

**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 №	№ 17798036-1
Тендердің атауы	Тауарды электрондық сатып алу желілік трафикті талдау жүйесі
Лоттың №	№ 88200802-ОТ1
Лоттың атауы	Деректерді жіберу желісі трафигін талдау және өңдеу үшін жабдық
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*	263030.900.000045
Тауардың атауы*	Деректерді жіберу желісі трафигін талдау және өңдеу үшін жабдық
Өлшем бірлігі*	Комплект
Саны (көлемі)*	1
Бірлік бағасы, қосылған құн салығын қоспағанда*	117613663.79
Қосылған құн салығын қоспағанда, сатып алуға бөлінген жалпы сома*	117613663.79
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 60 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 функционалдықы, техникалық, сапалық, өнімділігі мен басқа да сипаттамаларының сипатталуы	ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК Желілік трафикті талдау жүйесі (NTA) 1. Жалпы мәліметтер Желілік трафикті талдау жүйесі (бұдан әрі — Жүйе) желілік қауіптерді және зиянды бағдарламалық қамтамасыз етуді жасаңды интеллекте пен машиналық оқыту технологияларын қолдана отырып (оның ішінде «нөлдiк күн» қауіптері мен бүркемеленген шабуылдарды) анықтауға арналған. Бұл ретте сегментішілік (east-west) және сыртқы (north-south) трафикті басымдықпен талдау көзделеді, ал деректер тек Тапсырыс берушінің желілік инфрақұрылымы шегінде өңделеді: трафик пен метадеректер Тапсырыс берушінің желісі шегінен шықпауға тиіс. Жүйе аппараттық-бағдарламалық кешен (АБК) форматында жеткізілуі тиіс. Жүйе қосымша коннекторларды, аралық сервистер мен серверлерді пайдаланбай, қолданыстағы инфрақұрылыммен интеграциялануы тиіс. 2. Жүйенің функционалдықы мүмкіндіктеріне қойылатын талаптар Жүйе мынадай функционалдықы қолдауы тиіс: - Деректерді және трафикті желілік инфрақұрылым шегінен тыс берусіз жергілікті (on-premises) орналастыру; - Орталықтандырылған және бөлінген архитектуралар үшін Standalone (дербес) және Sensor (сенсор) орналастыру режимдері; - Гибридті тәсіл негізінде желілік ауытқуларды және файлдық зиянды бағдарламалық қамтамасыз етуді анықтау: қолтанбалық антивирустық қозғалтқыш және жасаңды нейрондық желі (ANN) негізіндегі патенттелген жіктеу тетігі; - Басқару арналарын (Command-and-Control), ботнеттерді, әлсіз және қауіпсіз емес шифрларды, сондай-ақ желідегі компрометация индикаторларын (IoC) анықтау; - North/South және East/West бағыттарындағы басым кірулерді дәл анықтау; - Жалған іске қосылулар санын Тапсырыс берушінің трафигін ескере отырып азайту үшін жергілікті (on-premises) қайта оқытумен және бейімдеумен машиналық оқыту негізінде трафикті профильдеу; - Автоматтандырылған ден қою іс-қимылдары (карантин) үшін сол өндірушінің қорғау құралдарымен (желіаралық экран, NAC, коммутатор), сондай-ақ API арқылы үшінші тарап жүйелерімен интеграция; - Күдікті файлдарды алдын ала және динамикалық (детонациялық) талдау үшін құмсалғышпен (sandbox) интеграция; - Журналдар мен есептерді орталықтандырылған журналдау жүйесіне, SIEM және SOAR жүйелеріне экспорттау; - Қауіпсіздік аналитикасы мақсаттары үшін машиналық оқытуды қолдана отырып NetFlow деректерін қабылдау және талдау; - Оқиғаларды торап және құрылғы туралы деректермен байыту үшін Active Directory (AD) жүйесімен интеграция; - SOC талдаушыларына түсетін жүктемені азайту мақсатында инциденттерді, ауытқуларды және бастапқы себептерді талдауды автоматтандыратын «виртуалды қауіпсіздік талдаушының» функциясы; - IPv6 хаттамасын қолдау; - Пайдалы жүктемені ұстау және сақтаудың (payload capture/storage) кіріктірілген функциясы, сондай-ақ үшінші тараптың жоғары жылдамдықты ұстау платформаларын пайдалану мүмкіндігі; - Желілік ауытқуларды талдау адросының мынадай хаттамаларды қолдауы: TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL; - Желілік ауытқуларды талдау адросының NetFlow хаттамасын қолдауы; - Зиянды бағдарламалық қамтамасыз етудің (ЗБК) миллиондаған қасиеттері мен көрсеткіштері бойынша оқытылған кіріктірілген жасаңды нейрондық желілер (ANN) жиынтығын пайдалана отырып ЗБК-ны талдауды қолдау; - «Нөлдiк пациентті» айқындау, өндірушінің Outbreak дерекқорлары (хэш, ЗБК отбасы) бойынша іздеу, желідегі ЗБК-ны және оның нұсқаларын айқындау үшін Scenario-Based, Outbreak Search, Similarity қозғалтқыштарын қолдау; - ЗБК-ны талдау адросының мынадай файл түрлерін қолдауы: 32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, Hangul Office, TAR, XZ, GZIP, BZIP2, RAR, LZH, LZW, ARJ, CAB, 7Z, PHP, XML, POWERSHELL, BAT, HTA, UPX, ACTIVEMIME, MIME, HLP, BASE64, BINHEX, UUE, FSG, ASPACK, GENSRIPT, SHELLSCRIPT, PERLSRIPT, MSC, PETITE, ACCESS, SIS, HOSTS, NSIS, SISX, INF, EZ2IMAGE, FATMACH, CPIO, AUTOIT, MSOFFICEX, OPENOFFICE, TNEF, SWF, UNICODE, PYARCH, EGG, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, LNK, KGB, Z, ACE, JAR, APK, MSI, MACH O, DMG, DOTNET, XAR, CHM, ISO, CRX, INNO, TMX, FLAC, XXE, WORDML, WORDBASIC, OTF, WOFF, VSDX, EMF, DAA, GPG, PYTHON, CSS, AUTOITSCRIPT, RPM, EML, REGISTRY, PFILE, CEF, PRC, CLASS, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN; - Компрометация индикаторларын (IoC, Indicator of Compromise) CSV, PDF, STIXv2 форматтарында экспорттауды қолдау; - ЗБК шабуылын MITRE ATT&CK; матрицасына сәйкестендіруді қолдау, шабуылда қолданылған техникалар мен тактикаларды көрсету үшін шығысты сүзу мүмкіндігімен шабуылды MITRE ATT&CK; матрицасына графикалық түрде сәйкестендіруді бейнелеу; - Хосттарды сүзу үшін Allow / Deny тізімдерін қолдау; - Жасаңды нейрондық желілерді (ANN) пайдалана отырып жүргізілген талдау негізінде шабуыл сценарийлерінің ЗБК қасиеттерін қолдана отырып ЗБК-ны саралау мен жіктеуді мынадай тәсіспен қолдау: Industroyer, Wiper, Downloader, Redirector, Dropper, Ransomware, Worm, Password Stealer, Rootkit, Banking Trojan, InfoStealer, Exploit, Clicker, Virus, Application, CoinMiner, DoS, BackDoor, WebShell, Search Engine Poisoning, Proxy, Trojan, Phishing, Fileless; - ЗБК-ның өртүрлі түрлерін хосттың IP-мекенжайы бойынша жіктеу мүмкіндігі; - Файлсыз ЗБК-ны (хостқа орнатылмайтын, бірақ орталық процессор ресурстарын пайдалана отырып жедел жадта жұмыс істейтін ЗБК) жеке санатта жіктеу мүмкіндігі; - DNS-мекенжайлар мен IP-мекенжайлар негізінде ботнеттерді анықтау және айқындау мүмкіндігі, бот-желі атауын, көздер мен тағайындау мекенжайларын көрсетуді қолдаумен; - Машиналық оқыту (ML) әдістерін пайдалана отырып трафикті профильдеу және желілік ауытқуларды сәйкестендіру мүмкіндігі; - Зиянды Web-белсенділікті анықтау және атау мүмкіндігі (құрылғыларды және пайдаланушы URL-мекенжайларын анықтау, ЗБК бар-жоғына сканерлеумен қатар зиянды Web-белсенділікті іздеу), Web-ресурстар санаттары бойынша жіктеумен; - Кіріктірілген шабуылдарды анықтау және болдырмау жүйесі (IPS) арқылы желілік шабуылдарды анықтау мүмкіндігі; - Желіде берік емес криптографиялық шифрлар мен хаттамалардың пайдаланылуын анықтау мүмкіндігі, сессияның көзі мен тағайындалуын графикалық интерфейсте көрсетумен; - ЗБК-ны виртуалды талдаушы функционалы арқылы ЗБК талдауын автоматтандыру мүмкіндігі, ЗБК жіктелімін, сенімділік деңгейін, шабуыл көзі мен тағайындалу IP-мекенжайларын, желідегі тарихын және ЗБК қасиеттері бойынша жіктелімін көрсететін ЗБК талдау әдістерін автоматты түрде қалыптастырумен; - Шабуылдың уақыт бойынша даму тәсібін графикалық түрде бейнелеу және шабуыл көзін қадағалау мүмкіндігі; - Web-ресурстардан ЗБК-ның алғашқы үлгісінің жүктелуіне жол бермеу мүмкіндігі, inline blocking қолдауы; - Желіде және файлдарда ЗБК анықталған кезде ден қою іс-қимылдарын қолдану үшін сыртқы жүйелермен интеграцияны қолдау, бұрын енгізілген Fortinet шешімдерімен және үшінші тарап жүйелеріне арналған API шақыруларымен; 3. Жүйені әкімшілендіруге және басқаруға қойылатын талаптар Жүйе әкімшілендіру мен басқарудың мынадай функционалын қолдауы тиіс: - Жүйе әкімшілері үшін екі факторылы аутентификацияны қолдау; - LDAP, RADIUS хаттамаларын пайдалана отырып әкімшілердің аутентификациясын қолдау; - Жүйені әкімшілендірудің рөлдік моделін (RBAC, Role Based Access Control) қолдау; - Браузерді пайдалана отырып графикалық интерфейс (GUI) арқылы жүйені толық басқаруды қолдау; - Автоматтандыру, файлдарды беру және жүйеге сұрау нәтижелерін алу үшін REST API қолдауы; - Жүйе әкімшілеріне SMTP хаттамасы бойынша электрондық пошта арқылы хабарламалар жіберуді қолдау; - SNMP хаттамасы арқылы жүйені желілік мониторингтеуді, оның ішінде SNMP Traps көмегімен хабарламалар жіберуді қолдау; - Оқиғалар журналдарын SYSLOG хаттамасы бойынша сыртқы жүйелерге жіберуді қолдау; - STIX/JSON (ЗБК) форматында жергілікті журналдауды қолдау; - Жүйе журналдарын SIEM жүйесіне экспорттауды қолдау; - Статикалық IP-маршруттауды қолдау; 4. Жүйенің аппараттық бөлігінің техникалық сипаттамалары: Жүйе мынадай сипаттамаларға ие болуы тиіс: Орналастыру және интеграция; - Орналастыру режимі: Standalone, Sensor; - Sniffer / SPAN / 802.1q қолдауы; - IPv6 қолдауы; - Қауіпсіздік экожүйесімен интеграция: желіаралық экрандар / NAC / коммутаторлар / құмсалғыштар; - NetFlow қолдауы; - Пайдалы жүктемені ұстау және сақтау нативті түрде қолдау табуы тиіс; сондай-ақ үшінші тараптың жоғары жылдамдықты ұстау платформаларын қолдау көзделуі тиіс. Шаcси және интерфейстер: - Пішін-фактор: кемінде 2U, сөреге монтажалалады; - Интерфейстердің жалпы саны: кемінде 2x 10G SFP+ (sniffer); 2x 10G SFP+ (басқару және резерв); 2x RJ45 (HA); 1x RJ45 (консоль); - Трафикті ұстау интерфейстері (sniffer): кемінде 2x 10G SFP+ (оптика немесе мыс; трансиверлер Жүйені жеткізу жиынтығына кіруі тиіс); - Сақтау көлемі: кемінде 2x 7,68 TB (RAID 1), пайдалы көлемі 7,68 TB, жинақтауштар алынбалы және ыстық ауыстыру мүмкіндігімен; - Әдепкі RAID деңгейі: RAID 1 (бағдарламалық RAID); - Коректендіру блогы: резервтелген, ыстық ауыстыру мүмкіндігімен. Өнімділік; - Талдаудың өткізу қабілеті (аралас корпоративтік трафик): кемінде 7,5 Гбит/с; - NetFlow өңдеу жылдамдығы: кемінде секундына 100 000 ағын; - Зиянды бағдарламалық қамтамасыз етуді талдаудың өткізу қабілеті: кемінде сағатына 170 000 файл; - Зиянды бағдарламалық қамтамасыз етуді жіктеу санаттарының саны: кемінде 26; Жіктеу технологиясы: жабық өндірістің анықтаудың негізгі алгоритмі ретінде іске асырған жасаңды нейрондық желі (ANN) негізіндегі жіктеу тетігі; функционалдықы жағынан баламалы, бірақ техникалық тұрғыдан өзгеше іске асырылған жіктеу тетіктері сәйкес келетіндер ретінде қараламайды. Физикалық және климаттық сипаттамалар: Габариттері (Б x Е x Т): 88,9 x 444,5 x 574,0 мм-ден аспайды. Массасы: 16 кг-нан аспайды. Айнымалы токпен коректендіру: кемінде 100-240 В AC, кемінде 50-60 Гц. Энергия тұтыну: 163 Вт-тан аспайды (бос жүрісте) / 345 Вт-тан аспайды (толық жүктеме кезінде). Жылу бөлу: кемінде сағатына 1207,5 БТЕ. Жұмыс температурасы: 0°C-тан 40°C-қа дейін, жабыққа тікелей күн сәулесінің түсуінен. Сақтау температурасы: -20°C-тан 70°C-қа дейін. Ылғалдылық: 5%-дан 90%-ға дейін, конденсациясыз. Трансиверлерге қойылатын талаптар: - Мыс SFP+ трансивері — саны: кемінде 2 (екі) дана. Модуль түрі: SFP+, 10GBASE-T, деректерді беру жылдамдығы кемінде 10 Gbps, беру ортасы — мыс интерфейсі (Cat6A немесе одан жоғары кабель), беру қашықтығы — кемінде 30 м, айырғыш түрі — RJ-45; - Оптикалық SFP+ трансивері — саны: кемінде 5 (бес) дана. Модуль түрі: SFP+, 10GBase-SR, деректерді беру жылдамдығы кемінде 10 Gbps, беру ортасы — көпмодалы оптикалық талшық, толқын ұзындығы кемінде 850 нм, беру қашықтығы — кемінде 300 м (OM3) / 550 м (OM4), айырғыш түрі — дуплексті LC; 5. Жеткізуге қойылатын талаптар Жүйе бір өндірушіден бірыңғай жиынтықпен, өртүрлі өндірушілердің позицияларынан жинақталмай жеткізілуі тиіс. Құрамы мынадай: Осы техникалық ерекшеліктің 4-тарауында көрсетілген техникалық талаптарға жауап беретін АБК; Ұсынылатын құрылғыда қолданылатын NetFlow талдауын қолдау; Осы техникалық ерекшеліктің 4-тарауында көрсетілген егжей-тегжейлі талаптар мен санына сәйкес 10G SFP+ порттарына арналған трансиверлер (трафикті ұстау және басқару). Жүйенің аппараттық бөлігі өндірістен алынбаған және end-of-sale/end-of-life мәртебесінде тұрмаған, ағымдағы сериялық шығарылымдағы модель болуы тиіс және лицензиялар мен сервистермен бірге бірыңғай зауыттық жеткізу жиынтығы ретінде, өртүрлі көздерден жиналған жеке позициялар түрінде емес жеткізілуі тиіс. 6. Кепілдік қызмет көрсетуге қойылатын талаптар Кепілдік Жеткізу қойылған күннен бастап кемінде 12 айды құрауы тиіс. Жеткізуші қолдауға арналған премиум жазылмды қамту шарттарын (БҚ/қозғалтқыштарды жаңартуды, жабыққа арналған RMA шарттарын және техникалық қолдаудың SLA-сын қоса алғанда) көрсетуі тиіс. Жеткізуші өндірушінің техникалық қолдауы мен fitmware және қозғалтқыштар жаңартуларының техникалық қолдаудың бүкіл қолданылу мерзімі ішінде қолжетімділігін растауы тиіс. 7. Техникалық қолдауға қойылатын талаптар Жеткізуші Жүйені кемінде 12 ай мерзімге және кемінде 5x8 режимінде (жұмыс уақыты дүйсенбіден жұмаға дейінгі жұмыс күндері сағат 9:00-ден 18:30-ға дейін) техникалық қолдаумен қамтамасыз етуі тиіс. Мұндай стандартты қолдау Жүйені пайдалануға байланысты проблемаларды тегін шешуге және Жүйені тегін жаңартуға (БҚ және/немесе қозғалтқыштардың жана 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.) ұсынуды 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 ағылшын немесе қазақ, немесе орыс тілінде қолжетімді болуы тиіс. Жеткізуші Интернет желісінде жүйені техникалық құжаттамасына және әкімшілендіру жөніндегі құжаттамаға алдын ала тіркеусіз ашық қолжетімділікті қамтамасыз етуі тиіс. 8. Тендерге қатысу өтінімінің құрамында ұсынылатын растайтын құжаттарға қойылатын талаптар Өлеуетті 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, куәліктің) көшірмесін. Ресми өкілдің (дилердің немесе дистрибьютордың) хаты ұсынылған жағдайда, қосымша осы ресми өкілдің Қазақстан Республикасының аумағындағы мәртебесін растайтын өндіруші құжатының көшірмесі ұсынылады;
Ілеспе қызметтер (қажет 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-шаралар орындалуы тиіс: - Тапсырыс берушінің талаптарына, инфрақұрылым ерекшеліктеріне және үздік практикаларға сәйкес архитектураны әзірлеу; - Әзірленген және келісілген архитектураға сәйкес орнату; - Саясаттар мен қағидаларды әзірлеу, баптау және бейімдеу;

Өлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Өлеуетті 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.

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Национальная компания "КазАвтоЖол"
Наименование организатора	Филиал "Дирекция платных автомобильных дорог" АО "Национальная компания "КазАвтоЖол"
№ тендера	№ 17798036-1
Наименование тендера	Электронные закупки товара система анализа сетевого трафика
Номер лота	№ 88200802-ОТ1
Наименование лота	Оборудование для анализа и обработки трафика сетей передачи данных
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*	263030.900.000045
Наименование товара*	Оборудование для анализа и обработки трафика сетей передачи данных
Единица измерения*	Комплект
Количество (объем)*	1
Цена за единицу, без учета налога на добавленную стоимость*	117613663.79
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*	117613663.79
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 60 календарных дней.
Размер авансового платежа*	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов накупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристикикупаемых 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 анализа сетевого трафика (NTA) 1. Общие сведения Система анализа сетевого трафика (далее — Система) предназначена для обнаружения сетевых угроз и вредоносного ПО с использованием технологий искусственного интеллекта и машинного обучения (в том числе угроз «нулевого дня» и замаскированных атак), с приоритетным анализом внутрисегментного (east-west) и внешнего (north-south) трафика, с обработкой данных исключительно в пределах сетевой инфраструктуры Заказчика — трафик и метаданные не должны покидать сеть заказчика. Система должна предоставляться в формате аппаратно-программного комплекса (АПК). Система должна интегрироваться с текущей инфраструктурой без использования дополнительных коннекторов и промежуточных сервисов и серверов. 2. Требования к функциональным возможностям Системы Система должна поддерживать следующий функционал: - Локальное (on-premises) развертывание без передачи данных/трафика за пределы сетевой инфраструктуры. - Режимы развертывания Standalone (автономный) и Sensor (сенсор) — для централизованных и распределенных архитектур. - Обнаружение сетевых аномалий и файлового вредоносного ПО с использованием гибридного подхода: сигнатурный антивирусный движок и патентованный механизм классификации на основе искусственной нейронной сети (ANN). - Обнаружение каналов управления (Command-and-Control), ботнетов, слабых/небезопасных шифров, а также индикаторов компрометации (IoC) в сети. - Точное обнаружение вторжений в направлениях North/South и East/West. - Профилирование трафика на основе машинного обучения с локальным (on-premises) дообучением/адаптацией для снижения количества ложных срабатываний с учётом трафика заказчика. - Интеграция со средствами защиты того же производителя (межсетевой экран, NAC, коммутатор) для автоматизированных действий реагирования (карантин), а также со сторонними системами через API. - Интеграция с песочницей (sandbox) для предварительного и динамического (детонационного) анализа подозрительных файлов. - Экспорт журналов и отчётов в централизованную систему логирования / SIEM / SOAR. - Приём и анализ данных NetFlow с применением машинного обучения для целей аналитики безопасности. - Интеграция с Active Directory (AD) для обогащения событий данными об узле/устройстве. - Функция «виртуального аналитика безопасности», автоматизирующая анализ инцидентов, аномалий и первопричин с целью снижения нагрузки на аналитиков SOC. - Поддержка IPv6. - Встроенная функция захвата и хранения полезной нагрузки (payload capture/storage), с возможностью использования сторонних плат высокоскоростного захвата. - Поддержка ядра анализа сетевых аномалий следующих протоколов: TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTPSP, RPC, SIP, RDP, SNMP, MySQL, MSSQL, PGSQL. - Поддержка ядра анализа сетевых аномалий протокола NetFlow. - Поддержка анализа вредоносного ПО (BPO) с использованием встроенного множества искусственных нейронных сетей (ANN), прошедших тренировки на миллионах свойств и показателей BPO. - Поддержка движков Scenario-Based, Outbreak Search, Similarity для определения «нулевого пациента», поиска по базам данных производителя Outbreak (хэш, семейство BPO), определения BPO и его вариантов в сети. - Поддержка ядра анализа BPO следующих типов файлов: 32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, Hangu, Office, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW, ARJ, CAB, 7z, PHP, XML, POWERSHELL, BAT, HTA, UPX, ACTIVEMIME, MIME, HLP, BASE64, BINHEX, UUE, FSG, ASPACK, GENSRIPT, SHELLSCRIPT, PERLSRIPT, MSC, PETITE, ACCESS, SIS, HOSTS, NSIS, SISX, INF, E32IMAGE, FATMACH, CPIO, AUTOIT, MSOFFICEX, OPENOFFICE, TNEF, SWF, UNICODE, PYRARCH, EGG, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, LNK, KGB, Z, ACE, JAR, APK, MSI, MACH O, DMG, DOTNET, XAR, CHM, ISO, CRX, INNO, THMX, FLAC, XHE, WORDML, WORDBASIC, OTF, WOFF, VSDX, EMF, DAA, GPG, PYTHON, CSS, AUTOITSRIPT, RPM, EML, REGISTRY, PFIFE, CEF, PRC, CLASS, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN. - Поддержка экспорта индикаторов компрометации (IoC, Indicator of Compromise) в форматах CSV, PDF, STIXv2 - Поддержка сопоставления атаки BPO на матрицу MITRE ATT&CK, отображение в графическом виде сопоставления атаки на матрицу MITRE ATT&CK; с возможностью обеспечения фильтрации вывода для отображения техник и тактик, используемых в атаке. - Поддержка списков Allow / Deny для фильтрации хостов. - Поддержка следующего списка дифференциации и классификации BPO с использованием свойств BPO сценариев атак на основе анализа с использованием искусственных нейронных сетей (ANN): Industroyer, Wiper, Downloader, Redirector, Dropper, Ransomware, Worm, Password Stealer, Rootkit, Banking Trojan, InfoStealer, Exploit, Clicker, Virus, Application, CoinMiner, DoS, BackDoor, WebShell, Search Engine Poisoning, Proxy, Trojan, Phishing, Fileless. - Возможность классификации различных типов BPO в разрезе IP-адреса хоста. - Возможность классификации бесфайлового BPO (BPO, не устанавливаемого на хост, но оперирующего в оперативной памяти с использованием ресурсов центрального процессора) в отдельной категории. - Возможность обнаружения и определения ботнетов на основе DNS-адресов, IP-адресов с поддержкой показа имени бот-сети, адресов источников и адресов назначения. - Возможность профилирования трафика с использованием методов машинного обучения (ML) и идентификации сетевых аномалий. - Возможность детектирования и именования вредоносных Web активностей (детектирование устройств / пользовательских URL и поиска вредоносных Web активностей, наряду со сканированием на предмет наличия BPO) с классификацией по категориям Web ресурсов. - Возможность детектирования сетевых атак с помощью встроенной системы обнаружения и предотвращения атак (IPS). - Возможность обнаружения использования нестойких крипто шифров и протоколов в сети с отображением источника и назначения сессии в графическом интерфейсе. - Возможность использования автоматизации анализа BPO с помощью функциональности виртуального аналитика BPO с автоматизацией генерации отчётности анализа BPO, отображающей классификацию BPO, уровень уверенности, IP-адреса источника и назначения атаки, историю в сети и разбивку по свойствам BPO. - Возможность отображения цепи развития атаки во времени с отслеживанием источника атаки в графическом виде. - Возможность предотвращения загрузки первого образа BPO с web-ресурсов, поддержка inline blocking. - Поддержка интеграции с внешними системами для использования ответных действий при обнаружении BPO в сети и файлах с ранее внедренными решениями Fortinet и вызовы API для сторонних систем. 3. Требования к администрированию и управлению системой Система должна поддерживать следующий функционал администрирования и управления: - Поддержка двухфакторной аутентификации для администраторов системы - Поддержка аутентификации для администраторов с использованием протоколов LDAP, RADIUS. - Поддержка ролевой модели администрирования системы (RBAC, Role Based Access Control). - Поддержка полного управления системой посредством графического интерфейса (GUI) с использованием браузера. - Поддержка REST API для автоматизации, подачи файлов и получения результатов запроса в систему. - Поддержка рассылки уведомлений для администраторов системы по электронной почте по протоколу SMTP. - Поддержка сетевого мониторинга системы посредством протокола SNMP, в том числе рассылка уведомлений с помощью SNMP Traps. - Поддержка отправки журналов событий на внешние системы по протоколу SYSLOG. - Поддержка локального журналирования в формате STIX/JSON (BPO). - Поддержка экспорта журналов системы в SIEM. - Поддержка статической IP маршрутизации. 4. Технические характеристики аппаратной части Системы: Система должна обладать следующими характеристиками: Развертывание и интеграция: - Режим развертывания: Standalone, Sensor. - Поддержка Sniffer / SPAN / 802.1q. - Поддержка IPv6; - Интеграция с экосистемой безопасности: межсетевые экраны / NAC / коммутаторы / песочницы; - Поддержка NetFlow; - Захват / хранение полезной нагрузки: должна поддерживаться нативно; также должна быть поддержка сторонних плат высокоскоростного захвата. Шасси и интерфейсы: - Форм-фактор: не менее 2U, монтируется в стойку - Общее количество интерфейсов: не менее 2x 10G SFP+ (sniffer); 2x 10G SFP+ (управление и резерв); 2x RJ45 (HA); 1x RJ45 (консоль) - Интерфейсы захвата трафика (sniffer): не менее 2x 10G SFP+ (оптика или медь; трансиверы должны быть в комплекте поставки Системы) - Объём хранилища: не менее 2x 7,68 Tb (RAID 1), 7,68 Tb полезного объёма, накопители съёмные / с возможностью горячей замены. - Уровень RAID по умолчанию: RAID 1 (программный RAID). - Блок питания: Резервированный, с возможностью горячей замены. Производительность: - Пропускная способность анализа (смешанный корпоративный трафик): не менее 7,5 Гбит/с - Скорость обработки NetFlow: не менее 100 000 потоков/сек - Пропускная способность анализа вредоносного ПО: не менее 170 000 файлов/час - Количество категорий классификации вредоносного ПО: не менее 26 Технология классификации: Механизм классификации на основе искусственной нейронной сети (ANN), реализованный производителем оборудования как основной алгоритм обнаружения; функционально эквивалентные, но технически иначе реализованные механизмы классификации не рассматриваются как соответствующие Физические и климатические характеристики: Габариты (В x Ш x Г): не более 88,9 x 444,5 x 574,04 мм Масса: не более 16 кг Питание переменного тока: не менее 100-240 В AC, не менее 50-60 Вт Энергопотребление: не более 163 Вт (в простое) / не более 345 Вт (при полной нагрузке) Тепловыделение: не менее 1207,5 БТЕ/ч Рабочая температура: От 0°C до 40°, без прямого солнечного воздействия на оборудование Температура хранения: От -20°C до 70°C Влажность: От 5% до 90%, без конденсации Требования к трансиверам: - Медный трансивер SFP+ — количество: не менее 2 (двух) штук. Тип модуля: SFP+, 10GBASE-T, скорость передачи данных не менее 10 Gbps, среда передачи — медный интерфейс (кабель Cat6a или выше), дальность передачи — не менее 30 м, тип разъёма — RJ-45. - Оптический трансивер SFP+ — количество: не менее 5 (пяти) штук. Тип модуля: SFP+, 10GBase-SR, скорость передачи данных не менее 10 Gbps, среда передачи — многомодовое оптическое волокно, длина волны не менее 850 нм, дальность передачи — не менее 300 м (OM3) / 550 м (OM4), тип разъёма — duplexный LC. 5. Требования к поставке Система должна предоставляться единым комплектом от одного производителя, без сборки из позиций разных производителей, следующий состав: АПК отвечающее техническим требованиям, отраженным в главе 4 настоящей технической спецификации; Поддержка анализа NetFlow, действующая на предлагаемом устройстве; Трансиверы для портов 10G SFP+ (захват трафика и управление) согласно детальным требованиям и количеству, отраженным в главе 4 настоящей технической спецификации. Аппаратная часть Системы должна являться текущей серийно выпускаемой моделью, не снятой с производства и не находящейся в статусе end-of-sale/end-of-life, и должно поставляться совместно с лицензиями и сервисами, единым заводским комплектом поставки, а не отдельными позициями, собранными из разных источников. 6. Требования к гарантийному обслуживанию Гарантия должна составлять не менее 12 месяцев с поставки, Поставщик должен указать условия покрытия премиальной подписки на поддержку (включая обновления ПО/движков, условия RMA на оборудование и SLA технической поддержки). Поставщик должен подтвердить доступность технической поддержки производителя и обновлений firmwate/движков на весь срок действия технической поддержки. 7. 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 18:30, 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, измененный статус заявок и т.п. Работа с таким сервисом и коммуникация с представителями Поставщика должна быть доступна на казахском или английском, или русском языке. Поставщик должен предоставлять открытый доступ (без какой-либо предварительной регистрации) к технической документации и документации по администрированию системы в сети Интернет. 8. Требования к подтверждающим документам, предоставляемым 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 предоставления письма официального представителя (дилера или дистрибьютора) дополнительно предоставляется 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 архитектуры согласно требованиям Заказчика, особенностей инфраструктуры и лучших практик; - Установка 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.