Advanced Correlation Engine 솔루션이 그러한 항목에 관련된 모든 활동을 추적하기 시작하고 실시간 활동에 따라 오르고 내리는 동적인 위험 점수를 산정합니다. 위험 점수가 특정 임계값을 초과하면 McAfee Advanced Correlation Engine 솔루션 내에서 이벤트가 생성됩니다. 이 이벤트는 보안 분석가에게 위협 조건 확산을 경고하는 데 사용되거나 기존의 규칙 기반 상관 분석 엔진에서 더 큰 규모의 사고에 대한 조건으로 사용될 수도 있습니다. McAfee Advanced Correlation Engine 솔루션은 시간 경과에 따른 완벽한 위협 조건 분석 및 조사를 위해 완전한 위험 점수 감사 추적을 유지합니다.

사용 사례

기업 위험 모델링

McAfee Advanced Correlation Engine 솔루션은 기업 위험을 효과적으로 모델링할 수 있는 플랫폼을 제공합니다. 고위 권한을 가진 직원이 일급 기밀 문서에 액세스하는 것은 방위 조직의 위험 요소가 될 수 있고 심각한 질병을 진단받은 유명인 환자의 기록 유출은 병원의 위험 요인이 될 수 있습니다. McAfee Advanced Correlation Engine 솔루션은 중요한 속성의 점수를 지정함으로써 완벽한 조직 모델링을 제공하고 정상 임계값이 초과되면 기준선을 만들고 알림을 전송합니다.

중요 데이터에 대한 사전 예방적 위험 평가

McAfee Advanced Correlation Engine 솔루션이 실시간 데이터를 모니터링함에 따라 두 상관 분석 엔진을 동시에 사용하여 위험과 위협이 발생하기 전에 탐지할 수 있습니다. 위험 점수는 기존 상관관계 로직에서 사용할 수 있습니다. 예를 들어 기존의 규칙 기반 위협 탐지 시그니처는 "브루트 포스 로그인 이벤트 후에 발생하는 악성 프로그램 이벤트"일 수 있습니다. 일반적으로 시그니처가 트리거되면 이벤트가 이미 발생한 것입니다. 하지만 McAfee Advanced Correlation Engine 솔루션을 사용하면 브루트 포스 로그인 이벤트 후 위험 점수의 20% 증가와 같은 위험 요인을 통합할 수 있습니다. 이 이벤트가 발견되면 McAfee Advanced Correlation Engine 솔루션은 다가오는 사고에 대한 사전 예방적인 경보를 제공하여 피해가 발생하기 전에 조치를 취할 수 있도록 합니다.

반복되는 위협 평가

위협을 파악하거나 위반 사항을 발견하고 그것이 처음부터 계속 존재했는지 고민하는 경우가 종종 있습니다. 기록 모드에서 McAfee Advanced Correlation Engine 솔루션을 배포함으로써 여기에 설정된 기록 데이터 집합을 기존 상관 분석 엔진 및 규칙 없는 상관 분석 엔진을 통해 재생할 수 있습니다.

새로 발견된 위협이 언제 처음 구체화되었는지 파악함으로써 해당 조건의 근본 원인을 파악할 가능성이 훨씬 높아집니다.

작동 모드

실시간 상관관계 모드

- 즉각적인 위협 탐지를 위한 실시간 이벤트 데이터의 규칙 기반 상관관계 분석
- 위협 진행에 따른 탐지를 위한 실시간 이벤트 데이터의 규칙 없는 상관관계 분석

기록적 상관관계 모드

- 반복되는 위협 감지를 위한 기록적인 이벤트 데이터의 규칙 기반 상관관계 분석
- 반복되는 위협 평가를 위한 기록적인 이벤트 데이터의 규칙 없는 상관관계 분석

상관관계 기능

- 동시적인 규칙 기반 및 규칙 없는 상관관계 분석
- 모든 지원 데이터 소스의 데이터 상관관계 분석
- 분산된 네트워크 및 수집기에서 데이터 상관관계 분석
- 수백 개의 사전 정의된 이벤트 상관관계 규칙 포함
- 규칙 없는 상관관계를 위한 구성 편집기 포함
- 규칙 사용자 정의 또는 새로운 규칙 생성을 위한 편리한 GUI 이벤트 상관관계 규칙 편집기 포함

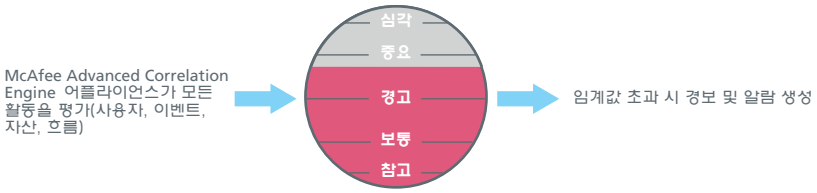

그림 1. 위험 기반 상관관계를 통해 우선 순위 자산에 대한 위협 가능성을 감지할 수 있습니다.

자세한 내용은
www.mcafee.com/kr/products/siem/index.aspx

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

41606ds_adv-corr-engine_1112B_fnl_ETMG