IBM Security

Azure 위협 관리 평가

데이터 유출로 인한 피해는 막대한 비용에만 그치는 것이 아니라, 무거운 책임과 기업 이미지 실추로 이어집니다.

386만 달러

데이터 유출 사고 평균 비용[1]

150달러

유실/유출된 기록당 평균 비용[1]

[1] 2020년 데이터 유출 사고 비용 보고서, Ponemon Institute 작성, IBM 의뢰

Azure 환경의 보안 수준을 업그레이드하는 IBM 표적 위협 관리 평가 솔루션

Azure Threat Management Accelerator는 Azure 하이브리드 멀티클라우드의 보안 허점을 찾아냅니다. 보안 관제, 인시던트 대응, 컴플라이언스, 거버넌스 차원에서 보안 프로그램의 개선 방안도 제시합니다.

IBM Azure Threat Management Accelerator의 첨단 검토 기능으로 다음 과제를 해결할 수 있습니다.

클라우드 보안 전략

- Azure 및 하이브리드 멀티클라우드 보안 전략

보안관제

- 인시던트 대응 계획
- 위협 차단, 탐지, 대응
- SOAR(Security Orchestration, Automation and Response: 런북 및 플레이북

거버넌스와 컴플라이언스

- 조직 구조
- 정책과 절차
- 컴플라이언스 요건

IBM

Azure 위협 관리 평가: 형식과 결과물

성숙도 평가는 IBM 위협 관리 컨설턴트가 진행하는 가상 대화형 세션의 형식으로 진행됩니다.

일반적인 성숙도 평가 세션은 인터뷰, 결과 문서화, 최종 보고서 제출까지 **총 3일 정도** 걸립니다.

주요 이점

- 세션에서 학습한 내용을 토대로 우선 순위를 정해 클라우드 보안 전략을 비즈니스 목표와 연계하고, 클라우드 보안 실태를 더 면밀하게 점검할 수 있습니다.
- 고객은 수집된 정보를 간추려 정리하고, 개선할 영역을 제시하며, 클라우드 보안 수준을 강화하기 위한 다음 단계를 우선 순위에 따라 제안하는 보고서를 받습니다. 이 보고서는 고객 기밀 정보로 간주됩니다.

기대 효과

이 워크숍에서는 하이브리드 멀티클라우드 보안관제의 전 범위에서 비즈니스 워크로드를 보호하는 데 필요한 보안 구성요소에 초점을 맞춥니다.

IBM은 체계적인 상담을 통해 고객의 Azure 클라우드 인프라를 이루는 요소를 점검합니다. 또한 관련 보안 기능에 관한 맵/갭 분석을 수행하고 주요 관찰 결과 및 초기의 권장 사항을 문서화합니다.

영업 팀 상담
1 877-426-3774
Priority 코드: Security
IBM Security Services for Cloud: 자세히 보기