IBM Resilient Security Orchestration, Automation and Response on Cloud

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

1. 클라우드 서비스

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud 는 조직에서 사고 대응과 관련된 사람, 프로세스, 기술을 오케스트레이션하고 자동화할 수 있도록 해줍니다.

IBM Resilient SOAR Platform on Cloud 는 사고 대응과 개인정보 보호 대응 관리를 일원화하여 조직이 이벤트 및 사고에 대응하는 더 신속하고 더 유연하며 자동화된 방식을 제공합니다. Resilient SOAR Platform on Cloud 는 조직이 다음을 수행할 수 있도록 성공적인 사이버 보안 방어의 토대를 제공합니다.

- 업계 표준 및 우수 사례에 기초한 대응 계획 마련.
- 보안 및 IT 도구와의 더 용이한 통합 및 이벤트와 사고에 대한 대응 오케스트레이션.
- 조직 전반의 협업을 통해 다양한 이해 당사자가 사고 대응 과정에서 자신의 역할과 작업을 이행할 수 있는 도구를 갖춤.

IBM Resilient SOAR Platform 은 다양한 규모와 복합적인 조직에 맞게 설계되었으며 여러 가지 선택적 추가 기능(add-ons)과 함께 구입할 수 있습니다. 고객은 구입한 오퍼링이나 추가 기능(add-on)에 명시되어 있지 않은 기능은 사용할 수 없습니다.

1.1 오퍼링

고객은 사용 가능한 다음 오퍼링 중에서 선택할 수 있습니다.

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration 은 사이버 보안 방어의 기초를 제공합니다. 고객은 업계 표준 및 우수 사례에 기초한 대응 계획을 마련하고 보안 및 IT 도구와 용이하게 통합하며 이벤트 및 사고에 대한 대응을 오케스트레이션할 수 있습니다. 이 클라우드 서비스는 조직 간의 협업이 용이하도록 하여 사고 대응 과정에서 다양한 이해 당사자가 자신의 역할과 작업을 수행할 수 있도록 합니다.

보안 팀은 플랫폼의 특수 사례 관리 기능을 사용하여 사이버 보안 이벤트 및 사고에 대해 협업할 수 있습니다. Dynamic Playbooks 는 빠르게 진화하는 공격에 적응하고 팀은 플레이북, 데이터 필드, 디스플레이 레이아웃을 사용자 정의하여 효율성 개선을 위해 프로세스를 신속하게 반복할 수 있습니다. 시뮬레이션은 대응 프로세스의 개선을 지원합니다. 내장 및 설치 가능한 통합은 보안 팀의 의사 결정에 필요한 컨텍스트를 수집하고 구입한 월별 조치(Actions per Month) 수량에 따라 개선 조치를 조정할 수 있도록 데이터를 강화합니다. 이메일 수집 및 구문 분석은 다른 도구로부터 이관할 수 있는 간단한 방법을 제공합니다. 액세스는 SAML 인증을 사용하여 보호할 수 있습니다. 투명성 및 위험 분석은 분석 및 보고를 통해 지원됩니다. 이 오퍼링은 아래의 기타 모든 추가 기능(add-ons)을 위해 필요합니다.

1.2 선택적 서비스

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions 는 플랫폼의 오케스트레이션 기능을 활성화합니다. 다양한 위협 인텔리전스 피드와의 통합을 포함하여, 내장 및 설치 가능한 통합은 개선 조치의 오케스트레이션 뿐만 아니라 보안 팀의 의사 결정에 필요한 컨텍스트를 수집하기 위해 자동화된 인리치먼트를 제공합니다.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy 는 고객이 정보 보호 위반을 평가하고 이에 대응할 수 있도록 해줍니다. 이 오퍼링을 통해 마련된 대응 계획은 정보 유형, 레코드 수량 및 적용되는 규제 국가에

맞게 조정됩니다. 고객은 사고 대응 계획을 세부적으로 조정할 수 있도록 글로벌 정보 보호 위반 통지 규정의 기본 제공 지식 기반에 액세스할 수도 있습니다.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams 는 여러 팀 간의 사용자 관리와 데이터의 분리를 제공합니다. 민감한 정보에 대해서는 Workspaces 및 맞춤형 역할 기반 액세스 제어를 통해 액세스를 제한하여 알아야 할 필요가 있는 사용자에게만 알리도록 합니다. 사용자 및 그룹 관리는 사용자 권한의 Active Directory 를 활용하여 단순화합니다. 별도의 그룹들이 자체 조직을 가질 수 있도록 구성할 수도 있습니다.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP 는 여러 조직을 통해 케이스 관리, 프로세스, 커스터마이제이션 및 플레이북 관리 기능을 제공합니다. 여러 조직의 이벤트 및 사고를 하나의 큐에서 볼 수가 있어 관리 보안 서비스 제공자(MSSP) 분석가에게 고객에 대한 종합적인 시각을 제공합니다. 조직별 구성이 포함된 플레이북은 표준화된 프로세스와 맞춤형 프로세스 모두에 대한 단순 관리 기능을 제공합니다.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production 은 고객이 테스트, 성능 조정, 결함 진단, 내부 벤치마킹, 품질 보증 활동 설명 및/또는 공개된 API(Application Progamming Interfaces)를 사용하여 내부적으로 사용되는 클라우드 서비스의 추가 기능 또는 확장 기능의 개발을 포함하여(단, 이에 한하지 않음) 내부 비프로덕션 활동 용도에 한해서만 사용할 수 있는 IBM Resilient SOAR Platform 의 별도의 인스턴스입니다.

1.3 Acceleration 서비스

IBM Security Expert Labs (SEL) for Resilient Services 오퍼링은 Resilient 배치에 있어 아키텍처 및 구현에 대하여 안내하는 Resilient 전문가의 시간을 제공하는 원격 제공 서비스입니다. IBM Resilient Security, Orchestration and Response 오퍼링(클라우드 서비스 또는 온프레미스 소프트웨어 형식 중 하나)은 이러한 서비스의 선행 조건입니다.

1.3.1 IBM SEL for Resilient Base Starter Service

IBM 은 5 일 간의 원격 인게이지먼트에서 다음을 제공합니다.

- IBM Security Resilient 아키텍처에 대한 정의 지원
- IBM Security Resilient 설치 및 구성(해당하는 경우)
- 고객의 현재 사고 대응 계획을 구성하고 사용하도록 분석가 및 디자이너를 훈련하고 고객 조직의 핵심 요구사항을 반영
- 고객 조직의 고유 프로세스에 기반한 IBM Security Resilient 구성 플레이북
- 고객 조직의 필요 및 업계 우수 사례에 따라 정의된 KPI 및 메트릭 추적 방법 및
- 엔드투엔드 프로세스를 지원, 자동화 및 오케스트레이션하는 통합 기회 파악.

1.3.2 IBM SEL for Resilient Premium Starter Service

IBM 은 3 일 간의 원격 인게이지먼트에서 다음을 수행합니다.

- IBM Security Resilient 아키텍처에 대한 정의 지원
- IBM Security Resilient 설치(해당하는 경우)
- 고객의 환경에 IBM Security Resilient 초기 구성 및
- 고객의 현재 사고 대응 계획을 구성하고 사용하도록 분석가 및 디자이너를 훈련하고 조직의 핵심 요구사항을 반영.

1.3.3 IBM SEL for Resilient Additional Day

IBM 은 Base 또는 Premium Starter 서비스 외에, 1 일 간의 원격 인게이지먼트 동안 미리 합의된 IBM Security Resilient 관련 활동을 수행합니다. 예를 들면, 다음과 같습니다.

- IBM Security Resilient 또는 확장 기능의 설치 또는 구성에 대한 추가 지원(해당하는 경우),
- 고객의 핵심 SOAR 솔루션으로 IBM Security Resilient 를 사용할 준비가 되도록 분석가에 대한 추가 교육 또는 지원,
- 고객 조직의 핵심 요구사항을 반영하는 자체 '플레이북'을 구성하고 사용하는 방법을 디자이너에게 안내, 또는
- IBM Security Resilient 환경을 빠르게 스캔하여 잠재적 개선 영역 권장.

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://www.ibm.com/dpa/dpl 에 명시된 기타 데이터 보호법이 적용되는 경우 그 범위에 한해 적용됩니다.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

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.

- 승인된 사용자(Authorized User)는 어떠한 방법, 어떠한 형태로든(예, 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버 등을 통해) 직접 또는 간접적으로 클라우드 서비스에 액세스하도록 권한이 부여된 고유한 사용자를 의미합니다.
- 동시 사용자(Concurrent User)는 특정 시점에 직접적 또는 간접적으로(예를 들어 다중 송신 프로그램, 디바이스 또는 애플리케이션 서버를 통해) 클라우드 서비스에 동시에 액세스하는 사용자입니다. 클라우드 서비스에 여러 번 동시에 액세스하는 한 명의 개인은 동시 사용자 한 명으로 계산됩니다.
- 인게이지먼트(Engagement)는 클라우드 서비스들과 관련된 전문 서비스 또는 교육 서비스입니다.
- 항목(Item)은 클라우드 서비스에서 관리하거나 처리하거나 클라우드 서비스 사용과 관련된 특정 항목의 발생을 의미합니다. 본 클라우드 서비스의 목적상, 하나의 항목은 하나의 조치(Action)입니다. 조치(Action)란 클라우드 서비스가 다른 소프트웨어 프로그램에 대해 수행한 오케스트레이션이나 자동화 요청입니다.

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 추가 기능(Add-On) 권한 요구사항

고객은 기본 클라우드 서비스 및 추가 기능(Add-On) 클라우드 서비스 모두에 대해 동등한 수와 유형의 권한을 취득해야 합니다.

5.3 사용 제한사항

각 고객은 매월 최대 십만(100,000) 개의 위협 서비스(Threat Service) 조회를 작성할 수 있습니다. 고객은 위협 서비스가 활성화되어 있으면 사고에 아티팩트를 추가하여 위협 서비스 조회를 작성합니다. 그 이후 2 일마다 사고는 열려 있고 활성 상태를 유지하므로 신규 위협 서비스 조회는 자동으로 생성됩니다.

각 고객은 승인된/동시 사용자(Authorized/Concurrent User)당 일일 최대 백(100) 개의 알림 이메일을 생성할 수 있습니다. 고객이 관리하는 구성에 따라 복원성(Resilient) 플랫폼에서는 알림 이메일을 생성합니다.

5.4 추가 데이터 처리 및 보호 정보

혼란을 방지하기 위해, IBM Resilient SOAR Platform on Cloud 는,

- 컨텐츠를 저장 시(at rest)에 암호화하지 않습니다.
- 어떠한 특수 범주의 개인정보도 처리하도록 설계되지 않았습니다. 및
- 요청이 없는 경우 자유 텍스트 필드에 개인 데이터를 입력하지 않습니다.

암호화 및 처리 대상 개인정보 유형에 관한 자세한 정보는 위의 2 조에 언급된 데이터 시트 URL 에서 확인할 수 있습니다.

6. 우선 적용 조항

6.1 데이터 사용

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 서비스의 향상을 위해서 클라우드 서비스의 일부로 컨텐츠 및 컨텐츠에서 생성된 기타 정보(인사이트 제외)를 사용합니다. IBM 은 또한 위협 감지 및 보호 용도로 컨텐츠에 내장된 위협 식별자 및 기타 보안 정보를 공유할 수 있습니다.