IBM QRadar on Cloud

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

1. 클라우드 서비스

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM QRadar on Cloud

IBM QRadar on Cloud 오퍼링은 IBM Security QRadar SIEM 제품을 기반으로 하는 IBM 클라우드에서 고급 보안 인지 솔루션을 제공합니다. 이를 통해 고객은 on-premise 환경과 클라우드 환경 모두에서 생성된 이벤트를 수집, 상관관계 및 저장하고 근무지 사이트에 배치된 QRadar SIEM 제품과 마찬가지로 보안과 위협 관리를 수행합니다. IBM 은 오퍼링의 일부로 24x7 기준의 인프라스트럭처 모니터링도 제공하며 최신 소프트웨어 레벨이나 중요 패치가 제공될 때마다 적용합니다.

이 클라우드 서비스에는 90 일의 검색 가능한 활성 스토리지가 포함되며 초당 100 이벤트(100 Events per Second, EPS)의 수량으로 권한이 부여됩니다.

1.2 선택적 서비스

1.2.1 IBM QRadar on Cloud Temporary Upgrade

임시의 개월 수 동안에 로그 이벤트 수집과 처리 목적으로 1,000 EPS 의 추가 용량을 제공하는 서비스 업그레이드입니다. 고객은 오퍼링이 지원할 수 있는 최대 EPS 레벨의 한도로 업그레이드의 여러 유닛을 구입할 수 있습니다. 이 파트의 목적은 당해 연도 동안 "spike" 중에 적용 대상이 되어야 하는 고객이 임시 용량 업그레이드를 통해 해당 요구사항을 충족할 수 있도록 하는 것입니다. 기간이 종료되면 이러한 임시 용량 증가분은 고객의 환경에서 제거됩니다.

1.2.2 IBM QRadar on Cloud Data Capacity

데이터 용량 업그레이드는 추가 스토리지를 추가하고 분석 기간을 확장합니다. 해당 용량 업그레이드는 각 100 EPS 업그레이드 구매에 대해 최대 만 1 년(full year)의 이벤트 데이터 저장을 고객에게 제공합니다.

1.2.3 IBM QRadar on Cloud Flows Add-On

IBM QRadar SIEM 및 플로우 프로세서와 통합하여 계층 3 네트워크 가시성 및 플로우 분석을 제공함으로써 고객 네트워크 전체의 활동을 감지, 발견하고 대응할 수 있도록 고객을 지원합니다.

이 클라우드 서비스에는 90 일의 검색 가능한 활성 스토리지가 포함되며 분당 10,000 플로우(10,000 Flows per Minute, FPM)의 수량으로 권한이 부여됩니다.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

네트워크 디바이스와 애플리케이션의 보안 취약성을 사전에 감지하고 발견하여 컨텍스트를 추가하고 개선 및 완화 활동의 우선 순위를 지정하도록 지원합니다.

1.2.5 IBM QRadar on Cloud Log Archival

고객이 사용등록된 기간 동안 클라우드 서비스의 이벤트 데이터를 아카이브할 수 있도록 합니다. IBM 은 고객과 협력하여 지정된 이벤트를 오브젝트 스토리지에 아카이브 용도로 작성합니다. 고객의 요청에 따라 IBM 은 해당 요청으로부터 3 영업일 이내에 최대 30 일 분량의 아카이브된 이벤트 데이터를 클라우드 서비스의 고객 인스턴스에 재마운트합니다. 해당 데이터는 아카이브 오브젝트 스토리지에 리턴되기 전에 48 시간 동안 사용 가능한 상태로 유지됩니다. 고객은 3 개월의 기간당 최대 두 번의 요청을 할 수 있습니다. 해당 용량 업그레이드는 각 100 EPS 업그레이드 구매에 대해 최대 만 1 년(full year)의 데이터 저장을 고객에게 제공합니다.

1.2.6 IBM QRadar on Cloud Flows Add-On Data Capacity

데이터 용량 업그레이드는 각 10,000 FPM 업그레이드 구입에 대해 최대 만 1 년(full year)의 플로우 데이터 저장을 고객에게 제공합니다.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

이 오퍼링은 고객이 사용등록된 기간 동안 클라우드 서비스의 플로우 데이터를 아카이브할 수 있도록 합니다. IBM 은 고객과 협력하여 지정된 플로우 레코드를 오브젝트 스토리지에 아카이브 용도로 작성합니다. 고객의 요청에 따라 IBM 은 해당 요청으로부터 3 영업일 이내에 최대 30 일 분량의 아카이브된 플로우 데이터를 클라우드 서비스의 고객 인스턴스에 재마운트합니다. 해당 데이터는 아카이브 오브젝트 스토리지에 리턴되기 전에 48 시간 동안 사용 가능한 상태로 유지됩니다. 고객은 3 개월의 기간당 최대 두 번의 요청을 할 수 있습니다. 해당 용량 업그레이드는 구입한 각 10,000 FPM 업그레이드에 대해 최대 만 1 년(full year)의 데이터 저장을 고객에게 제공합니다.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

IBM QRadar on Cloud for Non-Production Environment 오퍼링은 이 클라우드 서비스의 전용 테스트 인스턴스를 제공합니다. 이를 통해 고객은 on-premise 환경과 클라우드 환경 모두에서 생성된 이벤트를 수집, 상관관계 및 저장하고 전용 테스트 환경 내의 근무지 사이트에 배치된 QRadar SIEM 제품과 마찬가지로 보안과 위협 관리를 수행합니다. IBM 은 오퍼링의 일부로 24x7 기준의 인프라스트럭처 모니터링도 제공하며 최신 소프트웨어 레벨이나 중요 패치가 제공될 때마다 적용합니다. 고객은 이 클라우드 서비스를 비 프로덕션 테스트 용도로만 사용할 수 있습니다.

이 클라우드 서비스에는 90 일의 검색 가능한 활성 스토리지가 포함됩니다.

1.3 Acceleration 서비스

1.3.1 IBM QRadar on Cloud Optimization Service

원격으로 제공되는 이 사용등록 서비스의 경우 IBM 은 고객의 클라우드 서비스 인스턴스의 현재 상태를 평가하고 개선이 필요한 영역을 확인하는 QRadar on Cloud Health Status 보고서를 통해 고객에게 결과를 전달하는 검토 회의를 고객과 함께 수행합니다.

또한, IBM 은 고객의 요청에 따라 다음 컨설팅 서비스 중 하나를 1 년 기간 이내에 최대 8 일 동안 고객에게 제공합니다.

- 클라우드 서비스에 추가 로그 소스를 추가하는 작업 지원
- 추가적인 검색, 보고서 및 대시보드 구성
- 기존 QRadar 배치에 대한 추가 조정 작업, 및
- 관련 QRadar 주제에 대한 지식 이전 작업.

1.3.2 설치(Setup) 서비스

다음 설치(setup) 서비스는 원격으로 제공되며 별도로 주문이 가능합니다. 주문된 각 서비스는 달리 명시하지 않은 한, 시간을 모두 사용했는지(해당하는 경우) 여부에 관계 없이 구입 시점으로부터 90 일에 만료됩니다. 서비스에는 킥오프 콜을 스케줄링하는 지정된 IBM Engagement Manager 가 포함됩니다.

a. IBM QRadar on Cloud Deployment Services

이 서비스는 IBM 이 다음 중 일부 또는 전체를 수행하는 동안에 40 시간의 전문 서비스를 제공합니다.

IBM 은 고객의 보고 요구사항을 정의하기 위한 최대 16 시간의 SIEM 아키텍처 검토를 수행하며 고객의 요구사항을 정의하고 파악할 수 있도록 돕는 솔루션 아키텍처 보고서를 통해 관련 결과를 고객에게 전달합니다.

이 보고서에는 다음이 포함됩니다.

- 고객의 준수, 감사 및 보안 인텔리전스 요구사항을 충족하기 위한 고객 정의 보고 요구사항.
- IBM 이 구현 과정을 지원할 수 있는 보안 인텔리전스 요구사항, 유스 케이스 및 앱(최대 10 개 유스 케이스 및 최대 2 개 앱).

- 유스 케이스를 지원하기 위해 필요한 고객의 로그 및 플로우 소스의 고급 정보.
- 방화벽, 포트 등 네트워크 인프라스트럭처 주의사항.

IBM 은 솔루션 아키텍처 보고서를 기초로 하여 잔여 시간에 따라 다음을 수행합니다.

- 최대 10 개 로그 소스 유형의 최대 3 개 인스턴스에 대한 이벤트 컬렉션을 클라우드 서비스에 구성. 필요에 따라 이 활동에서는 고객의 관련 담당자에게 지식을 이전하여 추가 로그 소스를 추가할 수 있도록 합니다. 이 서비스에는 표준 QRadar Device Support Modules(DSMs)에서 지원하는 로그 소스만 포함됩니다.
- 초기 튜닝. 이에는 다음이 포함됩니다: a) out-of-the-box 규칙, 저장된 검색, 누적 시계열 그래프 및 보고서 활성화, b) 노이즈의 원인 확인과 제거, 및 c) NFS, CIFS 또는 iSCSI 를 통한 오프라인 스토리지 구성.
- 솔루션 아키텍처 문서에 기록된 IBM QRadar App Exchange 의 10 개 유스 케이스 및 2 개 앱 구현.

b. IBM QRadar on Cloud Custom Parser Service

이 서비스는 클라우드 서비스로 전송하게 되는 고객의 비표준 로그 소스 유형을 지원하기 위해 단일 사용자 정의 구문 분석기/uDSM 를 개발하는 기능을 제공하며 다음 작업을 포함합니다.

- 하나의 비표준 로그 소스 유형에 대한 사용자 정의 구문 분석기 작성(원격 수행 작업)
- uDSM 작성, 구성 및 맵핑
- 사용자 정의 uDSM 배치 및 테스트, 및
- 로그 소스에 대한 최대 25 개 메시지 유형의 구문 분석.

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=FB0F42F0750011E6865BC3F213DB63F7

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.

- 계약(Engagement)은 클라우드 서비스들과 관련된 프로페셔널 서비스 또는 트레이닝 서비스입니다.
- 초당 이벤트(Events Per Second)는 클라우드 서비스에서 처리하거나 클라우드 서비스 사용과 관련된 특정 이벤트의 초당 발생 횟수를 의미합니다.
- 분당 플로우(Flows per Minute)는 클라우드 서비스에서 관리하거나 처리한 분당 플로우 수입니다. 하나의 플로우는 두 호스트 간의 통신에 대한 하나의 레코드입니다. 동일한 소스 IP, 대상 IP, 소스 포트, 대상 포트 및 프로토콜이 포함된 패킷은 하나의 플로우 레코드로 결합됩니다.
- 자산(Asset)은 클라우드 서비스에서 액세스하거나 관리하는, 고유하게 식별된 유형(tangible)의 가치 자원이나 항목입니다.

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 인에이블링 소프트웨어(Enabling Software)

인에이블링 소프트웨어는 다음 조건에 따라 고객에게 제공됩니다.

인에이블링 소프트웨어(Enabling Software)	해당 라이센스 조항(해당하는 경우)
데이터 게이트웨이(Data Gateway)	고객은 데이터 게이트웨이 사본을 최대 10 부의 한도 내에서만 설치하고 사용할 수 있습니다.