한국아이비엠주식회사
(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩

TEL : (02)3781-7800
www.ibm.com/kr

2012년 6월

Printed in Korea

IBM Security Systems
QRadar 보안 인텔리전스 플랫폼

KR1CX03D

귀사의 보안, 어떠신가요?
보이는 부분은 빙산의 일각에 불과합니다

QRadar로 전체를
통합적이고 광범위하게
보안해야 할 때입니다

QRadar 보안 인텔리전스 플랫폼

IBM Security Systems

IBM Security Systems
QRadar 보안 인텔리전스 플랫폼

Contents

IBM, 보안 정보운용 소프트웨어 업체 'Q1 Labs' 인수

IBM 분석 포트폴리오의 보안 인텔리전스 향상

(2011년 10월 00일)_ IBM은 최근 고객사에 보다 효과적인 정보 보안 지원을 위해 보안정보 소프트웨어 공급 업체인 'Q1 랩(Q1 Labs)' 을 인수하기로 최종 계약했다고 발표했다.

Q1 랩은 네트워크, 애플리케이션, 사용내역, 모바일, 신분증 판독기 등 클라우드와 전통적 PC 환경 모두를 아우르는 다양한 소스 데이터로부터 보안 관련 정보를 수집하고 분석하는 소프트웨어 공급업체다. Q1 랩의 보안정보 및 사건관리(SIEM) 소프트웨어는 보안에 대한 통찰력과 조직의 포괄적인 위험 관리 현황 정보를 임직원에게 제공하면서 IT 담당자와 예산 관리자가 보안 사고에 대처하고 고객을 보다 효과적으로 보호할 수 있도록 위험 모델 추적 관리를 지원한다.

IBM은 Q1 랩의 고급 분석론을 고객의 핵심 보안 도메인에 적용함으로써 해당 조직에 총체적인 보안 대시 보드를 제공하고 각종 보안 위협 요인으로부터 고객사들이 보다 똑똑하게 데이터 보호하도록 지원할 방침이다. 또한, 승인되지 않은 정보에 무단으로 접근하는 등의 각종 위법행위를 방지하기 위해 기업 전체 적용할 보안 정책에 반하는 행위를 자동적으로 포착하고 경고할 수 있다.

IBM X-Force 2010 상반기 동향 및 리스크 보고서에서 강조된 바와 같이, 최근 모바일 보안에 대한 우려와 고급 보안 위협이 증가하면서 기업은 현재 상당한 보안 위협에 직면해 있다. 동시에 이러한 위협을 발견하고 내부 스파이 탐지, 사업 위험 예측 등 규제 권한을 다루는 장비를 갖추어야 할 필요성이 부각 되고 있다.

Q1 랩의 브랜든 해니건(Brendan Hannigan) CEO는 "방어선 내에서 대응하는 수준으로는 더 이상 모든 위협으로부터 안전할 수 없다" 며 "IBM은 보안 사고 후 대처하는 방식을 통합 예측 접근 방식으로 패러다임을 바꾸는 선도적인 위치에 있다" 고 밝혔다. 이어서 "IBM의 포괄적인 보안 포트폴리오와 Q1 랩의 보안정보 분석 역량을 융합하여 지속적으로 정보 보안 트렌드를 주도하고 차별화시킬 것" 이라고 덧붙였다.

IBM

1

QRadar
보안 인텔리전스 플랫폼

조직의 규모와 상관 없이 보안 인텔리전스에 대한 수요가 증가하고 있습니다. 법률 준수에 대한 의무가 강화되고 데이터 위협 및 위반은 끊임없이 조직에 과제를 안겨주고 있습니다. 이 모든 것들은 그 어느 때보다 증가하고 있는 사용자와 기기에 의해 생성된 엄청난 양의 데이터와 이벤트로 인해 더욱 심각해지고 있습니다. 이를 해결할 수 있는 새로운 방법을 찾아내지 않으면 보안 문제가 생길 수 있습니다.

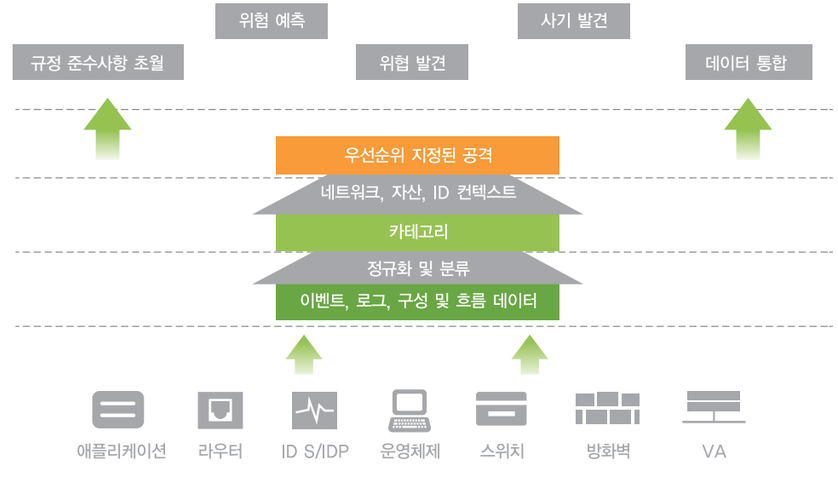
이제 보안 인텔리전스는 선택이 아닌 필수 입니다.

오늘날의 보안 과제에 대한 종합 인텔리전스 및 가시성

IBM Qradar Security Intelligence Platform(이하 Qradar)은 높은 가치를 지닌 비용 효율적인 차세대 보안 인텔리전스 플랫폼입니다. QRadar는 SIEM, 위험 관리, 로그 관리, 네트워크 행동 분석, 보안 이벤트 관리 등 서로 다른 기능을 하나의 종합 보안 인텔리전스 솔루션으로 통합한 제품으로, 가장 지능적인 자동화된 통합형 보안 인텔리전스 솔루션입니다. QRadar는 네트워크, 데이터 센터, 어플라이언스 등에 어떤 일이 벌어지고 있는지를 파악할 수 있도록 가시성을 사용자에게 제공하므로 규제사항을 준수하며 IT 자산을 보다 잘 보호할 수 있습니다.

전세계 1,600여 고객이 가장 지능적인 자동화된 통합형 보안 인텔리전스 솔루션으로 QRadar를 선택하였습니다. QRadar를 이용하면 다음과 같은 장점이 있습니다.

[종합 보안 인텔리전스 제공]



타제품이 찾아내지 못하는 위협 발견

인터넷 기반의 위협 및 사기가 점점 더 정교해지고 있습니다. 조직의 데이터 내에 인텔리전스가 숨겨져 있어 직원이 기업 소유의 정보를 빼내려는 시도나 신용카드 정보를 빼내기 위해 침투하려는 봇넷, 국제 스파이 행위 등 다양한 범위의 위험을 발견할 수 있습니다. QRadar는 최우선순위의 공격을 파악하여 기업의 데이터를 보호하고 사용자, 애플리케이션 및 네트워크 행동에서 잘못된 부분을 발견할 수 있도록 합니다.

데이터 통합

매일 엄청난 양의 레코드와 이벤트를 생성해내는 다수의 기업에는 기존 네트워크 장치를 통해 생성된 이벤트 및 로그 데이터 안에 수많은 정보가 존재합니다. 안타깝게도 이러한 정보는 대개 개별적으로 보존되며, 잊혀지기 쉬워 항상 충분히 활용되지 않습니다. QRadar는 기존에는 별개로 존재하던 네트워크, 보안, 인프라 운영을 하나의 실용적이고 확장 가능한 인텔리전스 플랫폼으로 수렴합니다. 이를 통해 조직에서는 중요한 내용에 대해 신속하게 대응할 수 있고, 네트워크 및 보안 정보를 ID 및 애플리케이션 인식 수준으로 낮춰 네트워크 위협과 정책 위반을 보다 효과적이고 보다 잘 해결할 수 있습니다.

내부 사기 발견

조직에 가장 큰 위협 중 일부는 내부에서 발생하며, 기업은 개인과 악의적인 행동을 정확하게 연결시키는데 필요한 인텔리전스가 부족한 경우가 많습니다. 사용자와 애플리케이션을 모니터링함으로써 정상적인 사용자 행동의 기준선을 지정하여 비정상적이거나 위험한 행동과 취약점을 파악하기 쉽습니다.

비즈니스에 대한 위험 예측

보안 및 IT 팀은 침해 행위가 실제로 발생하며, 그 어느 때보다 취약성의 범위가 커지고 있는 상황에서 위험을 보다 잘 관리해야 하는 어려움에 직면하고 있습니다. Qradar는 공격받는 도중 그리고 공격 이후 어떤 위험이 존재하는지 파악할 뿐 아니라, 공격받기 이전에 "what if?" 란 질문을 많이 하여 그 해답을 제시함으로써 운영 효율성을 높이고 네트워크 보안 위험을 줄일 수 있는 공격 전 솔루션을 제공합니다.

규정 준수사항 초월

Sarbanes- Oxley, HIPAA, PCI DSS, NERC 등의 사항을 준수하는데 있어 오늘날의 기업이 느끼는 부담은 점점 더 커지고 있습니다. 조직에서 생성되는 대량의 데이터와 이벤트는 감사 추적의 핵심입니다. QRadar는 모든 감시 피드를 수집하고, 상관관계를 파악 및 통합해 운영자를 위한 보다 정확한 데이터, 인시던트 대응 관리자를 위한 세분화된 범죄 수사, 그리고 감사자를 위한 보다 완전한 보고를 산출합니다.

지능화, 통합화 및 자동화

QRadar는 로그, 위협, 취약성 및 위험 관련 데이터를 수집하고 저장, 분석 및 쿼리하기 위한 통합된 아키텍처를 제공합니다. QRadar는 매우 지능적인 자동화된 통합 솔루션이므로 조직에서는 서로 다른 QRadar 모듈을 이용하여 운영자, 분석가, 감사자 등 다양한 역할과 요구사항을 가진 여러 부서와 직원을 보유함으로써 이익을 얻게 됩니다.

지능화

보다 많은 데이터를 감시하고 보다 지능적인 분석 기술을 이용하여 타 제품이 찾아내지 못하는 위협을 QRadar가 발견합니다. 이로써 타 제품에서는 실현할 수 없는 가시성을 제공합니다.

통합화

로그 관리, SIEM 및 위기 관리를 하나의 솔루션으로 통합하기 위해 새롭게 고안된 QRadar는 SIEM "인텔리전스" 를 손상시키지 않으면서 대량의 로그 관리 기능을 제공합니다.

- **모든 검색, 필터링, 규칙 작성 및 보고 기능을 위한 공동 플랫폼**
- **모든 로그 관리, 위기 모델링, 취약성 우선순위 지정, 인시던트 발견 및 영향 분석 작업을 위한 직관적 단일 사용자 인터페이스**

자동화

Qradar는 규정 준수 및 정책 기능과 함께 자동화된 보안 및 네트워크 장치 검색으로 배포와 관리가 간단합니다. QRadar는 지루한 검색을 자동화하고, 기존의 보안 인텔리전스 플랫폼에 심각한 손상을 주는 기능을 튜닝하여 치명적인 복잡성을 제거합니다.

2

차세대 SIEM을 위한 비즈니스 사례

네트워크 보안 인텔리전스에 대한 통합된 접근 방식으로 운영 효율성 제공 및 비용 절감

개요

가장 효과적인 IT 기술로 선정된 것은 모든 규모의 기업과 산업 전 분야에서 가장 우려하고 있는 기술입니다. 현 경제 상황에서 기업은 제한된 예산을 어떤 분야에 할당해야 이 불확실한 시대에 탄탄한 성공 기업으로 살아남을 수 있는지 그 우선순위를 정하는 어려운 작업을 수행해야 합니다.

이러한 고충을 가장 절실히 느끼고 있는 것은 중요한 네트워크 서비스와 애플리케이션을 제공하는 업체들입니다. 어려운 경제 상황에서도 이 업체들은 다음과 같은 다양한 요구사항을 충족시켜야 합니다.

- 점점 더 강화되고 늘어나는 규제 사항의 준수
- 계속해서 진화하는 위협으로부터 IT 자산 보호
- 기존 및 새로운 기술 솔루션에 대한 보안 관리 제공

따라서 기업은 경제적 측면을 우선시하는 어려운 선택을 해야 할 것이며, 솔루션 선택 시 전략적으로 판단해야 합니다.

[Discover Fraud]

규제 사항 준수에 대한 부담 증가

지난 몇 년간 규제 사항 준수에 대한 부담이 상당히 증가하였으며, 이는 모든 산업 분야에 영향을 미쳤습니다. 규제 사항의 항목은 많으며, 이를 준수하지 않을 경우 그 불이익은 상당합니다. 이와 같은 규제 사항들은 계속 진화하고 있으며, 기업 전반에 상당히 많은 영향을 미치고 있습니다. 규제 사항을 준수하지 않을 경우, 그 불이익은 산업 분야에 따라 달라집니다. 그러나 모든 산업 분야에 공통적인 사항은 규제 사항을 준수하지 않을 경우 순이익에 상당히 큰 영향을 미칠 수 있다는 사실입니다. 재정적 불이익과 내재하는 보안 위험은 수량화하기 쉬우므로 기업에서는 규제 사항을 준수하지 않을 경우 초래하는 위험과 비용에 대해 보다 절실히 인지하게 되었습니다. 일반적인 사회 통념으로는 기업이 "의무를 완수" 하고, 상식적인 통제를 통해 기업의 IT 자산을 보호하는 최선의 방법인 규제 사항을 준수하며, 중요 업무용 데이터에 대한 보호 방법을 구현할 것을 요구합니다.

도전 과제 1

[Threats found]

[IBM Qrader]

도전 과제 2

네트워크 위협의 증가

보안 전문가들은 기업 내부 및 외부의 위협으로 인한 위험이 점점 더 늘어나고 있다는 사실을 인지하고 있습니다. 뉴스에서는 심각한 침해 행위 배후에 존재하는 복잡하고 정교한 범죄 조직에 대해 보도하고 있으며, 지난 몇 년간 컴퓨터 기반 정보를 빼내는 데 소요되는 시간은 상상을 초월합니다. 그 결과 신용카드 데이터, 의료 정보, 전매 지적 재산 등을 비롯한 수많은 기밀 자료를 해킹하는 보안 침해 사례를 조사하고 대응하기 위해 상당한 금액을 투자하고 있습니다.

기업에서의 네트워크 보안 침해로 인해 파생된 문제는 지대한 영향을 미치고 있으며, 이를 해결하는데 상당한 비용이 소요됩니다. 따라서 기업은 신중히 판단해야 하며, 범죄 피해를 입지 않도록 네트워크를 공격하는 복잡하고 통합된 위협을 발견할 수 있는 능력을 제공할 적절한 보안 관리를 실행해야 합니다.

"CSO 매거진에서 실시한 2011 사이버 보안 감시 설문조사 (Cyber Security Watch Survey)에 따르면, 607 명의 응답자 중 58%가 네트워크 시스템 및 데이터에 대한 접근 권한이 없는 외부인으로 인한 공격이 가장 많았다고 답했으며, 21%가 접근 권한이 있는 내부인, 직원 및 계약자로 인한 공격이 가장 많았다고 응답했습니다. 그리고 33%의 응답자는 내부인의 공격으로 인한 손실이 더 크다고 답했습니다."

운영비의 지속적인 증가

IT 기업에게 주어진 과제는 네트워크가 계속 변화하고 있다는 사실입니다. 새로운 기술이 등장하고 낡은 기술은 사라집니다. 기업에서는 새로운 기술이 기업의 IT 보안 프로그램에 어떤 영향을 미칠지 평가해야 하며, 비즈니스에 요구되는 보안 요구사항을 충족시키는 적절한 관리가 이루어지도록 해야 합니다.

어려운 경제 상황에서 기업은 비즈니스에 요구되는 보안 요구사항을 충족하며 전체 비용까지 절감시키는 솔루션을 고려해야 합니다. 산업 리서치 전문업체인 IDC의 "2010 전세계 보안 프로그램 상위 10가지 제품 예측(Worldwide Security Products 2010 Top Ten Predictions)" 이란 보고서에 따르면, 시장의 핵심 동인은 서로 밀접하게 연관된 이슈 기술이나 SAAS, 클라우드, 가상화 그리고 모바일에 주력하는 것으로 예상합니다.

IDC의 보안 제품 및 서비스 담당 프로그램 부사장인 크리스찬 크리스티안센 (Christian Christiansen)은 "고객은 위협, 예산, 규제 사항 등으로 인해 점점 더 증가하고 있는 어려움을 해결하기 위한 유연한 보안 플랫폼을 요구합니다." 라고 말하면 다음과 같이 덧붙였습니다. "고객이 당면한 중요한 과제는 지나치게 많은 보안 솔루션 중 위험에 대해 유연하게 대처할 수 있는 보안 솔루션을 선택하는 것입니다."

확실히 기업은 새로운 기술을 인수하는데 있어 매우 까다롭게 선별해야 합니다. 앞서 말한 IDC 보고서에서 언급한 기술은 자동화된 보안 관리 기술입니다.

도전 과제 3

솔루션 1

보안 **인텔리전스**

"보안 인텔리전스" 는 기업의 모든 보안 데이터에서 유출한 수행 가능한 정보로 정확도를 높이고, 전체 보안 이벤트 타임라인을 통해 발견 및 보호에서 업데이트 관리까지 컨텍스트를 제공합니다.

Qradar는 전체 보안 인텔리전스 타임라인을 지원합니다. 가능한 공격을 신속히 파악하고, 이를 적절한 관리자에게 알려 공격을 중지하는 한편, 원인을 파악하기 위해 인시던트 대응 절차를 활성화하는 것이 필요합니다.

IBM Security Systems의 주요 제품인 QRadar는 SIEM, 로그 관리, 네트워크 행동 분석, 보안 이벤트 관리 등 서로 다른 기능을 하나의 종합 보안 인텔리전스 솔루션으로 통합한 제품으로, 가장 지능적인 자동화된 통합형 보안 인텔리전스 솔루션입니다. QRadar는 네트워크 및 데이터 센터, 어플라이언스 등에 어떤 일이 벌어지고 있는지를 파악할 수 있는 중요한 가시성을 사용자에게 제공하므로 규제 사항을 준수하며 IT 자산을 보다 잘 보호할 수 있습니다.

솔루션 2

지능화, 통합화 및 **자동화**

QRadar는 로그, 위협, 취약성, 위험 관련 데이터를 수집하고 저장, 분석 및 쿼리하기 위한 통합된 아키텍처를 제공합니다.

QRadar은 매우 지능적인 자동화된 통합형 솔루션이므로, 기업은 (운영자, 분석가, 감사자 등) 다양한 역할과 요구사항을 가진 여러 부서와 직원을 보유함으로써 이를 통해 다음과 같은 이익을 얻게 됩니다.

- **지능화:** QRadar는 보다 많은 데이터를 감시하고 보다 지능적인 분석 기술을 이용하므로, 타 제품이 찾아내지 못하는 위협을 발견합니다. 이처럼 타 제품에서 체험할 수 없는 가시성을 제공합니다.
- **통합화:** 로그 관리, SIEM 및 위기 관리를 하나의 솔루션으로 통합하기 위해 새롭게 고안된 QRadar는 SIEM "인텔리전스" 를 손상시키지 않으면서 대량의 로그 관리 기능을 제공합니다.
- **모든 검색, 필터링, 규칙 작성 및 보고 기능을 위한 공통 플랫폼**
- **모든 로그 관리, 위기 모델링, 취약성 우선순위 지정, 인시던트 발견 및 영향 분석 작업을 위한 직관적인 단일 사용자 인터페이스**
- **자동화:** Qradar는 규정 준수 및 정책 기능과 함께 자동화된 보안 및 네트워크 장치 검색으로 배포와 관리가 간단합니다. QRadar는 지루한 검색을 자동화하고, 기존의 보안 인텔리전스 플랫폼에 심각한 손상을 주는 기능을 튜닝하여 치명적인 복잡성을 제거합니다.

솔루션 3

규제 준수 관리·보안을 희생시키지 않는 발군의 **규제 준수 컨텐츠**

현재 환경에서 네트워크 및 보안 기술을 포괄하는 모니터링 및 관리 솔루션은 규제 준수 계획을 지원하고 입증하는데 핵심적 역할을 합니다.

QRadar는 기업과 단체, 정부 기관에 책임과 투명성 그리고 가측성을 제공합니다. 이러한 특징은 규제 사항 준수를 담당하는 IT 보안 프로그램이 성공적으로 임무를 수행하는데 중요한 사항입니다.

정책 또는 규제를 준수하는 것이 단계별로 차이가 있음을 이해하고 있기 때에 QRadar는 다음과 같은 특징을 제공합니다.

- **책임:** 누가 무엇을 언제 했는지 제공
- **투명성:** 보안 관리, 비즈니스 애플리케이션, 보호되고 있는 자산에 대한 가시성 제공
- **가측성:** 기업 내 위험에 대한 지표 및 보고

"S1의 목표는 PCI DSS 규제 사항을 준수하고, 유지관리에 너무 많은 비용이 드는 시스템을 교체하는 것이었습니다. 시간적인 제약이 심한 가운데 IBM의 QRadar 덕택에 S1에서는 효율적이고 간편하게 솔루션을 배포하고 구현할 수 있었습니다." – S1, Inc. 사례 연구

솔루션 4

위협 관리 – 다른 솔루션이 찾아내지 못하는 **복잡한 외부 공격 및 내부 사기 발견**

정보 중심 기업에서는 계속 진화하는 위협 보다 한 발 앞서기 위해 노력합니다.

기존의 SIEM 솔루션은 광범위한 감시 능력이 부족하기 때문에 이러한 노력을 충족시키기에 부족합니다. 결과적으로 이들은 필요한 모든 정보를 한 곳에 모아 효과적으로 연관시키고 위협을 발견하는 일이 불가능합니다. 사기와 같이 보다 복잡한 위협을 발견하기 위해서는 네트워크 운영팀과 보안 운영팀 간의 상관 관계를 개선할 수 있도록 모든 네트워크 및 보안 솔루션 전체에 있는 정보를 활용하는 것이 중요합니다.

QRadar의 위협 관리 기능은 네트워크 운영 및 보안 운영 간에 위협의 틈을 없애고, 네트워크에 필요한 감시를 제공하여 오늘날 보다 복잡하고 교묘해진 IT 기반의 위협을 발견합니다. 기존의 SIEM 솔루션 대부분은 수백만 개의 이벤트를 수천 개의 관련된 경고로 바꿔놓을 수 있을지도 모릅니다. 그러나 이러한 수천 개의 경고도 여전히 수동으로 분석하고 연관시켜야 합니다. 상관 관계를 파악하는 기존의 방식에서 한 발 더 나아가면 전체 인프라에 걸쳐 보다 나은 결론을 도출해낼 수 있습니다. 이를 통해 상황을 개선하기 위해 반드시 필요한 정보와 함께 가장 중요하고 반드시 해결해야 하며, 관리가 가능하고 우선순위가 지정된 보안 위협 항목이 제공됩니다.

QRadar의 위협 관리 기능에 제공하는 이점에는 다음과 같은 것들이 있습니다.

- **관련 있는 모든 네트워크 및 보안 데이터의 통합으로 위협을 보다 잘 인지하고, 거짓 긍정(false positive)을 최소화함**
- **다른 솔루션이 찾아내지 못하는 위협을 발견하도록 하는 행동 분석을 비롯한 효과적인 보안 인텔리전스**
- **업계 선두의 이벤트 상관 관계 파악 능력으로 한치의 오차 없이 정확하게 보안 인시던트를 (내부 사기의 경우, 일반 사용자에 이르는 범위까지) 발견함으로써 보안 인시던트를 관리하는 인력의 수고를 최소**

솔루션 5

운영 효율성 향상 및 **비용 절감**

기업은 중앙 집중식 보안 관리 솔루션이 없는 경우, 노동 집약적이며 위험이 큰 잠재적 보안 인시던트를 놓치기 쉬운 일련의 절차들에 의지해야 합니다. 또한 하나 이상의 규제 사항에 영향을 받으나, 중앙 집중식 로그 관리 또는 SIEM 솔루션이 없는 기업은 규제 준수 노력을 입증하지 못하거나, 규제 준수 감사를 통과하지 못할 위험이 있습니다.

QRadar는 가장 지능적이고 자동화된 통합 솔루션을 제공함으로써 비용을 절감하고, 여러 분야에 대한 운영 효율성을 향상시킵니다.

"기업 네트워크에 들어오고 나가는 엄청나게 많은 애플리케이션 트래픽을 분석하는데 QRadar를 이용하기 않았다면, 위협으로 간주하는 변칙들을 파악하는 일은 거의 불가능했을 것입니다."

– 고든 푸드 서비스(Gordon Food Service) 사례 연구

솔루션 6

로그 관리 – 우선적으로 처리해야 하는 **수십 개의 인시던트로 압축된 수억 개의 이벤트**

로그, 위협 및 규제 준수 계획과 관련 있는 모든 원본 데이터를 수집하고 저장하는 것이 필수지만, 그 누구도 문제를 발견하고 해결하기 위해 이 모든 정보를 일일이 꼼꼼하게 조사할 수는 없습니다. 따라서 수백만 개의 이벤트 기록들을 조치 가능한 소규모의 위협 요인들로 압축한 다음 우선순위를 지정하는 것이 보안 운영자에게 가장 중요한 사항입니다.

QRadar는 통합된 실시간 이벤트 상관 관계, 위협 발견, 규제 준수 보고 및 감사를 통해 수집된 모든 정보를 지능적으로 축소시키는 기능을 제공합니다.

QRadar의 기본 프레임워크에는 모든 네트워크화된 시스템 및 애플리케이션 전체에 걸쳐 확장 가능하며 보안된 로그 관리 기능을 제공하는 능력이 포함되어 있습니다. 또한 이벤트 로그를 수집, 보관 및 관리하는 작업을 하는 기업을 위해 완전한 로그 관리 솔루션을 제공합니다.

로그 관리에 있어 QRadar가 제공하는 이점에는 다음과 같은 것들이 있습니다.

- **전사적으로 이벤트 로그 수집 및 관리를 자동화하여 기존에 수동으로 진행해 온 작업을 최소화함**
- **효과적인 이벤트 분석 및 아카이브된 로그의 검색으로 보안 인시던트를 신속히 조사하며, 특정 규제 준수 감사 요구사항을 충족시킬 수 있음**
- **수집된 이벤트 로그의 통합을 보장하는 보안된 로그 관리 기능**
- **초당 수백, 수천 개의 이벤트를 지원하는 솔루션 범위**
- **효율적인 로그 저장을 위한 높은 압축력**

솔루션 7

기업의 **위험 예측**

기업은 네트워크가 악용되기 전에 정보 위험을 평가해야 합니다. 따라서 "what if" 의 상황을 사전에 파악함으로써 운영 효율성을 향상시키고, 네트워크 보안 위험을 줄일 수 있습니다. 로그 관리 및 SIEM과 함께 위험 관리를 추가한다면 기업은 사이버 범죄에 대해 선제 공격을 할 수 있습니다. 효과적인 보안 분석 및 시뮬레이션, 그리고 시각화 도구를 이용하여 QRadar의 위험 관리 솔루션은 매일 위협하는 보안 위험에서 벗어나고, 적극적인 위험 기반 접근법을 택할 수 있는 능력을 제공합니다.

위험 관리에 있어 QRadar가 제공하는 이점에는 다음과 같은 것들이 있습니다.

- **다양한 위험 지표를 활용한 규제 준수 업무의 자동화 및 규제 준수 위험의 평가**

"QRadar를 이용함으로써 이전에는 알지 못하고 지나간 이슈들에 대해 쉽게 대응할 수 있게 되었습니다. 최선의 노력을 기울이고 있지만, 보안 리소스가 제한된 상황에서 만 개 이상의 호스트에 대해 모든 이슈를 찾아내고 처리하기란 사실상 불가능합니다. QRadar를 통해 호스트의 중요도, 이벤트의 심각도 및 확실성 여부에 따라 무엇을 먼저 처리해야 하는지 그 우선순위를 정할 수 있습니다." **– 웨인 주립 대학교 사례 연구**

- **여러 공급업체의 구성 감사를 간소화하여 장치 구성의 일관성 유지 및 구성 변화로 인한 위험 평가**
- **강화된 보안 모델링 및 시뮬레이션을 통해 새로운 애플리케이션 및 인프라 배포 등 네트워크 변화로 인한 위험 파악**
- **이미 존재하고 있을지 모르는 보안 위험을 정확히 찾아낼 수 있도록 하여 네트워크에서 언제 트래픽이 발생하고, 발생 가능한지에 대한 통찰을 확보하기 위해 효과적인 네트워크 보안 시각화 활용**

QRadar는 기업의 네트워크 보안 인텔리전스 프로그램의 성숙도 상태와 일치할 수 있는 포괄적인 마이그레이션 경로를 제공하고, 최초의 프로젝트부터 대규모의 분산된 글로벌 배포까지 용이하게 지원합니다.

3

결론

기업에 있어서 효과적인 IT 네트워크 보안 인텔리전스 프로그램을 제공하는 일은 간단하지 않습니다. 전반적으로 IT 보안을 개선시키기 위한 동기는 운영 개선, 규제 사항 준수 등 다양한 요인에서 기인하지만, 해를 입히려는 위험으로부터 IT 자산을 보호한다는 하나의 목표를 가지고 있습니다. 예전부터 기업은 특정 IT 위험을 완화시키기 위해 많은 중요한 솔루션에 투자해 왔습니다. 앞으로도 기업은 기존의 솔루션을 이용하고, 이러한 솔루션이 제공하는 정보로부터 가치를 통합하는 방법을 검토해야 합니다.

Qradar는 네트워크 보안 인텔리전스에 대한 통합된 접근 방식으로 기업에 향상된 운영 효율성 및 비용 절감 능력을 제공하여 규제 준수 사항을 초월하며, 내부인 사기를 찾아내고, 위험을 예측하고, 데이터 사일로를 통합함으로써 타 제품이 찾아내지 못하는 위협을 발견하는데 있어 차별화된 가치를 제공합니다.

"CEO 또는 CIO가 제게 네트워크 이슈에 대해 묻는 경우, 바로 문제에 대해 설명하고 정확한 트래픽 업데이트를 제공할 수 있습니다. 저와 우리 팀 모두 전문가다워 보입니다. 이는 모두에게 이득이 되는 일입니다. QRadar에 투자한 것은 정말 가치 있는 결정이었습니다. 다른 솔루션들과 실제로 비교해본 결과 정말 탁월한 선택이었습니다."

– UDR, Inc. 사례 연구