

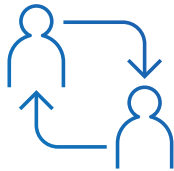
IBM Cloud Pak for Security

하이브리드, 멀티클라우드 보안의 핵심은 통합 가시성을 확보하는 것입니다.

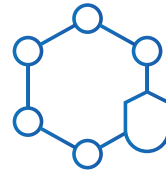
대부분의 경우 보안 데이터는 다양한 툴, 클라우드, 온프레미스 IT 환경에 분산되어 있습니다. 이로 인해 비용이 많이 들고 복잡한 통합 작업을 수행해야 하므로 위협 요소를 놓치는 일이 발생합니다. IBM Cloud Pak for Security는 모든 환경에서 실행 가능하며, 인프라에 독립적인 공통의 운영 환경을 사용하여 기존의 보안 툴들을 보다 신속하게 통합합니다. 또한 하이브리드 멀티클라우드 환경 전반의 위협 요소에 대해 심도 있는 통찰력을 생성할 수 있는 플랫폼을 제공합니다. 따라서 사용자는 데이터를 기존 위치에 그대로 유지하면서, 신속하게 위협 요소를 검색하고 이에 대한 대응을 조절하거나 자동화할 수 있습니다.



데이터 이동 없이
보안 인사이트
확보



자동화 기술로 더욱
신속하게 보안 사고
해결



모든 환경에서 실행
가능 및 개방형 통합
보안

솔루션 특징점

보안 환경을 종합적으로 파악하기 위해 모든 데이터 소스를 연결하고
검색하여 **드러나지 않은 위협 요소를 신속하게 발견합니다.**

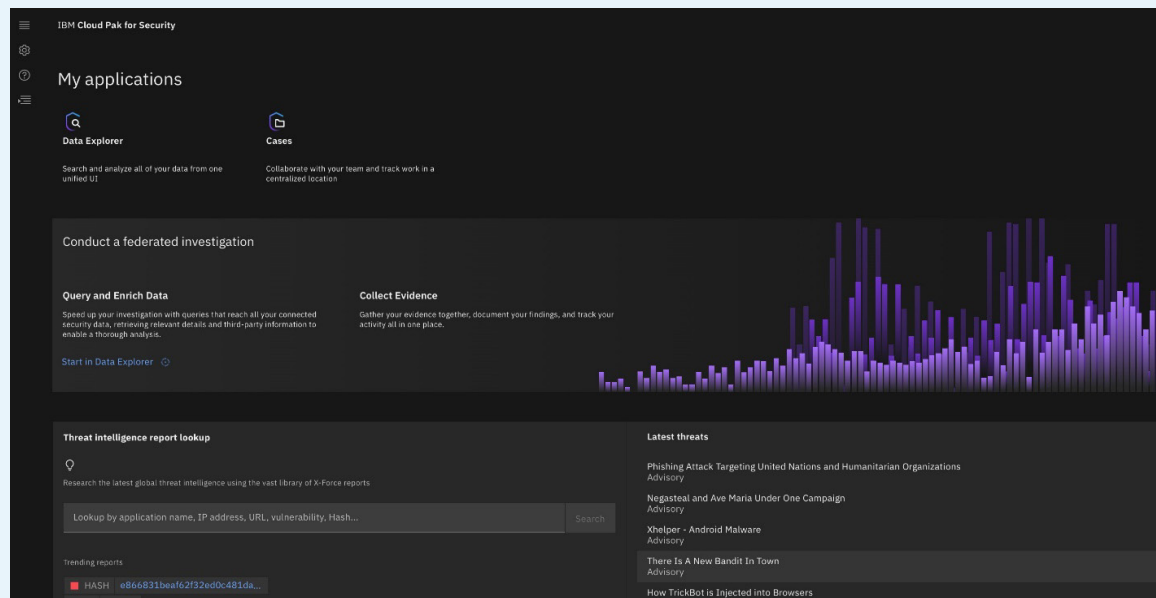
데이터 이동 없이 개방형 표준을 통해 기존의 보안 툴에
연결함으로써 **보안 데이터의 비용을 절감합니다.**

타사 툴과의 통합을 통해 반복적인 수작업을 조정 및 자동화하고
조사를 진행하여 **대응 시간을 단축합니다.**

Red Hat OpenShift 엔터프라이즈 애플리케이션 플랫폼과 사전
통합된 컨테이너 기반 소프트웨어를 통해 **온프레미스, 퍼블릭
클라우드, 프라이빗 클라우드 등 어디에서나 실행됩니다.**

IBM 및 타사 데이터 커넥터의 개방형 생태계에 연결하는 솔루션을
통해 **보안 가시성을 강화합니다.**

온디맨드 컨설팅에서 맞춤형 개발에 이르는 IBM Security Expert
Labs의 다양한 기술 서비스를 통해 **팀의 역량을 확대합니다.**



IBM Cloud Pak for Security

제품 및 서비스 오퍼링

IBM Security Data Explorer

IBM Security Data Explorer를 통해 보안 분석가는 IBM 및 타사 데이터 소스 전반에서 통합적인 조사를 수행할 수 있습니다. 보안 정보 및 이벤트 관리(SIEM), 엔드포인트 탐지 및 대응(EDR)과 같은 보안 툴, 그리고 Elastic과 같은 데이터 레이크에 저장된 데이터로부터 통합된 인사이트를 도출합니다. 또한 QRadar 및 Splunk와 같은 SIEM 툴이 모니터링하는 멀티클라우드 환경에서도 유용한 인사이트를 확보할 수 있습니다. 간단한 쿼리 빌더와 하나의 워크플로우를 사용하여 여러 데이터 소스를 검색함으로써 조사에 필요한 시간을 크게 단축할 수 있습니다. 이러한 이점들을 바탕으로 보안관제센터(SOC)는 더 많은 일을 더욱 신속하게 수행할 수 있으며, 보안 분석가들은 모든 데이터 소스에서 침해지표(IOC)와 위협 요소들을 찾아낼 수 있습니다.

IBM Security Orchestration, Automation and Response(SOAR)

IBM Cloud Pak for Security의 SOAR 기능은 보안 분석가/CERT들이 공통적인 보안 운영 및 사고 대응(IR) 프로세스를 자동화하도록 지원하고 복잡한 문제를 해결하는 데 필요한 단계별 가이드를 제공합니다. 사고 발생 상황에 따라 중요한 보안 정보에 신속하게 액세스할 수 있어 정확한 의사 결정과 문제 해결을 위한 조치를 취할 수 있도록 해줍니다. 또한, 자동화 기능을 통해 보안 분석가의 생산성을 높이고 배포된 기술의 효율성을 개선함으로써 오늘날 보안팀이 직면하고 있는 기술 격차와 잦은 보안 경보에 따른 반복적인 대응 업무로 인한 피로를 개선합니다.

IBM Security Expert Labs 서비스

IBM Security Expert Labs에서는 Cloud Pak for Security를 뒷받침하는 서비스를 제공합니다. 이 팀은 IBM Security 제품의 라이프사이클 전 단계(도입, 확장, 최적화)에 걸쳐서, 필요한 비즈니스 및 기술에 대한 전문 컨설팅/구축 서비스를 제공합니다. IBM은 고객마다 각기 다른 보안 프로그램을 보유하고 있다는 점에 대한 이해를 바탕으로, 설치 및 구현, 커넥터 개발, 서비스 지원을 포함한 Cloud Pak for Security의 구현 및 컨설팅을 제공합니다.

