Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Мәдениет және ақпарат министрлігі" мемлекеттік мекеме
Ұйымдастырушының атауы:	"Қазақстан Республикасының Мәдениет және ақпарат министрлігі" мемлекеттік мекеме
Конкурстың №:	№ 17976004-1
Конкурстың атауы:	«Құжаттардың бірыңғай электрондық архиві» ақпараттық жүйесі үшін ақпараттық қауіпсіздіктің жедел орталығын қосу қызметтеріне
Лоттың нөмірі:	№ 88480163-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:	33793103.45
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	33793103.45
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	С даты вступления договора в силу по 31 декабря 2027 года, но не менее 15 календарных дней.
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	1. Жалпы талаптар 1.1. Сатып алынатын қызметтердің атауы: «Құжаттардың бірыңғай электрондық архиві» ақпараттық жүйесі үшін ақпараттық қауіпсіздіктің жедел орталығының қызметтері (бұдан әрі - АҚЖО) 1.2. Сатып алу нысанасы ақпараттық қауіпсіздіктің жедел орталығының (АҚЖО) қызметтері болып табылады, олар ақпараттық қауіпсіздік инциденттерін мониторингтеу, талдау және оларға ден қоюды қамтамасыз етуге бағытталған. Жабдықты, бағдарламалық қамтамасыз етуді және лицензияларды жеткізу көрсетілген қызметтерді көрсету үшін қажетті көлемде ғана жүзеге асырылады және сатып алудың негізгі нысанасына — АҚЖО қызметтерін көрсетуге қатысты қосалқы сипатта болады. 1.3. Қызмет көрсету орны: «Қазақстан Республикасының Мәдениет және ақпарат министрлігі» мемлекеттік мекемесі, Астана қаласы, «Есіл» ауданы, Мәңгілік Ел даңғылы 8, 14 кіреберіс 1.4. Сатып алынатын қызметтердің сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары: 1.4. Негізгі терминдер мен анықтамалар: АҚ – ақпараттық қауіпсіздік. SIEM (Security Information and Event Management) – қауіпсіздік оқиғалары туралы ақпаратты жинауға және талдауға арналған бағдарламалық өнімдердің сыныбы. АТ – ақпараттық технологиялар. ITIL – АТ-мен байланысты бизнес-үдерістерді басқару, баптау және үздіксіз дұрыстау әдіснамасы. SLA – қызмет көрсету деңгейі туралы келісім. FQDN – толық домендік атау. Байланыстылық – компьютерлер арасындағы өзара әрекеттесу мүмкіндігі. АЖ – ақпараттық жүйе. VPN – виртуалды жеке желі. АҚҰҰО – «Мемлекеттік техникалық қызмет» АҚ Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы. Оқиға – стандартты қызметтердің бір бөлігі болып табылмайтын және қызметтер сапасының үзілуіне немесе төмендеуіне әкелуі мүмкін кез келген оқиға. ТЕ – техникалық ерекшелік. Қызметтер көрсету Тапсырыс берушінің АТ-инфрақұрылымының АҚ-ның қазіргі заманғы қатерлерінен қорғалу деңгейін арттыруға, сондай-ақ ақ АҚ оқиғаларының туындау тәуекелдерін барынша азайту бойынша алдын алу шараларын жүргізуге бағытталған. Қызметтер көрсету шеңберінде мынадай міндеттер шешілуі тиіс: • Тапсырыс берушінің инфрақұрылымында Қызметтер компоненттерін өрістетуді қоса алғанда, оқиғалар мониторингін және АҚ оқиғаларын өңдеуді ұйымдастыру және жүзеге асыру. Осы техникалық ерекшелік (бұдан әрі – ТЕ) жоғарыда көрсетілген міндеттерді шешуді қамтамасыз ететін Қызметтерді көрсетуге қойылатын жалпы және жеке талаптарды қамтиды. Ақпарат таралып кететін техникалық арналарды және арнайы техникалық құралдарды ақпараттық қауіпсіздіктің жедел орталығымен анықтау бойынша көрсетілетін қызметтер, оның ішінде: - қосылатын оқиға көздерінің жиынтық саны 50-ден (елуден) аспайтын оқиғалар мен желілік ағындар коллекторларын (LOG/FLOW Collector) ұсыну; Өнім беруші АҚЖО-ның техникалық құралдарын жеткізуді, орнатуды, қосуды және баптауды жеткізу мен енгізудің нақты көлемін ескере отырып, 15 күнтізбелік күн ішінде, бірақ Мемлекеттік сатып алуды жүзеге асыру қағидаларының 569-тармағында белгіленген

	ең төменгі мерзім өткеннен ерте емес жүзеге асырады. Орнату, қосу және баптау фактісі Тапсырыс беруші мен Өнім беруші қол қойған жазбаша актімен ресімделеді. 1.5. Тапсырыс беруші осы ТЕ-нің 3.6-тармағында белгіленген мерзімде қажетті ресурстарды ұсынады және көздердің қосылуын қамтамасыз етеді. 2. Қызметтерге қойылатын талаптар 2.1. Қызметтер көрсету шеңберінде мынадай функциялар мен қосымша сервистер қолжетімді болады: 1) Өнім берушінің SIEM жүйесіне қосылған Тапсырыс берушінің серверлік жабдықтарында және желілік құрылғыларында тіркелген АҚ оқиғаларын мониторингілеу; 2) Мониторинг аймағында АҚ оқиғаларын анықтау; 3) Тапсырыс берушіні анықталған оқиғалар, оларға ден қою әдістері туралы хабардар ету, сондай-ақ оларды жою жөнінде ұсынымдар беру; 4) Оқиғаларға ден қою үдерісінде сараптамалық қолдау көрсету; 5) Тапсырыс берушінің АТ-инфрақұрылымын осалдықтардың бар-жоғына сканерлеу — айына кемінде 1 (бір) рет (кемінде 512 бірегей IP-мекенжай); 6) Тапсырыс берушінің өтінімі бойынша Қызметтер көрсету мерзімі ішінде 2 (екі) рет Тапсырыс берушінің АТ-инфрақұрылымына енуге тестілеу және оның қорғалуын талдау (кемінде 128 бірегей IP-мекенжай); 7) АҚ сыни оқиғаларын тексеру кезінде кеңес беру; 8) Ақпараттық қауіпсіздік талаптарына сәйкестікті растау сынақтарынан өту бойынша көмек көрсету және консультациялар ұсыну; 9) «Құжаттардың бірыңғай электрондық архиві» АЖ үшін ақпараттық қауіпсіздіктің жедел орталығы қызметін көрсету шеңберінде ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға сәйкестігіне ақпараттық қауіпсіздік аудитін жүргізу (шарттың қолданылу мерзімі ішінде 1 (бір) рет), жазбаша есеп пен ұсынымдар ұсыну; 10) Мониторинг аймағына кірмейтін жүйелерге қатысты күдікті оқиғалар анықталған жағдайда, одан әрі тергеп-тексеруді Тапсырыс беруші дербес жүзеге асырады. Өнім беруші қажет болған жағдайда сындылық дәрежесін айқындау үшін Тапсырыс берушіге консультация береді, мәселенің көзін анықтау мақсатында қосымша талдау жүргізеді және Тапсырыс берушінің мамандарына инцидентті жоюға жәрдемдеседі; 11) Есептік деректерді орталықтандырылған сақтауды, қол жеткізу құқықтарының аражігін ажыратуды, артықшылықты сеанстарды басқаруды, сеанстарды жазуды және пайдаланушылардың әрекеттерін журналға тіркеуді қамтамасыз ететін артықшылықты қол жеткізуді басқару және мониторингтеу сервисі (3 (үш) пайдаланушыға); 2.2. Кеңейтілген сараптама Тапсырыс берушінің сұрау салуы бойынша ТЕ-ке 6-қосымшаға сәйкес мониторинг аймағының қосымша кеңейтілген сараптамасы ұсынылуы мүмкін. 2.3. Қызметтер осы техникалық ерекшелікке сәйкес ақпараттық қауіпсіздік инциденттерін мониторингтеу мен оларға ден қоюдың мынадай құралдарын пайдалана отырып көрсетіледі:: • ақпараттық қауіпсіздік оқиғаларын басқару жүйесі (SIEM); • басқару және артықшылықты қолжетімділік мониторингі сервисі; • осалдықтар сканері (Vulnerability Scanner). 2.4. Ұсынылатын қаражат шарттың қолданылу мерзіміне шешімдерді өндірушілердің техникалық қолдауымен

	сүйемелденуі тиіс, бұл тапсырыс берушіге ұсынылатын веб-ресурстарға (бар болса) сілтемелері бар өндірушінің немесе оның ресми өкілінің (дистрибьютордың) ресми хатымен расталуы тиіс. 2.5. Қызметтер көрсету шеңберінде туындауы мүмкін оқиғалар шегінің деңгейі. Әрбір АҚ оқиғасы үшін техникалық ерекшелікке осы ТЕ-ке № 2 қосымшаға сәйкес басымдық белгіленеді. АҚ оқиғаларына ден қою техникалық ерекшелікке осы ТЕ-ке № 3 қосымшада келтірілген уақытша сипаттамалармен айқындалған мерзімде жүзеге асырылады. 3. Өнім беруші міндетті: 3.1. Төмендегіні қоса алғанда, Тапсырыс беруші толтырған сауалнама парағының негізінде қосылатын ақпараттық жүйелер (АЖ) бөлігінде Тапсырыс берушінің АТ-инфрақұрылымына талдау (зерттеу) жүргізу: 1) ақпараттық қауіпсіздік оқиғаларының қосылатын көздерінің (бұдан әрі - көздер) құрамы бойынша ұсынымдар беру; 2) Өнім берушінің білім базасына сәйкес стандартты және стандартты емес көздерді типтеу; 3) Тапсырыс берушінің шабуылдарды анықтаудың қолданыстағы сценарийлерін қосуға және жаңа сценарийлерін әзірлеуге қажеттілігін айқындау; 4) талап етілетін лицензиялардың көлемін анықтау. Осы кезеңде мынадай мәліметтер жинақталуы тиіс: 1) көздің атауы; 2) көздің функционалын сипаттау (АЖ-ге қатыстылығы); 3) орналастыру алаңы; 4) өндіруші/марка/модель; 5) ОЖ түрі/нұсқасы; 6) БЖ түрі/нұсқасы; 7) FQDN; 8) IP-мекенжай. 3.2. Осы техникалық ерекшелікке сәйкес ұйымдастырушылық-техникалық шешімдер айқындалуы және әзірленуі тиіс: 1) Қызметтер көрсетудің нысаналы архитектурасы; 2) файлдық сақтау орындарының сыйымдылығын есептеуді қоса алғанда, Тапсырыс беруші бөлетін есептеу ресурстарына қойылатын техникалық ерекшеліктер мен талаптар; 3) Қызметтер компоненттерін өрістету тәртібі, оның ішінде Тапсырыс берушінің алаңында; 4) Тапсырыс беруші мен киберқатерлерге мониторинг және ден қою орталығының алаңында Қызметтер құрауыштарының желіаралық өзара іс-қимылының тәртібі мен ұйымдастырылуы. 3.3. Өнім беруші көздерді қосуды орындауы керек: 1) Тапсырыс беруші мен Өнім берушінің алаңы арасында келісілген параметрлер бойынша Өнім берушінің жабдығында қорғалған VPN-қосылуды (бұдан әрі - VPN-қосылыс) ұйымдастыру. Бөлінген алаңдар арасында L3 байланысы болмаған жағдайда олардың әрқайсысымен VPN-қосылыстарды орнатуды қамтамасыз ету қажет; 2) SIEM-жүйе компоненттерін орнатуды жүргізу. Қажет болған жағдайда Тапсырыс берушіге есептеу ресурстарына, сақтаудың кіші жүйелеріне қойылатын талаптарды және Қызметтердің қосымша компоненттерін орнату үшін конфигурациялау жөніндегі ұсынымдарды ұсыну; 3) Тапсырыс берушінің АТ-инфрақұрылымына SIEM конфигурациялауды және бейіндеуді орындау, бұл ақпараттық қауіпсіздіктің бұзушылықтары мен оқиғаларын анықтау сценарийлерінің жұмыс қабілеттілігіне кепілдік береді; 4) көздерді ақпараттық қауіпсіздік оқиғаларын мониторингілеу және талдау сервисіне қосу жөніндегі нұсқаулықтарды жіберу; 5) стандартты емес көздер үшін 3 (үш) жеке адаптерге дейін әзірлеу; 6) Тапсырыс берушінің Өнім берушімен келісілген ерекше сұрау салулары негізінде

	оқиғалар мен корреляция қағидаларының санаттарын кеңейтуді қоса алғанда, шабуылдарды анықтаудың жаңа сценарийлерін әзірлеу; 7) осы техникалық ерекшелікке сәйкес SIEM-жүйесінің компоненттері, көздер мен өнім берушінің алаңы арасындағы желілік байланысты тексеруді жүргізу. 3.4. Мониторинг және киберқатерлерге ден қою орталығының базасында Өнім беруші міндетті: 1) барлық түрлі оқиға көздерінен келіп түсетін бірыңғай «кіру нүктесі» болып табылатын кезекші ауысымның бірінші желісі талдаушыларының күшімен 24/7 режимінде ақпараттық қауіпсіздік оқиғаларын талдауды қамтамасыз етуге. Бірінші желінің талдаушылары ақпараттық қауіпсіздік оқиғаларын өңдеуді, жалған іске қосылуларды бастапқы тексеруді, бастапқы талдау жүргізуді және оқыс оқиғалар санаттары мен қағидалар негізінде ақпараттық қауіпсіздік оқиғаларын бөліп көрсетуді, ITIL стандарттарына сәйкес (санаттау, басымдық беру, SLA) оқиғаларды тіркеуді және кейіннен сүйемелдеуді қамтамасыз етуге тиіс; 2) Тапсырыс берушінің алаңында да, Өнім берушінің алаңында да орнатылған SIEM-жүйе компоненттерінің жай-күйінің мониторингі; 3) VPN-арнасының жай-күйіне мониторинг жүргізу; 4) 8/5 режимінде екінші желі талдаушыларының күшімен оқиғаларды өңдеу бойынша ұсынымдар беру, сондай-ақ ақпараттық қауіпсіздіктің типтік оқиғаларын шешу. Осы үрдіс шеңберінде мамандандырылған құралдарды пайдалана отырып тереңдетілген талдау жүргізу, сондай-ақ Тапсырыс берушінің инфрақұрылымындағы өзгерістерге сәйкес корреляция қағидаларын бейімдеу қамтамасыз етілуге тиіс. Қажет болған жағдайда, Тапсырыс берушінің сұрау салуы бойынша корреляция қағидаларына ерекшеліктер қосу; 5) үшінші сараптамалық желінің күшімен сыни деңгейдегі оқиғаларды тергеп-тексеруді жүргізу, расталған оқиғаларды жою жөнінде ұсынымдар беру, сондай-ақ ретроспективті талдау жүргізу және релевантты қауіп-қатерлер мен шабуылдар, оларды анықтау және қарсы іс-қимыл тәсілдері туралы ақпаратты өзектендіру; 6) Киберқауіпсіздік инциденттері мен қатерлерін сараптау, техникалық тергеп-тексеру; 7) Киберқауіпсіздік инциденттері мен қатерлеріне сараптама жүргізу, техникалық тергеп-тексеру; 8) Киберқауіпсіздік қатерлерін мониторингтеу, талдау және болжау; 9) Киберқауіпсіздік инциденттерінің салдарын оқшаулау және бейтараптандыру; 10) Тапсырыс берушінің инфрақұрылымында оқиға анықталған жағдайда, оқиға туралы ақпаратты АҚҰҰО-ға беруді қамтамасыз етуге; 11) әрбір анықталған ақпараттық қауіпсіздік оқиғасы бойынша бір байланыс арнасы бойынша есептілікті ұсыну: электрондық пошта, телефон қоңырауы. 3.5. Тапсырыс берушіге ден қою және ақпараттық қауіпсіздік оқиғаларын басқару жүйелерінің интерфейсіне қол жеткізуді ұсыну қамтамасыз етілуі тиіс. Жеке кабинеттің функционалы мыналарды қамтуы тиіс: 1) оқиғалардың мәртебесі бойынша өзекті ақпаратқа қол жеткізу; 2) оқиғаларды дербес тіркеу мүмкіндігі; 3) орын алған оқиғалар бойынша статистиканы қарау; 4) әрбір анықталған оқиға бойынша есептілік; 5) Өнім берушіден есептер мен хабарламалар алу. 3.6. Тапсырыс беруші шарт күшіне енген күннен бастап

	14 (он төрт) жұмыс күні ішінде Қызметтерді енгізу үшін Өнім беруші сұратқан қажетті ресурстарды ұсынуға және бөлуге, сондай-ақ көрсетілген мерзімде барлық қажетті көздердің SIEM жүйесіне қосылуын қамтамасыз етуге міндетті. 3.7. Өнім беруші Тапсырыс берушінің көмегімен қызмет көрсету үшін қажетті компоненттер мен Тапсырыс берушінің АТ-инфрақұрылымы арасындағы желілік байланысты ұйымдастыруға міндетті. 3.8. Өнім беруші Тапсырыс берушімен келісілген параметрлер бойынша Тапсырыс берушінің алаңы мен Өнім берушінің алаңы арасында Тапсырыс берушінің жабдығында қорғалған VPN-қосылысын ұйымдастыруға тиіс. 3.9. Өнім беруші ай сайын, есепті айдан кейінгі айдың 3 (үшінші) күнінен кешіктірмей, ал желтоқсан айының есебін 2027 жылғы 20 желтоқсаннан кешіктірмей Тапсырыс берушіге жабдық орналастырылған әрбір алаң бойынша көрсетілген Қызметтер туралы егжей-тегжейлі есептерді ілеспе хатпен бірге, Тапсырыс берушінің кеңсесінде міндетті түрде тіркей отырып ұсынуға міндетті. 4. Өнім беруші мен Тапсырыс берушінің өзара әрекеттесуі 4.1. АҚ қамтамасыз ету мәселелері бойынша Өнім беруші мен Тапсырыс беруші арасындағы өзара әрекеттесу тәртібін белгілейтін және АҚ оқиғаларын анықтауға және оларға ден қоюға байланысты рәсімдерді сипаттайтын Регламент әзірленеді. 4.2. Өнім беруші мен Тапсырыс берушінің мониторинг орталығының өзара әрекеттесуі: 1) көрсетілетін қызметтердің талап етілетін сапа параметрлеріне сәйкес келмеуіне өтінімдерді тіркеу; 2) сервисті қалпына келтіру үрдісін ұйымдастыру; 3) екі тараптың жауапты басшыларын қызметтердің талап етілетін сапасын қалпына келтіруге байланысты мәселелерді шешу барысы туралы өзара хабардар ету. 4.3. Өнім беруші тәулігіне 24 сағат, аптасына 7 күн қызмет көрсетуге міндетті. 4.4. АҚЖО қызметін көрсету кезеңінде Өнім беруші мен Тапсырыс беруші арасындағы жауапкершілік аймақтарының аражігін ажырату техникалық ерешелікке осы ТЕ-ке №5 қосымшада көрсетілген. 4.5. Оқиғаларды анықтау кезіндегі Тараптардың өзара әрекеттесу рәсімі Оқиғаны Тапсырыс беруші анықтаған жағдайда, ол регламентте көрсетілген Өнім берушінің техникалық қызметінің байланыс деректері бойынша Өнім берушіні хабардар етеді. Өнім беруші оқиғаны тіркейді және Тапсырыс берушіге мынадай деректерді хабарлайды: 1) тіркелген оқиғаның нөмірі; 2) тіркеу уақыты; 3) тақырып (қысқаша сипаттама); 4) оқиға туралы ақпарат; 5) оны жою жөніндегі ұсынымдар. 4.6. Тапсырыс берушіден оқиға туралы хабарлама Өнім берушіге электрондық пошта арқылы жіберіледі. АҚ оқиғасына ден қою деп оқиғаның тетіктерін анықтауға, зиянды барынша азайтуға және оқиғаның болашақта қайталануын болдырмауға бағытталған іс-қимылдардың құрылымдалған жинағы түсініледі. АҚ оқиғаларын анықтау және оларға ден қою жөніндегі іс-қимылдар, сондай-ақ олардың реттілігі техникалық ерекшелікке осы ТЕ-ке № 1 қосымшада берілген. 4.7. Тапсырыс берушінің өтініштерін тіркеу кезінде Тараптардың өзара әрекеттесу рәсімі Тапсырыс берушіге техникалық ерекшелікке осы ТЕ-ке № 4 қосымшада көрсетілген көрсеткіштерге сәйкес сұрау

	салуларды жіберу мүмкіндігі беріледі. Бұл үшін Тапсырыс берушінің уәкілетті өкілі хат тақырыбында сәйкестендіргішті көрсете отырып, Өнім берушінің электрондық мекенжайына мынадай пішімде сұрау салу жіберуі тиіс: 1) Хат тақырыбы: сәйкестендіргіш (сервис-менеджер ұсынады), сұраудың қысқаша мәні. 2) Хат денесі: сұрау салудың егжей-тегжейлі сипаттамасы, сұрау салудың басымдығын көрсету. 5. Қызметтерді тиісінше көрсету шарттары 5.1. Қызметтер көрсетуде үзілістерге әкеп соққан оқиғалар мен басқа да мән-жайлар үшін, егер олар мынадай себептердің бірінен туындаса, Өнім беруші жауапты болмайды: 1) Тапсырыс берушіні алдын ала хабардар ете отырып, Қызметтер көрсетуге қатысатын жабдықта жоспарлы немесе апаттық жөндеу жұмыстарын жүргізу; 2) Тапсырыс берушінің сұрауы бойынша Тапсырыс беруші немесе Өнім беруші жүргізетін Қызметтерді көрсетуге қатысатын жабдықтардағы жұмыстар; 3) Ешқандай оқыс оқиғалар анықталмаған жағдайда Тапсырыс берушінің сұрау салуы бойынша Қызметтерді тестілік көрсету; 4) Тапсырыс берушінің Қызметтер көрсету деңгейінде белгіленген мерзімде Өнім берушіге оқиғаларды анықтауға және жоюға жәрдемдесуді қамтамасыз етуден бас тартуы немесе қабілетсіздігі; 5) Тапсырыс берушінің регламент талаптарына сәйкес қызмет көрсету шеңберінде бағдарламалық жасақтаманы немесе жабдықты баптау үшін қажетті деректерді 5 (бес) жұмыс күнінен аспайтын мерзімде ұсынудан бас тартуы немесе қабілетсіздігі; 6) Өнім берушіні хабардар етпей, Тапсырыс берушінің қорғалатын ресурстардың құрамына және конфигурациясына олардың уақытша қол жетімсіздігіне және соның салдарынан Қызметтер көрсетудегі үзіліске әкелуі мүмкін өзгерістер енгізу жөніндегі жұмыстарды жүргізуі; 7) Тапсырыс берушінің бағдарламалық және/немесе бағдарламалық-аппараттық жасақтамасының көрсетілетін Қызметтермен жұмысқа қабілетсіздігі немесе үйлеспеушілігі; 8) Шарттың талаптарына сәйкес еңсерілмейтін күш жағдайларының басталуы. 6. Өнім берушінің құқықтары. 6.1. Өнім беруші шабуылдарды анықтау сценарийін іске асыру үшін Тапсырыс берушіден қажетті ақпаратты (оның ішінде АТ-инфрақұрылымы туралы ақпаратты) сұратуға, сондай-ақ бұл ақпаратты жалған іске қосылуларды барынша азайту мақсатында Шарт бойынша өз міндеттемелерін орындау үшін ғана пайдалануға құқылы. 6.2. Сұрау салу Өнім берушімен қалыптастырылады және Тапсырыс беруші тарапынан уәкілетті тұлғаға электрондық пошта арқылы жіберіледі. Сұрау салуда өтініштің себебі көрсетілуге тиіс. Тапсырыс беруші осы сұрау салу бойынша кері байланысты 3 (үш) жұмыс күні ішінде беруге міндетті, қажет болған жағдайда мерзім тараптардың келісімі бойынша түзетілуі мүмкін. Сұратылған ақпараттың мысалдары мыналарды қамтуы мүмкін, бірақ олармен шектелмейді: 1) DNS-серверлер тізімі; 2) қауіпсіздік сканерлерінің IP-мекенжайлары; 3) интернет желісінен қол жетімді ресурстар тізімі; 4) Тапсырыс берушіге тиесілі жаһандық IP-мекенжайлар тізімі; 5) ақпараттық жүйелер әкімшілерінің есептік жазбаларының тізімі; 6) ақпараттық жүйелер мен ресурстардың иелері туралы ақпаратты; 7)

	IP-мекенжайдың пайдаланушыға немесе жүйеге тиесілігі туралы деректер. Ақпарат Тапсырыс берушінің Қызметтерді қосу және Тапсырыс берушінің уәкілетті өкілдерімен сұхбат жүргізу үшін тиісті сауалнама парақтарын толтыру жолымен ұсынылады. 7. Өнім берушінің жабдықтарына жоспарлы техникалық қызмет көрсету 7.1. Өнім беруші Қызметтер көрсетілетін кіші жүйелерге жоспарлы техникалық қызмет көрсетуді немесе жетілдіруді жүргізуге құқылы. Бұл жұмыстар жоспарлы жөндеу жұмыстары болып саналады және Қызметтер көрсетуде үзілістерге әкелуі мүмкін. Жоспарлы жөндеу жұмыстары 19:00-ден 08:00-ге дейінгі аралықта (Астана қаласының уақыты) не Тапсырыс берушімен келісілген басқа уақытта Қызметтер көрсетуде ықтимал үзіліспен жүргізіледі. 7.2. Өнім беруші Тапсырыс берушіні жұмыстар басталғанға дейін 1 (бір) жұмыс күнінен кешіктірмей Қызметтер көрсетуде үзілістер тудыруы мүмкін жоспарлы жөндеу жұмыстарын жүргізу туралы хабардар етуге міндеттенеді. Жұмыстар Тапсырыс берушінің сұрауы бойынша орындалатын жағдайлар, сондай-ақ егер жоспарлы жөндеу жұмыстары Қазақстан Республикасының мемлекеттік органдарының немесе құзыретті телекоммуникациялық органдарының талабы бойынша жүргізілсе, Өнім беруші көрсетілген мерзімде хабарлай алмайтын жағдайлар бұған жатпайды. 7.3. Тапсырыс беруші қажет болған жағдайда техникалық мүмкіндік болған кезде Өнім беруші ескеретін жұмыстарды жүргізу мерзімдерін түзету жөнінде ұсыныстар жібере алады. Өнім беруші жіберген хабарламада мынадай ақпарат көрсетіледі: жоспарлы жөндеу жұмыстарын жүргізу уақыты; 1) жұмыстарды жүргізу күні; 2) жұмыстың ұзақтығы; 3) жұмыстар туралы ақпарат беретін жауапты тұлғаның байланыс деректері; 4) Тапсырыс беруші қызметкерлерінің жұмыстарға, мысалы, Тапсырыс берушінің ақпараттық жүйелерінің жұмысқа қабілеттілігіне тексеру жүргізу үшін қатысу қажеттілігі. 7.4. Тапсырыс беруші жұмыстарға қатысу үшін жауапты қызметкерлер бөлуге міндеттенеді. Қызметкерді көрсетілген мерзімде тарту мүмкін болмаған жағдайда, Тапсырыс беруші жұмыстарды жүргізу мерзімдерін түзету жөнінде ұсыныстар жібереді. 7.5. Егер жоспарлы жұмыстар тоқтатылса, Өнім беруші Тапсырыс берушіні шешім қабылданғаннан кейін қысқа мерзімде хабардар етеді. 7.6. Тапсырыс беруші, сондай-ақ, егер бұл жұмыстар қорғалатын ресурстардың уақытша қол жетімсіздігіне және соның салдарынан Қызметтер көрсетудегі үзіліске әкеп соғуы мүмкін болса, Өнім берушіні ол өз жабдығында жоспарлы жұмыстар жүргізілетіні туралы хабардар етуге міндетті. Хабарлама жұмыс басталғанға дейін 1 (бір) жұмыс күнінен кешіктірілмей жіберілуге тиіс. Тапсырыс берушінің хабарламасында келесі ақпарат көрсетілуі тиіс: 1) жоспарлы жұмыстарды жүргізу уақыты мен күні; 2) жұмыстың ұзақтығы; 3) жұмыстар туралы ақпарат беретін жауапты тұлғаның байланыс деректері. 7.7. Жоспарлы жұмыстарды жүргізу мерзімдері өзгерген жағдайда Тапсырыс беруші Өнім берушіні қысқа мерзімде, бірақ жұмыс басталғанға дейін 1 (бір) жұмыс күнінен кешіктірмей хабардар етуге міндетті. Жоспарлы жұмыстарды тоқтату кезінде Тапсырыс беруші Өнім

	берушіні қысқа мерзімде хабардар етуге міндетті. 7.8. Тапсырыс берушіден немесе Өнім берушіден барлық хабарламалар регламентте көрсетілген уәкілетті өкілдердің электрондық мекенжайларына жіберілуі тиіс. 8. Өнім берушінің жабдықтарындағы апаттық жөндеу жұмыстары 8.1. Базасында Қызметтер көрсетілетін кіші жүйелердің апаттық жөндеу жұмыстары Қызметтер көрсетуде кезеңдік үзілістер немесе болашақта апаттық жағдайға әкеп соғуы мүмкін сапа параметрлерінің едәуір нашарлауы тіркелген жағдайларда жүргізіледі. 8.2. Өнім беруші Тапсырыс берушіні апаттық жөндеу жұмыстарын жүргізу туралы олар басталғанға дейін кемінде 4 (төрт) сағат бұрын хабардар етуге міндетті. 8.3. Тапсырыс беруші, өз кезегінде, егер олар қорғалатын ресурстардың уақытша қол жетімсіздігіне және соның салдарынан Қызметтер көрсетудегі үзіліске әкеп соғуы мүмкін болса, Өнім берушіні өз жабдығында апаттық жөндеу жұмыстарын жүргізу туралы хабардар етуге міндетті. Хабарлама жұмыс басталғанға дейін кемінде 2 (екі) сағат бұрын жіберілуге тиіс. 8.4. Хабарламалар осы техникалық регламентте көрсетілген уәкілетті өкілдердің электрондық мекенжайларына жіберіледі. Хабарламада мыналар көрсетілуі тиіс: 1) апаттық жөндеу жұмыстарының уақыты, күні және ұзақтығы; 2) жүргізілетін жұмыстар туралы ақпарат беретін жауапты тұлғаның байланыс деректері; 3) Тапсырыс беруші қызметкерлерінің апаттық жөндеу жұмыстарына қатысу қажеттілігі туралы ақпарат (егер жұмыстарды Өнім беруші жүргізсе). 9. Тапсырыс берушіде бар зиянды немесе күдікті объектілерді талдау: 9.1. Зерттеу объектісі: бір күдікті файл. Құрамдас файлдарды (архивтерді) талдау жағдайында жалпы архив емес, архив құрамына кіретін әрбір жеке файл зерттеу объектісі болып табылады. Егер құрамдас орындалатын файлдар (өздігінен ашылатын архивтер, инсталляторлар) талданса, зерттеу объектісі осы архивтердің немесе инсталяторлардың функционалы (сценарийі) болып табылады. Егер алынған файлдардың функционалын зерттеу қажет болса, олардың әрқайсысы жеке зерттеу объектісі ретінде қарастырылады. 9.2. Зерттеу көлемі: Тапсырыс берушінің талабы бойынша. 9.3. Зерттеулерді жүргізудің негізгі ықтимал кезеңдері (кезеңдер олардың орындылығына, қолданылуына қарай, файлдың пішімімен құрылымын, сондай-ақ зерттеу міндеттерін шешу қажеттілігін ескере отырып жүргізіледі. Бұл нақты файлды талдау кезінде барлық көрсетілген кезеңдер орындалмауы мүмкін, бірақ зерттеу мақсаттарына қол жеткізуге мүмкіндік беретін кезеңдер орындалуы тиіс дегенді білдіреді: 9.4. Объектіні базалық статистикалық зерттеу: 1) Файл пішімі мен өлшемін анықтау; 2) Хэш-сомаларды есептеу (MD5, SHA-256); 3) Цифрлық қолтаңбаның болуын айқындау; 4) Файлдағы жолдарды алу және талдау; 5) Файлды компиляциялау құралдарын сәйкестендіру; 6) Импортталған функцияларды, секцияларды, компиляция уақытын және басқа да уақыт белгілерін қоса алғанда, файл тақырыбын талдау (егер мұндай деректер бар болса). 9.5. Ашық көздер бойынша деректерді іздеу: 1) Google.com және Virustotal.com көмегімен объектіні сәйкестендіретін хэш-сомаларды іздеу

	(Тапсырыс берушінің келісімі бойынша объектіні ресурсқа жүктеумен немесе жүктеусіз); 2) Google.com және басқа да сервистерді пайдалана отырып, объектіде қамтылған ерекше жолдарды іздеу. Мұндай жолдардың тізімін зерттеу объектісінің ерекшеліктеріне байланысты талдаушы таңдайды. 9.6. Тереңдетілген статикалық және қажет болған жағдайда динамикалық талдау: 1) Талдау объектісінің дизассемблирленген, декомпилирленген немесе өзге де қолжетімді кодын зерттеу (файл пішіміне байланысты); 2) Қажет болған жағдайда және техникалық мүмкіндік болған кезде - объектіні оқшауланған виртуалды ортада, интернетке қол жеткізумен немесе қол жеткізусіз дұрыстауды жүргізу (Тапсырыс берушінің келісімі бойынша). 9.7. Компрометация сәйкестендіргіштерін бөлу (зиянды функционал анықталған жағдайда): 1) Жинақталған ақпаратты құрылымдау және зерттелетін объект жұққан жүйеде анықталуы мүмкін индикаторлардың мынадай ықтимал топтарын бөліп анықтау: мьютекстердің, файлдардың, тізілім кілттерінің, процестердің атаулары, IP-мекенжайлар, домендік атаулар, есептік деректер, зиянды БҚ жасайтын пайдаланушылардың аттары мен құпия сөздері. 9.8. Зерттелетін объектінің функционалдық сипаттамасы: 1) Объектіні оның таралу мүмкіндіктері мен орындайтын функциялары бойынша жіктеу (мысалы: троян, құрт, вирус, бэкдор, тиегіш және т.б.). Зиянды функционал анықталған жағдайда бұл сипатталады немесе егер зерттеу оның бар екенін растамаса, оның жоқтығы көрсетіледі. 9.9. Объектіні бейтараптандыру үшін ұсынымдар дайындау: 1) Егер объектіде зиянды функционал болса, объектінің жұқтыруын анықтау, оны бейтараптандыру және жүйелерді (жұмыс станцияларын, серверлерді немесе басқа жабдықтарды) қалпына келтіру үшін ұсынымдар қалыптастыру. Егер зиянды функционал анықталмаса, бұл да көрсетіледі. 10. Желілер арасындағы экранға қойылатын техникалық талаптар Құрылғылар саны – 1 дана. Next Generation Firewall (NGFW) функционалы; Қолданбаларды бақылау және веб-трафикті сүзгілеу (Application Control & URL Filtering); Шешім Ену әрекеттерінің алдын алу жүйесінің (IPS) функционалын қамтамасыз етуі тиіс; IPS жүйесі төмендегі механизмдер негізінде қауіптерді анықтауды қамтамасыз етуі керек: Белгілі шабуылдар мен эксплойттарды анықтау үшін сигнатуралық талдау (Signature Analysis); Стандартқа сай емес немесе зиянды трафикті анықтау үшін протоколдар аномалияларын бақылау және талдау (Protocol Anomaly Analysis); Қолданбалардың қажетсіз белсенділігін бақылау және бұғаттау үшін қолданба басқаруы (Application Control); Бұрын белгісіз шабуылдар мен аномалды әрекеттерді анықтау үшін мінез-құлық талдауына негізделген анықтау (Behavior Analysis); Қауіптерді проактивті анықтау мүмкіндігі бар антивирустық қорғау (Antivirus); Антивирустық шешім зиянды веб-сайттарға қолжетімділікті болдырмауы, сондай-ақ кіріс зиянды файлдарды анықтап, бұғаттауы тиіс (Anti-virus); Боттар мен зиянды бағдарламалардан қорғау (Anti-Bot); Anti-Bot қосымшасы бірнеше деңгейлі анықтау механизмін қолдануы тиіс, оған IP, URL және DNS

	мекенжайларының беделі, байланыс протоколдарының үлгілері бойынша боттарды анықтау, сондай-ақ DNS хаттамасындағы шабуылдардан автоматты қорғауға арналған зерделі аналитика механизмдері, соның ішінде DGA-дан қорғау тетіктері кіреді; Электрондық поштаны спамнан қорғау (Anti-Spam) зияткерлік талдау негізінде; Оқшауланған ортада орындалуын эмуляциялау мүмкіндігімен файлдарды талдау және нөлдік күн қатерлерін анықтауға арналған песочница (sandbox) функционалы; Қауіпсіздік шлюзі қосылыстардың күйін бақылау үшін трафиктің егжей-тегжейлі талдауы және қолданбалар жағдайын пайдаланып желілік ағындарды басқаруды қамтамасыз етуі тиіс; Шешім DHCP сервері және ретранслятор (relay) режимдерінде жұмыс істеуді қолдауы тиіс; Шешім Transparent (Bridge) режимінде жұмыс істеу мүмкіндігін қолдауы тиіс; Жергілікті желіге қолжетімділікті шектеу үшін MAC мекенжайларының ақ тізіміне негізделген саясатты қолдау; QoS механизмдеріне негізделген саясатты қолдау; Белгілі бір IP-дереккөз, IP-мекенжай немесе сервис үшін өткізу қабілетін шектеу немесе кепілдендіру, сондай-ақ кідірістерді басқару мүмкіндігі; VPN-трафик үшін QoS ережелерін икемді баптау мүмкіндігі, оның ішінде артықшылықтарды, өткізу қабілетінің шектеуін немесе кепілдендірілуін орнату; Шешім веб-қолданбаларды зиянды кодтар мен шабуылдардан қорғау үшін кіріктірілген ену әрекеттерінің алдын алу жүйесінің (IPS) функционалын қамтамасыз етуі тиіс. Жүйе желілік червьтерді, буферді толтыру шабуылдарын, SQL-инъекцияларды, командалық инъекцияларды, сайт аралық скриптингті (XSS) бұғаттауы, сондай-ақ HTTP-червьтерін бұғаттауға арналған баптауға болатын модульді қолдауы тиіс. Сонымен қатар, жүйе каталогтарды айналып өту (Directory Traversal), зиянды немесе дұрыс емес HTTP тақырыптарын (Header Rejection), сондай-ақ зиянды HTTP кодтарын қорғауды қамтамасыз етуі керек; Шешім HTTP/3 over QUIC протоколын қолдауы тиіс; Лицензия бар жағдайда құмсалғыш (Sandboxing) функционалы (бұлтта немесе жергілікті бөлінген құрылғыда инспекция) қамтамасыз етілуі тиіс; Шешім пайдаланушыларды сәйкестендіру және бақылау (Identification & User Control) функционалын қамтамасыз етуі тиіс; Райдаланушылар идентификаторларын Microsoft Active Directory қауіпсіздік оқиғаларын талдау арқылы алу мүмкіндігі; Домен құрамына кірмейтін құрылғылар мен пайдаланушылар үшін браузер арқылы идентификатор бойынша аутентификацияны қолдау; Пайдаланушылар компьютерлеріне саясат бойынша орнатылатын және идентификаторларды қауіпсіздік шлюзіне жіберетін арнайы агент болуы тиіс; Кіріктірілген VPN қолдауы (Site-to-Site VPN, Remote Access VPN); Райдаланушыларды Active Directory, RADIUS, LDAP арқылы аутентификациялау; IP/MAC-мекенжай бойынша пайдаланушыларды аутентификациялау және икемді қауіпсіздік ережелерін қолдау; Қазақстан Республикасының ақпаратты қорғау саласындағы заңнамасының талаптарына сәйкес келетін заманауи криптографиялық шифрлау және аутентификациялау алгоритмдерін қолдау; Шешім кемінде келесі Diffie-Hellman топтарын қолдауы

	тиіс: Топ 1 (768 бит), Топ 2 (1024 бит), Топ 5 (1536 бит), Топ 14 (2048 бит), Топ 19 және Топ 20; Шешім кіріктірілген сертификаттау орталығын (CA) да, сыртқы үшінші тарап сертификаттау орталықтарын да қолдануды қолдауы тиіс; Шешім кемінде келесі деректер тұтастығын қамтамасыз ету механизмдерін қолдауы тиіс: MD5, SHA-1, SHA-256, SHA-512 және AES-XCBC алгоритмдерін пайдалану; Құзыреттерді тиімді бөлу үшін рөлдік қолжетімділікті басқару (RBAC) қолдауы; Шешім екі факторлы аутентификацияны қамтамасыз етуі тиіс, соның ішінде сыртқы екі факторлы аутентификация жүйелерімен интеграция арқылы немесе өндірушінің кіріктірілген механизмі арқылы; Пайдаланушылар, топтар, IP-мекенжайлар, қолданбалар, қолданба санаттары және басқа параметрлер бойынша қауіпсіздік саясаттарын баптау мүмкіндігі; Саясаттарды кесте бойынша белсендіру мүмкіндігі, оның ішінде уақыттық шектеулер мен қолжетімділік шарттары; Қауіпсіздік саясаты бұзылған кезде автоматты түрде есептерді қалыптастыру; Қолданбаларды басқару дерекқоры кемінде 10 000 белгілі қолданбаны қамтуы тиіс; Шешім кемінде 250000 Web 2.0 виджетіне егжей-тегжейлі қауіпсіздік бақылауын қамтамасыз етуі тиіс; Сыртқы интеграциясыз кіріктірілген екі факторлы аутентификация жүйесі;; 200 миллионнан астам URL-ді қамтитын URL-категоризацияны қамтамасыз ету; Лицензия бар жағдайда құмсалғыш (Sandboxing) функционалы (инспекция – бұлтта немесе жергілікті бөлінген құрылғыда). Желілік функциялар және істен шығуға төзімділік Жүктемені басымдыққа қарай интеллектуалды басқару үшін SD-WAN қолдауы (SD-WAN); Жүктемені теңгеру үшін өткізу қабілетін басқару (Traffic Shaping); Сыртқы телеметрия және осалдық мониторинг жүйелерімен интеграция; Маршрутизация протоколдарын қолдау: OSPFv2, BGPv4, RIP, PIM (SM, DM, SSM), IGMP; IPv6 және dual-stack туннелдеу IPv4-over-IPv6 қолдауы; Ақау кезінде автоматты ауысу мүмкіндігі бар Active/Passive кластерлеу; Бұлттық портал арқылы орталықтандырылған басқару; Сыртқы интеграциясыз кіріктірілген екі факторлы аутентификация жүйесі; Желілік қосылыстарды егжей-тегжейлі визуализациялау және пайдаланушылардың аномалды әрекеттерін талдау мүмкіндігі.. Өнімділік NGFW өткізу қабілеті: кемінде 1,2 Gbps; Threat Prevention (Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot және бұлттық Sandbox функционалы қосылғанда): кемінде 750 Mbps; IPS өткізу қабілеті: кемінде 1,7 Gbps; Firewall өткізу қабілеті: кемінде 2,2 Gbps; VPN AES-128 өткізу қабілеті: кемінде 1,4 Gbps; Жаңа қосылыстарды орнату жылдамдығы: кемінде 16 000 қосылыс/сек; Бір мезгілдегі максималды қосылыстар саны: кемінде 1 000 000; Процессор және желілік интерфейстер жүктемесін кеңейтілген мониторингтеу мүмкіндігі; Өндірушінің қолдауы/жазылымы 12 айға ұсынылады және актімен расталатын лицензияны белсендіру/пайдалануға енгізу күнінен бастап есептеледі. 12 айлық кепілдік мерзімі жабдықты/БҚ-ны пайдалануға енгізу (қабылдау) актісіне қол қойылған күннен бастап есептеледі. Жеткізілген жабдық/БҚ

	бойынша кепілдік міндеттемелер/қолдау қызметтер көрсету мерзімі аяқталған кезде тоқтатылмайды және кепілдік кезеңі ішінде қолданылады. Аппараттық сипаттамалар WAN порты: кемінде 1× 10/100/1000Base-T RJ-45; LAN порттары: кемінде 6× 10/100/1000Base-T RJ-45; Консоль порты: кемінде 1× USB-C; USB порттары: кемінде 2× USB 3.0; Жұмыс температурасының диапазоны: 0°C-тан 40°C-қа дейін Қосымша талаптар Мобильді қосымша арқылы басқаруды қолдау; Саясаттарды орталықтандырылған басқару мүмкіндігі; Жылдам енгізу (Zero Touch Deployment) қолдауы; Нақты уақыт режимінде есеп беру және лог жүргізу мүмкіндігі; Бір интерфейс арқылы бірнеше қауіпсіздік шлюзін басқару мүмкіндігі; Қауіпсіздік сертификаттауларын қолдау: CB 62368-1, UL 62368-1, FCC IC Class B, CE, VCCI, RoHS, REACH, WEEE; Осы Техникалық ерекшелікте көрсетілген жабдықтар, бағдарламалық қамтамасыз ету және лицензиялар жеткізуші тарапынан тек АҚЖО қызметтерін көрсету мақсатында жеткізіледі және өздігінен сатып алу нысаны болып табылмайды. Көрсетілген элементтердің құны қызметтердің құнына кіреді және бөлек есептелмейді. 11. EDR класты бағдарламалық қамтамасыз етуге қойылатын талаптар EDR (Endpoint Detection and Response) ақпараттық қауіпсіздік құралдарына лицензия талаптары бағдарламалық қамтамасыз ету Қазақстан Республикасы Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 2026 жылғы 2 маусымдағы № 279/НҚ бұйрығына сәйкес, сенімді бағдарламалық қамтамасыз ету және электрондық өнеркәсіп өнімдері тізіліміне енгізілуі тиіс. Жалпы (жүйелік) талаптар: 11.1. Архитектура талаптары 11.1.1. Орталықтандырылған архитектура: Жүйе біртұтас деректер өңдеу орталығында орналастырылған. Барлық деректерді өңдеу және басқару орталықтандырылған түрде жүзеге асырылады. 11.1.2. Істен шығуға төзімділік және деректерді сақтық көшірмелеу: Деректерді сақтық көшірмелеу және автоматты қалпына келтіруді қолдау. Жоғары қолжетімділікті қамтамасыз ету үшін түйіндерді баптау. 11.1.3. Деректер қауіпсіздігі: Деректерді тасымалдау кезінде (TLS 1.2/1.3) және сақтау кезінде шифрлау. Рөлдік қолжетімділікті басқару (RBAC) негізінде қолжетімділікті бақылау. 11.1.4. Өнімділік және жүктеме: Үлкен көлемдегі телеметрияны нақты уақыт режимінде өңдеу. Инфрақұрылымға минималды талаптар: процессор – 4 ядродан, ЖЖҚ – 16 ГБ, SSD-дискілер. 11.1.5. Интеграция және үйлесімділік: Стандартты API интерфейстерін қолдау (REST, JSON). SIEM, SOAR және басқа киберқауіпсіздік құралдарымен интеграция. 11.1.6. Мониторинг және басқару: Веб-консоль арқылы орталықтандырылған басқару. Жүйенің күйін нақты уақыт режимінде мониторингтеу. Журнал жүргізу және есеп беру мүмкіндігі. Журналдағы оқиғаларды сүзгілеу, корреляциялау және ақпараттық қауіпсіздік оқиғаларын талдауды қамтамасыз ететін аналитикалық сұраулар тілдерін және іздеу механизмдерін қолдау. Оқиғалар журналынан ақпарат іздеу үшін KQL/ES|QL сұраныс тілін қолдау. Қосымша талаптар - Жүйенің on-premise, қоғамдық бұлттар және гибридті

	нұсқаларда жұмыс істеу мүмкіндігі. - Локалды және мультиоблачное орналастыруды қолдайтын, ашық деректер схемасы бар масштабталатын іздеу платформасы. - Функционалдық талаптар бір шешім аясында да, бірнеше шешімді біріктіру арқылы да орындалуы мүмкін, бастысы осы Техникалық ерекшеліктегі барлық талаптардың сақталуы. - Сыртқы шешімдермен интеграция модульдерін басқару және консоль арқылы интеграция пакеттерін қосу мүмкіндігі. - Инциденттерді іздеу, талдау, жауап беру және приоритизациялау үшін AI-ассистентті қолдау; ассистент LLM чат-бот түрінде ұсынылуы тиіс. - Соңғы құрылғылар топтарына саясаттар тағайындау мүмкіндігі. - Рөлдік қолжетімділік (RBAC) және консоль операторларының әрекеттерін аудиттеу қолдауы - Консоль аналитиктердің инциденттер бойынша бірлесіп жұмыс жасауын қолдауы, соның ішінде делегирование және статустарды өзгерту мүмкіндігі. - Корпоративтік периметрден тыс жүйелерді қорғау үшін VPNсыз соңғы нүктелерді басқару мүмкіндігі. - Оқиғаларды талдау үшін алдын ала орнатылған және бапталатын дашбордтардың болуы. - Іске қосылған процестер арасындағы байланыстарды масштабталатын визуализациялау. - Шектеусіз әкімшілер санын қолдау. - Басқару консолі мен модульдер арасындағы деректер алмасуы TLS 1.2 арқылы жүзеге асуы тиіс. - Өнім отандық өндірістен не өзге өндірістен болуы, тапсырыс берушінің Қазақстан Республикасының аумағында пайдалануына құқық беретін құқық иеленушінің қолданыстағы лицензиясы болуы және Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының талаптарына сәйкес келуі тиіс («Киберқауіпсіздік туралы» Қазақстан Республикасы Заңының 61-бабы 3-тармағының 2) тармақшасы). - Осы Техникалық ерекшелікте көрсетілген жабдықтар, бағдарламалық қамтамасыз ету және лицензиялар жеткізуші тарапынан тек АҚЖО қызметтерін көрсету мақсатында жеткізіледі және өздігінен сатып алу нысаны болып табылмайды. Көрсетілген элементтердің құны қызметтердің құнына кіреді және бөлек есептелмейді. Функционалды талаптар 11.2. Операциялық жүйелерді қолдау 11.2.1.Жұмыс станциялары: -Windows: Windows 10, Windows 11 (x64). -macOS: macOS 11 Big Sur және одан жоғары нұсқалары. - Linux: Ubuntu 18.04 LTS және одан жоғары, Debian 10 және одан жоғары. 11.2.2.Серверлер: - Windows Server 2016, 2019, 2022. - Linux: Red Hat Enterprise Linux 8, CentOS 7.9-2009 және одан жоғары. 11.2.3.Мобильді құрылғылар: - Android: Android 9.0 және одан жоғары нұсқалары. - iOS: iOS 13 және одан жоғары нұсқалары. 11.2.4.Виртуалды орта: -VMware, Hyper-V, KVM-де виртуализацияны қолдау. 11.3. Сканерлеу түрлері 11.3.1.Қол жетімділікті сканерлеу (On-access): - Файлдарды жасау, ашу, өзгерту немесе орындау кезінде оларды автоматты түрде сканерлеу. 11.3.2.Сұраныс бойынша сканерлеу (d-demand): - Сканерлеуді агент интерфейсі арқылы қолмен іске қосыңыз. 11.3.3.Алынбалы медианы сканерлеу: -Қосылған USB құрылғыларын, сыртқы қатты дискілерді және басқа алынбалы медианы тексеріңіз. 11.3.4.Жоспарлы сканерлеу: - Кесте бойынша реттелетін сканерлеу тапсырмалары (күнделікті, апта сайын,

	ай сайын). 11.3.5.Жедел жадты сканерлеу: - Жедел жадтағы процестер мен деректерді зиянды бағдарлама белгілерінің бар-жоғын тексеру. 11.3.6.Жүйені терең сканерлеу: - Мазмұнын егжей-тегжейлі талдай отырып, бүкіл файлдық жүйені сканерлеу. 11.4. Сканерленетін Архив форматтары 11.4.1.Қолдау көрсетілетін Архив форматтары: -7zip, ace, arj, bzip2, cab, gz, gzip, jar, rar, tar, tgz, xz, zip, zipx. 11.4.2.Сканерлеу ерекшеліктері: - Ішкі архивтерді ашу. - Көп томдық архивтерді қолдау. - Барлық қолдау көрсетілетін форматтарда зиянды мазмұнды сканерлеу. Сканерленетін желілік протоколдар Қолдау көрсетілетін хаттамалар: - HTTP, HTTPS -FTP, FTPS -IMAP, IMAPS -SMTP, SMTPS -POP3, POP3S - DNS Сканерлеу ерекшеліктері: - Кіріс және шығыс трафикті талдау. - Деректерді беру хаттамаларында зиянды элементтерді анықтау. - TLS қолдауымен шифрланған трафикті тексеру. Сканерленетін желілік ресурстар Қолдау көрсетілетін ресурстар: SMB (Windows Shares), NFS (Network File System), WebDAVСканерлеу ерекшеліктері: - Желілік ресурстардың мазмұнын қауіп-қатерге талдау. - Файлдардың қол жетімділігі мен өзгеруін тексеру. - Рұқсатсыз кіруді анықтау. Ақпараттың тұтастығы мен қолжетімділігін қамтамасыз етуге қойылатын талаптар Жергілікті деректерді сақтау: антивирустық агент графикалық интерфейс арқылы көруге болатын жергілікті есептер қоймасына ие болуы керек. - Қосымша талдау үшін есептерді файлға экспорттауға қолдау болуы керек. Карантин: анықталған зиянды файлдарды жергілікті қоймаға жылжыту мүмкіндігі (карантин), содан кейін қажет болған жағдайда қалпына келтіру. Қауіптерді анықтаудағы әрекеттер: - Процестерді аяқтау. - Файлдарды жою. - Пайдаланушы ережелеріне негізделген жалған позитивтерді елемеу. Мінез-құлықты талдау: - Зиянды белсенділікті анықтау үшін процестердің мінез-құлқын талдау мүмкіндігі. -Осалдықтарды пайдалану әрекеттерін анықтау. Араласудан қорғау: - Процестерді тоқтатудан және антивирустық агент файлдарын жоюдан қорғау. - Параметрлерді рұқсатсыз өзгертуден қорғау үшін құпия сөзді орнату мүмкіндігі. Антивирустық компоненттерді жаңарту: - Интернет, Жергілікті сервер немесе желілік каталог арқылы жаңарту. - Қолтаңбалар мен қауіп-қатер базасын автоматты түрде жаңарту. 11.5. Компоненттің тұтастығы мен қолжетімділігін қамтамасыз етуге қойылатын талаптар 11.5.1.Рұқсатсыз араласудан қорғау: - Агент процестерін тоқтатудан немесе жоюдан қорғау. - Авторизациясыз параметрлердің өзгеруін бұғаттау. - Әкімшілік консоль арқылы кіру құқығын орнату. 11.5.2.Өзін-өзі емдеу механизмдері: - Апаттар кезінде сыни қызметтерді автоматты түрде қайта іске қосыңыз. - Файлдық жүйелер мен компоненттер конфигурацияларының тұтастығын бақылау. 11.5.3.Қол жеткізуді басқару және аутентификация: - Жүйе конфигурациясының барлық өзгерістерін журналға жазу. 11.5.4.Өнімділік мониторингі: - Ескертулермен жүйенің жай-күйін үздіксіз бақылау. - Нақты уақыттағы компоненттердің күйі туралы есептер. 11.5.5.Жаңартулар мен түзетулер: - Тұрақты жаңартулар мен қауіпсіздік патчтары. - Қорғалған байланыс арналары арқылы

	қолтаңба базалары мен қауіпсіздік саясатын жаңарту. 11.6. Антивирустық компоненттер мен қолтаңба жиынтығын жаңарту көздері 11.6.1.Қашықтағы көздер: - Интернет арқылы қол жетімді өндірушінің сервері (https). -Бұлтты сақтау. 11.6.2.Жаңартуларды автоматтандыру: - Реттелетін автоматты жаңарту кестесі. - Веб-консоль арқылы жаңартуларды қолмен іске қосуды қолдау. 11.6.3.Қорғалған деректерді беру: - Жаңартуларды қауіпсіз тасымалдау үшін TLS пайдалану. - Орнату алдында компоненттердің сандық қолтаңбаларын тексеру. Орталықтандырылған басқару мүмкіндіктері Орталықтандырылған орнату және жаңарту: - Орталық консольден жүйе компоненттерін орнату, жаңарту және жою. - Барлық соңғы нүктелердегі қауіпсіздік саясатын басқару. Мониторинг және бақылау: - Нақты уақыт режимінде жүйенің жұмысын орталықтандырылған бақылау. - Оқиғалар журналдарын және жаңарту тарихын қарау. Конфигурацияны басқару: - Топтық саясатты қолдана отырып, жүйе параметрлерін теңшеу. - Пайдаланушылардың қол жеткізу құқықтары мен рөлдерін басқару. Оқиғаларға жауап беру: - Құрылғыларды оқшаулауға командалар жіберу. - Процестерді, файлдарды және желілік қосылымдарды бұғаттау. - Соңғы нүктелерде қашықтағы командаларды орындау. Есептер мен хабарламалар: - Қауіпсіздік туралы егжей-тегжейлі есептер шығару. - Қауіпсіздік оқиғалары мен жүйенің жаңартулары туралы реттелетін хабарламалар. Сыртқы жүйелермен Интеграция: - Siem, SOAR және басқа қауіпсіздік жүйелерімен Интеграция. -Басқа ат шешімдерімен өзара әрекеттесуге арналған API. 11.7. Оқиғаларға жауап беру 11.7.1.Инциденттерге ден қою жөніндегі іс-қимылдар: - Процесті аяқтаңыз; - Файлды жою; - Файлды жұмыс станциясынан аналитиктің компьютеріне немесе ДК қоймасына жүктеңіз; - Жүйелік артықшылықтары бар Операциялық жүйе пәрменін орындаңыз; - Автоматты түрде іске қосылатын нысандарды/сценарийлерді алыңыз; - Орындалатын файлдарды бұғаттау (хэш, Файл атауы); - Оқиғаларға жауап беру үшін Playbook құру функциясы. Басқа жүйелермен Интеграция 11.7.2.SIEM жүйелерімен Интеграция: - Деректерді алмасудың стандартты протоколдары мен интерфейстері (API, syslog, REST, webhook және басқалары) арқылы өндірістік SIEM жүйелерімен интеграцияны қолдау. - Нақты уақыттағы оқиғалар мен анықталған қауіптер туралы деректерді беру. 11.7.3.SOAR интеграциясы: - Soar платформалары арқылы жауап беру процестерін автоматтандыруды қолдау (мысалы, IBM Resilient, ServiceNow). 11.7.4.Осалдықтарды басқару жүйелерімен Интеграция: -Осалдықты сканерлеу жүйелерімен байланыс (мысалы, Tenable, Qualys). 11.7.5.Қол жеткізуді басқару жүйесімен Интеграция: - Есептік жазбаларды басқаруға арналған LDAP, Active Directory интеграциясы. -SAML арқылы SSO қолдау. 11.7.6.API және веб-ілмектер: - Оқиғалар, қауіптер мен оқиғалар туралы деректерді алу үшін REST API. -Ескерту жүйелеріне деректерді жіберуге арналған Веб-ілмектер. 11.7.7.Бұлтты интеграция: - Amazon AWS, Microsoft Azure, Google Cloud бұлтты қызметтерін қолдау. -Бұлтты ресурстарды басқару және деректерді қорғау үшін кіріктірілген

	интеграциялар. 11.7.8.Техникалық интеграция: - Күдікті хаттарды талдауға арналған пошта жүйелерімен Интеграция (SMTP/IMAP). - Киберқауіптер туралы деректерді бөлісу үшін STIX/TAXII есеп форматтарын қолдау. 11.8. Техникалық қолдау Жеке техникалық менеджерге қойылатын талаптар Өнім беруші жеке техникалық менеджерді бөледі, ол: 11.8.1. Тапсырыс берушінің сұраныстарын өңдеумен айналысады. 11.8.2. Техникалық қолдау жұмыстарын ұйымдастырады. 11.8.3. Тапсырыс берушіні сұрау салуларды шешудің ағымдағы жай-күйі туралы хабардар етеді. 11.8.4. Жұмыс күндері Астана уақыты бойынша дүйсенбіден жұмаға дейін сағат 9.00-ден 18.00 дейінгі телефон және электрондық пошта арқылы қолжетімді. Техникалық қолдаудың реакция уақытына қойылатын талаптар Техникалық қолдау демалыс және мереке күндерін қоса алғанда, интернет-портал және (немесе) телефон және (немесе) электрондық пошта арқылы тәулік бойы қолжетімді болуы тиіс. Жауап беру уақыты: - Сыни деңгей-30 минуттан аспайды - Жоғары деңгей-4 жұмыс сағатынан аспайды - Орташа деңгей-6 жұмыс сағатынан аспайды - Төмен деңгей-8 жұмыс сағатынан аспайды "Сыни деңгей" -бүкіл жергілікті желі (немесе желінің маңызды бөлігі) жұмыс істемейді, бұл негізгі бизнес-процестерді тоқтатады. "Жоғары деңгей" - өнім толығымен істен шыққан, бірақ негізгі бизнес-процестердің үздіксіздігі бұзылмайды. "Орта деңгей" - өнім ішінара істен шыққан (сәйкес емес жұмыс істейді), бірақ өнімнің жұмысының нәтижесінде пайдаланушының басқа бағдарламалық жасақтамасы істен шыққан жоқ. "Төмен деңгей" - басқа маңызды емес қызмет сұрауларын білдіреді. Жоғарыда айтылмаған барлық оқиғалар осы сыни деңгейге жатады. Техникалық қолдау сұрауларының түрлері - Өнімді орнату, конфигурациялау және жұмыс істеу процесінде оқиғаларды шешу бойынша кеңес беру. - Зиянды бағдарламалармен жұқтырылған файлдарды емдеу бойынша кеңестер; - Антивирустық қолтаңбалар жиынтығын басымдықпен шығаруды жүзеге асыру, оның ішінде: - берілген жиынтықтан жекелеген зиянды заттарды анықтау, осындай жиынтықтың зиянды заттарының әрқайсысы үшін қолтаңбалардың дайындығына қарай; - осы жиынтыққа қолтаңбалар дайын болғаннан кейін бір уақытта зиянды заттар жиынтығын анықтау. - Антивирустық бағдарламалық қамтамасыз етуді өндірушінің білікті мамандарымен (вирустық талдаушылар, компьютерлік криминалистика және инциденттерге ден қою жөніндегі мамандар), зиянды кодты зерттеу, Компьютерлік криминалистика және компьютерлік инциденттерге ден қою мәселелері бойынша қажеттілігіне қарай, бірақ жыл ішінде 50 сағаттан аспайтын консультациялар; Бағдарламалық жасақтаманы жаңартуға қойылатын талаптар – Антивирустық қолтаңбалар жиынтығын жаңарту жиілігі-аптасына кемінде бір рет. - "Орталықтандырылған басқарылатын антивирустық қорғау ДК" және "Sandbox компоненті бар ақпараттық қауіпсіздік инциденттерін анықтау және орталықтандырылған әрекет ету ДК" агенттерін жаңарту кезеңділігі – тоқсанына кемінде бір рет. - Өнім беруші анықталған осалдықты сипаттайтын Тапсырыс берушінің сұранысы бойынша компоненттердің бағдарламалық

	жасақтамасына түзетулер (патчтар) шығаруды қамтамасыз етуі керек. Жабдықтың ақаулыққа төзімділігін қамтамасыз етуге қойылатын талаптар Өнім берушіде компоненттердің серверлік жабдықтарына арналған қосалқы бөлшектер, құралдар, керек-жарақтар мен материалдар болуы керек және жабдық істен шыққан жағдайда олардың сыни деңгейге сәйкес тұрақты жұмысын қалпына келтіруі керек. Деректерді сақтауға және өңдеуге қойылатын талаптар: - 7 күнге дейін сақталатын толық телеметрия. - TLS протоколы арқылы қорғалған байланыс арнасы арқылы барлық деректер мен метадеректерді шифрлау. Жеткізу талаптары Жабдықтар мен бағдарламалық қамтамасыз етуді жеткізу бір жолғы түрде жүзеге асырылады, бірақ Қазақстан Республикасы мемлекеттік сатып алуды жүзеге асыру қағидаларының 569-тармағында белгіленген ең төменгі мерзім аяқталғаннан кейін ғана. Өнімділікті тексеруге қойылатын талаптар Тапсырыс берушінің аумағында шарт талаптарына сәйкес тауардың жұмыс қабілеттілігі мен толықтығын тексеру және тексеру үшін жеткізуді жүзеге асыру. Жұмыс қабілеттілігін тексеру іске қосу және сынамалық қосу, зақымданулардың, ақаулардың, жарықтардың, коррозияның болмауын көзбен шолып тексеру жолымен жүзеге асырылады. 12. Ақпараттық қауіпсіздік саласындағы шешімдердің архитектуралық принциптері мен жіктелуіне қойылатын талаптар 1. Шешімдер сыныбына сәйкестік қағидаты Ақпараттық қауіпсіздікке (АҚ) қойылатын әрбір функционалдық Талап АҚ архитектурасы мен әдіснамасында белгіленген шешімдердің жеке, нақты айқындалған сыныбына сәйкес келетін шешіммен іске асырылуға тиіс 2. Функционалдық талаптар бір шешім шеңберінде де, бірнеше шешімді біріктіру арқылы да жүзеге асырылуы мүмкін, бастысы осы Техникалық ерекшеліктегі барлық талаптардың орындалуы. 3. Дербестік өлшемшарты Әрбір енгізілген шешім ақпараттық қауіпсіздікті қамтамасыз етудің дербес және тәуелсіз функциясын орындауға міндетті.
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)	Әлеуетті өнім беруші оны жеңімпаз деп анықтаған және Мемлекеттік сатып алу туралы шарт жасасқан жағдайда мыналарды ұсынуға міндетті: Техникалық ерекшелікте көзделген өнімдерді жеткізуге (ұсынуға) Өнім берушінің құқығын растайтын құқық иеленушінің (өндірушінің) немесе оның ресми өкілінің хаттары (сертификаттары) шарт күшіне енген күннен бастап 10 (он) жұмыс күні ішінде ұсынылады. Көрсетілген хат Техникалық ерекшелікке енгізілген әрбір өнім үшін бөлек ұсынылуы керек және мыналарды қамтуы керек: 1. Вендор құрастырған және ресми растаған техникалық ерекшелік талаптары мен тиісті өнімнің/шешімнің сипаттамаларын егжей-тегжейлі салыстыратын кесте. 2. Вендордан осы өнімнің сертификатталғандығы және / немесе тиісті бағдарламалық қамтамасыз етуді пайдалану үшін өзекті нұсқада қолдау көрсетілетіндігі туралы растау;

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Министерство культуры и информации Республики Казахстан"
Наименование организатора	Государственное учреждение "Министерство культуры и информации Республики Казахстан"
№ конкурса:	№ 17976004-1
Наименование конкурса:	Услуги оперативного центра информационной безопасности для информационной системы «Единый электронный архив документов»
Номер лота:	№ 88480163-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:	33793103.45
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	33793103.45
Срок оказания услуги:	Шарт күшіне енген күннен бастап 2027 жылғы 31 желтоқсанды қоса алғанда, бірақ кемінде 15 күнтізбелік күннен кем болмауы тиіс.
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	1. Общие требования 1.1. Наименование закупаемых услуг: Услуги оперативного центра информационной безопасности для информационной системы «Единый электронный архив документов» (далее – ОЦИБ). 1.2. Предметом закупки являются Услуги оперативного центра информационной безопасности (ОЦИБ), направленные на обеспечение мониторинга, анализа и реагирования на инциденты информационной безопасности. Поставка оборудования, программного обеспечения и лицензий осуществляется исключительно в объёме, необходимом для оказания указанных услуг, и носит вспомогательный характер по отношению к основному предмету закупки — оказанию услуг ОЦИБ. 1.3. Место оказания услуги: Государственное учреждение "Министерство культуры и информации Республики Казахстан», город Астана, район «Есиль», проспект Мәңгілік Ел 8, подъезд 14 1.4. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых услуг: 1.4. Основные термины и определения: ИБ – информационная безопасность. SIEM (Security Information and Event Management) – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности. ИТ – информационные технологии. ITIL – методология управления, отладки и непрерывного улучшения бизнес-процессов, связанных с ИТ. SLA – соглашение об уровне обслуживания. FQDN – полное доменное имя. Связность – возможность взаимодействия между компьютерами. ИС – информационная система. VPN – виртуальная частная сеть. НКЦИБ – Национальный координационный центр информационной безопасности АО «Государственная техническая служба». Инцидент – любое событие, которое не является частью стандартных услуг и может вызвать прерывание или снижение качества услуг. ТС – техническая спецификация. Оказание Услуг направлено на повышение уровня защищенности ИТ-инфраструктуры Заказчика от современных угроз ИБ, а также проведение превентивных мер по минимизации рисков возникновения инцидентов ИБ. В рамках оказания Услуг должны быть решены следующие задачи: • Организация и осуществление мониторинга событий и обработки инцидентов ИБ, включая развертывание в инфраструктуре Заказчика компонентов Услуг. Настоящая техническая спецификация (далее – ТС) содержит общие и частные требования к оказанию Услуг, обеспечивающих решение вышеуказанных задач. Услуги по выявлению технических каналов утечки информации и специальных технических средств оперативным центром информационной безопасности, включающие: - предоставление коллекторов событий и сетевых потоков (LOG/FLOW Collector) с суммарным количеством подключаемых источников событий не более 50 (пятидесяти); Поставщик осуществляет поставку, установку, подключение и настройку технических средств ОЦИБ в течении 15 календарных дней, но не ранее истечения минимального срока, установленного пунктом 569 Правил осуществления государственных закупок, с учетом фактического объема поставки и внедрения. Факт установки, подключения и настройки оформляется письменным актом,

	подписанным Заказчиком и Поставщиком. 1.5. Заказчик предоставляет необходимые ресурсы и обеспечивает подключение источников в срок, установленный пунктом 3.6 настоящей ТС. 2. Требования к услуге 2.1. В рамках оказания Услуг поддерживаются следующие функции и дополнительные сервисы: 1) Мониторинг событий ИБ, зафиксированных на серверном оборудовании и сетевых устройствах Заказчика, подключённых к SIEM-системе Поставщика; 2) Выявление инцидентов ИБ в зоне мониторинга; 3) Информирование Заказчика о выявленных инцидентах, методах реагирования на них, а также предоставление рекомендаций по их устранению; 4) Предоставление экспертной поддержки в процессе реагирования на инциденты; 5) Сканирование ИТ-инфраструктуры Заказчика на уязвимости — не реже 1 (одного) раза в месяц (не менее 512 уникальных IP-адресов); 6) Проведение тестирования на проникновение и анализа защищенности ИТ-инфраструктуры Заказчика — 2 (два) раза в течение срока оказания Услуг по заявке Заказчика (не менее 128 уникальных IP-адресов); 7) Консультирование при расследовании критичных инцидентов ИБ; 8) Оказание помощи и консультаций при прохождении испытаний на соответствие требованиям информационной безопасности; 9) Проведение аудита информационной безопасности (1 (один) раз в течение действия договора) в рамках оказания услуги оперативного центра информационной безопасности для ИС «Единый электронный архив документов» на соответствие Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности с представлением письменного отчета и рекомендаций; 10) В случае выявления подозрительных событий, касающихся систем, не входящих в зону мониторинга, дальнейшее расследование Заказчик осуществляет самостоятельно. Поставщик при необходимости консультирует Заказчика для определения степени критичности, проводит дополнительный анализ с целью выявления источника проблемы и содействует специалистам Заказчика в устранении инцидента; 11) Сервис управления и мониторинга привилегированного доступа (на 3 (три) пользователя), обеспечивающий централизованное хранение учетных данных, разграничение прав доступа, управление привилегированными сеансами, запись сеансов и журналирование действий пользователей; 2.2. Расширенная экспертиза По запросу Заказчика может быть предоставлена дополнительная расширенная экспертиза зоны мониторинга согласно приложению 6 к настоящей ТС. 2.3. Услуги оказываются в соответствии с настоящей технической спецификацией с использованием следующих средств мониторинга и реагирования на инциденты информационной безопасности: 1) система управления событиями информационной безопасности (SIEM); 2) сервис управления и мониторинга привилегированного доступа; 3) сканер уязвимостей (Vulnerability Scanner), обеспечивающий обнаружение узлов, выявление уязвимостей операционных систем и приложений, оценку их критичности и формирование отчетов с рекомендациями по устранению; 2.4. Предлагаемые средства должны сопровождаться технической

	поддержкой от производителей решений на срок действия договора, что должно быть подтверждено официальным письмом от производителя или его официального представителя (дистрибьютора) со ссылками на веб-ресурсы (при наличии), предоставляемым заказчику. 2.5. Уровень критичности инцидентов, которые могут возникнуть в рамках оказания Услуг. Для каждого инцидента ИБ устанавливается приоритет в соответствии с приложением № 2 к настоящей ТС. Реагирование на инциденты ИБ осуществляется в сроки, определенные временными характеристиками, приведенными в приложении № 3 к настоящей ТС. 3. Поставщик должен: 3.1. На основании опросного листа, заполненного Заказчиком, проводить анализ (обследование) ИТ-инфраструктуры Заказчика в части подключаемых информационных систем (ИС), включая: 1) выдачу рекомендаций по составу подключаемых источников событий информационной безопасности (далее – источники); 2) типизацию источников на стандартные и нестандартные, в соответствии с базой знаний Поставщика; 3) определение потребностей Заказчика в подключении существующих и разработке новых сценариев выявления атак; 4) определение объема требуемых лицензий. На данном этапе должны быть собраны следующие сведения: 1) название источника; 2) описание функционала источника (принадлежность к ИС); 3) площадка размещения; 4) производитель/марка/модель; 5) тип/версия ОС; 6) тип/версия ПО; 7) FQDN; 8) IP-адрес. 3.2. В соответствии с настоящей технической спецификацией, должны быть определены и выработаны организационно-технические решения по: 1) целевой архитектуре оказания Услуг; 2) техническим характеристикам и требованиям к вычислительным ресурсам, выделяемым Заказчиком, включая расчет емкости файловых хранилищ; 3) порядку развертывания компонентов Услуг, в том числе на площадке Заказчика; 4) порядку и организации межсетевого взаимодействия компонентов Услуг на площадке Заказчика и центра мониторинга и реагирования на киберугрозы. 3.3. Поставщик должен выполнить подключение источников: 1) организовать защищенное VPN-соединение на оборудовании Поставщика (далее – VPN-соединение) между площадкой Заказчика и Поставщика по согласованным параметрам. В случае отсутствия L3-связности между распределенными площадками необходимо обеспечить установление VPN-соединений с каждой из них; 2) произвести инсталляцию компонентов SIEM-системы. При необходимости предоставить Заказчику требования к вычислительным ресурсам, подсистемам хранения и рекомендации по конфигурированию для установки дополнительных компонентов Услуг; 3) выполнить конфигурирование и профилирование SIEM под ИТ-инфраструктуру Заказчика, что гарантирует работоспособность сценариев выявления нарушений и инцидентов информационной безопасности; 4) направить инструкции по подключению источников к сервису мониторинга и анализа событий информационной безопасности; 5) разработать до 3 (трех) индивидуальных адаптеров для нестандартных источников; 6) разработать новые сценарии выявления атак, включая расширение категорий инцидентов и правил

	корреляции на основе специфичных запросов Заказчика, согласованных с Поставщиком; 7) провести проверку сетевой связности между компонентами SIEM-системы, источниками и площадкой Поставщика в соответствии с настоящей технической спецификацией. 3.4. На базе центра мониторинга и реагирования на киберугрозы Поставщик должен: 1) обеспечивать анализ событий информационной безопасности в режиме 24/7 силами аналитиков первой линии дежурной смены, которая является единой «точкой входа» для всех поступающих от различных источников событий. Аналитики первой линии должны обеспечивать обработку инцидентов информационной безопасности, первичную проверку ложных срабатываний, проведение первичной аналитики и выделение инцидентов информационной безопасности на основе категорий инцидентов и правил, регистрацию и последующее сопровождение инцидентов в соответствии со стандартами ITIL (категоризация, приоритизация, SLA); 2) мониторинг состояния компонентов SIEM-системы, установленных как на площадке Заказчика, так и на площадке Поставщика; 3) мониторинг состояния VPN-канала; 4) предоставление рекомендаций по обработке инцидентов силами аналитиков второй линии в режиме 8/5, а также решение типовых инцидентов информационной безопасности. В рамках этого процесса должно быть обеспечено проведение углубленной аналитики с использованием специализированных инструментов, а также адаптация правил корреляции в соответствии с изменениями в инфраструктуре Заказчика. При необходимости, добавление исключений в правила корреляции по запросу Заказчика; 5) проведение расследований инцидентов критического уровня силами третьей экспертной линии, предоставление рекомендаций по устранению подтвержденных инцидентов, а также проведение ретроспективной аналитики и актуализация информации о релевантных угрозах и атаках, способах их обнаружения и противодействия; оценка состояния защищенности и устойчивости объектов информатизации (аудит кибербезопасности); 6) Экспертиза инцидентов и угроз кибербезопасности, техническое расследование; 7) Мониторинг, анализ и прогнозирование угроз кибербезопасности; 8) Локализация и нейтрализация последствий инцидентов кибербезопасности; 9) Реагирование на угрозы и инциденты кибербезопасности; 10) в случае обнаружения инцидента ИБ в инфраструктуре Заказчика обеспечить передачу информации об инциденте в НКЦИБ в порядке и сроки, установленные законодательством Республики Казахстан в сфере информатизации, с одновременным уведомлением Заказчика; 11) предоставление отчетности по каждому выявленному инциденту информационной безопасности по одному из каналов связи: электронная почта, телефонный звонок. 3.5. Заказчику должно быть обеспечено предоставление доступа к интерфейсу систем реагирования и управления инцидентами информационной безопасности. Функционал личного кабинета должен включать: 1) доступ к актуальной информации по статусу инцидентов; 2) возможность самостоятельной регистрации инцидентов; 3) просмотр статистики по произошедшим инцидентам; 4)

	отчетность по каждому выявленному инциденту; 5) получение отчетов и уведомлений от Поставщика. 3.6. Заказчик обязан в течение 14 (четырнадцати) рабочих дней со дня вступления договора в силу предоставить и выделить необходимые ресурсы, запрашиваемые Поставщиком для внедрения Услуг, а также обеспечить подключение всех необходимых источников к SIEM-системе в указанный срок. 3.7. Поставщик при содействии Заказчика обязан организовать сетевую связность между компонентами, необходимыми для оказания Услуги, и ИТ-инфраструктурой Заказчика. 3.8. Поставщик должен организовать защищенное VPN-соединение на оборудовании Заказчика между площадкой Заказчика и площадкой Поставщика по параметрам, согласованным с Заказчиком. 3.9. Поставщик обязан ежемесячно, не позднее 3 (третьего) числа месяца, следующего за отчетным и декабрьский отчет не позднее 20 декабря 2027 года предоставлять Заказчику подробные отчеты об оказанных Услугах по каждой площадке, на которой размещено оборудование с сопроводительным письмом с обязательной регистрацией в канцелярии Заказчика. 4. Взаимодействие Поставщика и Заказчика 4.1. Разрабатывается Регламент, который устанавливает порядок взаимодействия между Поставщиком и Заказчиком по вопросам оказания услуг по обеспечению ИБ и описывает процедуры, связанные с выявлением и реагированием на инциденты ИБ. 4.2. Взаимодействие центра мониторинга Поставщика и Заказчика включает: 1) регистрацию заявок на несоответствие оказываемых услуг требуемым параметрам качества; 2) организацию процесса восстановления сервиса; 3) взаимное информирование ответственных руководителей обеих сторон о ходе решения вопросов, связанных с восстановлением требуемого качества услуг. 4.3. Поставщик обязан оказывать услуги 24 часа в сутки, 7 дней в неделю. 4.4. Разграничение зон ответственности между Поставщиком и Заказчиком на период оказания услуги ОЦИБ указано в приложении №5 к настоящей ТС. 4.5. Процедура взаимодействия Сторон при выявлении инцидентов В случае обнаружения инцидента Заказчиком, он уведомляет Поставщика по контактным данным технической службы Поставщика, указанный в регламенте. Поставщик регистрирует инцидент и сообщает Заказчику следующие данные: 1) номер зарегистрированного инцидента; 2) время регистрации; 3) тема (краткое описание); 4) информация об инциденте; 5) рекомендации по его устранению. 4.6. Уведомление об инциденте от Заказчика направляется Поставщику по электронной почте. Под реагированием на инцидент ИБ понимается структурированный набор действий, направленный на установление деталей инцидента, минимизацию ущерба и предотвращение повторения инцидента в будущем. Действия по выявлению и реагированию на инциденты ИБ, а также их последовательность, представлены в приложении № 1 к настоящей ТС. 4.7. Процедура взаимодействия Сторон при регистрации обращений Заказчика Заказчику предоставляется возможность отправлять запросы в соответствии с показателями, указанными в приложении № 4 к настоящей ТС. Для этого уполномоченный представитель

	Заказчика должен отправить запрос на электронный адрес Поставщика с указанием идентификатора в теме письма в следующем формате: 1) Тема письма: идентификатор (предоставляется сервис-менеджером), краткая суть запроса. 2) Тело письма: подробное описание запроса, указание приоритета запроса. 5. Условия надлежащего оказания Услуг 5.1. Поставщик не несет ответственности за инциденты и другие обстоятельства, повлекшие перерывы в оказании Услуг, если они вызваны одной из следующих причин: 1) проведение плановых или аварийных ремонтных работ на оборудовании, участвующем в оказании Услуг, с предварительным уведомлением Заказчика; 2) работы на оборудовании, участвующем в оказании Услуг, проводимые Заказчиком или Поставщиком по запросу Заказчика; 3) тестовое оказание Услуг по запросу Заказчика, при условии, что не было выявлено никаких инцидентов; 4) отказ или неспособность Заказчика обеспечить содействие Поставщику в установлении и устранении инцидентов в сроки, установленные уровнем оказания Услуг; 5) отказ или неспособность Заказчика предоставить необходимые данные для настройки программного обеспечения или оборудования в рамках оказания Услуг в соответствии с требованиями регламента, в срок не более 5 (пяти) рабочих дней; 6) проведение работ Заказчиком по внесению изменений в состав и конфигурацию защищаемых ресурсов без уведомления Поставщика, что может привести к их временной недоступности и, как следствие, к перерыву в оказании Услуг; 7) неработоспособность или несовместимость программного и/или программно-аппаратного обеспечения Заказчика с оказываемыми Услугами; 8) наступление обстоятельств непреодолимой силы в соответствии с условиями Договора. 6. Права Поставщика 6.1. Поставщик вправе запрашивать у Заказчика информацию, необходимую для реализации сценария выявления атак (в том числе информацию об ИТ-инфраструктуре), а также использовать эту информацию исключительно для выполнения своих обязательств по Договору, с целью минимизации ложных срабатываний. 6.2. Запрос формируется Поставщиком и направляется по электронной почте уполномоченному лицу со стороны Заказчика. В запросе должна быть указана причина обращения. Заказчик обязан предоставить обратную связь по данному запросу в течение 3 (трех) рабочих дней, при необходимости срок может быть скорректирован по согласованию сторон. Примеры запрашиваемой информации могут включать, но не ограничиваются: 1) список DNS-серверов; 2) IP-адреса сканеров безопасности; 3) список ресурсов, доступных из сети интернет; 4) список глобальных IP-адресов, принадлежащих Заказчику; 5) список учетных записей администраторов информационных систем; 6) информацию о владельцах информационных систем и ресурсов; 7) данные о принадлежности IP-адреса пользователю или системе. Информация предоставляется путем заполнения Заказчиком соответствующих опросных листов для подключения Услуг и интервьюирования уполномоченных представителей Заказчика. 7. Плановое техническое обслуживание оборудования Поставщика 7.1. Поставщик

	вправе проводить плановое техническое обслуживание или усовершенствование подсистем, на базе которых оказываются Услуги. Эти работы считаются плановыми ремонтными работами и могут повлечь за собой перерывы в оказании Услуг. Плановые ремонтные работы проводятся в интервале с 19:00 до 08:00 (время г. Астана) либо в другое время, согласованное с Заказчиком, с возможным перерывом в оказании Услуг. 7.2. Поставщик обязуется уведомить Заказчика о проведении плановых ремонтных работ, которые могут вызвать перерывы в оказании Услуг, не позднее, чем за 1 (один) рабочий день до начала работ. Исключение составляют случаи, когда работы выполняются по запросу Заказчика, а также ситуации, когда Поставщик не может уведомить в указанный срок, если плановые ремонтные работы проводятся по требованию государственных органов или компетентных телекоммуникационных органов Республики Казахстан. 7.3. Заказчик, при необходимости, может направить предложения по корректировке сроков проведения работ, которые будут учтены Поставщиком при наличии технической возможности. В уведомлении, направленном Поставщиком, указывается следующая информация: 1) время проведения плановых ремонтных работ; 2) дата проведения работ; 3) продолжительность работ; 4) контактные данные ответственного лица, предоставляющего информацию о работах; 5) необходимость участия сотрудников Заказчика в работах, например, для проведения проверок работоспособности информационных систем Заказчика. 7.4. Заказчик обязуется выделить ответственных сотрудников для участия в работах. В случае невозможности привлечения сотрудника в указанный срок, Заказчик направляет предложения по корректировке сроков проведения работ. 7.5. Если плановые работы отменяются, Поставщик уведомляет Заказчика в кратчайшие сроки после принятия решения. 7.6. Заказчик также обязан уведомить Поставщика о проведении плановых работ на своем оборудовании, если эти работы могут привести к временной недоступности защищаемых ресурсов и, как следствие, к перерыву в оказании Услуг. Уведомление должно быть направлено не позднее чем за 1 (один) рабочий день до начала работ. В уведомлении от Заказчика должны быть указаны: 1) время и дата проведения плановых работ; 2) продолжительность работ; 3) контактные данные ответственного лица, предоставляющего информацию о работах. 7.7. В случае изменения сроков проведения плановых работ Заказчик обязан уведомить Поставщика в кратчайшие сроки, но не позднее, чем за 1 (один) рабочий день до начала работ. При отмене плановых работ Заказчик также обязан уведомить Поставщика в кратчайшие сроки. 7.8. Все уведомления от Заказчика или Поставщика должны направляться на электронные адреса уполномоченных представителей, указанных в регламенте. 8. Аварийные ремонтные работы на оборудовании Поставщика 8.1. Аварийные ремонтные работы подсистем, на базе которых оказываются Услуги, проводятся в случаях, когда фиксируются периодические прерывания в оказании Услуг или значительное ухудшение параметров качества, которое может

	привести к аварийной ситуации в будущем. 8.2. Поставщик обязан уведомить Заказчика о проведении аварийных ремонтных работ не менее чем за 4 (четыре) часа до их начала. 8.3. Заказчик, в свою очередь, обязан уведомить Поставщика о проведении аварийных ремонтных работ на своем оборудовании, если они могут привести к временной недоступности защищаемых ресурсов и, как следствие, к перерыву в оказании Услуг. Уведомление должно быть направлено не менее чем за 2 (два) часа до начала работ. 8.4. Уведомления направляются на электронные адреса уполномоченных представителей, указанных в настоящем техническом регламенте. В уведомлении должны быть указаны: 1) время, дата и продолжительность аварийных ремонтных работ; 2) контактные данные ответственного лица, предоставляющего информацию о проводимых работах; 3) информация о необходимости участия сотрудников Заказчика в аварийных ремонтных работах (если работы проводятся Поставщиком). 9. Анализ вредоносных или подозрительных объектов, имеющихся у Заказчика: 9.1. Объект исследования: один подозрительный файл. В случае анализа составных файлов (архивов) объектом исследования является каждый отдельный файл, входящий в состав архива, а не архив в целом. Если анализируются составные исполняемые файлы (самораспаковывающиеся архивы, инсталляторы), объектом исследования является функционал (сценарий) этих архивов или инсталляторов. Если необходимо исследовать функционал извлечённых файлов, каждый из них рассматривается как отдельный объект исследования. 9.2. Объём исследований: по требованию Заказчика. 9.3. Основные возможные этапы проведения исследований (этапы проводятся исходя из их целесообразности, применимости, с учётом формата и структуры файла, а также необходимости для решения задач исследования. Это означает, что при анализе конкретного файла могут выполняться не все указанные этапы, но должны быть выполнены те, которые позволят достичь целей исследования): 9.4. Базовое статическое исследование объекта: 1) Определение формата и размера файла; 2) Подсчёт хэш-сумм (MD5, SHA-256); 3) Определение наличия цифровой подписи; 4) Извлечение и анализ строк, содержащихся в файле; 5) Идентификация средств компиляции файла; 6) Анализ заголовка файла, включая импортированные функции, секции, время компиляции и другие временные метки (если такие данные имеются). 9.5. Поиск данных по открытым источникам: 1) Поиск хэш-сумм, идентифицирующих объект, с помощью Google.com и Virustotal.com (с загрузкой или без загрузки объекта на ресурс, по согласованию с Заказчиком); 2) Поиск примечательных строк, содержащихся в объекте, с использованием Google.com и других сервисов. Список таких строк выбирается аналитиком в зависимости от особенностей объекта исследования. 9.6. Углубленный статический и при необходимости динамический анализ: 1) Исследование дизассемблированного, декомпилированного или иного доступного кода объекта анализа (в зависимости от формата файла); 2) При необходимости и наличии технической возможности – проведение

	отладки объекта в изолированной виртуальной среде, с доступом или без доступа к интернету (по согласованию с Заказчиком). 9.7. Выделение идентификаторов компрометации (в случае обнаружения вредоносного функционала): 1) Структурирование собранной информации и выделение следующих возможных групп идентификаторов, которые могут быть обнаружены в системе, зараженной исследуемым объектом: имена мьютексов, файлов, ключей реестра, процессов, IP-адреса, доменные имена, учетные данные, имена и пароли пользователей, создаваемых вредоносным ПО. 9.8. Характеристика функционала исследуемого объекта: 1) Классификация объекта по его возможностям распространения и выполняемым функциям (например: троян, червь, вирус, бэкдор, загрузчик и другие.). В случае выявления вредоносного функционала это описывается, либо указывается на его отсутствие, если исследование не подтвердило его наличие. 9.9. Подготовка рекомендаций для нейтрализации объекта: 1) Формирование рекомендаций для обнаружения заражения объектом, его нейтрализации и восстановления систем (рабочих станций, серверов или другого оборудования), если объект содержит вредоносный функционал. Если вредоносный функционал не выявлен, это также указывается. 10. Технические требования к межсетевому экрану Количество устройств – 1 шт. Функционал Next Generation Firewall (NGFW); Контроль приложений и фильтрация веб-трафика (Application Control & URL Filtering); Решение должно обеспечивать функционал Системы предотвращения вторжений (IPS); Система IPS должна обеспечивать обнаружение угроз на основе следующих механизмов: Сигнатурный анализ для выявления известных атак и эксплойтов; Отслеживание и анализ аномалий протоколов для выявления нестандартного или вредоносного трафика; Управление приложениями для контроля и блокировки нежелательной активности приложений; Обнаружение на основе анализа поведения для выявления ранее неизвестных атак и аномального поведения. Антивирусная защита (Antivirus) с возможностью проактивного обнаружения угроз; Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам, а также обнаруживать и блокировать входящие вредоносные файлы; Защита от ботов и вредоносных программ (Anti-Bot); Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи, а также иметь механизмы, применяющие интеллектуальную аналитику для автоматической защиты от атак в протоколе DNS, включая механизмы защиты от DGA; Защита электронной почты от спама (Anti-Spam) с использованием интеллектуального анализа; Функционал песочницы (sandbox) для анализа файлов и выявления угроз нулевого дня с возможностью эмуляции выполнения в изолированной среде; Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа трафика и состояния приложений для отслеживания и управления сетевыми потоками; Решение должно поддерживать работу DHCP

	в режимах сервера и ретранслятора (relay); Решение должно поддерживать возможность работы в режиме Transparent (Bridge); Решение должно поддерживать политику, основанную на белом списке MAC адресов для ограничения доступа к локальной сети; Решение должно поддерживать политику, основанную на механизмах QoS; Решение должно обеспечивать возможность гарантирования или ограничения пропускной способности, а также управления задержкой для определённого IP-источника, IP-назначения или сервиса; Решение должно поддерживать настройку правил QoS для VPN-трафика, включая возможность гибкого определения параметров приоритезации, ограничения или гарантирования пропускной способности; Решение должно обеспечивать функционал интегрированной системы предотвращения вторжений (IPS) для защиты веб-приложений от вредоносного кода и атак. Система должна обеспечивать блокировку сетевых червей, атак переполнения буфера, SQL-инъекций, инъекций команд, межсайтового скриптинга (XSS), а также поддерживать настраиваемый модуль блокировки HTTP-червей. Дополнительно система должна обеспечивать защиту от обхода каталогов (Directory Traversal), вредоносных или некорректных HTTP-заголовков (Header Rejection), а также от вредоносного HTTP-кода; Решение должно поддерживать протокол HTTP/3 over QUIC; Решение должно обеспечивать функционал Песочницы (Sandboxing) (инспекция в облаке или на выделенном локальном устройстве) при наличии лицензии; Решение должно обеспечивать функционал Идентификации и контроля пользователей; Должно обеспечивать возможность получения идентификаторов пользователей путем анализа событий безопасности Microsoft Active Directory; Должно поддерживать аутентификацию пользователей по идентификатору с использованием браузера, предназначенную для устройств и пользователей, не являющихся частью домена; Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности; Встроенная поддержка VPN (Site-to-Site VPN, Remote Access VPN); Аутентификация пользователей через Active Directory, RADIUS, LDAP; Поддержка аутентификации пользователей по IP/MAC-адресу с гибкими правилами безопасности; Поддержка современных криптографических алгоритмов шифрования и аутентификации, соответствующих требованиям законодательства Республики Казахстан в области защиты информации; Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20; Решение должно поддерживать использование как встроенного центра сертификации (CA), так и внешних сторонних центров сертификации; Решение должно поддерживать как минимум следующие механизмы обеспечения целостности данных с использованием алгоритмов: MD5, SHA-1 SHA-256, SHA-512 и AES-XCBC; Поддержка ролевого управления доступом (RBAC) для эффективного разграничения полномочий; Решение

	должно обеспечивать поддержку двухфакторной аутентификации как через интеграцию с внешними системами двухфакторной аутентификации, так и посредством встроенного механизма двухфакторной аутентификации, предоставляемого производителем; Возможность настройки политик безопасности с разделением по пользователям, группам, IP-адресам, приложениям, категориям приложений и другим параметрам; Возможность активации политик по расписанию, включая временные ограничения и условия доступа; Автоматическая генерация отчетов о нарушениях политик безопасности; База данных управления приложениями должна содержать свыше 10000 известных приложений; Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов; Встроенная система двухфакторной аутентификации без сторонних интеграций; Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL; Решение должно обеспечивать функционал «песочницы» Sandboxing (инспекция – в облаке или на выделенном локальном устройстве). Сетевые функции и отказоустойчивость Поддержка SD-WAN для интеллектуального управления трафиком с учетом приоритизации нагрузки; Поддержка управления полосой пропускания (Traffic Shaping) для балансировки нагрузки; Интеграция с внешними системами телеметрии и мониторинга уязвимостей; Поддержка маршрутизации: OSPFv2, BGPv4, RIP, PIM (SM, DM, SSM), IGMP; Поддержка IPv6, dual-stack туннелирование IPv4 поверх IPv6; Кластеризация в режиме Active/Passive с автоматическим переключением в случае отказа; Централизованное управление через облачный портал; Возможность детальной визуализации сетевых соединений и анализ аномального поведения пользователей. Производительность Пропускная способность NGFW: не менее 1,2 Gbps; Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачный Sandbox): не менее 750 Mbps; Пропускная способность IPS: не менее 1,7 Gbps; Пропускная способность Firewall: не менее 2,2 Gbps; Пропускная способность VPN AES-128: не менее 1,4 Gbps; Скорость установки новых соединений: не менее 16 000 соединений/сек; Максимальное количество одновременных соединений: не менее 1 000 000; Возможность расширенного мониторинга нагрузки на процессор и сетевые интерфейсы; Поддержка/подписка производителя предоставляется на 12 месяцев и исчисляется с даты активации лицензии/ввода в эксплуатацию, подтверждаемой актом. Гарантийный срок 12 месяцев исчисляется с даты подписания акта ввода (приемки) оборудования/ПО. Гарантийные обязательства/поддержка в части поставленного оборудования/ПО не прекращаются с окончанием срока оказания услуг и действуют в течение гарантийного периода. Аппаратные характеристики WAN-порт: не менее 1x 10/100/1000Base-T RJ-45; LAN-порты: не менее 6x 10/100/1000Base-T RJ-45; Консольный порт: не менее 1x USB-C; USB-порт: не менее 2x USB 3.0; Диапазон рабочих температур: от 0°C до

	40°C; Дополнительные требования Поддержка управления через мобильное приложение; Возможность централизованного управления политиками; Поддержка быстрого развертывания (Zero Touch Deployment); Поддержка отчетности и ведения логов в режиме реального времени; Возможность управления несколькими шлюзами безопасности через единый интерфейс; Поддержка сертификаций безопасности: CB 62368-1, UL 62368-1, FCC IC Class B, CE, VCCI, RoHS, REACH, WEEE; Оборудование, программное обеспечение и лицензии, указанные в настоящей Технической спецификации, поставляются Поставщиком исключительно в целях обеспечения оказания услуг ОЦИБ и не являются самостоятельным предметом закупки. Стоимость указанных элементов включается в стоимость услуг и отдельно не тарифицируется. 11. Требования к программному обеспечению класса EDR Требования к лицензии на средства защиты информации EDR. Программное обеспечение должно быть включено в реестр доверенного программного обеспечения и продукции электронной промышленности, в соответствии с приказом Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 2 июня2026 года № 279/НҚ. Общие (системные) требования: 11.1.Требования к архитектуре 11.1.1Централизованная архитектура: - Система развернута в едином центре обработки данных. - Обработка всех данных и управление выполняется централизованно. 11.1.2.Отказоустойчивость и резервное копирование: - Поддержка резервного копирования данных и автоматического восстановления. - Настройка узлов для обеспечения высокой доступности. 11.1.3.Безопасность данных: - Шифрование данных в движении (TLS 1.2/1.3) и в состоянии покоя. - Управление доступом на основе ролей (RBAC). 11.1.4.Производительность и нагрузка: - Обработка большого объема телеметрии в режиме реального времени. - Минимальные требования к инфраструктуре: процессор от 4 ядер, 16 ГБ ОЗУ, SSD-диски. 11.1.5.Интеграция и совместимость: - Поддержка стандартных интерфейсов API (REST, JSON). - Интеграция с SIEM, SOAR и другими инструментами кибербезопасности. 11.1.6.Мониторинг и управление: - Централизованное управление через веб-консоль. - Мониторинг состояния системы в режиме реального времени. - Поддержка журналирования и ведения отчетов. - Поддержка языков аналитических запросов и механизмов поиска, обеспечивающих фильтрацию, корреляцию и анализ событий информационной безопасности в журналах событий. Дополнительные требования - Возможность работы системы в on-premise, публичных облаках и гибридном исполнении. - Масштабируемая поисковая платформа с открытой схемой данных, поддерживающая локальное и мультиоблачное размещение. - Функциональные требования могут быть реализованы как в рамках одного решения, так и посредством интеграции нескольких решений при условии выполнения всех требований настоящей ТС. - Возможность управления модулями интеграции со сторонними решениями и подключения пакетов интеграции через консоль. - Наличие интеллектуальных механизмов автоматизации

	анализа и приоритизации инцидентов (при наличии у поставщика), не являющихся обязательным условием соответствия ТС. - Назначение политик на группы конечных устройств. - Поддержка ролевого доступа и аудита действий операторов консоли. - Консоль должна поддерживать совместную работу аналитиков над инцидентами, включая делегирование и изменение статусов. - Управление конечными точками без VPN для защиты систем за пределами корпоративного периметра. - Наличие предустановленных и настраиваемых дашбордов для анализа событий. - Масштабируемая визуализация связей запущенных процессов. - Поддержка неограниченного числа администраторов. - Обмен данными между консолью управления и модулями через TLS 1.2. - Продукт отечественного производства, либо иного производства, имеющий действующую лицензию правообладателя на использование заказчиком на территории Республики Казахстан и соответствовать требованиям законодательства Республики Казахстан в области информационной безопасности (подпункт 2 пункта 3 статьи 61 ЗРК о Кибербезопасности). - Оборудование, программное обеспечение и лицензии, указанные в настоящей Технической спецификации, поставляются Поставщиком исключительно в целях обеспечения оказания услуг ОЦИБ и не являются самостоятельным предметом закупки. Стоимость указанных элементов включается в стоимость услуг и отдельно не тарифицируется. Функциональные требования 11.2. Поддержка операционных систем 11.2.1.Рабочие станции: -Windows: Windows 10, Windows 11 (x64). -macOS: Версии от macOS 11 Big Sur и выше. -Linux: Ubuntu 18.04 LTS и выше, Debian 10 и выше. 11.2.2.Серверы: -Windows Server 2016, 2019, 2022. -Linux: Red Hat Enterprise Linux 8, CentOS 7.9-2009 и выше. 11.2.3.Мобильные устройства: -Android: Версии от Android 9.0 и выше. - iOS: Версии от iOS 13 и выше. 11.2.4.Виртуальные среды: -Поддержка виртуализации на VMware, Hyper-V, KVM. 11.3. Типы сканирований 11.3.1.Сканирование при доступе (On-access): -Автоматическое сканирование файлов при их создании, открытии, изменении или выполнении. 11.3.2.Сканирование по требованию (On-demand): -Запуск сканирования вручную через интерфейс агента. 11.3.3.Сканирование съемных носителей: -Проверка подключенных USB-устройств, внешних жестких дисков и других съемных носителей. 11.3.4.Плановое сканирование: -Настраиваемые задания сканирования по расписанию (ежедневное, еженедельное, ежемесячное). 11.3.5.Сканирование оперативной памяти: -Проверка процессов и данных в оперативной памяти на наличие признаков вредоносного ПО. 11.3.6.Глубокое сканирование системы: - сканирование всей файловой системы с детальным анализом содержимого. 11.4. Сканируемые форматы архивов 11.4.1.Поддерживаемые форматы архивов: -7zip, ace, arj, bzip2, cab, gz, gzip, jar, rar, tar, tgz, xz, zip, zipx. 11.4.2.Особенности сканирования: - Распаковка вложенных архивов. -Поддержка многотомных архивов. - Сканирование на наличие вредоносного содержимого внутри всех поддерживаемых форматов. Сканируемые сетевые протоколы Поддерживаемые протоколы: -HTTP,

	HTTPS -FTP, FTPS -IMAP, IMAPS -SMTP, SMTPS -POP3, POP3S -DNS Особенности сканирования: -Анализ входящего и исходящего трафика. -Обнаружение вредоносных элементов в протоколах передачи данных. -Инспекция зашифрованного трафика с поддержкой TLS. Сканируемые сетевые ресурсы Поддерживаемые ресурсы: SMB (Windows Shares), NFS (Network File System), WebDAV Особенности сканирования: -Анализ содержимого сетевых ресурсов на наличие угроз. -Проверка доступа и изменений файлов. -Обнаружение несанкционированного доступа. Требования к обеспечению целостности и доступности информации Локальное хранение данных: Антивирусный агент должен иметь локальное хранилище отчетов с возможностью просмотра через графический интерфейс. -Должна быть поддержка экспорта отчетов в файл для дальнейшего анализа. Карантин: Возможность перемещения обнаруженных вредоносных файлов в локальное хранилище (карантин) с последующим восстановлением при необходимости. Действия при обнаружении угроз: -Завершение процессов. -Удаление файлов. -Игнорирование ложных срабатываний на основе пользовательских правил. Анализ поведения: -Возможность анализа поведения процессов для выявления вредоносной активности. -Обнаружение попыток эксплуатации уязвимостей. Защита от вмешательства: -Защита от остановки процессов и удаления файлов антивирусного агента. -Возможность установки пароля для защиты настроек от несанкционированного изменения. Обновление антивирусных компонентов: -Обновление через интернет, локальный сервер или сетевой каталог. -Автоматическое обновление сигнатур и базы угроз. 11.5. Требования к обеспечению целостности и доступности компонента 11.5.1.Защита от несанкционированного вмешательства: -Защита процессов агента от остановки или удаления. -Блокировка изменений настроек без авторизации. -Настройка прав доступа через административную консоль. 11.5.2.Механизмы самовосстановления: -Автоматический перезапуск критических служб при сбоях. -Контроль целостности файловых систем и конфигураций компонентов. 11.5.3.Контроль доступа и аутентификация: -Журналирование всех изменений конфигурации системы. 11.5.4.Мониторинг работоспособности: -Непрерывный мониторинг состояния системы с оповещениями. -Отчеты о статусе компонентов в режиме реального времени. 11.5.5.Обновления и исправления: -Регулярные обновления и исправления безопасности. -Обновление баз сигнатур и политик безопасности через защищенные каналы связи. 11.6. Источники обновления компонентов антивируса и набора сигнатур 11.6.1.Удаленные источники: -Сервер производителя, доступные через интернет (HTTPS). - Облачное хранилище. 11.6.2.Автоматизация обновлений: -Настраиваемый график автоматических обновлений. -Поддержка ручного запуска обновлений через веб-консоль. 11.6.3.Защищенная передача данных: -Использование TLS для безопасной передачи обновлений. -Проверка цифровых подписей компонентов перед установкой. Возможности централизованного управления Централизованная установка и обновление: -Установка, обновление и удаление компонентов

	системы с центральной консоли. -Управление политиками безопасности на всех конечных точках. Мониторинг и контроль: -Централизованный мониторинг работы системы в режиме реального времени. -Просмотр журналов событий и истории обновлений. Управление конфигурацией: -Настройка параметров системы с применением групповых политик. -Управление правами доступа пользователей и ролями. Реагирование на инциденты: -Отправка команд на изоляцию устройств. -Блокировка процессов, файлов и сетевых подключений. -Выполнение удаленных команд на конечных точках. Отчеты и уведомления: -Генерация детализированных отчетов о безопасности. -Настраиваемые уведомления об инцидентах безопасности и обновлениях системы. Интеграция с внешними системами: -Интеграция с SIEM, SOAR и другими системами безопасности. -API для взаимодействия с другими ИТ-решениями. 11.7. Реагирование на инциденты 11.7.1.Действия по реагированию на инциденты: -Завершить процесс; -Удалить файл; -Загрузить файл с рабочей станции на компьютер аналитика или в хранилище ПК; -Выполнить команду операционной системы с системными привилегиями; -Получить автоматически запускаемые объекты/скрипты; -Блокировка исполняемых файлов (хэш, имя файла); -Функционал создания Playbook для реагирования на инциденты. Интеграция с другими системами 11.7.2.Интеграция с SIEM-системами: - Поддержка интеграции с промышленными SIEM-системами посредством стандартных протоколов и интерфейсов обмена данными (API, syslog, REST, webhook и иные). -Передача данных об инцидентах и обнаруженных угрозах в реальном времени. 11.7.3.Интеграция с SOAR: -Поддержка автоматизации процессов реагирования через платформы SOAR (например, IBM Resilient, ServiceNow). 11.7.4.Интеграция с системами управления уязвимостями: -Обмен данными с системами сканирования уязвимостей (например, Tenable, Qualys). 11.7.5.Интеграция с системой управления доступом: -Интеграция с LDAP, Active Directory для управления учетными записями. -Поддержка SSO через SAML. 11.7.6.API и веб-хуки: -REST API для получения данных о событиях, угрозах и инцидентах. -Веб-хуки для передачи данных в системы оповещения. 11.7.7.Облачные интеграции: -Поддержка облачных сервисов Amazon AWS, Microsoft Azure, Google Cloud. -Встроенные интеграции для управления облачными ресурсами и защиты данных. 11.7.8.Техническая интеграция: -Интеграция с почтовыми системами для анализа подозрительных писем (SMTP/IMAP). -Поддержка форматов отчетов STIX/TAXII для обмена данными о киберугрозах. 11.8. Техническая поддержка Требования к персональному техническому менеджеру Поставщик выделяет персонального технического менеджера, который: 11.8.1. Занимается обработкой запросов заказчика. 11.8.2. Организовывает работы по технической поддержке. 11.8.3. Информирует заказчика о текущем состоянии решения запросов. 11.8.4. Доступен в рабочие дни по телефону и электронной почте с понедельника по пятницу с 9.00 часов до 18.00 часов по времени Астаны. Требования ко времени реакции технической поддержки Техническая поддержка

	должна быть доступна в круглосуточном режиме включая выходные и праздничные дни посредством интернет-портала и (или) телефона и (или) электронной почты. Время реагирования: - Критичный уровень – не более 30 минут - Высокий уровень – не более 4 рабочих часов - Средний уровень – не более 6 рабочих часов - Низкий уровень – не более 8 рабочих часов «Критический уровень»- вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес-процессы. «Высокий уровень»- продукт полностью выведен из строя, но непрерывность основных бизнес процессов не нарушается. «Средний уровень» - продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение пользователя не выведено из строя в результате работы продукта. «Низкий уровень» - означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности. Типы запросов в техническую поддержку - Консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта. -Консультации по лечению файлов, зараженных вредоносными программами; - Осуществление приоритетного выпуска набора антивирусных сигнатур, в том числе: - детектирование отдельных вредоносов из предоставленного набора, по мере готовности сигнатур для каждого из вредоносов такого набора; - детектирование набора вредоносов в одно время, после готовности сигнатур для всего этого набора. - Консультации у квалифицированных специалистов производителя антивирусного программного обеспечения (вирусных аналитиков, специалистов по компьютерной криминалистике и реагированию на инциденты), по вопросам исследования вредоносного кода, компьютерной криминалистике и реагированию на компьютерные инциденты, по мере необходимости, но не более 50 часов в течение года; Требования к обновлению программного обеспечения - Периодичность обновления набора антивирусных сигнатур – не реже одного раза в неделю. - Периодичность обновления агентов “ПК антивирусной защиты с централизованным управлением” и “ПК обнаружения и централизованного реагирования на инциденты информационной безопасности с компонентом Sandbox” – не реже одного раза в квартал. - Поставщик должен обеспечить выпуск исправлений (патчей) для программного обеспечения компонентов по запросу заказчика, в котором описывается обнаруженная уязвимость. Требования к обеспечению отказоустойчивости оборудования Поставщик должен иметь запасные части, инструменты, принадлежности и материалы для серверного оборудования компонентов и, в случае выхода из строя оборудования, восстановить их стабильное функционирование в соответствии с уровнем критичности. Требования к хранению и обработке данных: - Полная телеметрия с хранением на срок до 7 дней. - Шифрование всех данных и метаданных по защищенному каналу связи по протоколу TLS. Требования к поставке Поставка оборудования и программного обеспечения осуществляется единовременно, но не ранее истечения минимального срока, установленного

	пунктом 569 Правил осуществления государственных закупок. Требования к проверке работоспособности: Осуществление поставки для проверки работоспособности и комплектности товара, согласно условиям договора, на территории Заказчика. Проверка работоспособности осуществляется путем активаций и пробного подключения, визуального осмотра на отсутствие повреждений, дефектов, трещин, коррозии. 12. Требования к архитектурным принципам и классификации решений в области информационной безопасности 1. Принцип соответствия классу решений Каждое функциональное требование к информационной безопасности (ИБ) должно быть реализовано решением, которое соответствует отдельному, четко определенному классу решений, установленному архитектурой и методологией ИБ. 2. Функциональные требования могут быть реализованы как в рамках одного решения, так и посредством интеграции нескольких решений при условии выполнения всех требований настоящей ТС. 3. Критерий самостоятельности Каждое внедряемое решение обязано выполнять самостоятельную и независимую функцию обеспечения информационной безопасности.
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, в случае определения его победителем и заключения договора о государственных закупках, обязан предоставить: Письма (сертификаты) правообладателя (производителя) или его официального представителя, подтверждающие право Поставщика на поставку (предоставление) продуктов, предусмотренных технической спецификацией, представляются в течение 10 (десяти) рабочих дней со дня вступления договора в силу. Дополнительно Поставщик представляет: 1. Таблицу соответствия требований технической спецификации характеристикам предлагаемых продуктов (решений), составленную Поставщиком. 2. Подтверждение от вендора о том, что данный продукт сертифицирован и/или поддерживается в актуальной версии для использования соответствующего программного обеспечения.