Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Төрегелді Шарманов атындағы Ұлттық медицина университеті" коммерциялық емес акционерлік қоғамы
Ұйымдастырушының атауы:	"Төрегелді Шарманов атындағы Ұлттық медицина университеті" коммерциялық емес акционерлік қоғамы
Конкурстың №:	№ 17930563-1
Конкурстың атауы:	Киберқауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Лоттың нөмірі:	№ 88515813-ОК1
Лоттың атауы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	801019.000.000010
Қызметтің атауы:	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	12000000
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	12000000
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	техникалық сипаттамаға сәйкес
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	1. Сатып алынатын тауарлардың, жұмыстар мен көрсетілетін қызметтердің функционалдық, техникалық, сапалық және пайдалану сипаттамаларының сипаттамасы Осы Техникалық ерекшелік (бұдан әрі – ТЕ) киберқауіпсіздікті қамтамасыз ету жөніндегі қызметтерді көрсетуге (бұдан әрі – Қызмет) қойылатын негізгі міндеттер мен талаптардың сипаттамасын қамтиды. Қызмет Тапсырыс берушінің ақпараттық жүйелерін киберқауіпсіздік саласындағы белгіленген талаптарға сәйкестігіне сынақтан өткізуді, сондай-ақ ақпараттық қауіпсіздік оқиғаларына үздіксіз мониторинг жүргізуді, киберқауіпсіздік оқиғаларын уақтылы анықтауды, талдауды және сүйемелдеуді, осалдықтарды анықтауды, Тапсырыс берушінің ақпараттық жүйелері мен ақпараттық инфрақұрылымының қорғалу деңгейін арттыру жөнінде ұсынымдар беруді қамтиды. 2. Қызметке қойылатын талаптар Қызмет төменде көрсетілген талаптарға сәйкес көрсетілуі тиіс. 2.1. Функционалдық талаптар Қызмет Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НҚ «Цифрлық үкіметтің цифрлық объектілері мен аса маңызды цифрлық объектілерді киберқауіпсіздік талаптарына сәйкестігіне сынақтан өткізу әдістемесі мен қағидаларын бекіту туралы» бұйрығына, сондай-ақ киберқауіпсіздік саласындағы Қазақстан Республикасының өзге де қолданыстағы нормативтік құқықтық актілері мен мемлекеттік стандарттарына сәйкес көрсетілуі тиіс. Тапсырыс берушінің жүйелерін талаптарға сәйкестігіне сынақтан өткізу жөніндегі киберқауіпсіздікті қамтамасыз ету қызметіне мыналар кіреді: 1) Бастапқы кодтарды талдау: • бағдарламалық қамтылымдағы кемшіліктерді анықтау; • бастапқы кодты талдау нәтижелерін тіркеу; • бастапқы кодтарды талдау нәтижелері бойынша хаттама ұсыну. 2) Киберқауіпсіздік функцияларын сынақтан өткізу: • қауіпсіздік функцияларының техникалық құжаттама талаптарына, Қазақстан Республикасының нормативтік құқықтық актілеріне және Қазақстан Республикасының аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттарға сәйкестігін бағалау, оның ішінде қажет болған жағдайда бағдарламалық құралдарды қолдану; • сынақ нәтижелерін бақылау нәтижелерін, сәйкестікті немесе сәйкессіздікті бағалауды және анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдарды (қажет болған жағдайда) көрсете отырып, есепте тіркеу; • киберқауіпсіздік функцияларын сынақтан өткізу нәтижелері бойынша хаттама ұсыну. 3) Жүктемелік сынақтан өткізу: • мамандандырылған бағдарламалық құралда сынақ конфигурациясы мен сценарийін баптау; • мамандандырылған бағдарламалық құралды іске қосу; • сынақ объектісіне түсетін жүктемені тіркеу; • сынақ объектісінің нақты өткізу қабілетін арттыру немесе төмендету жөніндегі ұсынымдарды көрсете отырып, жүктемелік сынақ есебін қалыптастыру және ұсыну; • жүктемелік сынақ нәтижелері бойынша хаттама ұсыну. 4) Желілік инфрақұрылымды тексеру: • желілік инфрақұрылымды қорғау функцияларының техникалық құжаттама талаптарына, Қазақстан Республикасының нормативтік құқықтық актілеріне және киберқауіпсіздік саласындағы Қазақстан

	Республикасының аумағында қолданыстағы стандарттарға сәйкестігін бағалау; • Тапсырыс берушінің желілік инфрақұрылымын, оның ішінде қажет болған жағдайда бағдарламалық құралдарды қолдана отырып, тексеру; • жалпы осалдықтар мен тәуекелдер базасындағы бағдарламалық қамтылымның белгілі осалдықтарын анықтау мақсатында бағдарламалық құрал арқылы сканерлеу жүргізу; • алынған сынақ нәтижелерін бақылау нәтижелерін, сәйкестікті немесе сәйкессіздікті бағалауды және анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдарды (қажет болған жағдайда) көрсете отырып, есепте тіркеу; • желілік инфрақұрылымды тексеру нәтижелері бойынша хаттама ұсыну. 5) Киберқауіпсіздікті қамтамасыз ету процестерін тексеру: • киберқауіпсіздікті қамтамасыз ету процестерінің киберқауіпсіздік саласындағы нормативтік құқықтық актілер мен стандарттар талаптарына сәйкестігін бағалау; • сынақ нәтижелерін бақылау нәтижелерін, сәйкестікті немесе сәйкессіздікті бағалауды және анықталған сәйкессіздіктерді түзету жөніндегі ұсынымдарды (қажет болған жағдайда) көрсете отырып, тіркеу; • серверлерді, виртуалды ресурстарды және желілік жабдықты бағдарламалық құралдар арқылы белгілі осалдықтардың бар-жоғына сканерлеу; • анықталған осалдықтарды жалған іске қосылу белгілерінің бар-жоғына талдау және олардың сындық деңгейіне қарай жою жөнінде ұсынымдар қалыптастыру (қажет болған жағдайда); • ақпараттық қауіпсіздікті қамтамасыз ету процестерін тексеру нәтижелері бойынша хаттама ұсыну. Киберқауіпсіздікті қамтамасыз ету процестерін тексеру Цифрлық үкіметтің цифрлық объектілері мен аса маңызды цифрлық объектілерді киберқауіпсіздік талаптарына сәйкестігіне сынақтан өткізу қағидаларының 31-тармағына сәйкес жүргізіледі. 2.2. Қызмет көрсету шеңберіндегі талаптар Қызмет көрсету шеңберінде Өнім беруші ақпараттық қауіпсіздік оқиғаларын орталықтандырылған түрде жинауды, өңдеуді, сақтауды және талдауды, Тапсырыс берушінің ақпараттық инфрақұрылымына тәулік бойы мониторинг жүргізуді, киберқауіпсіздік оқиғаларын анықтауды, Тапсырыс берушіні хабардар етуді және анықталған оқиғаларға ден қою мен оларды жою жөнінде ұсынымдар беруді қамтамасыз етуі тиіс, атап айтқанда: • Тапсырыс берушінің ақпараттандыру объектілеріне талдау жүргізіп, киберқауіпсіздік оқиғаларын басқару жүйесіне жіберу үшін қажетті тіркеу журналдарының тізбесін айқындау; • Жүйе агенттерін Тапсырыс берушінің ақпараттандыру объектілерінің тіркеу журналдарын жинаудың бірыңғай жүйесіне, сондай-ақ қажет болған жағдайда Тапсырыс берушінің ақпараттандыру объектісінің өзге де ақпараттық-коммуникациялық инфрақұрылым объектілеріне орнату; • Тапсырыс берушінің ақпараттандыру объектілерінен тіркеу журналдарын Жүйеге жинау, оларды өңдеу және киберқауіпсіздік оқиғалары мен инциденттерін анықтау мақсатында талдау; • мониторинг аймағында орын алған киберқауіпсіздік инциденттерін анықтау; • Тапсырыс берушіге киберқауіпсіздік инциденттерін жою және олардың алдын алу жөнінде ұсынымдар беру; • корреляция қағидаларын әзірлеу; • «Лог-файлдарды», жүйелік журналдарды жинауға

	арналған серверлік жабдықты және SIEM жүйесінің компоненттерін Тапсырыс беруші ұсынады; • киберқауіпсіздік саясатының талаптарын, басқару шараларын, киберқауіпсіздікті қамтамасыз ету процестері мен рәсімдерін қолдану; • Тапсырыс берушінің ақпараттандыру объектілерін осалдықтардың бар-жоғына лицензияланатын бағдарламалық қамтылымды қолдана отырып, audit және pentest режимдерінде, Тапсырыс берушімен келісілген жұмыстар кестесіне сәйкес аспаптық тексеру (бұдан әрі – осалдықтарға тексеру) жүргізу; • киберқауіпсіздік осалдықтарына жүргізілген тексеру нәтижелерін және Тапсырыс берушінің киберқауіпсіздік осалдықтарын жою жөніндегі ұсынымдарды ұсыну; • кезекші қызмет арқылы 24/7 режимінде мониторинг жүргізу; • Тапсырыс берушінің киберқауіпсіздікке жауапты қызметкерлеріне тұрақты түрде консультациялық қолдау көрсету; • Тапсырыс берушінің өтініштерін тәулік бойы қабылдауды және тіркеуді қамтамасыз ету; • дереккөздерден қауіпсіздік оқиғаларын қалыптастыруды № 52/НҚ «Цифрлық үкіметтің цифрлық объектілері мен аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларында» айқындалған форматтар мен жазба түрлеріне сәйкес баптау және оларды оқиғаларды жинау коллекторына жіберу; • корреляция қағидаларына сәйкес оқиғаларды нақты уақыт режимінде талдау; • Қазақстан Республикасының заңнамасында белгіленген талаптарға сәйкес, Өнім беруші өз бетінше анықтаған киберқауіпсіздік инциденті туралы анықталған сәттен бастап 15 минут ішінде Киберқауіпсіздікті үйлестіру ұлттық орталығына (бұдан әрі – КҮҰО) хабарлау. Өнім беруші пайдаланылатын бағдарламалық қамтылымға қолданыстағы лицензиялардың, жазылымдардың және техникалық қолдаудың болуын қамтамасыз етуі тиіс. КЖО-ға (ЦОК) қосылуға жататын ақпараттық жүйелердің, серверлердің, желілік жабдықтың және оқиғалардың өзге де дереккөздерінің тізбесі Орындаушы мен Тапсырыс беруші арасында бірлесіп айқындалады және келісілген оқиғалар дереккөздерінің тізбесінде тіркеледі. Қосымша оқиғалар дереккөздерін қосу Тапсырыс берушінің өтінімі негізінде және Тараптардың өзара іс-қимыл регламентінде белгіленген тәртіппен жүзеге асырылады. Өнім беруші өз жауапкершілік аймағы шегінде өзі ұсынатын КЖО (ЦОК) компоненттерінің, бағдарламалық қамтылымның, агенттер мен коллекторлардың жұмысқа қабілеттілігін қамтамасыз етуге міндетті. 2.3. Талдамалық және дайындық жұмыстары • киберқауіпсіздік оқиғаларын басқару жүйесіне жіберу үшін қажетті тіркеу журналдарының тізбесін айқындау мақсатында Тапсырыс берушінің ақпараттандыру объектілеріне талдау жүргізу; • лицензияланған SIEM жүйесінің агенттерін Тапсырыс берушінің ақпараттандыру объектілеріне баптау және орнату; • № 52/НҚ «Цифрлық үкіметтің цифрлық объектілері мен аса маңызды цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларында» айқындалған форматтар мен жазба түрлеріне сәйкес логтарды қалыптастыру үшін оқиғалар дереккөздерін баптау. 2.4. Оқиғаларды жинау, сақтау, өңдеу және талдау • SIEM жүйесінде тіркеу журналдарын жинауды,

	қабылдауды, дұрыс тіркеуді және сақтауды қамтамасыз ету. Жиналатын киберқауіпсіздік оқиғаларының сақталуы төмендегі көлемдер мен мерзімдерде қамтамасыз етілуі тиіс: • кемінде 62 күнтізбелік күн – іздеу, қарау және оқиғаларды талдау мүмкіндігін қамтамасыз ете отырып, Өнім беруші тарапындағы жедел сақтау қоймасында; • кемінде 3 (үш) жыл – Тапсырыс беруші тарапындағы архивтік сақтау қоймасында. Өнім беруші архивтік деректерді кейіннен оқу, іздеу және талдау мүмкіндігін қамтамасыз ететін келісілген форматта Тапсырыс берушіге беруді қамтамасыз етуге міндетті. Деректерді беру тәртібі, форматы, архивтеу кезеңділігі, сақтау қоймасының көлеміне қойылатын талаптар және Тараптардың жауапкершілігі Өзара іс-қимыл регламентімен айқындалады. Қызмет көрсету мерзімі аяқталғаннан кейін Өнім беруші қызмет көрсету кезеңіне жататын архивтік деректерді Тапсырыс берушіге беруге және оларды одан әрі пайдалану мүмкіндігін қамтамасыз етуге міндетті. 2.5. Мониторинг және ден қою • кезекші қызмет арқылы тәулік бойы (24/7 режимінде) мониторинг жүргізу; • мониторинг аймағында киберқауіпсіздік оқиғалары мен инциденттерін анықтау және Тапсырыс берушінің жауапты қызметкерлеріне уақтылы хабарлау; • Өнім беруші өз бетінше анықтаған инцидент туралы анықталған сәттен бастап 15 минуттан кешіктірмей КҮҰО-ға хабарлау; • анықталған киберқауіпсіздік инциденттерін жою және олардың қайталануына жол бермеу жөнінде ұсынымдар беру. 2.6. Қолдау және консультациялық қызметтер • Тапсырыс берушінің киберқауіпсіздік бөлімі қызметкерлеріне тұрақты түрде консультациялық қолдау көрсету; • Тапсырыс берушінің өтініштерін тәулік бойы қабылдау және тіркеу; • артықшылықты есептік жазбалармен орындалатын әрекеттерді верификациялау және киберқауіпсіздік оқиғаларын автоматтандырылған түрде тексеру; • жалған оң нәтижелер беретін оқиғаларды азайту бойынша бірлескен жұмыс жүргізу; • компьютерлік криминалистика және инциденттерді тергеп-тексеру саласында консультациялар беру. 2.7. Қосу және пайдалану • шарт жасалған және толтырылған техникалық сауалнама парағы ұсынылған күннен бастап 10 жұмыс күні ішінде Тапсырыс берушінің ресурстарын КЖО (ЦОК) инфрақұрылымына қосуды қамтамасыз ету; • Тапсырыс берушінің өтінімдері негізінде және Техникалық сауалнама парағына сәйкес оқиғалар дереккөздерін қосу; • Тапсырыс беруші мен Өнім берушінің алаңдары арасындағы деректерді беру арнасының жұмысқа қабілеттілігін Тапсырыс берушімен бірлесіп қамтамасыз ету. 2.8. Қосымша талаптар • Өнім беруші қызмет көрсету кезеңінің барлық мерзімінде пайдаланылатын барлық бағдарламалық қамтылым мен жабдыққа қолданыстағы лицензиялардың, жазылымдардың және техникалық қолдаудың болуын қамтамасыз етуге міндетті. 2.9. Қызметтердің сипаттамасы және есептілікке қойылатын талаптар Өнім беруші қызметтерді Тапсырыс берушінің қажетті техникалық сипаттамалары көрсетілген сұрауы негізінде ұсынады. • Алаңдар саны және орналасқан мекенжайы: 1 алаң, Астана қаласы, Бейбітшілік көшесі, 49А. • Платформаның төмендегі параметрлерге сәйкес жұмысқа қабілеттілігін

	қамтамасыз ету: • платформаны қызмет көрсету кезеңі – 2026 жылғы 31 желтоқсанға дейін; • тәулік бойы 24/7 режимінде жедел мониторинг жүргізу; • айына технологиялық терезелер саны – 1-ден аспауы тиіс; • тоқтап қалу туралы хабарлау – кемінде 60 минут бұрын; • технологиялық терезенің ең ұзақ ұзақтығы – айына 6 сағаттан аспауы тиіс; • Тапсырыс берушінің ақпараттық жүйелерінің қолжетімділігіне немесе жұмысына әсер етуі мүмкін жоспарланған технологиялық терезе туралы Тапсырыс берушіге жұмыстар басталатын болжамды күн мен уақыттан кемінде 3 (үш) жұмыс күні бұрын хабарлау. Көрсетілетін қызметтердің техникалық және әкімшілік параметрлері: • келіп түсетін киберқауіпсіздік оқиғалары мен желілік пакеттерді өңдеу және талдау; • инфрақұрылымның негізгі компоненттерінен логтарды автоматтандырылған түрде жинау және талдау – жүктеме көлемі кемінде 1 ГБ. Өнім беруші есепті айдан кейінгі айдың 10-күнінен кешіктірмей шарттың орындалуы туралы мәтіндік, кестелік және графикалық (диаграммалар, графиктер) ақпаратты қамтитын ай сайынғы талдамалық есепті ұсынуы тиіс. Есепте мыналар көрсетілуі қажет: • есепті кезеңдегі сұраулар мен инциденттер бойынша статистикалық деректер; • мониторинг аймағындағы киберқауіпсіздік жағдайын талдау; • проблемалық мәселелердің тізбесі және оларды шешу, сондай-ақ киберқауіпсіздік инфрақұрылымының жұмысын жақсарту жөніндегі ұсынымдар (бар болған жағдайда). Киберқауіпсіздік инцидентіне ден қоюдың басталу уақыты оны анықтаған және уәкілетті қызметкерлерге хабарлаған сәттен бастап төмендегі қағидат бойынша айқындалады. Киберқауіпсіздік инциденттерінің сындық деңгейлері 1. Сындарлы – 5-деңгей (қара түс) Электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және ақпараттандырудың өзге де объектілеріне елеулі теріс салдарлар келтіріп, қызметтерді ұсыну мүмкіндігінің болмауына әкеп соғатын сөзсіз орын алатын инциденттер. Ден қою мерзімі: анықталған сәттен бастап 15 минуттан аспауы тиіс. 2. Ауыр – 4-деңгей (қызыл түс) Электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және ақпараттандырудың өзге де объектілеріне елеулі теріс салдарлар келтіріп, қызметтерді ұсыну мүмкіндігінің болмауына әкеп соғуы ықтимал инциденттер. Ден қою мерзімі: анықталған сәттен бастап 30 минуттан аспауы тиіс. 3. Жоғары – 3-деңгей (қызғылт сары түс) Қызметтерді ұсынудың едәуір шектелуіне, жағдайдың айтарлықтай нашарлауына немесе электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және ақпараттандырудың өзге де объектілеріне елеулі теріс салдарлардың туындауына әкеп соғуы ықтимал инциденттер. Ден қою мерзімі: анықталған сәттен бастап 30 минуттан аспауы тиіс. 4. Орташа – 2-деңгей (сары түс) Қызметтерді ұсынудың шектелуіне, жағдайдың нашарлауына немесе электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және ақпараттандырудың өзге де объектілеріне елеусіз теріс салдарлардың туындауына әкеп соғуы ықтимал инциденттер. Ден қою мерзімі: анықталған

	сәттен бастап 1 сағаттан аспауы тиіс. 5. Төмен – 1-деңгей (жасыл түс) Қызметтерді ұсынудың шектелуіне, жағдайдың нашарлауына немесе электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және ақпараттандырудың өзге де объектілеріне елеусіз теріс салдарлардың туындауына әкеп соғуы мүмкін ықтималдығы төмен инциденттер. Ден қою мерзімі: анықталған сәттен бастап 2 сағаттан аспауы тиіс. 6. Маңыздылығы жоқ – 0-деңгей (ақ түс) Электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, телекоммуникация желілеріне және ақпараттандырудың өзге де объектілеріне әсер етпейтін елеусіз инциденттер. Ден қою мерзімі: анықталған сәттен бастап 2 сағаттан аспауы тиіс. 2.10. Оқиғалар мониторингі қызметін көрсету кезеңіндегі жауапкершілік аймақтарын бөлу Өнім беруші шартқа қол қойылғаннан кейін 15 жұмыс күні ішінде Тапсырыс берушімен бірлесіп Өзара іс-қимыл регламентін әзірлейді және келіседі. Қызмет көрсету кезеңіндегі жауапкершілік аймақтарын бөлу Өнім берушінің жауапкершілігі: 1. Мониторинг аймағына кіретін Тапсырыс беруші инфрақұрылымының элементтеріне қатысты тіркелген инциденттер бойынша ден қою жөнінде ұсынымдар беруді қоса алғанда, киберқауіпсіздік оқиғаларына мониторинг және талдау жүргізу. 2. Тапсырыс беруші мен Өнім берушінің алаңдарында орнатылған киберқауіпсіздік оқиғаларын басқару ішкі жүйесінің компоненттерінің жай-күйіне мониторинг жүргізу. 3. Киберқауіпсіздік оқиғаларын басқару ішкі жүйесінің дұрыс жұмыс істеуін қамтамасыз ету. 4. Логтарды жіберу үшін дереккөздерге агенттерді орнату. 5. Дереккөздерден желілік ағындарды коллекторларға бағыттау. 6. КЖО (ЦОК) ұсынған ұсынымдарға сәйкес киберқауіпсіздік инциденттеріне ден қоюды, инциденттерді оқшаулауды, олардың салдарын жоюды және штаттық жұмыс режимін қалпына келтіруді қамтамасыз ету. 7. Тапсырыс беруші мен Өнім берушінің алаңдары арасындағы ақпаратты берудің қорғалған арналарының жұмысқа қабілеттілігін қамтамасыз ету. 8. Тапсырыс беруші мен КЖО (ЦОК) алаңдары арасындағы ақпаратты берудің қорғалған арналарының жұмысқа қабілеттілігін қамтамасыз ету. Киберқауіпсіздік оқиғаларына мониторинг және талдау жүргізу кезінде Тапсырыс беруші мен Өнім беруші арасындағы міндеттерді бөлу. Тапсырыс берушінің жауапкершілігі: 1. Киберқауіпсіздік оқиғаларын басқару ішкі жүйесінің дұрыс жұмыс істеуін қамтамасыз ету. 2. Логтарды жіберу үшін дереккөздерге агенттерді орнату. 3. Дереккөздерден желілік ағындарды коллекторларға бағыттау. 4. КЖО (ЦОК) ұсынған ұсынымдарға сәйкес киберқауіпсіздік инциденттеріне ден қоюды, инциденттерді оқшаулауды, олардың салдарын жоюды және штаттық жұмыс режимін қалпына келтіруді қамтамасыз ету. 5. Тапсырыс беруші мен Өнім берушінің алаңдары арасындағы ақпаратты берудің қорғалған арналарының жұмысқа қабілеттілігін қамтамасыз ету. 6. КЖО (ЦОК) ұсынымдарын орындау және киберқауіпсіздік инциденттеріне уақтылы ден қою. 7. Жабдықтар мен ақпараттық жүйелердің өзекті тізбесін ұсыну. 8. Мониторинг аймағына кіретін серверлік, коммуникациялық және компьютерлік жабдықтардың,

	сондай-ақ ақпараттық жүйелердің өзекті тізбесін ұсыну. 9. Тапсырыс беруші мен КЖО (ЦОК) алаңдары арасындағы ақпаратты берудің қорғалған арналарының жұмысқа қабілеттілігін қамтамасыз ету. 2.11. Оқиғалар мониторингіне арналған бағдарламалық қамтылымға қойылатын функционалдық талаптар • Жүйе қосымша нодтарды қосу мүмкіндігімен деректердің үлкен көлемін өңдеу үшін көлденең масштабтауды қолдауы тиіс. • Жүйе нодтар арасында деректерді репликациялауды қамтамасыз ететін кластерлік архитектураны және бір немесе бірнеше нод істен шыққан жағдайда автоматты қалпына келтіру мүмкіндігін қолдауы тиіс. • Жүйеде деректер көлемін тиімді басқару үшін деректерді уақыт белгілері бойынша бөлу мүмкіндігі болуы тиіс. Сондай-ақ жылдам іздеуді қамтамасыз ететін индекстеу функциясы бар үлкен көлемдегі логтарды сақтауды қолдауы тиіс. • Жүйе өнімділікті қамтамасыз ету және сұрауларды біркелкі бөлу үшін жүктемені теңгергіштерді пайдалана отырып, нодтар арасында жүктемені бөлу мүмкіндігіне ие болуы тиіс. • Жүйеде кластер нодтарының жұмысын тұрақты бақылау, сондай-ақ өнімділікті қадағалау және істен шығулар немесе шамадан тыс жүктемелер туралы уақтылы хабарлау функциясы болуы тиіс. • Жүйе өнімділік, ресурстардың жүктелуі, нодтар мен индекстердің жай-күйі туралы деректерді ұсынатын барлық компоненттердің жай-күйіне мониторинг жүргізуді қамтамасыз етуі тиіс. • Жүйе CPU, RAM, дискілік кеңістікті пайдалану, оқу/жазу операцияларының өнімділігі, индекстеу және сұрауларды орындау кезіндегі кідірістер сияқты метрикаларды бақылауға мүмкіндік беруі тиіс. • Кластердің қандай да бір компоненттері шамадан тыс жүктелген, істен шыққан немесе өнімділікте ауытқулар байқалған жағдайда ескертулер мен хабарландыруларды баптау мүмкіндігі болуы тиіс. • Жүйе масштабтауды және инфрақұрылымды басқаруды жеңілдету үшін конвейерлік шешімдерді қолдауы тиіс. • Жүйе бір нод істен шыққан жағдайда кластердің істен шығуын болдырмау үшін бірнеше мастер-нодты пайдалануы тиіс. • Жүйе жоғары қолжетімділікті және істен шығуға төзімділікті қамтамасыз ету үшін бірнеше физикалық немесе виртуалды серверге орналастырылатын көпнодты архитектураны қолдауы тиіс. • Жүйе істен шығуға төзімділікті және географиялық тұрғыдан бөлінген орталарды қамтамасыз ету үшін индекстерді бірнеше кластер арасында репликациялау мүмкіндігіне ие болуы тиіс. • Жүйе өнімділік пен деректердің қолжетімділігін арттыру мақсатында деректерді бір кластерден екіншісіне оқу және репликациялау мүмкіндіктерін қамтамасыз етуі тиіс, бұл деректердің қолжетімділігін арттыру үшін әртүрлі өңірлерде бірнеше кластерді орналастыруға мүмкіндік береді. • Жүйе сұрауларды орындау жылдамдығын арттыру және нодтарға түсетін жүктемені азайту үшін кэштеуді қолдауы тиіс. • Жүйе деректердің жылыстауынан қорғау үшін тыныштық күйіндегі және нодтар арасында беру кезіндегі деректерді шифрлауды пайдалануы тиіс. • Жүйе авариялық жағдайлар кезінде қалпына келтіру үшін деректердің тұрақты резервтік көшірмесін жасауды қамтамасыз етуі тиіс. • Жүйеде ең аз тоқтап қалу уақытымен

	резервтік көшірмеден деректерді қалпына келтіру мүмкіндігі болуы тиіс. • Жүйе талдау үшін тек өзекті логтарды сақтай отырып, уақыт немесе деректер көлемі негізінде ескі логтарды жоюды басқаруға арналған деректерді сақтау саясатын қамтамасыз етуі тиіс. • Жүйе жедел жұмыс үшін бұдан әрі қажет емес, бірақ ретроспективті талдау немесе аудит үшін қажет болуы мүмкін деректерді архивтеу мүмкіндігіне ие болуы тиіс. • Жүйе индекстердің өмірлік циклін деректердің жасына және көлеміне, олардың сақтау мерзіміне немесе өзектілігіне байланысты автоматты түрде басқаруға мүмкіндік беруі тиіс. • Жүйе деректерді сақтау мерзіміне немесе оларға қол жеткізу жиілігіне байланысты өнімділігі төмен немесе арзанырақ ресурстарға көшіру функциясын пайдалануға мүмкіндік беруі тиіс. • Жүйе пайдаланушылардан сұрауларды қабылдайтын, оларды нодтар арасында бөлетін және нәтижелерді жинақтайтын үйлестіруші нодтарды қамтамасыз етуі тиіс. • Жүйе кіріс деректерді индекстеуге дейін өңдейтін, сүзгілер мен түрлендірулерді (нормализацияны) қолданатын нодты қамтамасыз етуі тиіс. • Жүйе деректердің сақталу ұзақтығына немесе оларға қол жеткізу жиілігіне байланысты сақтау деңгейлері арасында деректерді автоматты түрде көшіру мүмкіндігіне ие болуы тиіс. • Жүйеде сұрауларды жылдам басқаруға және түзетуге мүмкіндік беретін кіріктірілген сұрауларды орындау интерфейсі болуы тиіс. • Жүйеде күрделі сұрауларды тестілеуге, сұраулардың өнімділігін талдауға, деректер мен олардың құрылымын тексеруге арналған кіріктірілген интерфейс болуы тиіс. • Жүйеде кластерді басқару командаларын орындауға арналған кіріктірілген интерфейс болуы тиіс. • Жүйе әртүрлі дереккөздерден алынған деректерді корреляциялау арқылы қауіп-қатерлерді анықтауға арналған қағидаларды әзірлеу мүмкіндігін қамтамасыз етуі тиіс. • Жүйе қауіп-қатерлерге жедел ден қою үшін деректерді нақты уақыт режимінде өңдеуі және талдауы тиіс. • Жүйе сүзгілер мен күрделі логикалық шарттарды пайдалана отырып, қауіп-қатерлерді анықтаудың әртүрлі сценарийлеріне арналған қағидаларды баптауға мүмкіндік беруі тиіс. • Жүйе инциденттерді сындық деңгейі бойынша жіктеуге және тиісті ескертулерді (хабарландыруларды) іске қосуға мүмкіндік беруі тиіс. • Жүйе инциденттерді тіркеу және оларға ден қоюды автоматтандыру платформасымен интеграциялануы тиіс. • Жүйе Syslog, JSON, XML, CSV және басқа да форматтарды пайдалана отырып, әртүрлі дереккөздермен (серверлер, желілік құрылғылар, дерекқорлар және т.б.) интеграцияны қолдауы тиіс. • Жүйе инциденттерді басқаруға, талдауға және есептілікке арналған басқа платформалармен интеграциялау үшін API ұсынуы тиіс. • Жүйе деректерді толықтыру мақсатында қауіп-қатерлер туралы ақпараттың сыртқы көздерімен (IOC дерекқорлары) интеграцияны қамтамасыз етуі тиіс. • Жүйе соңғы нүктелерден логтарды жинауға және оларды лог-коллекторға немесе тікелей өңдеу үшін Жүйеге жіберуге арналған агенттерді қамтамасыз етуі тиіс. • Жүйе деректердің белгілі бір түрлерін жинауға, қажетсіз деректерді сүзуге және трафик көлемін барынша азайтуға арналған оңай

	бапталатын агенттерді қамтамасыз етуі тиіс. • Жүйе берілетін деректер көлемін азайту үшін деректерді сығуды, сондай-ақ логтарды желі арқылы SIEM жүйесіне жіберу кезінде оларды қорғау үшін шифрлауды қамтамасыз ететін лог-коллектор компонентін қолдауы тиіс. • Жүйе агенттер мен коллекторлардың орнатылған жүйеге түсетін жүктемесі барынша аз болатындай оңтайландырылуын қамтамасыз етуі тиіс. • Жүйе әртүрлі дереккөздерден алынған оқиғалар арасында күрделі корреляция шарттарын құру үшін AND, OR, NOT логикалық операторларын пайдалануды қамтамасыз етуі тиіс. • Жүйе жалған іске қосылулар санын азайту және шабуылдарды дәлірек анықтау мақсатында ұқсас немесе өзара байланысты оқиғаларды бір инцидентке біріктіруді қамтамасыз етуі тиіс. • Жүйе қауіп-қатерлердің нақты сценарийлері мен ұйымның талаптарына бейімделетін, оңай бапталатын қағидаларды қосу мүмкіндігін қамтамасыз етуі тиіс. • Жүйе қауіп-қатерлерге ден қою уақытын қысқарту үшін деректердің келіп түсуі мен қағидалардың іске қосылуы арасындағы ең аз кідірісті қамтамасыз етуі тиіс. • Жүйе анықталған инциденттерді оқиғаның түрі мен мәнмәтініне байланысты сындық деңгейлері бойынша (төмен, орташа, жоғары) жіктеу мүмкіндігін қамтамасыз етуі тиіс. • Жүйе заңды әрекеттерге байланысты жалған іске қосылулар санын азайту үшін ерекшеліктер мен сүзгілерді қосу мүмкіндігін қамтамасыз етуі тиіс. • Жүйе анықталған инциденттер туралы қауіпсіздік командаларын жедел хабардар ету үшін хабарландыруларды (электрондық пошта, мессенджерлермен немесе басқа жүйелермен интеграциялау) баптау мүмкіндігін қамтамасыз етуі тиіс. • Жүйе жылдам талдау жүргізу үшін инциденттің сипаты туралы толық ақпаратты, оның ішінде метадеректерді (уақыты, дереккөзі, оқиға түрі, қауіп деңгейі) қамтуы тиіс. • Жүйеде жедел ден қою және қауіпсіздіктің негізгі саясаттарын баптау үшін дайын қағидалар үлгілерін пайдалану мүмкіндігі болуы тиіс. • Жүйе корреляция дәлдігін арттыру және шабуылдардың жаңа түрлерін анықтау үшін тарихи деректер негізінде қағидаларды тұрақты түрде қайта қарау және баптау мүмкіндігін қолдауы тиіс. • Жүйе агенттерді орнатпай-ақ дереккөздерден логтарды тікелей берудің әртүрлі хаттамаларын қолдауы тиіс. • Жүйе деректерді одан әрі өңдеу, корреляциялау және талдау үшін әртүрлі дереккөздерден орталықтандырылған сақтау қоймасына жинауды қамтамасыз ететін лог-коллектор компонентін қолдауы тиіс. • Жүйе тұрақты өрнектер (regular expressions) негізінде сүзу қағидаларын құру мүмкіндігіне ие болуы тиіс. • Жүйе логтардағы белгілі бір оқиғаларға, мысалы шекті мәндердің асып кетуіне байланысты хабарландырулар немесе дабыл сигналдарын қалыптастыру қағидаларын қолдауы тиіс. • Жүйе деректерді әртүрлі мақсаттарға логикалық бағыттау қағидаларын қолдауы тиіс (мысалы, желілік логтарды бір сақтау қоймасына, ал қосымшалардың логтарын басқа сақтау қоймасына жіберу). • Жүйе көлденең масштабтауды қамтамасыз ету үшін логикалық бөлімдерді бөлуді қолдауы тиіс. Логикалық бөлімдер автоматты түрде фрагменттерге бөлініп, олар кластердің әртүрлі нодтарына орналастырылуы

	тиіс. • Әрбір логикалық бөлімге негізгі (primary) фрагменттердің оңтайлы саны тағайындалуы тиіс, бұл жүйенің үлкен көлемдегі деректермен жұмыс істеу өнімділігін арттыру үшін жүктемені бірнеше серверге бөлуге мүмкіндік береді. • Жүйе жоғары қолжетімділік пен істен шығуға төзімділікті қамтамасыз ету үшін фрагменттерді репликациялауды қолдауы тиіс. Логикалық бөлімдердің әрбір негізгі фрагменті үшін негізгі нод істен шыққан жағдайда автоматты түрде іске қосыла алатын репликалар құрылуы тиіс. • Қажет болған жағдайда жүйе деректерді жоғалтпай және жұмыстағы іркілістерді барынша азайта отырып, логикалық бөлімдердің фрагменттерін динамикалық қайта бөлу, олардың санын және репликаларын өзгерту мүмкіндігін қамтамасыз етуі тиіс. • Жүйе әкімшіге агенттердің конфигурациясын, жаңартуларын және мониторингін бір консольден басқаруға мүмкіндік беретін барлық агенттерді орталықтандырылған басқаруды қамтамасыз етуі тиіс. • Жүйе құрылғыларға физикалық қол жеткізуді қажет етпей, агенттерді қашықтан басқару, оның ішінде оларды жаңарту және құрылғылардан жою мүмкіндігін қолдауы тиіс. • Жүйе агенттер топтарына арналған саясаттарды құру және басқару мүмкіндігін қолдауы тиіс, олар қандай деректерді жинау және оларды қалай өңдеу керектігін айқындайды. • Жүйе агенттердің әртүрлі топтары үшін жиналатын логтар мен метрикалардың түрлерін, сондай-ақ деректерді өңдеу параметрлерін қоса алғанда, әртүрлі параметрлерді баптауға мүмкіндік беретін икемді саясаттарды қамтамасыз етуі тиіс. • Жүйе саясаттарға енгізілген өзгерістерді тағайындалған агенттердің барлық топтарына жедел таратуды қолдауы тиіс. • Жүйе агенттер арқылы берілетін деректерді шифрлауды қамтамасыз етіп, оларды рұқсатсыз қол жеткізуден қорғауы тиіс. • Жүйе агенттердің жұмысқа қабілеттілігін, өнімділігін және дұрыс жұмыс істеуін бақылауға мүмкіндік беретін барлық агенттердің жай-күйіне нақты уақыт режимінде мониторинг жүргізуді қамтамасыз етуі тиіс. • Жүйе агенттердің жұмысын тоқтатпай және деректерді жоғалтпай жоспарлы жаңартуды қолдауы тиіс. • Жүйе логтардағы ауытқулар мен күмәнді әрекеттерді анықтау арқылы деректерді талдау процесін автоматтандыруға мүмкіндік беретін машиналық оқыту мүмкіндіктерін қарастыруы тиіс. • Жүйе уақыттық қатарларға негізделген деректердегі ауытқуларды автоматты түрде анықтайтын машиналық оқыту модельдерін қамтамасыз етуі тиіс. • Жүйе пайдаланушының машиналық оқыту алгоритмдерін интеграциялауға мүмкіндік беруі тиіс. • Жүйе өнімділікке әсер етпей есептер мен талдамалық материалдарды жылдам қалыптастыру үшін жеделдетілген деректер модельдерін құруға және арнайы интерфейсті пайдалануға мүмкіндік беруі тиіс. • Жүйе пайдаланушыларға машиналық оқыту модельдерінің параметрлерін баптау және оңтайлы нәтижелерге қол жеткізу үшін оларды өз деректері негізінде оқыту мүмкіндігін ұсынуы тиіс. 2.12. Осалдықтарды сканерлеуге қойылатын функционалдық талаптар • Өнім беруші Тапсырыс берушімен бірлесіп сканерлеу көлемін (жүйелерді, желілерді, қосымшаларды) айқындайды; • Өнім беруші нысаналы жүйе, оның

	архитектурасы, пайдаланылатын технологиялары мен конфигурациясы туралы ақпарат жинауға міндетті; • Өнім беруші лицензияланған бағдарламалық қамтылымды қолдана отырып, pentest және audit режимдерінде сканерлеу жүргізеді; • Өнім беруші пайдаланылатын бағдарламалық қамтылым нұсқаларындағы белгілі осалдықтарды іздеуге бағытталған аспаптық сканерлеу жүргізуге міндетті; • Өнім беруші анықталған осалдықтардың сындық деңгейі мен ықтимал салдарын айқындау үшін сканерлеу нәтижелеріне бағалау жүргізеді; • Өнім беруші тәуекелдерге талдау жүргізеді; • Өнім беруші тәуекел деңгейін бағалайды: анықталған осалдықтарды пайдалану жүйе немесе ұйым үшін қандай дәрежеде ауыр салдарға әкелуі мүмкін екенін айқындайды; • Өнім беруші осалдықтардың басымдықтарын айқындайды. Қандай осалдықтарды жою ең жоғары басымдыққа ие екенін анықтайды; • Өнім беруші Тапсырыс берушімен алдын ала келісілген, анықталған осалдықтар, олардың сындық деңгейі және оларды жою жөніндегі ұсынымдар туралы толық ақпарат қамтылған есеп дайындайды; • Өнім беруші Тапсырыс берушіге осалдықтарды жою жөніндегі іс-қимыл жоспарын әзірлеуге консультациялық қолдау көрсетеді. 2.13. Бастапқы кодты статикалық талдау құралына қойылатын функционалдық талаптар 2.13.1. Жалпы талаптар Ұсынылатын шешімнің құрамында төмендегі мүмкіндіктер мен функциялар болуы тиіс: • лицензияланған бағдарламалық қамтылымды қолдана отырып, бастапқы код бойынша бағдарламалық қамтылымды (БҚ) ақпараттық қауіпсіздік талаптарына сәйкестігіне талдау; • debug info және бастапқы кодтар болмаған жағдайда byte-код бойынша (статикалық талдау әдісімен) бағдарламалық қамтылымды (БҚ) ақпараттық қауіпсіздік талаптарына сәйкестігіне талдау; • бағдарламалық қамтылымдағы декларацияланбаған мүмкіндіктерді (ДМ) іздеу; • қосымшаларды талдау нәтижелері бойынша пайдалануын ақпаратты қорғау құралдарын (АҚҚ) баптау арқылы болдырмауға болатын осалдықтар мен ДМ үшін АҚҚ баптау жөніндегі ұсынымдарды беру. Осалдықтар мен ДМ-ді іздеу төмендегі статикалық талдау алгоритмдерін, соның ішінде олармен шектелмей, қолдану арқылы жүзеге асырылуы тиіс: • үлгілер бойынша талдау әдісі арқылы іздеу; • басқару ағынын талдау әдісі арқылы іздеу; • taint-талдау әдісі арқылы іздеу; • синонимдерді талдау әдісі арқылы іздеу; • константаларды тарату әдісі арқылы іздеу. 2.13.2. БҚ-ны бастапқы код бойынша талдауға қойылатын талаптар БҚ-ны бастапқы код бойынша талдау төмендегі талаптарға сәйкес болуы тиіс: • шешім төмендегі бағдарламалау тілдеріндегі бастапқы кодқа талдау жүргізуі тиіс: Java, Java for Android, JavaScript, JSP, TypeScript, VBScript, Scala, HTML5, PHP, Python, Groovy, Kotlin, Go, Ruby, C#, C/C++, Objective C, Swift, ABAP, Apex, Solidity, PL/SQL, T/SQL, Visual Basic 6.0, Delphi, COBOL, VBA, 1C, ASP.NET, Perl, Vyper, VB.NET, LotusScript, Pascal, Dart, Rust, YAML, TOML, SQL, Bash, PowerShell, XML; • шешім тілдерді автоматты түрде тану арқылы көптілді жобаларға талдау жүргізе алуы тиіс; • шешім бастапқы кодты ішкі көрініске түрлендіруі тиіс; • шешім құрастыру құралдарымен

	интеграцияны қамтамасыз етуі тиіс; • алынған ішкі көрініске осы техникалық ерекшеліктің жалпы талаптарында сипатталған осалдықтар мен ДМ-ді іздеу әдістері қолданылуы тиіс. 2.13.3. БҚ-ны екілік код бойынша талдауға қойылатын талаптар БҚ-ны byte-код бойынша талдау төмендегі талаптарға сәйкес болуы тиіс: • шешім Java/Scala: JAR/WAR/EAR/AAR; C/C++: DLL/EXE; Android: APK; Apple iOS: IPA; Apple macOS: APP тілдері мен форматтарынан түрлендіру арқылы алынған byte-кодқа талдау жүргізуі тиіс; • шешім byte-кодты ішкі көрініске түрлендіруі тиіс; • алынған ішкі көрініске осы техникалық ерекшеліктің жалпы талаптарында сипатталған осалдықтар мен ДМ-ді іздеу әдістері қолданылуы тиіс. 2.13.4. Есептілікке қойылатын талаптар Шешім қосымшаны талдау нәтижелері бойынша төмендегі талаптарға сәйкес есептілікті ұсынуы тиіс: • барлық есептілік орыс және/немесе ағылшын тілдерінде ұсынылуы тиіс; • анықталған осалдықтар бойынша есеп файлын CSV, HTML, PDF, SARIF форматтарында қалыптастыру; • анықталған осалдықтар бойынша PCI DSS, OWASP Top 10, OWASP Mobile Top 10, HIPAA, CWE/SANS, OWASP MASVS стандарттарына сәйкестік туралы есеп файлын қалыптастыру. 2.13.5. Инфрақұрылымдық сервистермен интеграцияға қойылатын талаптар Ақпараттық жүйеде SVN/Git репозиторийлерімен, Jenkins, TeamCity, Azure DevOps Server, Gitlab CI CI/CD сервистерімен, GitHub, GitLab, BitBucket VCS хостингтерімен, Jira қателерді бақылау құралдарымен интеграциялау мүмкіндігі болуы қажет. Ашық кіріктірілген API көмегімен басқа жүйелермен және сервистермен интеграциялау мүмкіндігі қолжетімді болуы тиіс. 3. Байланыс нысаны Өнім беруші өз өкілдерінің байланыс деректерін (телефон нөмірі және электрондық пошта мекенжайы) ұсынуы тиіс. Орындаушы мен Тапсырыс беруші арасындағы коммуникация олардың өкілдері арасында телефон және/немесе электрондық пошта арқылы жүзеге асырылады. Құжаттардың электрондық нұсқалары Тапсырыс берушінің электрондық поштасына жіберілуі тиіс. Қағаз түріндегі нәтижелер Тапсырыс берушінің кеңсесіне мына мекенжай бойынша жеткізіледі: Астана қаласы, Бейбітшілік көшесі, 49А. 4. Қызмет көрсету мерзімі Қызмет көрсету мерзімі шартқа қол қойылған күннен басталады және 2026 жылғы 31 желтоқсанға дейін жалғасады. Өнім беруші шарт талаптары мен Тапсырыс берушінің талаптарына сәйкес барлық жұмыстарды орындауға міндеттенеді. 5. Қызмет көрсетуге қойылатын талаптар Осы бөлімде қызмет көрсетуге қойылатын негізгі талаптар көрсетілген: • Өнім беруші шарт талаптарын, сондай-ақ техникалық ерекшелікте немесе басқа да ресми құжаттарда көрсетілген кез келген қосымша талаптарды сақтауы тиіс; • Өнім беруші шартта немесе техникалық тапсырмада көрсетілген міндеттерді орындау мерзімдерін сақтауы және кез келген кідірістер немесе мерзімдердің өзгеруі туралы Тапсырыс берушіге хабарлауы тиіс; • Өнім беруші Тапсырыс берушімен ашық әрі тиімді коммуникацияны қамтамасыз етуге, сұрауларға жауап беруге және Астана уақыты бойынша сағат 08:30-дан 18:30-ға дейін жұмыстардың орындалу барысы туралы қажетті ақпаратты ұсынуға тиіс. 6.

	Құпиялылықты сақтауға қойылатын талаптар • Өнім беруші жұмыстарды Қазақстан Республикасының киберқауіпсіздікті қамтамасыз ету саласындағы заңнамасының талаптарына сәйкес орындауы тиіс; • Өнім беруші жұмыстарды орындау кезінде ақпараттық ресурстар мен жүйелерде орналасқан ақпараттың сақталуын, оның құпиялылығын, сондай-ақ Тапсырыс берушіден алынған құжаттардың сақталуы мен құпиялылығын қамтамасыз етуі тиіс; • Өнім беруші киберқауіпсіздік саласындағы Қазақстан Республикасының заңнамасының талаптарын қатаң сақтауға міндетті. Бұл дербес деректерді, коммерциялық құпияны қорғау, ақпаратты құқықтық қорғау туралы заңдардың және құпия ақпаратты өңдеу мен сақтауды реттейтін өзге де нормативтік актілердің талаптарын сақтауды қамтиды; • Өнім беруші ақпараттық ресурстар мен жүйелерде орналасқан ақпараттың сақталуын, сондай-ақ осы деректердің құпиялылығын қамтамасыз етуге міндетті. Бұл ақпаратты рұқсатсыз қол жеткізуден, өзгертуден, жоғалтудан немесе жоюдан қорғау шараларын қабылдауды қамтиды; • Өнім беруші Тапсырыс берушіден алынған құжаттар мен ақпараттың сақталуы мен құпиялылығын қамтамасыз етуге міндетті. Бұл құжаттарды рұқсатсыз қол жеткізуден және пайдаланудан қорғау шараларын қабылдауды, сондай-ақ жұмыстарды орындаудың бүкіл кезеңінде, сонымен қатар құпиялылық туралы келісімде және/немесе құпия ақпарат пен коммерциялық құпияны жария етпеу туралы міндеттемеде белгіленген мерзімдер мен шарттарда олардың сақталуын қамтамасыз етуді білдіреді. Аталған келісім мен міндеттеме Орындаушымен және/немесе тартылған мамандармен Тапсырыс берушінің ақпараттық жүйелеріне, техникалық құжаттамасына, бастапқы кодтарына, инфрақұрылымына және өзге де ақпаратына қол жеткізу берілгенге дейін жасалуы тиіс; • Өнім беруші ақпараттың жылыстауын немесе рұқсатсыз таратылуын болдырмау үшін деректерді шифрлау, құпиясөздерді орнату және басқа да техникалық қорғау құралдары сияқты ақпаратты сақтау мен өңдеудің қауіпсіз әдістерін пайдалануы тиіс; • Өнім беруші өз персоналын ақпараттың құпиялылығын қамтамасыз ету қағидалары мен рәсімдеріне оқытуға, сондай-ақ ақпаратты қорғау жүйесінің тиімділігін және оның заңнама мен қауіпсіздік стандарттарының талаптарына сәйкестігін қамтамасыз ету мақсатында жүйелі түрде тексеру мен аудит жүргізуге міндетті; • Қызмет көрсету басталғанға дейін және Тапсырыс берушінің ақпараттық жүйелеріне, бастапқы кодтарына, техникалық құжаттамасына, инфрақұрылымына және өзге де ақпаратына қол жеткізу берілгенге дейін Өнім беруші Тапсырыс берушімен құпиялылық туралы келісімге қол қояды. Өнім беруші сондай-ақ Тапсырыс берушінің ақпаратына қол жеткізілетін барлық өз қызметкерлерінің, консультанттарының, қосалқы мердігерлерінің және өзге де тартылған мамандарының құпия ақпарат пен коммерциялық құпияны жария етпеу туралы міндеттемелерге қол қоюын қамтамасыз етуге міндетті. Көрсетілген тұлғалардың құпиялылық талаптарын сақтауына Өнім беруші жауапты болады. 7. Қызмет көрсету орны Бейбітшілік көшесі, 49А, Абай көшесі, 47.

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)	Өнім беруші келісімшартт жасалған күннен бастап 3 жұмыс күні ішінде ұсынуға тиіс: • Қазақстан Республикасының Ұлттық аккредитация жүйесінде жарамды Аккредитация аттестаты; • Аккредиттелген зертханалар тізіліміне енгізілгенін растайтын құжаттар; • Ақпараттық жүйелерді сынауды қамтитын аккредитация саласындағы құжаттар; • Зертхана Паспортында көрсетілген мамандарды растайтын құжаттар. Өнім беруші жұмыстарды орындауды/қызмет көрсетуді бастар алдында Тапсырыс берушімен құпия ақпаратты жария етпеу туралы келісімге (NDA) қол қоюға міндетті.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Некоммерческое акционерное общество "Национальный медицинский университет имени Төрегелді Шарманова"
Наименование организатора	Некоммерческое акционерное общество "Национальный медицинский университет имени Төрегелді Шарманова"
№ конкурса:	№ 17930563-1
Наименование конкурса:	Услуги по обеспечению кибербезопасности
Номер лота:	№ 88515813-ОК1
Наименование лота:	Услуги по обеспечению информационной безопасности
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	801019.000.000010
Наименование услуги:	Услуги по обеспечению информационной безопасности
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	12000000
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	12000000
Срок оказания услуги:	согласно технической спецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	1. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых ТРУ Настоящая Техническая спецификация (далее – ТС) содержит описание основных задач и требований, предъявляемых к оказанию услуг по обеспечению кибербезопасности (далее – Услуга). Услуга включает в себя проведение испытаний информационных систем Заказчика на соответствие установленным требованиям в области кибербезопасности, а также оказание услуг непрерывного мониторинга событий информационной безопасности, своевременного выявления, анализа и сопровождения инцидентов кибербезопасности, выявления уязвимостей и предоставления рекомендаций по повышению уровня защищённости информационных систем и информационной инфраструктуры Заказчика. 2. Требования к Услуге Услуга должна соответствовать требованиям, перечисленным ниже. 2.1 Функциональные требования Услуга должна оказываться в соответствии с Приказом Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ «Об утверждении методики и правил проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности», а также иными действующими нормативными правовыми актами и государственными стандартами Республики Казахстан в сфере кибербезопасности. В услугу по обеспечению кибербезопасности на соответствие требованиям системы Заказчика входит: 1) Анализ исходных кодов: выявление недостатков ПО; фиксация результатов анализа исходного кода; предоставление протокола по результатам анализа исходных кодов. 2) Испытание функций кибербезопасности: оценка соответствия функций безопасности требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информационной безопасности, в том числе с применением программных средств (при необходимости); фиксация результатов испытания в отчете с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости); предоставление протокола по результатам испытаний функций кибербезопасности. 3) Нагрузочное испытание: настройка конфигурации и сценария испытания в специализированное программное средство; запуск специализированного программного средства; регистрация нагрузки на объект испытаний; формирование и выдача отчета нагрузочного испытания с указанием рекомендаций по увеличению или снижению реальной пропускной способности объекта испытаний; предоставление протокола по результатам нагрузочного испытания. 4) Обследование сетевой инфраструктуры: оценку соответствия функций защиты сетевой инфраструктуры требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере кибербезопасности; обследование сетевой инфраструктуры

	Заказчика, в том числе с применением программных средств (при необходимости); сканирование программным средством на наличие известных уязвимостей программного обеспечения из базы общих уязвимостей и рисков; фиксацию полученных результатов испытания в отчете с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости); предоставление протокола по результатам обследования сетевой инфраструктуры. 5) Обследование процессов обеспечения кибербезопасности: оценку соответствия процессов обеспечения кибербезопасности требованиям нормативных правовых актов и стандартов в сфере обеспечения кибербезопасности; фиксацию результатов оценки испытания с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости); сканирование серверов, виртуальных ресурсов и сетевого оборудования программными средствами на наличие известных уязвимостей; анализ выявленных уязвимостей на наличие ложного срабатывания и формирование рекомендаций по их устранению в зависимости от степени их критичности (при необходимости); предоставление протокола по результатам обследования процессов обеспечения информационной безопасности. Обследование процессов обеспечения кибербезопасности проводится в соответствии с пунктом 31 Правил проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности. 2.2 В рамках оказания услуг поставщик должен обеспечить централизованный сбор, обработку, хранение и анализ событий информационной безопасности, круглосуточный мониторинг информационной инфраструктуры Заказчика, выявление инцидентов кибербезопасности, уведомление Заказчика и предоставление рекомендаций по реагированию и устранению выявленных инцидентов, а именно: Анализ объекта информатизации Заказчика на предмет определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями кибербезопасности; Установку агентов Системы на единую систему сбора журналов регистрации событий объекты информатизации Заказчика и при необходимости на иные объекты информационно-коммуникационной инфраструктуры объекта информатизации Заказчика; Сбор журналов регистрации событий с объектов информатизации Заказчика в Системе, их обработку и анализ с целью выявления событий кибербезопасности и инцидентов кибербезопасности; Выявление инцидентов кибербезопасности, произошедших в зоне мониторинга; Предоставление рекомендаций Заказчику по устранению инцидентов кибербезопасности и дальнейшему их предупреждению; Разработка правил корреляций; Серверное оборудование для сбора «Лог-файлов», системных журналов, компонентов SIEM-системы предоставляется Заказчиком. Применение требований политики кибербезопасности, мер управления, процессов и процедур обеспечения кибербезопасности; Проведение

	инструментального обследования объектов информатизации Заказчика на наличие уязвимостей с применением лицензируемых программных обеспечении в режиме audit, pentest (далее – обследование на уязвимости) согласно графику проведения работ, согласованному с Заказчиком; Предоставлять результаты обследования на уязвимости кибербезопасности и рекомендации по устранению уязвимостей кибербезопасности Заказчика; Мониторинг 24*7 Дежурной службой; Регулярное консультирование ответственных сотрудников отдела по кибербезопасности Заказчика; Обеспечение круглосуточного приема и регистрации обращений Заказчика; Настройку источников событий на формирование событий безопасности в соответствии с форматами и типами записей, определенными в Правилах проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов № 52/НҚ и отправки в коллектор сбора событий; Анализ событий в реальном времени в соответствие с правилами корреляции; Уведомление, в соответствии с требованиями законодательства Республики Казахстан, Национального координационного центра кибербезопасности (далее – НКЦКБ) о самостоятельно выявленном инциденте кибербезопасности в течение 15 минут с момента выявления; Поставщик должен обеспечивать наличие действующих лицензий, подписок и технической поддержки на используемое программное обеспечение. Перечень информационных систем, серверов, сетевого оборудования и иных источников событий, подлежащих подключению к ЦОК, определяется совместно Исполнителем и Заказчиком и фиксируется в согласованном перечне источников событий. Подключение дополнительных источников событий осуществляется на основании заявки Заказчика и в порядке, установленном Регламентом взаимодействия сторон. Поставщик обязан обеспечить работоспособность предоставляемых им компонентов ЦОК, программного обеспечения, агентов и коллекторов в пределах своей зоны ответственности. 2.3. Аналитические и подготовительные работы - Проведение анализа объектов информатизации Заказчика для определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями кибербезопасности. - Настройку и установку агентов лицензированной SIEM-системы на объекты информатизации Заказчика. -Настройка источников событий на формирование логов в соответствии с форматами и типами записей, определенными в Правилах проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов № 52/НҚ. 2.4. Сбор, хранение, обработка и анализ событий -Сбор, прием, корректная регистрация и хранение журналов регистрации событий в SIEM-системе. Хранение собираемых событий кибербезопасности должно обеспечиваться в следующих объёмах и сроках: • не менее 62 календарных дней – в оперативном хранилище на стороне Исполнителя с обеспечением возможности поиска, просмотра и анализа событий; • не менее 3 (трёх) лет – в архивном хранилище на стороне Заказчика. Поставщик

	обязан обеспечить передачу архивных данных Заказчику в согласованном формате, обеспечивающем возможность их последующего чтения, поиска и анализа. Порядок передачи, формат данных, периодичность архивирования, требования к объёму хранилища и ответственность сторон определяются Регламентом взаимодействия. По окончании срока оказания услуг Поставщик обязан передать Заказчику архивные данные, относящиеся к периоду оказания услуг, и обеспечить возможность их дальнейшего использования. 2.5. Мониторинг и реагирование - Круглосуточный мониторинг (в режиме 24/7) дежурной службой. - Выявление событий и инцидентов кибербезопасности в зоне мониторинга и своевременное уведомление ответственных сотрудников Заказчика. -Уведомление НКЦКБ о самостоятельно выявленном инциденте в течение не более 15 минут с момента обнаружения. - Предоставление рекомендаций по устранению выявленных инцидентов кибербезопасности и предотвращению их повторного возникновения. 2.6. Поддержка и консультационные услуги - Регулярное консультирование сотрудников отдела кибербезопасности Заказчика. - Круглосуточный прием и регистрация обращений Заказчика. - Верификация действий с привилегированными учетными записями и автоматизированная проверка событий кибербезопасности. - Совместная работа над исключением ложноположительных событий. - Консультации в области компьютерной криминалистики и расследования инцидентов. 2.7. Подключение и эксплуатация - Подключение ресурсов Заказчика к инфраструктуре ЦОК в течение 10 рабочих дней с момента заключения договора и предоставления заполненного Опросного технического листа. - Подключение источников событий по заявкам Заказчика в соответствии с Опросным техническим листом. - Обеспечение работоспособности канала передачи данных между площадками Заказчика и Поставщика совместно с Заказчиком. 2.8. Дополнительные требования - Поставщик обязан обеспечить наличие действующих лицензий, подписок и технической поддержки на все используемое программное обеспечение и оборудование на весь период оказания услуг. 2.9. Описание услуг и требования к отчетности Поставщик предоставляет услуги на основе запроса Заказчика с указанием требуемых технических характеристик. - Количество площадок и адреса расположения: 1 площадка, город Астана, ул. Бейбитшилик 49а. - Обеспечение работоспособности платформы со следующими параметрами: - Период обслуживания платформы – по 31 декабря 2026 года; - Оперативный мониторинг в режиме работы 24/7; - Количество технологических окон за месяц - не более 1; - Уведомление о простоях - не менее чем за 60 минут; - Максимальная длительность технологического окна - не более 6 часов в месяц; - Уведомление Заказчика о планируемом технологическом окне не позднее чем за 3 (три) рабочих дня до предполагаемой даты и времени начала работ, способных повлиять на доступность или функционирование информационных систем Заказчика. - Технические и административные параметры оказываемых услуг: - Обработка и анализ поступающих событий

	кибербезопасности и сетевых пакетов; - Автоматизированный сбор и анализ логов с ключевых компонентов инфраструктуры - нагрузка не менее 1 ГБ. Поставщик не позднее 10 числа месяца, следующего за отчетным должен предоставить ежемесячный аналитический отчет с текстовой, табличной и графической (диаграммы, графики) информацией по исполнению Договора, а именно: - статистические данные по запросам и инцидентам за отчетный период; - анализ состояния кибербезопасности в зоне мониторинга; - перечень проблемных вопросов и рекомендации по их решению и улучшению работы инфраструктуры кибербезопасности (при наличии). Время начала реагирования на инцидент кибербезопасности с момента его обнаружения и уведомления уполномоченных работников определяется по следующему принципу: Уровни критичности инцидентов кибербезопасности 1. Критичный — уровень 5 (черный) Неизбежные инциденты, которые приведут к невозможности предоставления услуг и значительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации. Срок реагирования: с момента обнаружения — не более 15 минут. 2. Серьезный — уровень 4 (красный) Возможные инциденты, которые приведут к невозможности предоставления услуг и значительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации. Срок реагирования: с момента обнаружения — не более 30 минут. 3. Высокий — уровень 3 (оранжевый) Возможные инциденты, которые приведут к существенному ограничению предоставления услуг, существенному ухудшению ситуации или существенным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации. Срок реагирования: с момента обнаружения — не более 30 минут. 4. Средний — уровень 2 (желтый) Вероятные инциденты, которые приведут к ограничению предоставления услуг, ухудшению ситуации или незначительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации. Срок реагирования: с момента обнаружения — не более 1 часа. 5. Низкий — уровень 1 (зеленый) Маловероятные инциденты, которые могут привести к ограничению предоставления услуг, ухудшению ситуации или незначительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации. Срок реагирования: с момента обнаружения — не более 2 часов. 6. Некритичный — уровень 0 (белый) Нес существенные инциденты, не оказывающие влияния на электронные информационные ресурсы, информационные системы, сети телекоммуникаций и другие объекты информатизации. Срок реагирования: с момента обнаружения — не более 2 часов. 2.10. Разграничение зон ответственности на период оказания услуги мониторинга событий Поставщик после подписания Договора, в течение 15 рабочих дней совместно

	с Заказчиком разрабатывают и согласовывают Регламент взаимодействия; Разграничение зон ответственности на период оказания Услуг Ответсвтенность поставщика: 1) Мониторинг и анализ событий кибербезопасности, включая предоставление рекомендаций по реагированию на инциденты, зарегистрированные в отношении элементов инфраструктуры Заказчика, входящих в Зону мониторинга. 2) Мониторинг состояния компонентов подсистемы управления событиями кибербезопасности, установленных на площадках Заказчика и Поставщика. 3) Обеспечение корректного функционирования подсистемы управления событиями кибербезопасности 4) Установка агентов на источниках для отправки логов 5) Направление сетевых потоков с источников в коллекторы 6) Реагирование на инциденты кибербезопасности, локализация инцидентов, устранение их последствий и восстановление штатного режима работы согласно рекомендациям, предоставленным ЦОК. 7) Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и Поставщика 8) Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и ЦОК Распределение обязанностей между Заказчиком и услуг при оказании услуги мониторинга и анализа событий кибербезопасности. Ответсвтенность заказчика: 1) Обеспечение корректного функционирования подсистемы управления событиями кибербезопасности 2) Установка агентов на источниках для отправки логов 3) Направление сетевых потоков с источников в коллекторы 4) Реагирование на инциденты кибербезопасности, локализация инцидентов, устранение их последствий и восстановление штатного режима работы согласно рекомендациям, предоставленным ЦОК. 5) Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и Поставщика 6) Выполнение рекомендаций ЦОК и своевременное реагирование на инциденты кибербезопасности 7) Предоставление актуального перечня оборудования и информационных систем предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга. 8) Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и ЦОК 2.11. Функциональные требования к программному обеспечению мониторинга событий Система должна поддерживать горизонтальное масштабирование для обработки больших объемов данных с возможностью добавления дополнительных нод. Система должна поддерживать кластерную архитектуру с репликацией данных между нодами для обеспечения отказоустойчивости и автоматическое восстановление в случае сбоя одной или нескольких нод. Система должна иметь возможность разделения данных по временным меткам для более эффективного управления объемом данных. А также использоваться для хранения больших объемов логов с поддержкой индексации для быстрого поиска. Система должна иметь возможность распределение нагрузки между нодами с использованием балансировщиков нагрузки для обеспечения производительность и равномерное

	распределение запросов. Система должна иметь функциональность постоянного мониторинга работы нод кластера, а также отслеживание производительности и своевременное уведомление о сбоях или перегрузках. Система должна обеспечить мониторинг состояние всех компонентов, который предоставляет данные по их производительности, загрузке ресурсов, здоровью нод и индексов Система должна позволять отслеживать метрики, такие как использование CPU, RAM, дискового пространства, производительность операций чтения/записи, задержки в индексировании и запросах. Система должна иметь возможность настройки алертов и уведомлений, если какие-либо компоненты кластера работают с перегрузкой, возникли сбои, или наблюдаются аномалии в производительности Система должна поддерживать конвейеризированные решения для масштабируемости и легкости управления инфраструктурой. Система должна использовать несколько мастер-нод для предотвращения сбоев кластера в случае отказа одной ноды. Система должна поддерживать многоузловую архитектуру для распределения по нескольким физическим или виртуальным серверам для обеспечения отказоустойчивости. Система должна иметь возможность реплицировать индексы между несколькими кластерами для обеспечения отказоустойчивости и географически распределенных сред. Система должна. обеспечить возможности чтения и репликации данных с одного кластера на другой, что позволяет развернуть несколько кластеров в разных регионах для повышения производительности и доступности данных. Система должна поддерживать кеширования для увеличения скорости выполнения запросов и снижения нагрузки на ноды. Система должна использовать шифрования для данных в состоянии покоя и при передаче между нодами для защиты от утечек. Система должна обеспечить регулярное резервное копирование данных для восстановления в случае аварий. Система должна иметь Возможность восстановления данных из резервной копии с минимальным временем простоя. Система должна обеспечить политику хранения данных, чтобы управлять удалением старых логов на основе времени или объема данных, сохраняя только релевантные логи для анализа. Система должна иметь возможность архивирования данных, которые больше не нужны для оперативной работы, но могут понадобиться для ретроспективного анализа или аудита. Система должна позволять автоматически управлять жизненным циклом индексов в зависимости от возраста и объема данных в соответствии с их "сроком годности" или актуальностью. Система должна иметь возможность использование функции для перемещения данных на менее производительные или более дешевые ресурсы в зависимости от времени жизни данных. Система должна обеспечивать Координирующие ноды, которые принимают запросы от пользователей, распределяют их между нодами и собирают результаты. Система должна обеспечивать ноду для обрабатывания входящих данные до их индексации, применяя фильтры и преобразования(нормализация) Система должна иметь возможность автоматического перемещения данных

	между уровнями хранения в зависимости от того, как долго они хранятся или как часто к ним обращаются. Система должна иметь встроенный интерфейс для выполнения запросов позволяющий быстро управлять и отлаживать запросы. Система должна иметь встроенный интерфейс для тестирования сложных запросов, анализа производительности запросов, проверки данных и их структуры Система должна иметь встроенный интерфейс для возможности выполнять команды управления кластером Система должна обеспечить правила, которые должны быть разработаны для обнаружения угроз через корреляцию данных из множества различных источников Система должна обрабатывать и анализировать данные в реальном времени, чтобы оперативно реагировать на угрозы. Система должна позволять настройку правил для различных сценариев обнаружения угроз с возможностью использования фильтров и сложных логических условий. Система должна классифицировать инциденты по уровню критичности и запускать соответствующие алерты (уведомления). Система должна интегрироваться с платформой для регистрации инцидентов и автоматизации реагирования на инциденты. Система должна поддерживать интеграцию с различными источниками данных (серверы, сетевые устройства, базы данных и др.), используя такие форматы, как Syslog, JSON, XML, CSV и т.д. Система должна предоставлять API для интеграции с другими платформами для управления инцидентами, аналитики и отчетности. Система должна обеспечить интеграцию с внешними источниками информации о текущих угрозах (базы данных IOC) для обогащения данных. Система должна обеспечить агенты для сбора логов с конечных точек и отправки их в лог коллектора или напрямую в Систему для обработки. Система должна обеспечить легко настраиваемые агенты для сбора специфических типов логов, фильтрации ненужных данных и минимизации трафика. Система должна поддерживать компонент лог коллектор для сжатия данных для уменьшения объема передаваемых данных, а также шифрование для защиты логов при их передаче по сети в сторону SIEM системы. Система должна обеспечить агенты и коллекторы, которые оптимизированы для минимальной нагрузки на систему, где они установлены, чтобы не снижать производительность конечных устройств. Система должна обеспечить использование логических операторов (AND, OR, NOT) для построения сложных условий корреляции между событиями из разных источников. Система должна обеспечить агрегацию событий объединения похожих или связанных событий в один инцидент для уменьшения объема ложных срабатываний и более точного определения атак. Система должна обеспечить возможность добавление легко настраиваемых и адаптируемых правил под конкретные сценарии угроз и требования организации. Система должна обеспечить обеспечить минимальные задержки между поступлением данных и срабатыванием правил, чтобы сократить время реакции на угрозы. Система должна обеспечить возможность классифицировать выявленные инциденты по уровням критичности (низкий, средний, высокий) в зависимости от

	типа и контекста события. Система должна обеспечить возможность добавления исключений и фильтров для снижения количества ложных срабатываний, связанных с легитимной активностью. Система должна обеспечивать возможность настройки уведомлений (email, интеграции с мессенджерами или другими системами), чтобы оперативно уведомлять команды безопасности о выявленных инцидентах. Система должна содержать полную информацию о характере инцидента, включая метаданные (время, источник, тип события, уровень угрозы) для быстрого анализа. Система должна иметь возможность использования готовых шаблонов правил для быстрого реагирования и настройки базовых политик безопасности. Система должна иметь возможность регулярного пересмотра и настройки правил на основе исторических данных для улучшения точности корреляции и выявления новых типов атак. Система должна поддерживать различные протоколы передачи логов напрямую с источников без установки агентов. Система должна поддерживать компонент лог-коллектора, который обеспечивает сбор данных с различных источников в централизованное хранилище для дальнейшей обработки, корреляции и анализа. Система должна иметь возможность создавать правила фильтрации на основе регулярных выражений Система должна поддерживать правила для генерации уведомлений или алертов на основе определённых событий в логах, таких как превышение пороговых значений Система должна поддерживать правила для логического маршрутизации данных между различными целями (например, отправка сетевых логов в одно хранилище, а логов приложений — в другое). Система должна поддерживать разбиение логических разделов для обеспечения горизонтального масштабирования. Логические разделы должны автоматически делиться на фрагменты, которые распределяются по разным узлам кластера. Каждому логическому разделу должны присвоены оптимальное количество основных (primary) фрагментов, что позволяет распределить нагрузку на несколько серверов для повышения производительности системы при больших объёмах данных. Система должна поддерживать репликацию фрагментов, чтобы обеспечить высокую доступность и отказоустойчивость. Для каждого основного фрагмента логических разделов должны создавать реплики, которые могут автоматически активироваться в случае сбоя основного узла. В случае необходимости система должна предоставлять возможности динамического перераспределения фрагментов логических разделов, что позволяет администраторам изменять их количество и реплик без потери данных и с минимальными перебоями в работе. Система должна предоставлять централизованное управление всеми агентами, позволяя администратору управлять конфигурацией, обновлениями и мониторингом агентов из одной консоли. Система должна поддерживать возможность удалённого управления агентами, включая обновление и удаление на устройствах, без необходимости физического доступа к ним Система должна поддерживать возможность создания и управления политиками для групп агентов, которые определяют, какие

	данные собирать и как их обрабатывать. Система должна обеспечить гибкие политики и которые позволять настраивать разные параметры для различных групп агентов, включая типы собираемых логов и метрик, а также параметры обработки данных. Система должна поддерживать возможность мгновенного распространения изменений в политике на все назначенные группы агентов. Система должна обеспечить шифрование передаваемых данных через агентов, обеспечивая защиту от несанкционированного доступа. Система должна обеспечивать мониторинг состояния всех агентов в реальном времени, позволяя отслеживать их работоспособность, производительность и корректность функционирования. Система должна поддерживать плановые обновления агентов без прерывания их работы и потери данных. - Система должна предусмотреть возможности машинного обучения, которые позволяют автоматизировать процесс анализа данных, выявляя аномалии и подозрительное поведение в логах. Система должна обеспечивать модели машинного обучения, которые автоматически идентифицируют аномалии в данных, основанных на временных рядах. Система должна позволять интегрировать пользовательские алгоритмы машинного обучения. Система должна позволять создавать ускоренные модели данных и использовать специальный интерфейс для быстрого построения отчётов и аналитики без влияния на производительность. Система должна предоставлять пользователям возможности настраивать параметры моделей машинного обучения и обучать их на своих собственных данных для достижения оптимальных результатов. 2.12. Функциональные требования к сканированию на уязвимости Поставщик определяет совместно с Заказчиком объем сканирования (системы, сети, приложения); Поставщик обязан собрать информацию о целевой системе, ее архитектуре, используемых технологиях и конфигурации; Поставщик проводит сканирование с применением лицензированного ПО в режимах pentest и audit; Поставщик обязан провести инструментальное сканирование, которое ищет известные уязвимости в используемых версиях программного обеспечения; Поставщик проводит оценку результатов сканирования для определения критичности и потенциальных последствий обнаруженных уязвимостей; Поставщик проводит анализ рисков; Поставщик проводит оценку уровня риска: Определение, насколько серьезные могут быть последствия использования обнаруженных уязвимостей для системы или организации; Поставщик делает приоритезацию уязвимостей. Определяет, какие уязвимости требуют наивысшего приоритета в устранении; Поставщик подготавливает отчет, предварительно согласованный с Заказчиком, в котором детально представлена информация об обнаруженных уязвимостях, их критичности и рекомендациях по устранению; Поставщик консультирует Заказчика в составлении плана действий по устранению уязвимостей. 2.13. Функциональные требования к инструменту статического анализа исходного кода 2.14.1. Общие требования: В составе поставляемого решения должны быть следующие возможности и функции: - Анализ программного обеспечения (ПО)

	на соответствие требованиям информационной безопасности по исходному коду с применением лицензированного ПО. - Анализ программного обеспечения (ПО) на соответствие требованиям информационной безопасности по byte-коду (методом статического анализа) при отсутствии debug info и исходных кодов. - Поиск недекларированных возможностей (НДВ) в ПО. - По результатам анализа приложений решение должно выдавать рекомендаций по настройке средств защиты информации (СЗИ) для таких уязвимостей и НДВ, эксплуатация которых может быть предотвращена при помощи настройки СЗИ. Поиск уязвимостей и НДВ должен осуществляться при помощи следующих алгоритмов статического анализа, включая но не ограничиваясь: - Поиск при помощи метода анализа по шаблонам; - Поиск при помощи метода анализа потока управления; - Поиск при помощи метода taint-анализа; - Поиск при помощи метода анализа синонимов; - Поиск при помощи метода распространения констант. 2.14.2. Требования к анализу ПО по исходному коду: Анализ ПО по исходному коду должен удовлетворять следующим требованиям: - Решение должно выполнять анализ исходного кода на языках: - Java, Java for Android, JavaScript, JSP, TypeScript, VBScript, Scala, HTML5, PHP, Python, Groovy, Kotlin, Go, Ruby, C#, C/C++, Objective C, Swift, ABAP, Apex, Solidity, PL/SQL, T/SQL, Visual Basic 6.0, Delphi, COBOL, VBA, 1C, ASP.NET, Perl, Vyper, VB.NET, LotusScript, Pascal, Dart, Rust, YAML, TOML, SQL, Bash, PowerShell, XML. - Решение должно уметь выполнять анализ мультиязычных проектов с автоматическим распознаванием языков; - Решение должно транслировать исходный код во внутреннее представление; - Решение должно обеспечивать интеграцию со средствами сборки; - Над полученным внутренним представлением должны применяться методы поиска уязвимостей и НДВ, описанные в общих требованиях настоящей технической спецификации. 2.14.3.Требования к анализу ПО по бинарному коду: Анализ ПО по byte-коду должен удовлетворять следующим требованиям: - Решение должно выполнять анализ byte-кода, полученного посредством трансляции из языков: Java/Scala: JAR/WAR/EAR/AAR; C/C++: DLL/EXE; Android: APK; Apple iOS: IPA; Apple macOS: APP; - Решение должно транслировать byte-код во внутреннее представление; - Над полученным внутренним представлением должны применяться методы поиска уязвимостей и НДВ, описанные в общих требованиях настоящей технической спецификации. 2.14.4.Требования к отчетности: Решение должно предоставлять отчетность по результатам анализа приложения, соответствующую следующим требованиям: - Вся отчетность должна предоставляться на русском и/или английском языках; - Формирование файла отчета с выявленными уязвимостями в форматах: CSV, HTML, PDF, SARIF; - Формирование файла отчета с выявленными уязвимостями на соответствие стандартам: PCI DSS, OWASP Top 10, OWASP Mobile Top 10, HIPAA, CWE/SANS, OWASP MASVS. 2.14.5. Требования к интеграции с инфраструктурными сервисами: ИС необходима возможность по интеграции с репозиториями SVN/Git. Сервисами CI/CD Jenkins,

	TeamCity, Azure DevOps Server, Gitlab CI. VCS хостингами GitHub, GitLab, BitBucket. Средствами отслеживания ошибок Jira. С помощью открытого встроенного API должна быть доступна интеграция с другими системами и сервисами. 3.Форма коммуникации Поставщик должен предоставить контактные данные (номер телефона и адрес электронной почты) своих представителей для осуществления коммуникаций. Коммуникации между Исполнителем и Заказчиком осуществляются по телефону и/или электронной почте между их представителями. Электронные версии документов должны быть направлены на электронную почту Заказчика. Доставка печатных результатов производится в офис Заказчика по адресу: г. Астана, ул.Бейбитшилик 49а. 4. Срок оказания услуги Срок оказания услуг начинается с даты подписания договора и продолжается по 31 декабря 2026 года. Поставщик обязуется выполнить все работы согласно условиям договора и требованиям Заказчика. 5. Требования к оказанию услуг В данном разделе указаны основные требования к оказанию услуг: − Поставщик должен соблюдать условия договора, а также учитывать любые дополнительные требования, указанные в технической спецификации или в других официальных документах; − Поставщик должен соблюдать сроки выполнения задач, указанные в контракте или техническом задании, и уведомлять Заказчика о любых задержках или изменениях в сроках; − Поставщик должен поддерживать открытую и эффективную коммуникацию с Заказчиком, отвечать на запросы и предоставлять необходимую информацию о ходе выполнения задач с 08-30 до 18-30 по часовому поясу Астаны. 6. Требования к соблюдению конфиденциальности − Поставщик должен выполнять Работы в рамках и соответствии с требованиями законодательства Республики Казахстан в сфере обеспечения кибербезопасности; − Поставщик при выполнении Работ должен обеспечить сохранность информации, находящейся в информационных ресурсах и системах, ее конфиденциальность, обеспечивать сохранность и конфиденциальность документов, получаемых от Заказчика; − Поставщик должен строго соблюдать требования законодательства Республики Казахстан в сфере обеспечения кибербезопасности. Это включает в себя соблюдение законов о защите персональных данных, коммерческой тайны, правовую защиту информации и другие нормативные акты, регулирующие обработку и хранение конфиденциальной информации; − Поставщик обязан обеспечивать сохранность информации, находящейся в информационных ресурсах и системах, а также обеспечивать конфиденциальность этих данных. Это включает в себя защиту информации от несанкционированного доступа, изменения, утраты или уничтожения; − Поставщик обязан обеспечивать сохранность и конфиденциальность документов и информации, получаемых от Заказчика. Это означает, что Поставщик должен принимать меры по защите документов от несанкционированного доступа и использования, а также обеспечивать их сохранность в течение всего срока выполнения работ, а также в сроки и на условиях, установленных соглашением о конфиденциальности и/или обязательством о

	неразглашении конфиденциальной информации и коммерческой тайны, подписываемыми с Исполнителем и/или привлеченными специалистами до предоставления доступа к информационным системам, технической документации, исходным кодам, инфраструктуре и иной информации Заказчика; − Поставщик должен использовать безопасные методы хранения и обработки информации, такие как шифрование данных, установку паролей и другие технические средства защиты, чтобы предотвратить утечку или несанкционированное распространение конфиденциальной информации; − Поставщик обязан обучать свой персонал правилам и процедурам обеспечения конфиденциальности информации, а также соблюдать регулярную проверку и аудит системы защиты информации для обеспечения ее эффективности и соответствия требованиям законодательства и стандартам безопасности. − До начала оказания услуг и предоставления доступа к информационным системам, исходным кодам, технической документации, инфраструктуре и иной информации Заказчика Поставщик подписывает с Заказчиком соглашение о конфиденциальности. Поставщик также обязан обеспечить подписание обязательств о неразглашении конфиденциальной информации и коммерческой тайны всеми своими работниками, консультантами, субподрядчиками и иными привлеченными специалистами, которым будет предоставлен доступ к информации Заказчика. Поставщик несет ответственность за соблюдение указанными лицами требований конфиденциальности 7. Место оказания услуг: Бейбитшилик 49а, Абая 47.
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)	Поставщик в течение 3 рабочих дней с даты заключения договора должен предоставить: действующий Аттестат аккредитации в Национальной системе аккредитации Республики Казахстан; подтверждающие документы о включении в реестр аккредитованных лабораторий; подтверждающие документы в области аккредитации, включающие испытания информационных систем; подтверждающие документы специалистов, включенных в Паспорт лаборатории. Поставщик обязан до начала выполнения работ/оказания услуг заключить с Заказчиком соглашение о неразглашении конфиденциальной информации (NDA).