IBM QRadar on Cloud

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

1. Облачная Услуга

1.1 Предложения

Клиент может выбрать из следующих доступных предложений:

1.1.1 IBM QRadar on Cloud

Предложение IBM QRadar on Cloud предоставляет расширенное решение по аналитике безопасности в среде IBM Cloud на основе продукта IBM Security QRadar SIEM. Оно позволяет Клиентам собирать, сопоставлять и хранить информацию о событиях, генерируемых в локальных и облачных средах, и осуществлять управление безопасностью и угрозами аналогично тому, как они делали бы это с помощью продукта QRadar SIEM, развёрнутого локально. В составе этого предложения IBM предоставляет также круглосуточный (в режиме 24x7) мониторинг инфраструктуры и применяет новейший уровень программного обеспечения (ПО) или критически важных временных исправлений ПО при наличии таковых.

Эта Облачная Услуга предусматривает активное хранение данных с возможностью поиска в течение 90 (девяноста) дней и предоставляет право на обработку 100 Событий в Секунду (EPS).

1.2 Дополнительные Услуги

1.2.1 IBM QRadar on Cloud Temporary Upgrade

Расширенная версия услуги, которая предоставляет дополнительную мощность в 1000 EPS для сбора и обработки зарегистрированных событий, но только на ограниченное количество месяцев. Клиент может приобрести несколько единиц этой расширенной версии, вплоть до максимального уровня EPS, который предложение в состоянии поддерживать. Этот компонент призван помочь Клиенту, который сталкивается со случаями резкого увеличения количества событий в течение года, удовлетворять такие потребности с помощью временного увеличения мощности. По окончании такого периода эти временно добавленные мощности будут удалены из среды Клиента.

1.2.2 IBM QRadar on Cloud Data Capacity

Эта услуга расширяет ёмкость хранилища и период анализа. В рамках услуги Клиенту предоставляется возможность хранения данных о событиях вплоть до 1 полного года для каждых 100 дополнительно приобретённых Событий в Секунду.

1.2.3 IBM QRadar on Cloud Flows Add-On

Интеграция с IBM QRadar SIEM и обработчиками потоков данных обеспечивает анализ потоков данных и прозрачность сети на уровне 3, что позволяет упростить обнаружение выполняемых по сети операций и реагирование на них.

Эта Облачная Услуга предусматривает активное хранение данных с возможностью поиска в течение 90 (девяноста) дней и предоставляет право на обработку 10 000 Потоков в Минуту (FPM).

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Упреждающее распознавание и выявление уязвимостей в безопасности приложений и сетевых устройств предоставляет контекстную информацию и помогает определить приоритет действий по устранению и смягчению последствий.

1.2.5 IBM QRadar on Cloud Log Archival

Предоставляет Клиенту возможность архивировать данные событий, получаемые из Облачной Услуги, в период действия подписки. IBM вместе с Клиентом обеспечит запись определённых событий в объектном хранилище для целей архивирования. По запросу Клиента IBM восстановит данные событий, архивированные за период до 30 (тридцати) дней, в экземпляре Облачной Услуги Клиента в течение 3 (трёх) рабочих дней с момента такого запроса. Данные будут доступны

Клиенту в течение 48 часов, после чего они будут возвращены в хранилище архивных объектов. Клиент может осуществлять до двух таких запросов в течение трёхмесячного периода. Увеличение ёмкости предоставляет Клиенту возможность хранения данных вплоть до 1 полного года для каждых 100 дополнительно приобретённых Событий в Секунду.

1.2.6 IBM QRadar on Cloud Flows Add-On Data Capacity

Эта услуга расширяет ёмкость хранилища и период анализа и предоставляет Клиенту возможность хранения данных потоков вплоть до 1 полного года для каждых 10 000 дополнительно приобретённых Потоков в Минуту.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

Это предложение предоставляет Клиенту возможность архивировать данные потоков, получаемые из Облачной Услуги, в период действия подписки. IBM вместе с Клиентом обеспечит запись определённых записей потоков в объектном хранилище для целей архивирования. По запросу Клиента IBM восстановит данные потоков, архивированные за период до 30 (тридцати) дней, в экземпляре Облачной Услуги Клиента в течение 3 (трёх) рабочих дней с момента такого запроса. Данные будут доступны Клиенту в течение 48 часов, после чего они будут возвращены в хранилище архивных объектов. Клиент может осуществлять до двух таких запросов в течение трёхмесячного периода. Увеличение ёмкости предоставляет Клиенту возможность хранения данных вплоть до 1 полного года для каждых 10 000 дополнительно приобретённых Потоков в Минуту.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

Предложение IBM QRadar on Cloud for Non-Production Environment предоставляет выделенный тестовый экземпляр Облачной Услуги. Оно позволяет Клиентам собирать, сопоставлять и хранить информацию о событиях, генерируемых в локальных и облачных средах, и осуществлять управление безопасностью и угрозами аналогично тому, как они делали бы это с помощью продукта QRadar SIEM, развёрнутого локально, только в пределах выделенной тестовой среды. В составе этого предложения IBM предоставляет также круглосуточный (в режиме 24x7) мониторинг инфраструктуры и применяет новейший уровень ПО или критически важных временных исправлений ПО при наличии таковых. Клиент имеет право использовать эту Облачную Услугу только для целей непроизводственного тестирования.

Эта Облачная Услуга предусматривает активное хранение данных с возможностью поиска в течение 90 (девяноста) дней.

1.3 Услуги по ускорению внедрения (Acceleration Services)

1.3.1 IBM QRadar on Cloud Optimization Service

Для этой услуги, предоставляемой дистанционно по подписке, IBM проведёт обзорное совещание с Клиентом для оценки текущего состояния экземпляра Облачной Услуги Клиента и предоставит Клиенту результаты в виде отчёта QRadar on Cloud Health Status, в котором будут указаны области для улучшения, если такие будут выявлены.

Кроме того, по запросу Клиента IBM будет предоставлять ему любые из указанных ниже консультационных услуг вплоть до 8 (восьми) в течение 1 года:

- Помощь в добавлении дополнительных источников журналов событий в Облачную Услугу;
- Настройка дополнительных поисковых запросов, отчётов и информационных панелей;
- Дополнительная настройка имеющегося развёртывания QRadar; и
- Передача знаний о релевантных субъектах QRadar.

1.3.2 Услуги настройки

Указанные далее услуги по настройке заказываются отдельно и предоставляются в дистанционном режиме. Срок действия каждой заказанной услуги истекает через девяносто (90) дней с момента покупки (если не указано иное) независимо от того, были ли использованы все положенные часы (если это применимо). В рамках Услуг будет назначен менеджер проекта со стороны IBM, который будет планировать вводные совещания.

a. **IBM QRadar on Cloud Deployment Services**

Данная услуга предусматривает предоставление профессиональных услуг продолжительностью 40 (сорок) часов, в течение которых IBM выполнит некоторые или все следующие задачи:

IBM проведёт оценку архитектуры SIEM в течение максимум 16 часов для определения требований Клиента к отчётности и предоставит Клиенту полученные результаты в виде отчёта об архитектуре решения, который поможет определить и зафиксировать требования Клиента.

Этот отчёт должен содержать следующие данные:

- Требования к отчётности, определённые Клиентом, призванные помочь Клиенту соблюдать требования по соответствию нормативам, аудиту и анализу безопасности.
- Требования к анализу безопасности, варианты использования и приложения, с внедрением которых может помочь IBM (до 10 (десяти) вариантов использования и до 2 (двух) приложений).
- Общая информация об источниках журналов событий и потоков Клиента, которые потребуются для поддержки вариантов использования.
- Рекомендации по сетевой инфраструктуре, такой как брандмауэры и порты.

На основании отчёта об архитектуре решения IBM выполнит следующие действия, насколько это позволит оставшееся время:

- Настройка коллекции событий максимум для 3 (трёх) экземпляров максимум 10 (десяти) типов источников журналов событий в Облачной Услуге. Эта деятельность предусматривает передачу знаний соответствующим сотрудникам Клиента, чтобы они могли добавлять источники журналов событий по мере необходимости. В состав этой услуги входят только источники журналов событий, поддерживаемые стандартными модулями QRadar Device Support Module (DSM).
- Начальная настройка, которая включает: a) активацию готовых правил, сохранённых поисковых запросов, графиков и отчётов по накопленным временным рядам; b) определение и удаление источников шума; и c) настройку автономного хранилища с использованием NFS, CIFS или iSCSI.
- Внедрение 10 (десяти) вариантов использования и 2 (двух) приложений IBM QRadar App Exchange, указанных в документе по архитектуре решения.

b. **IBM QRadar on Cloud Custom Parser Service**

Эта услуга предусматривает разработку одного пользовательского анализатора/uDSM для поддержки нестандартных типов источников журнала событий Клиента, передаваемых в Облачную Услугу, и выполнение следующих задач:

- Создание пользовательского анализатора для одного нестандартного типа источника журнала событий (работа выполняется дистанционно);
- Создание, настройка и сопоставление uDSM;
- Развёртывание и тестирование пользовательского uDSM; и
- Анализ до двадцати пяти типов сообщений для источника журнала событий.

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=FB0F42F0750011E6865BC3F213DB63F7

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:

- Поручение – это профессиональные услуги или услуги по обучению, связанные с Облачными Услугами.
- Событий в Секунду - это количество конкретных произошедших за секунду событий, обрабатываемых Облачными Услугами или связанных с использованием Облачных Услуг.
- Потоков в Минуту - это количество потоков в минуту, которыми управляют или которые обрабатывают Облачные Услуги. Поток - это запись обмена данными между двумя хостами. Пакеты, которые содержат один и тот же исходный IP-адрес, целевой IP-адрес, исходный порт, целевой порт и протокол, объединяются в одну запись Потока.
- Актив – это уникально идентифицируемый вещественный ресурс или объект, имеющий ценность, к которому обращаются или которым управляют Облачные Услуги.

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 Поддерживающее программное обеспечение

В Облачную Услугу входит следующее Поддерживающее Программное обеспечение:

Поддерживающее Программное обеспечение	Применимые условия лицензий (при наличии таковых)
Data Gateway	Клиент может устанавливать и использовать до 10 (десяти) копий Data Gateway.

6. Условия, имеющие преимущественную силу

6.1 Использование данных

Несмотря ни на какие противоречащие положения раздела "Содержимое и защита данных" базовых условий соглашения об Облачной Услуге между сторонами, преимущественную силу имеют следующие положения: 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.