IBM Application Security on Cloud

이용 약관은 본 IBM 이용 약관 – SaaS 특정 오퍼링 조항(이하 "SaaS 특정 오퍼링 조항")과 IBM 이용 약관 – 일반 조항(이하 "일반 조항") 문서(URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/ 참조)로 구성됩니다.

조항이 상충하는 경우에는 SaaS 특정 오퍼링 조항이 일반 조항에 우선하여 적용됩니다. IBM SaaS 를 주문하거나 액세스하거나 사용함으로써 고객은 이용 약관에 동의합니다.

이용 약관에는 해당 IBM International Passport Advantage 계약, IBM International Passport Advantage Express 계약 또는 선택한 IBM SaaS 오퍼링에 관한 IBM 국제 계약(IBM International Agreement for Selected IBM SaaS Offerings)이 적용되며 이용 약관과 함께 전체 계약을 구성합니다.

1. IBM SaaS

다음 IBM SaaS 오퍼링에는 본 SaaS 특정 오퍼링 조항이 적용됩니다.

- IBM Application Security Analyzer

2. 과금 체계

IBM SaaS 는 거래서류에 지정된 바와 같이 다음 과금 체계 하에서 판매됩니다.

a. **애플리케이션 인스턴스(Application Instance)** – 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 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.

b. **액세스(Access)** – IBM SaaS 구입 시 사용되는 측정 단위입니다. 액세스는 IBM SaaS 를 사용할 수 있는 권리입니다. 고객은 고객의 라이센스 증서(PoE) 또는 거래서류에 규정된 측정 기간 동안 IBM SaaS 를 사용하기 위하여 반드시 액세스 권한을 취득하여야 합니다.

3. 대금 및 청구

IBM SaaS 에 대한 청구 금액은 거래서류에 명시됩니다.

3.1 사용량별 요금제(Pay per Use)

사용량별 요금제 옵션은 거래서류에 명시된 요율에 따라 서비스를 사용한 그 다음 달에 청구됩니다.

3.2 월 분할(Partial Month) 요금

거래서류에 명시된 월 분할 요금은 비례 배분하여 산정될 수 있습니다.

4. 기술 지원

기술 지원은 등록 기간(Subscription Period) 동안 그리고 IBM 이 고객에게 IBM SaaS 에 대한 액세스를 허용한다고 통지한 후 온라인 포럼을 통해 제공되며 고객이 사용량별(Pay per Use) 요금제를 사용하는 기간 동안 표준 지원으로 제공됩니다. 고객은 IBM SaaS 내에서 지원 티켓을 제출하거나 지원을 위한 채팅 세션을 오픈할 수 있습니다. IBM 은 기술 지원 담당자 정보와 절차에 대해 설명하는 IBM Software as a Service Support Handbook 을 이용할수 있게 합니다.

심각도(Severity)	심각도 정의	대응 시간 목표	대응 시간 범위
1	**심각한 업무 영향/서비스 다운:** 중대한 업무 기능이 작동하지 않거나 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 상당히 제한되거나 업무 기한을 준수하지 못하게 됩니다.	2 영업시간 이내	월요일 – 금요일 영업시간
3	**사소한 업무 영향:** 서비스 또는 기능을 이용할 수 있으며 운영에 대한 심각한 영향이 없는 것을 의미합니다.	4 영업시간 이내	월요일 – 금요일 영업시간
4	**최소 업무 영향:** 조사 또는 비기술적 요청	1 영업일 이내	월요일 – 금요일 영업시간

4.1 고객 데이터에 대한 접근

IBM 은 서비스 문제점을 진단하고 서비스에서 고객의 애플리케이션 스캔을 용이하게 하기 위한 용도로 고객의 데이터에 접근할 수 있습니다. IBM 은 결함을 수정하거나 IBM 제품 또는 서비스에 대한 지원을 제공하기 위한 목적으로만 고객의 데이터에 접근합니다.

5. IBM SaaS 오퍼링 추가 조항

보안 스캔(Security Scans)에서 애플리케이션의 모든 보안 위험을 식별하지는 못할 수 있습니다.

고객은 법률, 규정 또는 관례에 기초한 준수 의무를 이행할 수 있도록 IBM SaaS 를 사용할 수 있습니다. 본 서비스에서 제공한 지침이나 사용 권장사항은 법적 자문이나 회계 또는 기타 전문적인 의견은 아니며 필요한 법적 자문이나 전문가의 의견은 고객이 직접 얻어야 합니다. 고객 및 고객의 활동, 애플리케이션 및 시스템이 관련 법률, 규정, 표준 및 관례를 준수하도록 할 책임은 고객에게 있습니다. 본 서비스를 사용한다고 해서 법률, 규정 또는 관례에 대한 준수가 보장되지는 않습니다.

IBM SaaS 는 고객이 스캔하고자 선택한 웹 사이트와 웹 또는 모바일 애플리케이션에 대해 침투 및 비침투 테스트를 수행합니다. 해당 테스트에는 다음을 포함한(단, 이에 한하지 않음) 특정 위험성이 수반됩니다.

a. 테스트 하에서 애플리케이션을 실행하는 동안 고객의 컴퓨터 시스템이 정지하거나 장애가 발생하여 시스템을 일시적으로 사용할 수 없거나 데이터가 손실될 수 있습니다.

b. 테스트 중에 고객 시스템의 성능과 처리량 및 연관된 라우터와 방화벽의 성능과 처리량이 일시적으로 저하될 수 있습니다.

c. 과다한 로그 메시지가 생성되어 로그 파일 디스크 공간이 과도하게 소모될 수 있습니다.

d. 취약성 조사로 인해 데이터가 변경되거나 삭제될 수 있습니다.

e. 침입 감지 시스템에서 알람을 트리거할 수 있습니다.

f. 테스트 중인 웹 애플리케이션의 이메일 기능이 이메일을 트리거할 수 있습니다.

및

g. 클라우드 서비스가 이벤트 검색 용도로 모니터링되는 네트워크의 트래픽을 가로막을 수 있습니다.

고객이 테스트 중인 애플리케이션의 인증 로그인 신임 정보를 서비스에 입력할 경우 고객은 프로덕션 사용자가 아닌 테스트 계정에 대한 신임 정보만 입력해야 합니다. 프로덕션 사용자 신임 정보를 사용하면 서비스를 통해 개인 정보가 전송될 수 있습니다.

IBM SaaS 는 프로덕션 웹 애플리케이션을 스캔하도록 구성될 수 있습니다. 고객이 스캔 유형을 "프로덕션"으로 설정하는 경우 해당 서비스는 위에 설명된 위험을 감소시키는 방식으로 스캔을 수행하도록 설계됩니다. 단, 특정 상황에서 클라우드 서비스는 테스트된 프로덕션 사이트와 인프라스트럭처 내에서 성능 저하나 불안정성이 나타날 수 있습니다. IBM 은 프로덕션 사이트를 스캔하는 클라우드 서비스 사용의 적합성에 대해 일체의 보증이나 주장을 제공하지 않습니다.

서비스가 고객의 웹 사이트, 웹 애플리케이션, 모바일 애플리케이션 또는 기술 환경에 적합하거나 안전한지 판단할 책임은 고객에게 있습니다.

본 IBM SaaS 는 모바일 및 웹 애플리케이션과 웹 서비스 내의 잠재된 다양한 보안 및 준수 문제점을 식별하기 위해 설계되었습니다. 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 웹 애플리케이션, 시스템 및 직원에 대한 보안과 준수 및 구제 조치는 전적으로 고객의 책임입니다. 서비스에서 제공한 정보를 사용하거나 사용하지 않는 것은 전적으로 고객의 재량입니다.

일부 법률은 컴퓨터 시스템에 침입하거나 액세스하고자 하는 어떠한 불법적인 시도도 금지합니다. 고객은 서비스를 사용하여 고객이 소유하거나 고객에게 스캔 권한이 부여된 웹 사이트 및/또는 애플리케이션이 아닌 다른 웹 사이트 및/또는 애플리케이션을 스캔해서는 안되며, 고객은 이를 확인할 책임이 있습니다.

5.2 쿠키

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

5.3 파생 혜택 사업장

해당하는 경우, 세금은 IBM SaaS 의 혜택이 제공되는 것으로 고객이 정한 사업장을 기준으로 부과됩니다. 고객이 추가 정보를 제공하지 않는 한, IBM 은 IBM SaaS 주문 시 1 차 혜택 사업장으로 제출한 비즈니스 주소에 따라 세금을 적용합니다. 고객은 이러한 정보를 최신 상태로 유지하고 변경사항이 있는 경우 IBM 에 제공해야 할 책임이 있습니다.

부록 A

1. IBM Application Security on Cloud 일반 명세

IBM Application Security on Cloud 는 고객이 다양한 애플리케이션의 보안 취약성(예: SQL 인젝션, 크로스 사이트 스크립팅, 데이터 유출)을 식별할 수 있는 단일 지점을 제공합니다. 이 서비스에는 각각 해당 애플리케이션의 보안 문제점을 식별해내는 다양한 유형의 애플리케이션 보안 스캐닝 기술이 포함됩니다.

IBM Application Security on Cloud 는 다음 기능을 제공합니다.

- 보안 취약성에 대한 모바일 애플리케이션 스캐닝(Scanning Mobile Applications for security vulnerabilities). 동적(블랙박스) 및 대화식(글래스박스) 보안 분석 기술을 통해 수행됩니다.
- 보안 취약성에 대한 프로덕션 또는 사전 프로덕션 웹 사이트 스캐닝(Scanning production or pre-production Web sites for security vulnerabilities). 동적(블랙박스) 보안 분석 기술을 통해 수행됩니다.
- 보안 취약성에 대한 웹 및 데스크탑 애플리케이션 내 데이터플로우 스캐닝(Scanning the dataflows within Web and Desktop applications for security vulnerabilities). 정적(화이트박스) 보안 분석 기술을 통해 수행됩니다.
- 취약성 확인 결과와 개발자가 수행할 수 있는 개선 단계가 포함된 높은 수준의 개요를 포함하는 보안 취약성 상세 보고서.
- 다양한 DevOps 플랫폼(예: Maven, IBM UrbanCode)과의 통합