IBM Cloud Pak for Security

개방형 멀티클라우드 플랫폼으로 보안 현대화

조직이 비즈니스를 클라우드로 이동함에 따라 보안 데이터가 다양한 툴, 클라우드, 온프레미스 IT 환경에 분산되는 경우가 많습니다. 이 때문에 위협을 놓치는 문제가 발생하고 문제 해결을 위해 종종 고비용의 복잡한 통합을 수행할 수 밖에 없습니다.

IBM Cloud Pak® for Security 는 하이브리드, 멀티클라우드 환경 전반에서 위협과 위험에 대한 심층적인 인사이트를 얻기 위해 기존의 보안 툴을 신속하게 통합하도록 지원하는 플랫폼을 제공합니다. 인프라와 독립적으로 어디서나 실행되는 공통 운영 환경을 사용하면 위협을 재빨리 찾고 조치를 조정하고 대응을 자동화하는 동시에 데이터를 본래 위치에 그대로 둘 수 있습니다.

- 모든 데이터 소스를 연결 및 검색하여 환경을 완벽하게 파악하고 이를 통해 **드러나지 않은 위협을 빠르게 탐지하세요.**
- 데이터를 이동하지 않고 개방형 표준을 통해 기존 보안 툴에 연결하여 **보안 데이터 비용을 절감하세요.**
- 반복적인 수작업을 자동화하고 타사 통합을 통해 조사를 촉진하여 **대응 시간을 단축하세요.**
- Red Hat OpenShift 와 사전 통합된 컨테이너화된 소프트웨어로 **온프레미스, 퍼블릭 또는 프라이빗 클라우드 등 어디서나 실행하세요.**
- IBM 및 타사 데이터 연결업체의 개방형 생태계와 연결된 솔루션을 통해 **보안 가시성을 향상하세요.**

주요 특징

- 데이터 이동 없이 보안 인사이트 확보
- AI 와 자동화를 활용하여 보안 인시던트에 빠르게 대응
- 아키텍처가 어디서나 실행되도록 현대화

– 온디맨드 컨설팅부터 맞춤형 개발까지 추가적인 스킬을 활용하여 **팀의 역량을 확장하세요.**

IBM Cloud Pak for Security 플랫폼

IBM Cloud Pak for Security 는 통합된 경험과 원활한 워크플로우로 툴, 팀, 데이터를 연결하는 통합 플랫폼입니다. SOC(Security Operations Center) 및 데이터 보안과 같은 여러 보안 기능은 기존에는 서로 분리되어 있었습니다. 따라서 엔터프라이즈 전반에서 가시성과 협업을 저해했습니다. IBM Cloud Pak for Security 는 이와 같이 전에는 사일로화되었던 팀을 연결하므로, SOC 및 데이터 보안 분석가는 중앙집중식 플랫폼 역량을 기반으로 인시던트와 아티팩트를 공유할 수 있습니다.

보안 리더와 분석가는 플랫폼 전반에서 개괄적이거나 상세한 지표와 분석 결과를 표시하는 사전 구축된 맞춤형 대시보드로 보안 운영에 대한 가시성을 확보할 수 있습니다. 이들은 위협 인텔리전스, SIEM(Security Information and Event Management) 모니터링, 케이스 관리, SOAR(Security Orchestration, Automation and Response) 지표, 사용자 행동 분석, 위험 관리에 대한 정보를 포함하는 대시보드를 쉽게 구축할 수 있습니다.

IBM Cloud Pak for Security 에 사용된 오픈소스 기술과 개방형 표준 덕분에 이 플랫폼은 다양한 IBM 및 타사 보안 툴과 클라우드 솔루션에 연결할 수 있습니다. OASIS Open Cybersecurity Alliance 를 공동 설립하고 오픈소스 기술에 기여하면서 IBM 은 수십 개의 회사와 파트너십을 맺었습니다. 공동 개발된 오픈소스 기술을 통해 이러한 파트너십은 상호운용성을 장려하고 보안 커뮤니티 전반에서 벤더 종속성을 줄이는 데 도움을 줍니다.

운영 방법

IBM Cloud Pak for Security 플랫폼은 보안 팀이 활용할 수 있는 모듈형 제품과 솔루션으로 구성되어 있습니다. 통합된 사용자 경험과 중앙집중식 케이스 관리를 통해 제품과 솔루션이 함께 결합되므로 분석가는 플랫폼 전반에서 원활한 통합 워크플로우를 활용할 수 있습니다. 또한 유연한 라이센스와 비볼륨 기반 가격 덕분에 조직들은 필요한 기능을 선택하고 요구 사항이 변함에 따라 기능을 쉽게 추가할 수 있습니다.

IBM Cloud Pak for Security 제품 및 솔루션

IBM Security Threat Intelligence Insights

Threat Intelligence Insights 는 보안 분석가가 조직의 프로파일을 기반으로 조직과 가장 관련성이 큰 위협을 찾아내고 우선 순위를 부여하는 데 도움을 주는, 활용 가능하고 상세한 위협 인텔리전스를 제공합니다. 이 솔루션은 전 세계에서 실시된 보안 조사를 통해 얻은 X-Force Threat Intelligence 의 인사이트를 지원하고 연결된 모든 데이터 소스를 스캔하여 위협이 환경에 영향을 미치는지를 확인할 수 있습니다. 위협이 감지되면 플랫폼 내에서 케이스가 자동으로 생성되고, 분석가는 사일로화된 여러 소스에서 원활하게 조사를 더 실시하고 IBM Cloud Pak for Security 의 통합 워크플로우를 활용하여 사이버 위협을 해결할 수 있습니다.

IBM Security Data Explorer

Data Explorer 는 분석가가 IBM 및 타사 데이터 소스 전체를 통합적으로 조사하는 데 유용한 솔루션입니다.
SIEM(Security Information and Event Management), EDR(Endpoint Detection and Response) 등의 보안 툴에서 얻은 인사이트와 Elastic 같은 데

이터 레이크에 저장된 데이터를 연결할 수 있습니다. 또한 분석가는 QRadar 및 Splunk 와 같은 SIEM 툴이 모니터링하는 멀티클라우드 환경에 대한 인사이트를 확보할 수 있습니다. Data Explorer 는 분석가가 단순한 쿼리 빌더와 하나의 워크플로우를 사용하여 여러 데이터 소스를 쿼리하도록 지원하므로 조사 시간을 상당히 단축하는 데 도움이 됩니다. 그러므로 SOC 팀은 더 많은 작업을 더 빨리 수행할 수 있고 분석가는 침해 지표(IOC)와 위협을 모든 데이터 소스에서 찾을 수 있습니다.

IBM Security SOAR

SOAR 은 일반 보안 운영과 인시던트 대응(IR) 프로세스를 자동화하고 복잡한 문제 해결에 필요한 단계를 처음부터 끝까지 안내하여 보안 분석가의 역량을 강화시켜 줍니다. 사고 발생 상황과 관련된 중요한 보안 정보를 빠르게 확인함으로써 정확하게 의사 결정하고 결정적인 조치를 실행할 수 있게 됩니다. SOAR 은 자동화, 타사 통합, 동적 케이스 관리를 활용하여 보안 분석가의 생산성을 향상하고 배포된 기술의 효과성을 개선하므로 사이버 보안 스킬 부족 문제와 알림으로 인한 피로를 완화합니다.

IBM Security QRadar

QRadar 는 내부자 위협, 첨단 위협, 클라우드 보안 등을 포함한 수백 가지의 보안 적용 사례에 대한 지원을 즉시 제공하여 보안 및 IT 생태계를 위해 500 가지 이상의 검증된 통합과 가시성을 결합합니다. SOC 분석가는 사용자, 엔드포인트, 클라우드, 애플리케이션, 네트워크 전반에 대한 중앙집중화된 인사이트를 얻을 수 있습니다. QRadar 의 분석 엔진은 알려진 위협과 알려지지 않은 위협을 나타내는 비정상 행동과 이상 활동을 찾아내기 위해 다양한 분석 기능을 사용합니다. QRadar 의 분석 기능과 모델은 Fortune 선정 100 대 기업을 수년간 보호해온 보안 우수 사례에 따라 조정되고 향상되었습니다.

IBM Security Guardium Insights

Guardium Insights 는 숨겨진 위협과 이상 행동을 발견하기 위해 여러 데이터 소스를 통합적으로 파악하고, 장기적으로 규정 준수 및 감사 로그를 저장하고, 첨단 분석과 머신 러닝(ML)을 활용하여 조직의 데이터 아키텍처를 간소화하도록 구축된 데이터 보안 허브입니다. 보안 전문가는 수년에 해당하는 과거 보안 데이터로부터 몇 초 안에 온프레미스 및 클라우드 데이터베이스 전반에 대한 주요 위험 인사이트를 얻을 수 있습니다. Guardium Insights 는 Cloud Pak for Security 토대를 기반으로 데이터 보안 전문가가 데이터 보안 이벤트를 발견하고 이에 대한 조치를 취하기 위해 IT 및 보안 조직 내의 SOC 분석가 및 기타 인력과 협업할 수 있도록 지원합니다.

IBM Security Risk Manager

Risk Manager 는 IT 환경 전반의 위험 데이터를 맥락화하고 위험 벡터 및 자산 중요도와 관련된 인사이트의 상관관계를 파악하여 보안 리더에게 조직의 보안 위험에 대한 가시성을 제공합니다. 보안 전문가는 여러 소스 제품을 통해 데이터 보안, SIEM, 아이덴티티 분야 전반에서 작업을 수행하여 위험을 평가할 수 있습니다. 이들은 비즈니스가 사용할 수 있는 대시보드에서 위험 상태를 신속하게 이해하고, Cloud Pak for Security 에서 케이스를 생성하고 SOAR 기능을 활용하여 보안 팀 전체 그리고 인시던트 대응 담당자와 협력할 수 있습니다.

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 구축하여 불확실성의 시대에서 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/kr-ko/security 를 방문해 주십시오.

추가 정보

IBM Cloud Pak for Security 에 대한 추가 정보를 얻으려면 IBM 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 웹사이트(https://www.ibm.com/products/Cloud-pak-for-Security)를 방문하십시오.