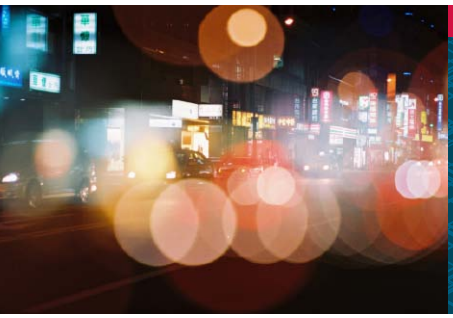

SIEM: 더 큰 비즈니스 문제를 해결하는 다섯 가지 요구 사항

SIEM(보안 정보 및 이벤트 관리) 솔루션이 실제 작업 환경에서 10년 이상 구현되면서 이제 보편적 솔루션으로 인정받고 있습니다. 이벤트 수집, 상관 관계, 알림, 필수 규정 컴플라이언스 입증과 같은 기능이 기본적으로 탑재되어 있으며, 대부분의 SIEM 솔루션은 이러한 요구 사항을 해결합니다. 하지만 환경이 변화하고 있습니다. 조직은 표적 공격, 지속적 공격과 같은 새로운 위협에 직면하고 있고, 모바일, 클라우드, 가상화와 같은 새로운 추세가 나타나고 있으며, 고객 확보, 운영 효율성, 비용 절감에서 비즈니스 우선 순위가 변화하고 있습니다. 그 결과 SIEM 사용 사례에는 더 큰 비즈니스 문제를 해결할 수 있는 진화된 기능이 필요합니다.

McAfee는 SIEM 사용자와 이야기하면서 SIEM에서 가장 큰 문제가 무엇인지에 대해 질문했습니다. 사용자들이 가장 중요하게 지적한 다섯 가지 문제는 다음과 같습니다.

- 빅 데이터 보안
- 상황 인식
- 실시간 컨텍스트
- 관리 용이성
- 통합 보안

SIEM에서 특히 사용자가 위협을 완화시키거나, 추세를 따르거나, 비즈니스 우선 순위에 맞추는 데 있어 보안 및 위험 관리 전략을 더욱 효과적으로 지원하려면 이러한 다섯 가지 문제를 해결해야 합니다. 각 문제는 해당 고객 사례 연구 및 사용 사례와 함께 설명합니다.

사용 사례: 빅 데이터 보안

- 더 많은 소스에서 더 많은 피드를 사용하여 데이터 캡처 확장
- 매우 많은 데이터 세트에서 분석 및 포렌식 수행
- 빅 데이터 보안의 속도 및 볼륨 요구 사항을 위해 최적화
- 직원 및 프로세스 효율성 향상

1. 빅 데이터 보안

빅 데이터 보안을 사용할 수 있다면 그 가치가 어마어마할 수 있습니다. 레거시 SIEM 솔루션은 많은 수의 엔드포인트, 네트워크 및 데이터 소스와 통합하도록 설계되지 않았고 높은 이벤트 속도를 처리하거나 장기간 보존 정책을 유지하는 목적도 없었습니다. 그 결과, 관계형 데이터베이스와 원래 네트워크 중심 이벤트를 사용하여 설계된 유사 레거시 SIEM의 단점으로 인해 오늘날 동적 IT 인프라의 보안 요구 사항을 충족하지 않습니다. 즉, 효과적이고 사용하기 용이한 속도와 확장성이 없는 것입니다.

사례 연구: 연방 정부

한 대규모 정부 기관은 SIEM의 수 페타바이트 관계형 데이터베이스 안에 저장된 빅 데이터 보안에 첨단 분석 기능을 적용하는 데 관심을 갖고 있었습니다. 하지만 간단한 보고서를 작성하는 데만도 몇 시간 혹은 며칠이 걸리는 경우도 있어서 해당 기관의 SIEM으로는 포렌식을 수행할 수 없었습니다.

McAfee® Enterprise Security Manager를 SIEM 솔루션으로 전환한 이후, 통합 장치의 수와 종류를 확장할 수 있었고 분석 기능에 데이터 및 사용자 중심 컨텍스트를 추가할 수 있었습니다. 이를 통해 정부 기관은 이벤트 속도와 저장된 데이터도 증가시킬 수 있었습니다. 이제 보고서를 몇 분 이내에 렌더링할 수 있어 포렌식 분석에 대한 전체적 접근 방식이 향상되었습니다.

사용 사례: 상황 인식
- 더 많은 ID 솔루션으로 상황 인식 보강
- 사람, 시기, 방법, 위치, 대상 확인
- 기간, 기타 사용자, 기타 대상 이해
- 랩톱, 스마트폰 등의 BYOD 자산 포함

2. 상황 인식

과거의 SIEM은 방화벽과 침입 탐지 시스템에서 이벤트 상관 관계를 분석하고 약간의 취약성 평가 데이터를 적용하는 데 지나지 않았던 단순한 도구였습니다. 현재에도 주로 네트워크 흐름 데이터에만 의존하는 SIEM이 있습니다. 물론 이러한 소스도 모두 중요하지만 응용프로그램, 데이터 컨텍스트, ID 정보로 SIEM을 보강해야 합니다. 그렇지 않을 경우, 실행 가능하고 시기 적절한 상황 정보가 포함된 이벤트를 이해하고 우선 순위를 정하는 데 더 많은 시간과 리소스가 필요합니다.

사례 연구: 의료 기관

지역 의료 기관에서 직원 민첩성을 높이기 위해 개인 태블릿을 사용할 수 있도록 지원하는 BYOD(Bring Your Own Device) 개념을 도입했습니다. 하지만 과거의 사건으로 인해 내부자 남용에 대해 우려하고 있었습니다. 이 의료 기관의 이전 SIEM 솔루션에는 장치(랩톱, 데스크톱, 태블릿, 가상 데스크톱)에 관계없이 중요한 데이터와 상호 작용하는 사용자를 파악하는 기능이 없었습니다.

McAfee Enterprise Security Manager를 사용하면서 ID 및 이동성 관리, Active Directory, LDAP 제품과 연결하여 사용자 및 장치 인식 기능을 확보했습니다. 기본 데이터베이스 지원과 같이 구조화된 데이터 저장소 및 구조화되지 않은 데이터 저장소와 통합되었고, DLP(데이터 손실 방지) 및 DAM(데이터베이스 활동 모니터링)과 통합되어 상황 인식은 더 완전해지고 내부자 위협은 완화되었습니다.

사용 사례: 실시간 컨텍스트
- 환경 안팎의 위협 이해
- 실시간 컨텍스트를 사용하여 SIEM 인텔리전스 향상
- 사고 식별 및 응답 시간 단축
- 추가 보안 정보 입력으로 위협 식별 및 우선 순위 결정

3. 실시간 컨텍스트

초기 SIEM 사용 사례 중 하나는 로그 관리, 즉 수집, 저장, 쿼리와 몇 가지 부가 기능이었습니다. 로그는 지금도 SIEM의 기본 구성 요소이지만, 오늘날의 SIEM에는 실시간 컨텍스트도 필요합니다.

그러한 컨텍스트의 예로는 McAfee GTI(McAfee Global Threat Intelligence)와 McAfee Vulnerability Manager가 있습니다. McAfee GTI는 실시간, 클라우드 기반 평판 서비스를 제공하며 McAfee Vulnerability Manager는 자산 취약성에 대한 조직 정보를 수집합니다.

사례 연구: 소매업체

포춘지 선정 100대 소매업체 중 SIEM과 McAfee 솔루션을 사용하지 않는 소매업체 한 곳을 대상으로 개념 증명을 수행했습니다. 이 소매업체는 첫째 주 동안 해당 네트워크에 들어오려고 시도하는 트래픽의 30% 이상이 악성 소스이거나 악성 페이로드가 포함되어 있었고, 두 가지 모두에 해당되는 경우도 있음을 발견했습니다.

McAfee Enterprise Security Manager를 사용하여 이벤트 정보와 McAfee GTI의 상관 관계를 분석하면서, 모든 매장과 데이터 센터에서 표적의 대상이 되고 있는 자산을 빠르게 식별하고 조직을 표적으로 하는 공격의 유형을 더 잘 이해할 수 있게 되었습니다. McAfee SIEM 솔루션은 최고 수준의 심각도를 판단한 다음 대응 우선 순위를 정했습니다. SIEM과 실시간 컨텍스트를 결합함으로써 더욱 빠른 위협 탐지, 우선 순위 지정, 교정이 가능해졌습니다.

사용 사례: 관리 용이성
- 동적 화이트리스트 및 하드웨어 지원 보안이 포함된 SIEM을 배포하여 고정 기능 장치 보호
- 사용자 지정 드릴다운으로 포렌식 간소화
- SIEM에 방화벽 및 IPS(침입 방지 시스템)를 통합하여 빠른 사고 응답 구현
- 향상된 보안으로 레거시 자산의 사용 기간 연장

4. 관리 용이성

레거시 SIEM의 아키텍처는 매우 경직되어 있으며 몇 가지 핵심 기능이 없습니다. 예를 들어, 지원되지 않는 이전 장치와 쉽게 통합되지 않아 정보를 유용하게 활용할 수 없습니다. 반면 차세대 SIEM은 쉽게 사용자 지정이 가능하며 특정 환경에 유연하게 맞출 수 있습니다. 바로 이러한 이유 때문에 많은 조직에서 SIEM을 차세대 전략으로 생각하고 있습니다.

사례 연구: 전기 회사

대규모 전기 회사가 Stuxnet 유형의 공격으로 인프라에 피해를 입고 수백만 명의 고객에게 정전 피해가 발생하지 않도록 보안 통제를 채택해야 했습니다. 이 전기 회사는 McAfee Enterprise Security Manager를 사용하여 기업 IT, SCADA, ICS(산업 제어 시스템) 영역에서 상황 인식을 달성하고 기본 장치, 응용프로그램, 프로토콜을 지원했습니다.

McAfee SIEM은 고객이 SCADA 및 ICS 장치와 사용자 지정 통합을 수행할 수 있는 도구를 제공했습니다. 그 결과 세 영역 전체에서 상관 관계, 이상 탐지, 추세 분석을 수행할 수 있게 되었습니다. 고객은 사용자 지정 이벤트 수집 외에도 고유한 대시보드, 보고서, 상관 관계 규칙, 알림을 쉽고 빠르게 구축했습니다. 따라서 SIEM을 보안, 필수 규정 컴플라이언스 입증, 자산 가용성에서 중요한 도구로 활용하여 정전 사고를 방지했습니다.

사용 사례: 통합 보안
- 보안 및 운영 워크플로 간소화
- 자동화 및 간편한 사용자 지정으로 복잡성 간소화
- 연동하는 보안 솔루션으로 가시성 및 상황 인식 향상
- 인텔리전스 및 통합으로 보안 향상

5. 통합 보안

SIEM은 전략적 보안 이니셔티브의 중요한 구성 요소이지만, 많은 보안 이니셔티브 중의 하나일 뿐입니다. 보안 및 컴플라이언스에서 통합된 솔루션은 개별 솔루션만 제공하는 경우에 비해 더 많은 기능을 제공할 수 있는 반면, 통합되지 않은 아키텍처는 복잡성만 가중시킵니다. 보안이 전략화되고 비즈니스 우선 순위에 따라 연계되는 대신, 전술적인 상태로 남는 이유는 대부분이 복잡성 때문입니다.

사례 연구: 재무 서비스

다국적 은행 고객이 다양한 공급업체의 개별 제품을 다량 소유하고 있었습니다. 일부 제품은 사용 중이었지만, 제한된 리소스로 인해 많은 제품을 정기적으로 사용 또는 유지 보수하지 않았습니다. 이 은행은 SIEM과 함께 통합 엔드포인트, 네트워크, 데이터 컨트롤을 활용하여 더욱 효과적으로 위험을 완화시키고 비용을 줄이는 동시에 보안을 비즈니스와 관련시킬 수 있을 것으로 판단했습니다.

이 은행은 공급업체 수를 줄이고 규모의 경제를 달성했으며 교육 비용과 에이전트, 콘솔, 서버 등의 수를 줄임으로써 계약 비용과 관련 비용을 몇 배 더 절감할 수 있었습니다. 비용 절감 외에도, 이 은행은 모든 기존 및 미래 솔루션을 McAfee Enterprise Security Manager와 완벽히 통합하여 보안 상황을 더 효과적으로 제어 및 확인할 수 있게 되었습니다.

주요 고려 사항

- 빅 데이터 보안이 제공하는 수집, 저장, 액세스, 처리 및 분석 문제를 쉽게 처리하는 능력이 얼마나 중요한가?
- 보안 이해 관계자들이 정보에 기반한 의사결정을 내리고 시기 적절한 작업을 수행해야 할 때 필요한 정보를 얻고 있는가?
- 보안 팀이 위협과 공격으로 인한 피해를 입기 전에 위협과 공격을 식별하는 데 필요한 실시간 컨텍스트가 있는가?
- 직관적 드릴다운 및 쉽게 사용자 지정 가능한 보기가 포함된 SIEM를 사용할 경우 보안 및 리소스에 어떤 영향을 미칠 것인가?
- 인프라 통합을 통해 보안, 가시성, 프로세스, 응답성을 어떻게 향상시킬 수 있는가?

지난 10년 동안에는 레거시 SIEM만으로 충분했던 솔루션이 오늘날의 요구 사항은 해결하지 못합니다. 빅 데이터, 보안 인텔리전스, 상황 인식, 성능, 이용 편의성, 통합에 대한 새로운 요구 사항에 대한 SIEM 사용 사례가 확장되었습니다. SIEM 솔루션은 복잡성을 새로 만드는 것이 아니라, 줄여야 합니다. SIEM에서 더 많은 것을 기대하십시오.

오늘날 SIEM은 더 크고 서로 연결되어 있으며 보안과 비즈니스 우선 순위가 정렬되어 있는 보안 프레임워크의 일부로 작동해야 합니다. SIEM은 보안을 더욱 전략화하고 실질적 비즈니스 가치를 제공하는 데 중요한 역할을 합니다.

McAfee의 SIEM 솔루션에 대해 자세히 알아보려면 www.mcafee.com/kr/products/siem/index.aspx를 방문하십시오.

Security Connected

McAfee의 Security Connected 플랫폼은 수백 개의 제품, 서비스, 파트너를 위한 공통 프레임워크를 제공하여 서로 학습하고, 컨텍스트별 데이터를 실시간으로 공유하며, 팀으로 활동하여 정보와 네트워크를 안전하게 보호합니다. 모든 조직이 이 플랫폼의 혁신적 개념, 최적화된 프로세스, 실용적 절감을 통해 보안 상태를 개선하고 운영 비용을 최소화할 수 있습니다.

McAfee
An Intel Company

한국맥아피(주)
서울특별시 강남구 역삼동 737
강남파이낸스센터 5층 135-984
+82.2.3458.9800
www.mcafee.com/kr

McAfee 및 McAfee 로고는 미국 및 기타 국가에서 McAfee, Inc. 또는 자회사의 등록 상표 또는 상표입니다. 기타 이름 및 브랜드는 각 소유자의 재산으로 주장될 수 있습니다. 이 문서의 제품 계획, 사양 및 설명은 정보용으로만 제공되고, 사전 통보 없이 변경될 수 있으며, 어떤 종류의 명시적 또는 암시적 보증도 없이 제공됩니다. Copyright © 2014 McAfee, Inc.
61099brf_focus-5-siem_0514_fnl_ETMG