IBM QRadar Advisor with Watson

본 서비스 명세서는 IBM 이 고객에게 제공하는 서비스에 대해 설명합니다. 고객이란 클라우드 서비스의 대상 회사, 승인된 사용자 또는 수령자를 의미하며 이들을 포함합니다. 관련 견적서와 라이센스 증서(PoE)는 별도의 거래서류(Transaction Documents)로 제공됩니다.

1. 클라우드 서비스

1.1 IBM QRadar Advisor with Watson Service

IBM QRadar Advisor with Watson 은 고객 및 보안 분석가가 위협을 신속하게 조사하고 대응할 수 있도록 코그너티브 분석을 확장합니다. 이 서비스는 Watson for Cyber Security 의 지식 기반(corpus)을 통해 구조화되지 않은 데이터(보안 웹 사이트, 블로그, 연구 논문 포함 등)를 활용하고 로컬 보안 사건과 상호연관시킵니다. 이를 통해 숨은 위협을 밝혀 내고 통찰력을 자동화함으로써 신속한 대응과 의사결정 개선을 도울 수 있습니다. QRadar Advisor with Watson 은 보안 분석가가 수많은 비정형 및 정형 데이터 소스의 지식 기반을 이용하고 이를 다시 당초 보안 공격(가령, 악성 파일, 의심되는 IP 주소, 악의적인 entity 및 이들과의 관계)과 관련된 위협 entity 에 맵핑하여, 보안 공격을 Watson 에 전송함으로써 위협을 감지할 수 있도록 합니다. 이는 보안 공격이 알려진 malware 캠페인과 관련성이 있는지 여부를 판단하는 데 특히 유용할 수 있습니다. 만약 관련성이 있는 경우, Watson 은 여러 통찰력 중에서 사용된 멀웨어의 배경, 악용된 취약점, 위협의 범위(잠재적으로 영향을 받는 추가 엔드포인트 포함)를 제공합니다.

클라우드 서비스를 사용하기 위해서는 고객은 활성화된 IBM Security QRadar 배치가 있어야 하고, 고객이 클라우드 서비스의 기능에 액세스하기 위해서 해당 배치에 클라우드 서비스의 인에이블링 코드가 설치되어 있어야 합니다. 클라우드 서비스에는 고객이 클라우드 서비스에 전송할 수 있는 보안 공격에 대한 쿼리들 수에 대해 'soft limit'이 있는데, 이는 고객이 권한이 부여된 바에 따라 1000 Events Per Second 당 일일 15 개의 비율로 보안 공격에 대한 쿼리들을 할 수 있음을 의미합니다. 이 한도를 초과하여 전송된 쿼리들의 경우에는 클라우드 서비스에서 처리하기는 하지만 우선 순위가 낮아지고 느린 속도로 리턴됩니다.

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial("Trial 클라우드 서비스")은 Trial 형식으로 IBM QRadar Advisor with Watson 의 기능을 제공합니다. 고객은 거래서류나 기타 문서에서 지정한 기간 범위 내에서 Trial 클라우드 서비스에 액세스하게 되며 기간이 종료되면 고객의 액세스는 종료됩니다. 고객은 또한 Trial 기간 동안 보안 공격에 대한 쿼리들을 일일 최대 5 회만 전송할 수 있습니다. Trial 클라우드 서비스는 별도의 보증 없이 '현상태(as is)' 제공되며 고객은 내부 테스트 및 non 프로덕션 용도로만 해당 서비스를 사용할 수 있습니다. 쿼리들에 대한 응답 시간은 Trial 동안에 현재 트래픽 수준에 따라 다를 수 있습니다.

2. 보안 설명

이 클라우드 서비스는 IBM SaaS 에 관한 IBM 데이터 보안 및 개인정보 보호 정책(http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp 참조)과 본 조건에서 제공한 추가 조건을 준수합니다. IBM 데이터 보안 및 개인 정보 보호 정책이 변경되더라도 클라우드 서비스의 보안 수준은 저하되지 않습니다.

고객은 데이터 관리자(data controller)로서 기술적 및 조직적 보안 조치가 처리대상인 위험 및 보호대상인 데이터 성격에 적절하다고 판단하는 경우, 개인 정보가 포함된 선택된 컨텐츠 처리에 이 클라우드 서비스를 사용할 수 있습니다. 고객은 이 클라우드 서비스는 민감한 개인 데이터나 추가적인 규제 요건이 적용되는 데이터를 보호하기 위한 기능을 제공하지 않는다는 점을 인지합니다. 고객은 IBM 은 컨텐츠에 포함된 데이터 유형에 대해 알 수 없으며 클라우드 서비스나 포함된 보안 조치의 적합성을 평가할 수 없다는 점을 인정합니다.

클라우드 서비스를 통해 고객은 다음 컨텐츠만 입력하고 관리할 수 있으며 이들 컨텐츠 중 일부는 관련 개인정보 보호법령상 개인 정보(PI)로 간주될 수 있습니다.

- 목적지(Destination)/소스(Source) IP 주소(IP Addresses)
- URL

- 도메인(Domains)
- 파일 해시(File Hashes)

2.1 보안 기능 및 책임사항

클라우드 서비스는 다음 보안 기능을 구현합니다.

클라우드 서비스에서는 IBM 네트워크와 고객의 IBM Security QRadar 배치 사이에서 데이터가 전송되는 동안 컨텐츠를 암호화합니다. 클라우드 서비스는 데이터 전송을 대기하는 정지 기간 동안 컨텐츠를 암호화하지 않습니다.

클라우드 서비스에서는 데이터에 대해 기능을 수행한 후에는 입력 컨텐츠를 유지(maintain or persist)하지 않습니다.

3. 기술 지원

클라우드 서비스에 대한 기술 지원은 아래 설명과 같이 이메일, 온라인 포럼 및 온라인 문제점 보고 시스템을 통해 제공됩니다. 기술 지원은 클라우드 서비스에 포함되며 별도의 오퍼링으로 제공되지 않습니다.

심각도	심각도 정의	대응 시간 목표	대응 시간 범위
1	**심각한 업무 영향/서비스 다운:** 중대한 업무 기능이 작동하지 않거나 중대한 인터페이스에 장애가 발생한 경우. 일반적으로 프로덕션 환경에 적용되며 서비스에 대한 액세스 불능으로 인해 운영에 중대한 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 영향이 없는 것을 의미합니다.	4 영업시간 이내	월요일 – 금요일 영업시간}
4	**최소 업무 영향:** 조사 또는 비기술적 요청.	1 영업일 이내	월요일 – 금요일 영업시간

클라우드 서비스의 베타에 참여하였으면서 QRadar Platform 7.2.7 버전을 계속 사용하고 있는 고객의 경우, 일부 기술 지원 문제가 해결되지 않을 수 있으며, 이러한 고객은 정식 기술 지원을 받기 위해서는 7.2.8 버전으로 업그레이드하여 최신 패치를 설치해야 합니다.

4. 권한 부여 및 대금 청구 정보

4.1 청구 체계

본 클라우드 서비스는 거래서류에 명시된 바와 같이 다음 청구 체계 하에서 제공됩니다.

a. **초당 100 이벤트(100 Events Per Second)** – 클라우드 서비스가 구매되는 경우 이용되는 산정 단위입니다. 이벤트는 클라우드 서비스에서 처리하거나 클라우드 서비스 사용과 관련된 특정 이벤트의 발생을 의미합니다. 라이센스 증서(PoE)나 거래서류에 명시된 산정 기간 동안 발생한 초당 이벤트 수(가장 가까운 100 단위로 올림)를 포괄할 수 있는 충분한 권한을 취득해야 합니다.

5. 기간 및 갱신 옵션

클라우드 서비스의 기간은 라이센스 증서에 명시된 바와 같이, IBM 이 고객에게 클라우드 서비스에 대한 고객의 액세스(접근) 권한에 대해 통지한 날부터 시작됩니다. 클라우드 서비스를 자동으로 갱신할지, 사용 계속 여부에 따라 갱신할지 또는 기간 만료 시 종료할지 여부는 라이센스 증서(PoE)에 명시합니다.

자동 갱신의 경우, 고객이 기간 만료일로부터 최소 90 일 이전에 갱신하지 않겠다는 서면 통지를 제공하지 않으면 클라우드 서비스는 라이센스 증서에 명시된 기간에 대해 자동으로 갱신됩니다.

계속적인 사용의 경우, 고객이 사전 90 일의 서면 종료 통지를 제출할 때까지 클라우드 서비스를 월단위로 계속 사용할 수 있습니다. 90 일 기간 이후에는 해당 역월(calendar month)의 말일까지 클라우드 서비스가 계속 제공됩니다.

6. 인에이블링 소프트웨어(Enabling Software)

고객은 클라우드 서비스의 사용이 용이하도록 인에이블링 소프트웨어를 고객 시스템에 다운로드하여 사용해야 합니다. 고객은 클라우드 서비스의 사용과 관련해서만 인에이블링 소프트웨어를 사용할 수 있습니다. 인에이블링 소프트웨어는 "현상태대로"("AS-IS") 제공됩니다.

고객은 클라우드 서비스에 대한 인에이블링 소프트웨어를 IBM Security App Exchange(https://exchange.xforce.ibmcloud.com/hub)에서 다운로드할 수 있습니다.

7. 추가 조건

7.1 일반사항

고객은 IBM 이 매스컴이나 마케팅 통신문에서 고객을 클라우드 서비스의 가입자로 공개적으로 언급할 수 있다는 데 동의합니다.

7.2 인에이블링 소프트웨어(Enabling Software)

고객은 클라우드 서비스의 사용이 용이하도록 인에이블링 소프트웨어를 고객 시스템에 다운로드하여 사용해야 합니다. 고객은 클라우드 서비스의 사용과 관련해서만 인에이블링 소프트웨어를 사용할 수 있습니다. 인에이블링 소프트웨어는 "현상태대로"("AS-IS") 제공됩니다.

고객은 클라우드 서비스의 인에이블링 소프트웨어를 IBM Security App Exchange(https://exchange.xforce.ibmcloud.com/hub)에서 다운로드할 수 있습니다.

7.3 클라우드 서비스의 적법한 사용

클라우드 서비스는 고객이 고객의 보안 환경과 데이터를 개선하는 것을 지원하기 위해 설계되었습니다. 클라우드 서비스의 사용에는 개인정보, 데이터 보호, 고용, 전자적 통신 및 저장에 관한 규정을 포함하여, 다양한 법률과 규정이 적용될 수 있습니다. 클라우드 서비스는 합법적인 목적과 방법으로만 사용해야 합니다. 고객은 적용되는 법률, 규정 또는 정책에 의거하여 클라우드 서비스를 사용하고 적용되는 법률, 규정 또는 정책을 준수할 모든 책임이 있다는 것에 동의합니다. 고객은 클라우드 서비스의 적법한 사용을 가능케 하는 데 필요한 동의, 허가 또는 라이센스를 취득할 것이거나 취득하였음을 보증합니다.

7.4 클라우드 서비스 만기

클라우드 서비스가 만료되거나 종료되기 전에 고객은 제공된 클라우드 서비스의 보고 또는 반출 기능을 사용하여 데이터를 추출할 수 있습니다.

7.5 보안 데이터

IBM 은 보안 활동을 포함하는 클라우드 서비스의 일부로 클라우드 서비스에서 수집된 비식별화 정보 및/또는 집계 정보("Security Data, 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.