IBM Application Security on Cloud

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

조건이 상충하는 경우에는 SaaS 특정 오퍼링 조건이 일반 조건에 우선하여 적용됩니다. IBM SaaS 를 주문하거나 액세스하거나 사용함으로써 고객은 이용 약관에 동의하게 됩니다.

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 조건이 적용됩니다.

- IBM Application Security Analyzer
- IBM Application Security on Cloud Consulting Services

2. 청구 체계

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

a. **작업(Job)** – IBM SaaS 가 구매되는 경우 이용되는 산정 단위입니다. 작업(Job)은 IBM SaaS 에서 더 이상 분할될 수 없는 오브젝트로서 모든 하위 프로세스가 포함된 컴퓨팅 프로세스를 의미합니다. 고객의 라이센스 증서(Proof of Entitlement)나 거래서류에 명시된 산정 기간 동안 IBM SaaS 에서 처리하거나 관리하는 작업 총 수를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

b. **애플리케이션 인스턴스(Application Instance)** – IBM SaaS 가 구매되는 경우 이용되는 산정 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 산정 기간 동안 IBM SaaS 에 연결된 애플리케이션 인스턴스 수에 적용될 충분한 권한을 취득해야 합니다.

   본 IBM SaaS 용도:

   - 동적 테스트(Dynamic Testing)용: 공용 또는 개인용 URL 을 통해 주소 지정 가능한 웹 사이트. 각 애플리케이션 인스턴스의 경우 단일 도메인에서 최대 1,000 페이지의 웹 사이트를 사용할 수 있습니다.
   - 정적 테스트(Static Testing)용: 단일 프로그래밍 언어로 실행 가능한 코드 유닛. 각 애플리케이션 인스턴스의 경우 최대 1,000,000 라인의 코드 유닛을 스캔할 수 있습니다.
   - 모바일 테스트(Mobile Testing)용: 모바일 디바이스에서 실행 가능한 바이너리 코드 유닛. 모바일 플랫폼(예: iOS, Android)마다 다른 애플리케이션 인스턴스를 구성합니다.

c. **인스턴스(Instance)** – IBM SaaS 가 구매되는 경우 이용되는 산정 단위입니다. 인스턴스는 IBM SaaS 의 특정 구성에 대한 액세스를 의미합니다. 고객의 라이센스 증서(Proof of Entitlement)나 거래서류에 명시된 산정 기간 동안 액세스하고 사용하기 위해 제공된 IBM SaaS 의 각 인스턴스에 대해 충분한 권한을 취득해야 합니다.

   각 인스턴스 권한의 경우 수행되는 작업 또는 애플리케이션 인스턴스(연결된 애플리케이션)의 수에는 제한이 없으나 단, 임의의 시점에서 실행 가능한 작업은 30 개를 넘을 수 없습니다.

d. **인게이지먼트(Engagement)** - 서비스가 구매되는 경우 이용되는 산정 단위입니다. 인게이지먼트는 IBM SaaS 와 관련된 전문 서비스 및/또는 교육 서비스로 구성됩니다. 각 인게이지먼트(Engagement)를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

3. 대금 및 청구

IBM SaaS 에 대한 청구 금액은 거래서류에 명시됩니다.

3.1 월 분할(Partial Month) 요금

거래서류에 명시된 월 분할 요금은 비례 배분하여 산정될 수 있습니다.

3.2 추가 요금

산정 기간 동안 IBM SaaS 실제 사용량이 라이센스 증서에 명시된 권한을 초과하면 거래서류에 지정된 대로 초과분에 대한 요금이 고객에게 부과됩니다.

3.3 Set Up 대금

set up 요금은 거래서류에 지정된 대로 고객에게 부과됩니다.

4. 기간 및 갱신 옵션

IBM SaaS 의 기간은 라이센스 증서에 명시된 바와 같이, IBM 이 고객에게 IBM SaaS 에 대한 고객의 액세스(접근) 권한에 대해 통지한 날부터 시작됩니다. 라이센스 증서는 IBM SaaS 가 자동으로 갱신되는지, 계속적으로 사용되는지 또는 기간 만료 시 종료되는지를 명시할 것입니다.

자동 갱신의 경우, 고객이 기간 만료일로부터 최소 30 일 이전에 갱신하지 않겠다는 서면 통지를 제공하지 않는 이상 IBM SaaS 는 라이센스 증서에 명시된 기간에 대해 자동으로 갱신됩니다.

계속적인 사용의 경우, 고객이 사전 30 일의 서면 종료 통지를 제출할 때까지 IBM SaaS 는 월단위로 계속 사용할 수 있습니다. 그러한 30 일 기간 이후의 역월(calendar month)의 말일까지 IBM SaaS 가 계속 제공됩니다.

5. 기술 지원

기술 지원은 사용등록 기간(Subscription Period) 동안 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 제공합니다.

심각도(Severity)	심각도 정의	대응 시간 목표	대응 시간 범위
1	**중대한 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 사용에 있어 상당히 제한되거나 고객이 업무 기한을 준수하지 못하게 되는 경우.	2 영업시간 이내	월요일 - 금요일 영업시간
3	**업무에 대한 사소한 영향:** 서비스 또는 기능을 이용할 수 있으며 운영에 대한 심각한 영향은 없습니다.	4 영업시간 이내	월요일 - 금요일 영업시간
4	**최소 업무 영향:** 질문 또는 비기술적 요청	1 영업일 이내	월요일 - 금요일 영업시간

5.1 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.

6. IBM SaaS 오퍼링 추가 조건

보안 스캔은 애플리케이션의 모든 보안 위험성을 식별할 수 있는 것은 아니며, 항공기 항법 시스템, 항공 교통 관제, 무기 시스템, 생명 유지 시스템, 핵시설 또는 보안 리스크를 식별하지 못하여 사망, 개인 상해 또는 재산 손해가 발생할 수 있는 기타 애플리케이션을 포함하여(단, 이에 한하지 않음) 안전 조치(fail-safe operation)가 필요한 위험한 환경에서 사용하도록 설계되거나 의도되지 않습니다. 보안 스캔이 중단이나 오류 없이 작동하는 것으로 보증되지 않습니다.

IBM SaaS 는 고객이 법령, 규정 또는 관례에 기초한 준수 의무를 준수할 수 있도록 지원하는 데 사용될 수 있습니다. 본 서비스에서 제공한 어떠한 지침이나 제안된 사용 또는 안내사항은 법적 자문이나 회계 또는 기타 전문 의견이 아니며 필요한 법적 자문이나 전문가의 의견은 고객이 직접 선임하여 얻어야 합니다. 고객 및 고객의 활동, 애플리케이션 및 시스템이 관련 법률, 규정, 표준 및 관례를 준수하도록 할 책임은 고객에게 있습니다. 본 서비스를 사용한다고 해서 법령, 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. 일부 법률은 컴퓨터 시스템에 침입하거나 액세스하고자 하는 어떠한 불법적인 시도도 금지합니다. 고객은 본 문서에 기술된 서비스를 수행하도록 IBM 에게 권한을 부여하며, 서비스에는 고객의 컴퓨터 시스템에 대해 허가된 접근이 포함된다는 점을 인정합니다. IBM 은 서비스를 수행하는 데 필요하다고 간주되는 경우 제 3 자에게 이러한 권한의 부여에 대해 공개할 수 있습니다.

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.

g. IBM SaaS 가 이벤트 탐색 용도로 모니터링되는 네트워크의 트래픽을 가로막을 수 있습니다.

테스트 활동 중에는 IBM 이 제공하거나 테스트 대상이 되는 웹 사이트 또는 애플리케이션과 관련된 모든 서비스 레벨 계약상 권리 또는 구제 조치는 적용되지 않습니다.

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 열거된 위험을 감소시키는 방식으로 스캔을 수행하도록 설계됩니다. 단, 특정 상황에서 IBM SaaS 는 테스트된 프로덕션 사이트와 인프라스트럭처 내에서 성능 저하나 불안정성이 나타날 수 있습니다. IBM 은 프로덕션 사이트를 스캔하는 IBM SaaS 사용의 적합성에 대해 일체의 보증이나 진술을 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.

IBM 이용 약관 – 일반 조건의 데이터 보호 조건에 명시된 고객 컨텐츠에는 애플리케이션 침입 테스트(Application Penetration Testing) 중에 IBM 에 액세스 가능해진 데이터도 포함되는 것으로 간주됩니다.

6.1 제 3 자 소유 시스템

본 문서에 의거한 테스트의 대상이 되는 제 3 자 소유의 시스템(본 조항의 목적상 애플리케이션 및 IP 주소를 포함하되 이에 한하지 않음)의 경우, 고객은 다음에 동의합니다.

a. 고객은 제 3 의 시스템에서 IBM 이 시행하는 테스트를 수행하기 전에 앞서서, 각 시스템 owner 로부터 IBM 이 해당 시스템에서 서비스를 제공하는 것을 승인하고, 나아가 "Permission to Perform Testing" 섹션상 조건들을 수락한다는 점을 명시하여 서명 날인한 문서를 확보하며, 이러한 승인된 문서 사본을 IBM 에 제공합니다.

b. IBM 원격 테스트를 통해 해당 시스템에서 식별된 위험, 문제점 및 취약점을 시스템 owner 에게 고지하여야 할 전적인 책임이 있습니다.

c. IBM 이 필요하다고 간주한 바에 따라 시스템 owner 와 IBM 간에 정보 교환을 조율하고 이행합니다.

고객은 다음에 동의합니다.

- 테스트 대상 시스템의 ownership 에 대한 변동사항이 있는 경우 즉시 IBM 에 알립니다.
- IBM 의 사전 서면 동의 없이는 인도물에 대해서나 IBM 이 서비스를 수행한 사실을 고객의 기업집단 외부로 공개하지 않습니다.
- 고객이 "제 3 자 소유 시스템" 조건의 요건을 준수하지 못하여 발생한 제 3 자의 클레임으로 인해 IBM 에 발생한 손실 또는 책임에 대해, 그리고 (a) 테스트 대상 시스템의 보안 위험성, 문제점 또는 취약점에 대한 테스트, (b) 고객에게 해당 테스트의 결과 제공, 또는 (c) 이러한 결과에 대한 고객의 사용 또는 공개와 관련하여 IBM, IBM 하도급자 또는 에이전트에게 제기된 제 3 자의 subpoenas 또는 배상 청구에 대해 전적으로 IBM 을 면책합니다.

6.2 쿠키

고객은 IBM 이 IBM SaaS 의 정상적인 운영과 지원 과정에서 트랙킹(tracking) 및 기타 기술을 사용하여 IBM SaaS 사용과 관련된 개인 정보를 고객(귀하의 직원 및 계약직 직원)으로부터 수집할 수 있다는 것을 인정하고 이에 동의합니다. IBM 은 사용자 경험을 개선하거나 고객과의 상호작용을 조정할 목적으로 IBM SaaS 의 효율성에 대한 사용 통계와 정보를 수집합니다. 고객은 관련 법령에 따라 IBM, 다른 IBM 회사들 및 이들의 하도급자들에서, 그리고 IBM 및 IBM 하도급자들이 비즈니스를 수행하는 어디서나, 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 직원 및 계약직 직원의 요청을 수용합니다.

IBM 은 보안 활동을 포함하는 IBM SaaS 의 일부로 IBM SaaS 에서 수집된 비식별화 정보 및/또는 집계 정보("보안 데이터")를 준비하고 관리합니다. 보안 데이터는 아래 (d)에서 제공한 경우를 제외하고, 고객 또는 개인을 식별하지 않습니다. 고객은 또한 IBM 이 다음 용도로만 보안 데이터를 사용하거나 및/또는 복사할 수 있다는 데 동의합니다.

a. 보안 데이터(Security Data)의 게시 및/또는 배포(예: 사이버 보안 관련 분석 및/또는 컴파일)

b. 제품이나 서비스 개발 또는 개선

c. 내부적으로 또는 제 3 자와의 연구 수행

d. 확인된 제 3 자 범죄자 정보의 합법적 공유.

6.3 혜택이 제공된 사업장

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

6.4 개인 정보 및 규제 대상인 컨텐츠 및 서비스

이 IBM SaaS 는 개인 정보 또는 민감한 개인 정보 등, 규제 대상인 컨텐츠에 대한 특정 보안 요구사항에 맞게 설계되지 않습니다. 고객은 IBM SaaS 와 관련하여 고객이 사용하는 컨텐츠 유형에 있어서, IBM SaaS 가 고객의 필요를 충족하는지 판단해야 합니다.

IBM 은 FCC(Federal Communications Commission)나 정부 규제 당국("정부 규제 기관")이 정한 서비스 공급자의 역할을 수행하지 않으며 FCC 나 정부 규제 기관이 정한 서비스를 제공하는 것을 의도하지 않습니다. FCC 나 정부 규제 기관이 본 문서에 의거해서 IBM 이 제공하는 서비스에 규제 요건이나 의무사항을 부과하는 경우, IBM 은 (a) 고객의 비용 부담을 통해서 제품을 수정하거나 교체하거나 대체하고 및/또는 (b) 고객에게 서비스를 제공하는 방식을 변경함으로써(예를 들어, 제 3 의 common carrier 로부터 해당 서비스를 구매하는 고객 에이전트로 역할을 수행) IBM 에 대한 해당 요건이나 의무사항의 적용이 되지 않도록 할 수 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, 공용 또는 사설 네트워크, 웹 사이트 스캐닝(Scanning production or pre-production, publicly facing or on private network, 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 플랫폼과의 통합

1.1 IBM Application Analyzer

IBM Application Analyzer 는 애플리케이션 인스턴스(Application Instance), 작업(스캔) 또는 정식 인스턴스(Instance)별로 주문할 수 있으며 허용되는 스캔 유형은 다음과 같습니다.

- Dynamic Analyzer – DAST 기술을 통한 사전 프로덕션 또는 프로덕션 웹 사이트 테스트
- Mobile Analyzer – IAST 기술을 통한 iOS 또는 Android 바이너리 테스트
- Static Analyzer – SAST 기술을 통한 바이트 코드 또는 소스 코드 데이터 플로우 테스트

1.2 Set Up 서비스

IBM Application Security on Cloud Consulting Services 는 Application Analyzer 의 제품화된 set up 서비스입니다. 이 서비스에서는 IBM 컨설턴트를 통해 애플리케이션 위험성 테스트 및 관리를 위한 지침과 지원을 제공합니다. IBM Application Security on Cloud Consulting Services 는 아래 명시된 수량으로 사용하여 다음 특정 서비스를 요청하고 활용할 수 있는 인게이지먼트(Engagememt) 블록으로 구입합니다.

a. Fast Start[1 인게이지먼트 유닛 사용]

Fast Start 서비스는 Application Security on Cloud 테스트 및 위험성 관리 기능을 사용하기 위한 전문 지식과 지침을 제공합니다. 고객이 Application Security on Cloud 포털의 성공적인 로그인을 확인하고 나면 IBM 은 최대 2 시간 동안 2 명의 활성 참여자가 있는 웹 컨퍼런스를 진행하여 스캔 유형을 포함하고 스캔을 실행하며 보고서를 검토하고 관련 도구 및 플러그인을 설치하는 기본 AppSec on IBM SaaS 구성 및 기능에 대한 교육을 제공합니다. Fast Start 서비스는 (a) 고객 교육 온라인 세미나(webinar), (b) 관련 도구 및 플러그인 설치 및 (c) 고객의 설치 및 최초 스캔 실행에 대한 지원이 완료되고 나면 완료됩니다.

b. Assessment Review[2 인게이지먼트 유닛 사용]

Assessment Review 서비스는 애플리케이션의 취약점을 이해하고 개선책을 우선 처리하며 테스트 결과를 검토하도록 지원을 제공합니다. IBM 은 최대 1 시간 동안 2 명의 활성 참여자가 있는 웹 컨퍼런스를 진행하여 (1) 취약점 테스트 방법, (2) 취약점 감지 방법, (3) 각 취약점의 위험성 및 (4) 취약점 해결을 돕는 일반 수정 권장사항의 제공을 포함하여 발견된 취약점의 개요 및

애플리케이션의 전반적인 보안 위험성과 발견된 애플리케이션 보안 취약점에 대한 세부 논의를 제공합니다. 전적으로 테스트 결과를 바탕으로 검토를 수행하여 소스 코드 자체의 검토는 해당되지 않습니다. 고객은 웹 컨퍼런스 이전에 테스트 결과를 검토하며 IBM 에게 테스트 결과를 검토하도록 확인합니다. Assessment Review 서비스는 웹 컨퍼런스가 완료되고 나면 완료됩니다.

c. Scan for Me[4 인게이지먼트 유닛 사용]

Scan for Me 서비스는 스캔을 구성하여 실행하고 결과의 유효성을 검증하며 결론을 검토하는 보고서 브리핑을 수행하는 IBM 애플리케이션 보안 전문가를 제공합니다. 고객은 스캔을 구성하여 실행하고 결과의 유효성을 검증하며 개선책 우선 처리의 권장사항을 제공하고 결과 보고서 브리핑을 수행하도록 고객의 ASoC 환경에 대한 IBM 컨설턴트 액세스를 허용합니다. IBM 은 최대 1 시간 동안 2 명의 활성 참여자가 있는 웹 컨퍼런스를 진행하여 (1) 취약점 테스트 방법, (2) 취약점 감지 방법, (3) 각 취약점의 위험성 및 (4) 취약점 해결을 돕는 일반 수정 권장사항의 제공을 포함하여 발견된 취약점의 개요 및 애플리케이션의 전반적인 보안 위험성과 발견된 애플리케이션 보안 취약점에 대한 세부 논의를 제공합니다. 요청이 있는 경우 최초 스캔 후 최대 30 일 동안 IBM 은 오직 보안 수정사항을 검증하기 위한 목적으로만 원본 스캔 구성을 사용하여 재스캔을 제공하며, 새로운 기능을 테스트하고 결과의 유효성을 검증하고 고객에게 보고서를 전달하기 위한 목적으로는 제공하지 않습니다. Scan for Me 서비스는 최초 스캔 결과를 검토하는 웹 컨퍼런스가 완료되거나 고객의 요청에 따라 재스캔을 완료하여 재스캔 보고서를 고객에게 전달하고 나면 완료됩니다.

d. Advisor on Demand[7 인게이지먼트 유닛 사용]

Advisor on Demand 서비스는 IBM SaaS 관련 활동에 사용할 수 있는 최대 20 시간의 IBM 컨설턴트 시간을 제공합니다. IBM 컨설턴트는 프로그램 관리, 보안 테스트 우선 처리, 개선 전략, 소스 코드 분석, 소스 코드 수정을 포함한(단, 이에 한하지 않음) 애플리케이션 보안 특정 토픽을 지원합니다. IBM 은 프로젝트 목표, 관련 기술, 적합한 타임라인, 예상 인도물 및 예상 Advisor on Demand 서비스 인게이지먼트 수를 포함하여, 고객의 특정 요구사항이 반영된 프로젝트 스케줄을 이해하고 작성하도록 고객과 협력합니다. 고객은 서비스 수행에 필요한 필수 애플리케이션, 시스템 및 문서에 대한 액세스 권한을 제공해야 합니다. Advisor on Demand 서비스는 최대 20 시간의 보안 전문 기술을 수행한 경우, 및/또는 프로젝트 스케줄 및/또는 프로젝트 스케줄에 정의되어 있는 문서화된 인도물이 고객에게 전달되고 나면 완료됩니다.

e. 애플리케이션 침투 테스트(Application Penetration Testing)

다음 세 가지 옵션이 있습니다.

(1) **준수/엔트리 레벨 애플리케이션 침투 테스트** - 최대 40 시간의 컨설턴트 시간을 포함하며 단일한 단계의 로직 결함 및 단순한 버전의 인젝션 결함에 초점을 둡니다. 15 인게이지먼트 유닛을 사용합니다.

(2) **표준 애플리케이션 침투 테스트** - 최대 60 시간의 컨설턴트 시간을 포함하며 다층적 워크플로우의 로직 결함, 복잡한 버전의 인젝션 결함, 복합 데이터 유형 분석으로 초점을 확대합니다. 21 인게이지먼트 유닛을 사용합니다.

(3) **고급 애플리케이션 침투 테스트** - 최대 80 시간의 컨설턴트 시간을 포함하며 컴파일 실행 파일의 리버스 엔지니어링, 사용자 정의 네트워크 프로토콜 해체, 공용 라이브러리 및 프레임워크 심층 분석으로 초점을 확대합니다. 27 인게이지먼트 유닛을 사용합니다.

애플리케이션 침투 테스트 서비스는 애플리케이션 테스트 및 공격, 테스트 보고서 전달, 결론 및 관련 위험성 보고서 브리핑을 수행하는 IBM 자원을 제공합니다.

IBM 은 최대 1 시간 동안 2 명의 활성 참여자가 있는 프로젝트 시작 콜을 진행하여 애플리케이션 플랫폼, 아키텍처, 프레임워크, 보조 인프라스트럭처, 애플리케이션의 알려진 보안 문제점 또는 관련 사항, 예비 테스트 스케줄, 비상 연락망을 포함한 고객의 환경과 조직을 검토합니다.

IBM 은 다음을 포함한(단, 이에 한하지 않음) 애플리케이션 침투 테스트를 수행합니다: SQL 인젝션, 교차 사이트 스크립팅 등 일반 취약점 식별, 입력 검증, 인증, 권한 부여 등 기존 보안 컨트롤의 강점과 약점 평가, 비즈니스 로직의 적절한 실행에 대한 검사, 보안 프로토콜의 적절한 사용에 대한 검증, 세션 핸들링 결함 식별 및 로그인, 비밀번호 복구, 비밀번호 정책 및 기타 사용자 관리 기능에

대한 적절한 보안 컨트롤의 검증. 애플리케이션 침투 테스트 보고서를 통해 결론을 문서화합니다. IBM 은 최대 1 시간 동안 보고서 브리핑을 위한 웹 컨퍼런스를 진행합니다. 애플리케이션 침투 테스트 서비스는 할당된 컨설턴트 시간을 사용하고 웹 컨퍼런스가 수행되고 애플리케이션 침투 테스트 최종 보고서가 고객에게 제공되면 완료됩니다.

1.2.1 Set Up 서비스 책임사항

IBM 은 다음을 수행합니다.

- 고객이 라이센스 증서별로 구입한 인게이지먼트 유닛을 사용하여 Set Up 서비스를 제공합니다.
- Set Up 서비스는 1.2 항에 기술된 완료 기준을 충족하면 완료됩니다.

고객은 다음에 동의합니다.

- 계약 기간 동안 고객이 요청한 모든 인게이지먼트 요청과 관련된 모든 대금 청구에 대해 책임을 집니다.
- 구입한 인게이지먼트 유닛은 최초 계약 기간 내에 반드시 사용해야 하며 계약 기간 종료일까지 미사용된 경우에는 만료된다는 점을 인정합니다.
- 모든 Set Up 서비스에 대한 공식 요청은 사용등록 종료일에서 최소 30 일 전에 개시되어야 합니다.

IBM 은 Set Up 서비스를 수행하는 과정에서 고객에게 정보 및 합리적 협조를 요청할 수 있습니다. 고객이 요청된 정보나 협조를 적절하게 제공하지 못하는 경우 IBM 의 판단에 따라 서비스에서 필요한 바에 따라 인게이지먼트 유닛 요금을 부과하거나 관련 서비스의 수행이 지연될 수 있습니다.

고객은 IBM 이 테스트를 정확하게 수행하도록 테스트 기간 동안 환경 준비와 유지보수에 관한 IBM 지침을 준수한다는 데 동의합니다.