Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті" коммерциялық емес акционерлік қоғамы
Ұйымдастырушының атауы:	"Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті" коммерциялық емес акционерлік қоғамы
Конкурстың №:	№ 17990001-1
Конкурстың атауы:	Антивирустық қорғау жүйесінің лицензиялары сатып алу (533)
Лоттың нөмірі:	№ 88469315-ОК2
Лоттың атауы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	582950.000.000001
Қызметтің атауы:	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	11460517
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	11460517
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	шарт жасасқан күннен бастап 16 күнтізбелік күндер ішінде
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12
Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Техникалық ерекшелік Оқиғаларды тергеу модулі бар антивирустық қорғау (бұдан әрі – «АЗ») 2600 құрылғыға (соңғы нүктеге) арналған, техникалық қолдау көрсетіле отырып жеткізіледі, жазылым мерзімі лицензия іске қосылған сәттен бастап кемінде 1 жыл болуы тиіс. Жеткізілетін АЗ пайдалану құқығына арналған лицензия кейінге қалдырылған белсендіру мүмкіндігін қолдауы тиіс. Лицензияны белсендіру өндірушіден жөнелту фактісі бойынша автоматты түрде жүргізілмеуі немесе алдын ала белгіленген күнге байланыстырылмауы тиіс. Лицензия өнім берушіден жөнелтілген сәттен бастап 2 (екі) ай ішінде кез келген күні белсендіру мүмкіндігін қамтамасыз етуі тиіс. Бағдарламалық қамтамасыз етуді енгізу және баптау кезеңінде өнім беруші енгізуді аяқтауға жеткілікті мерзімге (Тапсырыс берушімен келісу бойынша) жеткізілетін АЗ-ның толық функционалы бар уақытша лицензияларды ұсынуға міндетті. БҚ өнім беруші мен өндіруші тарапынан техникалық қолдаумен қамтамасыз етілуі тиіс. Техникалық қолдау көрсету нысаны – қашықтан (онлайн, қашықтан консультациялар, телефон, электрондық пошта, мамандандырылған портал). БҚ-ны қолдау мерзімі – 12 ай. Антивирустық қорғау (бұдан әрі – «АЗ») орнатылатын, барлық кіріктірілген қорғау модульдері бір виртуалды құрылғыға біріктірілген, қосымша бөгде бағдарламалық қамтамасыз етуді орнатуды болдырмайтын немесе бұлтта қолжетімді болатын виртуалды құрылғы түрінде жеткізілетін, бірыңғай басқару консолі бар масштабталатын шешім болуы тиіс. Бұл кез келген түрдегі және кез келген жерде орналасқан соңғы нүктелердің кез келген саны үшін қауіпсіздік саясатын орналастырудың, сақтаудың және басқарудың бірыңғай нүктесін қамтамасыз етуі тиіс. Масштабталуды қамтамасыз ету мақсатында шешімде дерекқор қызметтері, байланыс қызметтері, жаңарту қызметтері және веб-қызметтер үшін бөлінген компоненттер болуы тиіс. Жергілікті түрде орнатылатын АЗ бірыңғай бапталған виртуалды құрылғы (виртуалды образ) ретінде жеткізілуі тиіс. Қолдау көрсетілетін виртуалдандыру платформалары VMware, Microsoft, Red Hat, ядроға негізделген виртуалды машина немесе KVM, Oracle VM, Nutanix болуы тиіс. Виртуалды құрылғы негізгі виртуалдандыру платформаларымен үйлесімді бірнеше нұсқада (OVA, XVA, VHD, OVF, RAW) қолжетімді болуы тиіс. АЗ бірнеше виртуалды құрылғыны және нақты рөлдердің көптеген даналарын пайдалануға баптауды қолдауы, сенімділік пен масштабталуды қамтамасыз ету үшін кіріктірілген жүктемені теңгергіші болуы тиіс. Неғұрлым қауіпсіз ортаны қамтамасыз ету үшін АЗ бірнеше виртуалды құрылғы арасында қауіпсіз арна арқылы байланыс орнатуға арналған VPN-кластерін құруды қолдауы тиіс. АЗ Әкімші есептік жазбасын қосымша қорғауды қамтамасыз ету үшін екі факторлы аутентификацияны қолдауы тиіс. АЗ бірыңғай басқару нүктесі – веб-консоль арқылы басқарылуы тиіс. Вебконсоль виртуалды немесе физикалық компьютерлер мен серверлерді қорғайтын барлық қауіпсіздік модульдерін басқаруға, жалпы қауіпсіздікке және жаһандық қауіпсіздік қатерлерін бақылауға оңай қол жеткізуді қамтамасыз етуі тиіс. АЗ

	зиянды бағдарламалардан қорғаудың қолданыстағы шешімін қашықтан орналастыру және жою, қашықтан сканерлеу тапсырмаларын баптау және іске қосу мүмкіндіктеріне ие болуы тиіс. Веб-консоль басқарылмайтын жұмыс үстелі компьютерлеріне, серверлерге арналған қорғауды жеңілдету және автоматты түрде қолдану мақсатында қолданыстағы басқару жүйелерімен және мониторинг жүйелерімен біріктірілуі тиіс. Атап айтқанда, Microsoft Active Directory, VMware vCenter, Citrix XenServer, VMware Tanzu, Veeam Backup & Replication жүйелерінде пайда болатын және желіде анықталған құрылғыларды қамтуы тиіс. Веб-сервер орталық басқару консолінен лицензияланған сертификаттау орталығы немесе өз ұйымы берген цифрлық сертификаттарды импорттауға мүмкіндік беруі тиіс. Сертификаттарды импорттау түсінікті болуы және орталық басқару консолінен орындалуы тиіс. Шешім орталық консольде сертификаттар туралы мынадай ақпаратты көрсету мүмкіндігіне ие болуы тиіс: атауы, берілген орталығы, шығарылған күні және берілген сертификаттардың қолданылу мерзімінің аяқталу күні. АЗ соңғы нүктелер үшін қауіпсіздіктің бірнеше деңгейін қамтамасыз етуі тиіс: мінез-құлықты мониторингтеу арқылы зиянды бағдарламалардан қорғау, нөлдік күн қатерлерінен қорғау, қосымшалардың қара тізімдерін жасау және ықтимал қауіпті объектілерді шектеулі ортада оқшаулау, желіаралық экран, құрылғыларды басқару, контентті басқару, фишингтен қорғау. АЗ кіріктірілген жүктемені теңгергішке ие болуы тиіс. АЗ архитектурасының орталық логикасы кіріктірілген реляциялық емес дерекқорды және соңғы нүктелердің белгілі бір санынан асатын көлемде орналастыруға арналған құралды үшінші тараптың лицензиялық кілтін пайдалануды қажет етпей қолдануы тиіс. Антивирустық құралдар мынадай қауіпсіздік қызметтерін қамтуы тиіс: соңғы нүктелерді қорғау; виртуалды орталарды қорғау. АЗ пайдаланушылардың әрекеттерін сәйкестік тұрғысынан тіркеуі тиіс. АЗ пайдаланушының әрбір әрекеті бойынша толық журналдарға ие болуы тиіс. АЗ аудит журналдары бойынша күрделі іздеуді қолдауы тиіс. АЗ физикалық және виртуалды машиналар үшін бірыңғай саясат үлгісін және кез келген ортаға (физикалық немесе виртуалды) арналған бір орнатқышты пайдалануы тиіс. Сондай-ақ АЗ Linux операциялық жүйесімен басқарылатын физикалық соңғы нүктелер үшін (серверлер мен жұмыс станциялары) қолжетімді болуы тиіс. АЗ құрамына мынадай сканерлеу қозғалтқыштары кіруі тиіс. Сканерлеу қозғалтқышы орнату пакеттерін жасау кезінде автоматты түрде орнатылуы тиіс, бұл соңғы құрылғылар агенттеріне машиналардың конфигурацияларын анықтауға және сканерлеу технологияларын соған сәйкес бейімдеуге мүмкіндік береді. Сонымен қатар әкімші бірнеше сканерлеу технологиясының арасынан таңдау арқылы сканерлеу қозғалтқышын баптай алуы тиіс: 1. Жергілікті сканерлеу, бұл кезде сканерлеу соңғы құрылғының өзінде орындалады. 2. Гибридті сканерлеу (жеке бұлт) – орташа топтарға арналған, бұлттағы сканерлеуді және ішінара жергілікті сигнатураларды пайдаланады. 3. Шағын топтарға арналған жеке бұлттағы орталықтандырылған сканерлеу

	– сканерлеу жүктемесін соңғы нүктелерден мамандандырылған қауіпсіздік серверлеріне ауыстыру арқылы соңғы құрылғыларды қорғауды оңтайландыруға арналған. Сканерлеу үшін қауіпсіздік сервері қажет. Бұл жағдайда сигнатуралар жергілікті түрде сақталмайды және сканерлеу қауіпсіздік серверіне жүктеледі. АЗ құрамына мынадай қорғау модульдері кіруі тиіс: ● Зиянды бағдарламалардан қорғау Зиянды бағдарламалардан қорғау модулі сигнатуралық, эвристикалық және мінез-құлықтық талдауды пайдалана отырып, қауіптердің барлық түрлерін (вирустар, құрттар, трояндар, шпиондық және жарнамалық БҚ, кейлоггерлер, руткиттер және т.б.) көп деңгейлі анықтауды және олардың алдын алуды қамтамасыз етуі тиіс. ● Кеңейтілген қауіптерді бақылау Тіпті эвристикалық қозғалтқыштан да жасырынатын қауіптер үшін кеңейтілген қауіптерді бақылау түріндегі үшінші қорғаныс қабаты болуы тиіс. Кеңейтілген қауіптерді бақылау іске қосылған процестерді тұрақты түрде қадағалап, процестің түрін жасыру әрекеттері, процестің жад кеңістігінде кодты орындау (артықшылықтарды арттыру мақсатында жадты басып алу), репликация, файлдарды жылжыту, технологиялық процестер тізімінде жасырыну және т.б. сияқты күдікті әрекеттерді бағалауы тиіс. Әрбір күдікті әрекет процестің рейтингін арттырады. Белгіленген шекке жеткен кезде дабыл сигналы іске қосылады. Бұл модульге тек қолдау көрсетілетін Windows жұмыс үстелі және серверлік операциялық жүйелері үшін қолжетімділік болуы тиіс. ● Кеңейтілген Anti-Exploit Машиналық оқытуға негізделген Advanced Anti-Exploit технологиясы анықтау қиын эксплойттарды пайдаланатын нөлдік күн шабуылдарын бұғаттауы тиіс. Advanced Anti-Exploit нақты уақыт режимінде соңғы эксплойттарды қадағалап, қолданыстағы қауіпсіздік шешімдерін айналып өту үшін пайдаланылуы мүмкін жадтың зақымдану осалдықтарын жоюы тиіс. Технология браузерлер, Microsoft Office редакторлары, Adobe Reader және басқа да көптеген стандартты қосымшаларды қорғауы тиіс. Модуль жүйелік процестерді қадағалап, қауіпсіздік осалдықтары мен қолданыстағы процестерді ұстап алу әрекеттерінен қорғауы тиіс. ● Anti-Tampering Қауіпсіздік агентінің тұтастығына қауіп төндіру үшін пайдаланылуы мүмкін соңғы нүктедегі осал драйверлерді анықтауы тиіс. Windows және Linux операциялық жүйелерімен үйлесімді болуы тиіс. ● Post-Tampering Соңғы нүктеде қауіпсіздік агентінің кері шақыруларының зиянды түрде жойылғанын немесе ажыратылғанын, соның салдарынан тұтастықтың бұзылғанын анықтауы тиіс. Windows операциялық жүйелерімен үйлесімді болуы тиіс. ● Брандмауэр Брандмауэр қосымшалардың желіге және Интернетке қол жеткізуін бақылауы тиіс. Қол жеткізу белгілі және заңды қосымшалардың дерекқорына негізделе отырып автоматты түрде рұқсат етілуі тиіс. Сонымен қатар брандмауэр жүйені порттарды сканерлеуден қорғауы, Интернетке ортақ қол жеткізуді (ICS) пайдалануды шектеуі және жаңа түйіндер Wi-Fi арқылы қосылған кезде ескертуі тиіс. ● Желілік шабуылдардан қорғау Қатаң іріктеу әдісімен жасалатын шабуылдар, желілік «эксплойттар», парольдерді ұрлауға

	арналған бағдарламалар, жасырын жүктеу арқылы жұқтыру векторлары, боттар мен трояндар сияқты құралдарды пайдалана отырып, соңғы нүктелерге қол жеткізуді мақсат ететін желілік шабуылдарды тануға арналған қауіпсіздік деңгейі. ● Контентті бақылау Контентті бақылау модулі компанияның рұқсат етілген трафикке, веб-қолжетімділікке, деректерді қорғауға және қосымшаларды бақылауға қатысты саясатының сақталуын қамтамасыз етуі тиіс. Әкімшілер трафикті сканерлеу параметрлері мен ерекшеліктерін белгілеу, вебқолжетімділік кестесін жасау, белгілі бір веб-мекенжайларды немесе санаттарды бұғаттау немесе оларға рұқсат беру, деректерді қорғау қағидаларын баптау және нақты қосымшаларды пайдалануға рұқсаттарды белгілеу мүмкіндігіне ие болуы тиіс. ● Құрылғыларды бақылау Құрылғыларды бақылау модулі бұғаттау қағидалары мен ерекшеліктерін қолдана отырып, соңғы нүктелерге қосылатын сыртқы құрылғылар арқылы маңызды деректердің таралып кетуіне және зиянды БҚ-ның енуіне жол бермеуі тиіс. Бұл USB флэшжинақтауыштары, Bluetooth құрылғылары, CD/DVD ойнатқыштары, сақтау құрылғылары және т.б. сияқты құрылғылардың кең ауқымына арналған саясаттар арқылы жүзеге асырылуы тиіс. ● Антивирустық агент қорғанысын жергілікті өзгерту Басқару орталығының (Control Center) әкімшілері қауіпсіздік саясатының параметрлері арқылы соңғы құрылғылардың қарапайым пайдаланушыларына артықшылықты пайдаланушылар құқықтарын бере алады. Бұл модуль пайдаланушылар деңгейіне әкімшілік құқықтар беруге мүмкіндік беруі тиіс, бұл соңғы пайдаланушыларға жергілікті консольді пайдалана отырып, қауіпсіздік баптауларына қол жеткізуге және оларды өзгертуге мүмкіндік береді. ● Соңғы нүктелердің тәуекелдерін басқару (ERA) Соңғы нүктелердің тәуекелдерін басқару тәуекелдерді сканерлеу арқылы (сұрау бойынша немесе саясатта белгіленген кесте бойынша) Windows машиналарының осал тұстарын анықтауы, бағалауы және түзетуі тиіс. Бұл ретте тәуекел индикаторларының көп саны ескерілуі тиіс. Белгіленген тәуекел индикаторлары бойынша желіні алғашқы сканерлеуден кейін Әкімші тәуекелдерді басқару тақтасында желінің тәуекел жағдайына шолу алуы тиіс. Кейбір тәуекелдер басқару орталығынан автоматты түрде шешілуі тиіс, сондай-ақ әкімші соңғы нүктеге келтірілетін залалды азайту жөніндегі ұсынымдарды қарау мүмкіндігіне ие болуы тиіс. ● Ұйым активтеріне қауіп төндіру үшін шабуылдаушы жасай алатын қадамдар тізбегін визуалды түрде көрсету мақсатында бірнеше деректер көзін талдайтын және салыстыратын, болжамды шабуыл векторларының графиктерін құратын функционалдың болуы. ● Құмсалғыш (Sandbox) Құмсалғыш антивирустың антивирустық ядролары қол қоймаған күдікті файлдарды автоматты және терең талдау арқылы жаңа қауіптерден қорғаудың қуатты деңгейін қамтамасыз етуі тиіс. Құмсалғыштың қауіпсіз ортасы пайдалы жүктемелерді оқшауланған виртуалды ортада орындау, олардың мінезқұлқын талдау және файлдардың вирустық әрі зиянды сипатын көрсетуі мүмкін жүйедегі ең аз өзгерістер туралы хабарлау үшін технологиялардың кең жиынтығын пайдалануы тиіс. ● Exchange қорғау

	Exchange жүйесін зиянды бағдарламалардан қорғауды, спамнан және фишингтен қорғауды, контент пен электрондық хаттардың мазмұнын сүзгілеуді қамтамасыз етуі және хабар алмасудың қауіпсіз ортасын қамтамасыз ету әрі өнімділікті арттыру үшін Microsoft Exchange серверлерімен толық біріктірілуі тиіс. Зиянды бағдарламалар мен спамнан қорғаудың танылған технологияларын пайдалануы тиіс. Бағдарлама Exchange пайдаланушыларын ең жаңа әрі күрделі зиянды бағдарламалардан және пайдаланушылардың құпия әрі құнды деректерін ұрлау әрекеттерінен қорғауы тиіс. ● Оқиғаларды тергеу модулі Бұл оқиғаларды корреляциялау компоненті күрделі қауіптерді немесе белсенді шабуылдарды анықтауы тиіс. Корпоративтік интеграцияланған платформаның құрамында оқиғаларды тергеу модулі корпоративтік желіде жұмыс істейтін барлық құрылғылардың мүмкіндіктерін біріктіруі тиіс. Бұл компонент жедел әрекет ету топтары елеулі қауіптерді анықтап, оларға жауап берген кезде көмек көрсетуі тиіс. Соңғы нүктелер арқылы соңғы нүктені басқару жүйесінде компьютер мен операциялық жүйе деректерін біріктіру үшін қорғау модулін іске қосуға болады. Екі жақтан да метадеректерді жинау және өңдеу клиент-сервер платформасында жүзеге асырылуы тиіс. Оқиғаларды тергеу модулі анықталған оқиғалар туралы толық ақпаратты, оқиғалардың интерактивті картасын, түзету жөніндегі әрекеттерді және құмсалғышпен әрі кеңейтілген шабуылдарды анықтау модулімен интеграцияны қамтамасыз етуі тиіс. Физикалық және виртуалды соңғы құрылғылардағы антивирустық қорғау бағдарламалық құралдарына қойылатын талаптар Жұмыс станцияларын антивирустық қорғау бағдарламалық құралдары мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс: – Amazon EC2, Microsoft Azure бұлттық платформаларымен интеграциялау; – API кілттері арқылы үшінші тарап өндірушілерінің БҚ-мен интеграциялау; – А3 Microsoft серверлік рөлдері (DNS, DHCP, AD, Exchange, SharePoint) үшін кіріктірілген ерекшеліктерді ұсынуы тиіс. – Резиденттік антивирустық мониторинг; – Пайдаланушының немесе әкімшінің пәрмені бойынша антивирустық сканерлеу; – Кесте бойынша антивирустық сканерлеу; – Flesh жинақтауыштары анықталған кезде сканерлеуді іске қосу; – Соңғы нүктелер мен пайдаланушылардың тәуекелдерін сканерлеуді кесте бойынша немесе қолмен іске қосу; – Әкімші консоліндегі мәзір арқылы соңғы нүктелердегі тәуекелдерді (дұрыс бапталмаған конфигурациялар, есептік жазбаға байланысты тәуекелдер, жаңартылмаған қосымшаларға байланысты тәуекелдер және т.б.) орталықтандырылған түрде автоматты жою мүмкіндігі; – Тәуекелдерді сыни деңгейі, анықтау түрі, жағдайы бойынша сұрыптау мүмкіндігі; – Ұйымдағы инциденттер кезінде осы тәуекелдерді қадағалау үшін тәуекелдерді бақылау тізімдеріне қосу мүмкіндігі; – Ұйым тәуекелдері бойынша есептері бар оқуға ыңғайлы, бапталатын, интерактивті панельдің болуы; – Ұйымның халықаралық стандарттар талаптарына сәйкестігін бағалауға арналған, қолжетімді сәйкестік стандарттарының тізімін кеңейту мүмкіндігі бар модульдің болуы (CIS v8.0, CMMC 2.0, DORA, ISO/IEC

	27001:2022 және т.б.); – Cyber Hygiene стандартының талаптарына сәйкестігі бойынша бүкіл желілік инфрақұрылымға есептер жасау мүмкіндігі; – Эвристикалық талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау; – Қажет болған жағдайда антивирустық қорғауды ажырату функциясы; – Клиенттік жұмыс станциясынан бағдарламаны жою үшін пароль орнату функциясы; – Жасырын процестерді анықтау; – Операциялық жүйе жүктелгеннен кейін бірден және/немесе кесте бойынша тапсырмаларды іске қосу; – Антивирустық қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату функциясы; – Әкімші консолі арқылы агентті қайта орнатпай және жоймай, клиенттік машинадағы антивирустық агентті қашықтан қайта баптау, қорғау модульдерін қосу немесе ажырату мүмкіндігі; – Зиянды БҚ-ның соңғы нүктеге енуіне жол бермеу үшін электрондық поштаға келіп түсетін хабарламаларды (POP3, IMAP, MAPI) және веб-трафикті нақты уақыт режимінде тексеру және сканерлеу; – Басқа соңғы нүктелердің зиянды бағдарламалармен зақымдануын болдырмау үшін шығыс электрондық пошта хабарламаларын (SMTP, MAPI) тексеру; – Зиянды бағдарламалардың бар-жоғын сканерлеуден трафиктің белгілі бір түрін алып тастау; – Көрсетілген процестерді немесе қосымшаларды сканерлеуден алып тастау; – Anti-Exploit тексеруіне арналған қосымшаларды қосу және редакциялау, сондай-ақ анықталған кезде қорғаныс әрекеттерін редакциялау; – Желілік шабуылдардан қорғау режимдерін редакциялау; – Бұғатталған немесе рұқсат етілген вебсайттар тізімін жасау арқылы веб-ресурстарға қол жеткізуді басқару; – Белгілі бір уақыт аралықтарында немесе кесте бойынша пайдаланушыларға немесе қосымшаларға веб-қолжетімділікке рұқсат беру немесе тыйым салу функциясы; – Санаттар бойынша веб-сүзгінің болуы (сайттардың мазмұны негізінде қолжетімділікті динамикалық сүзгілеу); – Пайдаланушылардың жеке немесе құпия ақпаратты интернет-алаяқтарға кездейсоқ жария етуіне жол бермеу үшін белгілі фишингтік веб-беттерді автоматты түрде бұғаттайтын фишингтен қорғау функциясының болуы; – Жабдықтың мынадай түрлерін бұғаттауға, сондай-ақ белгілі бір рұқсаттарды (рұқсат ету, бұғаттау, тек оқуға рұқсат беру, әкімші баптауы) белгілеуге мүмкіндік беретін құрылғыларды бақылау модулінің болуы: Bluetooth құрылғылары, CDROM құрылғылары, иілгіш дискілерге арналған дискіжетектер, IEEE 1284.4, IEEE 1394, кескіндерді өңдеу құрылғылары, модемдер, таспалы жинақтауыштар, портативті Windows құрылғылары, COM/LPT порттары, SCSI Raid, принтерлер, желілік адаптерлер, сымсыз желілік адаптерлер, ішкі және сыртқы сақтау құрылғылары; – Қосымшалар үшін белсенді сүзгілеу режимі, сондай-ақ оны ажырату мүмкіндігі; – Ықтимал қалаусыз қосымшалардың бар-жоғын сканерлеу; – Security Account Manager жүйесімен байланысты кілттерді қоса алғанда, тізілімнің маңызды кілттерін рұқсатсыз қол жеткізуден немесе пайдаланудан қорғау функциясының болуы; – Шабуылдар тізбегінің бастапқы кезеңдерінде күрделі қауіптерді анықтау мүмкіндігін арттыратын, ядро деңгейінде Windows API шақыруларын бақылаудың қосымша функциясының

	болуы; – Windows Encrypting File System деректерін қорғау модулінің рұқсатсыз қол жеткізуден, рұқсатсыз араласудан және бопсалаушы бағдарламалардан қорғауы; – Вирус-бопсалаушылардың салдарын жеңілдету (Қалпына келтіру режимі – сұрау бойынша немесе автоматты түрде): – * Тікелей соңғы нүктеде орындалатын процестерді бақылау мүмкіндігі. – * Қашықтан қол жеткізу жүзеге асырылатын ортақ желілік ресурстарды мониторингтеу мүмкіндігі. Егер соңғы нүкте файлдық сервер болып табылса немесе қолжетімді желілік ресурстары болса, осы параметрді пайдалану мүмкіндігі. – RDP қосылымдарын сканерлеу; – Шифрланған трафикті ұстап алу – HTTPS, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS; – TLS handshake ұстап алу; – Шешім орталықтандырылған басқару консолі арқылы құпия деректерді (мысалы, Т.А.Ә., телефон нөмірлері, банк деректемелері, PIN-кодтар, электрондық пошта мекенжайлары) қорғау қағидаларын жасау мен баптауды қолдауы тиіс. Бұл ретте шығыс веб және пошта трафигін сканерлеу және бұғаттау мүмкіндігі болуы тиіс. Шешім бұғаттау туралы пайдаланушыларға хабарлауды және ерекшеліктерді (сенімді мекенжайлар мен сайттар) баптауды қамтамасыз етуі тиіс; – Сенімді процестерді, файлдар мен қалталарды тексеруден алып тастау мүмкіндігі; – Орнату кезінде клиенттік жұмыс станциясын үйлеспейтін БҚ-ның бар-жоғына алдын ала тексеру; – Жұмыс станцияларына клиентті орнату кезінде вирустар мен зиянды БҚ-ға алдын ала сканерлеу жүргізу; – Алдыңғы тексеруден кейінгі жағдайы өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету; – Тапсырмалардың басымдығына байланысты жұмыс станциясының ресурстарын антивирус пен басқа қосымшалар арасында бөлуді реттеу: антивирустық сканерлеуді фондық режимде жалғастыру мүмкіндігі; – Қосымшалардың қара тізімдерін жасау; – Антивирустық бағдарламаның жұмысы туралы егжей-тегжейлі есептер жасау; – Ақпаратты көрсету параметрлерін егжей-тегжейлі баптау және бүкіл ұйым бойынша жаппай әрекеттерді орындау мүмкіндігі бар егжейтегжейлі интерактивті панельдер жасау; – Басқару орталығының басты бетінде графиктері мен блок-схемалары бар кіріктірілген жылдам есептердің болуы, оларды редакциялау және қосу мүмкіндігі; – Соңғы нүктедегі проблемаларды жоюға арналған кіріктірілген қашықтан жөндеу функциясының болуы. Exchange антивирустық қорғау бағдарламалық құралдарына қойылатын талаптар – Хаттардың спам немесе спам емес екенін анықтау үшін әртүрлі сүзгілер мен механизмдердің үйлесімін пайдалана отырып, спам мен фишингке қарсы бірнеше қорғаныс қабатының болуы; – Жаңа және белгісіз спам қауіптерін анықтауға арналған эвристикалық сүзгінің болуы. Сүзгі антиспам зертханасының ішінде спамның үлкен көлемі негізінде автоматты түрде оқытылуы тиіс. Оқыту барысында ол спам мен заңды хабарламаларды ажыратуды, бұрын қаралған электрондық поштаны пайдалана отырып, өте ұқсас белгілер негізінде жаңа спамды тануды үйренуі тиіс; – Бұлттағы спам-хаттардың «цифрлық іздерінің» үнемі жаңартылып отыратын дерекқорын қолдау. Ерекше белгілері бар сұраулар бұлттық серверлерге

	жіберіліп, олардың спам болып табылатыны жедел тексерілуі тиіс. Тіпті ерекше белгілер дерекқордан табылмаған жағдайда да, олар жақында алынған басқа сұраулармен салыстырылуы тиіс және белгілі бір шарттар орындалған кезде электрондық хабарлама спам ретінде белгіленуі мүмкін; – RBL сүзгісінің болуы; – Жіберушілердің ақ тізімдерінің болуы; – Антиспуфинг; – Exchange пошта серверін зиянды қауіптердің барлық түрлерінен (вирустар, трояндар, шпиондық бағдарламалар, руткиттер, жарнамалық БҚ және т.б.) қорғауға арналған зиянды бағдарламалардан қорғау модулінің болуы. Бұл модуль белгіленген әрекеттерге сәйкес вирус жұққан немесе күдікті объектілерді анықтау, оларды емдеуге әрекет жасау немесе вирус жұққан объектілерді оқшаулау арқылы қорғауды қамтамасыз етуі тиіс; – Хаттың тақырыбы, атауы, тіркемесі, белгіленген өрнек бойынша поштаны бұғаттау; – Кіріктірілген құмсалғышқа қойылатын талаптар - Мінез-құлықты терең талдау үшін күдікті объектілерді соңғы нүктелерден құмсалғышқа автоматты түрде және қолмен жіберу мүмкіндігінің болуы; - Пәрмен жолы аргументі бар үлгілерді қолмен тексеру мүмкіндігі; - URL мекенжайларын қолмен тексеру мүмкіндігі; - Машиналық оқыту және мінез-құлықты талдау; - Күдікті әрекеттерді анықтау және олар туралы есеп беру; - Тәуекелге ұшыраған индикаторлар туралы ақпаратты ерте алу; - Күдікті БҚ-ны талдау режимдерінің болуы: - Мониторингке алынған объектілер пайдаланушы үшін қолжетімді болып қала береді. - Талдау нәтижесі қайтарылғанға дейін пайдаланушының объектіге қол жеткізуі бұғатталады. - Құмсалғыш зиянды бағдарламалардың мінезқұлқын егжей-тегжейлі есептермен түсінуді қамтамасыз етуі тиіс. Оқиғаларды тергеу модуліне қойылатын талаптар – Әрбір EDR агентінде соңғы нүктені тұрақты түрде бақылайтын және ақпарат пен күдікті оқиғаларды қауіпсіз түрде жіберетін оқиғаларды тіркеу құралы болуы тиіс. – Гибридті инфрақұрылымдардағы (әртүрлі ОЖ басқаруымен жұмыс істейтін жұмыс станциялары, серверлер немесе контейнерлер) бірнеше соңғы нүктені қамтитын кеңейтілген шабуылдарды анықтау мүмкіндігі. – Қауіптерді талдау модулі қосымша тергеу және әрекет ету үшін соңғы нүктелердегі оқиғаларды жинап, оларды басымдық берілген инциденттер тізіміне бөлуі тиіс. – EDR күдікті файлдарды құмсалғышта детонациялау үшін жіберуі, содан кейін құмсалғыштың қорытындысын инциденттер туралы EDR есептерінде пайдалануы тиіс. – EDR мониторинг тақтасы әкімшілер ескертулер мен визуализацияларды қарап, содан кейін қауіптерді зерттеп, оларға тиімді әрекет ете алуы үшін кез келген құрылғыдан нақты уақыт режимінде қолжетімді болуы тиіс. – EDR сенсоры агентке кіріктірілуі, соңғы нүктелер мен қосымшалардың мінез-құлқы туралы деректерді жинау және беру үшін оларды өңдеуі тиіс. – Қауіпсіздік аналитикасы – сенсор жинаған метадеректерді түсіндіру үшін пайдаланылатын ішкі компонент. – Шешім шабуыл белгілерін іздеу мақсатында соңғы нүктелердегі оқиғаларды бақылауы және осындай белсенділік анықталған кезде инцидентті іске қосуы тиіс. – Шешім MITRE шабуыл индикаторлары мен жеке қауіптер

	аналитикасы негізінде базалық жүйелерді жасау мүмкіндігіне ие болуы тиіс. – Базалық деңгейден кез келген ауытқу инцидент ретінде тіркелуі тиіс. – Шешім белгілі бір уақыт аралығында сенсор анықтаған барлық қауіпсіздік оқиғаларын сүзуге, зерттеуге және оларға қатысты шаралар қабылдауға көмектесетін құралдарды ұсына отырып, инциденттерді талдауды қолдауы тиіс. – Шешім қауіпсіздік оқиғасының қауіпті екеніне сенімділік дәрежесін көрсететін шынайылық бағасының мәнін беруі тиіс. – Шешім MITRE ATT&CK; білім базасымен интеграциялануы және қауіпсіздік оқиғаларын соған сәйкес белгілеуі тиіс. – Қауіпсіздік оқиғаларын файл атаулары, IP мекенжайлары, хост атаулары немесе IOC бойынша іздеуге болады. Сондай-ақ пайдаланушыға күрделі критерийлер негізінде өткен оқиғаларды қарауға мүмкіндік беретін кеңейтілген іздеу функциясы ұсынылуы тиіс. Алдын ала анықталған сұраулар қауіпсіздік оқиғаларын іздеудің пайдалы жағдайларына арналған. – Оқиғаның әсеріне шолу және оқиғаның әрбір түйіні туралы толық ақпарат. – Уақыт шкаласы функциясы қауіпсіздік оқиғаларының даму барысы туралы ақпаратты хронологиялық тәртіппен жинауы тиіс. – Ағымдағы қауіпсіздік оқиғасы кезінде шешім автоматты түрде қабылдайтын бұғаттау әрекеттері туралы ақпаратты жинау функциясы. – Шешім MD5 / SHA256 хэшмәндерін пайдалана отырып, файлдарды/процестерді бұғаттау тізіміне қосуы тиіс. Мұны қауіпсіздік инцидентінен жасауға немесе CSV файлынан импорттауға болады. – Шешім ортада процестердің орындалуын тоқтатуы тиіс. – Шешім файлды карантинге орналастырып, тиісті элементті сақтауы және оның пайдалы деректерін орындауына жол бермеуі тиіс. – Шешім басқару консолімен байланысты сақтай отырып, хостты желіден оқшаулауға мүмкіндік беруі тиіс. – Шешім шабуылдың желіде таралуына жол бермеу үшін тиісті файлды немесе процесті бұғаттау тізіміне қосуы тиіс. – Файлды ерекшелік ретінде қосу мүмкіндігі – зиянды емес файл үшін бұл параметр заңды әрекеттерді тексеруден алып тастауға пайдаланылуы мүмкін. – Шешім одан әрі зерттеу үшін ішкі компоненттер мен үшінші тарап шешімдерін пайдалануы тиіс: • VirusTotal • Құмсалғыш • Google – Шешім шабуылдарды жедел тергеу, криминалистикалық деректерді жинау және бұзушылықтарды жою үшін хостқа қашықтан қосылуы тиіс. Бұл белгісіздікті жояды және шабуыл салдарынан болатын тоқтап қалу уақытын айтарлықтай қысқартады. – Шешім авторизацияланған пайдаланушыға/әкімшіге тікелей консольден басқарылатын соңғы нүктелерге қауіпсіз қол жеткізу мүмкіндігін беруі тиіс. – Қашықтағы соңғы нүктеге сәтті қосылғаннан кейін қауіпті дереу жою немесе одан әрі тергеу үшін деректер жинау мақсатында операциялық жүйеде бірнеше бапталатын қабықша пәрмені тікелей орындалуы мүмкін. – Шешім сондай-ақ алдын алу деңгейлері бұғаттайтын қауіпсіздік оқиғаларын визуализациялауды қамтамасыз етуі тиіс. – Шешім API арқылы жауап әрекеттерін орындау мүмкіндігін ұсынуы тиіс. Қолдау көрсетілетін операциялық жүйелерге қойылатын талаптар Windows операциялық жүйелері • Windows 7, 8, 10, 11, Windows Server 2022, 2019, 2016. A3 Windows

	кластерінің істен шығуға төзімді технологиясын (Windows Server Failover Cluster – WSFC) қолдауы тиіс. Linux операциялық жүйелері Mac OS операциялық жүйелері
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Некоммерческое акционерное общество "Карагандинский национальный исследовательский университет имени академика Е.А.Букетова"
Наименование организатора	Некоммерческое акционерное общество "Карагандинский национальный исследовательский университет имени академика Е.А.Букетова"
№ конкурса:	№ 17990001-1
Наименование конкурса:	Приобретение лицензий системы антивирусной защиты (533)
Номер лота:	№ 88469315-ОК2
Наименование лота:	Услуги по предоставлению лицензий на право использования программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	582950.000.000001
Наименование услуги:	Услуги по предоставлению лицензий на право использования программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	11460517
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	11460517
Срок оказания услуги:	в течение 16 календарных дней со дня заключения договора
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Техническая спецификация Антивирусная защита с модулем расследования инцидентов(далее – «АЗ») на 2600 устройств (конечных точек) с предоставлением технической поддержки, срок подписки не менее 1 года с момента активации лицензии. Поставляемая лицензия на право использования АЗ должна поддерживать возможность отложенной активации. Активация лицензии не должна производиться автоматически по факту отгрузки от производителя или быть привязана к заранее определённой дате. Лицензия должна предоставлять возможность активации в любой день в течение 2 (двух) месяцев с момента отгрузки от поставщика. На период внедрения и настройки программного обеспечения поставщик обязан предоставить временные лицензии с полным функционалом поставляемого АЗ на срок, достаточный для завершения внедрения (по согласованию с заказчиком). ПО должно обеспечиваться технической поддержкой от поставщика и производителя. Форма оказания технической поддержки – дистанционно (онлайн, удалённые консультации, телефон, электронная почта, специализированный портал). Срок поддержки ПО - 12 месяцев. Антивирусная защита (далее – «АЗ») должна представлять собой масштабируемое решение, с единой консолью управления поставляемое в качестве виртуального устройства, установленного локально, со всеми встроенными модулями защиты в одно виртуальное устройство для предотвращения установки дополнительного стороннего программного обеспечения или доступной в облаке, что должно обеспечивать единую точку для развертывания, соблюдение и управление политиками безопасности для любого количества конечных точек, любого типа, в любом месте. В целях масштабируемости решение должно иметь выделенные компоненты для служб баз данных, служб связи, обновлений и веб-служб. Локально установленная АЗ должна поставляться как единое настроенное виртуальное устройство (виртуальный образ). Поддерживаемыми платформами виртуализации должны быть VMware, Microsoft, Red Hat, виртуальная машина на основе ядра или KVM, Oracle VM, Nutanix. Виртуальное устройство должно быть доступно в нескольких вариантах, совместимых с основными платформами виртуализации (OVA, XVA, VHD, OVF, RAW). АЗ должна поддерживать настройку на использование нескольких виртуальных устройств и множество экземпляров конкретных ролей, иметь встроенный балансировщик нагрузки, чтобы обеспечить надежность и масштабируемость Для более безопасной среды АЗ должна поддерживать созданий VPN-кластера для связи по безопасному каналу между несколькими виртуальными устройствами. АЗ должна поддерживать двух факторную аутентификацию для обеспечения дополнительной защиты учетной записи Администратора. АЗ должна управляться из единой точки управления - веб-консоли, которая должна обеспечивать легкий доступ и управление общей безопасностью, глобальными угрозами безопасности и контроль над всеми модулями безопасности, защищающих виртуальные или физические компьютеры и сервера. АЗ должна иметь возможности удаленного развертывания и удаления существующего решения для защиты от

	вредоносных программ, настраивать и запускать задачи удаленного сканирования Веб-консоль должна интегрироваться в существующие системы управления и системы мониторинга, чтобы упростить и автоматически применять защиту для неуправляемых настольных компьютеров, серверов, которые появляются в Microsoft Active Directory, VMware vCenter, Citrix XenServer, VMware Tanzu, Veeam Backup & Replication и которые просто обнаружены в сети Вебсервер должен позволять импортировать цифровые сертификаты из центральной консоли управления, выданные лицензированным центром сертификации или их собственной организацией. Импорт сертификатов должен быть интуитивно понятным и выполняться с центральной консоли управления. Решение должно иметь возможность отображать в центральной консоли информацию о сертификатах: имя, центр выдачи, дату выпуска и дату истечения срока действия выданных сертификатов А3 должна обеспечивать несколько уровней безопасности для конечных точек: защита от вредоносного ПО с мониторингом поведения, защита от угроз нулевого дня, составление черных списков приложений и изоляция потенциально опасных объектов в ограниченной среде, межсетевой экран, управление устройствами, управление контентом, антифишинг. А3 должна иметь встроенный балансировщик нагрузки. Центральная логика архитектуры А3 должна использовать встроенную не-реляционную базу данных, и средство для развертываний, превышающих определенное количество конечных точек, без необходимости использования стороннего лицензионного ключа Антивирусные средства должны включать следующие службы безопасности: Защита конечных точек; Защита виртуальных сред; А3 должна регистрировать действия пользователя на соответствие. А3 должна иметь подробные журналы для каждого действия пользователя. А3 должна поддерживать сложный поиск журналов аудита А3 должна использовать единый шаблон политики для физических и виртуальных машин, и один установщик для любых сред (физических или виртуальных), также А3 должна быть доступной для физических конечных точек под управлением Linux (серверы и рабочие станции). А3 должна включать в себя следующие сканирующие движки Сканирующий движок должен автоматически устанавливается во время создания установочных пакетов, позволяя агентам конечных устройств определять конфигурации машин и соответствующим образом адаптировать технологии сканирования. Также администратор может подстроить сканирующий движок, выбирая между несколькими технологиями сканирования: 1. Локальное сканирование, когда сканирование выполняется на конечном устройстве 2. Гибридное сканирование (частное облако), для средних групп, использует сканирование в облаке и, частично, локальные сигнатуры. 3. Центральное сканирование в частном облаке для малых групп для оптимизации защиты конечных устройств путем переноса нагрузки по сканированию с конечных точек на специализированные серверы безопасности, требует для сканирования сервер безопасности. В этом случае сигнатуры не хранятся локально и сканирование выгружается на сервер

	безопасности. АЗ должна включать в себя следующие модули защиты: ● Защита от вредоносного ПО Модуль защиты от вредоносного ПО должен обеспечивать многоуровневое выявление и предотвращеание всех типов угроз (вирусы, черви, трояны, шпионское и рекламное ПО, кейлоггеры, руткиты и др.) с использованием сигнатурного, эвристического и поведенческого анализа. ● Расширенный контроль угроз Для угроз, которые ускользают даже от эвристического движка, присутствует третий слой защиты в виде расширенного контроля угроз. Расширенный контроль угроз постоянно отслеживает запущенные процессы и оценивает подозрительное поведение, такое как: попытки замаскировать тип процесса, выполнение кода в пространстве памяти процесса (захват памяти для привилегированной эскалации), репликация, перемещение файлов, скрытность в списке технологических процессов и т.д. Каждое подозрительное поведение повышает рейтинг процесса. Когда достигается порог, включается сигнал тревоги. Этот модуль доступен только для поддерживаемых настольных и серверных операционных систем Windows. ● Расширенный Anti-Exploit Основанная на машинном обучении, технология Advanced Anti-Exploit должна блокировать атаки нулевого дня, использующие трудно-обнаруживаемые эксплойты. Advanced Anti-exploit в режиме реального времени должен отслеживать последние эксплойты и устранять уязвимости повреждения памяти, которые могут использоваться для обхода существующих решений безопасности. Технология должна защищать большинство стандартных приложений, таких как браузеры, редакторы Microsoft Office и Adobe Reader и другие. Модуль должен следить за системными процессами и защищать от брешей в безопасности и перехватов существующих процессов. ● Анти- Тампериng Должен обнаруживать уязвимые драйверы на конечной точке, которые могут быть использованы для угрозы целостности агента безопасности. Должен быть совместим операционными системами Windows и Linux. ● Пост-Тампериng Должен определять, были ли обратные вызовы агента безопасности злонамеренно удалены или отключены на конечной точке, что привело к нарушению целостности. Должен быть совместим с операционными системами Windows. ● Брандмауэр Брандмауэр должен контролировать доступ приложений к сети и к Интернету. Доступ должен разрешается автоматически, основываясь на базе данных известных, легитимных приложений. Кроме того, брандмауэр должен защищать систему от сканирования портов, ограничивать использование общего доступа к Интернет (ICS) и предупреждать, когда новые узлы подключаются по Wi-Fi. ● Защита от сетевых атак Уровень безопасности, предназначенный для распознания сетевых атак, целью которых является получение доступа к конечным точкам при помощи таких средств как: атаки методом перебора, сетевые "эксплоиты", программы для кражи паролей, векторы заражения посредством скрытой загрузки, боты и трояны. ● Контроль контента Модуль Контентного Контроля должен обеспечивать соблюдение политики компании в отношении разрешенного трафика, веб-доступа, защиты данных и

	контроля приложений. Администраторы должны иметь возможность задавать параметры сканирования трафика и исключения, составлять график доступа к веб, блокировать или разрешать определенные веб-адреса или категории, настраивать правила защиты данных и устанавливать разрешения для использования конкретных приложений. ● Контроль устройств Модуль Контроля устройств должен предотвращать утечки критических данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя блокирующие правила и исключения с помощью политик для широкого спектра устройств (таких, как USB флэш-накопители, устройства Bluetooth, CD/DVDплееры, устройства хранения, и т.д.). ● Локальное изменение защиты антивирусного агента Администраторы Центра управления (Control Center) могут предоставлять права привилегированных пользователей обычным пользователям конечных устройств с помощью параметров политики безопасности. Данный модуль должен разрешать предоставление администраторских прав уровню пользователей, которые разрешат конечным пользователям получать доступ и изменять настройки безопасности, используя локальную консоль. ● Управление рисками конечной точки (ERA) Управление рисками конечных точек должно определять, оценивать и исправлять слабые стороны Windows машин с помощью сканирования рисков (по запросу или по расписанию в политике), учитывая огромное количество индикаторов риска. После первого сканирования вашей сети с определенными индикаторами риска, Администратор должен получить обзор состояния рисков сети в панели Управления рисками. Некоторые риски должны разрешаться автоматически из центра управления, а также администратор должен иметь возможность по просмотру рекомендаций по снижению ущерба конечной точки. ● Наличие функционала который анализирует и сопоставляет несколько источников данных, чтобы создать визуальное представление последовательности шагов, которые злоумышленник может предпринять для компрометации активов организации с построением графиков предположительных векторов атак. ● Песочница Песочница должна обеспечивать мощный уровень защиты от новейших угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусными ядрами антивируса. Безопасная среда Песочницы должна использовать обширный набор технологий для выполнения полезных нагрузок в изолированной виртуальной среде, анализировать их поведение и сообщать о мельчайших системных изменениях, которые могут свидетельствовать о вирусной и злонамеренной природе файлов. ● Защита Exchange Должна обеспечивать защиту Exchange от вредоносных программ, антиспам, антифишинг, фильтрацию контента и содержимого писем, полностью интегрироваться с серверами Microsoft Exchange, для обеспечения безопасной среды обмена сообщениями и повышения производительности. Использовать признанные технологии защиты от вредоносных программ и спама, программа должна защищать пользователей Exchange от новейших, самых сложных вредоносных программ и от попыток украсть

	конфиденциальные и ценные данные пользователей. ● Модуль расследования инцидентов Это компонент корреляции событий, должен выявлять сложные угрозы или активные атаки. В рамках корпоративной интегрированной платформы модуль расследования инцидентов должен объединять возможности всех устройств, работающих в корпоративной сети. Этот компонент должен приходить на помощь в случаях, когда группы немедленного реагирования распознают и отвечают на серьезные угрозы. Посредством конечных точек вы можете активировать защитный модуль в управлении конечной точки, чтобы объединять данные компьютера и операционной системы. Сбор и обработка метаданных с обеих сторон должна идти на платформе клиент-сервер. Модуль расследования инцидентов должен предоставлять детальную информацию по обнаруженным происшествиям, интерактивной карте происшествий, действиям по исправлению и интеграции с песочницей и Модуль обнаружения передовых атак Требования к программным средствам антивирусной защиты на физических и виртуальных конечных устройствах Программные средства антивирусной защиты рабочих станций должны обеспечивать реализацию следующих функциональных возможностей: – Интеграция с облачными платформами Amazon EC2, Microsoft Azure; – Интеграция со сторонними производителями ПО при помощи API ключей; – АЗ должна предоставлять встроенные исключения для ролей сервера Microsoft (DNS, DHCP, AD, Exchange, SharePoint). – Резидентный антивирусный мониторинг; – Антивирусное сканирование по команде пользователя или администратора; – Антивирусное сканирование по расписанию; – Запуск сканирования при обнаружении Flesh накопителей; – Запуск сканирования на риски конечных точек и пользователей, по расписанию или в ручную; – Возможность централизованного автоматического устранения рисков (неправильно настроенные конфигурации, риски, связанные с учетной записью, риски не обновлённых приложений и.т.д.) на конечных точках через меню в консоли администратора – Возможность сортировки рисков по степени критичности, типу обнаружения, состоянию; – Возможность добавления рисков в списки наблюдений для отслеживания этих рисков в инцидентах организации; – Наличие удобочитаемой, настраиваемой, интерактивной панели с отчетами по рискам организации; – Наличие модуля для оценки организации на соответствие требованиям международных стандартов с возможностью расширения списка доступных стандартов соответствия (CIS v8.0, CMMC 2.0, DORA, ISO/IEC 27001:2022, и.т.д.); – Возможность создания отчетов по всей сетевой инфраструктуре на соответствие требованиям стандарта Cyber Hygiene; – Защита от еще неизвестных вредоносных программ на основе эвристического анализа; – Функция отключения антивирусной защиты при необходимости; – Функция установки пароля на удаление программы с клиентской рабочей станции; – Обнаружение скрытых процессов; – Запуск задач по расписанию и/или сразу после загрузки операционной системы; – Функция установки только выбранных компонентов программного средства антивирусной защиты; –

	Возможность удаленной перенастройки антивирусного агента, добавление или отключение модулей защиты, на клиентской машине через консоль администратора без переустановки и удаления агента. – Сканирование входящих сообщений электронной почты (POP3, IMAP, MAPI) и вебтрафика проверка в режиме реального времени, для предотвращения проникновения вредоносного ПО в конечную точку. - Проверка исходящих сообщений электронной почты (SMTP, MAPI) для предотвращения заражения вредоносными программами других конечных точек. – Исключение определенного вида трафика из сканирования на наличие вредоносных программ; – Исключение из сканирования указанных процессов или приложений; – Добавление и редактирование приложений на проверку Anti-Exploit а также редактирования действий защиты при обнаружении; – Редактирование режимов защиты от сетевых атак; – Управления доступом к вебресурсам, путем создания списка заблокированных либо разрешенных веб-сайтов; – Функция разрешения или запрета на веб-доступ пользователям или приложениям в определенные интервалы времени или по расписанию; – Наличие Веб-фильтра по категориям (динамическая фильтрация доступа к сайтам на основе их содержимого) – Наличие защиты от фишинга с автоматической блокировкой известных фишинговых веб-страниц, чтобы пользователи случайно не раскрыли частную или конфиденциальную информацию интернет-мошенникам; – Наличие модуля контроля устройств для блокировки следующих типов оборудования а также возможностью задавать определенные разрешения (разрешить, заблокировать, только чтение, настройка администратора) - устройства Bluetooth, устройства CD-ROM, дисковые накопители на гибких дисках, IEEE 1284.4, IEEE 1394, устройства обработки изображений, модемы, ленточные накопители, портативные Windows-устройства, порты COM/LPT, SCSI Raid, принтеры, сетевые адаптеры, беспроводные сетевые адаптеры, внутренние и внешние хранилища; – Активный режим фильтрации для приложений, а также возможность отключения; – Сканирование на наличие потенциально нежелательных приложений; – Наличие функции защиты критических ключей реестра, в том числе связанных с Security Account Manager, от несанкционированного доступа или эксплуатации. – Наличие дополнительной функции отслеживания вызовов Windows API на уровне ядра, что повышает способность обнаруживать сложные угрозы на ранних этапах цепочки атак. – Наличие модуля защиты данных Windows Encrypting File System от несанкционированного доступа, несанкционированного вмешательства и от программ-вымогателей; – Смягчение последствий вирусов вымогателей (Режим восстановления- По запросу или автоматически): – * Возможность контроля процессов, которые выполняются непосредственно на конечной точке. – * Возможность мониторинга общих сетевых ресурсов, доступ к которым осуществляется удаленно. Возможность использовать этот параметр, если конечная точка является файловым сервером или имеет доступные сетевые ресурсы. – Сканирование RDP подключений; – Перехват зашифрованного трафика – HTTPS,

	FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS – Перехват TLS handshake – Решение должно поддерживать создание и настройку правил защиты конфиденциальных данных (например, ФИО, телефоны, банковские реквизиты, PIN-коды, адреса электронной почты) через централизованную консоль управления, с возможностью сканирования и блокировки исходящего веб- и почтового трафика. Решение должно обеспечивать уведомление пользователей о блокировке, настройку исключений (доверенные адреса и сайты); – Возможность исключить из проверки доверенные процессы, файлы и папки. – Предварительная проверка клиентской рабочей станции на несовместимое ПО при установке; – Предварительное сканирование на вирусы и вредоносное ПО при установке клиента на рабочие станции; – Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; – Регулировка распределения ресурсов рабочей станции между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме; – Создания черных списков приложений; – Создание детализированных отчетов работы антивирусной программы; – Создание детализированных, интерактивных панелей с подробной настройкой отображения информации на них и возможностью массовых действий по всех организации; – Наличие встроенных, быстрых отчетов с графиками и блок схемами на главной странице центра управления, возможность их редактирования и добавления – Наличие встроенной функции удаленной отладки для устранения проблем на конечной точке Требования к программным средствам антивирусной защиты Exchange – наличие нескольких защитных слоев против спама и фишинга, используя комбинации различных фильтров и механизмов, для определения являются ли письма спамом или нет; – наличие эвристического фильтра для обнаружения новых и неизвестных спамугроз. Фильтр должен автоматически обучается на больших объемах спама внутри антиспам-лаборатории. Во время обучения он должен учится различать спам и легитимные сообщения, распознавать новый спам на основе очень тонкого сходства, используя уже рассмотренную электронную почту – поддержка постоянно развивающейся базы данных "отпечатков" спам-почты в облаке. Запросы, содержащие характерные признаки, должны отправляться на облачные серверы и мгновенно проверяться, являются ли эти сообщения спамом. Даже если характерные признаки не найдены в базе данных, они должны сверяются с другими недавно полученными запросами, и при выполнении определенных условий, электронное сообщение может быть помечено как спам; – наличие фильтра RBL; – наличие белых списков отправителей; – Антиспуфинг; – Наличие модуля защиты от вредоносных программ для защиты почтового сервера Exchange от всех видов вредоносных угроз (вирусов, троянов, шпионских программ, руткитов, рекламного ПО, и т.д.), путем обнаружения зараженных или подозрительных объектов, попытками их лечения или путем изоляции инфицированных объектов, в соответствии с заданными действиями;

	– Блокировка почты по теме письма, названию, вложению, заданному выражению; – Требования к встроенной песочнице - наличие автоматической и ручной отправки подозрительных объектов из конечных точек в Песочницу для углубленного анализа поведения; - возможность ручной проверки образцов с аргументом командной строки; - возможность ручной проверки URL адресов; - машинное обучение и анализ поведения; - выявление и отчет о подозрительной деятельности; - получение ранней видимости индикаторов подверженных риску; - Наличие режимов анализа подозрительного ПО: * объекты, подвергшиеся мониторингу по-прежнему доступны для пользователя. * блокировка доступа пользователя к объекту отклоняется до тех пор, пока результат анализа не будет возвращен. - Песочница должна обеспечивать понимание поведения вредоносных программ с подробными отчетами Требования к модулю расследования инцидентов – Каждый агент EDR должен иметь регистратор событий, который постоянно контролирует конечную точку и безопасно отправляет информацию и подозрительные события. – Возможность для обнаружения продвинутых атак с участием нескольких конечных точек в гибридных инфраструктурах (рабочих станциях, серверах или контейнерах, работающих под управлением различных ОС) – Модуль Анализа угроз должен собирать и распределять события конечных точек в приоритетный список инцидентов для дополнительного расследования и реагирования. – EDR должен отправлять подозрительные файлы для детонации в песочнице, а затем использовать вердикт песочницы в отчетах EDR об инцидентах. – Панель мониторинга EDR в режиме реального времени должна быть доступна с любого устройства, чтобы администраторы могли просматривать предупреждения и визуализации, а затем исследовать угрозы и эффективно реагировать на них. – Датчик EDR должен быть встроен в агент, собирать и обрабатывать данные для передачи данных о поведении конечных точек и приложений. – Аналитика безопасности, внутренний компонент, используемый для интерпретации метаданных, собранных датчиком. – Решение должно отслеживать события конечных точек в поисках признаков атаки и инициировать инцидент при обнаружении такой активности. – Решение должно иметь возможность создавать базовые системы на основе индикаторов атаки MITRE и собственной аналитики угроз. – Любое отклонение от базовой линии должно регистрироваться как инцидент. – Решение должно обеспечивать поддержку анализа инцидентов, предоставляя инструменты, помогающие фильтровать, исследовать и принимать меры в отношении всех событий безопасности, обнаруженных датчиком в течение определенного интервала времени. – Решение должно присваивать значение оценки достоверности, указывающее степень уверенности в том, что событие безопасности является опасным. – Решение должно интегрироваться с базой знаний MITRE ATT & CK и соответствующим образом маркировать события безопасности. – События безопасности можно искать по именам файлов, IP-адресам, именам хостов или IOC. Так же должна быть предоставлена функция расширенного

	поиска, которая позволяет пользователю просматривать прошлые события на основе сложного критерия. Предопределенные запросы предназначены для полезных случаев поиска событий безопасности. – Обзор влияния события и подробная информация о каждом узле события. – Функция временной шкалы должна собирать информацию о развитии событий безопасности в хронологическом порядке. – Функция сбора информацию о блокирующих действиях, автоматически предпринимаемых решением при текущем событии безопасности. – Решение должно добавлять файлы / процессы в список блокировки, используя хеш-значения MD5 / SHA256. Это можно сделать из инцидента безопасности или импортировать из файла CSV. – Решение должно останавливать выполнение процессов в среде. – Решение должно помещать файл в карантин, сохраняя соответствующий элемент и не позволяя ему выполнять свои полезные данные. – Решение должно позволять изолировать хост от сети, сохранив связь с консолью управления. – Решение должно добавлять в список блокировки соответствующий файл или процесс, чтобы предотвратить распространение атаки в сети. – Возможность добавить файл как исключение - для не вредоносного файла этот параметр можно использовать для исключения законной активности. – Решение должно использовать внутренние компоненты и сторонние решения для дальнейшего исследования: • VirusTotal • Песочница • Google – Решение должно удаленно подключаться к хосту для быстрого расследования атак, сбора криминалистических данных и устранения нарушений. Это устраняет неопределенность и значительно сокращает время простоя в результате атаки. – Решение должно позволять авторизованному пользователю / администратору получить безопасный доступ к управляемым конечным точкам прямо с консоли. – После успешного подключения к удаленной конечной точке несколько настраиваемых команд оболочки могут быть выполнены непосредственно в операционной системе для немедленного устранения угрозы или сбора данных для дальнейшего расследования. – Решение должно также обеспечивать визуализацию событий безопасности, которые блокируются превентивными уровнями. – Решение должно предоставлять возможность выполнять ответные действия через API. Требование к поддерживаемым операционным системам Операционные системы Windows • Windows 7, 8, 10, 11, Windows Server 2022, 2019, 2016 A3 должна поддерживать технологию отказоустойчивого Windows-кластера (Windows Server Failover Cluster - WSFC). Операционные системы Linux Операционные системы Mac OS

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)	