IBM X-Force Threat Intelligence

본 서비스 명세서는 본 클라우드 서비스에 대해 설명합니다. 관련 주문 서류에서는 고객의 주문에 대한 가격 책정과 추가적인 세부사항을 제공합니다.

1. 클라우드 서비스

IBM X-Force Threat Intelligence 는 정보를 JSON(JavaScript Object Notation)으로 리턴하는 RESTful API 를 통해 IBM X-Force Exchange 에 대한 계획적 액세스를 제공합니다. 이 클라우드 서비스는 또한 STIX(Structured Threat Information eXpression) 및 TAXII(Trusted Automated eXchange of Indicator Information) 표준을 지원합니다. 클라우드 서비스는 사용자를 지원하는 다음 핵심 기능을 제공하도록 설계되었습니다.

a. 정형 및 비정형 컨텐츠로 구성된 특정 보안 조사 정보('컬렉션') 액세스.

b. 사고 유형(예: 멀웨어, 데이터 위반 또는 취약점)에 대한 설명 및 사고의 가관찰 항목 액세스.

c. 상세 리서치의 시작점이 되는 위협 지표를 통한 최신 종합 인텔리전스 및 이들 지표를 이해하기 위한 컨텍스트 확보.

d. 데이터(아래 정의 참조)와 고객의 오퍼링을 통합하여 위협 인텔리젼스 정보 활용.

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM X-Force Exchange Commercial API

IBM X-Force Exchange Commercial API(Application Programming Interface)는 사용자가 IBM 의 클라우드 기반 위협 인텔리전스 공유 플랫폼인 IBM X-Force Exchange 에서 위협 인텔리전스의 사용을 자동화할 수 있도록 합니다. 이 오퍼링은 만 개 항목 단위의 팩으로 판매됩니다.

1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise 는 사용자가 IBM 의 클라우드 기반 위협 인텔리전스 공유 플랫폼인 IBM X-Force Exchange 에서 위협 인텔리전스의 사용을 자동화할 수 있도록 합니다. 이 오퍼링은 인스턴스(Instance)별로 판매됩니다. 하나의 인스턴스(Instance)는 카테고리 피드, IP 및 URL 보고서, 취약성 피드 및 모든 TAXII 피드별로 IP 및 URL 에 대한 무제한의 액세스를 제공합니다. X-Force Exchange 에 없는 지표에 대한 요청은 월 100,000 개 항목으로 제한됩니다.

1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force 는 보안 도구 및 솔루션에 직접 입수하도록 정의된 실행 가능한 지표 세트를 사용자에게 제공합니다. 이 피드는 실행 가능한 손상 지표(IP 및 URL), 분석가 도출 손상 지표 및 DNS Early Warning 지표에 대한 액세스를 제공합니다. 피드는 STIX/TAXII, JSON, Text List 및 CSV 형식을 포함한 여러 형식으로 제공됩니다.

1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

이 클라우드 서비스는 무료로 제공되며 핵심 위협 인텔리전스를 통합하고 Cloud Pak for Security 의 Threat Intelligence Insights 애플리케이션 내에서 피처를 활성화하는 기능을 고객에게 제공합니다. 이 패키지로 고객은 X-Force 권고, 위협 및 및 관련 IOC(IP, URL, 취약점, 해시)를 포함한 X-Force Threat Intelligence 컨텐츠의 무료 티어에 대한 액세스를 제공받습니다. 또한 고객은 환경에서 악의적인 위협을 검색하고 식별할 수 있는 수동 Am-I-Affected 기능을 실행할 수 있습니다. IBM Cloud Pak for Security 의 일부로 사용 가능한 IBM Security Threat Intelligence Insights 애플리케이션은 이 클라우드 서비스를 사용하기 위한 선행 조건입니다.

1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security 는 X-Force 의 다음 세대의 위협 인텔리전스 및 기능을 Cloud Pak for Security 의 Threat Intelligence Insights 애플리케이션에 추가하는 기능을 고객에게 제공하는 프리미엄 패키지입니다. IBM 사고 대응 분석 팀(IRIS 팀)이 선별한 고급 위협 인텔리전스 컨텐츠에는 심층 멀웨어, 위협 그룹, 위협 활동 및 산업 분석 보고서, 시정 권장사항, 손상 지표(IOC) 등이 포함됩니다. 이 Advanced 패키지는 또한 고객이 Am-I-Affected 기능을 지속적으로 자동 실행하도록 하여 사용자의 환경에서 사전에 위협의 우선 순위를 정하여 식별할 수 있도록 합니다. IBM Cloud Pak for Security 의 일부로 사용 가능한 IBM Security Threat Intelligence Insights 애플리케이션은 이 클라우드 서비스를 사용하기 위한 선행 조건입니다.

2. 데이터 처리 및 보호 데이터 시트

IBM 데이터 처리 부칙(Data Processing Addendum: DPA)(http://ibm.com/dpa 참조) 및 아래 링크의 데이터 처리 및 보호 데이터 시트(Data Processing and Protection Data Sheet(s))(데이터 시트(들) 또는 DPA 별표(들)로 참조됨)는 클라우드 서비스에 대한 추가적인 데이터 보호 정보와 처리할 수 있는 컨텐츠의 유형, 관련 처리 활동, 데이터 보호 기능 및 컨텐츠의 보관 및 반환 정보와 관련한 옵션을 제공합니다. DPA 는 컨텐츠에 포함된 개인 데이터에 i) European General Data Protection Regulation (EU/2016/679)(GDPR) 또는 ii) http://ibm.com/dpa/dpl 에 명시된 기타 데이터 보호법이 적용되는 경우 그 범위에 한 해 적용됩니다.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1ECC13601F5911E69AAAC4D0C72C126B

3. 서비스 레벨(Service Levels) 및 기술 지원

3.1 SLA(Service Level Agreement)

IBM 은 다음 가용성 "서비스 레벨 계약"(이하 SLA)을 고객에게 제공합니다. IBM 은 아래 표와 같이 누적 클라우드 서비스 가용성에 따라 적용 가능한 최대의 보상을 적용합니다. 가용률은 약정 월의 총 시간(분)에서 약정 월의 총 Service Down(분)을 차감한 후 이를 약정 월의 총 시간(분)으로 나누어 산출합니다. Service Down 의 정의, 클레임 절차, 서비스 가용성 문제에 관한 IBM 문의 방법은 IBM Cloud 서비스 지원 핸드북(https://www.ibm.com/software/support/saas_support_overview.html)에서 확인할 수 있습니다.

가용성	크레디트 (월별 사용등록료*의 %)
99.9% 미만	2%
99.0% 미만	5%
95.0% 미만	10%

* 사용등록료는 클레임 대상이 되는 해당 월의 약정 요금입니다.

3.2 기술 지원

지원 문의 상세 정보, 심각도 레벨, 가용성 지원 시간, 응답 시간 및 기타 지원 정보와 절차를 포함하여, 클라우드 서비스에 대한 기술 지원은 IBM 지원 안내서(https://www.ibm.com/support/home/pages/support-guide/ 참조)에서 클라우드 서비스를 선택하면 확인할 수 있습니다.

4. 요금

4.1 청구 체계

클라우드 서비스에 대한 과금 체계는 거래서류에 명시됩니다.

이 클라우드 서비스에는 다음 청구 체계가 적용됩니다.

- 인스턴스(Instance)는 클라우드 서비스의 특정 구성에 대한 각 액세스입니다.
- 항목(Item)은 클라우드 서비스에서 관리하거나 처리하거나 클라우드 서비스 사용과 관련된 특정 항목의 발생을 의미합니다. 본 서비스의 목적상, 항목은 단일 쿼리에서 리턴된 각 결과입니다.
- 관리 가상 서버(Managed Virtual Server)(MVS)는 클라우드 서비스에서 관리하는 요청된 프로시저, 명령 또는 애플리케이션을 실행하는 프로세싱 유닛, 메모리 및 입/출력 기능으로 구성됩니다.

5. 추가 조항

2019 년 1 월 1 일 이전에 작성된 클라우드 서비스 계약들(또는 동등한 기본 클라우드 계약들)에는 https://www.ibm.com/acs 에서 제공한 조건들이 적용됩니다.

5.1 확인

고객은 i) IBM 또는 IBM 의 외부 감사원이 고객의 본 계약 준수를 확인하기 위해서 합리적으로 필요한 기록 및 시스템 도구 출력물을 유지하고, IBM 의 요청이 있는 경우 그러한 기록과 시스템 도구 출력을 제공하며, ii) 여하한의 필요한 권한을 즉시 주문하고, 해당 시점에 유효한 IBM 요율에 따라 해당 권한에 대해 그리고 이러한 확인 결과 결정된 기타 대금 및 채무에 대해 IBM 이 청구서에 명시한 대로 지급해야 합니다. 이러한 준수 확인 의무는 클라우드 서비스 기간 및 그 후 2 년 간 효력이 유지됩니다.

5.2 데이터

5.2.1 용어 정의

클라우드 서비스에는 IBM 데이터 및 커뮤니티 데이터에 대한 사용 또는 액세스가 포함됩니다. IBM 은 해당 데이터 및 클라우드 서비스를 통해 사용할 수 있는 모든 제 3 자 컨텐츠를 일체의 보증 없이 제공하며 해당 데이터 또는 제 3 자 컨텐츠에 액세스하거나 사용한 결과로 발생하는 손실에 대해 책임을 지지 않습니다. 다음의 용어 정의가 적용됩니다.

a. **데이터** – 클라우드 서비스를 통해 액세스할 수 있는 여하한 정보, 컨텐츠, 파일, 텍스트, 그래픽, 소프트웨어, 코드, 메시지, 검색 조회 결과, 검색 조회 입력, 토론 포럼 컨텐츠, 방법(method) 또는 기타 자료를 의미합니다.

b. **IBM 데이터** – IBM 이 클라우드 서비스를 통해 고객에게 가용케한 데이터를 의미하며 커뮤니티 데이터는 제외됩니다. IBM, IBM 의 라이센스 제공자 또는 IBM 의 공급자는 IBM 데이터에 대한 모든 권리, 소유권 및 이익을 보유합니다.

c. **커뮤니티 데이터** – 다른 클라우드 서비스 사용자가 클라우드 서비스를 통해 고객에게 가용케 한 데이터를 의미합니다.

5.2.2 IBM 데이터

(i) 고객의 리서치 및 위협 관련 조사를 지원하기 위한 고객의 개인적인 사용 목적으로 또는 (ii) IBM 데이터를 고객의 오퍼링에 통합하기 위한 사용 목적으로, 클라우드 서비스를 통해서만 IBM 데이터에 액세스하고 사용할 수 있는 제한적, 비독점적, 양도 불가능한 라이센스를 고객에게 부여합니다. 고객은 IBM 데이터 또는 클라우드 서비스의 주요 일부나 전체 컨텐츠를 복제하거나 복제를 시도해서는 안됩니다. 고객은 여하한 IBM 데이터에 포함되거나 첨부된 모든 저작권 표시, 정보 및 제한사항을 준수해야 하며, IBM 데이터에 포함된 여하한 텍스트, 저작권 또는 기타 재산권 표시를 제거하면 안됩니다. 고객은 클라우드 서비스에 대한 여하한 액세스 제한사항을 회피하거나 회피하고자 하는 시도는 허용되지 않습니다.

고객은 IBM 데이터를 고객의 오퍼링에 통합한 경우, 최종 사용자 계약에 다음 내용을 포함해야 합니다. (a) 직접적 손해에 대한 고객 및 제 3 자 공급자의 공동 책임을 합리적인 수준으로 제한하고 제 3 자 공급자에 대한 결과적 손해 및 기타 간접적 손해와 묵시적 보증에 대한 모든 책임을 면책하며 (b) 최종

사용자 계약으로 인해 발생한 고객의 최종 사용자의 모든 배상 청구는 고객에게만 제기하도록 하고 (c) 고객의 제품이나 서비스와 별도로 데이터를 사용하는 것을 금지하며 (d) 데이터를 재라이센스 부여하거나 달리 배포하는 것을 금지합니다.

또한 IBM 데이터를 고객의 오퍼링에 통합한 경우에는 관련 법률이나 계약의 조항에 의거해서 고객이 책임을 지는 손해에 추가하여, (a) 전술한 단락의 조항에 대한 비준수 또는 (b) IBM 이 인가하지 않은 IBM 데이터에 관한 주장, 진술, 배상 청구 또는 보증으로 인해 발생한 모든 제 3 자 배상 청구에 대해 IBM 을 변호하고 면책하며 손해가 없도록 보호합니다.

위에서 구체적으로 명시한 경우를 제외하고, 고객은 IBM 데이터를 복사, 수정, 복제, 전송, 판매, 판매제시, 대여, 리스, 라이센스 부여, 재라이센스, 재배포 또는 달리 제 3 자에게 가용케 할 수 없습니다.

5.2.3 커뮤니티 데이터

고객은 커뮤니티 데이터에 대한 액세스를 포함하여, 다른 클라우드 서비스 사용자와의 고객의 상호작용(interaction)에 대해 책임을 집니다. 일부 커뮤니티 데이터는 컬렉션 또는 위협에서 공유될 수 있습니다. 공용으로 사용 가능한 커뮤니티 데이터의 소유자는 클라우드 서비스 사용자에게 해당 커뮤니티 데이터 또는 그 일부를 사용, 복사, 복제, 수정 및/또는 2 차적 저작물을 작성 및 배포할 수 있는 비독점적, 전세계적, 지불 완료된 권리와 라이센스(공용 라이센스)를 부여했습니다. 공용 라이센스에 따라 커뮤니티 데이터를 복사, 복제, 배포 또는 달리 가용케 하는 경우, 고객은 커뮤니티 데이터에 대한 권한 표시를 반드시 제공해야 합니다. 고객은 컬렉션 또는 위협에서 제공된 데이터를 내부적이고 비상업적인 용도로만 사용할 수 있습니다. 고객은 IBM 정책 또는 본 서비스 명세서를 위반하거나 달리 불쾌한 커뮤니티 데이터에 노출될 수 있습니다.

커뮤니티 데이터에는 다른 클라우드 서비스 사용자의 사용자 프로파일 정보가 포함될 수 있습니다. 고객은 위협 인지 정보에 대해 다른 클라우드 서비스 사용자와 통신하기 위한 용도 외에는 프로파일 정보를 데이터마이닝, 복사 또는 달리 사용할 수 없습니다.

커뮤니티 데이터에는 IBM 이 운영하지 않는 웹 사이트의 링크가 포함될 수 있습니다. IBM 은 그러한 웹 사이트의 컨텐츠, 제품, 자료 또는 실무(개인정보 처리방침 포함)에 대해 책임을 지지 않습니다. 고객은 커뮤니티 데이터에 액세스함으로써 불쾌하거나 외설적이거나 달리 이의가 있을 수 있는 제 3 자 웹 사이트에 노출될 수 있다는 것을 이해합니다.

고객은 데이터에 부정확하거나 달리 제거되어야 하는 개인 정보가 포함되어 있다고 간주하는 경우에 X-Force IP Report 내에서 기고 기능을 사용하여 IBM 에 문의할 수 있습니다.

6. 우선 적용 조항

6.1 Cloudflare, Inc. 재처리자

다음은 클라우드 서비스에 대한 당사자 간의 데이터 보안 및 개인정보 보호 원칙에서 모든 상반되는 내용보다 우선하여 적용됩니다: 본 클라우드 서비스는 컨텐츠에 대한 재처리자의 하나로 Cloudflare, Inc.를 이용합니다. Cloudflare 는 클라우드 서비스의 제공을 최적화하기 위해 암호화되지 않은 양식으로 컨텐츠를 처리합니다. Cloudflare 는 레벨 1 서비스 공급자로 PCI 를 준수하며 ISO 27001 및 SOC 2 준수를 위해 노력하고 있습니다. (즉, 본 전반적인 클라우드 서비스는 PCI 준수 제품이 아닙니다.)