**УТВЕРЖДАЮ**

Государственный заказчик:

Руководитель Департамента информационных технологий

города Москвы

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**А.В.Ермолаев**

МП

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г.

**Обоснование**

**невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд**

В соответствии с частью 3 статьи 14 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и, руководствуясь порядком, утвержденным постановлением Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (далее – постановление Правительства Российской Федерации от 16.11.2015 № 1236), Департамент информационных технологий города Москвы (государственный заказчик) представляет обоснование невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств:

**Объект закупки (лот)**: поставка серверного и сетевого оборудования, оборудования систем хранения данных, прикладного программного обеспечения для обработки и хранения данных общегородских информационных систем «Единый реестр социальных льготников города Москвы» (АИС ЕРСЛ) и «Единое парковочное пространство города Москвы» ( АИС ЕПП).

**Обстоятельство, обусловливающее невозможность соблюдения запрета**: подпункт «а» пункта 2 Порядка подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд, утвержденного постановлением Правительства Российской Федерации от 16.11.2015 № 1236, а именно: *в едином реестре российских программ для электронных вычислительных машин и баз данных отсутствуют сведения о программном обеспечении, соответствующем тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке.*

**Класс (классы) программного обеспечения**: отсутствует, в связи с отсутствием на дату размещения извещения об осуществлении закупки приказа Министерства связи и массовых коммуникаций Российской Федерации об утверждении классификатора программ для электронных вычислительных машин и баз данных, необходимого к изданию в соответствии с подпунктом «а» пункта 7 постановления Правительства Российской Федерации от 16.11.2015 № 1236.

*Справочно: в соответствии с документом, размещенным на Официальном сайте оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» по адресу* [*https://reestr.minsvyaz.ru/upload/%D0%9A%D0%9B%D0%90%D0%A1%D0%A1%D0%98%D0%A4%D0%98%D0%9A%D0%90%D0%A2%D0%9E%D0%A0.pdf*](https://reestr.minsvyaz.ru/upload/%D0%9A%D0%9B%D0%90%D0%A1%D0%A1%D0%98%D0%A4%D0%98%D0%9A%D0%90%D0%A2%D0%9E%D0%A0.pdf)*, программное обеспечение, планируемое к закупке, относится к классу:*

*- 02.06 Системы мониторинга и управления*

**Требования к функциональным, техническим и эксплуатационным характеристикам программного обеспечения, являющегося объектом закупки**: *приведены в приложении к настоящему обоснованию*.

**Функциональные, технические и (или) эксплуатационные характеристики, по которым программное обеспечение, сведения о котором включены в реестр, не соответствует установленным государственным заказчиком требованиям к программному обеспечению, являющемуся объектом закупки**: *указание не требуется в связи с применением подпункта «а» пункта 2 Порядка подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд, утвержденного постановлением Правительства Российской Федерации от 16.11.2015 № 1236.*

ИСПОЛНИТЕЛЬ:

Начальник Управления закупок Д.В.Бондал

Приложение

к Обоснованию невозможности соблюдения запрета

на допуск программного обеспечения, происходящего из иностранных государств

**Требования**

**к функциональным, техническим и эксплуатационным характеристикам программного обеспечения,**

**являющегося объектом закупки**

| **№ п/п** | **Наименование товара** | **Ед. изм.** | **Кол-во** | **Функциональные, технические и эксплуатационные характеристики программного обеспечения, происходящего из иностранных государств.** |
| --- | --- | --- | --- | --- |
| 1 | D0WSCLL, IBM Security QRadar SIEM All-in-One Virtual 3190 Install License + SW Subscription & Support 12 Months svp\_e | шт. | 1 | **Система управления событиями безопасности (СУСБ), отвечающая следующим функциональным характеристикам:**   * сбор событий из журналов источников событий с сохранением результата обработки в централизованной базе данных; * интеграция с различными типами источников событий безопасности; * наличие функционал агрегации, нормализации и корреляции событий от источников. Параметры агрегации, нормализации и корреляции являются настраиваемыми; * возможность сбора событий с источников, неподдерживаемых штатно; * функционал формирования отчетов по событиям, сохраненным в централизованной базе данных. Функционал формирования отчетов является настраиваемым; * выполнение всех возложенных функций по получению, нормализации и корреляции при сборе событий; * доступность информации в течение двух месяцев в прямом доступе и в течение 12 месяцев в архиве (с возможностью восстановления); * поддержка протоколов syslog, rpc, http/https, snmp, ftp/sftp при взаимодействии с источниками событий; * централизованное управление всеми компонентами СУСБ и функционалом через Веб-интерфейс; * ролевая модель доступа пользователей к консоли управления без ограничения их количества; * функционал определения всех активов сети; * функционал автоматической классификации определенных активов в сети; * возможность разделения визуализаций через пользовательский интерфейс для использования во внедрениях SOC (Security Operations Center) и NOC (Network Operations Center); * наличие открытого API для доступа к информации, находящейся в базе данных системы; * возможность шифровать коммуникации между компонентами; * возможность интегрироваться с системами сторонних производителей (LDAP, AD) для обеспечения аутентификации; * автоматическое обновление конфигураций без дополнительных временных затрат со стороны пользователя системы. Например, обновление правил по отдельным системам и устройствам сторонних производителей; * возможность управления системой, создания аналитических отчетов и правил через веб-интерфейс пользователя; * возможность реализации отказоустойчивого внедрения без привлечения решений сторонних производителей, как на уровне сбора, так и на уровне корреляции событий; * гарантированная работа отдельных компонентов системы, при выходе из строя любой части системы; * наличие автоматического процесса резервного копирования конфигурации (Backup) и возможность восстановления (Recovery) конфигурации из графического интерфейса пользователя; * встроенный процесс анализа своего состояния и возможность оповещения пользователя при возникновении проблем; * возможность реализации в виде ПАК (программно-аппаратный комплект, Appliance), так и как ПО на серверах заказчика; * возможность интеграции с другими системами обеспечения безопасности и расследования инцидентов; * поддержка разнесенных баз данных для хранения информации о событиях; * хранение информации о событиях в проприетарной базе данных; * возможность доступа к информации о событиях через единый интерфейс пользователя; * обеспечение целостности собранной информации; * поддержка разнесенной модели для корреляции со всех коллекторов; * поддержка расширенной таксономии пользователей для событий и полей. Пользователь имеет возможность присваивать событиям любые имена; * возможность изменения поведения автоматического тегирования событий по важности согласно пожеланиям пользователя; * прозрачное получение, агрегирование, сортирование, фильтрация и аналитика данных по всем разнесенным компонентам системы; * наличие системы сбора журналов событий и их архивации, которая поддерживает как кратковременное хранение (online), так и долгосрочное (offline) хранение журналов событий; * возможность хранение журналов событий на внешних хранилищах; * функционал рационального использования хранилищ данных, а также архивации данных в архиве; * безагентный сбор журналов событий везде, где это возможно; * возможность распределять хранение журналов событий и их обработку по всей архитектуре системы; * предоставление доступ ко всей информации о событиях на протяжении длительного периода времени (12 месяцев) для дальнейших расследований; * возможность нормализовать стандартные поля событий (имена пользователей, IP адреса, имена хостов, устройства-источники событий) с различных устройств мультивендорной сети; * возможность стандартной категоризации событий без предварительной дополнительной настройки; * возможность хранения информации о событиях, как в исходном виде, так и в нормализованном виде для использования в дальнейших расследованиях; * возможность обрабатывать и нормализировать данные из полей, которые не поддерживаются изначально и не предоставляются с настройками out of the box; * анализ событий в режиме реального времени; * анализ событий на протяжении определенного периода времени; * возможность сбора и анализа событий по предустановленным пользователем фильтрам; * возможность получения дополнительной информации о событиях при необходимости (drill down); * возможность фильтрации событий; * отчетность по всем событиям, доступная через веб-интерфейс для пользователей; * возможность самостоятельной настройки отчетности и создания собственных отчетов пользователем; * возможность планирования генерации отчетов в определенный период времени; * предоставление примеров сгенерированных отчетов для более простого использования и генерации новых отчетов пользователем, а также наличие мастера создания отчетов; * наличие встроенных отчетов для типичных бизнес-требований заказчиков; * наличие встроенных отчетов по определенным требованиям стандартов (PCI, SOX, FISMA) а также лучших практик (NIST, ISO) без необходимости приобретения дополнительных лицензий; * удобный интерфейс для быстрой визуализации всей информации о сети и безопасности; * предоставление отчетов за определенный период времени по различным сегментам и системам в сети; * возможность автоматического распределения отчетов; * возможность оповещения по всем угрозам в сети на любых устройствах; * возможность корреляции информации с различных источников, которые никак не взаимодействую между собой; * возможность оповещения на основе обнаруженных аномалий и поведенческого анализа и изменений; * приоритезация оповещений в зависимости от требований пользователя, а также критичности активов; * возможность создания собственных настраиваемых оповещений; * мастер настройки оповещений для упрощения процесса их создания, а также улучшения точности результатов и уменьшения количества ложных срабатываний; * возможность создания оповещений при превышении/нарушении норм работы систем и их использования; * возможность ограничивать число одинаковых оповещений на единицу времени; * возможность использования графического интерфейса пользователя для настройки и демонстрации оповещений; * возможность применять активное воздействие и реакцию на оповещения. Например, запускать скрипт, или отправлять письмо по почте; * поддержка интеграции на уровне оповещений с другими системами безопасности и оповещения, которые функционируют в сети; * оповещение администратора при отсутствии логов в течении 120 минут с наблюдаемого устройства; * наличие встроенного функционала автоматического определения всех устройств и их инвентаризации по классам систем (например, почтовые сервера, сервера баз данных и пр.) для минимизации количества ложных срабатываний из-за недостатка информации о системах; * возможность корреляции по определенным последовательностям событий; * поддержка корреляции на основе дополнительных данных; * система должны поддерживать обработку поступающих событий со скоростью не менее 100 событий в секунду, с возможностью расширения производительности системы до 5000 событий в секунду без изменения существующей инсталляции. * возможность обеспечения следующего функционала при покупке дополнительных лицензий:   + масштабирование СУСБ на всю информационную систему Заказчика путем подключения источников событий информационной системы к СУСБ;   + сканирования уязвимостей, а также корреляция информации с систем сканирования уязвимостей сторонних производителей;   + управление рисками, включая:     - сбор и нормализация конфигураций коммутаторов, маршрутизаторов, брандмауэров, и других сетевых устройств Заказчика;     - сравнение конфигураций устройств и выявление их изменения;     - выявление и оповещение об изменениях конфигурации, если эти изменения выходят за рамки разрешенных пределов и политик;     - приоритезация уязвимости на базе конфигурации;     - запуск сценария атаки «что если» против конфигурации сети.   + контроль активности сети до уровня анализа работы приложений с целью выявления аномального сетевого траффика, включая:     - визуальное отображение профиля трафика в байтах, скорости передачи пакетов и количества коммуницирующих между собой хостов;     - определение приложений вне зависимости от TCP-порта. Поддержка идентификации приложений не только по общеизвестным портам, но и в других случаях, а также определение туннелированных приложения;     - определение “zero-day” событий;     - проведение поведенческого анализа трафика и уведомление об изменениях согласно заданных порогов изменения;     - обнаружение команд управления botnet-сетями;     - выявление потенциально опасных приложений в сетевом трафике (file sharing, peer-to-peer и т.д.);     - предоставление информации в нескольких интервалах времени (за неделю, день и час);     - представление трафика на основе IP адреса, группы IP адресов, источник/место назначения IP пар и т.д.;     - возможность контекстно связывать в реальном времени выявленные события безопасности со знаниями об активах в сети;     - возможность автоматически определять приоритет выявленных событий безопасности согласно относительной важности актива;     - возможность кастомизировать любые аналитические данные, установленные по умолчанию;     - возможность обеспечивать представление информации событий в реальном времени (как в оригинальном/сыром виде, так и в обработанном формате);     - возможность отсылать уведомление о тревогах определенными методами (т.е., SNMP trap, e-mail, и т.д.). * взаимодействие между компонентами СУСБ по защищенным протоколам сетевого взаимодействия в случае реализации распределенной архитектуры; * возможность индивидуальной аутентификации пользователей; * обеспечение разграничения прав доступа пользователей; * наличие механизма администрирования, предназначенного для выполнения функций по управлению системой; * возможность запуска ПО внутри виртуальной машины VMware. |
| 2 | D0WUKLL, IBM Security QRadar Virtual SIEM Event Capacity Increase of 100 EPS Install License + SW Subscription & Support 12 Months svp\_e | шт. | 1 | **Лицензия на увеличение производительности Системы управления событиями безопасности (СУСБ) на 100 событий в секунду** |