Приложение № 1 к приглашению на закупку.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на продление лицензии SIEM MaxPatrol 10

1. Общие положения

Техническое задание определяет минимальные функциональные, технические и эксплуатационные требования к лицензии программного продукта **SIEM MaxPatrol 10**, приобретаемой для нужд **ОАО «Керемет Банк»**.

Закупка осуществляется в целях обеспечения непрерывного функционирования системы централизованного мониторинга событий информационной безопасности Банка, централизованного сбора, обработки, корреляции и анализа событий информационной безопасности.

2. Цель закупки

Целью закупки является продление лицензии SIEM **MaxPatrol 10** для обеспечения:

1. централизованного сбора событий информационной безопасности.
2. обработки и нормализации поступающих событий.
3. корреляции событий информационной безопасности.
4. централизованного анализа событий.
5. выявления подозрительной и потенциально вредоносной активности.
6. мониторинга событий информационной безопасности.
7. проведения расследований инцидентов информационной безопасности.
8. обеспечения необходимого уровня контроля событий информационной безопасности Банка.
9. выполнения требований Национального банка Кыргызской Республики в части обеспечения мониторинга событий информационной безопасности.

3. Требования к приобретаемой лицензии

№	Наименование	Минимальные требования	Количество
1	**SIEM MaxPatrol 10**	Лицензия на программный продукт SIEM MaxPatrol 10 для централизованного сбора, обработки, корреляции и анализа событий информационной безопасности	**1 лицензия**

3.1. Лицензионные требования	Приобретаемая лицензия должна обеспечивать: 1. Количество контролируемых активов — не менее 650 активов. 2. Производительность обработки событий — не менее 2 250 EPS (Events Per Second). 3. Срок действия лицензии — 1 (один) год. 4. Возможность централизованного сбора событий информационной

	безопасности от подключенных источников. 5. Возможность обработки и анализа поступающих событий. 6. Возможность корреляции событий информационной безопасности. 7. Возможность выявления подозрительной активности и потенциальных инцидентов информационной безопасности. 8. Возможность централизованного мониторинга событий информационной безопасности. 9. Возможность хранения и последующего анализа собранных событий в пределах возможностей лицензируемой платформы.
4. Функциональные требования	**4.1. Сбора событий** 1. централизованного получения событий информационной безопасности. 2. подключения различных источников событий. 3. приема событий от серверного оборудования. 4. приема событий от сетевого оборудования. 5. приема событий от средств защиты информации. 6. приема событий от иных информационных систем Банка при наличии соответствующих интеграционных возможностей. **4.2. Обработки событий** Система должна обеспечивать: 1. прием и обработку поступающих событий. 2. нормализацию событий. 3. классификацию событий. 4. фильтрацию событий. 5. поиск и анализ событий. 6. централизованное представление информации о событиях информационной безопасности. **4.3. Корреляции событий** Система должна обеспечивать возможность:

	1. выявления взаимосвязанных событий. 2. определения подозрительных последовательностей событий. 3. формирования корреляционных правил. 4. выявления потенциальных инцидентов информационной безопасности. 5. автоматизированного анализа совокупности событий из различных источников. **4.4. Мониторинга и расследования** Система должна обеспечивать: 1. централизованный мониторинг событий информационной безопасности. 2. поиск событий по заданным параметрам. 3. анализ исторических событий. 4. получение информации о выявленных событиях и инцидентах. 5. использование результатов анализа при расследовании инцидентов информационной безопасности.
5. Требования по информационной безопасности	Приобретаемая лицензия и предоставляемое программное обеспечение должны обеспечивать возможность эксплуатации SIEM в соответствии с требованиями информационной безопасности Банка. Должна обеспечиваться возможность: 1. Разграничения прав доступа пользователей к функциям системы. 2. Аутентификации пользователей. 3. Разделения административных и пользовательских полномочий. 4. Регистрации действий пользователей и администраторов. 5. Контроля доступа к информации о событиях информационной безопасности. 6. Защищенного взаимодействия между компонентами системы в соответствии с поддерживаемыми механизмами защиты.

	7. Ведения журналов действий пользователей и администраторов. Контроля событий, связанных с функционированием самой системы SIEM.
6. Требования к поставщику	Поставщик обязан: 1. Предоставить действующую лицензию на программный продукт **SIEM MaxPatrol 10**. 2. Обеспечить срок действия лицензии **1 (один) год**. 3. Обеспечить лицензионный лимит **не менее 650 контролируемых активов**. 4. Обеспечить производительность лицензии **не менее 2 250 EPS**. 5. Предоставить документы, подтверждающие право использования программного продукта. 6. Обеспечить официальное происхождение лицензии. 7. Обеспечить техническую поддержку программного продукта в течение срока действия лицензии в соответствии с условиями производителя. 8. Предоставить документацию, необходимую для использования и администрирования программного продукта. 9. При необходимости обеспечить консультационную поддержку по вопросам лицензирования и эксплуатации программного продукта. Обеспечить продление лицензии без потери ранее накопленных данных, настроек и конфигураций системы.
7. Требования к технической поддержке	В течение срока действия лицензии Поставщик должен обеспечить возможность получения технической поддержки по вопросам: 1. функционирования программного продукта. 2. Лицензирования. 3. обновления программного обеспечения. 4. устранения выявленных ошибок. 5. восстановления работоспособности программного продукта.

	6. настройки и использования функциональных возможностей системы. Техническая поддержка должна предоставляться в соответствии с условиями производителя программного продукта.
8. Требования к коммерческому предложению	В коммерческом предложении необходимо указать: 1. Наименование программного продукта. 2. Производителя программного продукта. 3. Тип и состав предоставляемой лицензии. 4. Количество лицензируемых активов. 5. Максимальный объем обработки событий в EPS. 6. Срок действия лицензии. 7. Стоимость лицензии. 8. Стоимость технической поддержки, если она не включена в стоимость лицензии. 9. Условия предоставления лицензии. 10. Условия продления лицензии. 11. Срок предоставления лицензии после заключения договора. 12. Условия предоставления обновлений программного продукта. 13. Условия технической поддержки.
9. Срок и условия предоставления лицензии	1. Лицензия должна быть предоставлена Заказчику в электронном виде либо иным способом, предусмотренным производителем программного продукта. 2. Срок действия лицензии — **1 (один) год**. 3. Поставщик должен обеспечить своевременную активацию продленной лицензии до окончания срока действия текущей лицензии. 4. Предоставление лицензии не должно приводить к прекращению функционирования действующей системы SIEM. 5. Все необходимые действия по продлению лицензии должны быть выполнены Поставщиком в согласованные с Банком сроки.

10. Заключительные положения	1. Все расходы, связанные с предоставлением лицензии и предусмотренной технической поддержкой, должны быть включены в стоимость коммерческого предложения. 2. Все характеристики предлагаемой лицензии должны быть подтверждены официальной документацией производителя. 3. Поставщик несет ответственность за достоверность представленной информации о лицензионных возможностях предлагаемого программного продукта. 4. При выявлении несоответствия фактических лицензионных возможностей заявленным в коммерческом предложении Поставщик обязан устранить такое несоответствие в соответствии с условиями договора.

Начальник Отдела
информационной безопасности Багданов О.Б.