Тендерлік құжаттамаға
6-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы	"ҚазАвтоЖол" Ұлттық компаниясы" акционерлік қоғамы
Ұйымдастырушының атауы	"ҚазАвтоЖол" Ұлттық компаниясы" АҚ "Ақылы автомобиль жолдар дирекциясы" филиалы
Тендердің №	№ 17885924-1
Тендердің атауы	Бағдарламалық қамтамасыз ету тауарын электрондық сатылым
Лоттың №	№ 88200721-ОТ2
Лоттың атауы	Бағдарламалық қамтамасыз ету
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*	620129.000.000000
Тауардың атауы*	Бағдарламалық қамтамасыз ету
Өлшем бірлігі*	Дана
Саны (көлемі)*	1
Бірлік бағасы, қосылған құн салығын қоспағанда*	50862068.97
Қосылған құн салығын қоспағанда, сатып алуға бөлінген жалпы сома*	50862068.97
Жеткізу шарты (ИНКОТЕРМС 2010-ға сәйкес)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	с момента заключения договора в течение 30 календарных дней.
Аванстық төлем мөлшері*	0
Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	
Шығарылған жылы (Тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс)	2026
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауарлардың қажетті функционалдық, техникалық, сапалық, өнімділігі мен басқа да сипаттамаларының сипатталуы	ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК Контейнерлік орталарды қорғау жүйесі 1. Жалпы мәліметтер Контейнерлерді қорғау жүйесі Тапсырыс берушінің контейнерлендірілген инфрақұрылымын контейнерлердің өмірлік циклінің барлық кезеңдерінде — образдарды құрастырудан бастап пайдалануға және пайдаланудан шығаруға дейін — қорғауды қамтамасыз етуге арналған. Бұған образдарды, орындау ортасын (runtime), оркестрацияны, желілік өзара іс-қимылды және хост инфрақұрылымын қорғау кіреді. 2. Жүйенің функционалдық мүмкіндіктеріне қойылатын талаптар 2.1 Функционалдық талаптар Жүйе CI/CD процестерімен интеграцияны баптау мүмкіндігін қамтамасыз етуі тиіс: шешім қолданыстағы үздіксіз интеграция және орналастыру (Continuous Integration/Continuous Delivery) процестеріне енгізілуі және контейнерлердің өмірлік циклінің ерте кезеңдерінде қауіпсіздікті қамтамасыз етуі тиіс. Жүйе CI/CD процесінде Open Container Image Layout Specification (OCI) сәйкес келетін директориялардың сканерлеу мүмкіндігін қамтамасыз етуі тиіс. Жүйе Docker Hub, JFrog Artifactory, Sonatype Nexus Repository OSS, GitLab Registry, Harbor, Yandex Registry, Amazon Elastic Container Registry, Red Hat Quay, Microsoft Azure Registry, Google Artifact Registry, Сфера сияқты және Docker Registry API V2-мен үйлесімді өзге образдар тізілімдерімен интеграцияны баптау мүмкіндігін қамтамасыз етуі тиіс. Бұл тізілімдегі образдарды және репозиторийлердегі IaC-ті мыналардың бар-жоғына тексеру үшін қажет: - NVD және ККБ осалдықтар базаларды бойынша белгілі осалдықтар; - құпиялар (құпиясөздер, қолжетімділік кілттері, токендер); - зиянды бағдарламалық қамтамасыз ету; - конфигурациялардағы қателер. Осалдықтарға сканерлеуді жүзеге асыру үшін Жүйенің құрамында жалпыға қолжетімді осалдықтар дерекқорлары (ККБ, NVD) негізінде тұрақты жаңартылатын осалдықтар базаларды болуы тиіс. Компоненттерді Harbor тізілімінен тікелей жүгіну арқылы сканерлеу мүмкіндігін беретін функционал іске асырылуы тиіс. Контейнер образдарды құпиялардың бар-жоғын сканерлеу үшін Жүйеде образдардағы құпияларды іздеудің кіріктірілген саясаттары болуы тиіс. Контейнер образының және кластер торабының құрамындағы зиянды бағдарламалық қамтамасыз етуді анықтау үшін бағдарламалық шешім антивирустық база бойынша тексеруді орындауы тиіс. Тәуекелді қабылдау және тәуекелді қабылдаудан бас тарту бөлігінде тәуекелдерді басқарудың функционалдық мүмкіндігі қамтамасыз етілуі тиіс. Бағдарламалық қамтамасыз етуді пайдаланушының тәуекелді қабылдауы осы тәуекелді нақты образда, репозиторийде немесе жүйедегі барлық образдарда анықталғандар тізбесінен белгіленген уақыт аралығына не тұрақты түрде алып тастауды көздеуі тиіс. Жүйе CI/CD артефактілеріндегі, образдар тізілімдеріндегі, кластер тораптарындағы және орындау ортасындағы осалдықтарды бірыңғай интерфейс («бір терезе») арқылы орталықтандырылған зерттеу мүмкіндігін қамтамасыз етуі тиіс. Жүйеге қолжетімділікті басқару шеңберінде Жүйеде қолжетімді функционал бойынша ажыратылған рөлдік модель іске асырылуы тиіс. Жүйе пайдаланушылардың қолжетімділік құқықтарын басқару мүмкіндігін қамтамасыз етуі тиіс. Жүйеге қолжетімділік беру шеңберінде LDAP-пен, оның ішінде бірегей атау схемасын қолдана отырып, интеграция көзделуі тиіс. Жүйе аутентификация үшін Active Directory бірнеше доменін пайдалану мүмкіндігін қамтамасыз етуі тиіс. Жүйе Active Directory-де UTF-8 кодтауларын, оның ішінде топтар, атрибуттар және бірегей атаулар (ағылш. Distinguished names, DN) атауларында кирилл таңбаларын пайдалануды қолдауы тиіс. Жүйе пайдаланушылардың қолжетімділігін әкімшіктеу және қауіпсіздік саясаттарын қолдану үшін көріну салаларын икемді баптау мүмкіндігін қамтамасыз етуі тиіс (бақылanатын кластер, namespace, registry деңгейінен нақты образға дейін). Жүйе кейіннен автоматты тарату үшін хабарлама құралдарымен (электрондық пошта, Telegram) интеграцияны баптау мүмкіндігін қамтамасыз етуі тиіс. Жүйе пайдаланушыға контейнер образдарды талдауға көмектесу үшін ЖИ-құралымен интеграция мүмкіндігін қамтамасыз етуі тиіс. Жүйе пайдаланушыға контейнер образдарды талдауға көмектесу үшін сыртқы LLM-модельдермен (OpenAI API) интеграция мүмкіндігін қамтамасыз етуі тиіс. Жүйе есептерді PDF, HTML, CSV, JSON, XML форматтарында мыналар үшін жүктеп алу мүмкіндігін беруі тиіс: - контейнер образдары және кластер тораптарын сканерлеу нәтижелері; - салалық қауіпсіздік стандарттарына сәйкестікті тексеру нәтижелері; - қабылданған тәуекелдер. Жүйе өз функцияларын API арқылы пайдалануға мүмкіндік беруі, сондай-ақ OpenAPI Specification (OAS) сәйкес құжаттамаға ие болуы тиіс. Оған мынадай функциялар кіреді: - Ядро компоненттерінің жай-күйі туралы деректерді алу (Core Health Check); - Сканерлеу, образдар қауіпсіздігі, ден қою және орындау ортасы саясаттарын басқару; - Орындау ортасының профильдерін басқару; - Репутация көзінің пайдаланушылық тізімін басқару; - Жүйе оқиғаларының журналын алу; - Контейнерлер оқиғаларының журналын алу; - Кластер тораптары оқиғаларының журналын алу; - Тәуекелдерді басқару; - Автопрофильдеу міндеттерін басқару; - Образдар қолтаңбасын тексеру модульдерімен интеграция туралы деректерді алу; - Кластерлер, неймспейстер және контейнерлер туралы деректерді алу (торап туралы деректерді қоса алғанда); - Дашбордқа шығарылған деректерді алу; - Тізілімдерді сканерлеу нәтижелері туралы деректерді алу; - Агент-топтар туралы деректерді алу және оларды басқару, конфигурациялық файлдарды жүктеп алуды қоса алғанда; - Тізілімдер интеграциялары туралы деректерді алу және оларды басқару; - Хабарлама жүйелерімен байланған интеграциялар туралы деректерді алу; - Жүйеде бар сканерлеу міндеттері туралы деректерді алу; - Жиынтық және егжей-тегжейлі есептер туралы деректерді алу және оларды басқару; - Қосылған сканерлер туралы деректерді алу; - Сканерлеу міндеттерін құру; - Сканерлеу міндеттері және олардың мәртебелері туралы деректерді алу; - Образда анықталған осалдықтар, конфигурация қателері, құпия деректер және зиянды бағдарламалық қамтамасыз ету туралы деректерді алу; - Пайдаланушының осы рөлінде қолжетімді эндпойнттер туралы деректерді алу; - Қолдану салалары туралы деректерді алу; - Анықталған барлық осалдықтардың тізімін алу; - Нақты осалдық туралы деректерді алу; - Кластер тораптары туралы деректерді алу; - Кластер тораптарын сканерлеуді басқару. - Кластердің RBAC объектілері туралы деректерді алу. - Контейнер образы үшін жұмыс жүктемесі (ағылш. workload) туралы деректерді алу (кластер, атаулар кеңістігі, под). - Интеграцияланған образдар тізілімдерінің тізімін сұрату кезінде интеграция түрі туралы ақпаратты алу (қолмен немесе автоматты құрылған). - Белгілі бір торап үшін контейнерлер тізімін алу. Жүйеде кластер тораптарының жүйелік шақырулары (syscalls) аудиттеу тетігі қаланауы тиіс. Жүйе syslog хаттамасы бойынша CEF форматындағы хабарламаларды қабылдауды қолдайтын кез келген SIEM-жүйелермен интеграция мүмкіндігін мынадай функционалмен көздеуі тиіс: - пайдаланушы интерфейсі арқылы әртүрлі инстанстармен интеграцияны баптау; - алушы инстанстарды көрсете отырып, әртүрлі санаттағы жүйелік оқиғаларды (Әкімшілендіру, Алерттер, CI/CD, Саясаттар, Ресурстар, Сканерлер, Қолжетімділік контроллері, Контейнерлер оқиғалары, Рөлдер негізіндегі қолжетімділік, API) жіберу параметрлерін айқындау; - желілік трафикке (кіріс және шығыс), файлдық операцияларға, іске қосылатын процестерге қатысты контейнерлер оқиғаларын жіберу параметрлерін айқындау. Жүйе сыртқы құпиялар қоймасы HashiCorp Vault-пен интеграция мүмкіндігін беруі тиіс: - контейнерлерді қорғау компоненттері үшін алдын ала құрылған құпиялары оқу; - сервисаралық өзара іс-қимыл үшін пайдаланылатын TLS-сертификаттарды жасау үшін Vault PKI пайдалану. Жүйе компоненттердің жай-күйін тексеруге арналған кірістірілген құралдарды (Health Check тетіги) беруі тиіс, атап айтқанда: - кластер компоненттерінің жай-күйін визуалдау; - компоненттердің жай-күйі туралы ақпаратты қарау мүмкіндігі; - компоненттердің heartbeat мониторингі; - сыртқы жүйелерге компоненттердің жай-күйі туралы ақпаратты API тетігі арқылы беру; - компоненттердің өміршеңділігін жоғалтуы туралы нысаналы пайдаланушыларға хабарлау. Қызмет көрсету процестерін автоматтандыру, компоненттердің қауіпсіздігі мен сенімділігін қамтамасыз ету үшін автоматтандырылған қызмет көрсету және қолдау құралдарын енгізу қажет. Бұл мыналарды қамтуы тиіс: - компоненттерді автоматты жаңарту баптаулары; - компоненттердің жұмыс қабілетін автоматты қалпына келтіру алгоритмдері; - компоненттер туралы ақпаратты автоматты резервтік көшіру тетіктері. Жүйе 10 000-ға дейін желілік тораптан және инфрақұрылымдағы 40 000-ға дейін бірегей образдардан тұратын инфрақұрылымдардың үздіксіз мониторингін қамтамасыз етуі тиіс. Кластерлердегі атаулар кеңістіктері (namespaces) ішіндегі әртүрлі ресурстардың байланыстарын, оның ішінде олардың компоненттерінің желілік өзара іс-қимылын және компоненттердің қауіпсіздік проблемаларын визуалдаудың функционалдық мүмкіндігі қамтамасыз етілуі тиіс. Жүйе контейнер образдарды Runtime режимінде тексеруді қамтамасыз етуі тиіс: осалдықтардың, құпиялардың және зиянды бағдарламалық қамтамасыз етудің бар-жоғын тексеру. Жүйе контейнерлерді орындау кезінде файлдық қауіптерден қорғауды қамтамасыз етуі тиіс. Жүйе кластер тораптарын осалдықтардың бар-жоғына тексеруді қамтамасыз етуі тиіс. Жүйе оркестратор нодтарының операциялық жүйесін файлдық қауіптерден Runtime қорғауды қамтамасыз етуі тиіс. Кластер тораптарын салалық стандарттарға сәйкестігіне тексеруді, сондай-ақ осы тексеру нәтижелері бойынша жиынтық және егжей-тегжейлі есептерді қалыптастыруды іске асыру көзделуі тиіс. Оркестраторды кластерлер қауіпсіздігінің салалық стандарттарына сәйкестігіне сканерлеу, сондай-ақ осы тексеру нәтижелері бойынша жиынтық және егжей-тегжейлі есептерді қалыптастыру мүмкіндігі көзделуі тиіс. Жүйе кластердің RBAC объектілеріндегі өзгерістерді журналдау мүмкіндігін беруі тиіс. Жүйе контейнерлік инфрақұрылым компоненттерінің конфигурацияларын талдау мүмкіндігін қамтамасыз етуі тиіс, атап айтқанда: осы конфигурациялар пайдаланыла отырып орналастырылған қосымшалар мен сервистердің қауіпсіздігін, өнімділігін және сенімділігін қамтамасыз ету үшін контейнерлік ортаның баптаулары мен параметрлерін бағалау. Жүйе орындау ортасындағы оқиғаларды жинауды және тексеруді қамтамасыз етуі тиіс: - оқиғалар туралы деректерді жинау және талдау; - инциденттер туралы хабарлар. Жүйе қауіпсіздік саясаттарына сәйкес келмейтін образдарын іске қосылуына жол бермеу мақсатында орындау ортасында контейнерлердің іске қосылуын бақылауы тиіс. Жүйе желілік қосылыстардың репутациясы туралы ақпарат беру және алынған репутация негізінде қосылыстарды бұғаттау мүмкіндігін қамтамасыз етуі тиіс. Жүйе қорғау агентін кластердің әрбір торабында (node) пайдаланушылық қосымша контейнерлерінде араласпай, баптаған қауіпсіздік саясаттарына сәйкес қауіпсіздікті бақылауды жүзеге асыру үшін дербес жұмыс істейтін компонент ретінде беруі тиіс, атап айтқанда: - тораптарда іске қосылған контейнерлердің орындау ортасының қауіпсіздігін бақылау; - пайдалану ортасының оқиғаларын қауіпсіздік саясаттарына сәйкестігіне мониторингтеу, саясаттарға сәйкес келмейтін іс-қимылдарды бұғаттау. Жүйе баптаған қауіпсіздік саясаттарына сәйкес қауіпсіздікті бақылауды қамтамасыз етуі тиіс. Жүйе образдарда осалдықтар анықталған кезде ден қою саясатының сценарийлерін қолдану мүмкіндігін қамтамасыз етуі тиіс. Жүйе баптаған қауіпсіздік саясаттарына сәйкес келмеген кезде іс-қимылдарды бұғаттауды қамтамасыз етуі тиіс. Жүйе белгіленген қауіпсіздік қағидаларын бұзуы мүмкін белгілі бір іс-қимылдардың орындалуын немесе белгілі бір функциялардың пайдаланылуын болдырмауы тиіс. Жүйе тораптарда (nodes) баптаған қауіпсіздік саясаттарына сәйкес қауіпсіздікті бақылауды қамтамасыз етуі тиіс, атап айтқанда кластер контейнерлерінің желілік өзара іс-қимылын бақылауы тиіс (extended Berkeley Packet Filter технологиясы). Жүйе контейнерлер ішіндегі қосымшалар мен сервистер, процестер және контейнерлер операцияларын өзге ресурстар деңгейінде қауіпсіздік саясаттары мен шектеулерді басқару мүмкіндігін қамтамасыз етуі тиіс (extended Berkeley Packet Filter технологиясы). Жүйе контейнерлерді орындау кезінде бақылау мүмкіндігін қамтамасыз етуі тиіс (extended Berkeley Packet Filter технологиясы), атап айтқанда: - контейнерлер ішінде қосымшалар мен сервистердің іске қосылуын бақылау; - желілік белсенділікті бақылау; - күдікті белсенділікті (процестер мен желілік трафикті) бұғаттау. Жүйе контейнерлердің жұмысын шектеу бөлігінде процестер мен желі мониторингінің қағидаларын (орындау ортасының профильдерін) құру мүмкіндігін беруі тиіс: - образдарды қауіпсіз орналастыру параметрлерін көрсету және қолдану; - образдардан орналастырылған қосымшалардың қауіпсіз мінез-құлқының параметрлерін көрсету және қолдану. Жүйе орындау ортасының профильдерін автоматты қалыптастыру мүмкіндігін қамтамасыз етуі тиіс. Жүйе контейнерлердің жұмысына байланысты барлық оқиғалар үшін мынадай базалық өрістерді тіркеуі тиіс: - оқиғаның басталған күні мен уақыты; - k8s кластерінің сәйкестендіргіші; - k8s-тегі namespace атауы; - подтың атауы; - контейнердің атауы; - контейнер іске қосылған контейнер образы (репозиторийге сілтеме, тегпен бірге); - образдың бірегей сәйкестендіргіші (хэш). Желілік трафикке (кіріс және шығыс) қатысты контейнерлер оқиғаларын тіркеуден кеңейтілген мүмкіндіктері мыналарды қамтуы тиіс: - желілік коммуникация хаттамасы; - желілік пакеттің көзі және алушысы; - көз және алушы пайдаланатын порттар. Контейнердің файлдық жүйесі объектілеріне қолжетімділік (оның ішінде құру, жою, ашу) оқиғаларын тіркеуін кеңейтілген мүмкіндіктері мыналарды қамтуы тиіс: - қолжетімділікті жүзеге асырған процестің PID және PPID; - қолжетімділікті жүзеге асырған процестің euid, egid; - қолжетімділік жүзеге асырылған контейнердің файлдық жүйесіндегі файлдың атауы және орналасуы; - операция (оқу, жазу, жою). Іске қосылатын процестерге қатысты контейнерлер оқиғаларын тіркеудің кеңейтілген мүмкіндіктері мыналарды қамтуы тиіс: - процестің PID және PPID; - процестің euid, egid; - іске қосылатын орындалатын файлдың атауы (орналасуының толық жолымен); - command толық шығысы (аргументтермен). Жүйе образдардың қолтаңбасын тексеру және қолтаңбасы жарамсыз контейнерлердің іске қосылуына жол бермеу мүмкіндігін қамтамасыз етуі тиіс. Контейнерлердің қолтаңбасын тексеру үшін сыртқы валидаторлармен — Notary және/немесе CoSign — интеграция мүмкіндігі көзделуі тиіс. Жүйе динамикалық қолжетімділік контроллерімен (ағылш. Dynamic Admission Controller, DAC) жұмыс жылдамдығын оңтайландыру мүмкіндігін беруі тиіс. Мынадай мүмкіндік көзделуі тиіс: - қауіпсіздік саясаттарын қолдана отырып тексеруді жеделдету үшін образдар тізілімінде образ хэшін тексеруді өшіру (образдардың талаптарға сәйкестігін және тіркелмеген образдарды тексеру). - DAC өтініштерін өңдеуді 300 мс-қа дейін жеделдету үшін сканерлеу нәтижелерін kube-agent агенті жағында кэштеу. Жүйе S3-қоймада сақталатын деректердің ротация (жою) параметрлерін квоталар арқылы баптау мүмкіндігін беруі тиіс: уақыт бойынша немесе S3-бакеттің толу деңгейі бойынша. Жүйе сканерлеу тапсырмаларының орындалу кезектілігін баптау мүмкіндігін беруі тиіс. Жүйе CEL тілін пайдалана отырып образдарды пайдаланушылық қауіпсіздік саясаттарын (Assurance policies), қолжетімділікті бақылау саясаттарын (Admission controller policies) және пайдаланушылық стандарттарды (Benchmark frameworks) құру мүмкіндігін беруі тиіс. Жүйе толық конфигурацияны (саясаттар, агенттер топтары, профильдер және т.б.) шифрланған немесе ашық түрде экспорттауды және оны Linux/Windows/macOS арналған утилита арқылы шешімнің басқа даналарына импорттауды қолдауы тиіс. Жүйе nodeagent подтарын қайта орнатпай агенттер топтарының конфигурациясын динамикалық жаңартуды, өзгерістерді дереу қолданумен қамтамасыз етуі тиіс. Жүйе сканерленген образдарды SPDX және CycloneDX SBOM форматтарында интерфейс және API арқылы қарау мүмкіндігін беруі тиіс. Жүйе торап компоненттерін аудиттеу және бүкіл инфрақұрылымды орталықтандырылған бақылау үшін басқару торабына қауіпсіздік агенттерін орнатуды қолдауы тиіс. Жүйе шешім ядросы қызмет көрсетілетін кластерлердегі агенттермен байланысын жоғалтқан жағдайда ден қою саясаттары мен SIEM-жүйелерді пайдалана отырып хабарламалар алу мүмкіндігін қамтамасыз етуі тиіс. Жүйе CI-деті тексеру нәтижелеріне қолжетімділікті жобалардың көріну салаларына сәйкес араластыруді қамтамасыз етуі тиіс. Жүйе ақпараттық панельдегі деректерге қолжетімділікті қолдану салалары мен пайдаланушының қолжетімділік құқықтарын ескере отырып араластыруді қамтамасыз етуі тиіс. Жүйе сканерлеулер бойынша өзгей-тегжейлі ақпаратты (мысалы, сканерлердің өнімділік метрикалары, белгілі бір уақыт аралығында жүргізілген сканерлеулер, ОЖ түрі, соңғы сканерлеу күні және т.б.) API арқылы алу мүмкіндігін беруі тиіс. Жүйе өңделмеген (raw) қауіпсіздік оқиғаларын алу үшін API беруі тиіс. Жүйе образды тізілімде алдын ала іздеуісі, тікелей жол бойынша сканерлеуге мүмкіндік беруі тиіс. Жүйе орындау ортасының ағымдағы саясаттарын есепке алмай автопрофильдер құруды қолдауы тиіс. 2.2. Интерфейске қойылатын талаптар Жүйенің басқару консолі нысаналы пайдаланушы үшін интуитивті түсінікті интерфейсі бар WEB-қосымша ретінде іске асырылуы тиіс. Жүйенің басқару консолі мынадай элементтерден тұруы тиіс: - Басты мәзір. Басты мәзірдің бөлімдері мен кіші бөлімдері шешімнің негізгі функцияларына қолжетімділікті қамтамасыз етуі тиіс. - Жұмыс аймағы. Жұмыс аймағындағы ақпарат пен басқару элементтері басты мәзірде таңдалған бөлімге немесе кіші бөлімге байланысты болуы тиіс. Бағдарламалық қамтамасыз етудің пайдаланушы интерфейсіне автоматты түрде жүктелуі тиіс: - CI/CD процесінде жиналған образды сканерлеу нәтижелері; - қосылған образдар тізілімдерінен сканерленген образдардың тізбесі; - кластерлердегі атаулар кеңістіктері (namespaces) ішіндегі әртүрлі ресурстардың байланыстарын визуалдау; - кластер нодтарын сканерлеу нәтижелері; - кластер нодтарында анықталған осалдықтар туралы ақпарат; - кластер нодтарында зиянды бағдарламалық қамтамасыз етуді анықтау оқиғалары туралы ақпарат; - RBAC объектілері туралы ақпарат; - салалық стандарттарға сәйкестік туралы ақпарат; - контейнерлер мен кластер тораптары оқиғаларының журналы; - қабылданған тәуекелдер туралы ақпарат; - қауіпсіздік саясаттарының тізбесі және баптаулары; - қосылған образдар тізілімдерінен образдарды сканерлеу нәтижелері; - анықталған осалдықтар туралы ақпарат; - белгілі бір образдың қабаттары және әрбір қабатта табылған осалдықтар туралы ақпарат; - белгілі бір образдың ресурстары (компоненттері) және оларда табылған осалдықтар туралы ақпарат; - белгілі бір образда анықталған құпиялар туралы ақпарат; - белгілі бір образда анықталған зиянды бағдарламалық қамтамасыз ету туралы ақпарат; - белгілі бір образда анықталған конфигурация қателері туралы ақпарат; - белгілі бір образды сканерлеу тарихы; - образдар тізілімдерімен интеграция баптаулары; - хабарлама құралдарымен интеграция баптаулары; - LDAP-пен интеграция баптаулары; - SSO-мен интеграция баптаулары; - ЖИ-құралымен немесе сыртқы LLM-модельдермен интеграция баптаулары; - SIEM-жүйемен интеграция баптаулары; - образдар қолтаңбасын тексеру модульдерінің баптаулары; - қолжетімділікті басқару жөніндегі баптаулар; - авторизация баптаулары; - сканерлеу тапсырмаларының орындалу кезектілігінің баптаулары; - қауіпсіздік саясаттарының баптаулары; - қауіпсіздік оқиғаларының журналы; - Жүйенің есептік нысандары; - лицензиялар; - рөлдік модельді және көріну салаларын басқару жөніндегі баптаулар. - Жүйе компоненттері туралы ақпарат; 2.3. Сенімділікке қойылатын талаптар Жүйе Kubernetes, OpenShift оркестрация ортасында үздіксіз жұмыс істеуге қабілетті болуы тиіс. Шешім Тапсырыс берушінің ірі инфрақұрылымдары бар архитектурасына сай масштабтау мүмкіндігіне ие болуы тиіс. Жүйе Yandex Cloud, Amazon AWS EKS, Microsoft Azure AKS сияқты бұлтты орталарда орналастырылғанған кейін үздіксіз жұмыс істеуді қамтамасыз етуі тиіс. 2.4. Орнатуға қойылатын талаптар Мынадай орналастыру схемаларын көздеуі тиіс: - корпоративтік желінің ашық контурында орналастыру; - корпоративтік желінің жабық контурында орналастыру. Өнім Kubernetes ортасында қосымшаларды іске қосуды автоматтандыруға мүмкіндік беретін біріздендірілген Helm құралын пайдалана отырып орнатылуы тиіс. Жүйе қорғау агентін кластердің әрбір торабында (node) дербес жұмыс істейтін компонент ретінде орнату мүмкіндігін беруі тиіс. Ескертпе: корпоративтік желінің жабық контурында прокси-серверді пайдалана отырып орналастыру сценарийі де көзделуі тиіс. 2.5. Архитектураға қойылатын талаптар Сыртқы дерекқорларды басқару жүйелері пайдаланылған кезде контейнерлерді қорғау мынадай ДББЖ-мен жұмыс істеу мүмкіндігін қолдауы тиіс: - ClickHouse v25.* - PostgreSQL (Postgres Pro Standard/Enterprise) 15, 17, 18 - Pangolin 6.2.0. Контейнерлерді қорғау контейнерлердің орындау ортасы профильдерін пайдалана отырып орташының мониторингін іске асыру үшін Linux-дистрибутивтерінің және Linux ОЖ ядроларының мынадай нұсқаларын қолдауы тиіс: - CentOS 8.2.2004 + ядро 4.18.0-193. - Ubuntu 18.04.2 + ядро 4.18.0. - Debian 10 + ядро 4.19.0. - RHEL 9.4 + ядро 5.14. - Red Hat Enterprise Linux CoreOS 416.94.202408200132-0 + ядро 5.14.0-427.33.1.el9_4.x86_64. 3. Кепілдік қызмет көрсетуге қойылатын талаптар Кепілдік мерзімі кемінде 12 айды құрауы тиіс. 4. Техникалық қолдауға қойылатын талаптар Жеткізуші Жүйені кемінде 12 ай мерзімге және кемінде 5х8 режимінде (жұмыс уақыты дүйсенбіден жұмаға дейінгі жұмыс күндері сағат 9:00-ден 18:00-ге дейін) техникалық қолдаумен қамтамасыз етуі тиіс. Мұндай стандартты қолдау Жүйені пайдалануға байланысты проблемаларды тегін шешуге және Жүйені тегін жаңартуға (БК және/немесе қозғалтқыштардың жаңа нұсқаларын не түзетулерді алуға) мүмкіндік беруі тиіс. Жүйені пайдалану кезінде туындайтын проблемаларды шешу үшін Жеткізуші Тапсырыс берушіден немесе оның өкілдерінен өтінімдер қабылдауға арналған электрондық сервис (веб-портал, арнайы email-мекенжай, мобильді қосымша және т.б.) ұсынуы тиіс, мұндай өтінімдер қолдау жүйесінде автоматты түрде тіркелуі тиіс. Мұндай сервис өтінімдердің құрылғанын растау, өтінімдер мәртебесінің өзгеруі және т.б. функционалына ие болуы тиіс. Мұндай сервиспен жұмыс істеу және Жеткізушінің өкілдерімен коммуникация қазақ немесе орыс, немесе ағылшын тілінде қолжетімді болуы тиіс. Жеткізуші Интернет желісінде жүйенің техникалық құжаттамасына және әкімшілендіру жөніндегі құжаттамаға алдын ала тіркеусіз ашық қолжетімділікті қамтамасыз етуі тиіс. 5. Тендерге қатысу өтінімінің құрамында ұсынылатын растайтын құжаттарға қойылатын талаптар Әлеуетті жеткізуші тендерге қатысу өтінімінің құрамында мыналарды ұсынады: – ұсынылатын Жүйенің өндірушісінен не оның ресми өкілінен (дилерінен немесе дистрибьюторынан) әлеуетті жеткізушінің аталған өндірушінің өнімін Қазақстан Республикасының аумағында осы сатып алу шеңберінде жеткізуге құқығын растайтын, Тапсырыс берушінің атауы мен сатып алу нөмірі көрсетілген хаттың (сертификаттың, күәліктің) көшірмесін. Ресми өкілдің (дилердің немесе дистрибьютордың) хаты ұсынылған жағдайда, қосымша осы ресми өкілдің Қазақстан Республикасының аумағындағы мәртебесін растайтын өндіруші құжатының көшірмесі ұсынылады.
Іпеспе қызметтер (кажет болған жағдайда көрсетіледі) (монтаждау, іске қосу, дайындау, тексеру және тауарларды сынау)	Жеткізуші Жүйені енгізуді және Тапсырыс берушінің 2 қызметкерін Жүйені баптау мен онымен жұмыс істеу бойынша оқытуды қамтамасыз етуі тиіс. Жүйені енгізу шеңберінде мынадай іс-шараларды орындауы тиіс: - Тапсырыс берушінің дайындалған инфрақұрылымын және осы техникалық ерекшеліктің талаптарын ескере отырып Жүйені орналастыру схемасын әзірлеу және келісу; - әзірленген және келісілген архитектураға сәйкес орнату; - сарсаттар мен қағидаларды әзірлеу, баптау және бейімдеу.
Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

* мәліметтер сатып алу жоспарынан алынады (автоматты түрде көрсетіледі).

Ескерту:

1. Функционалдық, техникалық, сапалық, пайдаланушылық, өзге де сипаттамалар, ілеспе қызметтер бойынша әрбір талап және қосымша талаптар бөлек жолда көрсетіледі.

2. Өзге құжаттарда техникалық ерекшеліктің талаптарын белгілеуге жол берілмейді.

Приложение 6
к тендерной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Национальная компания "ҚазАвтоЖол"
Наименование организатора	Филиал "Дирекция платных автомобильных дорог" АО "Национальная компания "ҚазАвтоЖол"
№ тендера	№ 17885924-1
Наименование тендера	Электронные закупки товара программное обеспечение
Номер лота	№ 88200721-ОТ2
Наименование лота	Программное обеспечение
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*	620129.000.000000
Наименование товара*	Программное обеспечение
Единица измерения*	Штука
Количество (объем)*	1
Цена за единицу, без учета налога на добавленную стоимость*	50862068.97
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*	50862068.97
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*	с момента заключения договора в течение 30 календарных дней.
Размер авансового платежа*	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	
Год выпуска (Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора)	2026
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ Система защиты контейнерных сред 1. Общие сведения Система защиты контейнеров предназначена для обеспечения защиты контейнеризированной инфраструктуры Заказчика на всех этапах жизненного цикла контейнеров — от сборки образов до эксплуатации и вывода из эксплуатации, включая защиту образов, среды выполнения (runtime), оркестрации, сетевого взаимодействия и хостовой инфраструктуры. 2. Требования к функциональным возможностям Системы 2.1 Функциональные требования Система должна обеспечивать возможность настройки интеграции с CI/CD-процессами: решение должно быть встраиваемым в существующие процессы непрерывной интеграции и развертывания (Continuous Integration/Continuous Delivery), обеспечивая безопасность на ранних этапах жизненного цикла контейнеров. Система должна обеспечивать возможность сканирования директорий, соответствующих Open Container Image Layout Specification (OCI) в процессе CI/CD Система должна обеспечивать возможность настройки интеграции с реестрами образов такими, как Docker Hub, JFrog Artifactory, Sonatype Nexus Repository OSS, GitLab Registry, Harbor, Yandex Registry, Amazon Elastic Container Registry, Red Hat Quay, Microsoft Azure Registry, Google Artifact Registry, Сфера и иных совместимых с Docker Registry API V2 для проверки образов в реестре/IaC в репозиториях на наличие: - известных уязвимостей по базам уязвимостей NVD и БДУ; - секретов (паролей, ключей доступа, токенов); - вредоносного ПО; - ошибок в конфигурациях. Для осуществления сканирования на уязвимости Система должна иметь в своем составе регулярно обновляемые базы уязвимостей на основании общедоступных баз данных уязвимостей (БДУ, NVD). Необходимо реализовать функционал, который будет предоставлять возможность сканирования компонентов путем обращения напрямую из реестра Harbor. Для осуществления сканирования на наличие секретов в образах контейнеров Система должна иметь встроенные политики поиска секретов в образах. Для обнаружения вредоносного ПО в составе образа контейнера и узла кластера программное решение должно выполнять проверку по антивирусной базе. Должна быть обеспечена функциональная возможность управления рисками в разрезе принятия риска, отмены принятия риска. Принятие риска пользователем программного обеспечения должно предполагать исключение данного риска из перечня всех найденных в конкретном образе, репозитории или во всех образах в системе на заданный промежуток времени или перманентно. Система должна обеспечивать возможность централизованного исследования уязвимостей в артефактах CI/CD, реестров образов, узлов кластера и среды выполнения посредством единого интерфейса («одного окна»). В рамках управления доступом к Системе должна быть реализована ролевая модель, включающая в себя разграничение по доступному в Системе функционалу. Система должна обеспечивать возможность управления правами доступа пользователей. В рамках предоставления доступа к Системе должна быть предусмотрена интеграция с LDAP, в том числе с применением схемы уникального имени. Система должна обеспечивать возможность использования нескольких доменов Active Directory для аутентификации. Система должна поддерживать кодировки UTF-8 в Active Directory, в том числе с использованием кириллических символов, в названиях групп, атрибутов и уникальных имен (англ. Distinguished names, DN) Система должна обеспечивать возможность гибкой настройки областей видимости для разграничения доступа пользователей и применения политик безопасности (от уровня контролируемого кластера, namespace, registry до конкретного образа). Система должна обеспечивать возможность настройки интеграции со средствами уведомлений для дальнейшей автоматической рассылки (электронная почта, Telegram). Система должна обеспечивать возможность интеграции с ИИ-инструментом для помощи пользователю в анализе образов контейнеров. Система должна обеспечивать возможность интеграции с внешними LLM-моделями (OpenAI API) для помощи пользователю в анализе образов контейнеров. Система должна предоставлять возможность выгрузки отчетов в форматах PDF, HTML, CSV, JSON, XML для: - результатов сканирования образов контейнеров и узлов кластера - результатов проверок на соответствие отраслевым стандартам безопасности - принятых рисков Система должна позволять использовать свои функции посредством API, а также обладать документацией в соответствии с OpenAPI Specification (OAS), включая следующие функции: - Получение данных о состоянии компонентов ядра (Core Health Check); - Управление политиками сканирования, безопасности образов, реагирования и среды выполнения; - Управление профилями среды выполнения; - Управление пользовательским списком источника репутаций; - Получение журнала событий системы; - Получение журнала событий контейнеров; - Получение журнала событий узлов кластеров; - Управление рисками; - Управление задачами автопрофилирования; - Получение данных об интеграции с модулями проверки подписей образов; - Получение данных о кластерах, неймспейсах и контейнерах (включая данные об узле); - Получение данных, выведенных на дашборде; - Получение данных о результатах сканирования реестров ; - Получение данных и управление агент-группами, включая скачивание конфигурационных файлов; - Получение данных и управление интеграциями реестров; - Получение данных о настроенных интеграциях с системами уведомлений; - Получение данных о существующих в системе задачах на сканирование; - Получение данных и управление сводными и детальными отчетами; - Получение данных о подключенных сканерах; - Создание задач на сканирование; - Получение данных о задачах на сканирование и их статусах; - Получение данных об обнаруженных в образе уязвимостях, ошибках конфигурации, конфиденциальных данных и вредоносном ПО; - Получение данных о доступных данной роли пользователя эндпойнтах; - Получение данных об областях применения; - Получение списка всех обнаруженных уязвимостей; - Получение данных о конкретной уязвимости; - Получение данных об узлах кластера; - Управление сканированием узлов кластера. - Получение данных об объектах RBAC кластера - Получение данных о рабочей нагрузке (англ. workload) для образа контейнера (кластер, пространство имен, под). - Получение информации о типе интеграции (созданная вручную или автоматически) при запросе списка интегрированных реестров образов. - Получение списка контейнеров для определенного узла. В Системе должен быть заложен механизм аудита системных вызовов (syscalls) узлов кластера. Система должна предусматривать возможность интеграции с любыми SIEM-системами, поддерживающими прием сообщений в CEF формате по протоколу syslog со следующим функционалом: - настройка интеграции с различными инстансами с помощью пользовательского интерфейса; - определение параметров для отправки системных событий разных категорий (Администрирование, Алерты, CI/CD, Политики, Ресурсы, Сканеры, Контроллер доступа, События контейнеров, Доступ на основе ролей, API) с указанием инстансов получателей; - определение параметров для отправки событий контейнеров в отношении сетевого трафика (входящего и исходящего), файловых операций, запускаемых процессов. Система должна предоставлять возможность интеграции с внешним хранилищем секретов HashiCorp Vault: - Чтение предварительно созданных секретов для компонентов защиты для контейнеров; - Использование Vault PKI для создания TLS-сертификатов, которые используются для межсервисного взаимодействия. Система должна предоставлять встроенные инструменты для выполнения проверок состояния компонентов (механизм Health Check), а именно: - визуализация состояния компонентов кластера; - возможность просмотра информации о состоянии компонентов; - мониторинг heartbeat компонентов; - предоставление внешним системам информации по состоянию компонентов через механизм API; - уведомление целевых пользователей о потере жизнеспособности компонентов. Для автоматизации процессов обслуживания, обеспечения безопасности и надежности компонентов необходимо внедрение инструментов автоматизированного обслуживания и поддержки, что должно включать в себя: - настройки автоматического обновления компонентов; - алгоритмы автоматического восстановления работоспособности компонентов; - механизмы автоматического резервного копирования информации о компонентах. Система должна обеспечивать бесперебойный мониторинг инфраструктур до 10 000 сетевых узлов и до 40 000 уникальных образов в инфраструктуре. Должна быть обеспечена функциональная возможность визуализации связей различных ресурсов внутри пространств имен (namespaces) в кластерах, в том числе сетевого взаимодействия их компонентов, проблем безопасности компонентов. Система должна обеспечивать проверку образов контейнеров в Runtime: проверка на наличие уязвимостей, секретов и вредоносного ПО. Система должна обеспечивать защиту от файловых угроз во время выполнения контейнеров. Система должна обеспечивать проверку узлов кластера на наличие уязвимостей Система должна обеспечивать Runtime защиту ОС нод оркестратора от файловых угроз Должна быть предусмотрена реализация проверки узлов кластера на соответствие отраслевым стандартам, а также формирования сводных и детальных отчетов по результатам данной проверки. Должна быть предусмотрена возможность сканирования оркестратора на соответствие отраслевым стандартам безопасности кластеров, а также формирования сводных и детальных отчетов по результатам данной проверки. Система должна предоставлять возможность логировать изменения в объектах RBAC кластера Система должна обеспечивать возможность анализировать конфигурации компонентов контейнерной инфраструктуры, а именно: оценивать настройки и параметры контейнерной среды для обеспечения безопасности, производительности и надежности приложений и сервисов, развернутых с использованием этих конфигураций. Система должна обеспечивать сбор и проверку событий в среде исполнения: - сбор и анализ данных о событиях; - оповещение об инцидентах. Система должна контролировать запуск контейнеров в среде исполнения с целью не допускать запуска образов, не соответствующих политикам безопасности. Система должна обеспечить возможность предоставлять информацию о репутации сетевых соединений и блокировать соединения на основании полученной репутации Система должна предоставлять Агента защиты как самостоятельно функционирующего компонента на каждом узле (node) кластера без вмешательства в пользовательские контейнеры приложений для осуществления контроля безопасности в соответствии с настроенными политиками безопасности, в частности: - контроль безопасности среды выполнения контейнеров, запущенных на узлах; - мониторинг событий среды эксплуатации на соответствие политикам безопасности, блокирование действий, несоответствующих политикам. Система должна обеспечивать контроль безопасности в соответствии с настроенным политиками безопасности. Система должна обеспечивать возможность применения сценариев политики реагирования при обнаружении уязвимостей в образах. Система должна обеспечивать блокирование действий при несоответствии настроенным политикам безопасности; Система должна предотвращать выполнение определенных действий или использование определенных функций, которые могут нарушать установленные правила безопасности. Система должна обеспечивать контроль безопасности на узлах (nodes) в соответствии с настроенным политиками безопасности, в частности контролировать сетевое взаимодействие контейнеров кластера (технология extended Berkeley Packet Filter). Система должна обеспечивать возможность управления политиками безопасности и ограничениями на уровне приложений и сервисов внутри контейнеров, процессов и других ресурсов, которыми оперируют контейнеры (технология extended Berkeley Packet Filter). Система должна обеспечивать возможность контроля контейнеров во время выполнения (технология extended Berkeley Packet Filter), а именно: - контроль запуска приложений и сервисов внутри контейнеров; - контроль сетевой активности; - блокировка подозрительной активности (процессов и сетевого трафика). Система должна предоставлять возможность создания правил мониторинга процессов и сети (профилей среды выполнения) для ограничения работы контейнеров в части: - указания и применения параметров безопасного развертывания образов; - указания и применения параметров безопасного поведения приложений, развернутых из образов. Система должна обеспечивать возможность автоматического формирования профилей среды выполнения. Система должна фиксировать следующие базовые поля для всех событий, связанных с работой контейнеров: - дата и время наступления события; - идентификатор кластера k8s; - имя namespace в k8s; - имя пода: - имя контейнера; - образ контейнера, из которого запущен контейнер (ссылка на репозиторий вместе с тэгом); - уникальный идентификатор образа (хэш). Расширенные возможности регистрации событий контейнеров в отношении сетевого трафика (входящего и исходящего) должны включать: - протокол сетевой коммуникации; - источник и получатель сетевого пакета; - используемые источником и получателем порты. Расширенные возможности регистрации событий доступа (в т. ч. создания, удаления, открытия) к объектам файловой системы контейнера должны включать: - PID и PPID процесса, осуществившего доступ; - euid, egid процесса, осуществившего доступ; - имя и расположения файла в файловой системе контейнера, к которому осуществлялся доступ; - операция (чтение, запись, удаление). Расширенные возможности регистрации событий контейнеров в отношении запускаемых процессов должны включать: - PID и PPID процесса; - euid, egid процесса; - имя запускаемого исполняемого файла (с полным путем расположения); - полный вывод command (с аргументами). Система должна обеспечивать возможность проверки подписи образов и недопущения запуска контейнеров с невалидной подписью. Для проверки подписи контейнеров должна быть предусмотрена возможность интеграции с внешними валидаторами - Notary и/или CoSign. Система должна предоставлять возможность оптимизации скорости работы с динамическим контроллером доступа (англ. Dynamic Admission Controller, DAC). Должна быть предусмотрена возможность: - отключения проверки хеша образа в реестре образов для ускорения проверки с применением политик безопасности (проверки на соответствие образов требованиям и незарегистрированных образов). - кеширования результатов сканирований на стороне агента kube-agent для ускорения обработки обращений DAC до 300 мс. Система должна предоставлять возможность настройки параметров ротации (удаления) данных, которые хранятся в S3-хранилище, с помощью квот: по времени или по уровню заполнения S3-бакета. Система должна предоставлять возможность настройки очередности выполнения заданий на сканирование. Система должна предоставлять возможность создания пользовательских политик безопасности образов (Assurance policies), политик контроля доступа (Admission controller policies) и пользовательских стандартов (Benchmark frameworks) с использованием языка CEL. Система должна поддерживать экспорт полной конфигурации (политики, группы агентов, профили и др.) в зашифрованном или открытом виде и импорт её на другие экземпляры решения через утилиту для Linux/Windows/macOS. Система должна обеспечивать динамическое обновление конфигурации групп агентов без переустановки подов node-agent, с мгновенным применением изменений. Система должна предоставлять возможность просмотра отсканированных образов в виде SBOM форматах SPDX и CycloneDX через интерфейс и API. Система должна поддерживать установку агентов безопасности на узел управления для аудита компонентов узла и централизованного контроля всей инфраструктуры Система должна обеспечивать возможность получения уведомлений с использованием политик реагирования и SIEM-систем, если ядро решения теряет связь с агентами в обслуживаемых кластерах. Система должна обеспечивать разграничение доступа к результатам проверок в CI согласно областям видимости проектов. Система должна обеспечивать разграничение доступа к данным на информационной панели с учётом областей применения и прав доступа пользователя. Система должна предоставлять возможность получения детальной информации по сканированиям (например, метрики производительности сканеров, проведенные сканирования за определенный промежуток времени, тип ОС, дата последнего сканирования и т. д.) через API. Система должна предоставлять API для получения необработанных (raw) событий безопасности. Система должна позволять сканировать образ по прямому пути, без предварительного поиска в реестре. Система должна поддерживать построение автопрофилей без учёта текущих политик среды выполнения. 2.2. Требования к интерфейсу Консоль управления системы должно быть реализовано как WEB-приложение с интуитивно понятным для целевого пользователя интерфейсом. Консоль управления Системой должна состоять из следующих элементов: - Главное меню. Разделы и подразделы главного меню должны обеспечивать доступ к рабочим функциям решения. - Рабочая область. Информация и элементы управления в рабочей области должны зависеть от раздела или подраздела, выбранного в главном меню. Автоматически подгружаться в пользовательский интерфейс программного обеспечения должны: - результаты сканирования собранного образа в процессе CI/CD; - перечень просканированных образов из подключенных реестров образов; - визуализация связей различных ресурсов внутри пространств имен (namespaces) в кластерах; - результаты сканирования нод кластеров - информация об обнаруженных уязвимостях в нодах кластеров - информация о событиях обнаружения вредоносного ПО в нодах кластеров - Информация об объектах RBAC - информация о соответствии отраслевым стандартам - журнал событий контейнеров и узлов кластеров - информация о принятых рисках; - перечень и настройки политик безопасности; - результаты сканирования образов из подключенных реестров образов; - информация об обнаруженных уязвимостях; - информация о слоях определенного образа и найденных в каждом слое уязвимостях; - информация о ресурсах (компонентах) определенного образа и найденных в них уязвимостях; - информация об обнаруженных в определенном образе секретах; - информация об обнаруженном в определенном образе вредоносном ПО; - информация об обнаруженных в определенном образе ошибках конфигурации - история сканирования определенного образа; - настройки интеграций с реестрами образов; - настройки интеграций со средствами нотификации; - настройки интеграции с LDAP; - настройки интеграции с SSO; - настройки интеграции с ИИ-инструментом или со внешними LLMмоделями - настройки интеграции с SIEM-системой; - настройки модулей проверки подписей образов - настройки по управлению доступом; - настройки авторизации. - настройки очередности выполнения заданий на сканирование - настройки политик безопасности; - журнал событий безопасности; - отчетные формы Системы; - настройки лицензирования; - настройки по управлению ролевой моделью и областями видимости; - информация о компонентах Системы 2.3. Требования к надежности Система должна быть способна функционировать бесперебойно в среде оркестрации Kubernetes, OpenShift. Решение должно обладать возможностью масштабирования под архитектуру Заказчика с большими инфраструктурами. Система должна обеспечивать бесперебойное функционирование после развертывания в облачных окружениях, таких как Yandex Cloud, Amazon AWS EKS, Microsoft Azure AKS. 2.4. Требования к установке Должны быть предусмотрены следующие схемы развертывания: - развертывание в открытом контуре корпоративной сети; - развертывание в закрытом контуре корпоративной сети. Продукт должен устанавливаться с использованием унифицированного средства Helm, позволяющего автоматизировать запуск приложений в среде Kubernetes. Система должна предоставлять возможность установки Агента защиты как самостоятельно функционирующего компонента на каждом узле (node) кластера. Примечание: в закрытом контуре корпоративной сети также должен быть предусмотрен сценарий развертывания с использованием прокси-сервера. 2.5. Требования к архитектуре При использовании внешних систем управления базами данных защиты для контейнеров должен поддерживать возможность работы со следующими СУБД: - ClickHouse v25.* - PostgreSQL (Postgres Pro Standard/Enterprise) 15, 17, 18 - Pangolin 6.2.0. Защита для контейнеров должен поддерживать следующие версии Linux-дистрибутивов и версий ядер ОС Linux для реализации мониторинга среды выполнения с использованием профилей среды выполнения контейнеров: - CentOS 8.2.2004 + ядро 4.18.0-193. - Ubuntu 18.04.2 + ядро 4.18.0. - Debian 10 + ядро 4.19.0. - RHEL 9.4 + ядро 5.14. - Red Hat Enterprise Linux CoreOS 416.94.202408200132-0 + ядро 5.14.0-427.33.1.el9_4.x86_64. 3. Требования к гарантийному обслуживанию Гарантия должна составлять не менее 12 месяцев. 4. Требования к технической поддержке Поставщик должен обеспечить Систему технической поддержкой сроком не менее 12 месяцев и не менее чем в режиме 5x8 (рабочие часы с 9:00 до 18:00, в рабочие дни с понедельника по пятницу). Такая стандартная поддержка должна позволять бесплатное решение проблем, связанных с эксплуатацией Системы и бесплатное обновление Системы (получение новых версий ПО и/или движков или исправления). Для решения проблем при эксплуатации Системы Поставщик должен предоставлять электронный сервис (веб-портал, специальный email-адрес, мобильное приложение и т. д.) для создания заявок от Заказчика или его представителей с автоматической регистрацией таких заявок в системе поддержки. Такой сервис должен иметь функционал подтверждения создания заявок, изменений статуса заявок и т.п. Работа с таким сервисом и коммуникация с представителями Поставщика должна быть доступна на казахском или русском, или английском языке. Поставщик должен предоставлять открытый доступ (без какой-либо предварительной регистрации) к технической документации и документации по администрированию системы в сети Интернет. 5. Требования к подтверждающим документам, представляемым в составе заявки на участие в тендере Потенциальный поставщик в составе заявки на участие в тендере представляет: – копию письма (сертификата, свидетельства) от производителя предлагаемой Системы либо его официального представителя (дилера или дистрибьютора), подтверждающего право потенциального поставщика на поставку продукции данного производителя на территории Республики Казахстан в рамках настоящей закупки, с указанием наименования Заказчика и номера закупки. В случае представления письма официального представителя (дилера или дистрибьютора) дополнительно представляется копия документа производителя, подтверждающего статус данного официального представителя на территории Республики Казахстан.
Сопутствующие услуги (указываются при наличии) (монтаж, наладка, обучение, проверки и испытания товаров)	Поставщик должен обеспечить внедрение Системы и обучение 2-х сотрудников Заказчика по настройке и работе с Системой В рамках внедрения Системы, должны быть выполнены следующие мероприятия: - Разработка и согласование схемы развертывания Системы с учётом подготовленной инфраструктуры Заказчика и требований настоящей технической спецификации. ; - Инсталляция согласно разработанной и согласованной архитектуры; - Разработка, настройка и адаптация политик и правил.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о закупках (указываются при наличии) (потенциальный поставщик за не указание и непредставление указанных сведений не отклоняется)	

* сведения подтягиваются из плана закупок (отображаются автоматически).

Примечание:

1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.

2. Квалификационные требования, предъявляемые потенциальным поставщикам в иных документах не устанавливаются.