Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Еңбек ресурстарын дамыту орталығы" акционерлік қоғамы
Ұйымдастырушының атауы:	"Еңбек ресурстарын дамыту орталығы" акционерлік қоғамы
Конкурстың №:	№ 17953220-1
Конкурстың атауы:	TrendAI техникалық қолдау лицензиясын ұзарту қызметі
Лоттың нөмірі:	№ 83199070-ОК2
Лоттың атауы	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620920.000.000027
Қызметтің атауы:	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	63883077.59
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	63883077.59
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	Техникалық ерекшелікке сәйкес
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	TrendAI техникалық қолдау лицензиясын ұзарту қызметіне арналған ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК . Кепілдік мерзімі (айлар) - 2027 жылғы желтоқсанның 31-не дейін. Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы TrendAI техникалық қолдау лицензиясын ұзарту қызметі (бұдан әрі – TrendAI БҚ). Лицензияның сипаттамасы Жылдық лицензия TrendAI БҚ жаңартуларын алуға және техникалық қолдау көрсетуге құқық береді. Өнім беруші Шарт жасалған күннен бастап күнтізбелік 15 күннен кешіктірмей, ұсынылатын TrendAI БҚ лицензиясының осы техникалық ерекшелікте талап етілетін техникалық сипаттамаларына сәйкес келетін, өндірушінің ресми интернет-ресурсындағы веб-беттерге немесе техникалық құжаттарға тікелей сілтемелері бар ресми хат ұсынуы тиіс. TrendAI БҚ өндірушісі лицензияны Тапсырыс берушінің атына Шарт жасалған күннен бастап күнтізбелік 15 күннен кешіктірмей ұсынуы тиіс. Қолданыстағы TrendAI БҚ-ны толықтыру үшін жылдық лицензия «Мемлекеттік сатып алу туралы» Заңның 12-бабы 4-тармағының 2) тармақшасына сәйкес ұзартылуы тиіс. Лицензияның құрамына мыналар кіруі тиіс: 1) TrendAI Apex One On-premises – кемінде 350 дана, лицензияны 2027 жылғы 1 қаңтардан бастап 2027 жылғы 31 желтоқсанға дейін ұзарту; 2) TrendAI Apex One Endpoint Sensor (on-premises) – кемінде 350 дана. Лицензияға қатерлерді анықтау жөніндегі мынадай функциялар кіруі тиіс: машиналық оқыту; мінез-құлықты талдау (зиянды скрипттерден, зиянды кодты енгізуден, бопсалаушы бағдарламалардан, браузерлерге және жадқа жасалатын шабуылдардан қорғау); файлдардың беделін анықтау; нұсқаларды анықтау; таралу жиілігін тексеру; веб-сайттардың беделін анықтау; эксплойттарды пайдаланудың алдын алу (тораптың желілік экран, эксплойттардан қорғау); командалық серверлерді бұғаттау; деректердің сыртқа таралуының алдын алу; сыртқы құрылғыларды бақылау; сенімді файлдар базасы бойынша тексеру; «құмсалғышты» қатерлерді анықтау жүйесімен интеграциялау; қатерлерді анықтау және оқыс оқиғаларға ден қою; осалдықтардан қорғау. Лицензияны 2027 жылғы 1 қаңтардан бастап 2027 жылғы 31 желтоқсанға дейін ұзарту; 3) TrendAI Deep Discovery Email Inspector – Advanced Threat and Gateway Modules SW – кемінде 270 дана, лицензияны 2027 жылғы 1 қаңтардан бастап 2027 жылғы 31 желтоқсанға дейін ұзарту; 4) TrendAI Deep Security – Enterprise per server or cloud workload – кемінде 250 дана, лицензияны 2027 жылғы 1 қаңтардан бастап 2027 жылғы 31 желтоқсанға дейін ұзарту. Лицензиялар Шартқа қол қойылған күннен бастап күнтізбелік 15 күннен кешіктірілмей ұсынылуы тиіс және олардың қолданылу мерзімі 2027 жылғы 31 желтоқсанға дейін болуы тиіс. Басқару жүйесіне қойылатын талаптар Серверлік бөлік - Басқару жүйесі веб-консоль түрінде іске асырылуы, браузерлердің барлық өзекті нұсқаларын қолдауы және әкімшілік міндеттерді орындау үшін қосымша компоненттерді талап етпеуі тиіс; - Басқару жүйесін Windows операциялық жүйесімен жұмыс істейтін

	серверлерге (2012/2012 R2, 2016 – 64 бит, 2019 – 64 бит және одан жоғары) орнату мүмкіндігі болуы тиіс; - Басқару жүйесін Linux операциялық жүйесімен жұмыс істейтін серверлерге (RHEL 7, 8, 9 – барлығы 64 бит және одан жоғары) орнату мүмкіндігі болуы тиіс; - Басқару сервері 30 000-ға дейін қорғалатын торапты қолдауы тиіс; - Басқару жүйесінің барлық деректері сыртқы дерекқорда сақталуы тиіс; - Дерекқор ретінде Microsoft SQL (2014, 2016, 2017, 2019, 2022, RDS нұсқалары) қолдауы тиіс; - Дерекқор ретінде Oracle (19c, 23c нұсқалары) қолдауы тиіс; - Дерекқор ретінде PostgreSQL (11, 12, 13, 14 нұсқалары) қолдауы тиіс; - Басқару веб-консолімен жұмыс қорғалған қосылым (SSL) арқылы жүзеге асырылуы тиіс; - Басқару сервері мен дерекқор арасындағы байланыс қорғалған қосылым арқылы жүзеге асырылуы тиіс; - Басқару серверін дерекқорға қосу домендік аутентификацияны қолдауы тиіс; - Басқару серверінде барлық қосалқы компоненттерді (агенттерді, олардың бинарлық жаңартуларын және т.б.) жергілікті сақтау мүмкіндігі болуы тиіс; - Басқару сервері жаңа жүйелерге орнатуға қажетті қосымша компоненттерді жаңартулардың жаһандық орталығынан жүктей алуы тиіс; - Басқару сервері Windows платформаларында агенттерді автоматты түрде орналастыруға арналған арнайы скрипттерді жасауды қолдауы тиіс; - Басқару сервері Linux платформаларында агенттерді автоматты түрде орналастыруға арналған арнайы скрипттерді жасауды қолдауы тиіс; - Басқару сервері Solaris платформаларында агенттерді автоматты түрде орналастыруға арналған арнайы скрипттерді жасауды қолдауы тиіс; - Басқару сервері VMware vCenter жүйесімен (6.0 және одан жоғары нұсқалар) тікелей интеграцияны қолдауы тиіс; - Басқару сервері бірнеше VMware vCenter жүйесімен жұмыс істеуді қолдауы тиіс; - VMware vCenter жүйесімен жұмыс істеген кезде инфрақұрылымдағы барлық өзгерістер нақты уақытқа барынша жақын режимде бақылануы тиіс; - Басқару сервері VMware NSX жүйесімен (6.3 және одан жоғары нұсқалар) тікелей интеграцияны қолдауы тиіс; - Агентсіз режимде барлық қорғау функцияларын (антивирустық қорғау, желілік қорғау, тұтастықты бақылау) іске асыру үшін бір ғана виртуалды құрылғы пайдаланылуы тиіс; - VMware NSX Standard (тегін нұсқасы) қолданылған кезде жүйеде біріктірілген қорғауды (агентсіз және агенттер арқылы) іске асыруға арналған кіріктірілген логика болуы тиіс; - Жүйе vSphere Distributed Switch (vDS) жұмысын қолдауы тиіс; - Басқару жүйесі рөлдердің икемді моделін (RBAC) қолдауы және жұмыс аймақтары мен оларға берілетін құқықтарды егжей-тегжейлі баптау мүмкіндігін қамтамасыз етуі тиіс; - Басқару жүйесі құқықтарды делегирлеу режимін қолдауы тиіс; - Басқару жүйесі онымен жұмыс істеу кезінде орындалатын барлық әрекеттерді бақылап, тіркеуі және әр әрекет бойынша толық мәліметтерді сақтауы тиіс (мысалы, саясатқа кім және қашан өзгеріс енгізгені, содан кейін бизнес-сервистің жұмысында проблемалардың туындауы); - Басқару жүйесінде электрондық пошта арқылы қатерлер мен оқыс оқиғалар туралы хабарлау құралдары болуы тиіс; - Басқару жүйесінде

	SIEM жүйелеріне қатерлер мен оқыс оқиғалар туралы хабарламалар жіберуге арналған кіріктірілген құралдар болуы және мынадай форматтарды қолдауы тиіс: raw syslog, CEF, LEEF; - Жүйе қорғаудың әрбір модулі бойынша оқыс оқиғаларды SIEM оқиғаларды корреляциялау жүйелеріне жіберуді жеке баптауды қолдауы тиіс; - Басқару жүйесінде SAML 2.0 негізінде бөгде сәйкестендіру жүйелерімен интеграция көзделуі тиіс; - Басқару жүйесі компьютерлер туралы деректерді синхрондау үшін LDAP-пен жұмысты қолдауы тиіс; - Басқару жүйесі домендік пайдаланушыларға жүйеге қол жеткізу мүмкіндігін беру үшін LDAP-пен жұмысты қолдауы тиіс; - LDAP-пен жұмыс қорғалған режимде (LDAPS, Start TLS) жүзеге асырылуы тиіс; - Басқару жүйесінде бөгде жүйелермен интеграциялауға арналған ашық API болуы тиіс; - Жаңартулар жүйесі жаңартуларды тарату көздерінің иерархиясын қолдауы тиіс; - Басқару жүйесі желілік экран модулі үшін ашық порттарды тексеруді іске қосу мүмкіндігін қамтамасыз етуі тиіс; - Басқару жүйесі қорғалатын жүйелерді толық және жылдам антивирустық тексеруді қолмен іске қосу мүмкіндігін қамтамасыз етуі тиіс; - Басқару жүйесі агентті қолмен қалпына келтіруді (саясаттарды өшіру, басқару жүйесінен байланысты ажырату) қолдауы тиіс; - Басқару жүйесінде қорғалатын жүйелерді белгілердің (шарттардың) кең ауқымы бойынша еркін топтарға біріктіру құралдары болуы тиіс; - Жүйе шарттар мен оқиғалардың кеңейтілген тізбесі негізінде нысаналы жүйелерге сәйкес қорғау ережелерінің жиынтығын автоматты түрде қолдана алуы тиіс (компьютердің инфрақұрылымда пайда болуы, компьютердің бір хосттан екіншісіне ауысуы, компьютердің қосылуы, компьютердің IP-мекенжайының өзгеруі). Резиденттік қорғау модульдері (агенттер) - Агент функционалдық модульдерсіз, барынша жеңілдетілген ядро түрінде таратылуы тиіс; - Агент қосылған қорғау функциялары мен саясаттар негізінде функционалдық модульдерді серверден жүктей алуы тиіс; - Агент сервермен екіжақты режимде де (сервер де, агент те қосылымды бастай алады), сондай-ақ біржақты режимде де (қосылымды тек сервер немесе тек агент бастай алады) деректер алмаса алуы тиіс; - Агент графикалық интерфейсті толық жасыру арқылы жұмыс істей алуы тиіс; - Агент пәрмен жолы арқылы басқаруды қолдауы тиіс; - Агентте тек пәрмен жолы арқылы, оның ішінде парольді пайдалана отырып, ажыратылатын кіріктірілген өзін-өзі қорғау тетіктері болуы тиіс; - Агентті басқару серверімен бастапқы байланыстырмай орнату мүмкіндігі болуы тиіс (оны виртуалды серверлер мен орнату бейнелерінің стандартты үлгілеріне қосу үшін); - Агентті пәрмен жолы құралдарының көмегімен басқару серверіне байланыстыру мүмкіндігі болуы тиіс; - Агентті пәрмен жолы құралдарының көмегімен апаттық қалпына келтіру мүмкіндігі болуы тиіс. Қолдау көрсетілетін платформалар (агент) – Windows - Windows Server 2012/Windows Server 2012 R2; - Windows Server 2016; - Windows Server 2019 және одан жоғары. Қолдау көрсетілетін платформалар (агент) – Linux - Red Hat Enterprise Linux 7 және одан жоғары; - CentOS 7 және одан жоғары; - Oracle Linux 7

	және одан жоғары; - Ubuntu 18.04 және одан жоғары; - Debian 11 және одан жоғары. Торап деңгейіндегі желілік экран - L2 деңгейінде жұмыс істеуді қолдауы тиіс; - Тақырыптармен және фреймдермен жұмыс істеуді қолдауы тиіс; - Агенттер негізінде жұмыс істеуді қолдауы тиіс; - VMware ортасында агентсіз режимде жұмыс істеуді қолдауы тиіс; - Алдын ала орнатылған ережелер болуы тиіс; - Барлауды анықтау функциясын қолдауы, порттар диапазонын көрсету мүмкіндігімен порттарды сканерлеуді жүзеге асыруы тиіс; - Барлауды анықтау үшін OS Fingerprint функциясын қолдауы тиіс; - Қалыптан тыс TCP белсенділігін (null scan, SYN FIN scan, Xmax scan) анықтауды қолдауы тиіс; - Дереккөздер бойынша ерекшеліктер жасау мүмкіндігімен барлауды анықтауды қолдауы тиіс; - Интерфейстерді оқшаулауды баптау мүмкіндігі болуы тиіс; - Stateful inspection функциясын қолдауы тиіс; - Желілік экранның кесте бойынша жұмыс істеу мүмкіндігі болуы тиіс; - Тергеу жүргізу үшін пакеттер туралы деректерді жинау мүмкіндігі болуы тиіс; - Желілік ортаның контекстін ескере отырып жұмыс істеуі тиіс; - Желілік қозғалтқыштың жұмыс режимін: bypass (fail open) немесе бұғаттау (fail close) ретінде таңдау мүмкіндігі болуы тиіс; - Желілік қозғалтқыштың inline немесе tap режимінде (тестілік міндеттер үшін) жұмыс істеуін таңдау мүмкіндігі болуы тиіс; - TCP, UDP, ICMP қосылымдарының ең көп санын көрсету мүмкіндігі болуы тиіс; - Желілік сессиялар мен аномалиялардың әртүрлі күйлері үшін (SYN_SENT, CLOSED, CLOSING, ACK STORM, ESTABLISHED және басқалары) күту уақытын белгілеу мүмкіндігі болуы тиіс; - SRC және DST үшін IP-мекенжайлары бірдей қосылымдарды бұғаттауы тиіс; - Null IP үшін тыйымды баптау мүмкіндігі болуы тиіс; - TCP қосылымын «үнсіз» үзу мүмкіндігі болуы тиіс; - Cisco WAAS үшін bypass режимі болуы тиіс; - Қайталанатын немесе қабаттасатын деректері бар пакеттер (evasive retransmit) үшін қосылымды үзу параметрлерін баптау мүмкіндігі болуы тиіс; - TCP Checksum тексеру мүмкіндігі болуы тиіс; - Пакет фрагменттері үшін (fragment offset & size) ең төменгі мәндерді баптау мүмкіндігі болуы тиіс; - SSL сессиялары үшін (time & size) ең төменгі мәндерді баптау мүмкіндігі болуы тиіс; - SSL трафигіндегі белгісіз протоколды үзу мүмкіндігі болуы тиіс; - Туннельдерді (IPv4, IPv6) сүзу мүмкіндігі болуы тиіс; - Хостқа қатысы жоқ MAC-мекенжайлар үшін bypass режимін қолдану мүмкіндігі болуы тиіс. Торап деңгейінде басып кірудің алдын алу - Windows, Linux, Solaris операциялық жүйелеріндегі осалдықтардан (нақты осалдықтар мен эксплойттерге сілтеме жасай отырып) қорғауы тиіс; бұл «виртуалды патчинг» деп аталады; - Қолданбалы бағдарламалық қамтылымның осалдықтарынан (нақты осалдықтар мен эксплойттерге байланысты) қорғауы тиіс; бұл «виртуалды патчинг» деп аталады; - Осалдықтарды анықтау және олардың алдын алу ережелерінде нәтижелерді салыстыру үшін осалдықтардың жаһандық дереккорларына сілтемелер болуы тиіс (мысалы, Mitre, Microsoft); - Желілік деңгейде қолданбаларды бұғаттау (network application control) мүмкіндігі болуы тиіс; -

	Шешім құрамында параметрлерді баптау мүмкіндігі бар WAF санатындағы қорғау тетіктері (XSS, SQL инъекцияларынан қорғау) болуы тиіс; - Агенттер негізінде жұмыс істеуді қолдауы тиіс; - VMware ортасында агентсіз режимде жұмыс істеуді қолдауы тиіс (SSL трафигін ашу мүмкіндігінсіз); - HIPS модулінің тұтас деңгейінде жұмыс режимін (алдын алу немесе анықтау) таңдау мүмкіндігі болуы тиіс; - HIPS модулінің жеке ережелері деңгейінде жұмыс режимін (басып кірудің алдын алу немесе анықтау) таңдау мүмкіндігі болуы тиіс; - Қорғалатын жүйелерді автоматты және қолмен тексеру (аудит) арқылы операциялық жүйелер мен қолданбалардағы әлсіз тұстар мен осалдықтарды анықтау, кейіннен тиісті HIPS ережелерін іске қосу (немесе оларды пайдалану жөнінде ұсынымдар беру) мүмкіндігі болуы тиіс; - Осалдықтарды автоматты іздеу нәтижесінде алынған ережелерді тиісті қорғалатын жүйелерге немесе олардың саясаттарына автоматты түрде байланыстыру/ажырату мүмкіндігі болуы тиіс; - Басып кіруді анықтау/болдырмау ережелерінің жиынтығын оңтайландыру үшін тапсырмаларды жоспарлаушы арқылы осалдықтарды автоматты іздеу жүзеге асырылуы тиіс: өндірушілердің нақты патчтарымен жойылған осалдықтарға арналған ережелерді өшіру; өндірушілердің патчтарымен әлі жабылмаған жаңа осалдықтарға қатысты өзекті ережелерді қосу. Тұтастықты бақылау - Агент арқылы (Windows, Linux, Solaris, HP-UX, AIX) тұтастықты бақылау мүмкіндігі болуы тиіс; - VMware-мен интеграциялау арқылы агентсіз режимде тұтастықты бақылау мүмкіндігі болуы тиіс (тек Windows үшін және тек файлдар/қалталар бойынша); - VMware ортасында агентсіз режимде файлдарды тексеруді қайталауды болдырмау үшін кэштеуді пайдаланатын агентсіз құралдар қолданылуы тиіс; - Кэштің жарамдылық мерзімін және агентсіз тексеруге арналған ерекшеліктерді баптау мүмкіндігі болуы тиіс; - Файлдар мен қалталардың тұтастығын бақылау тетіктері болуы тиіс; - Тізілім кілттерінің тұтастығын бақылау тетіктері болуы тиіс; - Қызметтердің тұтастығын бақылау тетіктері болуы тиіс; - Порттардың тұтастығын бақылау тетіктері болуы тиіс; - Өзгерістерді нақты уақыт режимінде бақылау мүмкіндігі болуы тиіс; - Өзгерістерді heartbeat режимінде бақылау мүмкіндігі болуы тиіс; - Өзгерістерді қолмен бақылау мүмкіндігі болуы тиіс; - Сенімді өзгерістер жиынтығын қалыптастыру үшін эталондық дереккөздерді (жергілікті компьютерлер, «ақ тізімдегі» қолданбалардың жаһандық дерекқорлары) пайдалану мүмкіндігі болуы тиіс; - Хеш түрін (SHA-1 немесе SHA-256) таңдау мүмкіндігі болуы тиіс; - Бақыланатын нысандардың атрибуттарын таңдау мүмкіндігі болуы тиіс; - Тұтастықты бақылаудың тиісті ережелерін таңдау және кейіннен оларды іске қосу (немесе қосу жөнінде ұсынымдар беру) үшін қорғалатын жүйелерді автоматты және қолмен тексеру (аудит) мүмкіндігі болуы тиіс; - Автоматты іздеу нәтижесінде алынған ережелерді тиісті қорғалатын жүйелерге немесе олардың саясаттарына автоматты түрде байланыстыру/ажырату мүмкіндігі болуы тиіс. Оқиғаларды бақылау - Агент (Windows, Linux, Solaris, HP-UX, AIX) арқылы журнал деректерін алу

	және қалыпқа келтіру модулінің жұмыс істеу мүмкіндігі болуы тиіс; - Жүйелердің стандартты түрлеріне (event log, snort, syslog және басқалары) арналған журнал деректерін алу және қалыпқа келтіру тетіктері болуы тиіс; - Журнал деректерін алу және қалыпқа келтіру модулінің ережелері OSSEC синтаксисіне негізделуі тиіс; - Деректер декодерлерінің дайын жиынтығымен (regex) жұмыс істеу мүмкіндігі болуы тиіс; - Деректер декодерлерінің (regex) жеке жиынтығын жасау мүмкіндігі болуы тиіс; - Жеңілдетілген жолдық мәндер немесе regex құралдары арқылы ережелер жасау мүмкіндігі болуы тиіс; - Журнал деректерін алу және қалыпқа келтіру модулінің тиісті ережелерін таңдау және кейіннен оларды іске қосу (немесе қосу жөнінде ұсынымдар беру) үшін қорғалатын жүйелерді автоматты және қолмен тексеру (аудит) мүмкіндігі болуы тиіс; - Автоматты іздеу нәтижесінде алынған ережелерді тиісті қорғалатын жүйелерге немесе олардың саясаттарына автоматты түрде байланыстыру/ажырату мүмкіндігі болуы тиіс. Қолданбаларды бақылау - Windows және Linux жүйелерінде агент арқылы қолданбаларды бақылау модулінің жұмыс істеу мүмкіндігі болуы тиіс; - «Ақ тізім» режимінде жұмыс істеуі тиіс («ақ тізімге» кірмейтін барлық қолданбаларды іске қосуға тыйым салу); - Таңдамалы тыйым салу режимін қолдауы тиіс; - Жүйелер мен қолданбаларды жаңартуға байланысты нысандарды іске қосуға және орнатуға рұқсат беретін технологиялық «терезелерді» шектеусіз немесе белгілі бір уақыт кезеңіне қолдауы тиіс; - Қолданбаларды бақылау модулінің оқиғалар журналынан қолданбаларды іске қосуға тыйым салу немесе рұқсат беру мүмкіндігі болуы тиіс. Өндірушінің жаһандық порталы техникалық қолдау лицензиясының қолданылу мерзімі ішінде TrendAI БҚ өндірушісі шығарған TrendAI БҚ жаңартулары мен түзетулерін алуға мүмкіндік беруі тиіс. Өндірушінің жаһандық порталы техникалық қолдау мерзімі ішінде бағдарламалық қамтылымда пайдаланылатын барлық қажетті сигнатура жаңартуларын алу үшін TrendAI БҚ сервисіне қолжетімділікті қамтамасыз етуі тиіс. Лицензияға қойылатын қосымша міндетті талаптар - Лицензияны тексеру оны басқару консолінде белсендіру арқылы жүзеге асырылады. Кепілдік мерзімі және техникалық қолдау талаптары - Бағдарламалық қамтылымды пайдалану кезінде туындайтын мәселелерді шешу үшін жаһандық техникалық қолдау қызметіне жүгіну, сондай-ақ пайдаланушы мен әкімші нұсқаулықтарында сипатталмаған техникалық мәселелерді шешу кезінде жаһандық техникалық қолдау қызметінен консультациялар мен көмек алу мүмкіндігі болуы тиіс. Өнім беруші Тапсырыс берушінің өтініштерін электрондық өтініштер порталы (бар болған жағдайда), телефон немесе электрондық пошта арқылы 2027 жылғы 31 желтоқсанға дейін жұмыс күндері сағат 09:00-ден 18:30-ға дейін (дүйсенбіден жұмаға дейін, демалыс және мереке күндерін қоспағанда) қабылдап, жергілікті техникалық қолдау көрсетуі тиіс. Өнім берушіге қойылатын талаптар Жеткізілетін лицензиялардың көлемі TrendAI БҚ өндірушісінің ресми порталында көрсетілуі тиіс. Өнім беруші лицензияларды ұзартуды, баптауды және енгізуді осы

	техникалық ерекшелікке сәйкес толық көлемде орындауы тиіс. TrendAI БҚ лицензиясын белсендіруді Өнім берушінің қызметкерлері жүзеге асыруы тиіс. Қызмет көрсету орны: Астана қаласы, Сығанақ даңғылы, 70, «Сығанақ» бизнес-орталығы, 601-кабинет. Ақпаратты қорғау құралдары мен Тапсырыс берушінің ақпараттандыру объектілерін TrendAI БҚ-мен интеграциялауға арналған дайын қосымша болмаған жағдайда, TrendAI БҚ-ны интеграциялау жұмыстарын Өнім беруші жергілікті техникалық қолдаудың бүкіл қолданылу мерзімі ішінде жүзеге асырады. TrendAI БҚ-ға жергілікті техникалық қолдау көрсету мерзімі ішінде Өнім беруші TrendAI БҚ-ны ақпаратты қорғаудың жаңа құралдарымен және Тапсырыс берушінің басқа да ақпараттандыру объектілерімен (қосымшаларымен) интеграциялау жұмыстарын жүргізеді. Техникалық қолдаудың сипаттамасы - TrendAI БҚ бойынша өндірушінің техникалық қолдауы өндірушінің порталында электрондық түрде қамтамасыз етілуі тиіс; - Өндірушінің техникалық қолдау мерзімі лицензия белсендірілген күннен бастап 2027 жылғы 31 желтоқсанға дейін болуы тиіс. Өндірушінің техникалық қолдауы Тапсырыс берушінің уақыт белдеуін ескере отырып, 24х7 режимінде көрсетілуі тиіс. Жергілікті техникалық қолдау мыналарды қамтуы тиіс: - GMT+0500 уақыт белдеуі бойынша жұмыс күндері сағат 08:30-дан 18:00-ге дейін техникалық қолдау қызметтерін көрсету; - Тапсырыс беруші өтінім берген сәттен бастап (қолдау көрсетілетін уақыт аралығында) жауап беру уақыты 1 (бір) сағаттан аспауы тиіс; - Өтініштер саны шектелмеуі тиіс; - Электрондық пошта арқылы қолдау көрсету; - Телефон арқылы қолдау көрсету; - Өтініштерді эскалациялау; - TrendAI БҚ әзірлеушісінің білім базасына қол жеткізу; - Пайдаланылатын бағдарламалық қамтылымды жаңарту, оның ішінде сыни қателерді түзету (патчтар), жоспарлы жаңартулар (сервистік релиздер) және жаңа нұсқаға дейін жаңарту.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	Өнім беруші Шарт жасалған күннен бастап күнтізбелік 15 күннен кешіктірмей TrendAI ұсынылатын лицензиясының осы техникалық ерекшелікте талап етілетін техникалық сипаттамаларға сәйкес келетін өндірушінің ресми Интернет-ресурсынан веб-беттерге немесе техникалық құжаттарға тікелей сілтемелерді қамтитын ресми хатты ұсынуы тиіс. Өнім беруші өзі ұсынатын барлық лицензия ҚР немесе Орталық Азия аумағындағы ресми өкілден авторизацияланған хатты ұсына отырып, TrendAI БҚ өндірушісінің ресми дистрибьюторы (дилері) арқылы немесе өндірушіден сатып алынатынын растайды. Өнім беруші Шартқа қол қойылған күннен бастап 5 күнтізбелік күн ішінде техникалық қолдау үшін байланыс деректерін ұсынуы тиіс. Өнім беруші Шартқа қол қойғаннан кейін келісім жасалған күннен бастап 15 күнтізбеліктен кешіктірмей лицензияны енгізуді орындайтын және техникалық қолдау көрсететін TrendAI БҚ-мен жұмыс істеуге сертификатталған маманның деректерін ұсынуы тиіс.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Центр развития трудовых ресурсов"
Наименование организатора	Акционерное общество "Центр развития трудовых ресурсов"
№ конкурса:	№ 17953220-1
Наименование конкурса:	Услуга продления лицензии технической поддержки TrendAI
Номер лота:	№ 83199070-ОК2
Наименование лота:	Услуги по технической поддержке лицензионного программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620920.000.000027
Наименование услуги:	Услуги по технической поддержке лицензионного программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	63883077.59
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	63883077.59
Срок оказания услуги:	Согласно технической спецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ на услугу продления лицензии технической поддержки TrendAI. Гарантийный срок (в месяцах) - До 31 декабря 2027 года. Услуга продления лицензии технической поддержки TrendAI (далее – ПО TrendAI). Описание лицензии Годовая лицензия дает право на получение обновлений и техническую поддержку ПО TrendAI. Поставщик должен предоставить официальное письмо, в котором содержатся прямые ссылки на веб-страницы или технические документы с официального Интернет-ресурса производителя, соответствующим требуемыми настоящей технической спецификацией техническими характеристиками предлагаемой лицензии ПО TrendAI, не позднее 15 календарных дней с момента заключения Договора. Предоставление лицензии от производителя ПО TrendAI на имя Заказчика не позднее 15 календарных дней со дня заключения Договора. Годовая лицензия должна быть продлена согласно подпункту 2) пункта 4 статьи 12 Закона «О государственных закупках» для доукомплектования действующего ПО TrendAI. Компоненты лицензии должны включать в себя следующее: 1) TrendAI Apex One On-premises - не менее 350 шт., продление лицензии с 01 января 2027 года до 31 декабря 2027 года; 2) TrendAI Apex One Endpoint Sensor (on-premises) - не менее 350 шт. В лицензию должны входить следующие функции по обнаружению угроз: машинное обучение; поведенческий анализ (против вредоносных скриптов, внедрений вредоносного кода, программ-вымогателей, атак на браузеры и в памяти); репутация файлов; обнаружение вариантов; проверка распространенности; репутация веб-сайтов; предотвращение использования эксплойтов (МСЭ узла, защита от эксплойтов); блокировка командных серверов; предотвращение утечки данных; контроль внешних устройств; проверка по базе хороших файлов; интеграция «песочницы» с системой обнаружения угроз; обнаружение угроз и реагирование на инциденты; защита от уязвимостей; продление лицензии с 01 января 2027 года до 31 декабря 2027 года. 3) TrendAI Deep Discovery Email Inspector - Advanced Threat and Gateway Modules SW - не менее 270 шт., продление лицензии с 01 января 2027 года до 31 декабря 2027 года; 4) TrendAI Deep Security - Enterprise per server or cloud workload - не менее 250 шт., продление лицензии с 01 января 2027 года до 31 декабря 2027 года; Предоставить лицензии не позднее 15 календарных дней со дня подписания Договора со сроком действия до 31 декабря 2027 года. Требования к системе управления Серверная часть - Система управления должна быть реализована в виде веб-консоли, поддерживать все актуальные версии браузеров и не требовать дополнительных компонентов для осуществления административных задач; - Система управления может быть установлена на серверах под управлением Windows (2012/2012 R2, 2016 64 бита, 2019 64 бита и выше); - Система управления может быть установлена на серверах под управлением Linux (RHEL 7, 8, 9 - все 64 бита и выше); - Сервер управления должен поддерживать до 30000 защищаемых узлов; - Хранение всех данных системы управления осуществляется во внешней БД; -

	Поддержка Microsoft SQL в качестве БД (версии 2014, 2016, 2017, 2019, 2022, RDS); - Поддержка Oracle в качестве БД (версии 19c, 23c); - Поддержка PostgreSQL в качестве БД (версии 11, 12, 13, 14); - Работа с веб-консолью управления осуществляется по защищённому соединению (SSL); - Связь сервера управления с БД осуществляется по защищённому соединению; - Подключение сервера управления к БД должно поддерживать доменную аутентификацию. - Сервер управления должен иметь возможность локального хранения всех вспомогательных компонентов (агенты, их бинарные обновления и т.д.). - Сервер управления должен иметь возможность загрузки дополнительных компонентов, необходимых для установки на новые системы, из глобального центра обновлений. - Сервер управления должен иметь поддержку генерации специальных скриптов для автоматического разворачивания агентов под платформы Windows. - Сервер управления должен иметь поддержку генерации специальных скриптов для автоматического разворачивания агентов под платформы Linux. - Сервер управления должен иметь поддержку генерации специальных скриптов для автоматического разворачивания агентов под платформы Solaris. - Сервер управления должен поддерживать прямую интеграцию с системой VMware vCenter (с версии 6.0 и выше). - Сервер управления должен поддерживать работу с более, чем одним VMware vCenter. - При работе с VMware vCenter отслеживание всех изменений в инфраструктуре должно происходить в режиме, близком к реальному времени - Сервер управления должен поддерживать прямую интеграцию с системой VMware NSX (версии 6.3 или выше). - Работа в безагентном режиме должна обеспечиватся только одним виртуальным устройством для реализации всех защитных функций (антивирусная защита, сетевая защита, контроль целостности). - При работе с VMware NSX Standard (бесплатной версией), система должна иметь встроенную логику для комбинированной защиты (безагентно и с помощью агентов). - Система должна поддерживать работу с vSphere Distributed Switch (vDS). - Система управления должна поддерживать гибкую ролевую модель (RBAC) с возможностью детальной настройки областей и прав работы с ними. - Система управления должна поддерживать режим делегирования прав. - Система управления должна отслеживать и фиксировать все действия при работе с ней, а также сохранять подробные сведения по каждому из них (например, кто и когда внёс изменения в политики, после чего возникли проблемы с работой бизнес-сервиса). - Система управления должна иметь встроенные средства оповещения об угрозах и инцидентах через почту. - Система управления должна иметь встроенные средства оповещения об угрозах и инцидентах в SIEM системы с поддержкой следующих типов форматов: raw syslog, CEF, LEEF. – Система должна поддерживать отдельную настройку передачи инцидентов в системы корреляции событий (SIEM) для каждого модуля защиты в отдельности. – В системе управления должна быть предусмотрена интеграция со сторонними системами идентификации на основе SAML 2.0. - Система управления

	должна поддерживать работу с LDAP для синхронизации данных по компьютерам. - Система управления должна поддерживать работу с LDAP для обеспечения доступа доменных пользователей к системе. - Работа с LDAP должна работать в защищённом режиме (LDAPS, Start TLS). - Система управления должна иметь открытый API для интеграции со сторонними системами. - Система обновлений должна поддерживать иерархию для источников распространения обновлений. – Система управления должна иметь возможности запуска проверки открытых портов для модуля МСЭ. - Система управления должна иметь возможности ручного запуска полной и быстрой антивирусной проверки защищаемых систем. - Система управления должна иметь возможности ручного сброса агента (отключение политик, отвязывание от системы управления). - Система управления должна иметь инструменты для объединения защищаемых систем в произвольные группы по широкому набору признаков (условий). - Система должна иметь возможность автоматического применения релевантных целевым системам наборов правил защиты на основе расширенного списка условий и событий (компьютер появилась в инфраструктуре, компьютер переместилась с хоста на хост, компьютер включилась, у компьютера произошла смена IP). Модули резидентной защиты (агенты) - Агент должен распространяться в виде максимально облегченного ядра (без функциональных модулей). - Агент должен иметь возможность подгрузки функциональных модулей с сервера на основе включённых защитных функций и политик. - Агент должен иметь возможность обмена данными с сервером как в двустороннем режиме (как сервер, так и агент могут инициировать соединение), так и в одностороннем режиме (только сервер, или только агент может инициировать соединение). - Агент должен иметь возможности работы с полным сокрытием графической части. - Агент должен поддерживать управление из командной строки. - Агент должен иметь встроенные механизмы самозащиты, отключаемые только из командной строки (включая пароль). - Агент должен иметь возможность установки без первичной привязки к серверу управления (для включения его в стандартные шаблоны виртуальных серверов и установочных образов). - Агент должен иметь возможности привязки к серверу управления с помощью инструментов командной строки. - Агент должен иметь возможности аварийного сброса с помощью инструментов командной строки. Поддерживаемые платформы (агент) - Windows - Windows Server 2012/Windows Server 2012 R2; - Windows Server 2016; - Windows Server 2019 и выше; Поддерживаемые платформы (агент) - Linux - Red Hat Enterprise Linux 7 и выше; - CentOS 7 и выше; - Oracle Linux 7 и выше; - Ubuntu 18.04 и выше; - Debian 11 и выше; Межсетевой экран уровня узла - Поддержка работы на L2. - Поддержка работы с заголовками и фреймами. - Поддержка работы на базе агентов. – Поддержка работы в безагентном режиме (VMware). - Наличие предустановленных правил. - Поддержка обнаружения разведки - сканирование портов с возможностью указания диапазона. - Поддержка обнаружения разведки - OS

	Fingerprint. - Поддержка обнаружения разведки - аномальные TCP активности (null scan, SYN FIN scan, Xmax scan). - Поддержка обнаружения разведки - возможность создания исключений по источникам. - Возможность настройки изоляции интерфейсов. - Поддержка stateful inspection. - Возможность работы МСЭ по расписанию. - Возможность сбора данных пакета для расследования - Работа с поддержкой контекста (сетевое окружение). - Возможность выбора работы сетевого движка - bypass (fail open) или блокировка (fail close). - Возможность выбора работы сетевого движка - inline или tap (для тестовых задач). - Возможность указания максимального числа соединений (TCP, UDP, ICMP). - Возможность задать таймауты для различных состояний сетевых сессий и аномалий (SYN_SENT, CLOSED, CLOSING, ACK STORM, ESTABLISHED и других). – Блокировка соединений с идентичными IP для SRC и DST. - Возможность настройки запрета для Null IP. - Возможность "тихого" сброса TCP соединения. - Режим bypass для Cisco WAAS. - Возможности настройки сброса соединения для пакетов с дублирующимися или перекрывающимися данными (evasive retransmit). - Возможности проверки TCP Checksum. - Возможности настройки минимальных значений для фрагментов пакета (fragment offset & size). – Возможности настройки минимальных значений для SSL сессий (time & size). - Возможности сброса неизвестного протокола для SSL трафика. - Возможности фильтрации туннелей (IPv4, IPv6). - Возможность bypass для MAC адресов, не относящихся к хосту. Предотвращение вторжений уровня узла - Защита от уязвимостей в ОС Windows, Linux, Solaris (с привязкой к конкретным уязвимостям и эксплойтам) - т.н. "виртуальный патчинг". - Защита от уязвимостей прикладного ПО (с привязкой к конкретным уязвимостям и эксплойтам) - т.н. "виртуальный патчинг". - Правила обнаружения и предотвращения уязвимостей должны иметь ссылки на глобальные базы по уязвимостям для сопоставления результатов (например, Mitre, Microsoft). - Возможность блокировки прикладных приложений на сетевом уровне (network application control). - Наличие механизмов защиты класса WAF в составе решения (защита от XSS, SQL injections) с возможностью настройки параметров. - Поддержка работы на базе агентов. - Поддержка работы в безагентном режиме (VMware; без возможности вскрытия SSL). - Возможность выбора режимов работы (предотвращение или обнаружение) на уровне модуля HIPS целиком. - Возможность выбора режимов работы (предотвращение или обнаружение вторжений) на уровне отдельных правил модуля HIPS. - Возможности проверки (аудита) защищаемых систем в автоматическом и ручном режимах для выявления слабых мест и уязвимостей в приложениях и ОС с возможностью последующей активации соответствующих правил HIPS (или выдачи рекомендаций по их использованию) для устранения найденных проблем. - Возможность автоматической привязки/отключения правил, полученных в результате автоматического поиска уязвимостей, к целевым защищаемым системам или политикам для них. - Работа автоматического поиска

	уязвимостей через планировщика задач для оптимизации набора правил обнаружения/предотвращения вторжений (отключение правил для уязвимостей, уже закрытых реальными патчами от производителей систем и приложений; включение актуальных правил под новые найденные уязвимости, ещё не закрытые реальными патчами от производителей). Контроль целостности - Возможность работы контроля целостности с помощью агента (Windows, Linux, Solaris, HP-UX, AIX). - Возможность работы контроля целостности в безагентном режиме через интеграцию с VMware (только Windows и только для файлов/папок). - Использование безагентных средств для дедубликации проверки файлов в безагентном режиме (кэширование в среде Vmware). – Настройки срока жизни кеша и исключения для безагентной проверки. - Наличие механизмов мониторинга целостности файлов и папок. - Наличие механизмов мониторинга целостности ключей реестра. - Наличие механизмов мониторинга целостности служб. - Наличие механизмов мониторинга целостности портов. - Возможность отслеживания изменений в режиме реального времени. - Возможность отслеживания изменений в режиме heartbeat. – Возможность отслеживания изменений в ручном режиме. - Использование эталонных источников для формирования набора доверенных изменений (локальные компьтеры, глобальные базы "белых приложений"). - Возможность выбора типа хеша (SHA-1 или SHA-256) - Возможность выбора атрибутов для контроля сущностей. - Возможности проверки (аудита) защищаемых систем в автоматическом и ручном режимах для подбора релевантных правил контроля целостности и возможностью последующей активации этих правил (или выдачи рекомендаций по их включению). - Возможность автоматической привязки/отключения правил, полученных в результате автоматического поиска, к целевым защищаемым системам или политикам для них. Контроль событий - Возможность работы модуля извлечения и нормализации данных журналов с помощью агента (Windows, Linux, Solaris, HP-UX, AIX). - Механизмы работы модуля извлечения и нормализации данных журналов для стандартных типов систем (eventlog, snort, syslog и другие). - Работа правил модуля извлечения и нормализации данных журналов на основе синтаксиса OSSEC. - Возможность работы с готовым набором декодеров данных (regex). - Возможность создания своего набора декодеров данных (regex). - Возможность создания правил через упрощённые строковые значения или средствами regex. - Возможности проверки (аудита) защищаемых систем в автоматическом и ручном режимах для подбора релевантных правил модуля извлечения и нормализации данных журналов и возможностью последующей активации этих правил (или выдачи рекомендаций по их включению). - Возможность автоматической привязки/отключения правил, полученных в результате автоматического поиска, к целевым защищаемым системам или политикам для них. Контроль приложений - Возможность работы модуля контроля приложений с помощью агента (Windows, Linux). - Режим работы в режиме "белого списка" (запрет запуска всех приложений, не входящих в "белый"

	список). - Режим работы в режиме избирательного запрета. - Поддержка технологических "окон" (разрешение на запуск и установку объектов, связанных с обновлением систем и приложений) - бессрочно или на ограниченный период времени. - Возможность запрета или разрешения запуска из журнала событий модуля контроля приложений. Глобальный портал производителя должен предоставлять возможность получения обновлений и исправлений ПО TrendAI, выпускаемые производителем ПО TrendAI, в течение срока действия лицензии на техническую поддержку; Глобальный портал производителя должен обеспечивать доступ к сервису ПО TrendAI для получения всех необходимых обновлений сигнатур, используемых в программном обеспечении на протяжении срока действия технической поддержки. Дополнительные обязательные требования к лицензии - Проверка лицензии будет осуществляться путём активации её на консоли управления. Гарантийный срок и требования к технической поддержке - Должна быть возможность обращения в глобальную техническую поддержку для решения проблем, связанных с эксплуатацией программного обеспечения, а также получать у глобальной службы технической поддержки консультации и помощь при решении технических проблем, не описанных в руководствах пользователя и администратора; Поставщик должен оказывать локальную техническую поддержку с 9.00 до 18.30 в рабочие дни (с понедельника по пятницу за исключением выходных и праздничных дней) путем принятия обращений от Заказчика через электронный портал обращений (при наличии) или по телефону, или по электронной почте до 31 декабря 2027 года. Требование к поставщику Объем поставляемых лицензий должен отображаться на официальном портале производителя ПО TrendAI. Поставщик должен выполнить продление лицензий, настройку и внедрение в соответствии с настоящей технической спецификации в полном объеме. Активацию лицензии на ПО TrendAI должны производить работники поставщика. Место оказания услуги: г. Астана, пр. Сығанақ, 70, БЦ «Сығанақ», каб. 601. В случае отсутствия готового приложения по интеграции средствами защиты информации и объектами информатизации Заказчика в ПО TrendAI, работы по интеграции ПО TrendAI осуществляются Поставщиком в течение всего периода действия локальной технической поддержки. В течение срока действия локальной технической поддержки ПО TrendAI, Поставщик осуществляет работы по интеграции ПО TrendAI с новыми средствами защиты информации и другими объектами информатизации Заказчика (приложениями). Описание технической поддержки - Техническая поддержка от производителя на ПО TrendAI должна обеспечиваться в электронной форме на портале производителя. - Срок технической поддержки от производителя должен составлять до 31 декабря 2027 года со дня активации лицензии. Техническая поддержка от производителя должна осуществляться в режиме 24х7 учитывая часовой пояс Заказчика. Локальная техническая поддер 200жка должна включать в себя: - Оказание услуг технической поддержки в рабочие дни с 08:30 до 18:00 (GMT +0500). - Время

	реагирования не более 1-го (одного) часа (в период часового покрытия) с момента подачи заявки Заказчиком. - Не ограниченное количество обращений. - Поддержку по электронной почте. - Поддержку по телефону. - Эскалацию обращений. - Доступ к базе знаний разработчика ПО TrendAI. Обновление используемого программного обеспечения, (такие как исправление критических ошибок (патчи), плановое обновление (сервисные релизы) и обновление до новой версии.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	Поставщик должен предоставить официальное письмо, в котором содержатся прямые ссылки на веб-страницы или технические документы с официального Интернет-ресурса производителя, соответствующим требуемыми настоящей технической спецификацией техническими характеристиками предлагаемой лицензии ПО TrendAI, не позднее 15 календарных дней со дня заключения Договора. Поставщик подтверждает, что вся предлагаемая им лицензия будет закуплена через официального дистрибьютера (дилера) производителя ПО TrendAI или от производителя, предоставив авторизованное письмо от официального представителя на территории РК или Центральной Азии. Поставщик должен предоставить контактные данные для технической поддержки в течение 5 календарных дней со дня подписания Договора. Поставщик после подписания Договора должен предоставить данные специалиста, сертифицированного на работу с ПО TrendAI, который будет выполнять активацию лицензии и техническую поддержку не позднее 15 календарных дней со дня заключения договора.