Конкурстық құжаттама жобасын алдын ала талқылау хаттамасы
№17115523

Конкурстың № 16436681-1
Конкурстың атауы SIEM ақпараттық қауіпсіздік инциденттерін басқарудың бағдарламалық-аппараттық кешені
Конкурстық құжаттама жобасына ескертулерді, сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салуларды қабылдау мерзімі бастап 2026-02-25 17:12:47 дейін 2026-02-27 17:12:47
Ұйымдастырушының атауы "Электрондық қаржы орталығы" акционерлік қоғамы

Конкурстық құжаттама жобасына ескерту(лер), сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салу(лар) мынадай шешім(дер) қабылданған өнім беруші(лер)ге жіберілген:

№	Әлеуетті өнім берушінің БСН (БСН)/ БСН/УНП	Өтініш түрпаты (түсіндіру туралы ескерту, сұрау салу)	Түсіндіру туралы ескертуді, сұрау салуды жіберу күні мен уақыты	Өтініш мәтіні (ескерту, түсіндіру туралы сұрау)	Шешім қабылданды	Ауытқу себебі, түсіндіру мәтіні

1	220140000464	КҚ жобасына ескерту	Согласно подпункта 7 раздела «Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара» Технической спецификации закупаемых товаров Приложения 13 к конкурсной документации «Система должна представлять собой единую платформу мониторинга и реагирования на инциденты информационной безопасности, включающую встроенные механизмы корреляции событий (SIEM) и защиты конечных точек, управляемые из единой консоли. События и теле-метрия конечных точек должны использоваться непосредственно в корреляционных правилах системы без применения промежуточных интеграционных шлюзов, коннекторов, syslog-преобразователей, APIадаптеров или сторонних программных продуктов». Данное требование намеренно значительно сужает круг потенциальных программных решений и потенциальных поставщиков, которые могу участвовать в данном конкурсе/закупке.	2026-02-27 16:50:22	Отклонить замечания	АО «Центр электронных финансов» (далее-Заказчик), рассмотрев поступившее замечание к подпункту 7 раздела «Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара» Технической спецификации, сообщает следующее. Требование о том, что система должна представлять собой единую платформу мониторинга и реагирования на инциденты информационной безопасности, включающую встроенные механизмы корреляции событий (SIEM) и защиты конечных точек, управляемые из единой консоли, установлено исходя из архитектурных и эксплуатационных потребностей Заказчика. Указанное требование направлено на обеспечение: • сквозной нативной корреляции событий и телеметрии конечных точек без задержек передачи данных; • исключения потери или искажения событий при трансформации форматов; • минимизации времени выявления и реагирования на инциденты информационной безопасности (MTTD/MTTR); • сокращения количества точек отказа в инфраструктуре мониторинга; • упрощения администрирования и аудита действий операторов; • снижения совокупной стоимости владения (TCO). Отдельно отмечаем, что использование промежуточных интеграционных шлюзов, коннекторов, syslog-преобразователей, API-адаптеров либо сторонних программных продуктов формирует дополнительный инфраструктурный слой, который: • требует развертывания дополнительного серверного компонента либо виртуальных ресурсов; • влечёт дополнительные затраты на лицензирование, внедрение, сопровождение и резервирование; • увеличивает поверхность потенциальной атаки; • создает дополнительную точку отказа; • усложняет расследование инцидентов и проведение аудита; • может приводить к задержкам передачи телеметрии либо частичной утрате контекста событий. В условиях эксплуатации критически значимой информационной инфраструктуры Заказчика подобная фрагментация архитектуры и зависимость от промежуточных компонентов увеличивает операционные и информационные риски. Дополнительно сообщаем, что на рынке информационной безопасности (по состоянию на 2026 год) представлены платформенные решения нескольких производителей, в которых механизмы SIEM и защиты конечных точек являются модулями единой архитектуры и используют общую базу телеметрии и единые корреляционные механизмы без применения сторонних интеграционных продуктов. Таким образом, требование Технической спецификации является технически реализуемым и соответствует существующей рыночной практике. Техническая спецификация не содержит указания на конкретного производителя, товарный знак, модель или страну происхождения, а формулирует функциональные и архитектурные требования, обусловленные задачами обеспечения информационной безопасности и оптимизации эксплуатации. Учитывая изложенное, требование о единой платформе со встроенными механизмами корреляции и защиты конечных точек без применения промежуточных интеграционных компонентов носит объективно обоснованный характер, направлено на снижение рисков и затрат эксплуатации и не имеет целью ограничение конкуренции. Оснований для внесения изменений в указанный подпункт Технической спецификации не имеется.

2	220140000464	КҚ жобасына ескерту	Требование ТС о единой консоли для двух разных Систем - ограничивает поставщиков. В целом Система централизованного сбора, хранения, корреляции и анализа журналов событий информационной безопасности, сетевой активности и активности конечных точек (SIEM) и Система защиты конечных точек являются разными по классу системами ИБ и не обязательно могут и должны быть управляемыми из единой консоли. Это подтверждается пунктом 54 единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Правительством Республики Казахстан, в котором четко разделяется средства и системы, используемые в опытной и промышленной эксплуатации. Также отмечаем, что по тексту Технической спецификации неоднократно упоминается что речь в закупке идет о двух разных Системах. Если Заказчик планирует в рамках одной закупки приобретение двух разных Систем ИБ -хорошо, но нельзя требовать, чтобы у этих Систем была единая консоль управления, иначе это ведет к сужению участников закупок. Просим внести изменения в этот подпункт раздела и открыть возможность участия в этом конкурсе/закупке большему числу потенциальных поставщиков с различными продуктами/решениями.	2026-02-27 17:01:36	Отклонить замечания	АО «Центр электронных финансов» (далее-Заказчик), рассмотрев поступившее замечание к Технической спецификации касательно требования о наличии единой консоли управления, сообщает следующее. Требование о наличии единой консоли управления для системы централизованного сбора, хранения, корреляции и анализа журналов событий информационной безопасности (SIEM) и системы защиты конечных точек установлено Заказчиком исходя из архитектурных, эксплуатационных и организационных потребностей обеспечения информационной безопасности, а также необходимости повышения эффективности процессов мониторинга и реагирования на инциденты. Под единой консолью управления понимается наличие технологической возможности централизованного администрирования, мониторинга, управления политиками безопасности, корреляции событий и реагирования на инциденты через единый интерфейс либо интегрированную платформу управления. При этом Техническая спецификация не устанавливает требование о принадлежности решений к одному производителю. Реализация может быть обеспечена как нативной интеграцией, так и посредством управляющей платформы либо штатных механизмов интеграции. Дополнительно сообщаем, что на рынке информационной безопасности представлены решения нескольких производителей, предусматривающие наличие единой консоли управления для системы класса SIEM и системы защиты конечных точек либо их интеграцию в рамках единой управляющей платформы. Подобная архитектура является распространённой практикой при построении современных систем мониторинга и реагирования (ОЦИБ). Также обращаем внимание, что в случае отсутствия единой консоли управления Заказчику потребуется развертывание дополнительного серверного компонента (интеграционного либо управляющего сервера) для обеспечения взаимодействия и централизованного администрирования указанных систем. Это повлечёт дополнительные затраты на: • приобретение серверного оборудования либо вычислительных ресурсов виртуализации; • лицензирование программного обеспечения; • внедрение и настройку интеграции; • администрирование и сопровождение дополнительного компонента; • обеспечение резервирования и информационной безопасности данного узла. Таким образом, требование направлено на достижение оптимальной, экономически эффективной и эксплуатационно удобной архитектуры системы информационной безопасности. Ссылка на пункт 54 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденный постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832, не содержит запрета на установление Заказчиком архитектурных требований, направленных на обеспечение централизованного управления средствами информационной безопасности. Учитывая изложенное, требование: - соответствует текущим возможностям рынка и предложениям нескольких производителей и интеграторов; - поддерживается реальными продуктами, допущенными к использованию в РК; - носит обоснованный и недискриминационный характер; - направлено на достижение наилучшего соотношения цена /качество/ эксплуатационные характеристики. Оснований для внесения изменений в соответствующий подпункт Технической спецификации не имеется.

Осы конкурсқа қатысуға өтінімдер осы хаттама және бекітілген конкурстық құжаттаманың мәтіні мемлекеттік сатып алу веб-порталында орналастырылған сәттен бастап бес жұмыс күнінен кешіктірілмей қабылданады.

Председатель Правления Крамшеев Дияс Казбекович

Аббревиатураларды таратып жазу:
БСН – бизнес-сәйкестендіру нөмірі;
ЖСН – жеке сәйкестендіру нөмірі;
ССН – салық төлеушінің сәйкестендіру нөмірі;
ТЕН – төлеушіні есепке алу нөмірі;
Т.А.Ә. – тегі аты әкесінің аты (ол бар болса).

Протокол предварительного обсуждения проекта конкурсной документации №17115523

№ конкурса 16436681-1
Название конкурса Программно-аппаратный комплекс управления инцидентами информационной безопасности SIEM
Срок приема замечаний к проекту конкурсной документации, а также запросов о разъяснении положений конкурсной документации с 2026-02-25 17:12:47 по 2026-02-27 17:12:47
Наименование организатора Акционерное общество "Центр электронных финансов"

Замечание (я) к проекту конкурсной документации, а также запрос(ы) о разъяснении положений конкурсной документации направлены следующим(и) потенциальным поставщиком (ами), по которому (ым) принято(ы) следующее (ие) решение(я):

№	БИН (ИИН)/ ИНН/УНП потенциального поставщика	Тип обращения (замечание, запрос о разъяснении)	Текст обращения	Дата и время направления замечания, запроса о разъяснении	Принято решение	Причина отклонения, текст разъяснения

1	220140000464	Замечание к КД	Согласно подпункта 7 раздела «Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара» Технической спецификации закупаемых товаров Приложения 13 к конкурсной документации «Система должна представлять собой единую платформу мониторинга и реагирования на инциденты информационной безопасности, включающую встроенные механизмы корреляции событий (SIEM) и защиты конечных точек, управляемые из единой консоли. События и теле-метрия конечных точек должны использоваться непосредственно в корреляционных правилах системы без применения промежуточных интеграционных шлюзов, коннекторов, syslog-преобразователей, APIадаптеров или сторонних программных продуктов». Данное требование намеренно значительно сужает круг потенциальных программных решений и потенциальных поставщиков, которые могу участвовать в данном конкурсе/закупке.	2026-02-27 16:50:22	Отклонить замечания	АО «Центр электронных финансов» (далее-Заказчик), рассмотрев поступившее замечание к подпункту 7 раздела «Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара» Технической спецификации, сообщает следующее. Требование о том, что система должна представлять собой единую платформу мониторинга и реагирования на инциденты информационной безопасности, включающую встроенные механизмы корреляции событий (SIEM) и защиты конечных точек, управляемые из единой консоли, установлено исходя из архитектурных и эксплуатационных потребностей Заказчика. Указанное требование направлено на обеспечение: • сквозной нативной корреляции событий и телеметрии конечных точек без задержек передачи данных; • исключения потери или искажения событий при трансформации форматов; • минимизации времени выявления и реагирования на инциденты информационной безопасности (MTTD/MTTR); • сокращения количества точек отказа в инфраструктуре мониторинга; • упрощения администрирования и аудита действий операторов; • снижения совокупной стоимости владения (TCO). Отдельно отмечаем, что использование промежуточных интеграционных шлюзов, коннекторов, syslog-преобразователей, API-адаптеров либо сторонних программных продуктов формирует дополнительный инфраструктурный слой, который: • требует развертывания дополнительного серверного компонента либо виртуальных ресурсов; • влечёт дополнительные затраты на лицензирование, внедрение, сопровождение и резервирование; • увеличивает поверхность потенциальной атаки; • создает дополнительную точку отказа; • усложняет расследование инцидентов и проведение аудита; • может приводить к задержкам передачи телеметрии либо частичной утрате контекста событий. В условиях эксплуатации критически значимой информационной инфраструктуры Заказчика подобная фрагментация архитектуры и зависимость от промежуточных компонентов увеличивает операционные и информационные риски. Дополнительно сообщаем, что на рынке информационной безопасности (по состоянию на 2026 год) представлены платформенные решения нескольких производителей, в которых механизмы SIEM и защиты конечных точек являются модулями единой архитектуры и используют общую базу телеметрии и единые корреляционные механизмы без применения сторонних интеграционных продуктов. Таким образом, требование Технической спецификации является технически реализуемым и соответствует существующей рыночной практике. Техническая спецификация не содержит указания на конкретного производителя, товарный знак, модель или страну происхождения, а формулирует функциональные и архитектурные требования, обусловленные задачами обеспечения информационной безопасности и оптимизации эксплуатации. Учитывая изложенное, требование о единой платформе со встроенными механизмами корреляции и защиты конечных точек без применения промежуточных интеграционных компонентов носит объективно обоснованный характер, направлено на снижение рисков и затрат эксплуатации и не имеет целью ограничение конкуренции. Оснований для внесения изменений в указанный подпункт Технической спецификации не имеется.

2	220140000464	Замечание к КД	Требование ТС о единой консоли для двух разных Систем - ограничивает поставщиков. В целом Система централизованного сбора, хранения, корреляции и анализа журналов событий информационной безопасности, сетевой активности и активности конечных точек (SIEM) и Система защиты конечных точек являются разными по классу системами ИБ и не обязательно могут и должны быть управляемыми из единой консоли. Это подтверждается пунктом 54 единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Правительством Республики Казахстан, в котором четко разделяется средства и системы, используемые в опытной и промышленной эксплуатации. Также отмечаем, что по тексту Технической спецификации неоднократно упоминается что речь в закупке идет о двух разных Системах. Если Заказчик планирует в рамках одной закупки приобретение двух разных Систем ИБ -хорошо, но нельзя требовать, чтобы у этих Систем была единая консоль управления, иначе это ведет к сужению участников закупок. Просим внести изменения в этот подпункт раздела и открыть возможность участия в этом конкурсе/закупке большему числу потенциальных поставщиков с различными продуктами/решениями.	2026-02-27 17:01:36	Отклонить замечания	АО «Центр электронных финансов» (далее-Заказчик), рассмотрев поступившее замечание к Технической спецификации касательно требования о наличии единой консоли управления, сообщает следующее. Требование о наличии единой консоли управления для системы централизованного сбора, хранения, корреляции и анализа журналов событий информационной безопасности (SIEM) и системы защиты конечных точек установлено Заказчиком исходя из архитектурных, эксплуатационных и организационных потребностей обеспечения информационной безопасности, а также необходимости повышения эффективности процессов мониторинга и реагирования на инциденты. Под единой консолью управления понимается наличие технологической возможности централизованного администрирования, мониторинга, управления политиками безопасности, корреляции событий и реагирования на инциденты через единый интерфейс либо интегрированную платформу управления. При этом Техническая спецификация не устанавливает требование о принадлежности решений к одному производителю. Реализация может быть обеспечена как нативной интеграцией, так и посредством управляющей платформы либо штатных механизмов интеграции. Дополнительно сообщаем, что на рынке информационной безопасности представлены решения нескольких производителей, предусматривающие наличие единой консоли управления для системы класса SIEM и системы защиты конечных точек либо их интеграцию в рамках единой управляющей платформы. Подобная архитектура является распространённой практикой при построении современных систем мониторинга и реагирования (ОЦИБ). Также обращаем внимание, что в случае отсутствия единой консоли управления Заказчику потребуется развертывание дополнительного серверного компонента (интеграционного либо управляющего сервера) для обеспечения взаимодействия и централизованного администрирования указанных систем. Это повлечёт дополнительные затраты на: • приобретение серверного оборудования либо вычислительных ресурсов виртуализации; • лицензирование программного обеспечения; • внедрение и настройку интеграции; • администрирование и сопровождение дополнительного компонента; • обеспечение резервирования и информационной безопасности данного узла. Таким образом, требование направлено на достижение оптимальной, экономически эффективной и эксплуатационно удобной архитектуры системы информационной безопасности. Ссылка на пункт 54 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденный постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832, не содержит запрета на установление Заказчиком архитектурных требований, направленных на обеспечение централизованного управления средствами информационной безопасности. Учитывая изложенное, требование: - соответствует текущим возможностям рынка и предложениям нескольких производителей и интеграторов; - поддерживается реальными продуктами, допущенными к использованию в РК; - носит обоснованный и недискриминационный характер; - направлено на достижение наилучшего соотношения цена /качество/ эксплуатационные характеристики. Оснований для внесения изменений в соответствующий подпункт Технической спецификации не имеется.

Заявки на участие в данном конкурсе принимаются не позднее пяти рабочих дней с момента размещения данного протокола и текста утвержденной конкурсной документации на веб-портале государственных закупок

Председатель Правления Крамшеев Дияс Казбекович

Расшифровка аббревиатур:
БИН – бизнес-идентификационный номер;
ИИН – индивидуальный идентификационный номер;
ИНН – идентификационный номер налогоплательщика;
УНП – учетный номер плательщика;
Ф.И.О. – фамилия имя отчество (при его наличии).