IBM Resilient Security Orchestration, Automation and Response on Cloud

В настоящем Описании Услуги описывается Облачная Услуга. В соответствующих документах заказа указываются цены и дополнительные сведения о заказе Клиента.

1. Облачная Услуга

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud позволяет организациям обеспечить координацию и автоматизацию работы пользователей, процессов и технологий, связанных с реагированием на инциденты.

IBM Resilient SOAR Platform on Cloud оптимизирует реагирование на инциденты и управление реагированием на нарушение конфиденциальности за счёт автоматизации, ускорения и повышения гибкости этих процессов. Resilient SOAR Platform on Cloud создаёт основу для успешной защиты от киберугроз, которая позволяет организациям:

- Создавать планы реагирования, основанные на отраслевых стандартах и оптимальных методах.
- Упростить интеграцию систем безопасности и ИТ-систем и координировать процессы реагирования на события и инциденты.
- Осуществлять совместную работу в масштабах всей организации, предоставляя различным участникам процесса инструменты для выполнения их ролей и обязанностей по реагированию на инциденты.

IBM Resilient SOAR Platform подойдёт для организаций любого размера и сложности. Это решение можно приобретать вместе с несколькими дополнительными компонентами. Клиенту не разрешается использовать функции, если это не указано в приобретённом предложении или дополнительном компоненте.

1.1 Предложения

Клиент может выбрать из следующих доступных предложений:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration закладывает основу для защиты от киберугроз. Клиенты могут создавать планы реагирования на основе отраслевых стандартов и рекомендаций, упростить интеграцию систем безопасности и ИТ-систем и координировать процессы реагирования на события и инциденты. Облачная Услуга помогает наладить совместную работу в масштабах всей организации, способствуя эффективному распределению ролей и обязанностей по реагированию на инциденты среди всех заинтересованных лиц.

Специализированные средства управления обращениями помогают службам безопасности взаимодействовать при реагировании на события и инциденты, связанные с кибербезопасностью. Dynamic Playbooks могут адаптироваться к стремительно меняющимся угрозам, а сотрудники получают возможность дорабатывать процессы для повышения их эффективности путём настройки сценариев, полей данных и макетов выводимой информации. Моделирование даёт дополнительные возможности для отладки процессов реагирования. Встроенные и дополнительные средства интеграции обеспечивают обогащение данных для сбора контекстной информации, которая помогает службе безопасности принимать решения и координировать действия по реагированию в соответствии с количеством приобретённых Действий в Месяц. Средства получения и анализа сообщений электронной почты упрощают эскалацию проблем из других инструментов. Для защиты доступа может применяться аутентификация SAML. Средства аналитики и формирования отчётности обеспечивают прозрачность и помогают при анализе рисков. Это предложение является обязательным для всех других указанных ниже дополнительных услуг.

1.2 Дополнительные Услуги

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions обеспечивает функции координации на платформе. Встроенные и дополнительные средства интеграции, в том числе для интеграции с различными каналами информирования об угрозах, осуществляют автоматизированное обогащение данных для сбора контекстной информации, которая помогает службе безопасности принимать решения и координировать действия по реагированию.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy позволяет Клиентам проводить оценку нарушений конфиденциальности данных и реагировать на такие инциденты. Планы реагирования, создаваемые в рамках этого предложения, адаптируются с учётом типов данных, количества записей и действующей юрисдикции. Клиенты также могут получать доступ к встроенной базе знаний с правилами обеспечения конфиденциальности данных и уведомления о нарушениях. Эта база знаний способствует повышению эффективности планов реагирования на инциденты.

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

IBM Resilient SOAR Platform on Cloud Teams предоставляет средства управления пользователями и разделения данных для различных подразделений. Конфиденциальная информация предоставляется на основе принципа необходимого знания путём ограничения доступа к рабочим областям и настраиваемого управления доступом на основе ролей. Использование службы Active Directory для авторизации пользователей помогает упростить управление группами и пользователями. Возможна настройка собственных Организаций для отдельных групп.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP предоставляет средства управления обращениями, процессами и сценариями, а также средства настройки для различных Организаций. События и инциденты в различных Организациях можно просматривать в единой очереди, что позволяет аналитикам поставщика управляемых услуг безопасности (MSSP) получить полное представление о своих заказчиках. Сценарии, настроенные на уровне организации, упрощают управление стандартизированными и настраиваемыми процессами.

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

IBM Resilient SOAR Platform on Cloud Non-Production - это отдельный экземпляр IBM Resilient SOAR Platform, который Клиент может использовать только для внутренней непроизводственной деятельности, включая, в частности, тестирование, настройку производительности, диагностику сбоев, внутреннее эталонное тестирование, контроль качества и (или) разработку предназначенных для внутреннего использования дополнений или расширений для Облачной Услуги с помощью API.

1.3 Услуги по ускорению внедрения (Acceleration Services)

Предложения IBM Security Expert Labs (SEL) for Resilient Services — это дистанционные услуги, в рамках которых эксперты Resilient выдают рекомендации по архитектуре и внедрению в отношении развёртывания Resilient. Предварительным требованием для любой из этих Услуг является предложение IBM Resilient Security, Orchestration and Response – в виде Облачной Услуги или локального программного обеспечения.

1.3.1 IBM SEL for Resilient Base Starter Service

В течение 5-дневного удалённого взаимодействия, IBM предоставит:

- помощь при определении архитектуры IBM Security Resilient;
- установленный и настроенный экземпляр IBM Security Resilient (если применимо);
- обучение для аналитиков и проектировщиков по настройке и использованию планов реагирования на инциденты Клиента с учётом ключевых требований организации Клиента;
- сценарии IBM Security Resilient, настроенные с учётом уникальных процессов организации Клиента;
- способ отслеживания заданных KPI и показателей в соответствии с потребностями организации Клиента и лучшими отраслевыми практиками; и

- возможности интеграции для поддержки, автоматизации и управления комплексным процессом.

1.3.2 IBM SEL for Resilient Premium Starter Service

В течение 3-дневного удалённого взаимодействия, IBM:

- поможет определить архитектуру IBM Security Resilient;
- установит IBM Security Resilient (если применимо);
- выполнит начальную настройку IBM Security Resilient в среде Клиента; и
- проведёт обучение для аналитиков и проектировщиков по настройке и использованию планов реагирования на инциденты Клиента с учётом ключевых требований организации.

1.3.3 IBM SEL for Resilient Additional Day

В дополнение к услуге Base или Premium Starter в рамках 1-дневного удалённого взаимодействия IBM выполнит любые заранее оговорённые действия, относящиеся к IBM Security Resilient. Например:

- дальнейшая поддержка установки или настройки IBM Security Resilient или расширений (если применимо);
- дальнейшее обучение или поддержка аналитиков с целью обеспечения готовности к использованию IBM Security Resilient в качестве ключевого решения SOAR Клиента;
- помощь проектировщикам в настройке и использовании собственных сценариев, отражающих ключевые требования организации Клиента; или
- выполнение быстрого сканирования среды IBM Security Resilient с целью выявления областей для потенциальных улучшений.

2. Обработка и защита Данных – Спецификации

Дополнение IBM об Обработке Данных (DPA), приведённое на веб-странице http://ibm.com/dpa, и Спецификации обработки и защиты данных (именуемые спецификациями или Приложениями к DPA), ссылки на которые приводятся ниже, содержат дополнительную информацию о защите данных в Облачных Услугах и её вариантах в зависимости от типа Содержимого, подлежащего обработке, применяемых операциях обработки, функциях защиты данных и особенностях сохранения и возврата Содержимого. DPA применяется к персональным данным, входящим в Содержимое, в том случае, если, и в той мере, в какой применяются i) Общеевропейский регламент о защите персональных данных (GDPR) (EU/2016/679); или ii) другие законы о защите данных, указанные на веб-странице http://www.ibm.com/dpa/dpl.

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

3. Уровни обслуживания и Техническая поддержка

3.1 Соглашение об уровне обслуживания

IBM предоставляет Клиенту следующее соглашение об уровне обслуживания в отношении доступности услуг (SLA). IBM будет применять наивысший применимый размер компенсации на основе совокупных показателей доступности Облачной Услуги в соответствии с нижеприведённой таблицей. Показатель доступности в процентах вычисляется как общее число минут за договорной месяц минус общее число минут Простоя Услуги за договорной месяц, делённое на общее число минут в договорном месяце. Определение Простоя Услуги, процесс подачи претензий и способы информирования IBM о проблемах с доступностью услуги приводятся в справочнике по поддержке Облачных Услуг IBM, который можно найти на веб-странице по адресу: https://www.ibm.com/software/support/saas_support_overview.html.

Доступность	Кредит (% месячной платы за подписку*)
Менее 99,9%	2%
Менее 99,0%	5%
Менее 95,0%	10%

* Плата за подписку - это договорная цена за месяц, являющийся предметом претензии.

3.2 Техническая поддержка

Информацию о Технической поддержке для Облачной Услуги, включая контактные данные службы поддержки, уровни серьёзности, часы работы, время ответа и другие сведения о поддержке и применимых процессах, можно найти, выбрав раздел "Облачная Услуга" в руководстве IBM по поддержке, доступном на веб-странице по адресу https://www.ibm.com/support/home/pages/support-guide/.

4. Платежи

4.1 Системы расчёта оплаты

Системы расчёта оплаты для Облачной Услуги указываются в Документе по Транзакции.

К данной Облачной Услуге применяются следующие системы расчёта оплаты:

- Авторизованный Пользователь — это отдельный пользователь, которому разрешается осуществлять доступ к Облачным Услугам любым прямым или опосредованным способом (например, через программу-мультиплексор, устройство или сервер приложений) с помощью любых средств.
- Одновременно Работающий Пользователь - это пользователь, одновременно обращающийся к Облачной Услуге любым прямым или опосредованным способом (например, через программу-мультиплексор, устройство или сервер приложений) в любой момент времени. Лицо, одновременно с другими обращающееся к Облачной Услуге несколько раз, считается одним Одновременно работающим Пользователем.
- Поручение – это профессиональные услуги или услуги по обучению, связанные с Облачными Услугами.
- Элемент - это экземпляр конкретного элемента, который обрабатывается, управляется Облачной Услугой или связан с использованием Облачной Услуги. Для этой Облачной Услуги Элементом является Действие. Действие - это запрос на оркестровку или автоматизацию, отправляемый Облачной Услугой в другую компьютерную программу.

5. Дополнительные положения

К Соглашениям об Облачных Услугах (или эквивалентным базовым соглашениям об облачных инфраструктурах), заключённым до 1 января 2019 года, применяются положения, приведённые на веб-странице https://www.ibm.com/acs.

5.1 Проверка

Клиент будет i) сохранять и предоставлять по запросу записи и выходные данные системных инструментов в той мере, в какой это обоснованно необходимо IBM и её независимым аудиторам для проверки соблюдения Клиентом Соглашения, и ii) незамедлительно заказывать и оплачивать необходимые разрешения по действующим на тот момент тарифам IBM, а также вносить другие платежи и выполнять другие обязательства, выявленные в результате такой проверки, в соответствии со счетами IBM. Эти обязательства, связанные с проверкой соблюдения требований, остаются в силе в течение срока действия Облачной Услуги и в течение двух лет после его окончания.

5.2 Требование в отношении разрешений на дополнения

Клиент должен приобрести разрешения в одинаковом количестве и одного и того же типа как на базовую Облачную Услугу, так и на любое Дополнение (Add-On).

5.3 Ограничения использования

Каждый Клиент имеет право отправить максимум сто тысяч (100000) запросов Threat Service в месяц. Клиент создаёт запрос Threat Service путём добавления артефакта в инцидент при активации Threat Service. Каждые последующие два (2) дня, пока инцидент остаётся открытым и активным, будет автоматически создаваться новый запрос Threat Service.

Каждый Клиент имеет право создавать максимум сто (100) писем с уведомлениями в день на каждого Авторизованного / Одновременно работающего Пользователя. Письма с уведомлениями создаются платформой Resilient на основе конфигурации, управляемой Клиентом.

5.4 Дополнительная информация об обработке и защите данных

Во избежание сомнений, IBM Resilient SOAR Platform on Cloud:

- не обеспечивает шифрование Содержимого в процессе хранения;
- не предназначен для обработки каких-либо Особых Категорий Персональных Данных; и
- не требует ввода персональных данных в простые текстовые поля, если это не будет запрошено дополнительно.

Подробная информация о шифровании и типах обрабатываемых Персональных Данных доступна по ссылке на технический документ, указанной в Разделе 2.

6. Условия, имеющие преимущественную силу

6.1 Использование данных

IBM не будет использовать и раскрывать результаты использования Облачной Услуги Клиентом, являющиеся уникальными для Содержимого Клиента (Аналитические данные) или иным образом идентифицирующие Клиента. Однако IBM будет использовать Содержимое и другую информацию, полученную из Содержимого (за исключением Аналитических данных) в ходе предоставления Облачной Услуги, для усовершенствования Облачной Услуги. IBM может также распространять информацию об идентификаторах угроз и другие сведения о безопасности, которые есть в Содержимом, в целях обнаружения угроз и защиты от них.