IBM Security QRadar SIEM

통합 분석 보고 시스템을 통해 위협에 대한 보안 및 컴플라이언스 극대화

중점 사항

- 공통 데이터베이스 및 공유 대시보드 사용자 인터페이스로 로그 관리 및 네트워크 위협 보호 기술 통합
- 수천여 건에 달하는 보안 이벤트를 관리가 용이한 수상한 위협 목록으로 축소
- 장기적인 악성 코드 감지 및 추적을 통해 타 보안 솔루션으로 종종 놓칠 수 있는 최악의 위협 감지
- 고급 기능을 통한 내부 사기 감지
- 규제 의무 준수 및 컴플라이언스 지원

오늘날 네트워크는 과거 그 어느 때보다 더 광범위하고 복잡해져 악성 코드로부터 이러한 네트워크를 보호하는 일은 끝없는 과제입니다. 지적 자산 및 고객 정보를 보호하고 비즈니스 연속성을 모색하는 기업들은 단순히 로그 및 네트워크 데이터를 모니터링하는 데 그칠 것이 아니라 고급 툴을 활용하여 생산적인 방식으로 이러한 액티비티를 감지할 수 있어야 합니다. IBM® Security QRadar® SIEM은 사내 보안 운영 센터의 주요 솔루션으로써 수 년 동안 축적된 네트워크 데이터를 수집 및 정규화하고 상관 관계를 수행할 수 있습니다. 그 결과 보안 인텔리전스를 실현할 수 있는 것입니다.

이 제품의 중심에는 실시간 로그 이벤트 및 네트워크 데이터 캡처를 통해 잠재적 해커 공격에 대한 추적을 제공하는 확장형 데이터베이스가 탑재되어 있습니다. QRadar SIEM은 네트워크에 분산된 수천여 대의 장치에서 수집된 로그 소스 이벤트 데이터를 통합하여 모든 액티비티를 기본 형식으로 저장한 다음 잘못된 오류로부터 실제 위협을 식별하기 위해 상관 관계 활동을 즉시 수행하는 엔터프라이즈 솔루션을 말합니다. 이 솔루션은 딥 패킷 인스펙션(Deep Packet Inspection) 기술을 통해 특히 레이어 7 애플리케이션 페이로드 등 레이어 4 네트워크 데이터를 캡처합니다.

모든 QRadar 제품 구성 요소에 걸쳐 공유되는 직관적 사용자 인터페이스는 IT 담당자가 네트워크 공격을 재빨리 등급별로 식별하여 최소화하고, 수백여 건에 달하는 익명 액티비티에 대한 경고 및 패턴을 이상 목록으로 축소하여 더 이상 검사가 필요하지 않게 해줍니다.

위협 감지 및 우선순위화를 위한 실시간 가시성 제공

QRadar SIEM은 전체 IT 인프라에 걸쳐 컨텍스트 및 실행 가능한 감시를 제공함으로써 기업이 타 보안 솔루션으로는 종종 놓칠 수 있는 위협을 감지하고 최소화할 수 있게 지원합니다. 이러한 위협으로는 승인되지 않은 애플리케이션 사용, 내부 사기 및 수백여 건의 이벤트 "노이즈"로 쉽게 잊혀지기 쉬운 "잠재적 성향"을 지닌 악성 코드가 있습니다.

QRadar SIEM으로 수집할 수 있는 정보는 다음과 같습니다.

- **보안 이벤트:** 이벤트 및 방화벽, 가상 프라이빗 네트워크, 침입 감지 시스템, 침입 방지 시스템 등
- **네트워크 이벤트:** 스위처, 라우터, 서버, 호스트 등에서 감지되는 이벤트
- **네트워크 액티비티 컨텍스트:** 네트워크 및 애플리케이션 트래픽에서 감지되는 레이어 7 애플리케이션 컨텍스트
- **사용자 또는 액세스 컨텍스트:** ID, 액세스 관리 제품 및 취약성 스캔 장치에서 수집되는 컨텍스트 데이터
- **운영 체제 정보:** 네트워크 자산별 공급업체 이름 및 버전 번호
- **애플리케이션 로그:** ERP, 워크플로우, 애플리케이션 데이터베이스, 관리 플랫폼 등

감시 사항을 현재 위협으로 집중하기 위한 경고 건수의 감소 및 우선순위화

하루에 수백 또는 수십억 건에 달하는 이벤트를 만드는 기업들이 많이 있습니다. 이러한 데이터를 위협별 우선순위로 짧게 나누어 관리하는 일은 벅찬 과제입니다. QRadar SIEM은 대부분의 네트워크 로그 소스 장치를 검색하여 네트워크 데이터를 감시하고 네트워크에서 유효한 호스트 및 서버(자산)을 분류하여 사용 중인 애플리케이션, 프로토콜, 서비스 및 포트를 추적합니다. 또한 데이터를 수집, 저장 및 분석하여 위협 감지 및 컴플라이언스 보고 및 감사에서 사용할 이벤트에 대한 실시간 상관 관계를 수행합니다. 이렇게 수십억 건의 이벤트 및 데이터 흐름을 축소하여 비즈니스 적용 여부에 따라 현재의 위협을 우선순위별로 분류할 수 있습니다.

보안 전문가는 솔루션 설치 후 몇 주가 아닌 단 몇 일 이내에 QRadar SIEM이 주는 진정한 가치를 느끼기 시작하게 되며, 값 비싼 컨설턴트들을 고용하지 않고도 구축할 수 있습니다. 자동 검색 기능 및 사전 제공 템플리트 및 필터는 더 일반화된 IT 운영 툴을 통해 시스템에게 사내 시스템 환경을 일일이 알려주는 데 시간을 허비하지 않아도 됨을 의미합니다. 이 아키텍처는 하드웨어 기반 소프트웨어 전용 또는 가상 소프트웨어 어플라이언스로 제공되는 다수의 이벤트 프로세서 어플라이언스, 이벤트 컬렉터 어플라이언스, 플로우 프로세서 어플라이언스 및 중앙 콘솔로 구성된 모델을 도입한 것입니다. 더 소형화된 설비로 단일 올인원 솔루션을 시작할 수 있으며 필요에 따라 이벤트 및 플로우 프로세서 어플라이언스를 추가하여 콘솔 배치로 쉽게 업그레이드할 수 있습니다.

QRadar SIEM은 사전 제공된 고객별 룰을 기반으로 다양한 피드에 걸쳐 데이터를 캡처하여 위협을 관리 가능한 목록으로 축소해 줍니다.

위협 관리 효율성 극대화를 위한 과제 해결

보안 담당 부서는 잠재적 위협의 특성을 완전히 파악하기 위해 다음과 같은 주요 과제를 해결해야 합니다. 즉, 공격 대상, 비즈니스에 미치는 영향, 감시 대상 등 입니다. QRadar SIEM은 중요 인시던트 및 위협을 추적하고 지원 데이터 및 관련 정보에 대한 이력을 구현합니다. 공격 목표, 시점, 자산 가치, 취약성 상태, 사용자 ID 위협, 해커 프로파일, 기존 위협 중 현재 진행 중인 위협 및 레코드 등의 세부 정보는 모두 필요에 따라 인텔리전스를 사용할 수 있도록 보안 담당 부서원들에게 전달됩니다.

이벤트 및 흐름 데이터 분석 및 조사를 위한 위치 기반 실시간과 이력 검색은 액티비티 평가 및 인시던트 해결을 위한 기업의 역량을 극대화시킬 수 있습니다. 사용자들은 사용하기 쉬운 대시보드, 시계열 뷰, 드릴다운 검색, 패킷 레벨 콘텐츠 시각화 및 수백여 건의 사전 검색을 통해 데이터를 빨리 수집하여 이상 성향 및 기여도가 가장 높은 액티비티를 요약 및 파악할 수 있습니다. 또한 지역별로 대규모 분산 환경에 걸쳐 통합 검색을 수행할 수 있습니다.

애플리케이션 가시화 및 이상 성향 감지

QRadar SIEM은 애플리케이션, 호스트, 서버 및 네트워크 영역에 영향을 미치는 성향의 변화를 파악하기 위해 다양한 이상 성향 감지 기능을 지원합니다. 예를 들어 QRadar SIEM은 업무 외 시간 또는 장시간 애플리케이션 및 클라우드 기반 서비스의 사용 여부 및 이력 프로파일의 평균 이동 및 계절별 이용 패턴 등 네트워크 액티비티 패턴을 감지합니다. QRadar SIEM은 이러한 매일 및 주 단위 사용 프로파일을 인식하도록 학습하면서 IT 담당자들이 주요 편차를 빨리 파악할 수 있게 지원합니다.

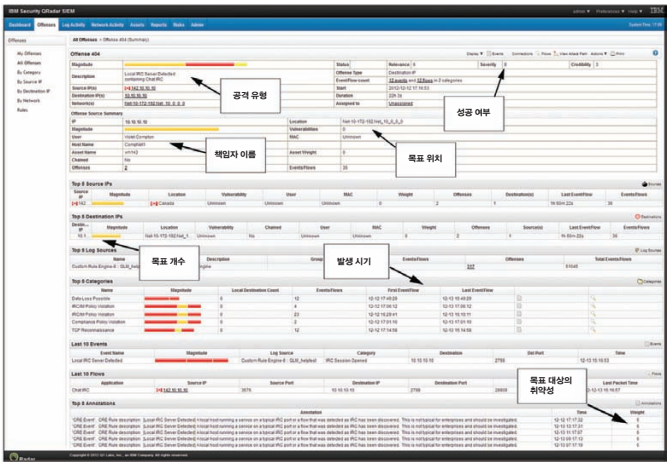
QRadar SIEM의 중앙집중식 데이터데이스는 로그 소스 이벤트 및 네트워크 트래픽을 하나로 저장하여 IP 소스에서 발생되는 양방향 네트워크 액티비티와 각각의 이벤트의 상관 관계를 연결합니다. 또한 저장소 용량을 절약하고 라이센스 요구 사항을 충족하기 위해 네트워크 트래픽을 그룹화하여 짧은 시간 내에 발생하는 작업을 단일 데이터베이스 항목으로 기록할 수 있습니다.

레이어 7에서 애플리케이션 트래픽을 감지할 수 있는 능력은 QRadar SIEM을 통해 사내 네트워크에 대한 정책, 위협 및 일반 네트워크 액티비티 모니터링을 정확히 분석하고 이에 대한 통찰을 제공할 수 있도록 지원합니다. QRadar SIEM은 IBM Security QRadar QFlow 또는 VFlow Collector 어플라이언스를 추가함으로써 네트워크에서 ERP, 데이터베이스, Skype, VoIP(Voice over IP) 및 소셜 미디어 등의 애플리케이션 사용을 모니터링할 수 있습니다. 여기에는 사용자와 사용 항목에 대한 통찰, 콘텐트 전송에 대한 분석 및 경고, 그리고 데이터 전송의 적절성 및 이용 패턴 초과 여부를 나타내는 기타 네트워크 및 로그 액티비티와의 상관 관계가 포함됩니다. QRadar SIEM은 출고 과정에서 다양한 이상 성향 감지 룰과 함께 제공되지만 보안 담당 부서가 직접 필터링 기능을 만들어 시간별 데이터에 대해 이상 성향 감지 여부를 적용할 수 있습니다.

직관적인 단일 콘솔 보안 솔루션 통제

QRadar SIEM은 부서별로 롤(Role) 기반 액세스와 실시간 분석, 인시던트 관리 및 보고에 대한 글로벌 뷰를 제공하는 중앙집중식 사용자 인터페이스를 통해 기업 보안 운영 센터를 위한 탄탄한 기반을 제공합니다. 보안, 네트워크 액티비티, 애플리케이션 액티비티, 시스템 모니터링 및 컴플라이언스 등 5개의 기본 대시보드도 제공하므로 사용자가 자신만의 작업 공간을 맞춤화하여 구성할 수 있습니다.

이 대시보드는 공격 시작의 징후를 알리는 경고 액티비티에 발생하는 스파이크를 쉽게 파악할 수 있게 해줍니다. 그래프를 클릭하면 보안 부서원들이 수상한 위협과 비교하여 강조 표시된 이벤트 또는 네트워크 흐름을 빨리 확인할 수 있게 해주는 드릴다운 기능이 시작됩니다. 뿐만 아니라, 빠른 시간 내에서 보고서를 작성할 수 있도록 특정 롤(Role), 장치, 컴플라이언스 규제 및 산업별로 준비된 수백여 개의 템플리트가 제공됩니다.



QRadar SIEM은 수상한 위협 속에 숨겨진 다양한 요인들에 대한 세부 정보와 기존 룰 튜닝 및 잘못된 오류를 최소화하기 위한 새로운 룰 추가 기능을 제공합니다.

가상 환경에서의 위협 보안

가상 서버는 물리적 서버처럼 보안에 매우 취약하기 때문에 포괄적인 보안 인텔리전스 솔루션이라면 가상 데이터 센터에 상주하는 애플리케이션 및 데이터를 보호하기 위한 적절한 기준이 있어야 합니다. IT 전문가들은 QRadar VFlow Collector 어플라이언스를 사용하여 가상 네트워크에서 발생하는 엄청난 양의 비즈니스 애플리케이션 액티비티에 대한 가시성을 극대화합니다. 또한 이들 애플리케이션이 보안 모니터링,

애플리케이션 레이어 성향 분석 및 이상 성향 감지용으로 사용되는지 파악할 수 있습니다. 작업자들은 보안 및 정책을 더 깊이 조사하기 위해 애플리케이션 콘텐츠를 캡처하기도 합니다.

컴플라이언스 관리를 위한 세부 데이터 액세스 및 사용자 액티비티 보고서 작성

QRadar SIEM은 기업에게 없어서는 안될 규제 의무 준수 및 컴플라이언스에 따른 보고의 투명성, 권한 및 평가 능력을 제공합니다. 감시 피드를 연결하고 통합하는 이 솔루션의 기능은 감사자들에게 IT 리스크에 대한 완전한 표준형 보고 방식과 산업 규제 요구 사항을 충족하기 위해 수백여 개에 달하는 보고서 및 룰 템플리트를 제공합니다.

기업은 자동 업데이트를 통해 최신 정책, 규제 및 모범 사례를 포함하는 QRadar SIEM의 확장 기능을 활용하여 컴플라이언스 기반 IT 보안 요구 사항을 효율적으로 충족할 수 있습니다. 또한 모든 네트워크 자산 프로파일을 HIPAA(Health Insurance Portability and Accountability Act) 컴플라이언스 감사에 영향을 받는 서버 등 비즈니스 기능에 따라 그룹화할 수 있습니다.

이 솔루션에 내장된 대시보드, 보고서 및 룰(Rule) 템플리트는 CobiT, SOX, GLBA, NERC/FERC, FISMA, PCI DSS, HIPAA, UK GSi/GCSx, GPG 등의 규제 및 컨트롤 프레임워크에 맞게 고안된 것입니다.

고가용성 및 재난 복구 기능 추가

고가용성 및 재난 복구 기능을 실현하기 위해 QRadar 어플라이언스 제품군에 해당하는 모든 멤버와 유사 보조 시스템을 페어링할 수 있습니다. 이벤트 프로세스 어플라이언스부터, 플로우 프로세서 어플라이언스를 거쳐 올인원 및 콘솔 SIEM 어플라이언스에 이르기까지 사용자들은 운영 연속성을 보장하기 위해 언제 어디서나 안정성과 보호 기능을 추가할 수 있습니다.

비즈니스 탄력성을 모색하는 기업의 경우 QRadar의 고가용성 솔루션은 자동 통합 장애 복구 및 시스템 사이에 완전한 디스크 동기화를 제공합니다. 이 솔루션은 아키텍처 관점에서 유연한 플러그 앤 플레이 어플라이언스를 통해 쉽게 구축할 수 있으므로 타사 오류 관리 제품을 추가로 설치하지 않아도 됩니다.

데이터 보호 및 복구를 모색하는 기업의 경우 QRadar의 재난 복구 솔루션은 주 QRadar 시스템에서 다른 시설에 있는 보조 병렬 시스템으로 라이브 데이터(예: 흐름 및 이벤트)를 전송합니다.

취약성에 대한 프로파일링

IBM Security QRadar Risk Manager는 네트워크에서 가장 취약한 자산을 확인하여 QRadar SIEM을 보완합니다. 또한 이 시스템이 자신에게 잠재적으로 노출되는 액티비티에 관여할 경우 경고를 생성합니다. 예를 들어, 기업은 패치되지 않은 애플리케이션, 장치 및 시스템에 대한 사내 네트워크를 스캔하고, 인터넷에 연결된 네트워크를 결정하여 각 애플리케이션에 대한 리스크 프로파일을 기반으로 우선순위를 조정할 수 있습니다. 자세한 정보는 QRadar Risk Manager 데이터 시트를 참조하시기 바랍니다.

네트워크 이벤트 및 흐름 캡처를 위한 포괄적 장치 지원 수용

QRadar SIEM은 거의 모든 벤더가 제공하고 엔터프라이즈 네트워크에 배치되는 450여 개의 제품 지원과 함께 네트워크 솔루션, 보안 솔루션, 서버, 호스트, 운영 체제 및 애플리케이션 등 다양한 시스템에 걸쳐 데이터 수집, 분석 및 상관 관계 연결을 제공합니다. 또한 QRadar SIEM은 IBM 및 타 공급업체가 제공하는 독자적 애플리케이션 및 최신 시스템을 지원하기 위해 쉽게 확장이 가능합니다.

왜 IBM인가?

IBM은 세계에서 가장 폭넓은 보안 리서치, 개발 및 구축 능력을 제공하는 기업입니다. IBM 솔루션은 기업이 자사의 보안 취약성을 최소화하고 성공적인 전략적 이니셔티브에 집중할 수 있도록 권한을 부여합니다.

추가 정보

IBM Security QRadar SIEM으로 어떻게 기업의 위협 관리 및 컴플라이언스 과제를 해결할 수 있는지 확인하려면 해당 지역의 IBM 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 다음 웹 사이트를 참조하십시오. **ibm.com**/security.

IBM Security 솔루션에 대하여

IBM Security는 가장 진보된 기업용 통합 보안 제품 및 서비스 포트폴리오 중 하나를 제공합니다. 세계적으로 유명한 IBM X-Force® 연구소가 지원하는 이 포트폴리오는 보안 인텔리전스를 통해 기업들이 전반적으로 자사 직원, 인프라, 데이터 및 애플리케이션을 보호할 수 있게 해주고 ID 및 액세스 관리, 데이터베이스 보안, 애플리케이션 개발, 리스크 관리, 엔드포인트 관리, 네트워크 보안 등을 위한 솔루션을 제공합니다. 또한 기업들이 리스크를 효과적으로 관리하고 모바일, 클라우드, 소셜 미디어 및 기타 엔터프라이즈 비즈니스 아키텍처에 대한 통합 보안을 구현할 수 있게 해줍니다. IBM은 세계에서 가장 폭넓은 보안 리서치, 개발 및 구축 능력을 제공하는 기업으로 매일 130여 개에 달하는 국가에서 130억 건의 보안 이벤트를 모니터링하고 3,000여 건에 달하는 특허를 가지고 있습니다.

추가적으로, IBM Global Financing은 가장 비용 효율적 방법과 전략적 방법으로 비즈니스에서 필요로 하는 소프트웨어 기능을 취득할 수 있도록 지원합니다. IBM은 신용 있는 고객과 협력하여 귀사의 비즈니스 및 개발 목표에 적합하고 효과적인 현금 관리를 가능하게 하며 귀사의 총소유 비용을 개선하는 맞춤형 재무 솔루션을 제공합니다. IBM Global Financing으로 중대한 IT 투자에 자본을 투입하고 귀사의 비즈니스를 발전시키십시오. 자세한 정보는 다음 웹사이트를 참조하시기 바랍니다. **ibm.com**/kr/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
2013년 1월

WGD03021-KRKO-00