IBM QRadar Advisor with Watson

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

1. 클라우드 서비스

IBM QRadar Advisor with Watson 은 고객 및 보안 분석가가 위협을 조사하고 대응할 수 있도록 코그너티브 분석을 QRadar Security Platform 으로 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 대응과 의사 결정을 위한 통찰력을 자동화합니다. 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.

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watson 을 사용하기 위해서는 고객은 로컬 온프레미스 환경이나 클라우드 배치 중 하나에 활성화된 IBM QRadar 배치가 있어야 하고 고객이 클라우드 서비스의 기능에 액세스하기 위해서 해당 배치에 클라우드 서비스의 인에이블링 소프트웨어가 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 100 Events Per Second 당 일일 1.5 개 요청 비율로 보안 공격에 대한 쿼리들을 클라우드 서비스로 전송할 수 있음을 의미합니다. 이 한도를 초과하여 전송된 쿼리들은 당일 나머지 시간 동안 클라우드 서비스에서 처리하지 않습니다.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise 는 일반적으로 초당 250,000 이벤트 이상을 초과하는 대형 보안 운영 센터(SOC) 배치에 가장 적합합니다. 클라우드 서비스의 기능에 액세스하기 위해서는 별도로 취득한 IBM QRadar 배치에 클라우드 서비스의 인에이블링 소프트웨어를 반드시 설치해야 합니다. IBM QRadar Advisor with Watson – Enterprise 는 고객의 IBM QRadar 배치 규모와 관계 없이 인스턴스(Instance)별 과금 체계에 따라 사용 가능합니다. 고객은 언제든지 큐에서는 25 개 제출로 제한됩니다.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack 은 QRadar Advisor with Watson 을 처음 사용하는 사용자를 위한 제품입니다. 이 클라우드 서비스는 제 1.1.1 항에서 설명한 바와 같이 QRadar Advisor with Watson 의 모든 기능을 갖추고 있지만 고객이 QRadar Advisor with Watson 을 처음 구매한 경우에만 사용이 가능하며 갱신되지 않습니다.

1.2 선택적 서비스

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment 는 클라우드 서비스를 내부 테스트 환경에 배치하고자 하는 고객을 위한 것이며 비 프로덕션 테스트 용도로만 사용될 수 있습니다. IBM QRadar

Advisor with Watson – Test Environment 는 프로덕션 용도의 클라우드 서비스 사용등록을 통해 보완되어야 합니다.

1.3 Acceleration 서비스

1.3.1 IBM QRadar Advisor with Watson Advanced Services

이 원격 제공 사용등록 서비스의 경우, IBM 은 다음 컨설팅 서비스 중 하나를 1 년 기간에 최대 5 일 동안 고객에게 제공합니다.

- 조사 및/또는 사고 대응 절차를 포함한 고객 SOC 프로세스 평가,
- 참조 세트 대응 재평가,
- 대규모 공격에 대한 자동 분석 조정,
- 유스 케이스 개발,
- QRadar Advisor with Watson 을 통합하는 SOC 프로세스 변경에 대한 권장사항 제공,
- QRadar Advisor with Watson 의 데이터를 가장 효율적으로 이해하고 고객의 기존 프로세스에 통합하는 방법에 대한 지침 제공,
- 관련 QRadar Advisor with Watson 주제에 대한 지식 이전 작업.

참고: 고객의 QRadar 배치 상태에 따라 이 서비스에 다음 활동들이 통합될 수 있습니다.

- 고객의 QRadar 배치에 대한 상태 확인,
- 기존 QRadar 배치에 대한 추가 조정 작업,
- 고객의 QRadar 배치에 추가 로그 소스를 추가하는 작업 지원.

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

이 설치(setup) 서비스는 원격으로 제공되며 달리 명시하지 않은 한, 시간을 모두 사용했는지(해당하는 경우) 여부에 관계 없이 구입 시점으로부터 90 일에 만료되는 40 시간의 전문 서비스를 포함합니다. 서비스에는 킥오프 콜을 스케줄링하는 지정된 IBM Engagement Manager 가 포함됩니다.

IBM 은 다음 사항의 일부 또는 전체를 수행합니다.

- 조사 및/또는 사고 대응 절차를 포함한 고객 SOC 프로세스 평가,
- 고객의 환경에서 QRadar Advisor with Watson 구현:
  - QRadar Advisor with Watson 설치,
  - 통합 특성을 QRadar Advisor with Watson 에 맵핑,
  - 참조 세트 대응 구현,
  - 대규모 공격에 대한 자동 분석 조정,
  - 유스 케이스 안내,
  - QRadar Advisor with Watson 을 통합하는 SOC 프로세스 변경에 대한 권장사항 제공.

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

이 설치(setup) 서비스는 5,000 EPS(초당 이벤트) 미만의 고객을 위한 서비스입니다.

이 원격 제공 서비스의 경우, IBM 은 다음 컨설팅 서비스 중 하나(또는 결합 형태)를 90 일 기간에 최대 16 시간 동안 고객에게 제공합니다.

- QRadar Advisor with Watson 설치.
- QRadar Advisor with Watson 권한 관리.
- 다음을 포함한 QRadar Advisor with Watson 구성:
  - 보안 프록시 서버 구성,
  - X-Force 교환 신임 정보 제출,
  - 승인된 서비스 토큰 작성,

- 분석 결과를 저장하기 위한 보관 정책 구성,
- 이벤트 특성 맵핑 사용자 정의,
- 참조 세트 내보내기,
- 위협 인텔리젼스 맵핑,
- 자산 ID 구성,
- 사용 최적화,

- 자동 공격 조사 및 결과(최소 하나의 유스 케이스 쇼케이스).
- 관계 그래프를 통한 통찰력 탐색.

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=0B439290AB5011E6BE74C84817AAB206

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.

- 초당 이벤트(EPS, Event Per Second)는 클라우드 서비스에서 처리하거나 클라우드 서비스 사용과 관련된 특정 EPS 의 발생을 의미합니다. 본 클라우드 서비스의 목적상, 초당 이벤트(Events per Second)는 고객의 IBM QRadar 배치에서 수집하고 처리한 항목입니다.
- 인스턴스(Instance)는 클라우드 서비스의 특정 구성에 대한 각 액세스입니다.
- 인게이지먼트(Engagement)는 클라우드 서비스들과 관련된 프로페셔널 서비스 또는 트레이닝 서비스입니다.

5. 추가 조건

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)

클라우드 서비스에는 다음 인에이블링 소프트웨어가 포함됩니다.

- IBM QRadar with Watson App(https://exchange.xforce.ibmcloud.com/hub)

5.2 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 법령, 규정 또는 정책에 의거하여 클라우드 서비스를 사용하고 적용되는 법령, 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.

6. 우선 적용 조항

6.1 데이터 사용

다음이 당사자들 간의 기본 클라우드 서비스 조건 중 컨텐츠 및 데이터 보호 조항에서 상반되는 내용보다 우선하여 적용됩니다: IBM 은 고객의 클라우드 서비스 사용(즉 고객의 컨텐츠(인사이트)에 고유한 사항 또는 달리 고객을 식별할 수 있는 사항)으로부터 발생하는 결과를 활용하거나 공개하지 않습니다. 그러나 IBM 은 클라우드 서비스를 제공하는 과정에서 고객 식별 항목을 제거하는 조건으로 추가적인 정보의 사용 없이는 여하한 개인 정보가 더 이상 특정 개인에게 귀속될 수 없게 된 컨텐츠 및 컨텐츠에서 발생하는 다른 정보(인사이트는 제외)를 사용할 수 있습니다. IBM 은 연구, 테스트 및 오퍼링 개발 목적으로만 해당 데이터를 사용합니다.