Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қарағанды қаласы әкімінің аппараты" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қарағанды қаласының мемлекеттік активтер және сатып алу бөлімі" мемлекеттік мекемесі
Конкурстың №:	№ 16391272-2
Конкурстың атауы:	Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Лоттың нөмірі:	№ 82829165-ОК1
Лоттың атауы	Ақпараттық жүйені қостау және техникалық қолдау көрсету бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620230.000.000001
Қызметтің атауы:	Ақпараттық жүйені қостау және техникалық қолдау көрсету бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	26000000
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	26000000
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	2026 жыл
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	10
Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша сатып алынатын қызметтердің техникалық ерекшелігі. Өнім беруші АҚ-ның туындайтын инциденттері бойынша Тапсырыс берушіні мониторингілеу және хабардар ету жөніндегі жұмыстарды қамтамасыз ету үшін әлеуетті өнім берушіде бар ресурстар (адами, аппараттық-бағдарламалық және өзге де) арқылы ОӘБ қызметін көрсетуге міндеттенеді. Ағымдағы КО шеңберіндегі қызметтер белгіленген сипаттамаларға сәйкес келуі немесе асып кетуі керек. Консультациялық қызметтер көрсету жөніндегі қызметтер Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасы және ҚР СТ ISO/IEC 27001 шеңберінде іске асырылады. Қызмет көрсету мерзімі: 2026 жылғы 31 желтоқсанға дейін. Қызмет көрсету орны: "Қарағанды қаласы әкімінің аппараты" ММ, Н. Назарбаев даңғылы, 39. Қызмет көрсету кезеңінде қызмет көрсету үшін Орындаушы пайдаланатын бағдарламалық қамтамасыз ету мен жабдыққа техникалық қолдаудың/ жазылудың болуы; Платформаның келесі параметрлермен жұмыс істеуін қамтамасыз ету: Платформаға қызмет көрсету мерзімі - 24/7/365; Бір айдағы технологиялық терезелер саны-1 - ден аспайды; Тоқтап қалу туралы хабарлама - кемінде 60 минут; Технологиялық терезенің максималды ұзақтығы - 6 сағаттан аспайды; Технологиялық терезе туралы хабарлама - 3 жұмыс күні. Көрсетілетін қызметтердің техникалық және әкімшілік параметрлері: АҚ және желілік пакеттердің кіріс оқиғаларын өңдеу және талдау; Секундына өңделетін оқиғалар саны - 2 500 EPS; Көздердің қосылатын саны-шектелмейді; Қосылатын оқиға көздерінің саны - шектелмейді; Тапсырыс берушінің қызметкерлері үшін оқиғаларды өңдеу жүйесіне қол жеткізу - кемінде 2 пайдаланушы; ОӘБ жүйесінде Жедел қол жеткізу үшін оқиғаларды сақтау - кемінде 180 күн. Корреляция ережелеріне сәйкес нақты уақыттағы оқиғаларды талдау (кем дегенде 400 ереже); Қауіпсіздік оқиғаларын мұрағаттық сақтау – 3 жыл; Жұмыс режиміндегі жедел мониторинг 24/7/365; ОӘБ жүйесінде ақ инцидентіне автоматты түрде қалыптасқан күдікті тіркеген сәттен бастап жұмысқа қабылдау уақыты: жоғары сыни - 15 минутқа дейін, орташа сыни - 15 минутқа дейін, төмен сыни - 60 минутқа дейін; 24/7/365 жұмыс режимінде АҚ оқиғасын бағалау, санаттау және хабарлау; Жұмысқа қабылданған сәттен бастап ақ оқиғасын бағалау, санаттау және хабарлау уақыты: жоғары сыни - 15 минутқа дейін, орташа сыни - 15 минутқа дейін, төмен сыни - 60 минутқа дейін; Қарсы іс - қимыл бойынша ұсынымдар қалыптастыра отырып, ақ инциденттерін талдау және тергеу - 2 сағат; 100 Ережеге дейін қызмет көрсету кезеңінде қосымша корреляция ережелерін әзірлеу. "Қазақстан Республикасының кейбір заңнамалық актілеріне ақпараттық қауіпсіздік, ақпараттандыру және цифрлық активтер мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы "Қазақстан Республикасының 2023 жылғы 11 желтоқсандағы № 44-VIII Заңына сәйкес мемлекеттік органдардың ақпараттандыру объектілерінің меншік иелері немесе иелері: Интернетке қол жеткізе алмайтын ақпараттандыру объектілерін қоспағанда, ақпараттандыру

	объектілерін өзара іс-қимыл бағдарламасына қосу; мемлекеттік органдардың ақпараттандыру объектілері бойынша өзара іс-қимыл бағдарламасында тіркелген анықталған осалдықтарды жою; Әлеуетті өнім берушіде ОССБ қызметтерін толыққанды көрсету үшін сертификатталған мамандардың болуы. Қызметтер тізімі: * техникалық қолдау; * техникалық қызмет көрсету; * есептеу қуатын басқару. * виртуалды серверлер мен инфрақұрылымды басқару; * барлық ОЦИБ қызметтерінің жұмысын қамтамасыз ететін виртуалды машиналардың өнімділігін бақылау; * АҚ оқиғаларды басқару жүйесін басқару (SIEM-жүйелер); * ҰБАО-мен интеграциялау үшін серверді дайындау; * Ubuntu үшін репозиторий серверін орнату және басқару; * Windows үшін репозиторий серверін орнату және басқару; Қызметтердің сипаттамасы: Ақ оқиғаларының мониторингі және мониторинг нәтижелерін талдау, Тапсырыс берушінің ақпараттандыру объектілерінің ИКИ. Әлеуетті өнім берушінің қызмет шеңберінде АҚ оқиғаларын жинау және сақтау үшін жабдықты (серверді) және БҚ ұсынуы. Тапсырыс берушінің ат инфрақұрылымында АҚ оқиғаларын мониторингілеу үшін аппараттық-бағдарламалық кешенді орнату; Тапсырыс беруші мен ОЦИБ платформасы арасында қорғалған байланыс арнасын орнату, желілік және қауіпсіздік параметрлерін орнату; Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ "электрондық үкімет" ақпараттандыру объектілерінің және ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларын бекіту туралы бұйрығының 12-бабында айқындалған жазбалардың форматтары мен түрлеріне сәйкес қауіпсіздік оқиғаларын қалыптастыруға оқиғалар көздерін баптау оқиғаларды жинау коллекторы; Оқиғаларды тіркеу журналдарының уақытын уақыт көзі инфрақұрылымымен синхрондауды орнату; Тапсырыс берушінің инфрақұрылымына оқиғаларды корреляциялау ережелерін әзірлеу және бейімдеу; АҚ оқиғаларының мониторингі және талдауы 24/7; Тапсырыс берушіні оқшаулау бойынша ұсынымдармен АҚ анықталған бұзушылықтар мен инциденттер туралы хабардар ету; Siem жүйесінің бақылау консолі мен қауіпсіздік оқиғаларына қол жеткізуді ұйымдастыру; АҚ ақпараттандыру объектілерінің АҚ-обеспечения, АҚ-ның қауіп-қатерлері мен инциденттерін қамтамасыз ету үшін қажетті ақпаратпен алмасу бойынша ҰҚКҰК-мен өзара іс-қимыл жасау; Тапсырыс беруші тарапынан заңнамалық талаптармен айқындалған кезең ішінде (3 ай - жедел қол жеткізу, 3 жыл - мұрағаттық) қауіпсіздік оқиғаларын жинауды, шоғырландыруды және сақтауды ұйымдастыру; Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу. Оқиғалар мониторингі қызметін көрсету кезеңіне жауапкершілік аймақтарын бөлу: Қызмет шеңберінде АҚ оқиғаларын жинау және сақтау үшін жабдықты (серверді) және БҚ ұсыну Тапсырыс берушінің ат инфрақұрылымында аппараттық-бағдарламалық кешенді орнату-әлеуетті өнім беруші; Тапсырыс беруші мен ОӘБ платформасы арасында қорғалған байланыс арнасын орнату, Желі параметрлерін және қауіпсіздік

	параметрлерін жүргізу – Тапсырыс беруші, әлеуетті өнім беруші; Қауіпсіздік оқиғаларын қалыптастыруға арналған оқиғалар көздерін заңнамалық талапта айқындалған жазбалардың форматтары мен түрлеріне сәйкес баптау және оқиғаларды жинау коллекторына жіберу - Тапсырыс беруші, әлеуетті өнім беруші; Оқиғаларды тіркеу журналдарының уақытын уақыт көзі инфрақұрылымымен синхрондауды орнату - әлеуетті жеткізуші; Тапсырыс берушінің инфрақұрылымына оқиғаларды корреляциялау ережелерін әзірлеу және бейімдеу - Тапсырыс беруші, әлеуетті өнім беруші; АҚ оқиғаларын мониторингілеу және талдау 24/7 - әлеуетті өнім беруші; Тапсырыс берушіні оқшаулау бойынша ұсынымдармен АҚ анықталған бұзушылықтар мен инциденттер туралы хабардар ету - әлеуетті өнім беруші; Жүйенің Siem бақылау консолі мен қауіпсіздік оқиғаларына қол жеткізуді ұйымдастыру-әлеуетті жеткізуші; Ақпараттандыру объектілерінің АҚ – обеспечения, АҚ-ның қауіп-қатерлері мен инциденттерін қамтамасыз ету үшін қажетті ақпаратпен алмасу бойынша ҰҚКҰК-пен өзара іс-қимыл-әлеуетті өнім беруші; Қауіпсіздік оқиғаларын жинауды, шоғырландыруды ұйымдастыру - әлеуетті өнім беруші; Тапсырыс беруші тарапынан заңнамалық талаптармен айқындалған кезең ішінде (3 ай - жедел қол жеткізу, 3 жыл - мұрағаттық) қауіпсіздік оқиғаларын сақтауды ұйымдастыру; Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу – әлеуетті өнім беруші; Тапсырыс берушінің алаңында да, тапсырыс берушінің алаңында да орнатылған АҚ оқиғаларын басқару ішкі жүйесінің құрамдас бөліктерінің жай-күйін мониторингтеу - әлеуетті өнім беруші; АҚ оқиғаларын басқару ішкі жүйесінің дұрыс жұмыс істеуін қамтамасыз ету-әлеуетті өнім беруші; Алаңдар арасында ақпаратты берудің қорғалған арналарының жұмысқа қабілеттілігін қамтамасыз ету - Тапсырыс беруші және әлеуетті өнім беруші; ОӘБ ұсынымдарын орындау және Ақ инциденттеріне уақтылы ден қою – Тапсырыс беруші; Серверлік, коммуникациялық және компьютерлік жабдықтардың, сондай – ақ мониторинг аймағына кіретін ақпараттық жүйелердің өзекті тізбесін ұсыну - Тапсырыс беруші. Осалдықтарды бақылау және мониторинг нәтижелерін талдау: Әлеуетті өнім берушінің қызмет шеңберінде АҚ оқиғаларын жинау және сақтау үшін жабдықты (серверді) және БҚ ұсынуы; Тапсырыс берушінің ат инфрақұрылымында аппараттық-бағдарламалық кешенді орнату; Тапсырыс беруші мен ОЦИБ платформасы арасында қорғалған байланыс арнасын орнату, желілік және қауіпсіздік параметрлерін орнату; Қауіпсіздік сканерінің тұтынушы жағында орналастыру және орнату; Тоқсан сайын кемінде бір рет желіні тоқсан сайын сканерлеу, Тапсырыс берушінің сыртқы және ішкі периметріндегі осалдықтарды аспаптық іздеу; Сканерлеу нәтижесінде алынған мәліметтерді талдау және бағалау, қауіптер деңгейі бойынша осалдықтарды жіктеу, жою бойынша ұсынымдар дайындау, анықталған осалдықтар және оларды жою шаралары туралы есепті қалыптастыру; Есепті Тапсырыс берушіге жіберу (ай сайын); АҚ ақпараттандыру объектілерінің АҚ-обеспечения, АҚ-ның қауіп-қатерлері мен инциденттерін қамтамасыз ету

	үшін қажетті ақпаратпен алмасу бойынша ҰҚКҰК-мен өзара іс-қимыл жасау; Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу; Қызмет көрсету кезеңіне жауапкершілік аймақтарын бөлу осалдықтар мониторингі: Қызмет шеңберінде АҚ оқиғаларын жинау және сақтау үшін жабдықты (серверді) және БҚ ұсыну; Тапсырыс берушінің АЖ-да аппараттық – бағдарламалық кешенді орнату - Тапсырыс беруші және әлеуетті өнім беруші; Тапсырыс беруші мен ОӘБ платформасы арасында қорғалған байланыс арнасын орнату, желілік және қауіпсіздік параметрлерін орнату - Тапсырыс беруші және әлеуетті өнім беруші; Қауіпсіздік сканерінің тұтынушы жағында орналастыру және орнату-тұтынушы және әлеуетті жеткізуші; Тапсырыс берушімен техникалық ерекшелікте айқындалған тәртіппен желіні осалдыққа сканерлеу; Сканерлеу нәтижесінде алынған мәліметтерді талдау және бағалау, қауіптер деңгейі бойынша осалдықтарды жіктеу, жою бойынша ұсынымдар дайындау, анықталған осалдықтар және оларды жою шаралары туралы есепті қалыптастыру - әлеуетті өнім беруші; Есепті Тапсырыс берушіге жіберу-әлеуетті өнім беруші (ай сайын); Ақпараттандыру объектілерінің АҚ – обеспечения, АҚ-ның қауіп-қатерлері мен инциденттерін қамтамасыз ету үшін қажетті ақпаратпен алмасу бойынша ҰҚКҰК-пен өзара іс-қимыл-әлеуетті өнім беруші; Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу – әлеуетті өнім беруші; ОӘБ ұсынымдарын орындау және Ақ инциденттеріне уақтылы ден қою – Тапсырыс беруші; Серверлік, коммуникациялық және компьютерлік жабдықтардың, сондай – ақ мониторинг аймағына кіретін ақпараттық жүйелердің өзекті тізбесін ұсыну - Тапсырыс беруші; Тапсырыс беруші мен Орындаушының алаңдары арасында ақпаратты берудің қорғалған арналарының жұмыс істеу қабілетін қамтамасыз ету - Тапсырыс беруші және әлеуетті өнім беруші. Оқиғаларды бақылауға арналған аппараттық - бағдарламалық кешенге қойылатын талаптар: Жүйе оның барлық компоненттері мен функционалдығын бірыңғай Веб-интерфейс арқылы орталықтандырылған басқаруды қамтамасыз етуі керек; Жүйеде желідегі активтерді анықтау мен жіктеудің кіріктірілген функционалы болуы керек; Жүйе өндірушінің қосымшалар дүкені арқылы қосымша қосымшаларды орнату арқылы өзінің функционалдығын кеңейте алуы керек, сонымен қатар өндіруші жаңартатын кіріктірілген дайындық базасы болуы керек; Жүйеде аномальды пайдаланушы әрекетін анықтайтын функционалдылық болуы керек (user Behavior Analytics); Жүйе компоненттер арасындағы байланысты шифрлай алуы керек; Жүйе аутентификацияны қамтамасыз ету үшін үшінші тарап жүйелерімен (LDAP, AD) біріктірілуі керек; Жүйе веб-пайдаланушы интерфейсі арқылы жүйені басқаруға, аналитикалық есептер мен ережелер жасауға мүмкіндік беруі керек; Жүйе жүйенің кез-келген бөлігі істен шыққан кезде жүйенің жеке компоненттерінің жұмысына кепілдік беруі керек. (Мысалы, орталық консоль істен шығады, бірақ үй коллекторлары жұмысын жалғастыруда); Жүйеде конфигурацияның сақтық көшірмесін жасаудың Автоматты процесі (Сақтық көшірме) және GUI-ден конфигурацияны қалпына

	келтіру (қалпына келтіру) мүмкіндігі болуы керек; Жүйе әртүрлі көп сатылы желілік құрылғылардан стандартты оқиға өрістерін (пайдаланушы имен, IP мекенжайлары, хост атаулары, оқиға көзі құрылғылары) қалыпқа келтіруі керек. Қалыпқа келтіру қосымша конфигурациясыз жүргізілуі керек; Жүйе алдын ала қосымша конфигурациясыз оқиғаларды стандартты санаттауды қамтамасыз етуі керек; Жүйе одан әрі тергеулерде пайдалану үшін оқиғалар туралы ақпаратты бастапқы түрінде де, қалыпқа келтірілген түрде де сақтай алуы керек; Жүйе бастапқыда қолдау көрсетілмейтін және параметрлермен қамтамасыз етілмеген өрістерден деректерді өңдей және қалыпқа келтіре алуы керек; Жүйе оқиғаларды нақты уақыт режимінде, белгілі бір уақыт аралығында, пайдаланушы алдын ала орнатқан сүзгілер бойынша талдауды қамтамасыз етуі керек; Жүйе қажет болған жағдайда оқиғалар туралы қосымша ақпарат алуға мүмкіндік беруі керек; Жүйе барлық оқиғалар туралы есеп беруі керек, есеп беру шешім қолданушылары үшін веб-интерфейс арқылы қол жетімді болуы керек; Жүйеде өзін өзі конфигурациялау және жеке есептерді жасау үшін есептерді теңшеу шебері болуы керек; Жүйе желідегі әртүрлі сегменттер мен жүйелер бойынша белгілі бір уақыт аралығында жасалған есептердің мысалдарын ұсынуы керек; Жүйеде Тапсырыс берушінің әдеттегі бизнес талаптары үшін кіріктірілген есептер болуы керек; Жүйе өзара әрекеттеспейтін әртүрлі көздерден ақпараттың корреляциясын қамтамасыз етуі керек; Жүйе ескертулерді теңшеу шеберін қамтамасыз етуі керек, анықталған ауытқулар мен мінез-құлықты талдау мен өзгерістерге негізделген ескертулерді қамтамасыз етуі керек, алдын-ала орнатылған саясат туралы ескертулерді қамтамасыз етуі керек (мысалы, тыйым салынған трафикті анықтаған кезде); Жүйе қосымша қауіпсіздік деректерін (географиялық орналасуы, белгілі ботнет, осалдық, тарату арналары және т.б.) байланыстыра алуы керек. Қосымша жүйелерді, үшінші тарап әзірлеушілерін қоспай деректерді автоматты түрде жинау; Жүйе бақыланатын желідегі құрылғыдан журналдар кіруді тоқтатқан жағдайда әкімшіге ескертуі керек (мысалы, х минут ішінде серверден журналдар жоқ); Жүйе әр түрлі типтегі құрылғылар мен жүйелерден ақпараттың корреляциясын қамтамасыз етуі керек, сонымен қатар барлық құрылғыларды автоматты түрде анықтаудың және оларды жүйелер кластары бойынша түгендеудің кіріктірілген функционалдығын қамтамасыз етуі керек (мысалы, пошта серверлері, мәліметтер базасының серверлері және т. б.).; Жүйе басқа көздерден алынған қосымша мәліметтер негізінде белгілі бір оқиғалар тізбегі бойынша корреляцияны қамтамасыз етуі керек; Жүйе бағдарламалық жасақтаманы жаңарту мүмкіндігін қолдауы керек. Жүйе келесі форма факторларын қолдауы керек: виртуалды апплинг, бағдарламалық жасақтама (өзінің аппараттық қуатына орнату үшін); Жүйе қосымша лицензияларды сатып алу немесе қолданыстағы компоненттерді ауыстыруды қажет етпестен архитектураға жаңа компоненттерді қосу арқылы бағдарламалық жасақтаманың функционалдығын оңай кеңейтіп, кеңейтуі керек. Желі қызметін

	бақылау: Жүйе трафикке мінез-құлық талдауын жүргізе білуі керек және берілген өзгеру шектеріне сәйкес өзгерістер туралы есеп бере алуы керек; Жүйе желінің логикалық дизайнына сәйкес трафиктің бөлінуін қолдауы керек, желідегі трафик ағындарының шығу тегі мен мақсатын, оның ішінде нақты уақыт режимінде географиялық аймақтарды анықтауы керек; Жүйе Интернетке кіретін/келетін/келетін жергілікті трафик пен трафик үшін тәуелсіз профильдерді бөліп, құруы керек, таңдау үшін кез-келген трафик ағынының параметрлерін қолдана отырып, пайдаланушы профильдерін құруды қамтамасыз етуі керек. Жүйе IP мекенжайы, IP мекенжайлар тобы, IP жұптарының көзі/тағайындалған орны және т. б. негізінде трафикті ұсынуды қолдауы керек.; Жүйе желідегі қолданба әрекетін бақыланатын құрылғыдағы қауіпсіздік оқиғасымен контекстік түрде байланыстыра алуы керек; Нақты уақыттағы жүйе анықталған қауіпсіздік оқиғаларын желідегі активтер туралы біліммен контексттік байланыстыруы, активтің салыстырмалы маңыздылығына сәйкес анықталған қауіпсіздік оқиғаларының басымдылығын автоматты түрде анықтауы, анықталған қауіпсіздік оқиғасының активтердің осалдығына қатысты ауырлығын анықтауы керек. Тәуекелдерді басқаруға қойылатын талаптар: Жүйе конфигурация файлын құрылғыдан көшірмей кемінде 50 құрылғыдан коммутаторлардың, маршрутизаторлардың, брандмауэрлердің және IPS конфигурацияларын жинауды және қалыпқа келтіруді қамтамасыз етуі керек; Жүйе конфигурация туралы ақпаратты келесі жабдықтан алуы керек: CheckPoint, Cisco CatOS, Huawei, Cisco IOS, Cisco Nexus, Cisco ASA, f5 BigIP, Fortinet FortiOS, HP ProVision, IBM ISS GX, IBM ISS SiteProtector, Juniper JunOS, Juniper Screen OS, McAfee Sidewinder, Nokia ipso, Paloalto Pan - os, SourceFire 3D, TIPPINGPOINT IPS, және generic SNMP. Келесі қосылу әдістерін міндетті қолдау: SSH, Telnet, https \ http, SCP, FTP \ SFTP \ TFTP, SNMP, CPSMS, SQL, NetConf. Кез келген қосылым портын орнату мүмкіндігін міндетті қолдау; Жүйе деректерді жинау үшін келесі аутентификация параметрлерін орнатуы керек: Username, пароль, SNMP get community, SNMP v2/v3, opsec entity SIC, opsec application object SIC, OPSEC SSL сертификаты; Осалдықтарды басқаруға қойылатын талаптар: Жүйе кем дегенде 1024 желі активтері үшін осалдықтарды басқару процесін қамтамасыз етуі керек; Жүйе активтердің шексіз саны үшін активтерді түгендеу мақсатында сканерлеуді қамтамасыз етуі керек; Осалдықтар туралы ақпарат қосымша қосымшаларды немесе кеңейтімдерді орнатпай ақ Siem жүйесінің интерфейсі арқылы қол жетімді болуы керек; Осалдықтарды басқару жүйесі деректерді пайдалануы керек SIEM осалдықтарды түзету процесінің басымдылығын қамтамасыз ету үшін жүйелер мен конфигурацияны басқару жүйелері; Табылған осалдықтар туралы деректер оқиғаларды анықтау үшін Siem корреляциялық ережелерінің іске қосылуына автоматты түрде әсер етуі керек; Әрбір осалдық актив иесіне автоматты түрде бекітілуі керек және табылған осалдықты түзету үшін уақыт аралығын орнату және оны автоматты түрде жою мүмкіндігі берілуі

	керек. Актив иесіне мыналар арқылы хабарлау қажет: электрондық пошта немесе Siem жүйесінің интерфейсі; Жүйе сканерлеу процесін автоматты түрде іске қосуға мүмкіндік беруі керек: кез-келген ақпараттық қауіпсіздік оқиғалары/инциденті, желідегі жаңа активті келесі мәліметтер негізінде анықтау: оқиғалар журналдары (logs), NetFlow деректері, jFlow деректері, sflow деректері, ipfix деректері, активтің ОЖ конфигурациясын өзгерту, немесе деңгейінде жаңа есептік жазба құру Актив ОЖ; Жүйе кесте бойынша инфрақұрылымды ішкі және сыртқы сканерлеудің функционалдығын қамтамасыз етуі керек; Сканерлеу саясаттары сканерлеу түріне (Web Scan, PCI Scan, Patch Scan, Discovery Scan, Database Scan, Full Scan), сондай-ақ жаңа сканерлеу саясаттарын немесе реттелетін үлгілерді жасау мүмкіндігіне сәйкес орнатылуы керек; Сканерлеу түрін анықтау керек: сканерлеу ХАТТАМАСЫ, сканерлеу порттарының ауқымы және сканерлеу активтерінің топтары; Осалдықтарды басқару жүйесі үшінші тарап қолданбаларын, дерекқорларды, қосымша интерфейстерді, терезелерді немесе басқа виртуалды құрылғыларды: IBM Guardium, AXIS Scanner, Beyond Security avds, digital Defence inc.іске қосуды және пайдалануды қажет етпей, веб - интерфейс арқылы инфрақұрылымдық интеграция арқылы келесі сканерлер үшін кесте бойынша сканерлеуді іске қосу және ақпаратты автоматты түрде алу параметрлерін орнатуға мүмкіндік беруі керек. AVS, eEye REM Scanner, FoundScan Scanner, SiteProtector, BigFix, Juniper NSM Profiler, McAfee VM, Microsoft SCCM, nCircle IP360 Scanner, Nessus Scanner, NMap Scanner, Outpost24 Vulnerability Scanner, Positive Technologies MaxPatrol, Qualys Detection Scanner, Qualys Scanner, Rapid7 NexPose Scanner, Saint Scanner, SecureScout Scanner, Tenable Security Center; Веб-қосымшаларды сканерлеу кезінде Open Web Application Security Project TOP 10 таксономияларына сәйкес осалдықтарды анықтауға мүмкіндік беретін эвристикалық талдау әдістерін қолданыңыз; Бірыңғай Siem интерфейсі арқылы пайдаланушы келесі мүмкіндіктерге ие болуы керек: Құрылғыларды, веб-қосымшаларды, ішкі желілерді және сыртқы периметрді сканерлеуді іске қосыңыз; Құрылғыларға, веб-қосымшаларға, ішкі желілерге және сыртқы периметрге арналған икемді сканерлеу сценарийлерін теңшеңіз, мысалы:әр 3 күн сайын, сағат 13.00-де сканерлеу; "Сканерлеу тереңдігін" теңшеңіз, мысалы - әкімші өкілеттіктерін пайдалану немесе онсыз. Үйлесімділік: Жүйенің барлық компоненттері бір жүйенің бөлігі болуы керек және бір веб - интерфейс арқылы басқарылуы керек; Жүйенің барлық модульдерін орналастыру Бірыңғай БҚ кескінінен қамтамасыз етілуі керек, ал қажетті функционалдылықты лицензия қосымша БҚ орнатуды қажет етпей іске қосуы керек; Жүйе қосымша модульдерді қосу арқылы өзінің функционалдық кеңейтімдерін қолдауы керек; Инфрақұрылымның осалдығы туралы барлық ақпарат, қауіпсіздік құрылғыларының конфигурациясы туралы мәліметтер (басып кірудің алдын алу жүйелері (IPS), маршрутизаторлар мен брандмауэрлер (firewall)), оқиғалар журналдарынан ақпарат (logs), ағындар

	желісінен ақпарат (NetFlow), және оқиғалар туралы ақпарат іске қосуды қажет етпестен жиналып, өңделіп, бірыңғай дерекқорда сақталуы керек және үшінші тарап қолданбаларын, дерекқорларды, қосымша интерфейстерді, терезелерді немесе сценарийлерді немесе басқа виртуалды құрылғыларды пайдалану; Жүйе бірыңғай дерекқорда жиналатын және өңделетін деректердің өзектілігіне кепілдік беруі керек - оқиғалар журналдарынан (logs) және ағындардан (flows) деректерді өңдеуді және корреляцияны қамтамасыз етуі керек, бұл жүйе оқиға көзінен немесе деректерді алғаннан кейін 1 секундтан аспайды. ағындардың бұлақтары (flows); Оқиғалар журналдары туралы ақпарат жинау көлемін шектеусіз кеңейту мүмкіндігі. АҚ оқиғаларын сақтауға және талдауға арналған серверлік қуаттарға қойылатын талаптар. AVX-512 архитектурасын қолдайтын соңғы/соңғы буын заманауи серверлік платформалар; Процессор кем емес: vCPU, 64 Cores, базалық тактілік жиілігі 2,9 Ггц-тен төмен емес; Жедел жады кемінде: 256 ГБ, жиілігі 2966 Mhz төмен емес; Репликациясы кем емес сақтау орны: SSD дискілерінде кемінде 5000 Гб кэштелген HDD. Репликациясы кем емес сақтау орны: SSD дискісі кемінде 5120 Гб. Бағдарламалық жасақтама өңделетін мәліметтер саны артқан кезде өнімділіктің қажетті өсуін қамтамасыз ететін масштабтау талаптарына сәйкес келуі керек. Инженерлік инфрақұрылымды ажыратпай жеткізушінің инфрақұрылымына қызмет көрсету мүмкіндігі үшін ДСҰ резервтік компоненттермен және АТ жүктемесіне қызмет көрсететін бірнеше тәуелсіз тарату арналарымен қамтамасыз етілуі тиіс. Кез-келген уақытта ат жүктемесінің жұмысын қамтамасыз ету үшін бір тарату арнасының, энергиямен жабдықтау жүйесінің кіріс бөлігінің де, механикалық жүйелердің де жұмысы жеткілікті. Кез келген белсенді инфрақұрылымдық компонент немесе тарату арнасының элементі ат жүктемесіне әсер етпестен жоспарлы қызмет көрсету үшін пайдаланудан шығару мүмкіндігіне ие болуы тиіс. Деректер орталығы Tier-2 стандартына сәйкес келуі керек және ақпараттық қауіпсіздік бойынша аттестаттаудан сәтті өту үшін ГТС талаптарына сәйкес келуі керек. Деректер орталығы келесі талаптарға сай болуы керек: Барлық арналардың ақпараттық қауіпсіздігін қорғай отырып, деректер орталығының қауіпсіздігі мен тіршілік әрекетінің барлық жүйелерін шығарумен жергілікті немесе қашықтағы мониторинг диспетчерлік орталығы; Тәулік бойы физикалық қорғау; ТОБЖ-ның кемінде 2 тәуелсіз енгізуі; Барлық жүйелерді тәулік бойы бақылауға арналған мамандандырылған үй-жай; Тіршілікті қамтамасыз ету мониторингі жүйелері ДБО жабық байланыс арналары арқылы жұмыс істеуі тиіс; Жеткізушіде L3–L5 OSI деңгейлерінде , 24/7/365 режимдерінде DDoS-шабуылдардан желіні қорғаудың болуы, Тапсырыс беруші құжаттамалық растауды талап етуге құқылы. Әлеуетті өнім берушінің 2 Тәуелсіз деректер орталығында болуы, Тапсырыс беруші colocation қызметтерін берушімен шарт түрінде растауды талап етуге құқылы. Тапсырыс берушінің өтініштерін тіркеу кезінде Тараптардың өзара іс-қимыл рәсімі. - Тапсырыс берушіге келесі көрсеткіштерге

	сәйкес сұраныстарды жіберу мүмкіндігі берілуі керек: - Өзгертуге сұрау салу (қызмет конфигурациясының өзгеруіне байланысты өтінімдер (ақ оқиғаларының көзін қосу/жою, сценарийді бейімдеу) - өтініштер саны шектелмейді; - Ақпараттық сұрау салу (қызмет бойынша консультациялық мәселелерге байланысты өтінімдер (шарт бойынша сұрақтар және т. б.) – өтініштер саны шектелмейді; - АҚ инцидентіне күдік (Тапсырыс берушінің АҚ инцидентіне күдікпен байланысты өтінім. Бастапқыда бұл өтінішке "төмен" басымдық беріледі. Қажет болған жағдайда Тапсырыс беруші басымдықты арттыра алады) – өтініштер саны шектелмейді. Ол үшін Тапсырыс берушінің уәкілетті өкілі орындаушының электрондық мекенжайына сұрау жіберуі тиіс. Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен Мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді) әлеуетті өнім берушіге қойылатын талаптар. Әлеуетті өнім беруші "Ақпараттандыру туралы" ҚР Заңының 7-2, 7-3-баптарына сәйкес АҚ оқиғаларының мониторингі қызметін көрсетеді және мәлімделген талаптарды орындауға байланысты барлық міндеттемелерді өзіне қабылдайды. Өнім беруші мамандарының Тапсырыс берушінің техникалық қызметімен тәулік бойы өзара іс-қимылын қамтамасыз ету және деректердің ықтимал ағып кетуін болдырмау үшін - әлеуетті өнім берушінің қызметі өнім берушінің сертификатталған өкілдерінің міндетті түрде Тапсырыс берушінің объектілерінде болу шартымен, Тапсырыс берушінің өтінімі бойынша ден қою уақыты 30 минуттан аспайтын Қарағанды қаласының аумағында орналастырылуға тиіс. Қызмет көрсету шеңберінде жеткізуші ақпараттық қауіпсіздіктің жедел орталығының платформасында мыналарды орындауы тиіс: –Бағдарламалық-аппараттық кешен мен желілік инфрақұрылымға аудит жүргізу; - Қолданыстағы СУИБ-ті зерделеу мен талдауды, пайдаланушылармен СУИБ-ті сақтау және орындау тұрғысынан сұхбаттасуды, СУИБ-ті заңнама талаптарына сәйкестікке келтіру бойынша ұсынымдар беруді қамтитын ақпараттық қауіпсіздік аудитін жүргізу; Өнім беруші Тапсырыс берушінің алғашқы 3 ай ішінде кемінде 3 АҚ-мамандарын іздестіру құралдарын, ақпаратты қорғау құралдарын әкімшілендіру дағдыларына оқытуды ақпараттық қауіпсіздіктің жедел орталығына физикалық бару мүмкіндігімен жүргізуге міндеттенеді; Оқыс оқиға анықталған жағдайда, ОАО қызметкерлері - Тапсырыс берушінің сұрауы бойынша Тапсырыс берушінің аумағына физикалық түрде келеді (қашықтан алып жүруге тыйым салынады) және кибершабуылды толық тергеумен және жоюмен айналысады және т.б. мерзімі мамандардың болуы оқиғаны оқшаулау уақытымен анықталады. Киберқауіпсіздікті оқытуға арналған онлайн платформа. Жеткізуші цифрлық гигиена және Киберқауіпсіздік бойынша оқыту платформасына қол жеткізуі керек. Жеткізуші келесі талаптарға сай болуы керек онлайн оқыту шешімдерін ұсынуға міндеттенеді. Функционалдық талаптар Қызметкерлерді оқыту: Платформа ұйымның қызметкерлеріне Цифрлық гигиена

	және киберқауіптер бойынша оқыту мүмкіндігін ұсынуы керек. Міндет-деректер қауіпсіздігі, жеке ақпаратты қорғау және цифрлық технологиялармен жұмыс істеу кезінде тәуекелдерді азайту туралы хабардарлықты арттыру. Платформа келесі негізгі тақырыптар бойынша курстар ұсынуы керек: - Сандық гигиена мен киберқауіпсіздікке кіріспе: - Интернеттегі негізгі қауіптер. - Қауіпсіз парольдермен жұмыс істеу принциптері. - Фишингтің, зиянды бағдарламалардың және әлеуметтік инженерияның әсері шабуылдар. - Жеке деректерді қорғау принциптері. - Интернеттегі қорғау шаралары: Фишингтік шабуылдардан қалай аулақ болуға болады. Екі факторлы аутентификацияны қолдану (2FA). Электрондық поштамен және веб-сайттармен жұмыс істеу кезіндегі қауіпсіздік тәжірибелері. - Инциденттерге ден қоюды үйрету: Деректердің бұзылуына немесе оқиғаға қалай дұрыс жауап беру керек қауіпсіздік. Қауіптерді анықтаудағы әрекеттер алгоритмдері. Қауіпсіз желілік мінез-құлық және сандық құрылғылармен жұмыс істеу бойынша ұсыныстар. Платформаға қойылатын техникалық талаптар: Тілдік қолдау: Платформа кем дегенде екі тілді қолдауы керек: қазақ және орыс. Сондай-ақ, қажет болған жағдайда ағылшын тілін қосу мүмкіндігі болуы керек. Тілдерді қолдау оқытудың барлық кезеңдерінде қол жетімді болуы керек. Бұлтқа қол жеткізу: қосымша бағдарламалық жасақтаманы орнатпай-ақ веб-шолғыш арқылы кіруді қамтамасыз ететін Платформа бұлтты болуы керек. Масштабтау: Платформа әр түрлі деңгейдегі қызметкерлерге де, ірі ұйымдарға да білім беру арқылы масштабтауды қолдауы керек. Пайдаланушы интерфейсі: платформада әр түрлі деңгейдегі пайдаланушыларға қол жетімді интуитивті интерфейс болуы керек. Интерфейс әртүрлі құрылғыларға (компьютерлер, ұялы телефондар және планшеттер) бейімделуі керек. Корпоративтік жүйелермен Интеграция: Платформа оқу материалдарын жіберуді және қабылдауды автоматтандыру үшін ішкі корпоративтік жүйелермен интеграцияны қолдауы керек. Есептер мен аналитика: Платформа оқу нәтижелері бойынша жауаптар құруды, сондай-ақ пайдаланушылардың үлгерімі мен курстардың тиімділігін бақылауды қолдауы керек. Деректер қауіпсіздігі: платформадағы барлық деректер Халықаралық ақпараттық қауіпсіздік стандарттарына сәйкес қорғалуы керек. Платформаға қойылатын техникалық талаптар Веб-шолғыш арқылы қол жеткізу: платформаға қосымша бағдарламалық жасақтама немесе аппараттық құрал орнатпай - ақ веб-шолғыш арқылы қол жеткізу керек. Көп тілділікті қолдау: Платформа қазақ, орыс және ағылшын тілдерін қолдауы тиіс. Мобильді қол жетімділік: Платформа кез-келген мобильді құрылғылардан қол жетімді болуы керек. Интерактивті оқыту: оқыту бейнематериалдар мен практикалық тапсырмаларды қоса алғанда, интерактивті болуы керек. Bug Bounty Платформасы. Жеткізуші багбаунти бағдарламаларын ұйымдастыру үшін тапсырыс берушінің ақпараттық жүйелеріндегі осалдықтарды іздеуге және есеп беруге тәуелсіз сарапшыларды (багхантерлерді) тартуды қамтамасыз ететін мамандандырылған платформаны ұсынуы керек. Платформа осалдықтарды іздеу

	процестерін автоматтандыруды, есептерді тексеруді, сарапшылармен өзара әрекеттесуді заңды түрде рәсімдеуді және сыйақы жүйесін қолдауы керек. Міндетті талап-техникалық тапсырманы (іздеу объектілері, осалдықтарды бағалау критерийлері, жария ету мерзімдері мен саясаттары) қалыптастыру және басқару мүмкіндігі.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Аппарат акима города Караганды"
Наименование организатора	Государственное учреждение "Отдел государственных активов и закупок города Караганды"
№ конкурса:	№ 16391272-2
Наименование конкурса:	Услуги по обеспечению информационной безопасности
Номер лота:	№ 82829165-ОК1
Наименование лота:	Услуги по сопровождению и технической поддержке информационной системы
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620230.000.000001
Наименование услуги:	Услуги по сопровождению и технической поддержке информационной системы
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	26000000
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	26000000
Срок оказания услуги:	2026 год
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	10

Описание требуемых характеристик, параметров и иных исходных данных	Техническая спецификация закупаемых услуг по обеспечению информационной безопасности. Поставщик обязуется оказать услугу ОЦИБ посредством имеющихся у потенциального поставщика ресурсов (человеческих, аппаратно-программных и иных) для обеспечения работ по мониторингу и оповещению Заказчика по возникающим инцидентам ИБ. Услуги в рамках текущей ТС должны соответствовать или превосходить обозначенные характеристики. Услуги по предоставлению консультационных услуг реализовываются в рамках законодательства Республики Казахстан в области информационной безопасности и СТ РК ISO/IEC 27001. Срок оказания услуги: до 31 декабря 2026 года. Место оказания услуги: ГУ «Аппарат акима города Караганды», пр. Н. Назарбаева, 39. Наличие технической поддержки/ подписки на программное обеспечение и оборудование, используемое Исполнителем для оказания услуг на период оказания услуги; Обеспечение работоспособности платформы со следующими параметрами: Период обслуживания платформы – 24/7/365; Количество технологических окон за месяц - не более 1; Уведомление о простоях – не менее 60 минут; Максимальная длительность технологического окна - не более 6 часов; Уведомление о технологическом окне - за 3 рабочих дня. Технические и административные параметры оказываемых услуг: Обработка и анализ поступающих событий ИБ и сетевых пакетов; Обрабатываемое кол-во событий в секунду – 2 500 EPS; Подключаемое количество источников – не ограничено; Количество подключаемых источников событий – не ограниченно; Доступ к системе обработки событий для работников Заказчика - не менее 2-х пользователей; Хранение событий для оперативного доступа в системе ОЦИБ - не менее 180 дней. Анализ событий в реальном времени в соответствие с правилами корреляции (не менее 400 правил); Архивное хранение событий безопасности – 3 года; Оперативный мониторинг в режиме работы 24/7/365; Время принятия в работу с момента фиксации автоматически сформированного подозрения на инцидент ИБ в системе ОЦИБ: высокая критичность - до 15 минут, средняя критичность - до 15 минут, низкая критичность - до 60 минут; Оценка, категорирование и информирование об инциденте ИБ в режиме работы 24/7/365; Время оценки, категорирования и информирования об инциденте ИБ с момента принятия в работу: высокая критичность - до 15 минут, средняя критичность - до 15 минут, низкая критичность - до 60 минут; Анализ и расследование инцидентов ИБ с формированием рекомендаций по противодействию - 2 часа; Разработка дополнительных правил корреляции в период предоставления услуги до 100 правил. Согласно Закону Республики Казахстан от 11 декабря 2023 года № 44-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационной безопасности, информатизации и цифровых активов» Собственники или владельцы объектов информатизации государственных органов обязаны принимать меры, обеспечивающие: подключение объектов информатизации к программе взаимодействия, за исключением объектов информатизации, не

	имеющих доступ к Интернету; устранение выявленных уязвимостей, зарегистрированных в программе взаимодействия по объектам информатизации государственных органов; Наличие у потенциального поставщика сертифицированных специалистов для полноценного оказания услуг ОЦИБ. Перечень услуг: • техническая поддержка; • техническое обслуживание; • администрирование вычислительных мощностей. • управление виртуальными серверами и инфраструктурой; • мониторинг производительности виртуальных машин, обеспечивающих работу всех служб ОЦИБ; • администрирование системы управления событиями ИБ (SIEM-системы); • подготовка сервера для интеграции с НКЦИБ; • настройка и администрирование сервера репозитория для Ubuntu; • настройка и администрирование сервера репозитория для Windows; Описание услуг: Мониторинг событий ИБ и анализ результатов мониторинга, ИКИ объектов информатизации Заказчика. Предоставление Потенциальным поставщиком оборудования (сервера) и ПО для сбора и хранения событий ИБ в рамках услуги. Установка аппаратно-программного комплекса для мониторинга событий ИБ в ИТ инфраструктуре Заказчика; Настройка защищенного канала связи между Заказчиком и платформой ОЦИБ, проведение сетевых настроек и настроек безопасности; Настройка источников событий на формирование событий безопасности в соответствии с форматами и типами записей, определенными ст.12 Приказа Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры» и отправки в коллектор сбора событий; Настройка синхронизации времени журналов регистрации событий с инфраструктурой источника времени; Разработка и адаптация правил корреляции событий под инфраструктуру Заказчика; Мониторинг и анализ событий ИБ 24/7; Информирование Заказчика о выявленных нарушениях и инцидентах ИБ с рекомендациями по локализации; Организация доступа к консоли мониторинга и событиям безопасности SIEM системы; Взаимодействие с НКЦИБ по обмену информацией, необходимой для обеспечения ИБ объектов информатизации, угрозами и инцидентам ИБ; Организация сбора, консолидации и хранения событий безопасности в течение периода, определенного законодательными требованиями (3 месяца - оперативный доступ, 3 года - архивный) на стороне Заказчика; Круглосуточный прием и регистрация обращений Заказчика. Разграничение зон ответственности на период оказания услуги мониторинга событий: Предоставление оборудования (сервера) и ПО для сбора и хранения событий ИБ в рамках услуги. Установка аппаратно-программного комплекса в ИТ инфраструктуре Заказчика – Потенциальный поставщик; Настройка защищенного канала связи между Заказчиком и платформой ОЦИБ, проведение сетевых настроек и настроек безопасности – Заказчик, Потенциальный поставщик; Настройка источников событий на формирование событий безопасности в

	соответствии с форматами и типами записей, определенными в законодательном требовании и отправки в коллектор сбора событий - Заказчик, Потенциальный поставщик; Настройка синхронизации времени журналов регистрации событий с инфраструктурой источника времени – Потенциальный поставщик; Разработка и адаптация правил корреляции событий под инфраструктуру Заказчика - Заказчик, Потенциальный поставщик; Мониторинг и анализ событий ИБ 24/7 – Потенциальный поставщик; Информирование Заказчика о выявленных нарушениях и инцидентах ИБ с рекомендациями по локализации – Потенциальный поставщик; Организация доступа к консоли мониторинга и событиям безопасности SIEM системы – Потенциальный поставщик; Взаимодействие с НКЦИБ по обмену информацией, необходимой для обеспечения ИБ объектов информатизации, угрозами и инцидентам ИБ – Потенциальный поставщик; Организация сбора, консолидации событий безопасности – Потенциальный поставщик; Организация хранения событий безопасности в течение периода, определенного законодательными требованиями (3 месяца - оперативный доступ, 3 года - архивный) на стороне Заказчика; Круглосуточный прием и регистрация обращений Заказчика – Потенциальный поставщик; Мониторинг состояния компонентов подсистемы управления событиями ИБ, установленных как на площадке Заказчика, так и на площадке Заказчика – Потенциальный поставщик; Обеспечение корректного функционирования подсистемы управления событиями ИБ – Потенциальный поставщик; Обеспечение работоспособности защищенных каналов передачи информации между площадками - Заказчик и Потенциальный поставщик; Выполнение рекомендаций ОЦИБ и своевременное реагирование на инциденты ИБ – Заказчик; Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга – Заказчик. Мониторинг уязвимостей и анализ результатов мониторинга: Предоставление потенциальным поставщиком оборудования (сервера) и ПО для сбора и хранения событий ИБ в рамках услуги; Установка аппаратно-программного комплекса в ИТ инфраструктуре Заказчика; Настройка защищенного канала связи между Заказчиком и платформой ОЦИБ, проведение сетевых настроек и настроек безопасности; Развертывание, и настройка на стороне Заказчика сканера безопасности; Не менее одного раза в квартал ежеквартальное сканирование сети, инструментальный поиск уязвимостей во внешнем и внутреннем периметре Заказчика; Анализ и оценка сведений, полученных в результате сканирования, классификация уязвимостей по уровню угроз, подготовка рекомендаций по устранению, формирование отчета о выявленных уязвимостях и мерах их устранения; Направление отчета Заказчику Ежемесячно; Взаимодействие с НКЦИБ по обмену информацией, необходимой для обеспечения ИБ объектов информатизации, угрозами и инцидентам ИБ; Круглосуточный прием и регистрация обращений Заказчика; Разграничение зон ответственности на период оказания услуги мониторинг уязвимостей: Предоставление оборудования (сервера) и ПО для

	сбора и хранения событий ИБ в рамках услуги; Установка аппаратно-программного комплекса в ИС Заказчика – Заказчик и Потенциальный поставщик; Настройка защищенного канала связи между Заказчиком и платформой ОЦИБ, проведение сетевых настроек и настроек безопасности - Заказчик и Потенциальный поставщик; Развертывание, и настройка на стороне Заказчика сканера безопасности - Заказчик и Потенциальный поставщик; Сканирование сети на уязвимости в порядке, определенном технической спецификацией с Заказчиком; Анализ и оценка сведений, полученных в результате сканирования, классификация уязвимостей по уровню угроз, подготовка рекомендаций по устранению, формирование отчета о выявленных уязвимостях и мерах их устранения – Потенциальный поставщик; Направление отчета Заказчику – Потенциальный поставщик Ежемесячно; Взаимодействие с НКЦИБ по обмену информацией, необходимой для обеспечения ИБ объектов информатизации, угрозами и инцидентам ИБ – Потенциальный поставщик; Круглосуточный прием и регистрация обращений Заказчика – Потенциальный поставщик; Выполнение рекомендаций ОЦИБ и своевременное реагирование на инциденты ИБ – Заказчик; Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга – Заказчик; Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и Исполнителя – Заказчик и Потенциальный поставщик. Требования к аппаратно-программному комплексу для мониторинга событий: Система должна обеспечивать централизованное управление всеми её компонентами и функционалом через единый Веб-интерфейс; Система должна иметь встроенный функционал определения и классификации активов в сети; Система должна иметь возможность расширения своего функционала за счёт установки дополнительных приложений через магазин приложений производителя, а также должна иметь встроенную репетиционную базу, которая обновляется производителем; Система должна иметь встроенный функционал обнаружения аномальной активности пользователей (User Behavior Analytics); Система должна иметь возможность шифровать коммуникации между компонентами; Система должна интегрироваться с системами сторонних производителей (LDAP, AD) для обеспечения аутентификации; Система должна предоставлять возможность управления системой, создания аналитических отчетов и правил через веб-интерфейс пользователя; Система должна гарантировать работу отдельных компонентов системы, при выходе из строя любой части системы. (Например, центральная консоль выходит из строя, но коллекторы логов продолжают функционировать); Система должна иметь автоматический процесс резервного копирования конфигурации (Backup) и возможность восстановления (Recovery) конфигурации из графического интерфейса пользователя; Система должна нормализовать стандартные поля событий (имена пользователей, IP адреса, имена хостов, устройства-источники событий) с различных устройств мультивендорной сети. Нормализация должна проводиться

	без дополнительной настройки; Система должна предоставлять стандартную категоризацию событий без предварительной дополнительной настройки; Система должна иметь возможность хранить информацию о событиях, как в исходном виде, так и в нормализованном виде для использования в дальнейших расследованиях; Система должна иметь возможность обрабатывать и нормализировать данные из полей, которые не поддерживаются изначально и не предоставляются с настройками; Система должна обеспечивать анализ событий в режиме реального времени, на протяжении определенного периода времени, по предустановленным пользователем фильтрам; Система должна предоставлять возможность получения дополнительной информации о событиях при необходимости; Система должна предоставлять отчетность по всем событиям, отчетность должна быть доступа через веб-интерфейс для пользователей решения; Система должна иметь мастер настройки отчетов для самостоятельной настройки и создания собственных отчетов; Система должна предоставлять примеры сгенерированных отчетов за определенный период времени по различным сегментам и системам в сети; Система должна иметь встроенные отчеты для типичных бизнес-требований заказчика; Система должна обеспечивать корреляцию информации с различных источников, которые никак не взаимодействую между собой; Система должна предоставлять мастер настройки оповещений, обеспечение оповещений на основе обнаруженных аномалий и поведенческого анализа и изменений, обеспечивать оповещения по предустановленным политикам (например, при обнаружении IM трафика, который запрещен); Система должна иметь возможность коррелировать дополнительные данные безопасности (географическое расположение, известный ботнет, уязвимость, каналы распространения и пр.). Автоматический сбор данных без подключения дополнительных систем, сторонних разработчиков; Система должна предупреждать администратора, если перестали поступать логи с устройства в сети, которое мониторится (например, нет логов от сервера в течении х минут); Система должна обеспечивать корреляцию информации с устройств и систем различного типа, а также обеспечивать встроенный функционал автоматического определения всех устройств и их инвентаризации по классам систем (например, почтовые сервера, сервера баз данных и пр.); Система должна обеспечивать корреляцию по определенным последовательностям событий, на основе дополнительных данных от других источников; Система должна поддерживать возможность обновления программного обеспечения. Система должна поддерживать следующие форм-факторы: виртуальный аплайнс, программный аплайнс (для установки на собственные аппаратные мощности); Система должна легко масштабироваться и расширять функционал программного обеспечения путем закупки дополнительных лицензий либо добавления новых компонентов в архитектуру без необходимости замены существующих компонентов. Контроль активности сети: Система должна уметь проводить поведенческий анализ трафика и сообщать об изменениях согласно заданных порогов

	изменения; Система должна поддерживать разделение трафика согласно логическому дизайну сети, определять происхождение и назначение потоков трафика в сети, в том числе и по географическим регионам в режиме реального времени; Система должна разделять и создавать независимые профайлы для локального трафика и трафика, идущего/приходящего в/из интернета, обеспечить создание пользовательских профайлов используя для выборки любые параметры потока трафика. Система должна поддерживать представление трафика на основе IP адреса, группы IP адресов, источник/место назначения IP пар и т.д.; Система должна иметь возможность контекстно связывать активность приложения в сети с событием безопасности на подконтрольном устройстве; Система в реальном времени должна контекстно связывать выявленные события безопасности со знаниями об активах в сети, автоматически определять приоритет выявленных событий безопасности согласно относительной важности актива, определять серьезность выявленного события безопасности по отношению к уязвимости активов. Требования к управлению рисками: Система должна обеспечивать сбор и нормализацию конфигураций коммутаторов, маршрутизаторов, брандмауэров и IPS с не менее 50 устройств без копирования конфигурационного файла с устройства; Система должна получать информацию о конфигурации со следующего оборудования: CheckPoint, Cisco CatOS, Huawei, Cisco IOS, Cisco Nexus, Cisco ASA, f5 BigIP, Fortinet FortiOS, HP ProVision, IBM ISS GX, IBM ISS SiteProtector, Juniper JunOS, Juniper Screen OS, McAfee SideWinder, Nokia IPSO, PaloAlto Pan - OS, SourceFire 3D, TippingPoint IPS, а также generic SNMP. Обязательная поддержка следующих методов подключения: SSH, Telnet, Https \ Http, SCP, FTP \ SFTP \ TFTP, SNMP, CPSMS, SQL, NetConf. Обязательная поддержка возможности задания любого порта подключения; Система должна задать такие параметры аутентификации для сбора данных как: Username, пароль, SNMP get community, SNMP v2/v3, OPSEC entity SIC, OPSEC application object SIC, OPSEC SSL certificate; Требования к управлению уязвимостями: Система должна обеспечивать процесс управления уязвимостями для не менее 1024 активов сети; Система должна обеспечивать сканирование с целью инвентаризации активов для неограниченного количества активов; Информация об уязвимостях должна быть доступной через интерфейс SIEM системы без необходимости установки дополнительных приложений или расширений; Система управления уязвимостями должна использовать данные с SIEM системы и системы управления конфигурациями для обеспечения приоритезации процесса исправления уязвимостей; Данные о найденных уязвимостях должны автоматически влиять на срабатывание корреляционных правил SIEM для выявления инцидентов; Каждая уязвимость должна быть автоматически закреплена за владельцем актива и должна предоставляться возможность задания интервала времени на исправление найденной уязвимости и автоматической проверки её устранения. Владелец актива должен быть уведомлен через: электронную почту или

	интерфейс SIEM системы; Система должна предоставить возможность автоматически запускать процесс сканирования при: любых событиях/инциденте информационной безопасности, выявления нового актива в сети на основе данных из: журналов событий (logs), данных по NetFlow, данных с jFlow, данных по sFlow, данных IPFIX, изменения конфигурации ОС актива, или создание новой учетной записи на уровне ОС актива; Система должна обеспечить функционал внутреннего и внешнего сканирования инфраструктуры по расписанию; Политики сканирования должны устанавливаться по типу сканирования (Web Scan, PCI Scan, Patch Scan, Discovery Scan, Database Scan, Full Scan), также возможность создавать новые политики сканирования или собственные шаблоны; Тип сканирования должен быть определен: протоколом проведения сканирования, диапазоном портов сканирования, и группами активов сканирования; Система управления уязвимостями должна предоставлять возможность задавать параметры запуска сканирования по расписанию и автоматического получения информации для следующих сканеров путем инфраструктурной интеграции через веб- интерфейс без необходимости запуска и использования сторонних приложений, баз данных, дополнительных интерфейсов, окон или других виртуальных устройств: IBM Guardium, AXIS Scanner, Beyond Security AVDS, Digital Defense inc. AVS, eEye REM Scanner, FoundScan Scanner, SiteProtector, BigFix, Juniper NSM Profiler, McAfee VM, Microsoft SCCM, nCircle IP360 Scanner, Nessus Scanner, NMap Scanner, Outpost24 Vulnerability Scanner, Positive Technologies MaxPatrol, Qualys Detection Scanner, Qualys Scanner, Rapid7 NexPose Scanner, Saint Scanner, SecureScout Scanner, Tenable Security Center; При сканировании веб-приложений использовать эвристические методы анализа, позволяющие обнаруживать уязвимости в соответствии с таксономиями Open Web Application Security Project TOP 10; Через единый интерфейс SIEM системы пользователь должен иметь возможность: Запускать сканирование устройств, веб-приложений, подсетей и внешнего периметра; Настраивать гибкие сценарии сканирования для устройств, веб-приложений, подсетей и внешнего периметра, например: сканирование каждые 3 суток, в 13:00 часов; Настраивать "глубину сканирования", например - с использованием полномочий администратора или без. Совместимость: Все компоненты системы должны быть частью единой системы и управляться через единый веб- интерфейс; Развертывание всех модулей системы должно обеспечиваться с единого образа ПО, а необходимый функционал активироваться лицензией без необходимости установки дополнительного ПО; Система должна поддерживать расширения своего функционала за счет добавления дополнительных модулей; Вся информация об уязвимостях инфраструктуры, данные о конфигурации устройств безопасности (систем предотвращения вторжение (IPS), маршрутизаторов и брандмауэров (firewall)), информация из журналов событий (logs), информация из сети потоков (NetFlow), и информацию об инцидентах должна собираться, обрабатываться и храниться

	в единой базе данных без необходимости запуска и использования сторонних приложений, баз данных, дополнительных интерфейсов, окон или скриптов или других виртуальных устройств; Система должна гарантировать актуальность данных, собираемых и обрабатываемых в единой базе данных - обеспечивать обработку и корреляцию данных из журналов событий (logs) и потоков (flows) с задержкой не более 1 секунды после получения данных системой от источника событий или родники потоков (flows); Возможность неограниченного расширения объема сбора информации о журналах событий. Требования серверным мощностям для хранения и анализа событий ИБ. Современные серверные платформы предпоследнего/последнего поколения, с поддержкой архитектуры AVX-512; Процессор не менее: vCPU, 64 Cores, с базовой тактовой частотой не ниже 2,9Ггц; Оперативная память не менее: 256 GB, с частотой не ниже 2966 Mhz; Хранилище с репликацией не менее: HDD с кэшированием на SSD-дисках не менее 5000 Gb. Хранилище с репликацией не менее: SSD-диск не менее 5120 Gb. Программно-аппаратная часть должна соответствовать требованиям масштабируемости, обеспечивающая требуемое увеличение производительности при увеличении количества обрабатываемых данных. Для возможности обслуживания инфраструктуры Поставщика без отключения инженерной инфраструктуры, ЦОД должен быть обеспечен резервными компонентами и несколькими независимыми каналами распределения, обслуживающими ИТ-нагрузку. Для обеспечения работы ИТ-нагрузки в любой отдельно взятый момент времени достаточно работы одного канала распределения, как входного участка системы энергоснабжения, так и для механических систем. Любой активный инфраструктурный компонент или элемент канала распределения должен иметь возможность вывода из эксплуатации для планового обслуживания, никак не затрагивая ИТ-нагрузку. ЦОД должен соответствовать стандарту Tier-2 и соответствовать требованиям ГТС для успешного прохождения аттестации по информационной безопасности. ЦОД должен соответствовать нижеследующим требованиям: Локальный или удаленный диспетчерский Центр мониторинга с выводом всех систем безопасности и жизнедеятельности ЦОД, с защитой информационной безопасности всех каналов; Круглосуточная физическая охрана; Не менее 2-х независимых вводов ВОЛС; Специализированное помещение для круглосуточного наблюдения за всеми системами; Системы мониторинга жизнеобеспечения ЦОД должны функционировать по закрытым каналам связи; Наличие у Поставщика защиты сети от DDoS–атак на уровнях L3-L5 OSI , в режимах 24/7/365, заказчик вправе потребовать документальное подтверждение. Наличие у потенциального поставщика присутствия в 2-х независимых ЦОДах, заказчик вправе потребовать подтверждение в виде договора с поставщиком услуг Colocation. Процедура взаимодействия сторон при регистрации Обращений Заказчика. Заказчику должна предоставляется возможность отправлять запросы согласно следующим показателям: - Запрос на изменение (Заявки, связанные с изменением конфигурации Услуги (добавление/удаление

	источника событий ИБ, адаптация сценария) – количество обращений не ограничено; - Информационный запрос (Заявки, связанные с консультационными вопросами, по Услуге (вопросы по Договору и тп) – количество обращений не ограничено; - Подозрение на Инцидент ИБ (Заявка, связанная с подозрением Заказчика на Инцидент ИБ. Изначально данному обращению присваивается «низкий» приоритет. При необходимости Заказчик может повысить приоритет) – количество обращений не ограничено. Для этого уполномоченный представитель Заказчика должен отправить запрос на электронный адрес исполнителя. Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается). Потенциальный поставщик оказывает услугу мониторинга событий ИБ в соответствии с статьями 7-2, 7-3, Закона РК «Об информатизации» и принимает на себя все обязательства, связанные с исполнением заявленных требований. Для обеспечения круглосуточного взаимодействия специалистов поставщика с технической службой Заказчика, и предотвращения возможной утечки данных – служба потенциального поставщика должна быть размещена на территории г. Караганды, с условием обязательного нахождения сертифицированных представителей Поставщика, на объектах Заказчика, с временем реагирования не более 30 минут по заявке Заказчика. В рамках оказания Услуги Поставщик на платформе Оперативного центра информационной безопасности должен выполнять: - Провести аудит программно –аппаратного комплекса и сетевой инфраструктуры; - Провести аудит информационной безопасности, включающего изучение и анализ действующего СУИБ, интервьюирование пользователей на предмет соблюдение и исполнения СУИБ, выдача рекомендации по приведению СУИБ к соответствию требования законодательства; Поставщик обязуется провести обучение в течение первых 3-х месяцев не менее 3-х ИБ-специалистов Заказчика навыкам администрирования поисковых средств, средств защиты информации с возможностью физического посещения оперативного центра информационной безопасности; В случае обнаружения инцидента, сотрудники ОЦИБ – по запросу Заказчика, физически пребывают на территорию заказчика (удаленное сопровождение запрещено) и занимаются полным расследованием и устранением кибератаки и т.д. Срок нахождение специалистов определяется временем локализации Инцидента. Онлайн-платформа для обучения кибербезопасности: Поставщик должен предоставить доступ к платформе обучения цифровой гигиене и кибербезопасности. Поставщик обязуется предоставить решения для онлайн-обучения, которые должны соответствовать следующим требованиям. Функциональные требования: Обучение сотрудников: Платформа должна предоставлять возможность проведения обучения для сотрудников организации по вопросам цифровой гигиены и киберугроз. Задача — повысить осведомленность о безопасности данных, защите личной информации и

	минимизации рисков при работе с цифровыми технологиями. Платформа должна предоставлять курсы по следующим ключевым темам: - Введение в цифровую гигиену и кибербезопасность: - Основные угрозы в интернете. - Принципы работы с безопасными паролями. - Влияние фишинга, вредоносных программ и социальных инженерных атак. - Принципы защиты личных данных. - Меры защиты в интернете: Как избежать фишинговых атак. Использование двухфакторной аутентификации (2FA). Практики безопасности при работе с электронной почтой и веб-сайтами. - Обучение реагированию на инциденты: Как правильно реагировать на утечку данных или инцидент безопасности. Алгоритмы действий при обнаружении угроз. Рекомендации по безопасному поведению в сети и работе с цифровыми устройствами. Технические требования к платформе: Языковая поддержка: Платформа должна поддерживать как минимум два языка: казахский и русский. Также должна быть возможность добавить английский язык по мере необходимости. Поддержка языков должна быть доступна на всех этапах обучения. Облачный доступ: Платформа должна быть облачной, обеспечивая доступ через веб-браузер без необходимости установки дополнительного программного обеспечения. Масштабируемость: Платформа должна поддерживать масштабирование, обеспечивая обучение как для малого числа сотрудников, так и для крупных организаций с различными уровнями знаний. Интерфейс пользователя: Платформа должна иметь интуитивно понятный интерфейс, доступный для пользователей с разным уровнем технической подготовки. Интерфейс должен адаптироваться под различные устройства (ПК, мобильные телефоны и планшеты). Интеграция с корпоративными системами: Платформа должна поддерживать интеграцию с внутренними корпоративными системами для автоматизации отправки и получения обучающих материалов. Отчеты и аналитика: Платформа должна поддерживать создание ответов по результатам обучения, а также отслеживание прогресса пользователей и эффективности курсов. Безопасность данных: Все данные на платформе должны быть защищены в соответствии с международными стандартами информационной безопасности. Технические требования к платформе: Доступ через веб-браузер: Платформа должна быть доступна через веб- браузер без необходимости установки дополнительного программного обеспечения или оборудования. Поддержка мульти-язычности: Платформа должна поддерживать казахский, русский и английский языки. Мобильная доступность: Платформа должна быть доступна с любых мобильных устройств. Интерактивное обучение: Обучение должно быть интерактивным, включая видеоматериалы и практические задания. Платформа Bug Bounty: Поставщик должен предоставить специализированную платформу для организации программ багбаунти, обеспечивающую привлечение независимых экспертов (багхантеров) к поиску и репортингу уязвимостей в информационных системах заказчика. Платформа должна поддерживать автоматизацию процессов поиска уязвимостей, верификацию отчетов, юридическое оформление взаимодействия с экспертами и систему вознаграждений.

	Обязательным требованием является возможность формирования и управления техническим заданием (объектами поиска, критериями оценки уязвимостей, сроками и политиками раскрытия).
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	