автономная некоммерческая организация
«Аналитический центр при Правительстве Российской Федерации»

УТВЕРЖДАЮ:
Руководитель
автономной некоммерческой организации
«Аналитический центр при
Правительстве Российской Федерации»

_____ К.М. Калинин

16 декабря 2020 г

ДОКУМЕНТАЦИЯ

о запросе цен в электронной форме на предоставление неисключительных прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

г. Москва, 2020 г.

Автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации» приглашает юридических и физических лиц, в том числе индивидуальных предпринимателей, которые соответствуют требованиям, установленным настоящей Документацией, принять участие в запросе цен в электронной форме (далее – запрос цен) на предоставление неисключительных прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

1. Законодательное регулирование

Настоящая Документация подготовлена на основе Гражданского кодекса Российской Федерации и Положения о закупочной деятельности автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации» (далее – Положение), утвержденного решением наблюдательного совета автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации» (протокол № 1 от 24 марта 2015 года, с изменениями, утвержденными протоколом № 7 от 20 июня 2017 года). В части, прямо не урегулированной законодательством Российской Федерации, проведение запроса цен регулируется настоящей Документацией и Положением.

2. Основные термины

Документация – комплект документов, содержащий всю необходимую информацию о предмете запроса цен, условиях исполнения договора, требованиях к Участникам, а также об условиях проведения запроса цен.

Заказчик – автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации» (Аналитический центр при Правительстве Российской Федерации).

Запрос цен – непродолжительная (до 7 календарных дней) процедура формального запроса технико-коммерческих предложений с выбором лучшего предложения по лучшей цене и без обязанности Заказчика заключить договор по результатам такой закупочной процедуры.

Заявка – комплект документов Участника, подтверждающих правоспособность и квалификацию Участника и содержащих предложение об условиях исполнения договора на поставку Продукции, являющейся предметом запроса цен.

Комиссия по закупкам, Комиссия – коллегиальный орган, создаваемый Заказчиком для выбора Поставщика путем проведения закупочных процедур с целью заключения договора.

Лот – часть закупаемой продукции, на которую в соответствии с извещением и Документацией допускается подача отдельной Заявки и заключение отдельного договора по итогам запроса цен.

Начальная (максимальная) цена договора – предельная цена Продукции, являющейся предметом запроса цен, рассчитанная Заказчиком в установленном порядке или определенная Заказчиком по результатам изучения конъюнктуры рынка.

Продукция, Предмет закупки – товары, работы или услуги, приобретаемые для нужд Заказчика.

Размещение закупки – публикация на электронной торговой площадке и сайте Заказчика информации о проведении Заказчиком закупочной процедуры.

Сайт Заказчика – сайт в информационно-телекоммуникационной сети Интернет, где размещается информация о проведении открытых закупочных процедур на приобретение Продукции для нужд Заказчика (http://ac.gov.ru).

Участник – участник запроса цен – потенциальный Поставщик, претендующий на поставку Продукции для нужд Заказчика.

Электронная площадка – электронная торговая площадка OTC-tender (www.otc-tender.ru).

3. Общие сведения о процедуре запроса цен

Запрос цен проводится в соответствии с законодательством Российской Федерации, но не является разновидностью торгов и не подпадает под регулирование статьями 447-449 части первой Гражданского кодекса Российской Федерации. Запрос цен также не является публичным конкурсом

и не регулируется статьями 1057-1061 части второй Гражданского кодекса Российской Федерации. Таким образом, данная процедура не накладывает на Заказчика соответствующего объема гражданско-правовых обязательств.

Участники самостоятельно несут все расходы, связанные с участием в запросе цен, подготовкой и подачей Заявок; Заказчик по этим расходам не отвечает и не имеет обязательств, независимо от хода и результатов данного запроса цен.

Заказчик вправе отклонить Заявку, если он установит, что Участник прямо или косвенно дал, согласился дать или предложил работнику Заказчика вознаграждение в любой форме: работу, услугу, какую-либо ценность в качестве стимула, который может повлиять на принятие Комиссией по закупкам решения по определению победителя.

Заказчик вправе отклонить Заявки Участников, заключивших между собой какое-либо соглашение с целью повлиять на определение победителя запроса цен.

3.1. Используемый способ закупки: запрос цен в электронной форме.

3.2. Наименование Заказчика: автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации».

Место нахождения: 107078, Москва, проспект Академика Сахарова, д. 12.

Почтовый адрес: 107078, Москва, проспект Академика Сахарова, д. 12.

Адрес электронной почты: torgi@ac.gov.ru.

Номер контактного телефона: +7 (916) 209 67 30.

Ответственное должностное лицо Заказчика: Чернявский Константин Александрович.

3.3. Предмет закупки: предоставление неисключительных прав на использование программ для ЭВМ (далее – неисключительные права или неисключительная лицензии)- Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» (далее – Продукт) для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

3.4. Место и сроки поставки Продукции:

Место поставки Продукции: г. Москва, проспект Академика Сахарова, дом 12.

Сроки поставки Продукции: Срок передачи Продукта: не позднее 25 декабря 2020г.

Период пользования Продукта: в соответствии со Спецификацией (Приложение № 1 к Документации).

4. Сведения о начальной (максимальной) цене договора:

9 024 000,00 (Девять миллионов двадцать четыре тысячи) рублей 00 копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

5. Форма, сроки и условия оплаты:

Оплата за предоставление неисключительных прав на использование Продукта осуществляется Заказчиком по факту предоставления неисключительных прав на использование Продукта в течение 10 (Десяти) рабочих дней с даты получения счета, выставленного на основании подписанного Сторонами акта передачи прав.

6. Порядок формирования цены договора:

Цена договора включает в себя все обязательные платежи и расходы, связанные с исполнением договора, в том числе стоимость передаваемых неисключительных прав, все уплачиваемые и взимаемые на территории Российской Федерации налоги, пошлины, сборы, страховые и другие обязательные платежи, стоимость дополнительных услуг, а также затраты по гарантийным обязательствам.

7. Порядок, место, время начала и окончания срока подачи Заявок

Запрос цен проводится на Электронной площадке (www.otc-tender.ru) в порядке, установленном регламентом данной Электронной площадки (www.otc-tender.ru) в соответствии с условиями и требованиями Документации.

Для участия в запросе цен Участник должен быть зарегистрированным на указанной Электронной площадке (www.otc-tender.ru), в том числе, получить аккредитацию участника Электронной площадки (www.otc-tender.ru) в соответствии с правилами, условиями и порядком регистрации, аккредитации, установленными данной Электронной площадкой (www.otc-tender.ru).

Заявка на участие в запросе цен подается Участником закупки в электронной форме.

Прием заявок осуществляется на Электронной площадке (www.otc-tender.ru).

Дата начала подачи Заявок: в день размещения документации на сайтах www.ac.gov.ru и www.otc-tender.ru.

Дата окончания срока подачи Заявок: 21 декабря 2020 года в 10:00 (мск).

Место подачи Заявок: Электронная площадка (www.otc-tender.ru)

8. Требования к участникам закупки и перечень документов, представляемых участниками закупки для подтверждения их соответствия установленным требованиям:

8.1. Участник должен соответствовать требованиям, предъявляемым в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставки Продукции, являющейся предметом Закупки, в том числе:

а) быть правомочным заключать договор;

б) обладать необходимыми лицензиями или свидетельствами для поставки Продукции, подлежащей лицензированию (регулированию) в соответствии с действующим законодательством Российской Федерации и являющейся предметом заключаемого договора;

в) обладать необходимыми сертификатами на Продукцию, являющуюся предметом заключаемого договора, в соответствии с действующим законодательством Российской Федерации;

г) не находиться в процессе ликвидации (для юридического лица) или банкротства;

д) не являться юридическим или физическим лицом, на имущество которого наложен арест по решению суда, административного органа и/или экономическая деятельность которого приостановлена;

е) не иметь за прошедший календарный год задолженности по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды, размер которой превышает двадцать пять процентов балансовой стоимости активов, определяемой по данным бухгалтерской отчетности за последний завершенный отчетный период;

ж) обладать профессиональной компетентностью, финансовыми и трудовыми (кадровыми) ресурсами, оборудованием и другими материальными возможностями, надежностью, опытом и репутацией, необходимыми для исполнения договора на поставку Продукции;

з) руководитель и главный бухгалтер юридического лица, являющегося Участником, не должны иметь непогашенной или неснятой судимости в сфере экономики;

и) Участник не должен быть включен в реестр недобросовестных поставщиков, предусмотренный Федеральным законом от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», а также в реестр недобросовестных поставщиков Аналитического центра при Правительстве Российской Федерации.

к) Участник закупки - юридическое лицо, которое в течение двух лет до момента подачи заявки на участие в закупке не было привлечено к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях.

8.2. Заявка на участие должна содержать:

а) фирменное наименование (наименование), сведения об организационно-правовой форме, о месте нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные, сведения о месте жительства (для физического лица), номер контактного телефона;

б) копии учредительных документов Участника (для юридических лиц);

в) копии документов о государственной регистрации юридического лица или физического лица в качестве индивидуального предпринимателя в соответствии с законодательством Российской Федерации; для физического лица - копии документов, удостоверяющих личность; надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица или государственной регистрации физического

лица в качестве индивидуального предпринимателя в соответствии с законодательством соответствующего государства (для иностранного лица);

г) копии свидетельства о постановке на учет в налоговом органе (для юридических и физических лиц), уведомления о постановке на учет в налоговом органе (для индивидуальных предпринимателей);

д) полученные не ранее чем за шесть месяцев до дня размещения на сайте Заказчика Извещения о проведении запроса цен:

- выписку или нотариально заверенную копию выписки из единого государственного реестра юридических лиц (для юридического лица);

- выписку или нотариально заверенную копию выписки из единого государственного реестра индивидуальных предпринимателей (для индивидуального предпринимателя);

е) копию документа, подтверждающего полномочия лица на осуществление действий от имени Участника - юридического лица (копия решения о назначении или об избрании, или приказа о назначении физического лица на должность, в соответствии с которым такое физическое лицо обладает правом действовать от имени Участника без доверенности (далее по тексту - руководитель). В случае, если от имени Участника действует иное лицо, Заявка на участие в запросе цен должна содержать также доверенность на осуществление действий от имени Участника, заверенную печатью Участника и подписанную руководителем Участника (для юридических лиц) или уполномоченным этим руководителем лицом, либо нотариально заверенную копию такой доверенности. В случае если указанная доверенность подписана лицом, уполномоченным руководителем Участника, Заявка на участие в запросе цен должна содержать также документ, подтверждающий полномочия такого лица;

ж) копию документа, удостоверяющего личность индивидуального предпринимателя или лица, действующего от имени юридического лица (индивидуального предпринимателя);

з) решение об одобрении или о совершении крупной сделки либо копию такого решения в случае, если для Участника поставка товаров, выполнение работ, оказание услуг, являющихся предметом договора, или внесение денежных средств в качестве обеспечения исполнения договора, обеспечения гарантийных обязательств являются крупной сделкой. В случае, если для данного Участника поставка товаров, выполнение работ, оказание услуг, являющиеся предметом договора, или внесение денежных средств в качестве обеспечения не являются крупной сделкой, Участник представляет соответствующее письмо;

и) копии документов, подтверждающих соответствие Участника требованиям, устанавливаемым в соответствии с законодательством Российской Федерации к лицам, осуществляющим выполнение работ, оказание услуг, поставку товара, являющихся предметом запроса цен (копии действующих лицензий по предмету запроса цен, допусков, членства в саморегулируемых общественных организациях, декларация о соответствии или иные документы);

к) копию уведомления о возможности применения Участником упрощенной системы налогообложения (для Участников, применяющих ее);

л) копии документов, подтверждающих обладание Участниками исключительными правами на объекты интеллектуальной собственности, если в связи с исполнением договора Заказчик приобретает исключительные права на объекты интеллектуальной собственности;

м) справка (или копия справки) налогового органа об исполнении Участником обязанности по уплате налогов, сборов, пеней и налоговых санкций и отсутствии задолженности;

н) оригиналы согласия на обработку персональных данных руководителя (лица осуществляющего действия от имени Участника), индивидуального предпринимателя или физического лица (Приложение № 3 к Документации)

о) Заявку (Приложение № 2 к Документации);

К Заявке в обязательном порядке должны быть приложены:

- предложение о функциональных характеристиках (потребительских свойствах) и качественных характеристиках. (Приложение № 1 к Заявке);

- копия, действующего на момент подачи заявки, договора, подтверждающего наличие соответствующих полномочий Участника от правообладателя прав на использование программ для

ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent».

- анкета Участника (Приложение № 2 к Заявке).

Все предоставленные документы должны быть в виде электронных документов в формате *.doc, *.docx или *.pdf и подписаны электронной подписью лица, имеющего право действовать от имени Участника.

9. Порядок предоставления документации о закупке: Документация доступна для ознакомления и скачивания на сайте Заказчика (www.ac.gov.ru) и сайте Электронной площадки (www.otc-tender.ru) без взимания платы.

10. Формы, порядок, дата начала и дата окончания срока предоставления Участникам Закупки разъяснений положений Документации, порядок внесения изменений:

10.1. Любой Участник вправе направить Заказчику запрос о разъяснении положений Документации:

а) через Электронную площадку (www.otc-tender.ru);

б) в письменной форме на почтовый адрес Заказчика, указанный в п. 3.2 Документации.

10.2. Датой начала срока предоставления разъяснений положений Документации является 1 (Первый) рабочий день с даты размещения Документации. Датой окончания срока предоставления разъяснений положений Документации является рабочий день, предшествующий дню окончания приема заявок на участие в закупке.

10.3. Заказчик после получения запроса от Участника в течение 3 (Трех) дней осуществляет подготовку разъяснений и размещает их на Электронной площадке. Разъяснение положений Документации не должно изменять Документацию.

Заказчик вправе не отвечать на запрос Участника, если он поступил позднее, чем за 3 (Три) рабочих дня до срока окончания подачи Заявок.

10.4. Заказчик по собственной инициативе или на основании запроса Участника вправе принять решение о внесении изменений в Документацию о проведении запроса цен и извещение о проведении закупки. В зависимости от характера изменений, внесенных в Документацию о проведении запроса цен, по решению Заказчика может быть продлен срок окончания подачи заявок.

10.5. Изменения, вносимые в извещение о закупке и в Документацию о проведении запроса цен в электронной форме, размещаются Заказчиком на сайте Заказчика (www.ac.gov.ru) и сайте Электронной площадки (www.otc-tender.ru)в течение 3 (Трех) дней со дня принятия решения о внесении изменений.

10.6. Участники, получившие Документацию о проведении запроса цен в электронной форме с сайта Заказчика (www.ac.gov.ru) или сайта Электронной площадки (www.otc-tender.ru), должны самостоятельно отслеживать изменения Извещения и Документации о проведении запроса цен в электронной форме. Заказчик не несет ответственности за несвоевременное получение Участниками информации с сайта Заказчика (www.ac.gov.ru) или сайта Электронной площадки (www.otc-tender.ru).».

11. Место, порядок, дата и время открытия доступа к Заявкам на участие в закупке:

Открытие доступа к Заявкам на участие в запросе цен осуществляется 21 декабря 2020 года в 10:00 (мск).

12. Критерии оценки и сопоставления Заявок на участие в Закупке.

Оценка заявок, поданных Участниками, производится по единственному критерию – «цена договора».

13. Порядок оценки и сопоставления Заявок

Комиссия по закупкам в срок, указанный в Документации, осуществляет оценку и сопоставление Заявок на участие в запросе цен, признанных соответствующими требованиям Документации.

Оценка заявок осуществляется в соответствии с критерием «цена договора».

Лучшей признается Заявка Участника, в которой предложена наименьшая цена договора.

В случае если Участник освобождается от исполнения обязанности налогоплательщика НДС, либо Участник не является налогоплательщиком НДС то цена, предложенная таким Участником в Заявке, не должна превышать установленную начальную (максимальную) цену без учета НДС.

При этом в указанном случае на стадии оценки и сопоставления Заявок для целей сравнения ценовые предложения всех Участников также учитываются без НДС.

14. Место и дата рассмотрения Заявок и подведения итогов закупки.

Рассмотрение Заявок и подведение итогов закупки осуществляются 21 декабря 2020 года по адресу: г. Москва, проспект Академика Сахарова, дом 12.

15. Условия допуска к участию в закупке:

15.1. Предложение участника закупки не должно превышать начальной (максимальной) цены договора, установленной Документацией.

15.2. Если Участником представлен не полный комплект документов или представленные документы оформлены с нарушением требований, установленных подпунктом 8.2. Документации и Приложением № 2 к Документации, то Комиссия по закупкам расценивает это как существенное несоответствие Заявки на участие в запросе цен требованиям, установленным Документацией, и данная Заявка не допускается к участию в запросе цен.

15.3. Результаты рассмотрения Заявок фиксируются в протоколе рассмотрения Заявок на участие в запросе цен. Протокол должен содержать сведения об участниках процедуры закупки, подавших Заявки на участие в запросе цен, решение о допуске участника процедуры закупки к участию в запросе цен и о признании его участником запроса цен или об отказе в допуске участнику процедуры закупки в участии в запросе цен с указанием положений Документации о проведении запроса цен, которым не соответствует Участник процедуры закупки или Заявка такого участника.

15.4. Протокол должен быть составлен и подписан членами Комиссии по закупкам не позднее 3 (Трех) дней с даты окончания рассмотрения Заявок, установленной Документацией о проведении запроса цен.

15.5. По решению Комиссии по закупкам вскрытие Заявок, рассмотрение Заявок Участников и принятие решения о допуске (отказе в допуске) Участников к участию в запросе цен может оформляться одним протоколом.

15.6. Протоколы, составленные в ходе проведения закупки, Заявки на участие в закупке, документация, изменения, внесенные в документацию, разъяснения положений документации подлежат хранению не менее трех лет.

16. Ограничение участия в определении поставщика: не предусмотрено.

17. Размер обеспечения исполнения договора: не установлен.

18. Сведения о предоставлении преференций: не установлены.

19. Содержание, форма, оформление и состав Заявки на участие в закупке:

Заявка на участие в запросе цен, оформленная согласно Приложению № 2 к Документации, подается Заказчику в электронной форме на сайте Электронной площадки (www.otc-tender.ru).

20. Преддоговорные переговоры.

20.1. Между Заказчиком и Участником, с которым заключается договор, могут проводиться преддоговорные переговоры (с оформлением протокола таких переговоров и его подписанием обеими сторонами), направленные на уточнение условий договора.

20.2. Допускается проводить преддоговорные переговоры по следующим вопросам:

а) по снижению цены договора и (если применимо) цен отдельных видов товаров, расценок на отдельные виды работ (услуг) без уменьшения количества товаров, объема работ, услуг;

б) по увеличению объемов Продукции без увеличения цен (расценок);

в) по сокращению сроков выполнения договора (его отдельных этапов) и (или) улучшению условий для Заказчика: отмена аванса, улучшение технических характеристик продукции и т.д.

г) по уточнению условий договора, которые не были зафиксированы в проекте договора, Документации и заявке Участника, с которым заключается договор.

20.3. Запрещаются преддоговорные переговоры, направленные на изменение условий заключаемого договора в пользу Участника, с которым заключается договор.

21. Заключение договора

21.1. Заказчик в течение 2 (Двух) рабочих дней со дня размещения протокола оценки и сопоставления Заявок (или протокола преддоговорных переговоров, если проводились) направляет победителю запроса цен проект договора, который составляется путем включения условий исполнения договора, предложенных победителем запроса цен в его Заявке, в проект договора, прилагаемый к Документации с учетом преддоговорных переговоров.

21.2. Договор по результатам запроса цен будет заключен на условиях предложения о цене договора победителя запроса цен: с учетом НДС – с победителем, являющимся налогоплательщиком НДС; без учета НДС – с победителем, применяющим упрощенную систему налогообложения.

21.3. Победитель должен подписать, заверить печатью, направленный ему Заказчиком договор, и представить Заказчику 2 (Два) экземпляра договора в течение 2 (Двух) рабочих дней с момента его получения.

21.4. В случае если победитель запроса цен не представил Заказчику подписанный договор в срок, установленный подпунктом 21.3 настоящей Документации, такой победитель признается уклонившимся от заключения договора.

22. Сведения о возможности Заказчика изменить объем Продукции, предусмотренный договором

22.1. Заказчик по согласованию с Участником, с которым заключен договор по результатам запроса цен, в ходе исполнения договора вправе изменить не более чем на 10 (Десять) процентов предусмотренный договором объем Продукции (товаров, работ, услуг) при изменении потребности Заказчика в Продукции, на приобретение которой заключен договор, или при выявлении потребности в дополнительном объеме Продукции, не предусмотренной договором, но связанных с Продукцией, предусмотренной договором. При этом Заказчик по согласованию с Участником, с которым заключен договор по результатам запроса цен, вправе изменить первоначальную цену договора пропорционально объему такой Продукции, но не более чем на 10 (Десять) процентов такой цены договора.

Приложение №1
к Документации
от «_____» _____ 2020 г.

СПЕЦИФИКАЦИЯ

на предоставление неисключительных прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

№ п/п	парт номер	Наименование Продукта	Кол-во (шт)	Срок использования.
1.	PT-MPSIEM-BASE-H1000	MaxPatrol SIEM, базовая лицензия на 1 000 узлов, гарантийные обязательства в течение 1 (одного) года	1	бессрочно
2.	PT-MPSIEM-SRV	MaxPatrol SIEM Server, гарантийные обязательства в течение 1 (одного) года	1	бессрочно
3.	PT-MPSIEM-AGT	MaxPatrol SIEM Agent, гарантийные обязательства в течение 1 (одного) года	1	бессрочно

ТРЕБОВАНИЯ К СИСТЕМЕ
Требования к Системе в целом

Функциональные компоненты программных средств Системы должны поддерживать развертывание как на физическом, так и на виртуальном оборудовании.

Система должна быть построена по модульному принципу и позволять ее использование и установку в различных конфигурациях.

В состав Системы должны входить следующие функциональные компоненты:

компонент управления;

компонент обработки;

компонент хранения;

компонент сбора событий;

компонент управления доступом;

база знаний с экспертизой вендора;

компонент обновления и конфигурирования;

компонент хранения индикаторов компрометации.

Таблица 1 — Требования к функциям компонентов Системы

№ п/п	Наименование компонента	Назначение компонента
1	Компонент управления	Компонент управления должен выполнять следующие функции: централизованное хранения конфигурации активов; централизованное управление компонентами системы; оперативное реагирование на инциденты ИБ и обеспечение взаимодействия подразделений организации при расследовании этих инцидентов; автоматизация процесса обнаружения уязвимостей; предоставление графического интерфейса пользователя
2	Компонент обработки	Компонент обработки должен осуществлять функции по обработке и хранению событий: агрегацию, нормализацию и корреляцию событий; автоматическое создание инцидентов; привязку событий к активам
3	Компонент хранения	Компонент хранения должен осуществлять централизованное хранение информации о событиях — как исходных, так и нормализованных
4	Компонент сбора событий	Компонент сбора событий должен обеспечивать сбор событий от различных источников и позволять осуществлять сканирование узлов корпоративной информационной системы (далее - КИС) в режимах черного и белого ящика
5	Компонент управления доступом	Компонент управления доступом должен обеспечивать доступ к системе через сервис единого входа, управление пользователями системы и журналирование действий пользователей
6	База знаний с экспертизой вендора	База знаний должна обеспечивать получение данных о новых уязвимостях и эксплойтах, данных, необходимых для структурирования сведений, собранных от объектов инфраструктуры, правил обработки событий
7	Компонент обновления и конфигурирования	Компонент обновления и конфигурирования должен обеспечивать проверку наличия, загрузку и установку новых версий отдельных компонентов Системы, а также обновление базы знаний
8	Компонент хранения индикаторов компрометации	Компонент хранения индикаторов компрометации должен обеспечивать доставку данных об угрозах информационной безопасности и индикаторах компрометации, характерных для отдельной организации в данный момент времени

Система с помощью функциональных компонентов должна обеспечивать реализацию следующих функциональных возможностей:

сбор событий;

управление активами;

обработку событий;

управление событиями;

обнаружение уязвимостей;

управление инцидентами;

отправку уведомлений;

визуализацию и построение отчетов;

обновление;

разграничение доступа пользователей Системы.

Унифицированное информационное взаимодействие между компонентами Системы должно обеспечиваться с использованием шины передачи данных и веб-служб, работающих на стеке протоколов TCP/IP.

Доступ к Системе должен осуществляться через веб-интерфейс.

Система должна предоставлять программный интерфейс (API) для взаимодействия с решениями других производителей.

Система должна поддерживать возможность подключения внешних систем хранения данных.

Целевые показатели системы:

Система должна поддерживать сбор событий не менее чем с 1000 узлов.

Требования к функциям Системы

Функции сбора событий

Компоненты Системы должны обеспечивать удаленный (сетевой) и локальный сбор событий.

Компоненты Системы должны обеспечивать как пассивный (без подключения к источнику), так и активный (с подключением к источнику) сбор событий.

Компоненты Системы должны обеспечивать возможность сбора событий в режиме, близком к режиму реального времени.

Управление сбором событий из различных типов источников должно осуществляться из единой консоли.

Система должна обеспечивать возможность фильтрации и поиска задач сбора данных по их атрибутам.

Учетные данные, необходимые для активного подключения к источникам, должны храниться в единой базе.

Должна быть обеспечена возможность использования одной записи с учетными данными для подключения к различным источникам с целью минимизации трудозатрат на корректировку учетных данных.

Система должна обеспечивать коррекцию времени в событиях от источника без дополнительной настройки источника.

Система должна обеспечивать стабильную работу с событиями, полученными от источников с некорректным временем.

Сбор событий должен быть реализован посредством модулей сбора данных на основе сохраняемых профилей.

В Системе должны быть предусмотрены предустановленные профили для сбора данных.

Пользователи Системы должны иметь возможность создавать собственные профили для сбора данных на базе системных (с возможностью редактирования различных параметров профиля, например, портов подключения, названий и полей таблиц, из которых производится сбор, частоты забора данных, количества передаваемых сообщений).

Система должна обеспечивать сбор событий с использованием следующих механизмов и протоколов:

сенсор в терминах протокола Cisco NetFlow;

сообщения стандарта syslog по протоколам TCP и UDP;

SNMP;

SMB;

WMI;

текстовые файлы в форматах 1CEnterprise8, AccordSucuCsvLog, FtpFileLog, Oracle Listener Log, SharePointServer, WindowsFileLog;

отслеживание изменений в БД следующих схем данных: DeviceLockLog, Dr Web Database, ForefrontEndpointProtectionLog, InfoWatchTrafficMonitor6.1, InfoWatchTrafficMonitorLog, KasperskySecurityCenter, Kontinent_ServerAccessLog, LinterVS_SAVZ, LinterVS_SOA, LinterVS_UD_NSD, LumensionEndpointSecurity, McAfeeEpoLog, McAfeeEpoLog4.5, OdbcLog MSSQL, OdbcLog Oracle, OracleAuditTrail, SCCMDetectSoftware, SCCMDetectUSBDevices, SCCMEvents, SecretNetLog, SecretNeLog_Oracle, SymantecEPMSecurityEvents, SymantecEPMSystemEvents, SymantecEPMVirusAlert, SystemCenterOperationsManager, Vipnet_StateWatcher, ZecurionZGate;

OPSEC LEA;

Windows Event Log;

результаты выполнения команд на сервере по протоколу SSH;
события платформы виртуализации VMware vSphere;
Система должна поддерживать получение данных из источников, указанных в таблице ниже (Таблица 2).

Таблица 2 — Перечень поддерживаемых источников событий

№ п/п	Наименование источника	Версия
Системы аутентификации, авторизации, учета		
	Cisco ACS	5.x
	RSA Authentication Manager	8.2, 8.3
	Avanpost IDM	5.3
Системы предотвращения утечек информации		
	InfoWatch Traffic Monitor	4.1, 6.1, 6.7
	Zecurion zGate (основной журнал)	7
	Zecurion zGate (журнал Zgate Proxy)	7
	«Конфидент», Dallas Lock	8.0, сборка 347.20, ред. K, C
Системы защиты приложений		
	Cisco Email Security Appliance (ESA)	7
	Positive Technologies Application Firewall	—
	McAfee Web Gateway	7.5
Бизнес-приложения		
	Microsoft SharePoint Server	2013
	1С:Предприятие	8.2, 8.3
	New Security Technologies SafeInspect	2.1
Системы управления базами данных		
	Microsoft SQL Server	2005, 2008, 2012, 2014
	Oracle Audit Trail	10g, 11g, 12c
	Oracle Database	10g, 11g, 12c
	Oracle MySQL	5.7.10
	Oracle Net Listener	10g, 11g, 12c
Системы защиты конечных узлов		
	Код безопасности Secret Net	7.6, 7.7
	Код безопасности Secret Net Studio	8.2, 8.3, 8.4
	Код безопасности vGate	2.7, 2.8, 3.0
	ESET Security Management Center	7.0
	Kaspersky Administration Kit	8.x
	Kaspersky Endpoint Security	10
	Kaspersky Security Center	8, 9, 10
	Symantec Endpoint Protection	12.1, 14
	Lumension Endpoint Security	4.4
	SmartLine DeviceLock DLP	7.3, 8.1
Антивирусное программное обеспечение		
	Kaspersky Security для Microsoft Exchange Servers	9
	Kaspersky Security для Microsoft SharePoint Server	9
	Kaspersky Security для Linux Mail Server	8.0
	Dr.Web Enterprise Security Suite	6, 10
Системы электронной почты		
	Microsoft Exchange Server	2003, 2007, 2010, 2013, 2016
	Postfix	2, 3
	Sendmail	8.x
Сетевые устройства		
	Avaya (Nortel) ERS	5500
	QTech QSW	3450-28T, 6500-52F, 8300-52F
	Cisco IOS	12.x, 15.x
	Cisco NX-OS	4.x, 5.x, 6.x, 7.x
	Cisco WLC	7.x
	Juniper JunOS	11.x, 12.x, 13.x, 14.x
	HPE Comware Software	5.x, 7.x
	Huawei	VRP 5.110

№ п/п	Наименование источника	Версия
Системы защиты сети		
	Arbor Networks Peakflow	7.6, 8.x
	WatchGuard FireWare XTMv	11.12.2
	Positive Technologies MaxPatrol 8	—
	Palo Alto Networks PAN-OS	6, 7, 8
	KerioControl Technologies	9.0
	Check Point GAiA OS	76, 77.10, 77.20, 77.30, R80
	S-Terra VPN Gate	4.1
	«Код безопасности», АПКШ «Континент»	3.7
Межсетевые экраны		
	Cisco ASA	8.x, 9.x
	FortiNet Fortigate	5.4.x
	McAfee (Forcepoint) Next Generation Firewall	5.3
Системы обнаружения и предотвращения вторжений		
	Cisco IPS	6.x
	Suricata	3.1
	Snort	2.9, 3
Операционные системы		
	FreeBSD	4.9–9.2
	Microsoft Windows	XP (только WMI), Vista, 7, 8, 8.1, 10, Server 2003 и Server 2003 R2 (только WMI), Server 2008, Server 2008 R2, Server 2012, Server 2012 R2
	Debian	7, 8, 9
	IBM AIX	5.3, 6.1, 7.1
	SUSE Linux Enterprise Service	11.x, 12.x
	CentOS	6.x, 7.x
Прокси-серверы		
	Cisco Web Security Appliance (WSA)	8.0
	Squid	3.0–3.5
	Entensys UserGate Proxy & Firewall	6
	Microsoft Forefront TMG	7.0
Системы виртуализации		
	VMware vSphere Hypervisor (ESXi)	5.5, 6.0, 6.5
	VMware vCenter	5.5, 6.0, 6.5
Веб-серверы		
	Apache HTTP Server	2
	Nginx	1.8, 1.9
	Microsoft Internet Information Services (IIS)	6.0, 7.5, 8.5
Системы динамической адресации		
	Microsoft DHCP Server	2008, 2012
	Microsoft DHCP Client	2008, 2012
	Microsoft Wndows DNS Server	2008, 2012
Системы управления обновлениями и конфигурацией		
	Microsoft Windows Server Update Services (WSUS)	Windows Server 2008, 2008R2, 2012, 2012 R2
Удостоверяющие центры		
	Microsoft Certification Authority (CA)	Windows Server 2008, 2008R2, 2012, 2012 R2
	RSA Certificate Manager	6.9
Системы мониторинга сети		
	Infotecs ViPNet StateWatcher	3.2
	Microsoft System Center Operations Manager (SCOM)	2012R2
Системы организации терминального доступа		
	Microsoft Windows Terminal Services	6.3

Система должна позволять подключать источники событий новых типов посредством дополнения множества правил преобразования событий (нормализации, агрегации).

Система должна позволять разрабатывать пользовательские модули сбора для работы с неподдерживаемыми поставщиками программных средств Системы протоколами передачи событий на скриптовом языке Python. Разработка и работа с такими модулями должна осуществляться через интерфейс Системы.

Запуск пользовательских модулей сбора должен осуществляться средствами агента Системы. Запуск модулей сторонними планировщиками не допускается в целях обеспечения информационной безопасности.

Система должна обеспечивать централизованную настройку и мониторинг работы модулей сбора событий из единой консоли управления.

При выполнении иерархической инсталляции Система должна обеспечивать отображение связей между площадками и возможность настройки правил репликации событий в цепочке иерархии.

Система должна обеспечивать возможность мониторинга источников, позволяя отслеживать:

задержку между временем возникновения событий и временем их получения Системой;

количество событий, получаемых в единицу времени.

Функции управления активами

Система должна обеспечивать идентификацию и добавление активов путем:

сбора и анализа событий;

сетевого сканирования для обнаружения узлов сети;

анализа защищенности по методам черного и белого ящика;

анализа сетевого трафика;

добавления актива пользователями (вручную).

Система должна обеспечивать идентификацию сетевых служб, использующих протоколы TCP и UDP в качестве протоколов транспортного уровня.

Система должна обеспечивать выявление и идентификацию активов, функционирующих в момент сканирования.

Система должна обеспечивать сбор идентификационных данных об активах (IP-адреса, имени узла, FQDN). Механизм идентификации должен обеспечивать выявление и корректную работу с кластерными конфигурациями активов.

Система должна обеспечивать выявление и идентификацию доступных в момент сканирования портов, использующих сетевые протоколы транспортного уровня.

Система должна обеспечивать сбор сведений о составе программного и аппаратного обеспечения сканируемого актива.

Система должна обеспечивать сбор параметров конфигурации актива по следующим протоколам удаленного управления: WMI, SAP RPC, SSH, Telnet, ODBC, SNMP, Checkpoint OPSEC.

Система должна обеспечивать автоматическую привязку событий к активам при условии, что в событии содержится идентификационная информация.

Система должна обеспечивать построение иерархии групп активов и управление ею.

Система должна обеспечивать автоматическое определение типа и роли узла по результатам сканирования в режимах черного или белого ящика.

Система должна обеспечивать построение и визуализацию топологии сети на актуальный момент времени на уровне L3 модели OSI.

Система должна иметь следующие механизмы для управления списком активов:

фильтрацию активов по заданному набору атрибутов и их значений с использованием специализированного языка запросов (в том числе с возможностью объединения запросов);

отображение активов, удовлетворяющих условиям пользовательского запроса, в таблице активов и на топологии;

возможность сохранения пользовательских запросов для последующего быстрого доступа к ним;

функции группировки и сортировки активов, анализа данных об активах.

Система должна обеспечивать отображение активов, участвовавших в событии или инциденте, на топологии сети.

Система должна обеспечивать расчет сетевой достижимости между выбранными активами на топологии с учетом протоколов и портов.

Система должна обеспечивать возможность задания активам уровня значимости и использование этой величины при количественной оценке опасности событий ИБ и инцидентов.

Система должна обеспечивать возможность мониторинга доступности активов (узлов, сетевых сервисов и устройств).

Система должна обеспечивать отслеживание изменений конфигурации активов, включая:

просмотр состояния актива на заданный момент времени в прошлом;

сравнение конфигураций актива в разные моменты времени;

экспорт истории конфигурации актива.

Система должна обеспечивать возможность просмотра информации об уязвимостях актива с указанием оценки CVSS и идентификатора CVE.

Система должна позволять объединять активы в динамические группы исходя из собранных данных об их конфигурации. Формирование динамических групп должно осуществляться как на основе пользовательских запросов, так и при помощи интерактивного конструктора запросов.

Система должна позволять добавлять в модель актива пользовательские поля и их описание.

Система должна позволять выполнять экспорт данных об активах в табличный список.

Функции обработки событий

Система должна обеспечивать нормализацию событий с использованием встроенных формул.

Система должна поддерживать возможность создания пользователями собственных формул нормализации.

Система должна обеспечивать агрегацию событий с использованием встроенных правил.

Система должна обеспечивать поддержку мультиязычных событий.

Система должна обеспечивать возможность корреляции событий в режиме, близком к режиму реального времени.

Система должна обеспечивать возможность проверки ранее полученных событий на наличие в них актуальных индикаторов компрометации.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие выявление целенаправленных атак в автоматическом режиме.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие в автоматическом режиме контроль действий пользователей и администраторов, выявление аномалий:

выявление активности на рабочих станциях в ночное время и выходные (праздничные) дни;

контроль VPN-соединений;

контроль выполнения команд, которые могут угрожать информационной безопасности КИС, на серверах и сетевом оборудовании;

контроль учетных записей;

контроль изменения конфигурации на сетевом оборудовании и серверах;

контроль установки и запуска новых сервисов ОС и сетевых служб.

Система должна предоставлять пользователю интерфейс создания пользовательских правил корреляции (визуальный конструктор привил корреляции) и возможность создания пользовательских правил корреляции на основе встроенных системных правил.

Система должна обеспечивать возможность управления списком активных правил корреляции с отображением статистики их срабатывания.

Система должна обеспечивать функцию многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции.

Система должна обеспечивать контроль потребляемой коррелятором памяти и при достижении порогового значения отключать нагружающие ее правила корреляции.

Система должна обеспечивать использование табличных списков при формировании правил корреляции. Пользователю должна быть доступна возможность их создания, удаления и редактирования через графический интерфейс.

Функциональность табличных списков должна позволять выполнять:

контроль времени жизни записей в таблице (TTL);

индексацию выделенных колонок в целях ускорения доступа к записям;

определение первичного ключа таблицы;

импорт и экспорт всего содержимого табличного списка.

При обращении к табличным спискам из правил корреляции должны быть доступны функции:

создания, обновления, удаления строк, а также очистки всей таблицы;

обогащения корреляционного события найденными данными из табличного списка;

выполнения математических функций инкремента, декремента, вычисления максимального, минимального и среднего при вставке данных в табличный список;

выполнения математических функций вычисления максимального, минимального, среднего и подсчета общего числа строк при выборке данных из табличного списка.

Система должна обеспечивать возможность задания правил обогащения событий, поступающих в систему, данными из табличных списков (в том числе данными из репутационных списков).

Система должна обеспечивать хранение исходных и нормализованных событий.

Функции управления событиями

Система должна содержать текстовое описание каждого события, предоставленное экспертами вендора.

Система должна обеспечивать категоризацию событий.

Система должна иметь следующие механизмы для управления списком событий:

фильтрацию событий по группе активов и периоду;

фильтрацию событий по заданному набору атрибутов и их значений с использованием специализированного языка запросов;

сохранение пользовательских фильтров для последующего быстрого доступа к интересующим событиям (с возможностью создания иерархического списка фильтров);

функции группировки и сортировки событий в выводе на экран по всем доступным полям;

анализ данных о событиях с помощью математических операций.

Функции управления инцидентами

Система должна обеспечивать автоматическое и ручное формирование инцидентов при обнаружении критичных с точки зрения пользователя событий.

Система должна обеспечивать импорт инцидентов из специально подготовленных файлов.

Система должна обеспечивать категорирование инцидентов.

Система должна обеспечивать управление автоматической генерацией инцидентов.

Система должна обеспечивать формирование инцидента с автоматической и ручной привязкой к нему событий.

Система должна обеспечивать просмотр и редактирование карточки инцидента.

Для управления списком инцидентов Система должна иметь следующие механизмы:

фильтрации инцидентов по группе активов и периоду;

фильтрации инцидентов по заданному набору атрибутов и их значений с использованием специализированного языка запросов;

фильтрации инцидентов с использованием системных и пользовательских фильтров;

сохранения пользовательских фильтров для последующего быстрого доступа (с возможность создания иерархического списка фильтров);

сортировки инцидентов по времени создания, статусу, критичности, категории, названию.

Система должна обеспечивать возможность построения процесса расследования инцидента: формирования поручений для расследования, определения порядка реагирования и устранения последствий инцидентов, назначения ответственных лиц.

Система должна обеспечивать хранение истории расследования инцидента.

Система должна обеспечивать наличие журнала изменений инцидента для регистрации изменений атрибутов и состояний инцидента.

Функции отправки уведомлений

Система должна обеспечивать возможность формирования и отправки уведомлений (по электронной почте):

об изменении списка активов в Системе;

изменении состава выбранных динамических групп активов (включении, исключении активов);

событиях и инцидентах — при их попадании под системный или пользовательский фильтр;

выходе параметров потока событий за пределы допустимых значений;

выполнении задач сбора данных;

состоянии Системы.

Система должна обеспечивать возможность отправки уведомления об изменении числа активов и изменениях в группах активов с помощью механизма webhook.

Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе пользователя о сбоях в работе, критичных для штатного функционирования сервисов.

Функции визуализации и построения отчетов

Система должна предоставлять оперативные данные об активах, событиях, инцидентах и мониторинге функционирования Системы в виде графиков, диаграмм и таблиц на виджетах и дашбордах.

Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов.

Система должна предоставлять возможность экспорта отчетов как минимум в одном из следующих форматов: PDF, XLSX, CSV.

Система должна обеспечивать отображение следующих статистических данных по инцидентам в графическом формате (на виджетах):

созданные инциденты,
закрытые инциденты за период,
незакрытые инциденты по уровню опасности,
среднее время устранения инцидента.

Система должна обеспечивать выпуск отчетов (стандартных и пользовательских) вручную или по расписанию.

Система должна предоставлять пользователю интерфейс создания пользовательских отчетов с данными об активах, событиях и инцидентах (конструктор отчетов).

Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:
по активам,
событиям,
инцидентам,
мониторингу.

Система должна обеспечивать построение следующих отчетов по активам:
инвентаризация групп пользователей Windows,
инвентаризация аппаратного обеспечения,
инвентаризация операционных систем,
инвентаризация узлов с открытыми портами,
инвентаризация сетевых сервисов,
инвентаризация ресурсов общего доступа,
инвентаризация ресурсов общего доступа по узлам,
инвентаризация программного обеспечения,
инвентаризация пользователей Windows,
инвентаризация служб Windows.

Система должна обеспечивать построение следующих отчетов по инцидентам:
распределение новых инцидентов по времени,
распределение утвержденных инцидентов по времени,
распределение инцидентов в работе по времени,
все открытые инциденты по времени,
распределение разрешенных инцидентов по времени,
распределение закрытых инцидентов по времени,
все завершенные инциденты по времени.

Система должна позволять автоматически обновлять список активов, событий и инцидентов в выводе на экран через определенные промежутки времени.

Графический интерфейс пользователя должен быть реализован по технологии Web.

Функции обновления

Система должна обеспечивать возможность обновления и расширения встроенных баз знаний вендора, в том числе формул нормализации и правил корреляции, в рамках действующей лицензии.

Система должна обеспечивать возможность обновления компонентов Системы без потери накопленных данных.

Функции разграничения доступа пользователей Системы

Система должна обеспечивать идентификацию и аутентификацию пользователей по уникальному идентификатору и паролю.

Система должна обеспечивать идентификацию и аутентификацию пользователей через сторонний LDAP-сервер.

В Системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета доступа пользователей к информации об определенных узлах (активах).

Система должна обеспечивать регистрацию действий пользователей при работе с компонентами Системы.

Приложение №2

к Документации

НА БЛАНКЕ ОРГАНИЗАЦИИ

№ _____
«___» _____ 2020 г Кому _____

ЗАЯВКА

на _____,

(указать наименование предмета запроса цен)

_____

(указать наименование и номер Лота, по которому Участник участвует в запросе цен, (в случае, если запрос цен проводится по нескольким лотам)

1. Изучив Документацию о проведении запрос цен на _____ *(указать наименование предмета запроса цен)* _____ *(фирменное наименование (наименование) Участника с указанием организационно-правовой формы, место нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные, сведения о месте жительства (для физического лица), номер контактного телефона)* в лице, _____ *(наименование должности руководителя и его Ф.И.О. (для юридического лица)* направляет настоящую Заявку на участие в запросе цен и сообщает о согласии участвовать в запросе цен на условиях, установленных в Извещении о проведении запроса цен и Документации о проведении запроса цен, и предлагает заключить договор на сумму _____ (сумма прописью) рублей 00 копеек, НДС не облагается на основании п.п. 26 п. 2 ст. 149 Части 2 Налогового кодекса Российской Федерации.

Цена Договора включает в себя все обязательные платежи и расходы, связанные с исполнением договора, в том числе стоимость передаваемых неисключительных прав, все уплачиваемые и взимаемые на территории Российской Федерации налоги, пошлины, сборы, страховые и другие обязательные платежи, стоимость дополнительных услуг, а также затраты по гарантийным обязательствам.

2. Мы заявляем, что на момент подачи Заявки на участие в запросе цен «___»_____20_ г. _____ *(указывается наименование и реквизиты запроса цен)*:

- в отношении_____ *(указывается фирменное наименование Участника)* ликвидация не проводится, решение арбитражного суда о признании _____ *(указывается фирменное наименование Участника)* банкротом и об открытии конкурсного производства отсутствует;
- деятельность _____ *(указывается фирменное наименование Участника)* не приостановлена в порядке, предусмотренном Кодексом Российской Федерации об административных правонарушениях;
- у _____ *(указывается фирменное наименование Участника)* отсутствует задолженность по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды за прошедший календарный год, размер которой превышает двадцать пять процентов балансовой стоимости активов _____ *(указывается фирменное наименование Участника)* по данным бухгалтерской отчетности за последний завершенный отчетный период.
- _____ *(указывается фирменное наименование Участника)* в течение двух лет до момента подачи Заявки на участие в закупке не было(а) привлечено(а) к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях.

3. Мы согласны придерживаться положений настоящей Заявки на участие в запросе цен до момента заключения договора, но в любом случае не менее 45 дней со дня вскрытия конвертов с Заявками на участие в запросе цен. Эта Заявка на участие в запросе цен будет оставаться для нас обязательной и может быть принята в любой момент до наступления вышеуказанных обстоятельств.

4. В случае, если наши предложения будут признаны лучшими, мы берем на себя обязательства подписать договор с автономной некоммерческой организацией «Аналитический центр при Правительстве Российской Федерации» на _____ *(указать наименование предмета запроса цен (лота)* в соответствии с требованиями Документации о проведении запроса цен и условиями наших предложений, в срок, установленный в Документации о проведении запроса цен.

5. В случае принятия решения о заключении с нами договора, мы обязуемся подписать договор на _____ *(указать наименование предмета запроса цен (лота)* в соответствии с

требованиями Документации о проведении запроса цен и условиями наших предложений по цене, содержащихся в настоящей Заявке на участие в запросе цен и установленных в Документации о проведении запроса цен в качестве критериев оценки Заявок на участие в запросе цен.

6. Мы извещены о включении сведений о _____ *(наименование организации или Ф.И.О. Участника)* в Реестр недобросовестных поставщиков Аналитического центра при Правительстве Российской Федерации в случае нашего уклонения от заключения договора.

7. Сообщаем, что для оперативного уведомления нас по вопросам организационного характера и взаимодействия с Заказчиком нами уполномочен _____ *(должность, Ф.И.О., телефон, электронная почта сотрудника – Участника).*

Все сведения о проведении запроса цен просим сообщать уполномоченному лицу.

8. В случае присуждения нам права заключить договор в период с даты получения проекта договора и до подписания официального договора настоящая Заявка на участие в запросе цен будет носить характер предварительного заключенного нами и Заказчиком договора о заключении договора на условиях наших предложений.

9. Наше местонахождение _____ *(для юридического лица)*, место жительства _____ (*для физического лица)*, почтовый адрес _____, телефон _____, факс _____.

10. Корреспонденцию в наш адрес просим направлять по адресу: _____.

11. К настоящей Заявке прилагаются документы на _____стр.

11.1 Приложение № 1

Предложение о функциональных характеристиках (потребительских свойствах) и качественных характеристиках.

11.2. **Копия, действующего на момент подачи заявки, договора, подтверждающего наличие соответствующих полномочий Участника от правообладателя прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent».**

11.3 Приложение № 2

Анкета Участника.

_____ _____

(подпись) (фамилия, имя, отчество подписавшего, должность)

М.П.

Приложение № 1
к Заявке

НА БЛАНКЕ ОРГАНИЗАЦИИ

№ _____
«___» _____ 2020 г. Кому _____

Предложение о функциональных характеристиках
(потребительских свойствах) и качественных характеристиках товаров

_____, (Участник)
наименование (юридического лица)/Ф.И.О. (для физического лица)

согласно на предоставление неисключительных прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

Наименование, количество, характеристики и цена приведены в таблице:

№ п/п	парт номер	Наименование Продукта	Кол-во (шт)	Срок использования	Цена за ед. руб., (без НДС)	Сумма в руб. (без НДС)
1.	PT-MPSIEM-BASE-H1000	MaxPatrol SIEM, базовая лицензия на 1 000 узлов, гарантийные обязательства в течение 1 (одного) года	1	бессрочно	*	*
2.	PT-MPSIEM-SRV	MaxPatrol SIEM Server, гарантийные обязательства в течение 1 (одного) года	1	бессрочно	*	*
3	PT-MPSIEM-AGT	MaxPatrol SIEM Agent, гарантийные обязательства в течение 1 (одного) года	1	бессрочно	*	*
	Итого					*

Всего неисключительные права на использование Продукта на сумму _____ (сумма прописью) рублей ___ копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

** Заполняется Участником запроса цен.*
Текст, выделенный курсивом, в заявке не воспроизводится

ТРЕБОВАНИЯ К СИСТЕМЕ

Требования к Системе в целом

Функциональные компоненты программных средств Системы должны поддерживать развертывание как на физическом, так и на виртуальном оборудовании.
Система должна быть построена по модульному принципу и позволять ее использование и установку в различных конфигурациях.
В состав Системы должны входить следующие функциональные компоненты:
компонент управления;
компонент обработки;
компонент хранения;
компонент сбора событий;
компонент управления доступом;

база знаний с экспертизой вендора;
компонент обновления и конфигурирования;
компонент хранения индикаторов компрометации.

Таблица 3 — Требования к функциям компонентов Системы

№ п/п	Наименование компонента	Назначение компонента
	Компонент управления	Компонент управления должен выполнять следующие функции: централизованное хранения конфигурации активов; централизованное управление компонентами системы; оперативное реагирование на инциденты ИБ и обеспечение взаимодействия подразделений организации при расследовании этих инцидентов; автоматизация процесса обнаружения уязвимостей; предоставление графического интерфейса пользователя
	Компонент обработки	Компонент обработки должен осуществлять функции по обработке и хранению событий: агрегацию, нормализацию и корреляцию событий; автоматическое создание инцидентов; привязку событий к активам
	Компонент хранения	Компонент хранения должен осуществлять централизованное хранение информации о событиях — как исходных, так и нормализованных
	Компонент сбора событий	Компонент сбора событий должен обеспечивать сбор событий от различных источников и позволять осуществлять сканирование узлов корпоративной информационной системы (далее - КИС) в режимах черного и белого ящика
	Компонент управления доступом	Компонент управления доступом должен обеспечивать доступ к системе через сервис единого входа, управление пользователями системы и журналирование действий пользователей
	База знаний с экспертизой вендора	База знаний должна обеспечивать получение данных о новых уязвимостях и эксплойтах, данных, необходимых для структурирования сведений, собранных от объектов инфраструктуры, правил обработки событий
	Компонент обновления и конфигурирования	Компонент обновления и конфигурирования должен обеспечивать проверку наличия, загрузку и установку новых версий отдельных компонентов Системы, а также обновление базы знаний
	Компонент хранения индикаторов компрометации	Компонент хранения индикаторов компрометации должен обеспечивать доставку данных об угрозах информационной безопасности и индикаторах компрометации, характерных для отдельной организации в данный момент времени

Система с помощью функциональных компонентов должна обеспечивать реализацию следующих функциональных возможностей:
сбор событий;
управление активами;
обработку событий;
управление событиями;
обнаружение уязвимостей;
управление инцидентами;
отправку уведомлений;
визуализацию и построение отчетов;
обновление;
разграничение доступа пользователей Системы.

Унифицированное информационное взаимодействие между компонентами Системы должно обеспечиваться с использованием шины передачи данных и веб-служб, работающих на стеке протоколов TCP/IP.

Доступ к Системе должен осуществляться через веб-интерфейс.

Система должна предоставлять программный интерфейс (API) для взаимодействия с решениями других производителей.

Система должна поддерживать возможность подключения внешних систем хранения данных.

Целевые показатели системы:

Система должна поддерживать сбор событий не менее чем с 1000 узлов.

Требования к функциям Системы

Функции сбора событий

Компоненты Системы должны обеспечивать удаленный (сетевой) и локальный сбор событий.

Компоненты Системы должны обеспечивать как пассивный (без подключения к источнику), так и активный (с подключением к источнику) сбор событий.

Компоненты Системы должны обеспечивать возможность сбора событий в режиме, близком к режиму реального времени.
Управление сбором событий из различных типов источников должно осуществляться из единой консоли.
Система должна обеспечивать возможность фильтрации и поиска задач сбора данных по их атрибутам.
Учетные данные, необходимые для активного подключения к источникам, должны храниться в единой базе.
Должна быть обеспечена возможность использования одной записи с учетными данными для подключения к различным источникам с целью минимизации трудозатрат на корректировку учетных данных.
Система должна обеспечивать коррекцию времени в событиях от источника без дополнительной настройки источника.
Система должна обеспечивать стабильную работу с событиями, полученными от источников с некорректным временем.
Сбор событий должен быть реализован посредством модулей сбора данных на основе сохраняемых профилей.
В Системе должны быть предусмотрены предустановленные профили для сбора данных.
Пользователи Системы должны иметь возможность создавать собственные профили для сбора данных на базе системных (с возможностью редактирования различных параметров профиля, например, портов подключения, названий и полей таблиц, из которых производится сбор, частоты забора данных, количества передаваемых сообщений).
Система должна обеспечивать сбор событий с использованием следующих механизмов и протоколов:
сенсор в терминах протокола Cisco NetFlow;
сообщения стандарта syslog по протоколам TCP и UDP;
SNMP;
SMB;
WMI;
текстовые файлы в форматах 1CEnterprise8, AccordSucuCsvLog, FtpFileLog, Oracle Listener Log, SharePointServer, WindowsFileLog;
отслеживание изменений в БД следующих схем данных: DeviceLockLog, Dr Web Database, ForefrontEndpointProtectionLog, InfoWatchTrafficMonitor6.1, InfoWatchTrafficMonitorLog, KasperskySecurityCenter, Kontinent_ServerAccessLog, LinterVS_SAVZ, LinterVS_SOA, LinterVS_UD_NSD, LumensionEndpointSecurity, McAfeeEpoLog, McAfeeEpoLog4.5, OdbcLog MSSQL, OdbcLog Oracle, OracleAuditTrail, SCCMDetectSoftware, SCCMDetectUSBDevices, SCCMEvents, SecretNetLog, SecretNeLog_Oracle, SymantecEPMSecurityEvents, SymantecEPMSystemEvents, SymantecEPMVirusAlert, SystemCenterOperationsManager, Vipnet_StateWatcher, ZecurionZGate;
OPSEC LEA;
Windows Event Log;
результаты выполнения команд на сервере по протоколу SSH;
события платформы виртуализации VMware vSphere;
Система должна поддерживать получение данных из источников, указанных в таблице ниже (Таблица 2).
Таблица 4 — Перечень поддерживаемых источников событий

№ п/п	Наименование источника	Версия
Системы аутентификации, авторизации, учета		
	Cisco ACS	5.x
	RSA Authentication Manager	8.2, 8.3
	Avanpost IDM	5.3
Системы предотвращения утечек информации		
	InfoWatch Traffic Monitor	4.1, 6.1, 6.7
	Zecurion zGate (основной журнал)	7
	Zecurion zGate (журнал Zgate Proxy)	7
	«Конфидент», Dallas Lock	8.0, сборка 347.20, ред. K, C
Системы защиты приложений		
	Cisco Email Security Appliance (ESA)	7
	Positive Technologies Application Firewall	—
	McAfee Web Gateway	7.5
Бизнес-приложения		
	Microsoft SharePoint Server	2013
	1С:Предприятие	8.2, 8.3
	New Security Technologies SafeInspect	2.1
Системы управления базами данных		
	Microsoft SQL Server	2005, 2008, 2012, 2014
	Oracle Audit Trail	10g, 11g, 12c
	Oracle Database	10g, 11g, 12c
	Oracle MySQL	5.7.10
	Oracle Net Listener	10g, 11g, 12c
Системы защиты конечных узлов		
	Код безопасности Secret Net	7.6, 7.7

№ п/п	Наименование источника	Версия
	Код безопасности Secret Net Studio	8.2, 8.3, 8.4
	Код безопасности vGate	2.7, 2.8, 3.0
	ESET Security Management Center	7.0
	Kaspersky Administration Kit	8.x
	Kaspersky Endpoint Security	10
	Kaspersky Security Center	8, 9, 10
	Symantec Endpoint Protection	12.1, 14
	Lumension Endpoint Security	4.4
	SmartLine DeviceLock DLP	7.3, 8.1
Антивирусное программное обеспечение		
	Kaspersky Security для Microsoft Exchange Servers	9
	Kaspersky Security для Microsoft SharePoint Server	9
	Kaspersky Security для Linux Mail Server	8.0
	Dr.Web Enterprise Security Suite	6, 10
Системы электронной почты		
	Microsoft Exchange Server	2003, 2007, 2010, 2013, 2016
	Postfix	2, 3
	Sendmail	8.x
Сетевые устройства		
	Avaya (Nortel) ERS	5500
	QTech QSW	3450-28T, 6500-52F, 8300-52F
	Cisco IOS	12.x, 15.x
	Cisco NX-OS	4.x, 5.x, 6.x, 7.x
	Cisco WLC	7.x
	Juniper JunOS	11.x, 12.x, 13.x, 14.x
	HPE Comware Software	5.x, 7.x
	Huawei	VRP 5.110
Системы защиты сети		
	Arbor Networks Peakflow	7.6, 8.x
	WatchGuard FireWare XTMv	11.12.2
	Positive Technologies MaxPatrol 8	—
	Palo Alto Networks PAN-OS	6, 7, 8
	KerioControl Technologies	9.0
	Check Point GAiA OS	76, 77.10, 77.20, 77.30, R80
	S-Terra VPN Gate	4.1
	«Код безопасности», АПКШ «Континент»	3.7
Межсетевые экраны		
	Cisco ASA	8.x, 9.x
	FortiNet Fortigate	5.4.x
	McAfee (Forcepoint) Next Generation Firewall	5.3
Системы обнаружения и предотвращения вторжений		
	Cisco IPS	6.x
	Suricata	3.1
	Snort	2.9, 3
Операционные системы		
	FreeBSD	4.9–9.2
	Microsoft Windows	XP (только WMI), Vista, 7, 8, 8.1, 10, Server 2003 и Server 2003 R2 (только WMI), Server 2008, Server 2008 R2, Server 2012, Server 2012 R2
	Debian	7, 8, 9
	IBM AIX	5.3, 6.1, 7.1
	SUSE Linux Enterprise Service	11.x, 12.x
	CentOS	6.x, 7.x
Прокси-серверы		
	Cisco Web Security Appliance (WSA)	8.0
	Squid	3.0–3.5
	Entensys UserGate Proxy & Firewall	6

№ п/п	Наименование источника	Версия
	Microsoft Forefront TMG	7.0
Системы виртуализации		
	VMware vSphere Hypervisor (ESXi)	5.5, 6.0, 6.5
	VMware vCenter	5.5, 6.0, 6.5
Веб-серверы		
	Apache HTTP Server	2
	Nginx	1.8, 1.9
	Microsoft Internet Information Services (IIS)	6.0, 7.5, 8.5
Системы динамической адресации		
	Microsoft DHCP Server	2008, 2012
	Microsoft DHCP Client	2008, 2012
	Microsoft Wndows DNS Server	2008, 2012
Системы управления обновлениями и конфигурацией		
	Microsoft Windows Server Update Services (WSUS)	Windows Server 2008, 2008R2, 2012, 2012 R2
Удостоверяющие центры		
	Microsoft Certification Authority (CA)	Windows Server 2008, 2008R2, 2012, 2012 R2
	RSA Certificate Manager	6.9
Системы мониторинга сети		
	Infotecs ViPNet StateWatcher	3.2
	Microsoft System Center Operations Manager (SCOM)	2012R2
Системы организации терминального доступа		
	Microsoft Windows Terminal Services	6.3

Система должна позволять подключать источники событий новых типов посредством дополнения множества правил преобразования событий (нормализации, агрегации).

Система должна позволять разрабатывать пользовательские модули сбора для работы с неподдерживаемыми поставщиками программных средств Системы протоколами передачи событий на скриптовом языке Python. Разработка и работа с такими модулями должна осуществляться через интерфейс Системы.

Запуск пользовательских модулей сбора должен осуществляться средствами агента Системы. Запуск модулей сторонними планировщиками не допускается в целях обеспечения информационной безопасности.

Система должна обеспечивать централизованную настройку и мониторинг работы модулей сбора событий из единой консоли управления.

При выполнении иерархической инсталляции Система должна обеспечивать отображение связей между площадками и возможность настройки правил репликации событий в цепочке иерархии.

Система должна обеспечивать возможность мониторинга источников, позволяя отслеживать:

задержку между временем возникновения событий и временем их получения Системой;

количество событий, получаемых в единицу времени.

Функции управления активами

Система должна обеспечивать идентификацию и добавление активов путем:

сбора и анализа событий;

сетевого сканирования для обнаружения узлов сети;

анализа защищенности по методам черного и белого ящика;

анализа сетевого трафика;

добавления актива пользователями (вручную).

Система должна обеспечивать идентификацию сетевых служб, использующих протоколы TCP и UDP в качестве протоколов транспортного уровня.

Система должна обеспечивать выявление и идентификацию активов, функционирующих в момент сканирования.

Система должна обеспечивать сбор идентификационных данных об активах (IP-адреса, имени узла, FQDN). Механизм идентификации должен обеспечивать выявление и корректную работу с кластерными конфигурациями активов.

Система должна обеспечивать выявление и идентификацию доступных в момент сканирования портов, использующих сетевые протоколы транспортного уровня.

Система должна обеспечивать сбор сведений о составе программного и аппаратного обеспечения сканируемого актива.

Система должна обеспечивать сбор параметров конфигурации актива по следующим протоколам удаленного управления: WMI, SAP RPC, SSH, Telnet, ODBC, SNMP, Checkpoint OPSEC.

Система должна обеспечивать автоматическую привязку событий к активам при условии, что в событии содержится идентификационная информация.

Система должна обеспечивать построение иерархии групп активов и управление ею.

Система должна обеспечивать автоматическое определение типа и роли узла по результатам сканирования в

режимах черного или белого ящика.

Система должна обеспечивать построение и визуализацию топологии сети на актуальный момент времени на уровне L3 модели OSI.

Система должна иметь следующие механизмы для управления списком активов:

фильтрацию активов по заданному набору атрибутов и их значений с использованием специализированного языка запросов (в том числе с возможностью объединения запросов);

отображение активов, удовлетворяющих условиям пользовательского запроса, в таблице активов и на топологии;

возможность сохранения пользовательских запросов для последующего быстрого доступа к ним;

функции группировки и сортировки активов, анализа данных об активах.

Система должна обеспечивать отображение активов, участвовавших в событии или инциденте, на топологии сети.

Система должна обеспечивать расчет сетевой достижимости между выбранными активами на топологии с учетом протоколов и портов.

Система должна обеспечивать возможность задания активам уровня значимости и использование этой величины при количественной оценке опасности событий ИБ и инцидентов.

Система должна обеспечивать возможность мониторинга доступности активов (узлов, сетевых сервисов и устройств).

Система должна обеспечивать отслеживание изменений конфигурации активов, включая:

просмотр состояния актива на заданный момент времени в прошлом;

сравнение конфигураций актива в разные моменты времени;

экспорт истории конфигурации актива.

Система должна обеспечивать возможность просмотра информации об уязвимостях актива с указанием оценки CVSS и идентификатора CVE.

Система должна позволять объединять активы в динамические группы исходя из собранных данных об их конфигурации. Формирование динамических групп должно осуществляться как на основе пользовательских запросов, так и при помощи интерактивного конструктора запросов.

Система должна позволять добавлять в модель актива пользовательские поля и их описание.

Система должна позволять выполнять экспорт данных об активах в табличный список.

Функции обработки событий

Система должна обеспечивать нормализацию событий с использованием встроенных формул.

Система должна поддерживать возможность создания пользователями собственных формул нормализации.

Система должна обеспечивать агрегацию событий с использованием встроенных правил.

Система должна обеспечивать поддержку мультиязычных событий.

Система должна обеспечивать возможность корреляции событий в режиме, близком к режиму реального времени.

Система должна обеспечивать возможность проверки ранее полученных событий на наличие в них актуальных индикаторов компрометации.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие выявление целенаправленных атак в автоматическом режиме.

В состав Системы должны входить встроенные правила корреляции, обеспечивающие в автоматическом режиме контроль действий пользователей и администраторов, выявление аномалий:

выявление активности на рабочих станциях в ночное время и выходные (праздничные) дни;

контроль VPN-соединений;

контроль выполнения команд, которые могут угрожать информационной безопасности КИС, на серверах и сетевом оборудовании;

контроль учетных записей;

контроль изменения конфигурации на сетевом оборудовании и серверах;

контроль установки и запуска новых сервисов ОС и сетевых служб.

Система должна предоставлять пользователю интерфейс создания пользовательских правил корреляции (визуальный конструктор привил корреляции) и возможность создания пользовательских правил корреляции на основе встроенных системных правил.

Система должна обеспечивать возможность управления списком активных правил корреляции с отображением статистики их срабатывания.

Система должна обеспечивать функцию многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции.

Система должна обеспечивать контроль потребляемой коррелятором памяти и при достижении порогового значения отключать нагружающие ее правила корреляции.

Система должна обеспечивать использование табличных списков при формировании правил корреляции. Пользователю должна быть доступна возможность их создания, удаления и редактирования через графический интерфейс.

Функциональность табличных списков должна позволять выполнять:

контроль времени жизни записей в таблице (TTL);

индексацию выделенных колонок в целях ускорения доступа к записям;

определение первичного ключа таблицы;

импорт и экспорт всего содержимого табличного списка.

При обращении к табличным спискам из правил корреляции должны быть доступны функции:

создания, обновления, удаления строк, а также очистки всей таблицы;

обогащения корреляционного события найденными данными из табличного списка;

выполнения математических функций инкремента, декремента, вычисления максимального, минимального и среднего при вставке данных в табличный список;

выполнения математических функций вычисления максимального, минимального, среднего и подсчета общего числа строк при выборке данных из табличного списка.

Система должна обеспечивать возможность задания правил обогащения событий, поступающих в систему, данными из табличных списков (в том числе данными из репутационных списков).

Система должна обеспечивать хранение исходных и нормализованных событий.

Функции управления событиями

Система должна содержать текстовое описание каждого события, предоставленное экспертами вендора.

Система должна обеспечивать категоризацию событий.

Система должна иметь следующие механизмы для управления списком событий:

фильтрацию событий по группе активов и периоду;

фильтрацию событий по заданному набору атрибутов и их значений с использованием специализированного языка запросов;

сохранение пользовательских фильтров для последующего быстрого доступа к интересующим событиям (с возможностью создания иерархического списка фильтров);

функции группировки и сортировки событий в выводе на экран по всем доступным полям;

анализ данных о событиях с помощью математических операций.

Функции управления инцидентами

Система должна обеспечивать автоматическое и ручное формирование инцидентов при обнаружении критичных с точки зрения пользователя событий.

Система должна обеспечивать импорт инцидентов из специально подготовленных файлов.

Система должна обеспечивать категорирование инцидентов.

Система должна обеспечивать управление автоматической генерацией инцидентов.

Система должна обеспечивать формирование инцидента с автоматической и ручной привязкой к нему событий.

Система должна обеспечивать просмотр и редактирование карточки инцидента.

Для управления списком инцидентов Система должна иметь следующие механизмы:

фильтрации инцидентов по группе активов и периоду;

фильтрации инцидентов по заданному набору атрибутов и их значений с использованием специализированного языка запросов;

фильтрации инцидентов с использованием системных и пользовательских фильтров;

сохранения пользовательских фильтров для последующего быстрого доступа (с возможность создания иерархического списка фильтров);

сортировки инцидентов по времени создания, статусу, критичности, категории, названию.

Система должна обеспечивать возможность построения процесса расследования инцидента: формирования поручений для расследования, определения порядка реагирования и устранения последствий инцидентов, назначения ответственных лиц.

Система должна обеспечивать хранение истории расследования инцидента.

Система должна обеспечивать наличие журнала изменений инцидента для регистрации изменений атрибутов и состояний инцидента.

Функции отправки уведомлений

Система должна обеспечивать возможность формирования и отправки уведомлений (по электронной почте):

об изменении списка активов в Системе;

изменении состава выбранных динамических групп активов (включении, исключении активов);

событиях и инцидентах — при их попадании под системный или пользовательский фильтр;

выходе параметров потока событий за пределы допустимых значений;

выполнении задач сбора данных;

состоянии Системы.

Система должна обеспечивать возможность отправки уведомления об изменении числа активов и изменениях в группах активов с помощью механизма webhook.

Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе пользователя о сбоях в работе, критичных для штатного функционирования сервисов.

Функции визуализации и построения отчетов

Система должна предоставлять оперативные данные об активах, событиях, инцидентах и мониторинге функционирования Системы в виде графиков, диаграмм и таблиц на виджетах и дашбордах.

Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов.

Система должна предоставлять возможность экспорта отчетов как минимум в одном из следующих форматов: PDF, XLSX, CSV.

Система должна обеспечивать отображение следующих статистических данных по инцидентам в графическом формате (на виджетах):

созданные инциденты,

закрытые инциденты за период,

незакрытые инциденты по уровню опасности,

среднее время устранения инцидента.

Система должна обеспечивать выпуск отчетов (стандартных и пользовательских) вручную или по расписанию.

Система должна предоставлять пользователю интерфейс создания пользовательских отчетов с данными об активах, событиях и инцидентах (конструктор отчетов).

Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:

по активам,

событиям,

инцидентам,

мониторингу.

Система должна обеспечивать построение следующих отчетов по активам:

инвентаризация групп пользователей Windows,

инвентаризация аппаратного обеспечения,

инвентаризация операционных систем,

инвентаризация узлов с открытыми портами,

инвентаризация сетевых сервисов,

инвентаризация ресурсов общего доступа,

инвентаризация ресурсов общего доступа по узлам,

инвентаризация программного обеспечения,

инвентаризация пользователей Windows,

инвентаризация служб Windows.

Система должна обеспечивать построение следующих отчетов по инцидентам:

распределение новых инцидентов по времени,

распределение утвержденных инцидентов по времени,

распределение инцидентов в работе по времени,

все открытые инциденты по времени,

распределение разрешенных инцидентов по времени,

распределение закрытых инцидентов по времени,

все завершенные инциденты по времени.

Система должна позволять автоматически обновлять список активов, событий и инцидентов в выводе на экран через определенные промежутки времени.

Графический интерфейс пользователя должен быть реализован по технологии Web.

Функции обновления

Система должна обеспечивать возможность обновления и расширения встроенных баз знаний вендора, в том числе формул нормализации и правил корреляции, в рамках действующей лицензии.

Система должна обеспечивать возможность обновления компонентов Системы без потери накопленных данных.

Функции разграничения доступа пользователей Системы

Система должна обеспечивать идентификацию и аутентификацию пользователей по уникальному идентификатору и паролю.

Система должна обеспечивать идентификацию и аутентификацию пользователей через сторонний LDAP-сервер.

В Системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета доступа пользователей к информации об определенных узлах (активах).

Система должна обеспечивать регистрацию действий пользователей при работе с компонентами Системы.

Руководитель _____ /_____/

(подпись) (расшифровка подписи)

Приложение № 2
к Заявке

АНКЕТА УЧАСТНИКА*

1. Для Участника: 1.1. Юридического лица – полное наименование организации и ее организационно-правовая форма. 1.2. Физического лица, в том числе зарегистрированного в качестве индивидуального предпринимателя – фамилия, имя, отчество.	
2. Для Участника: 2.1. Юридического лица – место нахождения (юридический адрес) 2.2. Индивидуального предпринимателя – серия, номер и дата выдачи свидетельства о государственной регистрации, адрес регистрации 2.3. Физического лица – паспортные данные (серия и номер паспорта, кем и когда выдан, код подразделения, адрес регистрации)	
3. Для Участника: 3.1. Юридического лица – ИНН, КПП, ОГРН, ОКПО 3.2. Индивидуального предпринимателя – ИНН, ОГРНИП 3.3. Физического лица – ИНН, СНИЛС	
4. Фактический (почтовый) адрес Участника	
Страна	
Адрес	
Телефон	
Факс	
5. Банковские реквизиты (может быть несколько):	
5.1. Наименование обслуживающего банка	
5.2. Расчетный счет	
5.3. Корреспондентский счет	
5.4. Код БИК	
6. Фамилия, имя, отчество генерального директора (лица имеющего право подписи без доверенности), номер телефона	

Мы, нижеподписавшиеся, заверяем правильность всех данных, указанных в анкете.

_____ _____ /_____/

(должность) (подпись) (ФИО)

М.П.

** Анкета участника размещается на электронной площадке в формате Word.*

Приложение № 3
к Документации

СОГЛАСИЕ
на обработку персональных данных Участника
(представителя Участника)

Я, _____ ,
(фамилия, имя, отчество)

паспорт серии _____ , номер _____ , выдан _____
(дата выдачи)

_____ ,
(наименование органа, выдавшего паспорт)

_____ ,
(адрес места регистрации)

в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ выражаю автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации» (далее – Аналитический центр при Правительстве Российской Федерации), зарегистрированному по адресу: Российская Федерация, г. Москва, проспект Академика Сахарова, д.12, согласие на обработку моих персональных данных.

Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя и отчество;

дата и место рождения;

паспортные данные;

адрес места регистрации;

биометрические персональные данные (фотография).

Целью обработки персональных данных является проявление должной осмотрительности при выборе контрагента для заключения договора и минимизации (исключения) налоговых и репутационных рисков при осуществлении делового сотрудничества с ним.

Действия с моими персональными данными могут включать в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработка моих персональных данных может осуществляться как с применением средств автоматизации, так и без применения таких средств.

Настоящее согласие предоставляется на срок подготовки и действия договора с Аналитическим центром при Правительстве Российской Федерации.

Я осведомлён о том, что настоящее согласие может быть отозвано мной в любое время на основании моего письменного заявления.

«__» _____ 20__ г. _____

Приложение № 3
к Документации

ПРОЕКТ

СУБЛИЦЕНЗИОННЫЙ ДОГОВОР № _____

г. Москва **«__» _____ 2020 г.**

Автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации», именуемая в дальнейшем СУБЛИЦЕНЗИАТ, в лице _____, действующего на основании_____ с одной стороны, и _____, именуемое в дальнейшем СУБЛИЦЕНЗИАР, в лице _____, действующего на основании _____, с другой стороны, совместно именуемые Стороны, заключили настоящий договор (далее - Договор) о нижеследующем:

1. ТЕРМИНЫ, ИСПОЛЬЗУЕМЫЕ В ДОГОВОРЕ

ПРАВООБЛАДАТЕЛЬ – юридическое или физическое лицо, обладающее исключительными правами на программы ЭВМ и базы данных.

ПРОДУКТ – экземпляр лицензионного программного обеспечения для ЭВМ и базы данных, а также любые носители с ними, документация и иные принадлежности, которые необходимы для использования программ для ЭВМ и баз данных КОНЕЧНЫМИ ПОЛЬЗОВАТЕЛЯМИ.

СУБЛИЦЕНЗИАР – юридическое лицо, обладающее правами на распространение и воспроизведение ПРОДУКТОВ, а также на передачу прав на распространение и использование ПРОДУКТОВ на законном основании.

СУБЛИЦЕНЗИАТ - КОНЕЧНЫЙ ПОЛЬЗОВАТЕЛЬ – пользователь (потребитель) ПРОДУКТОВ, непосредственно воспроизводящий ПРОДУКТ на компьютере, сервере путем инсталляции и запуска в соответствии с правилами лицензионного использования конкретного ПРОДУКТА, установленными соответствующими ПРАВООБЛАДАТЕЛЯМИ.

2. ПРЕДМЕТ ДОГОВОРА

2.1. СУБЛИЦЕНЗИАР, имея соответствующие полномочия от ПРАВООБЛАДАТЕЛЕЙ (сертификат), и действуя в соответствии с требованием ст.ст. 1235-1238, 1286 Гражданского кодекса Российской Федерации, обязуется поставить СУБЛИЦЕНЗИАТУ неисключительные права на использование ПРОДУКТА (простая неисключительная лицензия) в соответствии со Спецификацией (Приложение № 1 к Договору).

2.2. Право на использование ПРОДУКТА, предоставляемое (передаваемое) СУБЛИЦЕНЗИАТУ в соответствии с Договором, включает использование следующими способами: неисключительное право на воспроизведение ПРОДУКТА в качестве конечного пользователя, ограниченное правом инсталляции, копирования и запуска ПРОДУКТА в соответствии с лицензионным соглашением для конечного пользователя, подтверждаемого СУБЛИЦЕНЗИАТОМ при установке ПРОДУКТА.

2.3 Наименование ПРОДУКТА, права на распространение и использование которых передаются от СУБЛИЦЕНЗИАРА к СУБЛИЦЕНЗИАТУ, размер лицензионного платежа (вознаграждение) указываются в Спецификации (Приложение № 1 к Договору), счетах и Актах передачи прав, которые подписываются Сторонами при передаче прав.

2.4. Период пользования ПРОДУКТА в соответствии со Спецификацией (Приложение № 1 к Договору).

2.5. Срок передачи ПРОДУКТА: в течение 10 (Десяти) рабочих дней с даты заключения Договора, но не позднее 25 декабря 2020г.

2.6. Территория, на которой допускается использование СУБЛИЦЕНЗИАТОМ ПРОДУКТОМ устанавливается как вся территория страны СУБЛИЦЕНЗИАТА.

2.7. Договор заключен Сторонами по итогам проведения запроса цен в электронной форме.

Протокол № _____ от _____ 2020 г.

3. ЛИЦЕНЗИОННЫЕ ПЛАТЕЖИ И ПОРЯДОК РАСЧЕТОВ

3.1. Цена неисключительных прав, передаваемых СУБЛИЦЕНЗИАТУ по Договору, составляет _____ (сумма прописью) рублей ___ копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

3.2. Цена Договора включает в себя все обязательные платежи и расходы, связанные с исполнением Договора, в том числе стоимость передаваемых неисключительных прав, все уплачиваемые и взимаемые на территории Российской Федерации налоги, пошлины, сборы, страховые и другие обязательные платежи, стоимость дополнительных услуг, а также затраты по гарантийным обязательствам.

3.3. Оплата производится СУБЛИЦЕНЗИАТОМ по факту предоставления ПРОДУКТОВ, в течение 10 (Десяти) рабочих дней с даты получения счета, выставленного на основании подписанного Сторонами Акта передачи прав.

3.4. Передача неисключительных прав по Договору от СУБЛИЦЕНЗИАРА к СУБЛИЦЕНЗИАТУ оформляется Актом передачи прав, который подписывается Сторонами в течение 10 (Десяти) рабочих дней с момента активации лицензионного ключа.

Без Договора Акт передачи прав не имеет юридической силы.

3.5. В течение 10 (Десяти) рабочих дней с даты заключения Договора СУБЛИЦЕНЗИАР обязан предоставить СУБЛИЦЕНЗИАТУ возможность пользования ПРОДУКТАМИ, права на использование которых передаются ему по Договору, включая предоставление необходимых ключей, паролей доступа и т.п.

3.6. Датой оплаты считается день списания денежных средств с расчетного счета СУБЛИЦЕНЗИАТА.

Датой получения документов считается дата их регистрации в системе документооборота СУБЛИЦЕНЗИАТА.

В первичных учетных документах указывается дата и номер Договора.

4. ПРАВА И ОБЯЗАННОСТИ СУБЛИЦЕНЗИАТА

4.1. СУБЛИЦЕНЗИАТ обязуется:

Выплатить СУБЛИЦЕНЗИАРУ вознаграждение в порядке и размерах, предусмотренных Договором.

Строго придерживаться и не нарушать правил лицензионного использования ПРОДУКТОВ.

Не совершать относительно ПРОДУКТОВ другие действия, нарушающие российские и международные нормы по авторскому праву и использованию программных средств.

5. ПРАВА И ОБЯЗАННОСТИ СУБЛИЦЕНЗИАРА

5.1. СУБЛИЦЕНЗИАР обязуется:

Передать права СУБЛИЦЕНЗИАТУ на условиях, предусмотренных Договором.

Не совершать действия, противоречащие условиям Договора и наносящие ущерб СУБЛИЦЕНЗИАТУ.

5.2. СУБЛИЦЕНЗИАР дает согласие на осуществление Управлением делами Президента Российской Федерации (главным распорядителем средств федерального бюджета) и уполномоченными органами государственного финансового контроля проверок соблюдения порядка, целей и условий предоставления субсидий.

5.3. СУБЛИЦЕНЗИАР вправе в качестве первичных учетных документов использовать универсальный передаточный документ (УПД).

6. ПОРЯДОК ПЕРЕДАЧИ-ПРИЕМА ПРАВ

6.1. Права передаются СУБЛИЦЕНЗИАТУ в виде лицензионного ключа, представляющего собой буквенно-цифровую последовательность символов.

6.2. Способ передачи прав – в электронной форме, на электронную почту itm@ac.gov.ru.

6.3. При условии надлежащего выполнения СУБЛИЦЕНЗИАРОМ своих обязательств СУБЛИЦЕНЗИАТ в течение 10 (Десяти) рабочих дней со дня получения Акта передачи прав подписывает Акт передачи прав и направляет его СУБЛИЦЕНЗИАРУ.

6.4. В случае отказа СУБЛИЦЕНЗИАТА от подписания Акта передачи прав СУБЛИЦЕНЗИАТ делает соответствующую отметку в Акте передачи прав или составляет акт с перечнем недостатков и сроков их устранения. СУБЛИЦЕНЗИАР обязан устранить недостатки в установленные СУБЛИЦЕНЗИАТОМ сроки.

После устранения замечаний СУБЛИЦЕНЗИАР осуществляет передачу права в порядке, предусмотренном п.п. 6.3. - 6.4. Договора.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА

7.1. Договор вступает в силу с даты подписания обеими Сторонами и действует до полного исполнения Сторонами своих обязательств.

7.2. Договор может быть расторгнут по взаимному соглашению Сторон или по вступившему в законную силу решению арбитражного суда.

7.3. СУБЛИЦЕНЗИАТ может расторгнуть Договор в одностороннем внесудебном порядке в случае невыполнения СУБЛИЦЕНЗИАРОМ условий Договора.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. За неисполнение или ненадлежащее исполнение своих обязательств по Договору Стороны несут ответственность, в соответствии с действующим законодательством Российской Федерации.

8.2. В случае просрочки исполнения СУБЛИЦЕНЗИАТОМ обязательства, предусмотренного Договором СУБЛИЦЕНЗИАР вправе потребовать уплату неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. Такая пеня устанавливается Договором в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Банка России от не уплаченной в срок суммы.

8.3. СУБЛИЦЕНЗИАТ освобождается от уплаты неустойки, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине СУБЛИЦЕНЗИАРА.

8.4. В случае невыполнения СУБЛИЦЕНЗИАРОМ предусмотренных Договором обязательств в установленные сроки, СУБЛИЦЕНЗИАТ вправе потребовать уплату пени в размере до 0,5% от цены неисключительных прав по Договору за каждый день просрочки.

Штрафы начисляются за неисполнение или ненадлежащее исполнение СУБЛИЦЕНЗИАРОМ обязательств, предусмотренных Договором, за исключением просрочки исполнения СУБЛИЦЕНЗИАРОМ обязательств, предусмотренных Договором, в размере до 10 % цены неисключительных прав по Договору.

При этом СУБЛИЦЕНЗИАТ из сумм, подлежащих выплате СУБЛИЦЕНЗИАРУ, вправе удерживать суммы штрафных санкций и иных санкций, которые СУБЛИЦЕНЗИАР обязан уплатить СУБЛИЦЕНЗИАТУ в соответствии с разделом 8 Договора за ненадлежащее исполнение условий Договора.

8.5. СУБЛИЦЕНЗИАР освобождается от уплаты пени, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине СУБЛИЦЕНЗИАТА.

9. КОНФИДЕНЦИАЛЬНОСТЬ

9.1. Условия Договора, дополнительных соглашений к нему и иная информация, полученная СУБЛИЦЕНЗИАРОМ в соответствии с Договором, конфиденциальны и не подлежат разглашению СУБЛИЦЕНЗИАРОМ.

10. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ.

10.1. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Договору в случае действия обстоятельств непреодолимой силы, прямо или косвенно препятствующих исполнению Договора, то есть таких обстоятельств, которые независимы от воли Сторон, не могли быть ими предвидены в момент заключения Договора и предотвращены разумными средствами при их наступлении.

10.2. Сторона, подвергшаяся действию таких обстоятельств, обязана немедленно в письменном виде уведомить другую Сторону о возникновении, виде и возможной продолжительности действия соответствующих обстоятельств.

10.3. Наступление обстоятельств, предусмотренных настоящей статьей, при условии соблюдения требований п. 10.2 Договора, продлевает срок исполнения договорных обязательств на период, который в целом соответствует сроку действия наступившего обстоятельства и разумному сроку для его устранения.

10.4. В случае, если обстоятельства, предусмотренные настоящей статьей, длятся более 2 (Двух) месяцев, Стороны проводят переговоры для определения альтернативных способов исполнения Договора.

11. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

11.1. В случае изменения учредительных документов, банковских реквизитов, адресов, Сторона, у которой происходят такие изменения, обязана известить другую Сторону в течение 5 (Пяти) дней с момента изменений, путем направления в ее адрес надлежащим образом оформленного уведомления, без заключения дополнительного соглашения.

11.2. Споры по Договору рассматриваются в претензионном порядке. Стороны устанавливают срок рассмотрения претензий – 15 (Пятнадцать) дней с момента их получения. В случае не достижения соглашения спор передается на рассмотрение в Арбитражный суд города Москвы.

11.3. Любые изменения и дополнения к Договору действительны лишь при условии, что они совершены в письменной форме и подписаны уполномоченными представителями Сторон

11.4. Во всем остальном, что не предусмотрено в Договоре, Стороны руководствуются действующим законодательством Российской Федерации

11.5. Договор составлен в 2-х (двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

11.6. Приложение, указанное в настоящем Договоре и являющееся его неотъемлемой частью:

Приложение № 1 - Спецификация.

АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

СУБЛИЦЕНЗИАТ: **автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации»** Адрес: 107078, город Москва, проспект Академика Сахарова, д. 12, телефон: (495) 632-97-96 ОГРН 1157700000655 ИНН 7708244720 КПП 770801001 ОКПО 94194039 ОКТМО 45378000 Банковские реквизиты: УФК по г. Москве (л/с 711В0011001) Банк: ГУ Центрального Банка РФ по ЦФО БИК 044525000 р/с 40501810345251000279 _____/ /	**СУБЛИЦЕНЗИАР:** _____ / /

Приложение №1
к Договору № _____
от «_____» _____ 2020 г.

СПЕЦИФИКАЦИЯ

на предоставление неисключительных прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

№ п/п	парт номер	Наименование Продукта	Кол-во (шт)	Срок использования	Цена за ед. руб., (без НДС)	Сумма в руб. (без НДС)
1.	PT-MPSIEM-BASE-H1000	MaxPatrol SIEM, базовая лицензия на 1 000 узлов, гарантийные обязательства в течение 1 (одного) года	1	бессрочно	*	*
2.	PT-MPSIEM-SRV	MaxPatrol SIEM Server, гарантийные обязательства в течение 1 (одного) года	1	бессрочно	*	*
3	PT-MPSIEM-AGT	MaxPatrol SIEM Agent, гарантийные обязательства в течение 1 (одного) года	1	бессрочно	*	*
	Итого					*

Цена неисключительных прав, передаваемых СУБЛИЦЕНЗИАТУ по Договору, составляет _____ (сумма прописью) рублей ___ копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.

** Заполняется в соответствии с предложением победителя запроса цен в электронной форме*

Текст, выделенный курсивом, в заявке не воспроизводится.

ТРЕБОВАНИЯ К СИСТЕМЕ

Требования к Системе в целом

Функциональные компоненты программных средств Системы должны поддерживать развертывание как на физическом, так и на виртуальном оборудовании.
Система должна быть построена по модульному принципу и позволять ее использование и установку в различных конфигурациях.
В состав Системы должны входить следующие функциональные компоненты:
компонент управления;
компонент обработки;
компонент хранения;
компонент сбора событий;
компонент управления доступом;
база знаний с экспертизой вендора;
компонент обновления и конфигурирования;
компонент хранения индикаторов компрометации.

Таблица 5 — Требования к функциям компонентов Системы

№ п/п	Наименование компонента	Назначение компонента
	Компонент управления	Компонент управления должен выполнять следующие функции:

№ п/п	Наименование компонента	Назначение компонента
		централизованное хранения конфигурации активов; централизованное управление компонентами системы; оперативное реагирование на инциденты ИБ и обеспечение взаимодействия подразделений организации при расследовании этих инцидентов; автоматизация процесса обнаружения уязвимостей; предоставление графического интерфейса пользователя
	Компонент обработки	Компонент обработки должен осуществлять функции по обработке и хранению событий: агрегацию, нормализацию и корреляцию событий; автоматическое создание инцидентов; привязку событий к активам
	Компонент хранения	Компонент хранения должен осуществлять централизованное хранение информации о событиях — как исходных, так и нормализованных
	Компонент сбора событий	Компонент сбора событий должен обеспечивать сбор событий от различных источников и позволять осуществлять сканирование узлов корпоративной информационной системы (далее - КИС) в режимах черного и белого ящика
	Компонент управления доступом	Компонент управления доступом должен обеспечивать доступ к системе через сервис единого входа, управление пользователями системы и журналирование действий пользователей
	База знаний с экспертизой вендора	База знаний должна обеспечивать получение данных о новых уязвимостях и эксплойтах, данных, необходимых для структурирования сведений, собранных от объектов инфраструктуры, правил обработки событий
	Компонент обновления и конфигурирования	Компонент обновления и конфигурирования должен обеспечивать проверку наличия, загрузку и установку новых версий отдельных компонентов Системы, а также обновление базы знаний
	Компонент хранения индикаторов компрометации	Компонент хранения индикаторов компрометации должен обеспечивать доставку данных об угрозах информационной безопасности и индикаторах компрометации, характерных для отдельной организации в данный момент времени

Система с помощью функциональных компонентов должна обеспечивать реализацию следующих функциональных возможностей:
сбор событий;
управление активами;
обработку событий;
управление событиями;
обнаружение уязвимостей;
управление инцидентами;
отправку уведомлений;
визуализацию и построение отчетов;
обновление;
разграничение доступа пользователей Системы.
Унифицированное информационное взаимодействие между компонентами Системы должно обеспечиваться с использованием шины передачи данных и веб-служб, работающих на стеке протоколов TCP/IP.
Доступ к Системе должен осуществляться через веб-интерфейс.
Система должна предоставлять программный интерфейс (API) для взаимодействия с решениями других производителей.
Система должна поддерживать возможность подключения внешних систем хранения данных.
Целевые показатели системы:
Система должна поддерживать сбор событий не менее чем с 1000 узлов.

Требования к функциям Системы

Функции сбора событий

Компоненты Системы должны обеспечивать удаленный (сетевой) и локальный сбор событий.
Компоненты Системы должны обеспечивать как пассивный (без подключения к источнику), так и активный (с подключением к источнику) сбор событий.
Компоненты Системы должны обеспечивать возможность сбора событий в режиме, близком к режиму реального времени.
Управление сбором событий из различных типов источников должно осуществляться из единой консоли.
Система должна обеспечивать возможность фильтрации и поиска задач сбора данных по их атрибутам.

Учетные данные, необходимые для активного подключения к источникам, должны храниться в единой базе.
Должна быть обеспечена возможность использования одной записи с учетными данными для подключения к различным источникам с целью минимизации трудозатрат на корректировку учетных данных.
Система должна обеспечивать коррекцию времени в событиях от источника без дополнительной настройки источника.
Система должна обеспечивать стабильную работу с событиями, полученными от источников с некорректным временем.
Сбор событий должен быть реализован посредством модулей сбора данных на основе сохраняемых профилей.
В Системе должны быть предусмотрены предустановленные профили для сбора данных.
Пользователи Системы должны иметь возможность создавать собственные профили для сбора данных на базе системных (с возможностью редактирования различных параметров профиля, например, портов подключения, названий и полей таблиц, из которых производится сбор, частоты забора данных, количества передаваемых сообщений).
Система должна обеспечивать сбор событий с использованием следующих механизмов и протоколов:
сенсор в терминах протокола Cisco NetFlow;
сообщения стандарта syslog по протоколам TCP и UDP;
SNMP;
SMB;
WMI;
текстовые файлы в форматах 1CEnterprise8, AccordSucuCsvLog, FtpFileLog, Oracle Listener Log, SharePointServer, WindowsFileLog;
отслеживание изменений в БД следующих схем данных: DeviceLockLog, Dr Web Database, ForefrontEndpointProtectionLog, InfoWatchTrafficMonitor6.1, InfoWatchTrafficMonitorLog, KasperskySecurityCenter, Kontinent_ServerAccessLog, LinterVS_SAVZ, LinterVS_SOA, LinterVS_UD_NSD, LumensionEndpointSecurity, McAfeeEpoLog, McAfeeEpoLog4.5, OdbcLog MSSQL, OdbcLog Oracle, OracleAuditTrail, SCCMDetectSoftware, SCCMDetectUSBDevices, SCCMEvents, SecretNetLog, SecretNeLog_Oracle, SymantecEPMSecurityEvents, SymantecEPMSystemEvents, SymantecEPMVirusAlert, SystemCenterOperationsManager, Vipnet_StateWatcher, ZecurionZGate;
OPSEC LEA;
Windows Event Log;
результаты выполнения команд на сервере по протоколу SSH;
события платформы виртуализации VMware vSphere;
Система должна поддерживать получение данных из источников, указанных в таблице ниже (Таблица 2).
Таблица 6 — Перечень поддерживаемых источников событий

№ п/п	Наименование источника	Версия
Системы аутентификации, авторизации, учета		
	Cisco ACS	5.x
	RSA Authentication Manager	8.2, 8.3
	Avanpost IDM	5.3
Системы предотвращения утечек информации		
	InfoWatch Traffic Monitor	4.1, 6.1, 6.7
	Zecurion zGate (основной журнал)	7
	Zecurion zGate (журнал Zgate Proxy)	7
	«Конфидент», Dallas Lock	8.0, сборка 347.20, ред. K, C
Системы защиты приложений		
	Cisco Email Security Appliance (ESA)	7
	Positive Technologies Application Firewall	—
	McAfee Web Gateway	7.5
Бизнес-приложения		
	Microsoft SharePoint Server	2013
	1С:Предприятие	8.2, 8.3
	New Security Technologies SafeInspect	2.1
Системы управления базами данных		
	Microsoft SQL Server	2005, 2008, 2012, 2014
	Oracle Audit Trail	10g, 11g, 12c
	Oracle Database	10g, 11g, 12c
	Oracle MySQL	5.7.10
	Oracle Net Listener	10g, 11g, 12c
Системы защиты конечных узлов		
	Код безопасности Secret Net	7.6, 7.7
	Код безопасности Secret Net Studio	8.2, 8.3, 8.4
	Код безопасности vGate	2.7, 2.8, 3.0
	ESET Security Management Center	7.0

№ п/п	Наименование источника	Версия
	Kaspersky Administration Kit	8.x
	Kaspersky Endpoint Security	10
	Kaspersky Security Center	8, 9, 10
	Symantec Endpoint Protection	12.1, 14
	Lumension Endpoint Security	4.4
	SmartLine DeviceLock DLP	7.3, 8.1
Антивирусное программное обеспечение		
	Kaspersky Security для Microsoft Exchange Servers	9
	Kaspersky Security для Microsoft SharePoint Server	9
	Kaspersky Security для Linux Mail Server	8.0
	Dr.Web Enterprise Security Suite	6, 10
Системы электронной почты		
	Microsoft Exchange Server	2003, 2007, 2010, 2013, 2016
	Postfix	2, 3
	Sendmail	8.x
Сетевые устройства		
	Avaya (Nortel) ERS	5500
	QTech QSW	3450-28T, 6500-52F, 8300-52F
	Cisco IOS	12.x, 15.x
	Cisco NX-OS	4.x, 5.x, 6.x, 7.x
	Cisco WLC	7.x
	Juniper JunOS	11.x, 12.x, 13.x, 14.x
	HPE Comware Software	5.x, 7.x
	Huawei	VRP 5.110
Системы защиты сети		
	Arbor Networks Peakflow	7.6, 8.x
	WatchGuard FireWare XTMv	11.12.2
	Positive Technologies MaxPatrol 8	—
	Palo Alto Networks PAN-OS	6, 7, 8
	KerioControl Technologies	9.0
	Check Point GAiA OS	76, 77.10, 77.20, 77.30, R80
	S-Terra VPN Gate	4.1
	«Код безопасности», АПКШ «Континент»	3.7
Межсетевые экраны		
	Cisco ASA	8.x, 9.x
	FortiNet Fortigate	5.4.x
	McAfee (Forcepoint) Next Generation Firewall	5.3
Системы обнаружения и предотвращения вторжений		
	Cisco IPS	6.x
	Suricata	3.1
	Snort	2.9, 3
Операционные системы		
	FreeBSD	4.9–9.2
	Microsoft Windows	XP (только WMI), Vista, 7, 8, 8.1, 10, Server 2003 и Server 2003 R2 (только WMI), Server 2008, Server 2008 R2, Server 2012, Server 2012 R2
	Debian	7, 8, 9
	IBM AIX	5.3, 6.1, 7.1
	SUSE Linux Enterprise Service	11.x, 12.x
	CentOS	6.x, 7.x
Прокси-серверы		
	Cisco Web Security Appliance (WSA)	8.0
	Squid	3.0–3.5
	Entensys UserGate Proxy & Firewall	6
	Microsoft Forefront TMG	7.0
Системы виртуализации		
	VMware vSphere Hypervisor (ESXi)	5.5, 6.0, 6.5

№ п/п	Наименование источника	Версия
	VMware vCenter	5.5, 6.0, 6.5
Веб-серверы		
	Apache HTTP Server	2
	Nginx	1.8, 1.9
	Microsoft Internet Information Services (IIS)	6.0, 7.5, 8.5
Системы динамической адресации		
	Microsoft DHCP Server	2008, 2012
	Microsoft DHCP Client	2008, 2012
	Microsoft Wndows DNS Server	2008, 2012
Системы управления обновлениями и конфигурацией		
	Microsoft Windows Server Update Services (WSUS)	Windows Server 2008, 2008R2, 2012, 2012 R2
Удостоверяющие центры		
	Microsoft Certification Authority (CA)	Windows Server 2008, 2008R2, 2012, 2012 R2
	RSA Certificate Manager	6.9
Системы мониторинга сети		
	Infotecs ViPNet StateWatcher	3.2
	Microsoft System Center Operations Manager (SCOM)	2012R2
Системы организации терминального доступа		
	Microsoft Windows Terminal Services	6.3

Система должна позволять подключать источники событий новых типов посредством дополнения множества правил преобразования событий (нормализации, агрегации).
Система должна позволять разрабатывать пользовательские модули сбора для работы с неподдерживаемыми поставщиками программных средств Системы протоколами передачи событий на скриптовом языке Python. Разработка и работа с такими модулями должна осуществляться через интерфейс Системы.
Запуск пользовательских модулей сбора должен осуществляться средствами агента Системы. Запуск модулей сторонними планировщиками не допускается в целях обеспечения информационной безопасности.
Система должна обеспечивать централизованную настройку и мониторинг работы модулей сбора событий из единой консоли управления.
При выполнении иерархической инсталляции Система должна обеспечивать отображение связей между площадками и возможность настройки правил репликации событий в цепочке иерархии.
Система должна обеспечивать возможность мониторинга источников, позволяя отслеживать:
задержку между временем возникновения событий и временем их получения Системой;
количество событий, получаемых в единицу времени.

Функции управления активами

Система должна обеспечивать идентификацию и добавление активов путем:
сбора и анализа событий;
сетевого сканирования для обнаружения узлов сети;
анализа защищенности по методам черного и белого ящика;
анализа сетевого трафика;
добавления актива пользователями (вручную).
Система должна обеспечивать идентификацию сетевых служб, использующих протоколы TCP и UDP в качестве протоколов транспортного уровня.
Система должна обеспечивать выявление и идентификацию активов, функционирующих в момент сканирования.
Система должна обеспечивать сбор идентификационных данных об активах (IP-адреса, имени узла, FQDN). Механизм идентификации должен обеспечивать выявление и корректную работу с кластерными конфигурациями активов.
Система должна обеспечивать выявление и идентификацию доступных в момент сканирования портов, использующих сетевые протоколы транспортного уровня.
Система должна обеспечивать сбор сведений о составе программного и аппаратного обеспечения сканируемого актива.
Система должна обеспечивать сбор параметров конфигурации актива по следующим протоколам удаленного управления: WMI, SAP RPC, SSH, Telnet, ODBC, SNMP, Checkpoint OPSEC.
Система должна обеспечивать автоматическую привязку событий к активам при условии, что в событии содержится идентификационная информация.
Система должна обеспечивать построение иерархии групп активов и управление ею.
Система должна обеспечивать автоматическое определение типа и роли узла по результатам сканирования в режимах черного или белого ящика.
Система должна обеспечивать построение и визуализацию топологии сети на актуальный момент времени на уровне L3 модели OSI.

Система должна иметь следующие механизмы для управления списком активов:
фильтрацию активов по заданному набору атрибутов и их значений с использованием специализированного языка запросов (в том числе с возможностью объединения запросов);
отображение активов, удовлетворяющих условиям пользовательского запроса, в таблице активов и на топологии;
возможность сохранения пользовательских запросов для последующего быстрого доступа к ним;
функции группировки и сортировки активов, анализа данных об активах.
Система должна обеспечивать отображение активов, участвовавших в событии или инциденте, на топологии сети.
Система должна обеспечивать расчет сетевой достижимости между выбранными активами на топологии с учетом протоколов и портов.
Система должна обеспечивать возможность задания активам уровня значимости и использование этой величины при количественной оценке опасности событий ИБ и инцидентов.
Система должна обеспечивать возможность мониторинга доступности активов (узлов, сетевых сервисов и устройств).
Система должна обеспечивать отслеживание изменений конфигурации активов, включая:
просмотр состояния актива на заданный момент времени в прошлом;
сравнение конфигураций актива в разные моменты времени;
экспорт истории конфигурации актива.
Система должна обеспечивать возможность просмотра информации об уязвимостях актива с указанием оценки CVSS и идентификатора CVE.
Система должна позволять объединять активы в динамические группы исходя из собранных данных об их конфигурации. Формирование динамических групп должно осуществляться как на основе пользовательских запросов, так и при помощи интерактивного конструктора запросов.
Система должна позволять добавлять в модель актива пользовательские поля и их описание.
Система должна позволять выполнять экспорт данных об активах в табличный список.

Функции обработки событий

Система должна обеспечивать нормализацию событий с использованием встроенных формул.
Система должна поддерживать возможность создания пользователями собственных формул нормализации.
Система должна обеспечивать агрегацию событий с использованием встроенных правил.
Система должна обеспечивать поддержку мультиязычных событий.
Система должна обеспечивать возможность корреляции событий в режиме, близком к режиму реального времени.
Система должна обеспечивать возможность проверки ранее полученных событий на наличие в них актуальных индикаторов компрометации.
В состав Системы должны входить встроенные правила корреляции, обеспечивающие выявление целенаправленных атак в автоматическом режиме.
В состав Системы должны входить встроенные правила корреляции, обеспечивающие в автоматическом режиме контроль действий пользователей и администраторов, выявление аномалий:
выявление активности на рабочих станциях в ночное время и выходные (праздничные) дни;
контроль VPN-соединений;
контроль выполнения команд, которые могут угрожать информационной безопасности КИС, на серверах и сетевом оборудовании;
контроль учетных записей;
контроль изменения конфигурации на сетевом оборудовании и серверах;
контроль установки и запуска новых сервисов ОС и сетевых служб.
Система должна предоставлять пользователю интерфейс создания пользовательских правил корреляции (визуальный конструктор привил корреляции) и возможность создания пользовательских правил корреляции на основе встроенных системных правил.
Система должна обеспечивать возможность управления списком активных правил корреляции с отображением статистики их срабатывания.
Система должна обеспечивать функцию многоуровневой корреляции, когда результаты срабатывания правил корреляции подаются на вход другому правилу корреляции.
Система должна обеспечивать контроль потребляемой коррелятором памяти и при достижении порогового значения отключать нагружающие ее правила корреляции.
Система должна обеспечивать использование табличных списков при формировании правил корреляции. Пользователю должна быть доступна возможность их создания, удаления и редактирования через графический интерфейс.
Функциональность табличных списков должна позволять выполнять:
контроль времени жизни записей в таблице (TTL);
индексацию выделенных колонок в целях ускорения доступа к записям;
определение первичного ключа таблицы;
импорт и экспорт всего содержимого табличного списка.
При обращении к табличным спискам из правил корреляции должны быть доступны функции:
создания, обновления, удаления строк, а также очистки всей таблицы;
обогащения корреляционного события найденными данными из табличного списка;
выполнения математических функций инкремента, декремента, вычисления максимального, минимального и среднего при вставке данных в табличный список;

выполнения математических функций вычисления максимального, минимального, среднего и подсчета общего числа строк при выборке данных из табличного списка.
Система должна обеспечивать возможность задания правил обогащения событий, поступающих в систему, данными из табличных списков (в том числе данными из репутационных списков).
Система должна обеспечивать хранение исходных и нормализованных событий.

Функции управления событиями

Система должна содержать текстовое описание каждого события, предоставленное экспертами вендора.
Система должна обеспечивать категоризацию событий.
Система должна иметь следующие механизмы для управления списком событий:
фильтрацию событий по группе активов и периоду;
фильтрацию событий по заданному набору атрибутов и их значений с использованием специализированного языка запросов;
сохранение пользовательских фильтров для последующего быстрого доступа к интересующим событиям (с возможностью создания иерархического списка фильтров);
функции группировки и сортировки событий в выводе на экран по всем доступным полям;
анализ данных о событиях с помощью математических операций.

Функции управления инцидентами

Система должна обеспечивать автоматическое и ручное формирование инцидентов при обнаружении критичных с точки зрения пользователя событий.
Система должна обеспечивать импорт инцидентов из специально подготовленных файлов.
Система должна обеспечивать категорирование инцидентов.
Система должна обеспечивать управление автоматической генерацией инцидентов.
Система должна обеспечивать формирование инцидента с автоматической и ручной привязкой к нему событий.
Система должна обеспечивать просмотр и редактирование карточки инцидента.
Для управления списком инцидентов Система должна иметь следующие механизмы:
фильтрации инцидентов по группе активов и периоду;
фильтрации инцидентов по заданному набору атрибутов и их значений с использованием специализированного языка запросов;
фильтрации инцидентов с использованием системных и пользовательских фильтров;
сохранения пользовательских фильтров для последующего быстрого доступа (с возможность создания иерархического списка фильтров);
сортировки инцидентов по времени создания, статусу, критичности, категории, названию.
Система должна обеспечивать возможность построения процесса расследования инцидента: формирования поручений для расследования, определения порядка реагирования и устранения последствий инцидентов, назначения ответственных лиц.
Система должна обеспечивать хранение истории расследования инцидента.
Система должна обеспечивать наличие журнала изменений инцидента для регистрации изменений атрибутов и состояний инцидента.

Функции отправки уведомлений

Система должна обеспечивать возможность формирования и отправки уведомлений (по электронной почте):
об изменении списка активов в Системе;
изменении состава выбранных динамических групп активов (включении, исключении активов);
событиях и инцидентах — при их попадании под системный или пользовательский фильтр;
выходе параметров потока событий за пределы допустимых значений;
выполнении задач сбора данных;
состоянии Системы.
Система должна обеспечивать возможность отправки уведомления об изменении числа активов и изменениях в группах активов с помощью механизма webhook.
Система должна обеспечить индикацию собственного состояния и уведомления в интерфейсе пользователя о сбоях в работе, критичных для штатного функционирования сервисов.

Функции визуализации и построения отчетов

Система должна предоставлять оперативные данные об активах, событиях, инцидентах и мониторинге функционирования Системы в виде графиков, диаграмм и таблиц на виджетах и дашбордах.
Система должна обеспечивать возможность создания и конфигурирования пользовательских дашбордов.
Система должна предоставлять возможность экспорта отчетов как минимум в одном из следующих форматов: PDF, XLSX, CSV.
Система должна обеспечивать отображение следующих статистических данных по инцидентам в графическом формате (на виджетах):
созданные инциденты,
закрытые инциденты за период,
незакрытые инциденты по уровню опасности,
среднее время устранения инцидента.
Система должна обеспечивать выпуск отчетов (стандартных и пользовательских) вручную или по расписанию.

Система должна предоставлять пользователю интерфейс создания пользовательских отчетов с данными об активах, событиях и инцидентах (конструктор отчетов).
Система должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов:
по активам,
событиям,
инцидентам,
мониторингу.
Система должна обеспечивать построение следующих отчетов по активам:
инвентаризация групп пользователей Windows,
инвентаризация аппаратного обеспечения,
инвентаризация операционных систем,
инвентаризация узлов с открытыми портами,
инвентаризация сетевых сервисов,
инвентаризация ресурсов общего доступа,
инвентаризация ресурсов общего доступа по узлам,
инвентаризация программного обеспечения,
инвентаризация пользователей Windows,
инвентаризация служб Windows.
Система должна обеспечивать построение следующих отчетов по инцидентам:
распределение новых инцидентов по времени,
распределение утвержденных инцидентов по времени,
распределение инцидентов в работе по времени,
все открытые инциденты по времени,
распределение разрешенных инцидентов по времени,
распределение закрытых инцидентов по времени,
все завершенные инциденты по времени.
Система должна позволять автоматически обновлять список активов, событий и инцидентов в выводе на экран через определенные промежутки времени.
Графический интерфейс пользователя должен быть реализован по технологии Web.

Функции обновления

Система должна обеспечивать возможность обновления и расширения встроенных баз знаний вендора, в том числе формул нормализации и правил корреляции, в рамках действующей лицензии.
Система должна обеспечивать возможность обновления компонентов Системы без потери накопленных данных.

Функции разграничения доступа пользователей Системы

Система должна обеспечивать идентификацию и аутентификацию пользователей по уникальному идентификатору и паролю.
Система должна обеспечивать идентификацию и аутентификацию пользователей через сторонний LDAP-сервер.
В Системе должна быть реализована модель ролевого доступа, обеспечивающая возможность разрешения или запрета доступа пользователей к информации об определенных узлах (активах).
Система должна обеспечивать регистрацию действий пользователей при работе с компонентами Системы.

СУБЛИЦЕНЗИАТ: **автономная некоммерческая организация «Аналитический центр при Правительстве Российской Федерации»**	**СУБЛИЦЕНЗИАР:**
_____/ /	_____ / /

Приложение № 4
к Документации

ОБОСНОВАНИЕ НАЧАЛЬНОЙ (МАКСИМАЛЬНОЙ) ЦЕНЫ ДОГОВОРА

Предмет договора: на предоставление неисключительных прав на использование программ для ЭВМ - Программные продукты «MaxPatrol SIEM», «MaxPatrol SIEM Server» и «MaxPatrol SIEM Agent» для нужд автономной некоммерческой организации «Аналитический центр при Правительстве Российской Федерации».

1. Используемый метод определения начальной (максимальной) цены договора (далее – НМЦД) с обоснованием: метод сопоставимых рыночных цен (анализа рынка).
Заказчиком при определении НМЦД использовался метод сопоставимых рыночных цен (анализа рынка). Данный метод выбран в качестве приоритетного, применение иных методов определения НМЦД представляется нецелесообразным.

2. Для определения начальной (максимальной) цены договора были использованы следующие ценовые предложения:

- исх. № 33/526-В от 04.12.2020 г., ценовое предложение составляет – 9 212 000,00 рублей, без учета НДС;

- исх. б/н, ценовое предложение составляет – 9 024 000,00 рублей, без учета НДС;

- исх. б/н от 03.12.2020 г., ценовое предложение составляет – 9 118 000,00 рублей, без учета НДС;

Начальная (максимальная) цена договора была определена по минимальному ценовому предложению.

Таким образом начальная (максимальная) цена договора составляет 9 024 000,00 (Девять миллионов двадцать четыре тысячи) рублей 00 копеек, НДС не облагается на основании пп.26 п.2. ст.149 Налогового кодекса Российской Федерации.