**Техническая спецификация**

**Услуги по модернизации IBM Security QRadar SIEM, а также по постгарантийные и технические поддержки.**

|  |  |  |
| --- | --- | --- |
| **Общие требования** | | |
| **1** | **Наименование** | Модернизация IBM Security QRadar SIEM и оказания услуг по постгарантийной и технической поддержке |
| **2** | **Единицы измерения** | Услуга |
| **3** | **Количество** | 1 |
| **4** | **Общие требования** | В рамках оказания услуг Исполнитель должен:  - провести работы по модернизации IBM Security QRadar SIEM в соответствии с характеристиками текущей технической спецификации;  - обеспечить локальную техническую поддержку сроком на 12 месяцев IBM Security QRadar SIEM в соответствии с характеристиками текущей технической спецификации.  - обеспечить официальную постгарантийную поддержку сроком на 12 месяцев IBM Security QRadar SIEM со стороны производителя IBM. |
| **5** | **Условия услуг по технической поддержке** | Все обращения классифицируются на различные уровни обслуживания (SLA).  Уровни обслуживания отличаются временем обработки обращений (и другими параметрами) и зависят от категории обращения.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Устранение аварийных ситуаций** | | | | | | № | Серьезность /влияние на бизнес | Описание | Линия поддержки | Среднее время исполнения\* | | 1 | Высокий | Присваивается Инцидентам с полной или частичной потерей работоспособности Системы. Отсутствие доступа к системе у Заказчика. Полная утрата работоспособности Системой. Недоступность основных функции Системы. Ситуации данного приоритета обычно имеют одну или несколько характеристик: | 1 линия  2 линия | Не более 12 часов | | • Повреждение данных; | | • Не доступны основные функции Системы; | | • Система зависает на неопределённое время, бесконечно занимая ресурсы и не давая ответа; | | • Система не отвечает после аварийной остановки и перезапуска | | Отсутствие иных путей решения Инцидента | | 2 | Средний | Присваивается Инцидентам с не критическими сбоями в работе потерей работоспособности Системы, следствием которых является некомфортное использование или необходимость применения альтернативных способов управления Системой | 1 линия  2 линия | Не более 48 часов | | 3 | Низкий | Сбои элементов системы, не оказывающих влияния на общую работоспособность и журналирование событий | 1 линия  2 линия | Не более 72 часов | | **Прием обращений и регистрация Инцидента с момента поступления на 1 линию поддержки в рабочее время** | | | | Не более 15 минут | | **Сервисное обслуживание** | | | | | | № | Серьезность /влияние на бизнес | Описание | Линия поддержки | Среднее время исполнения\* | | 1 | Средний | Запросы, в которых сообщается о доработке/изменении функций, параметров Системы или отдельного сервиса Заказчика. Предоставление дискового пространства, в случае отсутствия собственного пространства у Заказчика. Выработка соответствующих рекомендаций по устранению ошибок в Системе/Платформе, Сопровождение процедуры переноса данных | 1 линия  2 линия | Не более 24 часов | | 2 | Низкий | Консультация по работе Системы.  Вопросы по настройке системы  Предоставлению технической документации/инструкций | 1 линия 2 линия | Не более 72 часов | | **Прием обращений и регистрация запроса на проведение Сервисного обслуживания с момента поступления на 1 линию поддержки в рабочее время** | | | | Не более 30 минут | | **Плановые работы** | | | | | | № | Серьезность /влияние на бизнес | Описание | Линия поддержки | Среднее время исполнения\* | | 1 | Низкий | Комплекс работ по сокращению рисков возникновения аварийных ситуаций и принятия, превентивных мер.  Выполнение процедуры детальной проверки состояния системы (Health Check)  Информирование клиента о выходе новых версий для Системы. | 1 линия | Время и сроки проведения плановых работ согласовываются с Заказчиком | | **Прием обращений и регистрация запроса по проведению Плановых работ с момента поступления на 1 линию поддержки в рабочее время** | | | | Не более 60 минут | |
| **6** | **Требования к исполнителю** | Требования к Исполнителю:  - Исполнитель должен иметь в штате минимум одного технического специалиста, квалификация которого подтверждена копиями сертификатов по установке и аналитики от производителя решения;  - Иметь 2 аналогичных опыта поставки услуг;  - Иметь авторизационное письмо от Производителя IBM.  - итогом завершения услуг должен стать акт, с подробным отчетом об оказанных услугах; |
|  | **Объем выполняемых услуг** | Исполнитель оказывает услуги пользуясь своими материалами, оборудованием и программным обеспечением:  - предоставление консультативной и технической поддержки по телефону, по электронной почте, средствами удаленного подключения через сеть «Интернет» по выделенному VPN каналу по обращениям в рамках решения технических проблем в режиме 8x5xNBD;  - настройка/оптимизация работы программного обеспечения;  - обновление компонентов, оценка производительности, выработка рекомендаций по оптимизации инфраструктуры.  - доступ к базе знаний о информационной системе и документации, инструментам для отладки и конфигурирования (инструменты анализа отладочной информации, справочники, базы ошибок и пр.);  - Исполнитель предоставляет для Заказчика первую линию поддержки. При необходимости Исполнитель может эскалировать запрос Заказчика, и подключить к решению проблемы сервисный центр компании Производителя. После получения ответа от сервисного центра компании Производителя, данный ответ и соответствующие рекомендации будут предоставлены Заказчику;  - заявки и обращения Заказчика должны регистрироваться у Исполнителя в Service Desk. Исполнитель должен предоставить Заказчику доступ на просмотр зарегистрированных заявок через Web-интерфейс, для прозрачности хода исполнения заявок. |
| **7** | **Место оказания услуг** | г.Ташкент ул.Навои 18А, 100011 |
| **Требования к работам по модернизации IBM Security QRadar SIEM** | | |
| **1** | **Модернизация и установка дополнительных серверов** | Исполнитель осуществляет работы по модернизации и установке дополнительных серверов IBM Security QRadar SIEM, включая, но не ограничиваясь:   * разработкой оптимальной схемы модернизации системы управления инцидентами информационной безопасности IBM Security QRadar SIEM;   - проведением процедуры оценки состояния системы с предоставлением отчета;   * при необходимости переинсталляция основного сервера QRadar;   - инсталляцией узла приложений QRadar AppHost;  - подключением всех узлов QRadar SIEM к ЛВС Заказчика;  - подключением всех дополнительных узлов QRadar к основной консоли IBM QRadar SIEM;  - обновлением всех серверов системы до актуальной версии системы. |
| **2** | **Базовая настройка всех компонентов системы** | Исполнитель осуществляет работы по базовой настройке серверов системы IBM Security QRadar SIEM, включая, но не ограничиваясь:  - обновлением модуля обновлений Системы;  - настройкой получения Системой автоматических обновлений;  - настройкой получения системой автоматических обновлений системы;  - настройкой пользователей системы и интеграции с LDAP;  - настройкой сетевой иерархии системы;  - настройкой взаимодействия системы с почтовым сервером;  - настройкой соединения с репутационной базой X-Force;  - настройкой сроков хранения событий, потоков и нарушений системы;  - осуществление миграции встроенных приложений с основной консоли QRadar на сервер приложений AppHost. |
| **3** | **Подключение источников событий** | Исполнитель осуществляет работы по подключению источников событий к системе IBM Security QRadar SIEM, включая, но не ограничиваясь:  - подключением дополнительных поддерживаемых источников событий к основной консоли QRadar согласно согласованному списку подключаемых источников;  - подключением дополнительных неподдерживаемых источников событий к основной консоли QRadar согласно согласованному списку подключаемых источников;  - настройкой парсинга событий с неподдерживаемых источников событий;  - настройкой уровня критичности подключенных источников событий. |
| **4** | **Подключение источников сетевых потоков** | Исполнитель осуществляет работы по подключению источников сетевых потоков к системе IBM Security QRadar SIEM, включая, но не ограничиваясь:  - подключением SPAN/RSPAN или netflow с сетевых устройств;  - подключением сетевых устройств (коммутаторы, маршрутизаторы, межсетевые экраны). |
| **5** | **Настройка корреляционных правил** | Исполнитель осуществляет работы по настройке корреляционных правил системы IBM Security QRadar SIEM, включая, но не ограничиваясь:  - расширением стандартного набора правил с использованием пакетов экспертизы от Производителя;  - созданием пользовательских правил под нужды Заказчика;  - созданием пользовательских правил для мониторинга Даркнет трафика;  - созданием пользовательских правил для мониторинга коммуникаций с зловредными хостами с помощью репутационных баз;  - созданием кастомных свойств событий;  - индексирование свойств событий;  - тестированием правил на наличие фолз-позитив событий совместно с Заказчиком;  - корректировкой правил в случае необходимости. |
| **6** | **Установка и настройка дополнительных приложений** | Исполнитель осуществляет работы по установке и настройке приложений для системы IBM Security QRadar SIEM, включая, но не ограничиваясь:  - настройкой стандартного набора приложений (Log Source Management, Use Case Manager, QRadar Assistant, QRadar Pulse);  - обновлением стандартного набора приложений (Log Source Management, Use Case Manager, QRadar Assistant, QRadar Pulse) до актуальных версий;  - установкой дополнительных приложений расширяющие функционал Системы;  - настройкой дополнительных приложений расширяющие функционал Системы. |
| **7** | **Настройка панелей визуализации событий и отчетов в Системе** | Исполнитель осуществляет работы по настройке панелей визуализации (Dashboard) и отчетов (Reports) для системы IBM Security QRadar SIEM, включая, но не ограничиваясь:  - настройкой предустановленных панелей визуализации Системы;  - установкой дополнительных панелей визуализации из наборов расширений от Производителя;  - созданием пользовательских панелей визуализации под нужды Заказчика;  - установкой дополнительных отчетов из наборов расширений от Производителя;  - созданием пользовательских отчетов под нужды Заказчика. |
| **8** | **Итоговой тестирование IBM QRadar SIEM** | Исполнитель осуществляет работы по тестированию IBM Security QRadar SIEM, включая, но не ограничиваясь:  - проведением итоговой процедуры проверки системы IBM QRadar SIEM;  - проведением тестирования системы IBM QRadar SIEM совместно с Заказчиком;  - корректировкой работы системы IBM QRadar SIEM после тестирования в случае необходимости. |
| **9** | **Срок выполнения работ по модернизации** | 60 календарных дней со дня заключения договора. По факту выполнения модернизации стартует техническая поддержка системы сроком 12 месяцев. |