ТЕХНИКАЛЫҚ СИПАТТАМА

1273101 сатып алу бойынша
Бағалы ұсыныстарға сұраным тәсілімен

Лот № 1 (20 У, 4589247) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: "Құрық Порты" ЖШС

Ұйымдастырушы: "Құрық Порты" ЖШС

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	20 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	"Check Point брандмауэріне лицензиялық жазылымдарды 12 айға ұзарту."
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Маңғыстау облысы, Қарақия ауданы, Құрық с.о., Құрық с., участок Сарша, строение 636
Жеткізу шарттары	-
Жеткізу мерзімі	01.2027 бастап 12.2027 дейін (қоса алғанда)
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

№ п/п	
1	**Сатып алынатын қызметтердің сипаттамасы**
	CheckPoint брандмауэріне лицензиялық жазылымдарды 12 айға ұзарту. **1.1. Жазылымдарды ұзартуға арналған жабдықтардың (аксессуарларды қоса алғанда) тізбесі:** 1.1.1. Check point брандмауэрлері 1570/1575 моделі (сериялық нөмірлері: 001c7fb13ed5, 001C7FB13F9E, 001C7FB9A447) – 3 дана. 1.1.2. Check point брандмауэрлері 6200 моделі (сериялық нөмірлері: 001c7fc515bc, 001C7FC5F59A) – 2 дана. 1.1.3. 5 Check Point шлюзін басқаруға арналған SMS басқару сервері (сериялық нөмірі: 02BDB0029AAC).

2	**Сатып алынатын қызметтердің талап етілетін функционалдық, техникалық, сапалық, пайдалану сипаттамалары**
	2.1. Жүйенің жалпы сипаттамасы Лицензиялық жазылым келесі буын брандмауэрінің орталықтандырылған басқару жүйесі үшін келесі функционалдылықты ұзартуды қамтамасыз етуі керек: 2.1.1. Оқиғалар журналында индекстелген іздеу; 2.1.2. Ақпараттық қауіпсіздік оқиғаларын хаттамалау; 2.1.3. Келесі буын брандмауэрлеріндегі ережелер мен саясаттарды хаттамалау; 2.1.4. Firewall, IPSEC VPN, IPS, пайдаланушыны сәйкестендіру, мобильді қол жетімділік, DLP, Қолданбаларды басқару, URL сүзу, анти-бот, вирусқа қарсы, Sandbox сияқты барлық біріктірілген шлюз қауіпсіздік қолданбаларында (виртуалды шлюздерді қоса) оқиғаларды жазу; 2.1.5. Firewall, IPSec VPN, IPS, пайдаланушы идентификациясы, мобильді қол жетімділік, DLP, Қолданбаларды басқару, URL сүзу, анти-бот, вирусқа қарсы, Sandbox сияқты барлық қолданбалардағы оқиғалардың корреляциясы; 2.1.6. Оқиғалар тізімін іздеу, оқиғаларды тергеу үшін егжей-тегжейлерді тереңдету; 2.1.7. Алдын ала белгіленген сағаттық, күнделікті, апталық және айлық есептерді, оның ішінде, ең болмағанда, негізгі оқиғаларды, негізгі көздерді, негізгі бағыттарды, негізгі қызметтерді, негізгі көздерді және олардың негізгі оқиғаларын, негізгі бағыттар мен олардың негізгі оқиғаларын, негізгі қызметтер мен олардың негізгі оқиғаларын жасау; 2.1.8. Есептерді электрондық пошта арқылы автоматты түрде тарату, FTP/Веб-серверге жүктеу, сыртқы пайдаланушы есептерін жіберу сценарийін құру мүмкіндігі. 2.1.9. Жазылым келесі буын Enterprise Based Protection брандмауэрлері үшін қолданыстағы функционалдылықты ұзартуды қамтамасыз етуі керек: 2.1.10. Қолтаңба және эвристикалық тексерулерді қолдану арқылы желілік шабуылдардың алдын алу – IPS; 2.1.11. Қолданбалар деңгейінде желілік қауіпсіздік саясатын және қолданбалардағы жеке мүмкіндіктерді іске асыру-Application Control; 2.1.12. Әр түрлі файл түрлері мен олардың мазмұны деңгейінде желілік қауіпсіздік саясатын жүзеге асыру - content Awareness;

	2.1.13. Веб-сайтқа кіруді басқару, фишингтік сілтемелерді автоматты түрде бұғаттау, пайдаланушылар үшін интернетке кіруді шектеу мүмкіндігі, кэштеу арқылы сайттарды жүктеу жылдамдығын азайту-URL Filtering; 2.1.14. Барлық желілік трафикті зиянды файлдар мен нысандарға тексеретін антивирустық шешім-Antivirus; 2.1.15. Ботнеттерді құру және шабуылдаушыға қажетті әрекеттерді жүзеге асыру мақсатында компьютерлерді пайдаланатын зиянды объектілер класынан қорғау бойынша мамандандырылған шешім-Anti-Bot; 2.1.16. Электрондық поштаны кешенді қорғау, барлық пошта хабарларын антивирустық тексеруді, қажетсіз поштаны (спамды) сүзуді және пошта серверлерін әртүрлі шабуылдардан, соның ішінде тым көп электрондық пошта хабарларын жіберу кезінде "қызмет көрсетуден бас тарту" шабуылдарынан қорғауды қамтиды-anti-Spam & Email Security; 2.1.17. DNS протоколының инспекциясы шеңберінде әртүрлі қауіптерді анықтауға мүмкіндік беретін қызмет, соның ішінде DNS Hijacking, DNS Tunneling типті шабуылдар, DGA – DNS Security тетіктерін пайдалана отырып, қауіпсіздік жүйелерін айналып өту әдістері; 2.1.18. Эксплуатация кезеңінде зиянды бағдарламаны анықтауға мүмкіндік беретін Механизм. Файлдарды корпоративтік желіге кірмес бұрын зиянды әрекеттерді анықтау үшін арнайы виртуалды ортада іске қосу арқылы тексеру-Threat Emulation; 2.1.19. Ықтимал қауіпті белсенді мазмұнды және ендірілген нысандарды жоятын, ықтимал қауіптерді жою үшін файлдарды қайта құратын және бизнес-процесті қолдау үшін пайдаланушыларға тазартылған мазмұнды лезде жеткізетін Механизм-Threat Extraction; 2.1.20. Әр түрлі желі сегменттері арасында қашықтан қосылуды жүзеге асыру және қорғалған IPSec протоколы арқылы соңғы пайдаланушыларды желіге қосу. Сондай-ақ, Layer – 3 VPN және SSL VPN-IPSec VPN, Mobile Access қоса алғанда, мобильді құрылғыларды корпоративтік желіге қосу (мобильді құрылғылардан кемінде 5 бір мезгілде қосылу) 2.1.21. Нақты уақыттағы веб-сайттарға белгісіз және белгілі фишингтік шабуылдардың алдын алу-Zero Phishing;

Қол қойған	Измуратов Олжас Амандыкович
Қол қойылған күні	25.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1273101
способом Запрос ценовых предложений

Лот № 1 (20 У, 4589247) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Порт Курык"

Организатор: Товарищество с ограниченной ответственностью "Порт Курык"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	20 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	"Продление лицензионных подписок на межсетевые экраны Check Point сроком на 12 месяцев."
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Мангистауская область, Каракиянский район, Курыкский с.о., с.Курык, участок Сарша, строение 636
Условия поставки	-
Срок поставки	с 01.2027 по 12.2027 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

№ п/п	
1	**Описание закупаемых услуг**
	Продление текущих лицензионных подписок на межсетевые экраны следующего поколения (NGFW) Check Point сроком на 12 месяцев. **1.1. Перечень оборудования (включая аксессуары) для продления подписок:** 1.1.1. Межсетевые экраны Chek Point модель 1570/1575 (серийные номера: 001C7FB13ED5, 001C7FB13F9E, 001C7FB9A447) – 3 шт. 1.1.2. Межсетевые экраны Chek Point модель 6200 (серийные номера: 001C7FC515BC, 001C7FC5F59A) – 2 шт. 1.1.3. Security Management Server (SMS) - сервер для управления 5 шлюзами Check Point (серийный номер: 02BDB0029AAC).

2	**Требуемые функциональные, технические, качественные, эксплуатационные характеристики закупаемых услуг**
	2.1. Общая характеристика, описание системы. Лицензионная подписка должна обеспечивать продление следующего функционала для системы централизованного управления межсетевыми экранами следующего поколения: 2.1.1. Индексированный поиск в журнале событий; 2.1.2. Протоколирования событий информационной безопасности; 2.1.3. Протоколирование правил и политик на межсетевых экранах следующего поколения; 2.1.4. Протоколирование событий во всех интегрированных приложениях безопасности на шлюзе (включая виртуальные шлюзы), включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрацию, Anti-Bot, Anti-Virus, Sandbox; 2.1.5. Корреляция событий из всех приложений, включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрация, Anti-Bot, Anti-Virus, Sandbox; 2.1.6. Поиск внутри списка событий, углубление в детали для расследования инцидентов; 2.1.7. Генерация предопределенных ежечасных, ежедневных, еженедельных и ежемесячных отчетов, в том числе, как минимум: Основные события, Основные источники, Основные пункты назначения, Основные сервисы, Основные источники и их основные события, Основные пункты назначения и их основные события, и Основные сервисы, и их основные события; 2.1.8. Автоматическое распространение отчетов по электронной почте, загрузка на FTP/Веб-сервер, возможность создания скрипта рассылки внешних пользовательских отчетов. 2.1.9. Подписка должна обеспечивать продление существующего функционала для межсетевых экранов следующего поколения Enterprise Based Protection: 2.1.10. Предотвращение сетевых вторжений за счет использования сигнатурных и эвристических проверок сетевых вторжений за счет использования сигнатурных и эвристических проверок – IPS; 2.1.11. Реализация политик сетевой безопасности на уровне приложений и отдельных функций в приложениях – Application Control; 2.1.12.Реализация политик сетевой безопасности на уровне различных типов файлов и их содержимого – Content Awareness; 2.1.13. Управление доступом к веб-сайтам, автоматическая блокировка фишинговых ссылок, возможность разграничения доступа в интернет для пользователей, сокращение скорости загрузки сайтов путем кеширования – URL Filtering; 2.1.14. Антивирусное решение, проверяющее весь сетевой трафик на наличие вредоносных файлов и объектов -

	Antivirus; 2.1.15. Специализированное решение по защите от класса вредоносных объектов, использующих компьютеры в целях построения ботнетов и реализации нужных злоумышленнику действий – Anti-Bot; 2.1.16. Комплексная защита электронной почты, включает в себя антивирусную проверку всех почтовых сообщений, фильтрацию нежелательной почты (спама) и защиту почтовых серверов от различных атак, в том числе от атак типа «отказ в обслуживании» при отправке чрезмерно большого числа почтовых сообщений – Anti-Spam & Email Security; 2.1.17. Сервис, позволяющий идентифицировать различные угрозы в рамках инспекции протокола DNS, включая атаки типа DNS Hijacking, DNS Tunneling, техники обхода систем безопасности с использованием механизмов DGA – DNS Security; 2.1.18. Механизм, позволяющий обнаруживать вредоносное ПО на этапе эксплойта. Проверка файлов путем их запуска в специальной виртуальной среде для обнаружения вредоносного поведения, прежде чем они попадут в корпоративную сеть – Threat Emulation; 2.1.19. Механизм, который удаляет потенциально опасный активный контент и встроенные объекты, реконструирует файлы для устранения потенциальных угроз и моментально доставляет очищенный контент пользователям для поддержания бизнес-процесса – Threat Extraction; 2.1.20. Реализация удаленных подключений между различными сегментами сетей и подключение конечных пользователей к сети по защищенному протоколу IPSec. А также, подключение мобильных устройств к корпоративной сети (минимум 5 одновременных подключений с мобильных устройств), включая в себя Layer-3 VPN и SSL VPN – IPSec VPN, Mobile Access 2.1.21. Предотвращение неизвестные и известные фишинговых атак на веб-сайты в режиме реального времени – Zero Phishing;

Подписал	Измуратов Олжас Амандыкович
Дата подписания	25.11.2026