

**Приложение 3**

**О порядке проведения закупок товаров, работ и услуг в ОАО «Керемет Банк»**

**Приглашение на участие в закупке**

Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Уважаемый Участник,

1. ОАО «Керемет Банк» приглашает Вас представить заявку на участие в тендере на закупку товара (работ, услуг).

Лот №1 Закуп SIEM системы

2. Условия поставки

|  |  |  |
| --- | --- | --- |
| № | Наименование  | Система SIEM  |
| 1 | Место поставки  | г.Бишкек ул.Тоголок Молдо 40/4 |
| 2 | Срок поставки | До 1 месяца |
| 3 | Условия оплаты | 50/50 |
| 4 | Цена с учетом налогов предусмотренных законодательством КР Валюта Сом |  |
| 5. | Наличие гарантии | не менее 1 года. |
| 6. | скидка | приветствуется |

3. Ваша заявка должна быть направлена не позднее «11» июля 2025 г. 11:00 местного времени, в запечатанном конверте, адресована, и доставлена по следующему адресу: г. Бишкек. ул. Тоголок Молдо 40/4 электронно по почте: tender@keremetbank.kg

6. Квалификационные данные

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование | Требования ОАО Керемет Банка | Поставщик |
| 1 | наличие опыта поставки (работы, выполнения) не менее \_\_\_\_\_\_ аналогичных по характеру и степени сложности договоров (минимальная стоимость договора составляет\_\_\_\_\_\_\_\_\_\_тыс.сом), договора по которым указывается опыт должны быть завершены не менее чем на 70 процентов на дату подачи Тендерной заявки | наличие опыта поставки работы, выполнения не менее 1 года на аналогичных по характеру и степени сложности договоров, договора по которым указывается опыт должны быть завершены не менее чем на 70 процентов на дату подачи Тендерной заявки |  |
| 2 | копии отчетов о финансовой деятельности Участника конкурса (балансы, отчеты о результатах хозяйственной деятельности, отчеты о движении денежных средств, отчеты о прибылях и убытках, аудиторские заключения) за указанный \_\_\_\_\_\_\_\_\_период времени. | За последний год. |  |
| 3 | справки о задолженности по уплате налогов и обязательных выплат в Социальный фонд Кыргызской Республики, и должны быть действительные на момент проведения Тендера | Обязательно актуальный за последний месяц. |  |
| 4 | наличие реквизитов для оплаты товаров/услуг по договору не санкционных банках. | Обязательно  |  |
| 5\* | документы, подтверждающие наличие финансовых ресурсов для выполнения Договора (собственные оборотные средства, доступ к кредитной линии (линиям), наличие других финансовых ресурсов); | Не требуется |  |
| 6\* | Наличие лицензии на проведение данного вида услуг (если требуется) | Требуются подтверждающие документы. |  |
| 7\* | Иные требования | Наличие гарантии не менее 1 года. |  |
| 8\* | Требованию к вендору | Вендор не должен быть в санкционном списке |  |

Пакет документов, направляемый в ОАО «Керемет Банк» должен содержать:

Устав (патент, свидетельство ИП)

Свидетельство о регистрации

Приказ о назначении руководителя

Копия паспорта руководителя

Ваша заявка должна быть действительна в течение \_\_\_\_\_\_\_\_\_\_ но не менее 30 рабочих дней, с даты принятия (вскрытия) котировок цен.

Техническое задание на закупку SIEM системы

г. Бишкек 03.07.2025 г.

**Описание**

Предмет закупки: первоначальное внедрение и техническая поддержка SIEM системы.

**Требования к поставщику**

 Исполнитель если не является производителем, то должен иметь партнерские отношения с производителем SIEM системы для оказания технической поддержки, подтвержденные авторизационным письмом от производителя SIEM системы с указанием партнерского статуса участника и необходимые для исполнения договора кадровые ресурсы.

### **Требования к оборудованию**

* Компоненты системы должны поддерживать установку как на физических, так и на виртуальных машинах.
* Основные компоненты (модули, отвечающие за сбор событий, корреляцию, хранение событий) должны поддерживать установку на операционной системе семейства Linux.
* Для хранения событий должна использоваться колоночная база данных для обеспечения высокой скорости поиска.

**Технические требования**

 - Компоненты системы должны поддерживать установку как на физических, так и на виртуальных машинах.

 - Система должна позволять развёртывание основных компонентов компонентов как на один физический или виртуальный сервер, так и на отдельные серверы для распределения вычислительной нагрузки.

 - Система должна поддерживать развёртывание нескольких агентов/коллекторов сбора событий, для сокращения нагрузки на один агент/коллектор или сбора событий в закрытых сегментах.

 - Система должна поддерживать масштабирование ключевых ее компонентов: коллектора, коррелятора и хранилища событий без необходимости приобретения дополнительных лицензий на ПО.

 - Система должна обеспечивать централизованное управление посредством веб-консоли без установки дополнительного ПО на АРМ администратора.

 - Система должна обеспечивать возможность централизованного обновления конфигурации или перезапуска компонентов, в том числе форсированного.

 - Система должна поддерживать автоматические обновления правил нормализации и правил корреляции, выпускаемых производителем. Система должна поддерживать обновление в том числе без прямого доступа к интернету.

 - Система должна обеспечивать как активный, так и пассивный сбор событий с источников данных:

 - пассивный (без подключения к источнику) сбор событий с использованием протоколов syslog, SNMP (Trap), Cisco NetFlow, sFlow

 - активный (с подключением и выполнением команд и запросов к источнику) сбор событий с использованием поддерживаемых протоколов и механизмов: DCE/RPC (WMI), CIFS/SMB (RPC), SSH, DCOM (RPC), Telnet, OPSEC LEA, ODBC API, VMware API

 - Система должна осуществлять сбор логов из различных программных и аппаратных источников.

 - Система должна поддерживать безагентский метод сбора и получения событий с источников (бе необходимости устанавливать агент на сам источник)

 - Система должна иметь централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

 - Система должна обеспечить возможность написания правил нормализации из веб-интерфейса системы для разбора событий, в том числе посредством регулярных выражений и возможностью проверки синтаксиса их написания на примере исходного события.

 - Система без дополнительных настроек разбора (нормализации) должна поддерживать получение событий в формате Syslog.

 - Система должна поддерживать возможность последовательного иерархического разбора (нормализации) событий.

 - Задачи по сканированию, поиску новых хостов и прочие сопряженные с риском задачи должны запускаться как по расписанию, так и с указанием запрещенного времени запуска.

 - Система должна обеспечивать возможность мониторинга поступления событий от источников с отслеживанием количества событий в указанный промежуток времени и автоматическим оповещением на электронную почту в случае отклонения от заданных параметров мониторинга для каждого из источников в частности;

 - Данные, предаваемые компонентами на пользовательский интерфейс, должны быть защищены при помощи HTTPS с использованием SSL сертификата.

 - Система должна обеспечивать возможность поиска по базе событий на основе произвольного поиска по базе событий с помощью конструктора запросов;

 - Система должна автоматически приоритизировать выявленные угрозы ИБ как с учётом уровня критичности правила корреляции, так и с учетом критичности и количества затронутых информационных активов.

 - Система должна иметь возможность интеграции со следующими системами:

 - LDAP-серверами на базе Microsoft Active Directory — для интеграции с внешними системами аутентификации и бесшовного соотнесения ролей пользователей Системы с ролями Microsoft Active Directory в рамках обеспечения единого входа в Систему (SSO);

 - системами электронной почты — для отправки сообщений электронной почты;

 - системами разрешения доменных имен — для сбора сведений об узлах, зарегистрированных в Cистеме;

 - системой точного времени Заказчика — для обеспечения единых меток даты/времени.

 - Система должна поддерживать вызов функций автоматизированного реагирования в результате срабатывания правил корреляции.

 - Система должна предоставлять инструменты визуализации (дашборды) и отчётности.

 - Система должна поставляться с предустановленным набором графических панелей (дашбордов) и отчётов.

 - Система должна поддерживать возможность создания пользовательских шаблонов и правил уведомлений о событиях и инцидентах.

 - Система должна поддерживать возможность создания пользовательских дашбордов и шаблонов отчетов.

 - Должна быть возможность взаимодействия с системой через REST API, а также открытая документация по REST API

 - Система должна поддерживать русский язык и английский язык (интерфейс, документация)

 - Система должна обеспечивать высокую производительность и поддерживать прием и обработку потока в размере не менее 1500 событий в секунду (EPS) и обеспечивать мониторинг событий для 500 активов.

**Требования к эксплуатационной документации**

 Эксплуатационная документация Системы должна включать Руководство пользователя (администратора) на русском языке.

 Документация, поставляемая в комплекте с Системой, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства.

**Требования к технической поддержке**

 Техническая поддержка программного обеспечения должна соответствовать следующим требованиям:

* предоставляться на русском языке сертифицированными специалистами производителя;
* web-сайт производителя должен быть на русском языке, иметь пополняемую базу знаний;
* предоставлять возможность использования персональной учетной записи пользователя для создания, обновления и мониторинга инцидентов;
* предоставлять техническую поддержку и консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта;
* регулярно информировать о промежуточных результатах и ходе решения запросов;
* предоставлять возможность предъявления претензий и жалоб на качество обслуживания на уровень руководителя технический поддержки регионального офиса или менеджера по работе с корпоративными клиентами;

**Требования к первоначальной установке и настройке системы**

 В обязательном порядке Поставщиком SIEM системы производится первоначальное развертывание системы, в том числе установка и настройка необходимого программного обеспечения. Также без дополнительной оплаты производится подключение и нормализация событий всех необходимых источников Банка (АБС, Active Directory, Корпоративная почта, корпоративный антивирус, терминальные сервера, сетевые оборудования, интернет банкинг, 1С предприятие, Linux сервера и т.д.).

 Предложение должно включать в себя организацию обучения работе с системой не менее двух сотрудников Заказчика за счёт Поставщика.

# Требования к срокам реагирования

Техническое консультирование по вопросам эксплуатации продукта и приём запросов на устранение негативных последствий инцидентов должно обеспечиваться посредством:

* Предоставления доступа Пользователю к Интернет-Порталу технической поддержки с возможностью размещения запросов в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни);
* Приёма запросов по электронной почте в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни) в случае невозможности создания запроса через Интернет- Портал;

Время реакции должно обеспечиваться согласно уровню критичности:

|  |  |
| --- | --- |
| Уровень критичности | Время реакции не более: |
| Уровень критичности 1 | Критический | 2 рабочих часа |
| Уровень критичности 2 | Высокий | 6 рабочих часа |
| Уровень критичности 3 | Средний | 8 рабочих часов |
| Уровень критичности 4 | Низкий | 10 рабочих часов  |

Уровни критичности инцидентов, относящихся к продукту

Уровень критичности 1 (критический) означает критическую проблему с Продуктом, влияющую на непрерывность бизнеса Пользователя посредством прерывания работоспособности Продукта или операционных систем Пользователя, или вызывающую потерю данных, установку стандартных настроек Пользователя в небезопасный режим или возникновение других проблем с безопасностью, при этом обходное решение отсутствует.

Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 1, включает в себя следующие инциденты:

* вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес- процессы.

Уровень критичности 2 (высокий) означает проблему высокого уровня критичности, вызывающую воздействие на функциональность Продукта, но не вызывающую повреждение/ потерю данных или прерывание работоспособности программного обеспечения. Уровень критичности 1 рассматривается, как Уровень критичности 2, когда известно обходное решение.

Перечень инцидентов, связанных с Продуктом и соответствующих Уровню критичности 2, включает в себя следующие инциденты:

* продукт полностью выведен из строя, но непрерывность основных бизнес процессов не нарушается.

Уровень критичности 3 (средний) означает некритичную проблему или запрос на обслуживание, не затрагивающие функциональность Продукта.

Перечень инцидентов, соответствующих Уровню критичности 3, включает в себя следующие инциденты:

* продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение Заказчика не выведено из строя в результате работы Продукта.

Уровень критичности 4 (низкий) означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности.