**ПРИГЛАШЕНИЕ № 248**

**к участию в конкурсе с неограниченным участием**

 «17» ноября 2023 г.

**ЗАО «Альфа телеком»** (далее - Компания) приглашает правомочных поставщиков представить свои конкурсные заявки на закупку **Программного обеспечения оперативного мониторинга состояния информационной безопасности (SIEM) (далее приглашение):**

Описание предмета закупки, характер, перечень, количество, место и сроки работ, требования, предъявляемые к поставщикам и иные требования установлены **в Требованиях к закупке (приложение 1 к Приглашению**).

1. Для участия в конкурсе необходимо:

|  |  |  |
| --- | --- | --- |
| **Подать конкурсную заявку в электронном виде согласно Требованиям к закупке (приложение 1) с установлением пароля доступа** | **По эл. адресу: tender@megacom.kg** | **Дата окончания приема конкурсных заявок:****27.11.2023г. 09:59 часов (GMT+6)** |
| **Направить пароль для доступа к конкурсной заявке** | **По электронному адресу: tender@megacom.kg** | **Дата окончания приема паролей к конкурсным заявкам:****27.11.2023г. с 10:00 до 11:59 часов (GMT+6)** |
| **Вскрытие конкурсных заявок состоится:** | **по адресу: г. Бишкек, ул. Суюмбаева, 123;** | ***ДАТА и Время вскрытия конкурсных заявок*:27.11.2023г. в 12:00** |

***! Вложенный файл (конкурсная заявка) не должен превышать 10мб, в случае превышение рекомендуется разделить и отправить несколькими сообщениями (письмами).***

***- Заявки, направленные с использованием облачных файлообменников не принимаются и не рассматриваются.***

1. При наличии вопросов по настоящему Приглашению поставщик может обратиться в Компанию по электронному адресу: **tender@megacom.kg** за получением разъяснений, но не позднее 3 рабочих дней до истечения окончательного срока представления конкурсных заявок. Разъяснения направляются обратившемуся поставщику по электронной почте, с которой был получен запрос, не позднее трех календарных дней с момента получения запроса.
2. При необходимости, Компания вправе внести изменения в настоящее Приглашение путем издания дополнений в любое время до истечения окончательного срока представления конкурсных заявок, но в любом случае не позднее 3 (трех) рабочих дней.
3. Компания может перенести окончательную дату подачи конкурсных заявок на более поздний срок, если вносятся поправки в настоящее Приглашение, о чем Компания информирует путем размещения соответствующей информации на официальном сайте Компании и информационном ресурсе, где было размещено объявление о проведении настоящего конкурса.
4. **Порядок подачи конкурсной заявки.** Поставщику, желающему участвовать в конкурсе необходимо согласно Требованиям к закупке (приложение 1 к Приглашению) заполнить конкурсную заявку (приложение 2 к Приглашению), приложить требуемые копии документов, установить к ним пароль доступа и отправить в электронном виде на электронную почту, указанную в п. 1 Приглашения, не позднее установленного срока. При этом, Поставщик обязуется сообщить/направить Компании пароль доступа не позднее установленного срока и вышеуказанным способом.

 Каждый участник конкурса может подать только одну конкурсную заявку.

1. Компания может установить фиксированную сумму гарантийного обеспечения конкурсной заявки (далее – ГОКЗ). Срок действия ГОКЗ должен совпадать со сроком действия конкурсной заявки. Данное требование устанавливается при необходимости.

ГОКЗ вносится в размере и форме, предусмотренных в конкурсной документации.

ГОКЗ возвращается не позднее трех рабочих дней в случаях:

1) истечения срока действия конкурсной заявки, указанного в конкурсной документации;

2) заключения договора и предоставления ГОИД, если предоставление такого гарантийного обеспечения предусмотрено в конкурсной документации;

3) отзыва конкурсной заявки до истечения окончательного срока представления конкурсных заявок;

4) прекращения процедур закупок без заключения договора.

5. Гарантийное обеспечение конкурсной заявки закупающей организацией удерживается в случаях:

1) отказа подписать договор на условиях, предусмотренных в конкурсной заявке победителя, за исключением случаев, если такой отказ связан с введением режима чрезвычайной ситуации или чрезвычайного положения, при условии опубликования объявления о закупке до введения таких режимов;

2) отказа предоставить гарантийное обеспечение исполнения договора;

3) отзыва конкурсной заявки после ее вскрытия и до истечения срока ее действия;

4) изменения условий конкурсной заявки после вскрытия конвертов с конкурсными заявками.

1. **Конкурсные заявки, поданные поставщиками позднее указанного срока и/или заявки, к которым не сообщен пароль до установленного срока, не принимаются и не рассматриваются.**

**Подавая свою конкурсную заявку, поставщик тем самым выражает свое согласие на все условия, указанные в проекте (-ах) договора (-ов) (Приложение 3 к Приглашению).**

**Не допускается внесение изменений в конкурсные заявки после истечения срока их подачи.**

1. Поставщик, подавший конкурсную заявку, может присутствовать на вскрытии конкурсных заявок. На вскрытии конкурсных заявок оглашается цена конкурсной заявки, а также список документов, приложенных к конкурсной заявке, и вносится в протокол вскрытия.
2. Во время оценки конкурсных заявок Компания вправе обратиться к поставщику за разъяснениями по поводу его конкурсной заявки. Запрос о разъяснениях и ответ на него должны подаваться в письменном виде по электронной почте.
3. Оценка конкурсных заявок осуществляется в соответствии с процедурами и критериями, предусмотренными в Требованиях к закупке (приложение 1 к Приглашению). Компания вправе запросить у поставщика исправление арифметических ошибок, допущенных в конкурсной заявке.

В случае если по итогам проведенной оценки поставщиками предоставлены конкурсные заявки с одинаковыми ценами и условиями, отвечающие требованиям конкурсной документации, то Компания направляет поставщикам, представившим одинаковые цены запрос по электронной почте о возможности снижения цены (предоставления скидки), выигравшей конкурсной заявкой считается заявка поставщика, предоставившего наименьшую цену (наибольшую скидку). В случае если после снижения цены (предоставления скидки) поставщики представили одинаковые предложения (цена, скидка), то победитель определяется посредством случайной выборки.

1. Компания отклоняет конкурсную заявку в случаях, если:

- участник, представивший конкурсную заявку, не соответствует квалификационным требованиям, установленным в Требованиях к закупке (приложение 1 к Приглашению);

- конкурсная заявка по существу не отвечает требованиям, установленным в Требованиях к закупке (приложение 1 к Приглашению);

- технические параметры, предложенные в конкурсной заявке, не соответствуют технической спецификации, установленной в Требованиях к закупке (приложение 1 к Приглашению);

- поставщик представил более одной конкурсной заявки;

- поставщик не предоставил гарантийное обеспечение конкурсной заявки;

- цена конкурсной заявки превышает планируемую сумму закупки;

- в случае отсутствия либо превышения цены в позиции, конкурсная заявка по данному Лоту будет признана не полной и в дальнейшем подлежит отклонению

- в случае выявления конфликта интересов согласно п. 6.5 Правил организации и осуществления закупок в ЗАО «Альфа Телеком».

1. Конкурс признается Компанией несостоявшимся в случаях, когда были отклонены все предложения поставщиков, не поступило ни одного предложения или минимальная цена по конкурсу превышает планируемую сумму закупки.
2. Компания может отменить конкурс в любое время до заключения договора, если отпала необходимость в дальнейшем приобретении предмета закупки.
3. Компания в течение двух рабочих дней с момента подведения итогов по конкурсу направляет поставщикам по электронной почте уведомления: победителю о том, что его заявка признана победившей, остальным участникам, что их заявки не признаны победившими.
4. Поставщик, определенный победителем конкурса, должен подтвердить уведомление о признании его победителем в течение трех рабочих дней путем направления ответного письма по электронной почте.
5. В случае нарушения победителем сроков: подтверждения заключения договора, подписания договора/возврата экземпляра договора Компании или внесения гарантийного обеспечения исполнения договора, Компания вправе заключить договор с поставщиком вторым в рейтинге.
6. Поставщик, участвующий в конкурсе, имеет право подать жалобу Компании относительно требований конкурсной документации не позднее двух рабочих дней до даты окончательного срока подачи конкурсных заявок или проведенной оценки по конкурсу не позднее двух рабочих дней после подведения итогов по конкурсу. Жалоба поставщика рассматривается Компанией в срок до 3-х рабочих дней. В случае несогласия поставщика с решением Компании по жалобе, поставщик вправе обратиться в судебные органы.

 Приложение:

1. Требования к закупке;
2. Форма конкурсной заявки;
3. Форма соответствия;
4. Проект Договора

**Руководитель отдела по закупкам Таалайбек кызы Айнура**

 *Исп.: Н. Шаршенов,*

 *тел:0312 905 244*

**Приложение 1 к Приглашению**

**Требования к закупке**

|  |
| --- |
| **1.Общие требования** |
| 1.1 | Язык конкурсной заявки  | Русский **(в случае если документ будет составлен на** иностранном языке, необходимо предоставить дополнительно перевод на русском языке) |
| 1.2 | Условия, место и срок поставки  | Электронным способом на эл. почту **не позднее десяти рабочих дней с даты заключения Договора**: InfSecurity@megacom.kg направляется уведомление о предоставлении права пользования программным обеспечением, лицензиями и технической поддержкой |
| 1.3 |  Срок предоставления услуг | С даты подписания Акта приема-передачи выполненных услуг, бессрочная лицензия |
| 1.4 | Условия оплаты и срок выплаты | 100% от цены договора выплачиваются в течение 10 банковских дней со дня получения электронной счета-фактуры, выставленного на основании и датой подписания сторонами Акта, подтверждающего право пользования программным обеспечением и лицензиями. **Оплата осуществляется:** * Поставщику-нерезиденту: Доллар США или другая иностранная валюта.
* Поставщику-резиденту в сомах КР

Оплата осуществляется путем перечисления денежных средств на расчетный счет Поставщика.\*При оплате нерезидентам КР за Лицензии на ТП/услуги при отсутствии межгосударственных соглашений об избежание двойного налогообложения будет удержан налог на доход иностранной организации по ставке 10%. |
| 1.5 | Цена конкурсной заявки | *В цену, указанную участниками конкурса, должны быть включены все налоги, сборы и другие платежи, взимаемые в соответствии с законодательством Кыргызской Республики, а также накладные расходы* |
| 1.6 | Валюта конкурсной заявки  | **Для резидентов КР:** Сом КР\* (\*Примечание: Если резидентом КР будет подана конкурсная заявка в другой валюте, то договор будет заключен в национальной валюте по курсу Национального банка КР на день вскрытия).**Для нерезидентов КР:** Доллар США или другая иностранная валюта.\*Оценка будет производиться в национальной валюте - сом по курсу Национального банка КР на день вскрытия конкурсных заявок. |
| 1.7 | **Для Юридических лиц**, копии документов, определяющих организационно-правовую форму юридического лица, место регистрации и основной вид деятельности: * Свидетельство о гос. регистрации/перерегистрации,
* Устав
* Приказа/решение/протокол об избрании/назначении исполнительного органа юр.лица (1-го лица)

**Для индивидуальных предпринимателей**: Свидетельство о регистрации в качестве индивидуального предпринимателя или действующий патент (при этом вид деятельности должен совпадать с предметом закупки и охватывать минимум период до полной поставки товара и передачи по акту) | Приложить копии(в случае если, данные документы составлены на иностранном языке, необходимо предоставить дополнительно перевод на русском языке). |
| 1.8 | Доверенность на лицо, подписавшее конкурсную заявку и представляющее интересы участника в торгах (если она подписывается не исполнительным органом – руководителем компании) | Приложить скан копию доверенности. |
| 1.9 | Авторский надзор, Технический надзор, или контроль за ходом выполнения работ/услуг, поставки товаров | После получения сообщения по эл. почте представителю ЗАО «Альфа Телеком» опредоставленииправа пользования программным обеспечением, лицензиями и технической поддержкой, Заказчик осуществляет проверку полученных прав на соответствие Спецификации на интернет-портале производителя ПО в течение 10 календарных дней. При соответствии прав пользования Спецификации,Заказчик подписывает Акт приема-передачи в течение пяти рабочих дней |
| 1.10 | Срок действия конкурсной заявки, в календарных днях | 60 (шестьдесят) календарных дней с даты вскрытия конкурсных заявок |
| 1.12 | Размер и форма гарантийного обеспечения исполнения договора (ГОИД) | Поставщик, которому будет присуждено право заключения договора, по итогам конкурса должен внести гарантийное обеспечение исполнения договора (ГОИД), в виде денежных средств, в размере: **2,5** **%** от общей суммы Договора путем перечисления денежных средств на банковский счет Компании в течение 5 банковских дней с даты заключения Договора. Гарантийное обеспечение исполнения договора или его остаток  после удержания начисленных неустоек и/или сохранения части ГОИД на период технической поддержки возвращается Исполнителю не позднее десяти рабочих дней с даты  подписания Акта приема передачи  оказанных услуг.*Порядок возврата ГОИД определяется в договоре.*  |
| 1.13 | Критерии оценки  | 1. \* Победившей может быть признана Конкурсная заявка, отвечающая по существу требованиям **конкурсной документации, квалификационным требованиям, техническим параметрам и имеющая наименьшую оцененную стоимость\*.**

\* при определении оцененной стоимости, от общей стоимости конкурсной заявки вычитается НДС (-12%), если участник-резидент КР является плательщиком НДС, соответственно, оценка заявок будет проводиться без учета НДС-12%. |
| **1.14** | **Другие необходимые документы, которые участники конкурса должны заполнить и предоставить** | **Заполнить: 1. Таблицу соответствия техническим требованиям (Приложение 2.1 к Приглашению);****2.Форму конкурсной заявки (Приложение № 2 к Приглашению)** |
| 1.15 | Условия договора | См. проект Договора (Приложение № 3) |
| **1.16** | **Выделяемая сумма** | **18 768 000 сом** |
| **2. Квалификационные требования** |
| 2.1 | Опыт аналогичных по характеру и степени сложности предоставлении услуг, в денежном выражении | Наличие опыта по характеру аналогичных поставок (услуг) за последние 2 года в сумме не менее 9 млн. (девять миллиона) сом или эквивалент в другой иностранной валюте. Подтвердить информацию о выполненных поставках (опыте) необходимо актами приема-передачи или счетами-фактурами. |
| 2.2 |  Авторизация:  | Приложить действующие авторизационное письмо от Правообладателя/Производителя ПО, действующее на территории КР со сроком авторизации не менее чем срок предоставления услуг.В случае, если предоставляется авторизационное письмо, выданное не Правообладателем/Производителем ПО, а их дистрибьютором, в целях установления его полномочий необходимо также предоставить авторизационное письмо, выданное данному дистрибьютору Правообладателем/Производителем ПО. |
| 2.3 | Наличие специализированных сотрудников | Не менее 2-х сотрудников с подтверждающими документами (сертификаты, подтверждение знаний от производителя и т.д. и т п.) |
| **2.4.** | **Другие документы** | **Предоставить полный пакет документов на продукт, подтверждающий соответствие техническим требованиям (на русском или английском языке)** |
| *\* В случае участия в конкурсе простого товарищества, каждый его участник должен отвечать установленным квалификационным требованиям.* |

|  |
| --- |
| **3. Существенные требования/ Технические спецификации** |

|  |
| --- |
| **Требования к программному обеспечению оперативного мониторинга состояния информационной безопасности (SIEM)** |
| **Наименование** | **Описание** | **Срок поставки** | **Кол-во** |
| **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:
	+ Astra Linux Special Edition 1.7.1;
	+ Oracle Linux версии 8.6
* Система должна обеспечивать высокую производительность и поддерживать прием и обработку потока в размере до 300 000 событий в секунду (EPS) на одном сервере.
* Для хранения событий должна использоваться нереляционная колоночная база данных для обеспечения высокой скорости поиска.
 | Срок поставки не более 10 рабочих дней | 7000 EPS |
| **Требования к архитектуре системы** | * Система должна поддерживать горизонтальное масштабирование ключевых ее компонентов: коллектора, коррелятора и хранилища событий без необходимости приобретения дополнительных лицензий на ПО.
* Сетевое взаимодействие всех компонентов SIEM должно выполняться по шифрованным каналам связи:
	+ Напрямую;
	+ Через сторонний брокер сообщений для передачи событий между источниками, коллекторами и корреляторами.
* Компоненты системы должны поддерживать установку в распределённых и изолированных сетях без необходимости доступа к сети Интернет.
* Система должна поддерживать возможность сбора событий из изолированных сегментов сети через дата-диод, в том числе при отсутствии возможности передачи событий с использованием UDP-пакетов.
* Система должна обеспечивать централизованное управление посредством веб-консоли без установки дополнительного ПО на АРМ администратора.
* Система должна поддерживать мультитенантность, позволяя в рамках единой инсталляции создавать независимые тенанты с возможностью разграничения прав доступа пользователей системы к событиям, инцидентам, правилам корреляции, нормализации, а также определенным настройкам системы по отношению к разным тенантам.
* Система должна поддерживать схемы иерархического развёртывания независимых инсталляций решения, глубина иерархии не ограничена.
* Система должна обеспечивать возможность централизованного обновления конфигурации или перезапуска компонентов, в том числе форсированного.
* Система должна поддерживать гибкую настройку маршрутизации событий между компонентами.
* Система должна обеспечивать режим работы отказоустойчивого кластера для всех компонентов с «горячим» переключением (High Availability);
* Система должна поддерживать работу с несколькими независимыми кластерами хранилища событий для возможности организации гибких схем географически распределенных систем.
* Архитектура решения должна обеспечивать возможность развертывания в географически распределенной инфраструктуре, как минимум в следующем объёме:
	+ Система должна поддерживать возможность передачи определенных событий из удалённых офисов на центральные корреляторы;
	+ Возможность локального сбора, нормализации, агрегации, фильтрации и обогащения событий ИБ в удаленных офисах за счет установки локального коллектора системы.
* Система должна предоставлять RESTful API для управления активами, активными листами, работы с зарегистрированными базовым и корреляционным событиям ИБ: поиск, получение контекстной информации по базовым и корреляционным событиям ИБ, управление статусом обработки.
* Система должна поддерживать автоматическое обновления правил нормализации и правил корреляции, выпускаемых производителем. Должна быть реализована возможность ревизии изменений оператором после получения оповещения о новых доступных ресурсах. Система должна поддерживать обновление в том числе без прямого доступа к интернету с использованием механизма «зеркала обновления».
 |  |
| **Требования к сбору, анализу и хранению событий** | * Система должна обеспечивать как активный, так и пассивный сбор событий с источников данных.
* Система должна обеспечивать унифицированную модель данных.
* Система должна обеспечивать сбор событий следующих типов:
* Netflow (v9, v5);
* sFlow;
* IPFIX;
* Syslog (TCP / UDP);
* CEF;
* JSON;
* CSV/TSV;
* XML;
* Regexp;
* Key/Value.
* Система должна предоставлять централизованный интерфейс управления списком сборщиков событий.
* Система должна обеспечивать активный сбор событий:
	+ Windows Event Log с помощью агента сбора;
	+ WMI;
	+ SNMP v1/v2/v3;
	+ Проходящих через брокеры сообщений Kafka, Nats;
	+ Хранящихся в БД (SQL), через выполнения запросов, обработку результатов (с поддержкой ID-based и Time-Based таблиц);
	+ Хранящихся в лог-файлах локально и на сетевых ресурсах (SMB, NFS, FTP).
* Система должна поддерживать возможность опциональное сохранения исходного (raw) события. Настройки должны предусматривать как безусловное сохранение события, так и сохранение только в случае ошибок разбора события.
* Система должна поддерживать возможность добавления пользовательских типов источников событий и соответствующей настройки правил разбора и нормализации.
* Система должна обеспечивать создание пользовательских парсерсов на основе поддерживаемых форматов и протоколов сбора данных.
* 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 форматах Syslog, CEF.
* Система должна поддерживать возможность последовательного иерархического разбора (нормализации) событий.
* Компонент сбора событий (коллектор) должен обеспечивать буферизацию событий на локальном диске на случай временной недоступности получателей событий, а также автоматическую пересылку буферизованных событий после восстановления соединения. Размер буфера для хранения событий должен быть настраиваемым.
* На этапе первоначальной обработки полученных событий компонент сбора (коллектор) должен обеспечивать:
	+ Нормализацию событий;
	+ Фильтрацию событий;
	+ Агрегацию событий (с возможностью применения математических функций);
	+ Модификацию/мутацию событий;
	+ Коррекцию времени событий;
	+ Потоковое обогащение событий в соответствии с перечнем источников обогащения (см. ниже).
* 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;
* Система должна обеспечивать возможность поиска по базе событий на основе произвольного поиска по базе событий с помощью конструктора запросов;
* Система должна обеспечивать возможность поиска по базе событий на основе SQL-like языка запросов с возможностью проведения группировок и вычислительных операций;
* Система должна обеспечивать возможность вывода статистики полей по базе событий;
* Система должна поддерживать импорт/экспорт контента и ресурсов: правил корреляции, парсеров, коннекторов и т.д.
 |  |
| **Требования к функциям обогащения событий** | * Система должна поддерживать обогащение событий как на коллекторах (на этапе сбора и обработки событий), так и на корреляторе (для обогащения коррелированных событий)
* Система должна иметь возможность лицензионного расширения для добавления функционала потокового обогащения событий посредством сопоставления событий с потоками данных об угрозах путем интеграции с платформой Threat Intelligence. Данные о найденных индикаторах компрометации должны сразу включаться в базовые события с возможностью дальнейшего использования в рамках корреляции.
* Система должна иметь возможность лицензионного расширения для добавления функционала подключения потоков данных об индикаторах компрометации как компании-производителя, так и сторонних поставщиков (OSINT-источники и по стандартному протоколу TAXII).
* Система должна иметь возможность подключения не менее 3 видов потоков данных от производителя системы.
* Система должна поддерживать следующих механизмы и источники для обогащения событий:
	+ Сведения об активах и группах информационных активов, имеющиеся во встроенной базе активов;
	+ Сведения о пользователях и группах, имеющиеся в службе каталогов Active Directory;
	+ DNS;
	+ База географических данных IP-адресов;
	+ Создаваемые пользователем словари;
	+ Сведения о часовом поясе источника событий;
	+ Контекстная информация Threat Intelligence (cведения об индикаторах компрометации и соответствующем контексте хэши файлов, URL-адреса, внешние IP-адреса).
* Система должна поддерживать возможность обогащения событий, содержащих IP-адреса, географическими данными на основе загруженных списков геоданных.
* Система должна поддерживать возможность использования геоданных, полученных из сервисов MaxMind и IP2Location.
* Система должна поддерживать создание пользовательских словарей для обогащения событий и возможность их наполнения через web-интерфейс и/или API.
* Словари, используемые для обогащения, должны поддерживать возможность добавления не менее 50000 записей.
* Система должна поддерживать возможность обогащения событий информацией о смещении времени источника событий относительно всемирного координированного времени (UTC).
 |  |
| **Требования к функциям корреляции событий** | * Система должна обеспечивать потоковую корреляцию событий ИБ в режиме близком к режиму реального времени.
* Компонент корреляции должен поддерживать применение активных списков (Active List / Reference Set) в правилах корреляции.
* Для активных списков должны поддерживаться как минимум следующие операции:
	+ Создание, удаление списков пользователем через UI;
	+ Проверка существования, добавление, изменение и удаление строк как результат работы правила корреляции;
	+ Импорт и экспорт списков в табличном формате;
	+ Поддержка настраиваемого времени жизни (TTL) для записей в активных списках;
	+ Поддержка возможности изменения набора колонок без пересоздания активного списка.
* Система должна поставляться с набором предустановленных правил корреляции, созданных на основе исследований актуальных угроз и способов атак, разработанных на базе матрицы MITRE ATTACK;
* Правила корреляции в Системе должны поддерживать:
	+ Корреляцию по количественному признаку;
	+ Корреляцию по последовательности событий;
	+ Операции выделения фрагментов события (substring, regexp и т.д.);
	+ Автоматическое оповещение при срабатывании правила корреляции;
	+ Корреляцию по глобальным и локальным переменным.
* Глобальные переменные корреляции должны действовать в пределах коррелятора, на котором они объявлены, и при применениях в правилах корреляции, должны иметь возможность принимать различные значения в рамках каждого условия срабатывания правила корреляции (селектора).
* Локальные переменные корреляции должны действовать только в рамках корреляционного правила и условия срабатывания правила корреляции (селектора) в котором они объявлены.
* Переменные корреляции должны поддерживать следующие функции:
	+ Получение информации из активного листа о значении в указанном столбце;
	+ Получение информации о значении в указанном столбце словаря;
	+ Возврат числа символов в строке;
	+ Перевод символов в строке в нижний регистр;
	+ Перевод символов в строке в верхний регистр;
	+ Добавление символов в конец строки;
	+ Добавление символов в начало строки;
	+ Возврат подстроки из строки по координатам начала и конца подстроки;
	+ Удаление из начала и/или конца строки указанных символов/подстроки;
	+ Замена в строке всех вхождений последовательности символов А на последовательность символов B;
	+ Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения;
	+ Получение из исходной строки результата, удовлетворяющего условию регулярного выражения;
	+ Получение временной метки в формате epoch;
	+ Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных cо временем в формате epoch;
	+ Преобразование времени из формата RFC3339 в формат epoch и наоборот;
	+ Округление времени в формате epoch (до секунд/минут/часов/суток);
	+ Получение интервала времени между двумя метками времени в формате epoch (в секундах/минутах/часах/днях);
	+ Основные математические операции:
		- Сложение;
		- Вычитание;
		- Умножение;
		- Деление;
		- Деление по модулю;
		- Округление числа (в большую/меньшую сторону);
		- Получение числа по модулю;
		- Возведение в степень.
 |  |
| **Требования к функциям реагирования** | * Система должна поддерживать вызов функций автоматизированного реагирования в результате срабатывания правил корреляции.
* Система должна поддерживать следующие механизмы реагирования:
	+ Автоматический запуск пользовательских скриптов (серверных);
	+ Принудительный запуск внеочередной проверки на вирусы или обновления баз через сервер управления средств защиты конечных точек как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции);
	+ Принудительный запуск внеочередного обновления баз через сервер управления средств защиты конечных точек как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции);
	+ Реагирование с использованием возможностей EDR-агентов как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции). Должны быть доступны следующие действия:
		- Сетевая изоляция хоста с настройкой исключений;
		- Запуск произвольных команд на хосте и получение результатов выполнения;
		- Создание правила запрета на основе параметров событий, получаемых SIEM
	+ Реагирование с использованием возможностей решений для защиты инфраструктуры промышленных предприятий как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции). Должно быть доступно изменение статуса актива.
	+ Управление учетными записями в Active Directory как в ручном режиме (из карточки учетной записи), так и автоматически (при срабатывании правила корреляции). Должны быть доступны следующие действия:
		- Добавление и удаление учетной записи из группы;
		- Сброс пароля учетной записи;
		- Блокировка учетной записи.
	+ Управление уровнем осведомленности сотрудников путем назначения соответствующих курсов из карточки учетной записи.
 |  |
| **Требования к управлению сведениями об активах** | * Система должна обеспечивать сбор и автоматическое обновление и хранение во встроенной базе данных в том числе следующей инвентаризационной информации об информационных активах:
	+ IP
	+ MAC
	+ FQDN
	+ Перечень установленного ПО
	+ Информация об актуальных уязвимостях ПО
	+ Информация об аппаратном обеспечении
	+ Дата последнего обновления защиты
	+ Статус защитного ПО, установленного на активе
* Система должна предоставлять возможность добавлять пользовательские поля в карточку актива;
* Система должна поддерживать следующие механизмы наполнения и обновления встроенной базы информационных активов:
	+ Автоматической сбор и обновление информации посредством интеграции с сервером управления от средств защиты конечных точек;
	+ Автоматический сбор и обновление информации посредством интеграции с средством защиты промышленных/технологических сетей;
	+ Ручное добавление отчетов по информации об активах и уязвимостях от сканера уязвимости;
	+ Ручное добавление или редактирование информации об активах через графический интерфейс Системы;
	+ Импорт активов через REST API.
* Система должна поддерживать создание пользовательских групп (категорий) активов;
* Система должна обеспечивать возможность автоматической категоризации активов на основе одного или комбинации признаков: ОС, IP адресации, FQDN, наличия CVE ID и версии ОС.
* При задании условий автоматической категоризации активов система должна поддерживать логические операторы И, ИЛИ, НЕ, а также их группировку.
* При задании условий автоматической категоризации активов система должна обеспечивать возможность тестирования заданных условий по имеющейся базе информационных активов.
* Система должна поддерживать возможности поиска по активам, сохраненных во встроенной базе данных.
* Система должна поддерживать функцию аудита активов и отслеживать следующие события:
	+ Добавление актива в систему;
	+ Изменение параметров актива (имя, IP-адрес, MAC-адрес, FQDN, ОС);
	+ Удаление актива из системы;
	+ Добавление сведений об уязвимости в актив;
	+ Удаление/изменение сведений об уязвимости актива;
	+ Изменение (добавление/удаление) категории актива
 |  |
| **Требования к функциям работы с инцидентами** | * Система должна обеспечить формирование карточки события обнаружения.
* Карточка должна поддерживать следующие возможности:
	+ Изменение приоритета инцидента;
	+ Назначение инцидента на выбранного аналитика;
	+ Переход к связанным базовых событий из карточки инцидента;
	+ Автоматическое ведение журнала изменений статуса и выполненных действий карточки;
	+ Отображение информационных активов, пользователей, связанных с инцидентом, а также доступной контекстной информации о них;
	+ Выделение информации о связанных с событием обнаружения активах и пользователях с указанием их ценности;
	+ Привязка дополнительных событий вручную для анализа причины инцидента;
* Должна быть реализована возможность объединения нескольких событий корреляции в единый инцидент, как в ручном режиме, так и автоматическом: на основе временного диапазона формирования события корреляции, на основе учетной записи пользователя.
* Должна быть реализована возможность ручной привязки дополнительной информации к инциденту - по пользователям, активам, событиям корреляции с возможности классификации инцидента.
 |  |
| **Требования к визуализации и отчётности** | * Система должна предоставлять инструменты визуализации (дашборды) и отчётности для следующих объектов:
	+ События;
	+ Алерты
	+ Инциденты;
	+ Активы;
	+ Источники событий.
* 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 обеспечивать отображение следующих данных по инцидентам в графическом формате (дашборды):
	+ созданные инциденты;
	+ закрытые инциденты за период;
	+ незакрытые инциденты по критичности;
	+ распределение инцидентов;
	+ инциденты по уровню критичности;
	+ затронутые активы и группы активов;
	+ источники событий с наибольшим количеством инцидентов;
	+ правила корреляции с наибольшим количеством инцидентов;
	+ распределение инцидентов по тенантам (со сравнением с прошлым периодом);
	+ распределение инцидентов по времени обнаружения (first seen);
	+ распределение количества затронутых инцидентами активов по тенантам.
* Система должна обеспечивать отображение следующих данных по событиям в графическом формате (дашборды):
	+ часто встречаемые внутренние IP-адреса в Netflow;
	+ часто встречаемые внешние IP-адреса в Netflow;
	+ статистика объемов трафика относительно портов;
	+ статистика по источникам с наибольшим количеством событий.
* Система должна поддерживать возможность создания пользовательских дашбордов и шаблонов отчетов.
* Система должна поддерживать создание графических панелей (дашбордов) на основе пользовательских запросов к хранилищу событий.
* Формирование и настройка пользовательских графических панелей (дашбордов) или отчётов должно полностью выполняться в графическом веб-интерфейсе.
* Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:
	+ по источникам;
	+ по инцидентам;
* Система должна обеспечивать построение отчетов по инцидентам со следующей информацией:
	+ количество активных инцидентов;
	+ количество нераспределенных инцидентов;
	+ распределенные инциденты по времени;
	+ последние инциденты по времени;
	+ количество инцидентов с распределением по уровню критичности;
	+ количество инцидентов по исполнителям;
	+ количество инцидентов с распределением по статусу;
	+ затронутые активы и группы активов;
	+ источники событий с наибольшим количеством инцидентов;
	+ правила корреляции с наибольшим количеством инцидентов;
	+ затронутые учетные записи;
	+ на основе произвольного поиска по базе событий с помощью конструктора.
* Система должна обеспечивать построение отчетов по источникам со следующей информацией:
	+ часто встречаемые внутренние IP-адреса в Netflow;
	+ часто встречаемые внешние IP-адреса в Netflow;
	+ статистика объемов трафика относительно портов;
	+ статистика по источникам с наибольшим количеством событий.
* Система должна обеспечивать возможность отправки отчетов по почте, размещения отчёта на сетевом хранилище и публикации отчёта через консоль управления системой.
* Система должна поддерживать рассылку отчетов по настраиваемому расписанию.
* Система должна предоставлять возможность экспорта отчетов в формате HTML, CSV, раздельный CSV, XLSX.
 |  |
| **Требования к безопасности** | * Система должна обеспечивать разграничение прав доступа на основе ролевой модели;
* Система должна обеспечивать разграничение прав доступа на основе ролевой модели
* Система должна регистрировать события доступа и значимых изменений конфигурации;
* Система должна поддерживать аутентификацию и авторизацию с использованием следующих механизмов:
	+ Локальная база учётных данным (по логину-паролю) пользователей;
	+ Active Directory.
* Система должна иметь встроенные механизмы противодействия попыткам подбора пароля.
 |  |
| **Требования к эксплуатационной документации** | * Эксплуатационная документация Системы должна включать Руководство пользователя (администратора).
* 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 решения;
* web-сайт производителя должен быть на русском языке, иметь пополняемую базу знаний, а также форум пользователей программных продуктов;
* 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;
* определять приоритет запроса к службе технической поддержки на основе влияния проблемы на бизнес-процессы;
* присваивать более высокий приоритет запросам пользователей расширенной технической поддержки относительно стандартных запросов;
* 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;

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

|  |  |
| --- | --- |
| 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  |

* праздничные дни);

Время реакции должно обеспечиваться согласно уровню критичности:Уровни критичности инцидентов, относящихся к продукту должны соответствовать следующему описанию: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.Дополнительные требования к технической поддержке:* Обеспечивать без дополнительной оплаты разработку производителем Системы парсеров, в количестве не менее чем для 10 (десяти) различных типов данных, изначально не поддерживаемых в стандартной поставке Системы.
 |  |
| **Дополнительные требования**  | Право на поставку должно быть подтверждено авторизационным письмом правообладателя. Наличие не менее 2-х специализированных инженеров. Наличие опыта по характеру аналогичных поставок (услуг) за последние 2 года в сумме не менее 10 млн. (десять миллионов) сом. Подтвердить путем предоставления договора, счет-фактуры, акта приема передачи. Договоры должны быть подтверждены Актами приемки или счет фактурами |  |  |

**БАНКОВСКИЕ РЕКВИЗИТЫ**

**для внесения ГОКЗ и ГОИД**

|  |  |
| --- | --- |
| **Для зачисления Кыргызских сомов** | **For transfer of US dollars** |
| **Intermediary Bank****(Банк-посредник)** |  | **Kookmin Bank, Seoul, South Korea** **SWIFT: CZNBKRSE** |
| **Bank of Beneficiary****(Банк получателя)** | ОАО “Айыл Банк”, г. Бишкек, Кыргызская Республика | **OAO AIYL BANK, Kyrgyz Republic, Bishkek** **SWIFT: AIYLKG22****Номер счета: 7C78USD013** |
| **Beneficiary (Получатель)** | ЗАО "Альфа Телеком",Счет № 1350100027537623   БИК: 135001 | **Beneficiary Name: CJSC Alfa Telecom****Beneficiary account: NO.1350100022480485****Address: KYRGYZSTAN, Bishkek, Suyumbaeva 123** |
| **Purpose of payment****(Назначение платежа)** | ***- Гарантийное обеспечение конкурсной заявки;******- Гарантийное обеспечение исполнения договора от \_\_\_\_ №\_\_\_\_;*** | **В назначении указать: за что, р/счет и наименование компании.** **Например**: Account replenishment, FOR FURTHER CREDIT TO ACCOUNT. NO.1350100022480485 CJSC Alfa Telecom USD |

**Примечание:** Расходы, связанные с банковским переводом, несет победитель конкурса.

**Приложение 2 к Приглашению**

**Форма**

|  |  |
| --- | --- |
|  | **КОНКУРСНАЯ ЗАЯВКА**КОМУ: **ЗАО «Альфа Телеком»** На Приглашение № \_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г. ОТ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(наименование поставщика)***Для резидентов КР:** |
|

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Наименование товара, Подробное описание** | **Кол-во** | **Цена****за ед. без НСП и НДС\*** | **Общая стоимость, без НСП и НДС\*** | **НСП** | **Сумма****НДС\*** | **Общая стоимость, с учетом НСП и НДС\*** |
| **Программное обеспечение оперативного мониторинга состояния информационной безопасности (SIEM)**(прописать подробную техспецификацию, модель и т.д.) | 1 |  |  |  |  |  |
|  **Итого:** |  |

**Для нерезидентов КР:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование товара, Подробное описание** | **Кол-во** | **Цена****за ед. с учетом всех налогов** | **Общая стоимость с учетом всех налогов** |
| **Программное обеспечение оперативного мониторинга состояния информационной безопасности (SIEM)**(прописать подробную техспецификацию, модель и т.д.) | 1 |  |  |
|  **Итого:** |  |

**Срок поставки составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рабочих дней**В цену, указанную поставщиком, должны быть включены все налоги, сборы и другие платежи, взимаемые в соответствии с законодательством Кыргызской Республики, накладные затраты, транспортные и другие затраты поставщика. **\*Сумма НДС в графах заполняется поставщиком, только в случае если он является плательщиком НДС в Кыргызской Республике на момент подачи конкурсной заявки.**Данная конкурсная заявка действительна в течение 60 (шестидесяти) календарных дней с даты вскрытия конкурсных заявок. Подавая настоящую конкурсную заявку, выражаем свое согласие заключить договор (в случае признания конкурсной заявки, выигравшей) на условиях, обозначенных в Требованиях к закупке и по форме Договора согласно приложению 3 к Приглашению. В случае принятия нашей Конкурсной заявки, мы обязуемся предоставить гарантийное обеспечение исполнения Договора на сумму \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, для надлежащего выполнения Договора и в сроки, указанные в Конкурсной документации.Также подавая конкурсную заявку подтверждаем и гарантируем свою правоспособность, наличие регистрации в установленном законодательством порядке, а также наличие необходимых разрешительных документов на осуществление нашей деятельности. Гарантируем, что лицо, подписавшее настоящую конкурсную заявку, обладает всеми необходимыми полномочиями на ее подписание.  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(ФИО) (должность) (подпись и печать)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023 года

 (дата заполнения)

**Приложение № 2.1 к Приглашению**

**Форма для заполнения соответствия техническим требованиям**

**(прописать по каждой позиции согласно существенных требований/технических спецификаций)**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование требований** | **Соответствует/Не соответствует** | **Примечание** |
| **1.** | **Требования к оборудованию** |  |  |
| 1.1 | Компоненты системы должны поддерживать установку как на физических, так и на виртуальных машинах. |  |  |
| 1.2 | Основные компоненты (модули, отвечающие за сбор событий, корреляцию, хранение событий) должны поддерживать установку на операционной системе семейства Linux:* + Astra Linux Special Edition 1.7.1;
	+ Oracle Linux версии 8.6
 |  |  |
| 1.3 | Система должна обеспечивать высокую производительность и поддерживать прием и обработку потока в размере до 300 000 событий в секунду (EPS) на одном сервере. |  |  |
| 1.4 | Для хранения событий должна использоваться нереляционная колоночная база данных для обеспечения высокой скорости поиска |  |  |
| **2.** | **Требования к архитектуре системы** |  |  |
| 2.1. | Система должна поддерживать горизонтальное масштабирование ключевых ее компонентов: коллектора, коррелятора и хранилища событий без необходимости приобретения дополнительных лицензий на ПО. |  |  |
| 2.2. | Сетевое взаимодействие всех компонентов SIEM должно выполняться по шифрованным каналам связи:* + Напрямую;

Через сторонний брокер сообщений для передачи событий между источниками, коллекторами и корреляторами |  |  |
| 2.3. | Компоненты системы должны поддерживать установку в распределённых и изолированных сетях без необходимости доступа к сети Интернет |  |  |
| 2.4. | Система должна поддерживать возможность сбора событий из изолированных сегментов сети через дата-диод, в том числе при отсутствии возможности передачи событий с использованием UDP-пакетов |  |  |
| 2.5. | Система должна обеспечивать централизованное управление посредством веб-консоли без установки дополнительного ПО на АРМ администратора |  |  |
| 2.6. | Система должна поддерживать мультитенантность, позволяя в рамках единой инсталляции создавать независимые тенанты с возможностью разграничения прав доступа пользователей системы к событиям, инцидентам, правилам корреляции, нормализации, а также определенным настройкам системы по отношению к разным тенантам |  |  |
| 2.7. | Система должна поддерживать схемы иерархического развёртывания независимых инсталляций решения, глубина иерархии не ограничена |  |  |
| 2.8. | Система должна обеспечивать возможность централизованного обновления конфигурации или перезапуска компонентов, в том числе форсированного |  |  |
| 2.9. | Система должна поддерживать гибкую настройку маршрутизации событий между компонентами |  |  |
| 2.10. | Система должна обеспечивать режим работы отказоустойчивого кластера для всех компонентов с «горячим» переключением (High Availability);  |  |  |
| 2.11. | Система должна поддерживать работу с несколькими независимыми кластерами хранилища событий для возможности организации гибких схем географически распределенных систем |  |  |
| 2.12. | Архитектура решения должна обеспечивать возможность развертывания в географически распределенной инфраструктуре, как минимум в следующем объёме:* + Система должна поддерживать возможность передачи определенных событий из удалённых офисов на центральные корреляторы;

Возможность локального сбора, нормализации, агрегации, фильтрации и обогащения событий ИБ в удаленных офисах за счет установки локального коллектора системы |  |  |
| 2.13. | Система должна предоставлять RESTful API для управления активами, активными листами, работы с зарегистрированными базовым и корреляционным событиям ИБ: поиск, получение контекстной информации по базовым и корреляционным событиям ИБ, управление статусом обработки |  |  |
| 2.14. | Система должна поддерживать автоматическое обновления правил нормализации и правил корреляции, выпускаемых производителем. Должна быть реализована возможность ревизии изменений оператором после получения оповещения о новых доступных ресурсах. Система должна поддерживать обновление в том числе без прямого доступа к интернету с использованием механизма «зеркала обновления». |  |  |
| **3.** | **Требования к сбору, анализу и хранению событий**  |  |  |
| 3.1. | Система должна обеспечивать как активный, так и пассивный сбор событий с источников данных |  |  |
| 3.2. | Система должна обеспечивать унифицированную модель данных |  |  |
| 3.3. | Система должна обеспечивать сбор событий следующих типов:* Netflow (v9, v5);
* sFlow;
* IPFIX;
* Syslog (TCP / UDP);
* CEF;
* JSON;
* CSV/TSV;
* XML;
* Regexp;
* Key/Value.
 |  |  |
| 3.4. | Система должна предоставлять централизованный интерфейс управления списком сборщиков событий |  |  |
| 3.5. | Система должна обеспечивать активный сбор событий:* + Windows Event Log с помощью агента сбора;
	+ WMI;
	+ SNMP v1/v2/v3;
	+ Проходящих через брокеры сообщений Kafka, Nats;
	+ Хранящихся в БД (SQL), через выполнения запросов, обработку результатов (с поддержкой ID-based и Time-Based таблиц);
	+ Хранящихся в лог-файлах локально и на сетевых ресурсах (SMB, NFS, FTP).
 |  |  |
| 3.6. | Система должна поддерживать возможность опциональное сохранения исходного (raw) события. Настройки должны предусматривать как безусловное сохранение события, так и сохранение только в случае ошибок разбора события |  |  |
| 3.7. | Система должна поддерживать возможность добавления пользовательских типов источников событий и соответствующей настройки правил разбора и нормализации |  |  |
| 3.8. | Система должна обеспечивать создание пользовательских парсерсов на основе поддерживаемых форматов и протоколов сбора данных |  |  |
| 3.9. | 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 |  |  |
| 3.10. | Система без дополнительных настроек разбора (нормализации) должна поддерживать получение событий в форматах Syslog, CEF |  |  |
| 3.11. | Система должна поддерживать возможность последовательного иерархического разбора (нормализации) событий |  |  |
| 3.12. | Компонент сбора событий (коллектор) должен обеспечивать буферизацию событий на локальном диске на случай временной недоступности получателей событий, а также автоматическую пересылку буферизованных событий после восстановления соединения. Размер буфера для хранения событий должен быть настраиваемым |  |  |
| 3.13. | На этапе первоначальной обработки полученных событий компонент сбора (коллектор) должен обеспечивать:* + Нормализацию событий;
	+ Фильтрацию событий;
	+ Агрегацию событий (с возможностью применения математических функций);
	+ Модификацию/мутацию событий;
	+ Коррекцию времени событий;
	+ Потоковое обогащение событий в соответствии с перечнем источников обогащения (см. ниже).
 |  |  |
| 3.14. | 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 |  |  |
| 3.15 | Система должна обеспечивать возможность поиска по базе событий на основе произвольного поиска по базе событий с помощью конструктора запросов |  |  |
| 3.16 | Система должна обеспечивать возможность поиска по базе событий на основе SQL-like языка запросов с возможностью проведения группировок и вычислительных операций |  |  |
| 3.17 | Система должна обеспечивать возможность вывода статистики полей по базе событий |  |  |
| 3.18 | Система должна поддерживать импорт/экспорт контента и ресурсов: правил корреляции, парсеров, коннекторов и т.д. |  |  |
| **4.** | **Требования к функциям обогащения событий** |  |  |
| 4.1 | Система должна поддерживать обогащение событий как на коллекторах (на этапе сбора и обработки событий), так и на корреляторе (для обогащения коррелированных событий) |  |  |
| 4.2 | Система должна иметь возможность лицензионного расширения для добавления функционала потокового обогащения событий посредством сопоставления событий с потоками данных об угрозах путем интеграции с платформой Threat Intelligence. Данные о найденных индикаторах компрометации должны сразу включаться в базовые события с возможностью дальнейшего использования в рамках корреляции |  |  |
| 4.3 | Система должна иметь возможность лицензионного расширения для добавления функционала подключения потоков данных об индикаторах компрометации как компании-производителя, так и сторонних поставщиков (OSINT-источники и по стандартному протоколу TAXII). |  |  |
| 4.4 | Система должна иметь возможность подключения не менее 3 видов потоков данных от производителя системы |  |  |
| 4.5 | Система должна поддерживать следующих механизмы и источники для обогащения событий:* + Сведения об активах и группах информационных активов, имеющиеся во встроенной базе активов;
	+ Сведения о пользователях и группах, имеющиеся в службе каталогов Active Directory;
	+ DNS;
	+ База географических данных IP-адресов;
	+ Создаваемые пользователем словари;
	+ Сведения о часовом поясе источника событий;
	+ Контекстная информация Threat Intelligence (cведения об индикаторах компрометации и соответствующем контексте хэши файлов, URL-адреса, внешние IP-адреса).
 |  |  |
| 4.6 | Система должна поддерживать возможность обогащения событий, содержащих IP-адреса, географическими данными на основе загруженных списков геоданных |  |  |
| 4.7 | Система должна поддерживать возможность использования геоданных, полученных из сервисов MaxMind и IP2Location |  |  |
| 4.8 | Система должна поддерживать создание пользовательских словарей для обогащения событий и возможность их наполнения через web-интерфейс и/или API |  |  |
| 4.9 | Словари, используемые для обогащения, должны поддерживать возможность добавления не менее 50000 записей |  |  |
| 4.10 | Система должна поддерживать возможность обогащения событий информацией о смещении времени источника событий относительно всемирного координированного времени (UTC) |  |  |
| **5.** | **Требования к функциям корреляции событий** |  |  |
| 5.1 | Система должна обеспечивать потоковую корреляцию событий ИБ в режиме близком к режиму реального времени |  |  |
| 5.2 | Компонент корреляции должен поддерживать применение активных списков (Active List / Reference Set) в правилах корреляции |  |  |
| 5.3 | Для активных списков должны поддерживаться как минимум следующие операции:* + Создание, удаление списков пользователем через UI;
	+ Проверка существования, добавление, изменение и удаление строк как результат работы правила корреляции;
	+ Импорт и экспорт списков в табличном формате;
	+ Поддержка настраиваемого времени жизни (TTL) для записей в активных списках;
	+ Поддержка возможности изменения набора колонок без пересоздания активного списка.
 |  |  |
| 5.4 | Система должна поставляться с набором предустановленных правил корреляции, созданных на основе исследований актуальных угроз и способов атак, разработанных на базе матрицы MITRE ATTACK |  |  |
| 5.5 | Правила корреляции в Системе должны поддерживать:* + Корреляцию по количественному признаку;
	+ Корреляцию по последовательности событий;
	+ Операции выделения фрагментов события (substring, regexp и т.д.);
	+ Автоматическое оповещение при срабатывании правила корреляции;
	+ Корреляцию по глобальным и локальным переменным.
 |  |  |
| 5.6 | Глобальные переменные корреляции должны действовать в пределах коррелятора, на котором они объявлены, и при применениях в правилах корреляции, должны иметь возможность принимать различные значения в рамках каждого условия срабатывания правила корреляции (селектора). |  |  |
| 5.7 | Локальные переменные корреляции должны действовать только в рамках корреляционного правила и условия срабатывания правила корреляции (селектора) в котором они объявлены |  |  |
| 5.8 | Переменные корреляции должны поддерживать следующие функции:* + Получение информации из активного листа о значении в указанном столбце;
	+ Получение информации о значении в указанном столбце словаря;
	+ Возврат числа символов в строке;
	+ Перевод символов в строке в нижний регистр;
	+ Перевод символов в строке в верхний регистр;
	+ Добавление символов в конец строки;
	+ Добавление символов в начало строки;
	+ Возврат подстроки из строки по координатам начала и конца подстроки;
	+ Удаление из начала и/или конца строки указанных символов/подстроки;
	+ Замена в строке всех вхождений последовательности символов А на последовательность символов B;
	+ Замена в строке последовательности символов, удовлетворяющих регулярному выражению, на последовательность символов и группы захвата регулярного выражения;
	+ Получение из исходной строки результата, удовлетворяющего условию регулярного выражения;
	+ Получение временной метки в формате epoch;
	+ Получение атомарных представлений времени (в виде год, месяц, день, час, минута, секунда, день недели) из полей и переменных cо временем в формате epoch;
	+ Преобразование времени из формата RFC3339 в формат epoch и наоборот;
	+ Округление времени в формате epoch (до секунд/минут/часов/суток);
	+ Получение интервала времени между двумя метками времени в формате epoch (в секундах/минутах/часах/днях);
 |  |  |
| 5.9 | Основные математические операции:* + - Сложение;
		- Вычитание;
		- Умножение;
		- Деление;
		- Деление по модулю;
		- Округление числа (в большую/меньшую сторону);
		- Получение числа по модулю;
		- Возведение в степень.
 |  |  |
| **6.** | **Требования к функциям реагирования** |  |  |
| 6.1. | Система должна поддерживать вызов функций автоматизированного реагирования в результате срабатывания правил корреляции |  |  |
| 6.2 | Система должна поддерживать следующие механизмы реагирования:* + Автоматический запуск пользовательских скриптов (серверных);
	+ Принудительный запуск внеочередной проверки на вирусы или обновления баз через сервер управления средств защиты конечных точек как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции);
	+ Принудительный запуск внеочередного обновления баз через сервер управления средств защиты конечных точек как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции);
	+ Реагирование с использованием возможностей EDR-агентов как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции). **Должны быть доступны следующие действия:**
		- Сетевая изоляция хоста с настройкой исключений;
		- Запуск произвольных команд на хосте и получение результатов выполнения;
		- Создание правила запрета на основе параметров событий, получаемых SIEM
	+ Реагирование с использованием возможностей решений для защиты инфраструктуры промышленных предприятий как в ручном режиме (из карточки актива), так и автоматически (при срабатывании правила корреляции). Должно быть доступно изменение статуса актива.
	+ Управление учетными записями в Active Directory как в ручном режиме (из карточки учетной записи), так и автоматически (при срабатывании правила корреляции). **Должны быть доступны следующие действия:**
		- Добавление и удаление учетной записи из группы;
		- Сброс пароля учетной записи;
		- Блокировка учетной записи.
	+ Управление уровнем осведомленности сотрудников путем назначения соответствующих курсов из карточки учетной записи.
 |  |  |
| **7.** | **Требования к управлению сведениями об активах** |  |  |
| **7.1** | Система должна обеспечивать сбор и автоматическое обновление и хранение во встроенной базе данных в том числе следующей инвентаризационной информации об информационных активах:* + IP
	+ MAC
	+ FQDN
	+ Перечень установленного ПО
	+ Информация об актуальных уязвимостях ПО
	+ Информация об аппаратном обеспечении
	+ Дата последнего обновления защиты
	+ Статус защитного ПО, установленного на активе
 |  |  |
| 7.2 | Система должна предоставлять возможность добавлять пользовательские поля в карточку актива |  |  |
| 7.3 | Система должна поддерживать следующие механизмы наполнения и обновления встроенной базы информационных активов:* + Автоматической сбор и обновление информации посредством интеграции с сервером управления от средств защиты конечных точек;
	+ Автоматический сбор и обновление информации посредством интеграции с средством защиты промышленных/технологических сетей;
	+ Ручное добавление отчетов по информации об активах и уязвимостях от сканера уязвимости;
	+ Ручное добавление или редактирование информации об активах через графический интерфейс Системы;
	+ Импорт активов через REST API.
 |  |  |
| 7.4 | Система должна поддерживать создание пользовательских групп (категорий) активов |  |  |
| 7.5 | Система должна обеспечивать возможность автоматической категоризации активов на основе одного или комбинации признаков: ОС, IP адресации, FQDN, наличия CVE ID и версии ОС |  |  |
| 7.6 | При задании условий автоматической категоризации активов система должна поддерживать логические операторы И, ИЛИ, НЕ, а также их группировку |  |  |
| 7.7 | При задании условий автоматической категоризации активов система должна обеспечивать возможность тестирования заданных условий по имеющейся базе информационных активов |  |  |
| 7.8 | Система должна поддерживать возможности поиска по активам, сохраненных во встроенной базе данных |  |  |
| 7.9 | Система должна поддерживать функцию аудита активов и отслеживать следующие события:* + Добавление актива в систему;
	+ Изменение параметров актива (имя, IP-адрес, MAC-адрес, FQDN, ОС);
	+ Удаление актива из системы;
	+ Добавление сведений об уязвимости в актив;
	+ Удаление/изменение сведений об уязвимости актива;
	+ Изменение (добавление/удаление) категории актива
 |  |  |
| **8.** | **Требования к функциям работы с инцидентами** |  |  |
| 8.1 | Система должна обеспечить формирование карточки события обнаружения |  |  |
| 8.2 | Карточка должна поддерживать следующие возможности:* + Изменение приоритета инцидента;
	+ Назначение инцидента на выбранного аналитика;
	+ Переход к связанным базовых событий из карточки инцидента;
	+ Автоматическое ведение журнала изменений статуса и выполненных действий карточки;
	+ Отображение информационных активов, пользователей, связанных с инцидентом, а также доступной контекстной информации о них;
	+ Выделение информации о связанных с событием обнаружения активах и пользователях с указанием их ценности;
	+ Привязка дополнительных событий вручную для анализа причины инцидента;
 |  |  |
| 8.3 | Должна быть реализована возможность объединения нескольких событий корреляции в единый инцидент, как в ручном режиме, так и автоматическом: на основе временного диапазона формирования события корреляции, на основе учетной записи пользователя |  |  |
| 8.4 | Должна быть реализована возможность ручной привязки дополнительной информации к инциденту - по пользователям, активам, событиям корреляции с возможности классификации инцидента |  |  |
| **9.** | **Требования к визуализации и отчётности** |  |  |
| 9.1 | Система должна предоставлять инструменты визуализации (дашборды) и отчётности для следующих объектов:* + События;
	+ Алерты
	+ Инциденты;
	+ Активы;
	+ Источники событий.
 |  |  |
| 9.2 | Система должна поставляться с предустановленным набором графических панелей (дашбордов) и отчётов |  |  |
| 9.3 | Система должна поддерживать возможность создания пользовательских шаблонов и правил уведомлений о событиях и инцидентах |  |  |
| 9.4 | Система должна обеспечивать отображение следующих данных по инцидентам в графическом формате (дашборды):* + созданные инциденты;
	+ закрытые инциденты за период;
	+ незакрытые инциденты по критичности;
	+ распределение инцидентов;
	+ инциденты по уровню критичности;
	+ затронутые активы и группы активов;
	+ источники событий с наибольшим количеством инцидентов;
	+ правила корреляции с наибольшим количеством инцидентов;
	+ распределение инцидентов по тенантам (со сравнением с прошлым периодом);
	+ распределение инцидентов по времени обнаружения (first seen);
	+ распределение количества затронутых инцидентами активов по тенантам.
 |  |  |
| 9.5 | Система должна обеспечивать отображение следующих данных по событиям в графическом формате (дашборды):* + часто встречаемые внутренние IP-адреса в Netflow;
	+ часто встречаемые внешние IP-адреса в Netflow;
	+ статистика объемов трафика относительно портов;
	+ статистика по источникам с наибольшим количеством событий.
 |  |  |
| 9.6 | Система должна поддерживать возможность создания пользовательских дашбордов и шаблонов отчетов |  |  |
| 9.7 | Система должна поддерживать создание графических панелей (дашбордов) на основе пользовательских запросов к хранилищу событий |  |  |
| 9.8 | Формирование и настройка пользовательских графических панелей (дашбордов) или отчётов должно полностью выполняться в графическом веб-интерфейсе. |  |  |
| 9.9 | Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:* + по источникам;
	+ по инцидентам;
 |  |  |
| 9.10 | Система должна обеспечивать построение отчетов по инцидентам со следующей информацией:* + количество активных инцидентов;
	+ количество нераспределенных инцидентов;
	+ распределенные инциденты по времени;
	+ последние инциденты по времени;
	+ количество инцидентов с распределением по уровню критичности;
	+ количество инцидентов по исполнителям;
	+ количество инцидентов с распределением по статусу;
	+ затронутые активы и группы активов;
	+ источники событий с наибольшим количеством инцидентов;
	+ правила корреляции с наибольшим количеством инцидентов;
	+ затронутые учетные записи;
	+ на основе произвольного поиска по базе событий с помощью конструктора.
 |  |  |
| 9.11 | Система должна обеспечивать построение отчетов по источникам со следующей информацией:* + часто встречаемые внутренние IP-адреса в Netflow;
	+ часто встречаемые внешние IP-адреса в Netflow;
	+ статистика объемов трафика относительно портов;
	+ статистика по источникам с наибольшим количеством событий.
 |  |  |
| 9.12 | Система должна обеспечивать возможность отправки отчетов по почте, размещения отчёта на сетевом хранилище и публикации отчёта через консоль управления системой |  |  |
| 9.13 | Система должна поддерживать рассылку отчетов по настраиваемому расписанию |  |  |
| 9.14 | Система должна предоставлять возможность экспорта отчетов в формате HTML, CSV, раздельный CSV, XLSX |  |  |
| **10.** | **Требования к безопасности** |  |  |
| 10.1 | Система должна обеспечивать разграничение прав доступа на основе ролевой модели |  |  |
| 10.2 | Система должна обеспечивать разграничение прав доступа на основе ролевой модели |  |  |
| 10.3 | Система должна регистрировать события доступа и значимых изменений конфигурации |  |  |
| 10.4 | Система должна поддерживать аутентификацию и авторизацию с использованием следующих механизмов:* + Локальная база учётных данным (по логину-паролю) пользователей;
	+ Active Directory.
 |  |  |
| 10.5 | Система должна иметь встроенные механизмы противодействия попыткам подбора пароля |  |  |
| **11.** | **Требования к эксплуатационной документации** |  |  |
| 11.1 | Эксплуатационная документация Системы должна включать Руководство пользователя (администратора). |  |  |
| 11.2 | Документация, поставляемая в комплекте с Системой, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства |  |  |
| **12.** | **Требования к технической поддержке** |  |  |
| 12.1 | **Техническая поддержка программного обеспечения должна соответствовать следующим требованиям:** |  |  |
| 12.1.1 | предоставляться на русском языке сертифицированными специалистами производителя решения |  |  |
| 12.1.2 | web-сайт производителя должен быть на русском языке, иметь пополняемую базу знаний, а также форум пользователей программных продуктов |  |  |
| 12.1.3 | предоставлять возможность использования персональной учетной записи пользователя для создания, обновления и мониторинга инцидентов |  |  |
| 12.1.4 | предоставлять техническую поддержку и консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта |  |  |
| 12.1.5 | определять приоритет запроса к службе технической поддержки на основе влияния проблемы на бизнес-процессы |  |  |
| 12.1.6 | присваивать более высокий приоритет запросам пользователей расширенной технической поддержки относительно стандартных запросов |  |  |
| 12.1.7 | регулярно информировать о промежуточных результатах и ходе решения запросов |  |  |
| 12.1.8 | предоставлять возможность предъявления претензий и жалоб на качество обслуживания на уровень руководителя технический поддержки регионального офиса или менеджера по работе с корпоративными клиентами |  |  |
| 12.2 | **Техническое консультирование по вопросам эксплуатации продукта и приём запросов на устранение негативных последствий инцидентов должно обеспечиваться посредством:** |  |  |
| 12.2.1 |

|  |  |
| --- | --- |
| 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  |

 |  |  |
| 12.2.2 | Предоставления доступа Пользователю к Интернет-Порталу технической поддержки с возможностью размещения запросов в режиме 24x7x365 (круглосуточно, включая выходные и праздничные дни)  |  |  |
| 12.2.3 | Уровни критичности инцидентов, относящихся к продукту должны соответствовать следующему описанию: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.Дополнительные требования к технической поддержке:Обеспечивать без дополнительной оплаты разработку производителем Системы парсеров, в количестве не менее чем для 10 (десяти) различных типов данных, изначально не поддерживаемых в стандартной поставке Системы. |  |  |
| **13.** | **Дополнительные требования** |  |  |
| 13.1 | Право на поставку должно быть подтверждено авторизационным письмом правообладателя |  |  |
| 13.2 | Наличие не менее 2-х специализированных инженеров |  |  |
| 13.3 | Наличие опыта по характеру аналогичных поставок (услуг) за последние 2 года в сумме не менее 10 млн. (десять миллионов) сом. Подтвердить путем предоставления договора, счет-фактуры, акта приема передачи. Договоры должны быть подтверждены Актами приемки или счет фактурами |  |  |

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ФИО

**Приложение 3 к Приглашению**

**Проект ДОГОВОРА**

**о поставке программного обеспечения**

г. Бишкек «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2023 г.

 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** в дальнейшем именуемое «**Сторона-1**», в лице директора \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании Устава, с одной стороны, и

 **ЗАО «Альфа Телеком»**, именуемое в дальнейшем **«Сторона-2»**, в лице Генерального директора Куренкеева А. С., действующего на основании Устава, с другой стороны, и совместно именуемые Стороны, заключили настоящий Договор о нижеследующем.

**1. Предмет договора**

* 1. Сторона-1 обязуется осуществить поставку Стороне-2 программного обеспечения и лицензионных ключей (далее – ПО) и доступ к технической поддержке на условиях постоянной неисключительной лицензии на его использование в количестве, по ценам и техническим параметрам, указанным в Приложении 1 к настоящему Договору (далее Спецификация), являющихся неотъемлемой частью настоящего Договора, а Сторона-2, в свою очередь, принимает надлежаще поставленное ПО/права и осуществляет оплату в порядке и размере, предусмотренном разделом 3 настоящего Договора.
	2. Все приложения и дополнительные соглашения к настоящему Договору являются неотъемлемой его частью.

**2. Права и обязанности сторон**

**2.1. Обязанности Стороны-1**

* + 1. Передать Стороне-2 по Акту приема-передачи ПО и право пользования технической поддержкой, которое включает в себя: лицензии, возможность получения новых версий ПО, обновлений, технической помощи по установке, настройке, устранению проблем в работе ПО, в строгом соответствии со Спецификацией к настоящему Договору, в порядке и на условиях, предусмотренных настоящим Договором и в строгом соответствии с Приложением 1.
		2. Незамедлительно информировать Сторону-2 о невозможности исполнения обязательств, в срок, предусмотренный настоящим Договором.
		3. Известить Сторону-2 по эл. почте InfSecurity@megacom.kg о предоставления права пользования ПО и технической поддержкой, а также способ получения доступа к установочным файлам ПО, инструкциям.
		4. Оповестить Сторону-2 об изменении юридического/фактического адреса, либо банковских реквизитов в течение 3 (трех) рабочих дней со дня их изменения.
		5. Сторона-1 гарантирует, что действует в рамках полномочий и объема прав, предоставленных ему правообладателем исключительных имущественных авторских прав на ПО.
		6. Сторона-1 подтверждает, что в случае превышения предоставления объема прав, предоставленных ему Правообладателем ПО, Сторона-1 несет ответственность перед Правообладателем ПО самостоятельно. В случае если такое превышение полномочий впоследствии сделает невозможным использование технической поддержки Стороной-2, то Сторона-1 обязуется возвратить денежные средства, полученные по настоящему Договору от Стороны-2.
		7. При возникновении затруднений при развертывании, установке, обновлении ПО и невозможности предоставления технической поддержки удаленным способом, выделить инженера для локальной настройки ПО на территории Стороны-2.
	1. **Обязанности Стороны-2:**
		1. Принять от Стороны-1 надлежаще переданное ПО и право пользования технической поддержкой и произвести оплату в соответствии с условиями настоящего Договора, в частности, с разделом 3 настоящего Договора.
		2. Оповестить Сторону-1 об изменении юридического/фактического адреса, электронного адреса, либо банковских реквизитов в течение 3 (трех) рабочих дней со дня их изменения.
		3. Передавать Стороне-1 необходимую информацию для выполнения обязательств по настоящему Договору.

**2.3. Права Стороны-2:**

**2.3.1.** В случае не предоставления Стороной-1 Стороне-2 прав доступа к ПО и технической поддержкой или несвоевременного предоставления таких прав согласно Договора, Сторона-2 вправе взыскать со Стороны-1 причиненные убытки и/или расторгнуть настоящий договор в одностороннем порядке.

**3. Стоимость договора и порядок оплаты**

* 1. Общая стоимость настоящего Договора составляет: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**сомов, с учетом всех налогов, предусмотренных действующим законодательством Кыргызской Республики для данных правоотношений. НДС 12% составляет **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сом, НсП=0%. Сторона-1 – плательщик НДС.

Стоимость Договора является окончательной и изменению не подлежит.

* 1. Сторона-2 осуществляет оплату по настоящему Договору в следующем порядке:

100 % от общей стоимости Договора, в течение 10 банковских дней с момента получения Стороной-2 оригинала счета-фактуры, выставленного Стороной-1 на основании подписанного сторонами и датой Акта приема-передачи прав доступа к ПО и технической поддержке.

* 1. Если Сторона-1 – плательщик НДС в период действия Договора меняет свой налоговый статус в отношении НДС, она обязана известить об этом Сторону-2 в течение 3 (трех) рабочих дней. При этом стоимость Договора подлежит пересчету на сумму обозначенного ранее НДС по п. 3.1. Если по какой-либо причине Сторона-1 не сможет выставить и предоставить счет-фактуру по НДС Стороне-2 по предоставлении прав доступа к технической поддержке, Стороны соглашаются с тем, что стоимость Договора подлежит пересчету на сумму обозначенного ранее НДС по п.3.1.
	2. При возникновении обстоятельств, указанных в п.3.3 Сторона-2 оплачивает сумму, указанную в 3.1., за вычетом суммы НДС в размере: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сом безакцептно, т.е. оплате подлежит сумма **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**.
	3. Если по любым причинам в дальнейшем счет-фактура Стороны-1 будет признан недействительным/утерянным/испорченным, Сторона-1 обязан известить об этом Сторону-2 и вернуть Стороне-2 сумму НДС по такому счету-фактуре в течение 10 рабочих дней.
	4. Оплата по настоящему договору осуществляется Стороной-2 в сомах путем перечисления денежных средств на расчетный счет Стороны-1, указанный в п.13 Договора.

**4. Порядок передачи прав**

**4.1.** Сторона-1 обязана передать Стороне-2 право доступа к ПО и технической поддержкой путем предоставления официального письма производителя (правообладателя исключительных прав ПО), о чем уведомляет Сторону-2 по эл. почтеInfSecurity@megacom.kg в течении 10 (десяти) рабочих дней с момента заключения договора. Срок действия прав доступа к технической поддержке определяется в Приложении 1 к Договору.

**4.2.** Не позднее истечения десяти рабочих дней, следующих за днем получения извещения, Сторона-2 осуществляет проверку полученных прав доступа к ПО и лицензионных ключей на соответствие Спецификации. При соответствии переданных прав Спецификации Сторона-2 подписывает Акт приема-передачи прав доступа к ПО и технической поддержке, и возвращает один экземпляр Акта Стороне-1. В случае если переданные права не соответствуют Приложению 1 к Договору, тогда Сторона-2 в этот же срок направляет мотивированный отказ от приемки или Стороны составляют Акт о выявленных несоответствиях, в котором Стороны согласовывают между собой срок устранения несоответствий, (но не более чем 10 рабочих дней) в течение которого Сторона-1 обязана устранить выявленные несоответствия. Установление срока устранения несоответствий не исключает наступления ответственности за нарушение Стороной-1 срока предоставления прав доступа к ПО и технической поддержке согласно пункту 6.2.

**4.3.** Факт передачи прав доступа к ПО, лицензиям и технической поддержке Стороной-2 подтверждается Актом приема-передачи прав доступа согласно Приложения 2 к Договору. С момента подписания Сторонами Акта обязанность Стороны-1 по передаче соответствующих прав считается исполненной.

**5. Гарантийное обеспечение исполнения договора**

**5.1.** Гарантийное обеспечение исполнения Договора Сторона-1 вносит в течение 5 банковских дней с момента заключения настоящего Договора в размере **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ сом**, составляющее **\_\_**% от общей суммы Договора. Гарантийное обеспечение исполнения Договора остается у Стороны-2 до подписания Акта приема-передачи прав доступа к ПО и технической поддержке.

**5.2.** В случае ненадлежащего исполнения или неисполнения Стороной-1 принятых на себя обязательств по настоящему Договору, Сторона-2 вправе, после направления требования об уплате неустойки Стороне-1 согласно условиям Договора, а именно п.6.5., в безакцептном порядке удержать из гарантийного обеспечения исполнения договора начисленную неустойку, а также убытки, которые могут наступить вследствие неполного/ненадлежащего исполнения или неисполнения Стороной-1 своих обязательств по настоящему Договору и/или в случае недостаточности суммы гарантийного обеспечения исполнения договора – удержать после направления требования об уплате неустойки, Стороне-1 согласно условиям Договора, а именно п.6.5., всю сумму гарантийного обеспечения исполнения договора и недостающую сумму из суммы оплаты.

**5.3.** Сторона-2 возвращает Стороне-1 сумму гарантийного обеспечения исполнения Договора в случае надлежащего исполнения Стороной-1 своих обязательств в течение 10 (десяти) рабочих дней с момента подписания Акта, подтверждающего предоставление права пользования ПО и технической поддержкой.

**5.4.** В целях обеспечения надлежащего исполнения договорных обязательств на период срока технической поддержки, Сторона-2 сохраняет у себя часть суммы ГОИД - в размере 10 % от суммы ГОИД, указанной в п. 5.1. Договора.

* 1. Оставшаяся сумма гарантийного обеспечения исполнения договора, после удержания из ГОИД неустоек согласно п. 6.3 Договора и сохранения части ГОИД согласно п. 5.4. Договора, возвращается Стороне-1 в течение 10-ти (десять) банковских дней со дня подписания Акта приема – передачи оказанных услуг.
	2. После выполнения Стороной-1 договорных обязательств по договору, Сторона-2 возвращает Стороне-1 оставшуюся сумму ГОИД, в течение десяти рабочих дней.
	3. В случае не внесения Стороной-1 ГОИД в срок, установленный в п. 5.1 Договора, Сторона-2 вправе расторгнуть Договор в порядке, предусмотренном в п. 10.1 Договора.

**6. Ответственность сторон**

**6.1.** За неисполнение или ненадлежащее исполнение обязательств по настоящему Договору стороны несут ответственность в соответствии с условиями настоящего Договора, а в случаях, не предусмотренных Договором, в соответствии с действующим законодательством Кыргызской Республики.

**6.2**. В случае нарушения Стороной-1 срока предоставления прав доступа к ПО и технической поддержке, указанного в п. 4.1. Договора, а также нарушения Стороной-1 сроков устранения несоответствий согласно п.4.2. Договора, Сторона-2 удерживает в безакцепном порядке из суммы, подлежащей оплате и/или из суммы гарантийного обеспечения исполнения договора неустойку в размере 0,1 (ноль целых одна десятая) % от суммы настоящего Договора за каждый день просрочки передачи прав, но не более 5 (пяти) % от общей стоимости Договора.

**6.3.** В случае если Сторона-1 передала Стороне-2 права не соответствующие Спецификации, Сторона-2 удерживает в безакцепном порядке из суммы, подлежащей оплате и/или из суммы гарантийного обеспечения исполнения договора неустойку в размере 0.1 (ноль целых одна десятая) % от стоимости Договора, за каждый день просрочки, с должной даты передачи прав до даты фактической передачи, но не более 5 (пяти) % от общей стоимости Договора.

**6.4.** В случае нарушения Стороной-2 сроков оплаты, указанных в п. 3.2. Договора, и при условии надлежащего исполнения Стороной-1 своих обязательств по Договору, Сторона-1 имеет право требовать от Стороны-2 уплаты неустойки в размере 0,1 % от суммы подлежащей оплате за каждый рабочий день просрочки, но не более 5 (пяти) % от общей стоимости Договора.

**6.5.** Требование об уплате неустойки, предусмотренной п.6.4 Договора должно быть оформлено в письменном виде, подписано уполномоченным представителем. В случаях, установленных в п. 6.2, 6.3. Договора, Сторона-2 направляет Стороне-1 уведомление об удержании из суммы, подлежащей оплате или из суммы гарантийного обеспечения исполнения договора неустойки в письменном виде за подписью уполномоченного лица.

**6.6.** Уплата неустойки не освобождает Стороны от исполнения своих обязательств по настоящему Договору.

**7. Форс-мажор**

* 1. Стороны освобождаются от ответственности, за частичное или полное неисполнение обязательств по настоящему Договору, при условии соблюдения условий настоящего раздела Договора, если это неисполнение явилось следствием обстоятельств непреодолимой силы (форс-мажор), которые соответствующая Сторона не могла ни предвидеть, ни предотвратить разумными мерами при той степени добросовестности, осмотрительности и заботливости, какая от нее требовалась по характеру соответствующего обязательства.
	2. К обстоятельствам непреодолимой силы относятся следующие, но не ограничиваются ими: наводнение, пожар, землетрясение, взрыв, шторм, оседание почвы и иные явления природы, эпидемии, а также война или военные действия, массовые беспорядки, принятие органами государственной власти или управления решения, акта, повлекшего невозможность исполнения настоящего Договора, в т. ч. наложение ареста на имущество/расчетные счета Сторон.
	3. В случае, когда форс-мажорные обстоятельства преодолены, действие настоящего Договора продлевается на срок, равный по продолжительности периоду действия форс-мажорных обстоятельств.
	4. О наступлении форс-мажорных обстоятельств, а также о предполагаемом сроке их действия, Сторона, для которой такие обстоятельства наступили, извещает в письменной форме другую Сторону, по возможности немедленно, но не позднее 5 (пяти) рабочих дней с момента их наступления. При отсутствии возможности отправить извещение в письменной форме, извещение подлежит отправлению в электронном виде на следующие электронные адреса: InfSecurity@megacom.kg и [\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_](file:///%5C%5Cmegacom.local%5Croot%5C%D0%91%D0%B8%D1%88%D0%BA%D0%B5%D0%BA%5C%D0%94%D0%B5%D0%BF%D0%B0%D1%80%D1%82%D0%B0%D0%BC%D0%B5%D0%BD%D1%82%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85%20%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B9%5C%D0%9E%D1%82%D0%B4%D0%B5%D0%BB%D0%B0%20%D0%B7%D0%B0%D0%BA%D1%83%D0%BF%D0%BE%D0%BA%20%D0%B8%20%D1%83%D1%87%D0%B5%D1%82%D0%B0%20%D0%BE%D0%B1%D0%BE%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%20%D0%98%D0%A2%5C%D0%97%D0%B0%D0%BA%D1%83%D0%BF%D0%BA%D0%B8%5C2022%5C%D0%A2%D0%9E%5Ceostapyuk%40megacom.kg). Не извещение или несвоевременное извещение о наступлении таких обстоятельств лишает права ссылаться на форс-мажорные обстоятельства.
	5. Если форс-мажорные обстоятельства продолжаются более 3 (трех) месяцев подряд, любая из Сторон вправе расторгнуть настоящий Договор, уведомив другую Сторону об этом не менее чем за 10 (десять) рабочих дней до расторжения.
	6. Сторона, ссылающаяся на форс-мажорные обстоятельства, в течение 30 (тридцати) календарных дней с момента окончания обстоятельств непреодолимой силы, обязана предоставить для подтверждения их наступления и прекращения другой Стороне документ соответствующего компетентного органа (для КР – Торгово-промышленная палата). Разумность сроков в данном случае определяется порядком документооборота соответствующего компетентного органа.

**8. Разрешение споров**

* 1. Стороны договорились разрешать любые споры, возникающие в связи с исполнением настоящего Договора, путем переговоров.
	2. Все претензии Сторон должны быть оформлены в письменном виде и подписаны уполномоченными лицами.
	3. Сторона, получившая претензию, обязана предоставить другой Стороне мотивированный ответ в течение 10 (Десяти) рабочих дней со дня получения претензии.
	4. Если Сторонам не удается найти взаимоприемлемого решения, спор подлежит разрешению в судебном порядке в судах общей юрисдикции Кыргызской Республики в соответствии с действующим законодательством Кыргызской Республики.

**9. Конфиденциальность**

* 1. Стороны согласились, что условия настоящего Договора, факт его заключения, коммерческая, финансовая, технологическая, техническая информация (вне зависимости от способа предоставления) и иная информация,  относящаяся прямо или косвенно к одной из сторон, которая ее раскрывает (далее Передающая сторона), а также любая другая информация, ставшая известной Сторонам в ходе исполнения настоящего Договора является Конфиденциальной информацией и предназначена исключительно для пользования Сторонами в целях надлежащего исполнения настоящего Договора.
	2. Каждая из Сторон обязуется соблюдать конфиденциальность в отношении информации, полученной от другой Стороны (далее Получающая сторона) и не разглашать ее третьим лицам без получения письменного согласия Передающей стороны.
	3. Стороны обязуются в течение срока действия настоящего Договора и в течение 5 (пяти) лет после его прекращения хранить в тайне Конфиденциальную информацию.
	4. Требования п. 9.1. Договора не распространяются на информацию, которая:

- на момент разглашения являлась общеизвестной/общедоступной информации во время ее получения;

- была получена в любое время из другого источника без каких-либо ограничений относительно ее распространения или использования;

- была известна Получающей стороне или находилась в ее распоряжении до ее получения;

- подлежит разглашению в соответствии с требованием и/или предписанием соответствующего государственного органа на основании законодательства КР.

**10. Расторжение договора**

**10.1.** Сторона-2 имеет право отказаться от исполнения настоящего Договора полностью или частично в одностороннем порядке с предварительным уведомлением Стороны-1 за 10 (десять) календарных дней до предполагаемой даты расторжения.

**11. Гарантии Сторон**

**11.1.** Каждая из Сторон, заключая настоящий Договор, подтверждает и гарантирует, что:

**11.1.1.** Является действующей по законодательству Кыргызской Республики, должным образом зарегистрированной и поставленной на учет во все компетентные государственные органы Кыргызской Республики;

**11.1.2.** Лицо, заключающее настоящий Договор от ее имени, обладает всеми необходимыми полномочиями на его заключение на момент подписания настоящего Договора;

**11.1.3.** Предоставленная друг другу информация является достоверной и сообщена в объеме, необходимом для надлежащего исполнения условий настоящего Договора, без каких-либо изъятий, искажений и неточностей;

**11.1.4.** Не имеет ограничений и запретов, препятствующих, ограничивающих и/или делающих невозможным заключить настоящий Договор;

**11.2.** Каждая Сторона самостоятельно несет ответственность за нарушение п. 11.1 настоящего Договора, а также за последствия, наступившие ввиду такого нарушения.

**11.3.** Каждая Сторона самостоятельно несет ответственность за своевременное оформление и продление сроков действия всех необходимых разрешений/лицензий и иных документов, необходимых для осуществления деятельности, предусмотренной настоящим Договором.

**12. Заключительные положения**

**12.1.** Настоящий Договор вступает в силу с момента его подписания обеими Сторонами и действует до полного исполнения Сторонами своих обязательств по нему.

**12.2.** Изменения и дополнения к настоящему договору действительны только в том случае, если составлены в письменной форме и подписаны обеими сторонами.

**12.3**. Настоящий Договор составлен в двух экземплярах, по одному экземпляру для каждой стороны, которые имеют одинаковую юридическую силу.

**12.4.** Договор, приложения и дополнительные соглашения к нему, а также документы, составленные во исполнение настоящего Договора, могут быть подписаны с использованием факсимильного воспроизведения подписи либо иного аналога собственноручной подписи.

**12.5.** Все уведомления, запросы, требования или любая другая корреспонденция по настоящему Договору выполняются в письменной форме на русском языке и доставляются курьером или предоплаченным заказным почтовым отправлением, а в случаях, когда корреспонденция предусмотрена настоящим Договором посредствам электронной почты, такая корреспонденция направляется по следующим адресам:

 **А. Электронный адрес от Стороны-1:**

 *-* ***\_\_\_\_\_\_\_\_\_\_\_\_\_****; Tел.: \_\_\_\_\_\_\_\_\_\_\_\_\_; Эл. почта:*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*;*

 **Б. Электронный адрес от Стороны-2:**

 ***- ОИТБ*** ***InfSecurity@megacom.kg***

**12.6.** Ни одна из сторон не может передавать свои права и обязательства по Договору третьим лицам без письменного согласия другой стороны.

**12.7.** Во всем остальном, что не предусмотрено настоящим Договором, стороны руководствуются действующим законодательством Кыргызской Республики

**13. Юридические адреса и реквизиты сторон:**

|  |  |
| --- | --- |
| **Сторона-1** | **Сторона-2** |
|  |  **ЗАО "Альфа Телеком"** г. Бишкек, ул. Суюмбаева, 123. Р\С: 1091820182530113 Бишкекский центральный филиал  ОАО "Оптима Банк",  БИК: 109018 SWIFT: ENEJKG22 **Для перечисления ГОИД:** ОАО «Айыл Банк»,  г. Бишкек, Кыргызская Республика ЗАО "Альфа Телеком", Счет № 1350100027537623  БИК: 135001 |
| **Директор****/\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** М.П. | **Генеральный директор****/Куренкеев А. С./\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  М.П. |

**Приложение №1**

**к Договору о поставке ПО № \_\_\_\_\_**

**от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2023г.**

**Спецификация**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Подробное описание** | **Срок действия прав доступа к технической поддержке** | **Кол-во лицензий** | **Стоимость (без учета НДС), Сом КР** | **НДС 12%,** **Сом КР** | **Итого стоимость с учетом налогов, Сом КР** |
| 1 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |  |  |  |
|  | **Итого, общая сумма составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сомов, в том числе сумма НДС 12% составляет **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** сом. |

|  |  |
| --- | --- |
| **Сторона-1:****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Директор \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.П. | **Сторона-2:****ЗАО "Альфа Телеком"**Генеральный директорКуренкеев А. С. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.П. |

**Приложение №2**

**к Договору о поставке ПО № \_\_\_\_\_\_\_**

**от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2023 г.**

**г. Бишкек**

**Акт**

**приема-передачи прав доступа к технической поддержке**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** в дальнейшем именуемое «**Сторона-1**», в лице директора**\_\_\_\_\_\_\_\_\_**, действующего на основании Устава, с одной стороны, и

и ЗАО **«Альфа Телеком»**, именуемое в дальнейшем Сторона-2, в лице Генерального директора Куренкеев А. С., действующего на основании Устава, с другой стороны, вместе именуемые — Стороны, а каждое по отдельности — Сторона, составили настоящий Акт приема-передачи о нижеследующем:

1. Сторона-1 предоставила Стороне-2 право доступа к программному обеспечению, лицензиям и технической поддержке следующего программного обеспечения:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование услуг** | **Подробное описание**  | **Срок действия прав доступа к технической поддержке** | **Кол-во, лицензий** | **Стоимость (без учета НДС), Сом КР** | **НДС, Сом КР** | **Итого, с учетом налогов (Сом КР)** |
|  |
|  |  |  |  |  |  |  |  |
|  | **ИТОГО:** |  |

 **2.** Стороны претензий друг к другу не имеют.

|  |  |
| --- | --- |
| **Сторона-1:****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Директор \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.П. | **Сторона-2:****ЗАО "Альфа Телеком"**Генеральный директорКуренкеев А. С. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.П. |

 **Форма согласована:**

|  |  |
| --- | --- |
| **Сторона-1:****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Директор \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.П. | **Сторона-2:****ЗАО "Альфа Телеком"**Генеральный директорКуренкеев А. С. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.П. |