IBM Security QRadar

가시성, 감지, 조사 및 대응

보안 팀이 직면한 문제는 충분히 많습니다. 더욱 정교해지고 늘어나고 있는 사이버 공격, 데이터의 폭발적 증가, 공격 표면의 확장, 연결되지 않은 보안 툴, 숙련된 보안 직원의 부족 등이 그 예입니다. 조직들은 의심스러운 알림을 조사하느라 1주일에 수백 시간을 사용하고 있지만, 이렇게 많은 시간을 사용해도 알림의 거의 17%도 조사하지 못하고 있습니다.[1] 고객의 신원 정보와 지적 재산을 보호하고 비즈니스 운영 중단을 방지하고자 하는 조직은 위협을 신속하게 감지하고 공격자가 재무적 손해와 평판 훼손을 유발하기 전에 정확하게 위협에 대처할 수 있도록 사전 예방적으로 환경을 모니터링해야 합니다.

시장을 선도하는 SIEM 솔루션인 IBM Security QRadar®는 통합된 가시성, 감지, 조사, 대응을 통해 보안 운영을 현대화하고 확장하면서 증가하는 위협을 방어하는 데 도움을 줍니다. QRadar 는 보안 팀에게 전사적인 보안 데이터에 대한 중앙집중식 가시성과 가장 우선적으로 대처해야 하는 위협에 대한 활용 가능한 인사이트를 제공합니다. 보안 분석가는 단일 인터페이스로 작업하면서 보안 상태를 신속하게 이해하고 가장 중대한 위협을 식별하고 자세한 정보를 확인할 수 있으므로, 워크플로우를 효율화할 수 있으며 여러 툴 사이에서 이동할 필요가 없습니다. QRadar 의

주요 특징

- 단일 인터페이스데이터에 대한 완전한 가시성 확보
- 이벤트를 기반으로 우선적으로 처리해야 할 가장 중요한 알림 목록 작성
- 자동화된 첨단 분석 및 위협 인텔리전스를 활용하여 조사 시간 단축
- 즉시 활용 가능한 사용 사례와 통합을 통해 신속하게 확장
- 규정 준수를 촉진하고 규제 위험 관리

[1] IDC, Insights from IDC's EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant (IDC 의 EDR 및 XDR 2020 설문조사에서 얻은 인사이트: 운영 과제와 이니셔티브가 풍부함), Doc #US47357921, 2021 년 1 월

이상 징후 감지 기능을 사용하면 보안 팀은 알려지지 않은 위협을 나타내는 것일 수 있는 사용자 행동의 변화를 신속하게 찾아낼 수 있습니다.

이 솔루션은 온프레미스 및 클라우드 기반 환경 전반에서 활동을 포괄적으로 파악하기 위해 엔터프라이즈 전반에서 방대한 양의 데이터를 수집합니다. 데이터가 수집될 때, QRadar 는 실시간으로 자동화된 보안 인텔리전스를 적용하여 신속하고 정확하게 위협을 감지하고 우선 순위를 지정합니다. 활용 가능한 알림은 잠재적 인시던트에 대한 풍부한 컨텍스트를 제공하므로 보안 분석가는 공격자의 영향을 제한하기 위해 재빨리 대응할 수 있습니다. QRadar 는 광범위한 보안 사용 사례를 지원하고 제한적인 맞춤화 노력으로 쉽게 확장할 수 있도록 특별히 설계되었습니다.

포괄적인 중앙집중식 가시성 확보

엔터프라이즈 네트워크는 기존의 온프레미스 IT 환경, 클라우드 기반 환경 및 운영 기술(operational technology, OT) 환경을 사용할 수 있습니다. 자산을 효과적으로 보호하고 위협을 정확하게 감지하고 규정을 준수하려면 이러한 환경은 모두 어느 정도의 감독을 요구합니다. 보안 팀이 위협을 감지하고 관리하기 위해 데이터 분석을 시작할 수 있으려면 먼저 별개의 보안 데이터에 대한 중앙집중식 가시성을 확보해야 합니다. QRadar 는 로그 및 플로우 데이터를 수집하고 구문 분석하고 정규화하여 조직이 사일로화된 환경에 대한 포괄적인 중앙집중식 가시성을 확보하도록 지원합니다. 보안 분석가는 단일 인터페이스에서 온프레미스, 클라우드, 하이브리드 환경을 모니터링할 수 있습니다.

이 솔루션에는 사전 구축된 DSM(Device Support Module)이 450 개 이상 포함되어 있습니다. DSM 은 조직이 투자한 다른 보안 기술과의 통합을 기본적으로 지원합니다. 고객은 QRadar 로 로그를 가리키기만 하면 됩니다. 그러면 이 솔루션은 로그 소스 유형을 자동으로 감지하고 올바른 DSM 을 적용하여 로그 데이터를 구문 분석하고 정규화할 수 있습니다. 그러므로 QRadar 고객은 다른 솔루션을 사용하는 고객보다 더 훨씬 더 빨리 운영을 시작할 수 있습니다. 또한, IBM Security App

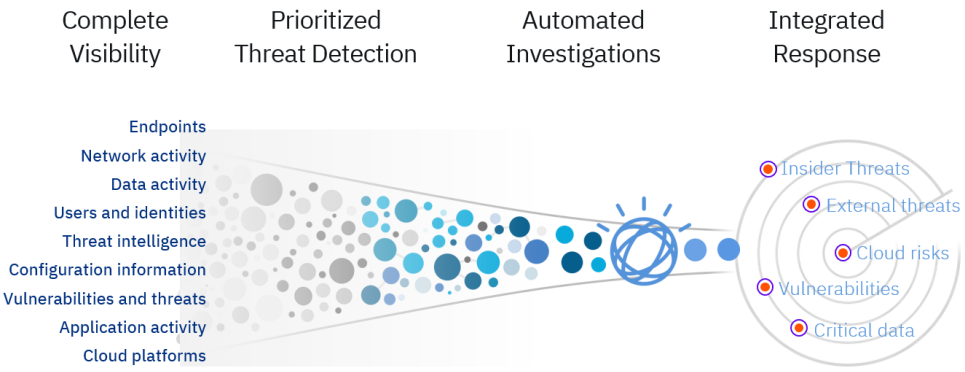
Exchange 에서 앱을 통해 추가 통합 기능을 쉽게 추가할 수 있습니다. 그리고 QRadar 는 직관적 그래픽 사용자 인터페이스(GUI)를 포함하는 간편한 DSM Editor 를 제공합니다. 이 GUI 를 통해 보안 팀은 맞춤형 애플리케이션의 로그를 구문 분석 하는 방법을 손쉽게 정의할 수 있습니다.

조직이 중요한 자산 또는 네트워크 세그먼트를 정의하도록 지원하는 자산 데이터베이스를 쉽게 마련하기 위해, QRadar 는 네트워크 플로우 데이터를 검사하여 사용 중인 애플리케이션, 프로토콜, 서비스, 포트를 기반으로 네트워크의 유효한 자산을 자동으로 식별하고 분류할 수 있습니다.

QRadar 는 고객이 전사적인 활동에 대한 포괄적인 가시성을 확보하도록 다양한 기술, 애플리케이션, 클라우드 서비스를 지원합니다. 이 데이터가 중앙집중화되면, 자동 분석을 통해 알려진 위협, 알려지지 않은 위협을 의미할 수 있는 이상 징후, 그리고 중요한 데이터를 노출시킬 수 있는 중요한 위험을 식별할 수 있습니다.

신속한 위협 감지를 위한 보안 인텔리전스 자동화

QRadar 는 알려진 위협과 알려지지 않은 위협을 식별하기 위해 로그, 이벤트, 네트워크 플로우, 사용자 활동, 취약성 정보, 위협 인텔리전스 등 여러 데이터 소스를 기반으로 자동으로 활동을 분석하고 상관관계를 파악합니다.

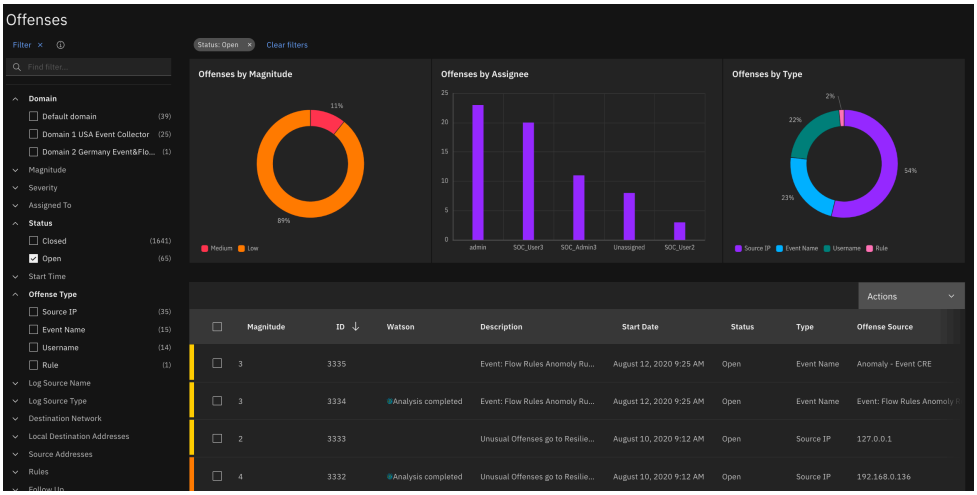


QRadar 는 조사가 필요한 가장 중대한 위협을 감지하고 이에 우선 순위를 부여하기 위해 다양한 소스의 데이터를 수집 및 분석하고 상관관계를 파악합니다.

QRadar 는 다음과 같은 소스를 포함하여 광범위한 소스에서 가져온 다양한 데이터 유형의 상관관계를 지능적으로 파악하고 분석을 수행합니다.

- 엔드포인트 데이터: Windows 이벤트 로그, Sysmon, EDR 솔루션 등
- 네트워크 활동 데이터: 방화벽, 게이트웨이, 라우터 또는 센서
- 취약성 데이터: 안티바이러스 툴, 취약성 스캐너, 침입 감지 시스템, 침입 방지 시스템, 데이터 손실 방지 시스템 등
- 클라우드 활동: Office365, SalesForce.com, Amazon Web Services(AWS), Microsoft Azure 및 Google Cloud 등 SaaS 및 IaaS 환경
- 사용자 및 아이덴티티 데이터: Active Directory, LDAP 또는 기타 아이덴티티 및 액세스 관리 솔루션에서 수집됨
- 애플리케이션 데이터: ERP(Enterprise Resource Planning) 솔루션, 애플리케이션 데이터베이스, SaaS 애플리케이션 등
- 위협 인텔리전스: IBM X-Force® 및 타사 위협 인텔리전스 피드 등의 소스
- 컨테이너 활동 데이터: Kubernetes 와 같은 컨테이너 관리 및 오케스트레이션 기술 소프트웨어

QRadar 는 알려진 위협과 알려지지 않은 위협을 감지하기 위해 수백 개의 사전 구축된 보안 사용 사례, 이상 징후 감지 알고리즘, 규칙, 실시간 상관관계 정책을 포함합니다. 위협이 발견되면 이 솔루션은 관련 보안 알림을 집계하여 "오펜스"라는 우선 순위가 부여된 단일 알림을 생성합니다. 오펜스는 위협의 심각도와 관련된 자산의 중대성을 기반으로 자동으로 우선 순위가 지정됩니다.



우선 순위가 부여된 위협 목록을 제공하는 QRadar 의 오펜스 화면

보안 분석가는 각 오펜스에서 단일 화면을 통해 위협 활동 내역을 모두 확인할 수 있습니다. 여기에서 분석가는 쉽게 특정 이벤트 또는 네트워크 플로우의 세부 정보를 확인하여 조사를 시작하거나 오펜스를 특정 분석가에게 할당하거나 종결할 수 있습니다. 새로운 관련 활동이 발생하면 오펜스가 자동으로 업데이트되므로 분석가는 언제든 최신 정보를 확인할 수 있습니다. 잠재적인 인시던트 각각에 대한 포괄적인 인사이트를 제공하는 동시에 알림의 총 개수를 줄여주는 이러한 고유한 접근법 덕분에 보안 분석가는 환경에서 가장 중대한 위협을 쉽게 이해할 수 있습니다.

비정상적인 네트워크, 사용자, 애플리케이션 활동 식별

공격자의 기술이 더욱 정교해지고 있으므로 알려진 위협 감지는 더 이상 그 자체로 충분하지 않습니다. 그 대신, 조직은 악의적 내부자, 자격 증명 침해 또는 파일리스 맬웨어 등 알려지지 않은 위협을 의미할 수 있는 네트워크, 사용자 또는 시스템 행동의 미세한 변화를 감지할 수 있어야 합니다.

QRadar 는 알려지지 않은 위협을 나타낼 수 있는 행동의 변화를 식별할 수 있는 다양한 이상 징후 감지 기능을 포함하고 있습니다. QRadar User Behavior Analytics 는 사용자 활동을 분석하여 악의적 내부자를 감지하고 사용자 자격 증명이 침해되었는지 판단합니다. 보안 분석가는 위험한 사용자와 이들의 비정상적 활동을 확인하고, 사용자의 위험 점수를 높인 기저 로그 및 플로우 데이터의 세부 정보를 확인할 수 있습니다.

SIEM 배포 환경의 일부로 선택 가능한 QRadar Network Insights 를 사용하면, 조직은 어느 시스템이 서로 통신했고 어느 애플리케이션이 관련이 있고 어느 정보가 패킷에서 교환되었는지에 대한 인사이트를 얻을 수 있습니다. 이 정보를 다른 네트워크, 로그, 사용자 활동과 연관시킴으로써, 보안 분석가는 호스트 침해, 사용자 침해 또는 데이터 유출 시도를 의미할 수 있는 비정상적 네트워크 활동을 찾아낼 수 있습니다.

QRadar 는 수많은 이상 및 행동 감지 규칙이 기본적으로 적용되어 배송되지만, 보안 팀은 자체 규칙을 생성하고 이상 징후 감지 설정을 변경하고 IBM Security App Exchange 에서 265 개 이상의 사전 구축된 앱을 다운로드하여 배포 환경을 강화할 수 있습니다.

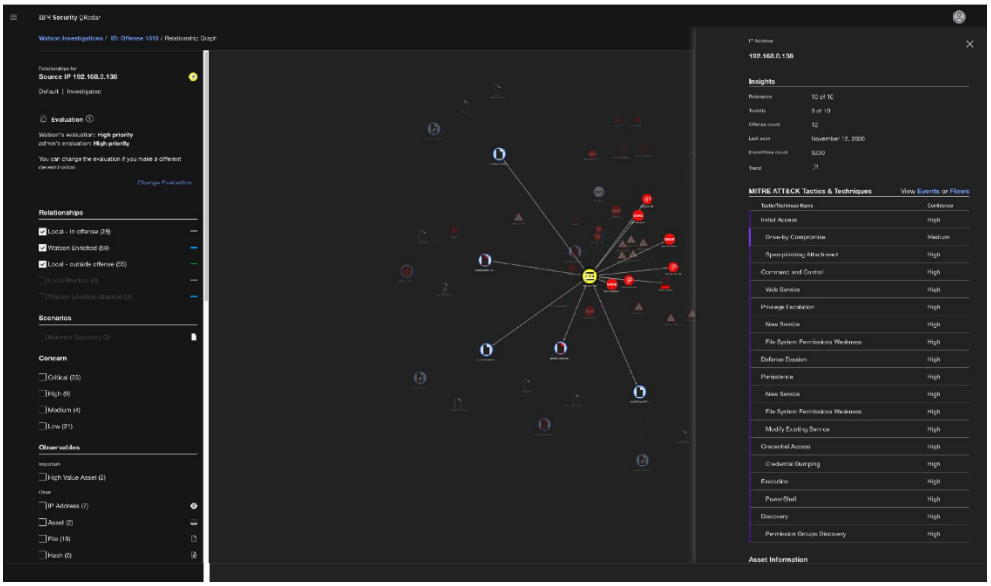
AI 및 자동화를 활용하여 조사 시간 단축

보안 팀은 매우 많은 알림과 수작업 그리고 부족한 인력으로 인해 부담을 느끼고 있으며, 이로 인해 극도의 피로를 느끼고 조직의 보안 태세를 약화시킬 수 있습니다. QRadar Advisor with Watson™은 AI 와 자동화를 사용하여 위협 알림을 조사하는 데 사용되는 시간을 며칠이나 몇 주에서 몇 분 또는 몇 시간으로 대폭 단축합니다. QRadar Advisor 는 우선 순위 지정 알림에 대한 조사를 수행하고 데이터의 상관관계를 파악하여 분석가가 업계 표준 MITRE ATT&CK 맵핑을 사용하여 근본 원인 분석 능력을 향상하는 동시에 더 큰 영향을 주는 전략적 분석과 위협 사냥에 집중할 수 있도록 지원합니다. 이를 통해 문제를 더 빨

리 해결하고 중단 시간을 단축하고 중대한 인시던트를 놓치는 횟수를 줄이고 분석가의 피로를 감소시키고 SOC/분석가 효율성을 높일 수 있습니다.

QRadar 는 단일 오펜스로 모든 관련 이벤트를 그룹화하여 우선 순위를 지정하며 보안 분석가가 공격으로 발전할 가능성이 있는 시나리오를 모두 파악할 수 있도록 지원합니다. 교차 조사 분석은 연결된 인시던트를 통해 조사를 자동으로 연결하여 알림에 대한 풍부한 컨텍스트를 제공합니다. 이를 통해 중복되는 노력을 줄이고 조사를 현재의 가능성 있는 인시던트와 알림에 국한시키지 않고 확대할 수 있습니다.

또한, Advisor with Watson 은 관련 침해 징후(indicators of compromise, IOC)를 발견하도록 설계된 코그너티브 인사이트 및 로컬 데이터 마이닝을 함께 제공합니다. QRadar 는 조사 내에서 관계를 그래프로 그려 개선된 조사 데이터를 시각화하고 다른 IOC, 자산, 사용자 또는 조사와 연결되어 있는지 살펴봅니다.



IOC, 자산, 사용자 또는 다른 조사와의 관계를 그래프로 그릴 수 있는 QRadar

또한, Advisor 는 MITRE ATT&CK 프레임워크로 조사를 맵핑하므로 보안 팀은 공격자의 전술과 기법을 시각화하고 ATT&CK 단계별로 이벤트와 플로우에 대한 자세한 정보를 확인하고 더욱 자신 있게 결정을 내릴 수 있습니다.

유도 기반 대응 및 케이스 관리를 통해 응답 시간 단축

IBM Security QRadar 를 IBM Security SOAR 와 통합하면 보안 팀은 단계별 플레이북, 수작업의 자동화, 일관적인 협업, 케이스 관리 조율을 통해 인시던트 대응 시간을 단축할 수 있습니다. 보안 분석가는 신속하고 효율적으로 의심스러운 오펜스를 QRadar 에서 IBM Security SOAR 로 에스컬레이션하고, 추가적인 자동화된 개선 작업을 시작하고, 전체 조사 프로세스를 촉진할 수 있습니다. 인시던트가 진화함에 따라, 모든 정보가 QRadar 와 IBM Security SOAR 사이에 동기화되므로 데이터 무결성을 완전히 달성할 수 있습니다. IBM Security SOAR 가 발견한 새로운 정보가 있는 경우 이 정보는 QRadar 로 다시 공급되어 감지 프로세스가 개선됩니다.

사전 구축된 컨텐츠, 규칙, 보고서로 규정 준수 관리 향상

QRadar 는 조직이 성공적으로 규정을 준수하고 규정 준수에 관해 보고하는 데 반드시 필요한 투명성, 책임성, 측정 가능성을 제공합니다. 이 솔루션은 위협 인텔리전스 피드의 상관관계를 파악하고 이러한 피드를 통합할 수 있으므로 감사자에게 IT 위험에 대한 보고를 위한 더욱 완전한 지표를 제공합니다. 수백 개의 사전 구축된 보고서와 규칙 템플릿은 업계의 규정 준수 요구 사항을 더 쉽게 충족하도록 지원할 수 있습니다.

네트워크 자산 프로파일은 비즈니스 기능(예: HIPAA(Health Insurance Portability and Accountability Act) 규정 준수 감사 대상인 서버)별로 그룹화할 수 있으므로 필요할 경우 관련 활동에 대해 더 쉽게 보고할 수 있습니다.

QRadar 는 GDPR(General Data Protection Regulation), FISMA(Federal Information Security Management Act), SOX(Sarbanes-Oxley), HIPAA, ISO 27001, PCI DSS(Payment Card Industry Data Security Standard) 등을 위한 규정 준수 패키지를 기본적으로 제공하며 조직이 위험과 규제 관련 노출을 관리하도록 지원하는 데 필요한 경험과 리소스를 보유하고 있습니다. 이러한 패키지는 Qradar 라이센스에 무료로 포함되어 있으며 IBM Security App Exchange 에서 제공됩니다.

변화하는 요구 사항에 맞게 손쉽게 확장

QRadar 의 유연하고 확장 가능한 아키텍처는 다양한 요구 사항을 가진 소규모 조직과 대규모 조직을 모두 지원합니다. 소규모 조직은 단일 올인원 솔루션으로 시작할 수 있으며, 이 단일 솔루션은 요구 사항이 변할 경우 분산된 배포 환경으로 쉽게 업그레이드할 수 있습니다. 대규모 기업은 대량의 데이터를 보유한 글로벌 분산 네트워크를 지원하기 위한 전용 구성요소를 배포할 수 있습니다.

IBM Security QRadar 는 이벤트 콜렉터, 이벤트 프로세서, 플로우 콜렉터, 플로우 프로세서, (저비용 스토리지 및 향상된 성능을 위한) 데이터 노드, 중앙 콘솔과 같은 구성요소를 포함하고 있습니다. 모든 구성요소는 하드웨어, 소프트웨어 또는 가상 어플라이언스로 이용할 수 있습니다. 소프트웨어와 가상 어플라이언스 옵션은 온프레미스 환경 또는 IaaS 환경에 배포하거나 하이브리드 환경에 분산시킬 수 있습니다.

배포 모델에 관계 없이, 지속적인 운영을 위해 필요할 경우 필요한 곳에 고가용성 및 재해 복구 보호 기능을 선택적으로 추가할 수 있습니다. 비즈니스 회복탄력성을 원하는 조직을 위해, QRadar 는 추가적인 타사 결함 관리 제품을 사용하지 않아도 통합된 자동 페일오버 및 시스템 간 전체 디스크 동기화 기능을 제

공합니다. 데이터 보호와 복구를 원하는 조직을 위해, QRadar 재해 복구 기능은 플로우 및 이벤트와 같은 라이브 데이터를 기본 QRadar 시스템에서 별도의 시설에 위치한 보조 병렬 시스템으로 전달할 수 있습니다.

결론

IBM Security QRadar 는 보안 분석가가 더 빠르고 효과적으로 문제를 분류하고 대응 결정을 내릴 수 있도록 가장 중대한 위협에 대한 활용 가능한 인사이트를 제공하기 위해 대량의 보안 데이터에 자동화된 지능적 분석을 적용하는, 시장을 선도하는 SIEM 솔루션입니다.

이 포괄적인 솔루션은 로그 관리, 네트워크 분석, 사용자 행동 분석, 위협 인텔리전스 및 AI 기반 조사 기능을 단일 솔루션(인시던트 대응을 위해 IBM Security SOAR 와 통합됨)으로 통합하며, 온프레미스, 클라우드, 하이브리드 환경 전반에서 포괄적인 가시성을 제공합니다.

IBM 이어야 하는 이유

IBM Security 는 기업 보안 제품 및 서비스를 위한 가장 앞선 통합형 포트폴리오 중 하나를 제공합니다. 세계적으로 유명한 IBM X-Force 연구소가 지원하는 이 포트폴리오는 비즈니스 환경에 보안을 구축을 구축하여 불확실성의 시대에 성장할 수 있도록 돕는 보안 솔루션을 제공합니다.

IBM 은 가장 광범위하고 깊이 있게 보안을 연구, 개발하고 제공하는 기업 중 하나입니다. 130 여개국에서 매월 1 조 개 이상의 이벤트를 모니터링하는 IBM 은 3,000 가지가 넘는 보안 특허를 보유하고 있습니다. 자세한 정보를 확인하시려면 ibm.com/security 를 방문해 주십시오.

추가 정보

IBM Security QRadar 에 대해 더 자세히 알아보려면 IBM 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 웹사이트 (https://www.ibm.com/security/security-intelligence/qradar)를 방문하십시오.