IBM 클라우드 서비스 명세

IBM Security AppScan Mobile Analyzer

다음은 주문자용 서비스 명세입니다.

1. 클라우드 서비스

클라우드 서비스 오퍼링은 아래 설명되어 있으며 선택되어 권한이 부여된 오퍼링은 주문서에 지정되어 있습니다. 주문서는 제공된 견적서와 클라우드 서비스의 시작일과 기간을 명시한 라이센스 증서로 구성됩니다. 청구서 작성은 클라우드 서비스를 프로비저닝한 후에 시작합니다.

1.1 IBM Security AppScan Mobile Analyzer

본 서비스는 Android 모바일 애플리케이션의 코드 레벨에서 보안 문제점을 식별합니다. 그것은 개발자가 애플리케이션 소스 코드를 제공하지 않고도 보안 취약점을 스캐닝할 수 있게 합니다. 스캔이 종료되면 서비스에서는 감지된 취약점의 상세 정보, 취약점으로 인한 모바일 애플리케이션의 잠재적 보안 위험, 취약점 수정 방법에 대한 제안이 포함된 보안 보고서를 생성합니다.

2. 보안 설명

2.1 보안 정책

IBM 은 정보 보안 팀을 운영하며 IBM 직원에게 통지하는 개인 정보 보호 및 보안 정책도 유지 관리합니다. IBM 은 IBM 데이터 센터를 지원하는 직원에게 개인 정보 보호 및 보안 교육을 받도록 요구합니다. IBM 보안 정책 및 기준은 매년 검토되어 재평가됩니다. IBM 보안 문제는 종합적인 사고 대응 절차에 따라 처리됩니다.

2.2 접근 권한 통제

고객 데이터에 대한 접근이 필요한 경우, 업무 분리 원칙에 따라 권한이 부여된 IBM 지원 담당자 및 서비스 운영 직원만 접근이 허용됩니다. IBM 직원(또는 그에 준하는)은 중간 "게이트웨이" 관리 호스트에 대한 이중(two-factor) 인증 방식을 사용합니다. 고객 데이터 접속 시 모든 연결은 암호화된 채널로 제공됩니다.

2.3 서비스 무결성 및 가용성

운영 체제와 애플리케이션 소프트웨어를 수정하려면 IBM 변경 관리 프로세스를 준수해야 합니다. 방화벽 규칙의 변경도 변경 관리 프로세스에 따라 수행되며 변경사항을 구현하기 전에 IBM 보안 직원(또는 그에 준하는)의 검토를 별도로 받습니다. IBM 은 데이터 센터를 24x7 원칙으로 감시합니다. 허가된 관리자와 제 3 자 벤더는 내외부 취약성 스캔닝을 정기적으로 실시하여 잠재적인 시스템 보안 문제를 발견하고 해결할 수 있도록 지원합니다. 모든 IBM 데이터 센터에는 악성 소프트웨어 감지(안티바이러스, 침입 감지, 취약성 스캐닝 및 침입 방지) 시스템이 사용됩니다. IBM 데이터 센터 서비스는 공용 네트워크에서 데이터를 전송하기 위해 다양한 정보 전달 프로토콜을 지원합니다. 예를 들면, HTTPS/SFTP/FTPS/S/MIME, site-to-site VPN 이 있습니다. 오프 사이트 저장 목적의 백업 데이터는 전송되기 전에 암호화됩니다.

2.4 활동 로깅

IBM 은 활동 로깅 용도로 구성된 시스템, 애플리케이션, 데이터 저장소, 미들웨어 및 네트워크 인프라스트럭처 디바이스의 활동 로그를 유지 관리합니다. 로그의 조작을 방지하고 중앙 집중적 분석, 경보 및 보고 기능을 수행할 수 있도록 활동 로깅은 중앙 로그 저장소에서 실시간으로 처리됩니다. 조작 방지를 위해 데이터는 서명됩니다. 이상 동작을 찾기 위해 정기 분석 보고서를 통해 로그를 실시간으로 분석합니다. 운영 직원(또는 그에 준하는)에게 이상 동작을 통지하고 필요한 경우 24x7 on-call 보안 전문가에게 문의합니다.

2.5 물리적 보안

IBM 은 IBM 데이터 센터에 대한 불법적인 물리적 접근을 제한하기 위해 마련된 물리적 보안 기준을 유지 관리합니다. 데이터 센터에 대해서는 이중 인증 방식과 감시 카메라를 통한 통제와 모니터링이 적용되는 제한적인 접근 지점만 제공됩니다. 데이터 센터에 대한 접근은 접근 권한이 승인된 직원(또는 그에 준하는)만 가능합니다. 운영 직원(또는 그에 준하는)은 승인 여부를 검증한 후 접근 권한을 부여하는 액세스 배지를 발행합니다. 해당 액세스 배지를 획득한 직원은 기타 상이한 액세스 배지는 포기해야 하며 활동 기간에만 데이터 센터 액세스 배지를 소유할 수 있습니다. 액세스 배지의 사용은 기록됩니다. 비 IBM 방문자는 근무지 사이트에 입장 시 등록을 해야 하고 근무지 사이트에 있는 동안 안내자가 동행합니다. 권한이 없는 개인이 현장을 방문할 수 있는 서비스 제공 지역, 물류장 및 기타 지점은 관리 하에 격리됩니다.

2.6 준수

IBM 은 IBM 개인정보 보호정책이 미국 상무부의 Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement 와 일치하는지 매년 증명합니다. IBM 은 프로덕션 데이터 센터에서 매년 업계 표준 SSAE 16 감사(또는 그와 동등한 감사)를 실시합니다. IBM 은 IBM 비즈니스 요건을 준수하기 위해 보안 및 개인 정보 보호 관련 활동을 검토합니다. IBM 팀은 IBM 의 정보 보안 정책을 준수하는지 여부를 확인하기 위해 정기적인 평가와 감사를 합니다. IBM 직원과 공급업체 직원은 매년 보안 인식 교육을 받습니다. 업무 윤리 강령, 기밀 보호 및 IBM 보안 의무를 준수할 의무와 업무 목표를 매년 직원에게 숙지시킵니다.

3. 권한 부여 및 대금 청구 정보

3.1 과금 체계

클라우드 서비스는 주문서에 명시된 바와 같이 다음 과금 체계 하에서 제공됩니다.

- 애플리케이션 인스턴스(Application Instance)는 IBM SaaS 구입 시 사용되는 측정 단위입니다. IBM SaaS 에 연결된 애플리케이션의 각 인스턴스에 대해 하나의 애플리케이션 인스턴스 권한이 필요합니다. 애플리케이션에 다중 구성요소가 존재하고 각 구성요소가 개별 용도 및/또는 사용자별로 사용되며 각 구성요소를 IBM SaaS 에 연결하거나 IBM SaaS 에서 관리할 수 있는 경우 각 구성요소는 개별 애플리케이션으로 간주됩니다. 또한 애플리케이션의 테스트, 개발, 스테이징(Staging) 및 프로덕션 환경은 각각 애플리케이션의 개별 인스턴스로 간주되며 각 인스턴스에 대한 권한이 필요합니다. 단일 환경에 있는 다중 애플리케이션 인스턴스는 각각 애플리케이션의 개별 인스턴스로 간주되며 각 인스턴스에 대한 권한이 필요합니다. 고객의 라이센스 증서(PoE)나 거래서류에 명시된 측정 기간 동안 IBM SaaS 에 연결된 애플리케이션 인스턴스 수를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

3.2 대금 및 청구

클라우드 서비스에 대해 지불하는 대금은 주문서에 명시됩니다.

3.3 Pay as you Go 요금제

Pay as you Go 옵션의 요금은 거래서류에 명시된 요율에 따라 서비스를 사용한 그 다음 달에 청구됩니다.

4. 기술 지원

등록 기간에는 클라우드 서비스에 대한 기술 지원이 제공됩니다.

지원 운영 시간은 다음과 같습니다.

이용 가능 시간, 온라인 문제점 보고 시스템 및 기타 기술 지원 교신 방법과 절차에 대한 정보는 IBM Software as a Service Support Handbook 에 설명되어 있습니다.

업무 시간 외 지원:

업무 시간 외 지원(상기의 정기 운영 시간 외)은 심각도 1 의 문제점에 한해 영업일, 주말 및 공휴일에 제공됩니다. 심각도 1 문제점의 경우 고객은 문제점을 진단하는 것을 24X7 기간 동안 지원할 수 있어야 하고, 그렇지 않은 경우에는 해당 문제점이 심각도 2 로 강등됩니다.

4.1 포럼 지원(Forum Support)

클라우드 서비스의 모든 고객에게는 IBM 지원 담당자와 개발자가 정기적으로 모니터링하는 포럼 지원이 제공됩니다.

a. 질문하기:

https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. 현재 게시물 보기:

https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 표준 지원

고객에게 Pay as you Go 요금이 발생하는 기간 동안 표준 지원이 제공됩니다. 고객은 클라우드 서비스 내에서 지원 티켓을 제출하거나 지원을 위한 채팅 세션을 오픈할 수 있습니다. 지원 절차에 대한 자세한 정보는 IBM 지원 웹 포털(https://support.ibmcloud.com) 또는 IBM SaaS Software Support Handbook(http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf)에서 확인할 수 있습니다.

심각도(Severity)	심각도 정의	대응 시간 목표	대응 시간 범위
1	**심각한 업무 영향/서비스 다운:** 중대한 업무 기능이 작동 불가능하거나 중대한 인터페이스에 장애가 발생했습니다. 일반적으로 프로덕션 환경에 적용되며 서비스에 대한 액세스 불능으로 인해 운영에 심각한 영향을 끼치는 경우를 의미합니다. 이 경우 즉각적인 해결책을 제공해야 합니다.	1 시간 이내	24x7
2	**상당한 업무 영향:** 서비스 업무 기능이 사용에 있어 상당히 제한되거나 귀하가 업무 기한을 준수하지 못하게 됩니다.	2 영업시간 이내	월요일 - 금요일 영업시간
3	**사소한 업무 영향:** 서비스 또는 기능을 이용할 수 있으며 운영에 대한 심각한 영향은 없습니다.	4 영업시간 이내	월요일 - 금요일 영업시간
4	**최소 업무 영향:** 조사 또는 비기술적 요청	1 영업일 이내	월요일 - 금요일 영업시간

5. Safe Harbor 준수

본 클라우드 서비스에 대한 US-EU and US-Swiss Safe Harbor Frameworks 준수 여부에 대해서는 결정된 바 없습니다.

6. 추가 정보

본 클라우드 서비스는 모바일 애플리케이션과 모바일 웹 서비스 내의 잠재된 다양한 보안 및 준수 문제점을 식별하기 위해 설계됩니다. 그러나 클라우드 서비스는 모든 취약점과 준수 위험성을 테스트하지는 않으며 보안 공격에 대비한 보호 장치로 사용되지 않습니다. 보안 위협, 규제 및 표준은 계속 변경되며 모든 변경사항이 서비스에 반영되지는 않습니다. 고객의 모바일 애플리케이션, 시스템 및 직원에 대한 보안과 준수 및 구제 조치는 전적으로 고객의 책임입니다. 서비스에서 제공한 정보를 사용하거나 사용하지 않는 것 전적으로 고객의 재량입니다.

6.1 파생 혜택 사업장

해당하는 경우, 세금은 귀하가 클라우드 서비스의 혜택이 제공되는 것으로 식별한 사업장을 기준으로 부과됩니다. 추가 정보를 제공하지 않는 한, IBM 은 클라우드 서비스 주문 시 1 차 혜택 사업장으로 제출한 비즈니스 주소에 따라 세금을 적용합니다. 귀하는 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM 에 제공해야 할 책임이 있습니다.

6.2 쿠키

귀하는 IBM 이 클라우드 서비스의 정상적인 운영과 지원 과정에서 추적 및 기타 기술을 사용하여 클라우드 서비스 사용과 관련된 개인 정보를 귀하(귀하의 직원과 계약직 직원)로부터 수집할 수 있다는 것을 인정하고 이에 동의합니다. IBM 은 사용자 경험을 개선하거나 상호작용을 조정할 목적으로 클라우드 서비스의 효율성에 대한 통계와 정보를 수집합니다. 귀하는 IBM, 기타 IBM 회사 및 하도급자 내부에서, 그리고 IBM 및 IBM 하도급자가 비즈니스를 수행하는 어디서나, 관련 법률을 준수하면서, 상기의 목적으로 수집된 개인 정보를 IBM 이 처리하기 위해 필요한 동의를 이미 획득했거나 획득할 것임을 확인합니다. IBM 은 수집된 개인 정보에 접근하거나 갱신하거나 정정하거나 삭제하고자 하는 고객 직원과 계약직 직원의 요청을 수용합니다.