McAfee Enterprise Log Search

수십억 개의 이벤트를 고속으로 검색하여 더욱 빠르게 추적

보안 팀은 갈수록 지나치게 증가하는 경보를 발생시키는 환경에서 빠르게 전환할 수 있는 도구를 필요로 합니다. 이러한 팀의 분석가는 풍부한 컨텍스트에 액세스할 수 있는 기능과 함께 사고와 관련 있는 이벤트 세부 정보를 신속하게 파악할 수 있는 능력을 갖추어야 합니다. McAfee® Enterprise Log Search는 압축되지 않은 원시 이벤트 데이터를 초고속으로 검색할 수 있는 기능을 통해 신속하게 위협에 대응합니다. Elasticsearch 지원 백엔드는 쿼리 성능을 최적화하여 원시 로그에 대한 즉각적인 액세스를 제공합니다. 향상된 검색 기능은 간단한 키워드의 자연어 입력과 대상이 지정된 데이터 검색을 위해 보다 정교한 정규식 패턴을 모두 사용한 쿼리를 지원합니다.

주요 이점

- 로그 보존과 빠른 검색을 위해 최적화된 로그 관리
- 고속 수집, 인덱싱 및 쿼리 성능을 지원하는 Elasticsearch 지원 백엔드
- 자연스러운 언어 검색
- 구문 분석된 데이터 보기에서 원시 로그로 쉽고 빠르게 전환
- McAfee Enterprise Security Manager와 완벽하게 통합됨
- 유연한 배포 옵션에 물리적 어플라이언스와 가상 어플라이언스 (자유롭게 혼합 가능)가 포함됨

최적화된 로그 관리

McAfee Enterprise Log Search는 역방향 인덱스를 활용하여 데이터를 저장하는 기술인 Elasticsearch를 기반으로 구축되었습니다. 역방향 인덱스는 검색어를 효율적으로 검색할 수 있는 구조로 데이터를 카탈로그화합니다. Elasticsearch는 고성능 수집 및 인덱싱이 가능하도록 설계되었으므로 McAfee Enterprise Log Search는 캡처되고 카탈로그화된 원시 데이터를 고속으로 검색할 수 있게 해줍니다.

McAfee Enterprise Log Search는 보안 정보 및 이벤트 관리(SIEM) 솔루션인 McAfee® Enterprise Security Manager의 구성요소입니다. 또 다른 보완 구성요소인 McAfee® Enterprise Log Manager는 포렌식 무결성을 위해 해싱(MD5) 인바운드 원시 로그를 통해 기록을 저장하고 저장 효율성을 위해 그러한 원시 로그를 압축하도록 설계되었습니다. 이러한 두 구성요소를 결합하면 특수 저장소 솔루션이 제공됩니다. 그러한 솔루션은 빠른 검색(McAfee Enterprise Log Search를 통해)과 컴플라이언스 로그 보존(McAfee Enterprise Log Manager를 통해)을 극대화하기 위해 동시에 사용할 수 있으므로 고객은 성능 저하 없이 두 기능을 모두 활용할 수 있습니다.

McAfee Enterprise Log Search를 사용하면 년(365일), 분기(90일) 또는 월(30일) 단위로 서로 다른 기간 동안 압축되지 않은 데이터를 저장하도록 보존 정책을 맞춤 설정할 수 있습니다. 사용자는 어떤 데이터 원본을 McAfee Enterprise Log Search와 결합시킬지 식별할 수 있으며 개별 보존 정책을 6개까지 추가할 수 있습니다.

McAfee에 문의

향상된 검색 기능

McAfee Enterprise Log Search 내 검색 기능은 널리 사용되는 검색 엔진과 유사하며 자연어 입력을 허용합니다. 검색 결과는 간단한 텍스트 또는 키워드에서 검색할 수 있습니다. 또한 검색은 부울 로직, 와일드카드 및 정규식(RegEx)을 포함한 보다 정교한 패턴으로 수행될 수 있습니다. 검색 결과의 범위를 좁히려면 데이터 소스 및 날짜를 기준으로 필터를 적용할 수 있습니다. 날짜 필터를 사용하면 사용자는 지난 1시간, 현재 날짜, 이전 연도 또는 사용자 정의 범위 등 로그 이벤트가 생성된 기간에서 선택할 수 있습니다.

McAfee Enterprise Security Manager와 통합됨

McAfee Enterprise Security Manager와의 긴밀한 통합 덕분에 분석가는 한 번의 클릭으로 구문 분석된 데이터에서 원시 데이터로 전환할 수 있습니다. McAfee Enterprise Security Manager에서 이벤트가 생성된 경우 구문 분석된 이벤트 파일은 소스 로그 파일 및 특정 원시 로그 기록에 직접 연결됩니다. 그러한 기록 또는 일부 기록에 대한 향상된 가시성을 원하는 분석가는 원시 로그 검색에 대한 메시지에서 해당 로그를 선택하기만 하면 됩니다. 보다 심층적인 원시 로그 검색을 위해 시작해야 할 추가 단계, 응용프로그램 또는 인터페이스가 없습니다.

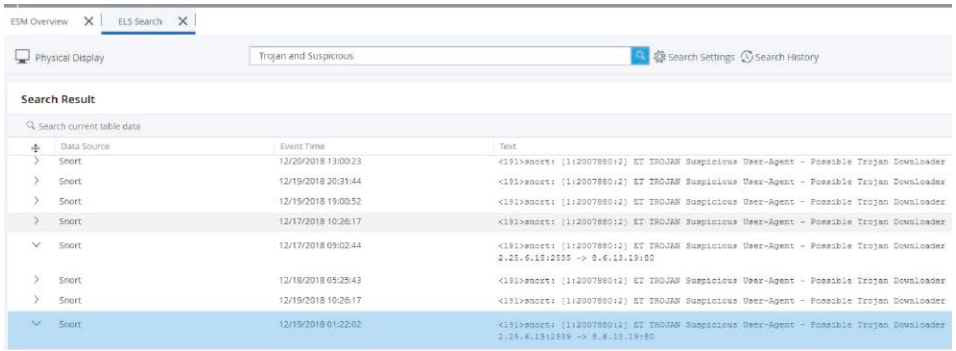

그림 1. 부울 로직을 사용한 키워드 검색을 통해 트로이 목마가 포함된 의심스러운 이벤트를 발견할 수 있습니다.

유연한 배포 및 가격 책정

유연한 제공 옵션에는 물리적 어플라이언스 및 가상 어플라이언스가 포함됩니다. 어플라이언스는 데이터 소스당 가격, EPS당 가격 또는 인덱싱된 데이터 볼륨별 가격이 아니라 특정 EPS(event-per-second) 용량을 수집할 수 있는 기능에 따라 평가되고 판매됩니다. 가상 시스템(VM)은 동일한 철학에 따라 라이선스가 부여되며 지정된 EPS를 지원하는 데 필요한 CPU 코어 수에 따라 판매됩니다. 그러므로 고객은 하드웨어를 교체하지 않고도 필요에 따라 코어를 추가할 수 있습니다.

필요한 데이터를 수집하여 빠르게 검색

McAfee Enterprise Log Search를 배포하는 경우 위협 대응에 일반적으로 6가지 유형의 로그를 사용할 수 있습니다. 이러한 로그는 보안 사고에 대한 특정 통찰력 및 컨텍스트를 제공할 수 있습니다.

로그 유형	일반적으로 사용 가능한 데이터
DNS 로그	▪ 쿼리되는 도메인 이름 ▪ DNS 쿼리의 소스 IP 주소 ▪ DNS 쿼리의 성공 또는 실패 ▪ 쿼리가 성공한 경우 확인된 IP 주소 ▪ TTL 응답 값 ▪ 사용된 DNS 서버
프록시 로그	▪ 연결 중인 도메인/IP 주소 ▪ 전송된 바이트 ▪ 연결 타임스탬프 ▪ 사용 중인 URI ▪ 참조 페이지 ▪ 사용자 에이전트 문자열
SMTP 로그	▪ 이메일 보낸 사람 도메인 ▪ 이메일 제목 ▪ 보낸 사람 IP 주소
Windows 로그	▪ Windows 보안 로그 이벤트 ▪ Windows 응용프로그램 로그 이벤트 ▪ Windows 시스템 로그 이벤트 ▪ Windows 코드 무결성 로그 이벤트
DHCP 로그	▪ 소스 MAC 주소 ▪ 제공된 IP 주소 ▪ 임대 기간 ▪ 요청 타임스탬프 및 임대 허가
VPN 로그	▪ 소스 IP 주소 ▪ 인증 ID ▪ VPN 연결 설정 타임스탬프 ▪ 연결 유형: 재개 또는 신규 ▪ 실패한 인증 시도(있는 경우) 및 해당 ID

자세히 알아보기

자세한 내용을 보려면 **https://www.mcafee.com/enterprise/ko-kr/products/siem-products.html**을 방문하십시오.

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