

## IBM QRadar Advisor with Watson

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

### 1. Облачная Услуга

IBM QRadar Advisor with Watson добавляет в QRadar Security Platform средства когнитивной аналитики, помогающие Клиентам и аналитикам безопасности расследовать угрозы и реагировать на них. Используя обширную базу знаний Watson for Cyber Security, этот компонент анализирует неструктурированные данные (среди которых веб-сайты о безопасности, блоги, исследовательские статьи) и сопоставляет результаты с локальными инцидентами безопасности. Благодаря этому решение способно помочь в выявлении скрытых угроз и автоматизации анализа операций реагирования и принятия решений. QRadar Advisor with Watson позволяет специалисту по безопасности отправить описание нарушения безопасности в Watson, чтобы с помощью его базы знаний, опирающейся на сотни тысяч источников структурированных и неструктурированных данных, обнаружить угрозу и её предпосылки и первопричины: вредоносные файлы, подозрительные IP-адреса, фальшивые объекты и взаимосвязи между ними. Это может быть особенно полезным при определении взаимосвязи какого-либо нарушения безопасности с известной вредоносной кампанией. Если такая связь прослеживается, Watson среди прочего выдает контекстную информацию о задействованном вредоносном ПО, использованных уязвимостях и области распространения угрозы (включая дополнительные конечные точки, которые также могут быть затронуты).

#### 1.1 Предложения

Клиент может выбрать из следующих доступных предложений.

##### 1.1.1 IBM QRadar Advisor with Watson

Для IBM QRadar Advisor with Watson требуется наличие у Клиента активного экземпляра IBM QRadar, развёрнутого в локальной среде или в облаке. Также у Клиента должно быть установлено поддерживающее ПО для Облачной Услуги, позволяющее Клиенту осуществлять доступ к функциям Облачной Услуги. Облачная Услуга имеет "мягкое ограничение" на количество запросов о нарушениях безопасности, которые Клиент может отправлять в Облачную Услугу в объёме 1,5 запроса в день на 100 Событий в Секунду (округляется до ближайшего числа запросов), на которые имеет право Клиент. Запросы, превышающие это ограничение, не будут обрабатываться Облачной Услугой в оставшуюся часть соответствующего дня.

##### 1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise лучше всего подходит для крупных центров обеспечения безопасности (SOC), стандартно обрабатывающих свыше 250000 Событий в Секунду. Для доступа к функциям Облачной Услуги Клиент должен установить в отдельно приобретённой системе IBM QRadar поддерживающее ПО для Облачной Услуги. Плата за IBM QRadar Advisor with Watson – Enterprise рассчитывается по количеству Экземпляров и не зависит от масштаба развёртывания IBM QRadar у Клиента. В любой момент количество заявок Клиента в очереди не должно превышать 25.

##### 1.1.3 IBM QRadar Advisor with Watson – Starter Pack

Услуга IBM QRadar Advisor with Watson – Starter Pack предназначена для тех, кто впервые пользуется QRadar Advisor with Watson. Эта Облачная Услуга предлагает все функции QRadar Advisor with Watson, перечисленные в разделе 1.1.1 выше, однако доступна только при первоначальной покупке Клиентом QRadar Advisor with Watson и не допускает продление.

### 1.2 Дополнительные Услуги

#### 1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment предназначена для Клиентов, которым требуется развернуть Облачную Услугу с внутренней тестовой средой. Это предложение можно

использовать только для непроизводственных задач тестирования. Для IBM QRadar Advisor with Watson – Test Environment требуется подписка на Облачную Услугу производственного уровня.

### 1.3 Услуги по ускорению внедрения (Acceleration Services)

#### 1.3.1 IBM QRadar Advisor with Watson Advanced Services

В рамках этой удалённой услуги, предоставляемой по подписке, IBM предоставит Клиенту любые из следующих консультационных услуг объёмом вплоть до 5 дней в течение 1 года:

- Оценка процесса SOC Клиента, включая процесс расследования инцидентов и/или реагирования на инциденты;
- Повторная оценка реагирования на контрольные наборы;
- Корректировка автоматического анализа серьёзных нарушений;
- Разработка сценария использования;
- Предоставление рекомендаций по изменению процесса SOC с применением QRadar Advisor with Watson;
- Предоставление указаний по наиболее эффективному анализу и внедрению данных QRadar Advisor with Watson в имеющиеся процессы Клиента;
- Передача знаний о релевантных субъектах QRadar Advisor with Watson.

ПРИМЕЧАНИЕ: Следующие операции могут быть включены в данную услугу в зависимости от статуса развёртывания QRadar Клиента:

- Проверка работоспособности развёрнутого экземпляра QRadar Клиента;
- Дополнительная настройка имеющегося развёрнутого экземпляра QRadar;
- Помощь в добавлении дополнительных источников журналов событий в развёрнутый экземпляр QRadar Клиента;

#### 1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Эта услуга настройки предоставляется дистанционно и включает сорок (40) часов профессиональных услуг, срок действия которых 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.

IBM выполнит некоторые или все следующие задачи:

- Оценка процесса SOC Клиента, включая процесс расследования инцидентов и/или реагирования на инциденты;
- Внедрение QRadar Advisor with Watson в среде Клиента:
  - Установка QRadar Advisor with Watson;
  - Сопоставление унифицированных свойств с QRadar Advisor with Watson;
  - Реализация реагирования на контрольные наборы;
  - Корректировка автоматического анализа серьёзных нарушений;
  - Подготовка указаний по сценариям использования;
  - Предоставление рекомендаций по изменению процесса SOC с применением QRadar Advisor with Watson.

## 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) Европейский

регламент о защите персональных данных (GDPR) (EU/2016/679); или ii) другие законы о защите данных, указанные на веб-странице <http://ibm.com/dpa/dpl>.  
<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206>

### 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](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:

- Событие в Секунду (EPS) - это конкретное произошедшее EPS, обрабатываемое Облачными Услугами или связанное с их использованием. В контексте данной Облачной Услуги События в Секунду - это события, которые собираются и обрабатываются в экземпляре IBM QRadar Клиента.
- Экземпляр – это каждый доступ к определённой конфигурации Облачных Услуг.
- Поручение – это профессиональные услуги или услуги по обучению, связанные с Облачными Услугами.

### 5. Дополнительные положения

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

#### 5.1 Поддерживающее Программное обеспечение

В Облачную Услугу входит следующее Поддерживающее Программное обеспечение:

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

## **5.2 Законное использование Облачной Услуги**

Облачная Услуга призвана помочь Клиенту в усовершенствовании условий безопасности и данных. Использование настоящей Облачной Услуги может повлечь применение различных законов или нормативных актов, в том числе тех, которые касаются конфиденциальности, защиты данных, трудовых отношений, а также электронного взаимодействия и хранения информации. Облачную Услугу можно использовать только в законных целях и законным способом. Клиент соглашается использовать Облачную Услугу в соответствии с применимыми законами, нормативными актами и правилами и берёт на себя всю ответственность за соблюдение применимых законов, нормативных актов и правил. Клиент заявляет, что он получит (или уже получил) любые согласия, разрешения или лицензии, необходимые для поддержки законного использования Облачной Услуги.

## **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 может использовать Содержимое и другую информацию (кроме Аналитических данных), полученную из Содержимого в ходе предоставления Облачной Услуги, при условии удаления персональных идентификаторов, что означает невозможность соотнести никакие персональные данные с конкретным человеком без использования дополнительной информации. IBM будет использовать такие данные исключительно в целях исследований, тестирования и разработки предложений.