Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	Қазақстан Республикасының Көлік министрлігі Автомобиль жолдары комитетінің «Жол активтері сапасының ұлттық орталығы» шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорны
Ұйымдастырушының атауы:	Қазақстан Республикасының Көлік министрлігі Автомобиль жолдары комитетінің «Жол активтері сапасының ұлттық орталығы» шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорны
Конкурстың №:	№ 17891305-1
Конкурстың атауы:	Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Лоттың нөмірі:	№ 88092853-ОК1
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:	8586206
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	8586206
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	

Қызмет көрсету мерзімі	Техникалық ерекшелік талаптарына сәйкес
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Функционалдық талаптар: 5 Функционалдық талаптар • Тапсырыс беруші инфрақұрылымының желілік құрылғыларынан коллектор-серверге жіберілген flow (ағындар) трафигін талдауды қолдау. Қолдау көрсетілетін протоколдардың түрлері төменде, «Функционалдық талаптар» бөлімінде тізілген. • Егер Тапсырыс беруші инфрақұрылымының желілік жабдығында қолдау көрсетілетін flow протоколдарын генерациялау және жіберу функционалы болмаса, 1 Гб/с жылдамдықта SPAN трафигін қабылдау және жүйе қолдайтын flow протоколына инкапсуляциялау арқылы арнайы құрылғы — зондпен flow трафигін генерациялау мүмкіндігі қарастырылуы тиіс. Жеткізу шеңберінде коллекторға кіріктірілген 1 (бір) зонд қарастырылуы тиіс. • Бірнеше интерфейсте трафикті талдауды қолдау • «Шикі» SPAN трафигін мониторингтеуді қолдау • NetFlow v5 мониторинг протоколын қолдау • NetFlow v9 мониторинг протоколын қолдау • jFlow мониторинг протоколын қолдау • IPFIX мониторинг протоколын қолдау • sFlow v2/4/5 RFC 3176 мониторинг протоколын қолдау • NetStream мониторинг протоколын қолдау • cFlowd мониторинг протоколын қолдау • NetFlow Lite мониторинг протоколын қолдау • Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2 стандарттарын қолдау • Бұлттық инфрақұрылымдардан Flow статистикасын жинау, сақтау және визуализациялауды қолдау: Amazon AWS (VPC FlowLogs), Microsoft Azure (VNet Flow Logs), Google Cloud Platform (VPC FlowLogs), оның ішінде бұлттық трафикті бірыңғай интерфейсте сүзу, егжей-тегжейлеу және көрсету мүмкіндігі; • IPFIX протоколы бойынша OneAccess, IXIA, VMware, Gigamon, Cisco Systems меншікті өрістерін мониторингтеуді қолдау • Айнымалы ұзындықтағы IPFIX жазбаларын қолдау • Үшінші тарап өндірушілердің IPFIX модификацияларын қолдау, оның ішінде VMware NSX, Gigamon және Ixia IPFIX Extensions • Drill-down (деректерге тереңдеу) тәсілін қолдай отырып, желілік өзара іс-қимылдарды талдау және бақылау мүмкіндігі; • Құрылымдалған көпқадамды тергеулерді қолдау, жеке аналитикалық сұрауларды бірыңғай процеске біріктіру, сақтау, қайта пайдалану, бірлесіп қол жеткізу және талдау нәтижелерін құжаттау мүмкіндігімен; • Тергеулер шеңберінде динамикалық сүзгілер мен қайта пайдаланылатын айнымалыларды қолдау; • NTP протоколы бойынша жүйелік уақытты синхрондауды қолдау; • DNS кэшін қолдау; • DNS-тен алынған домен атауларымен Flow-жазбаларын байытуды қолдау; • Cisco AVC стандартын қолдау, оның ішінде желі өнімділігі метрикалары (AVC ART) және HTTP мәндері (хост атауы және URL); • Желі өнімділігін мониторингтеуді қолдау. RTT, SRT, delay, jitter, retransmission, out-of-order пакеттерін жинау және талдау; • ISO OSI 7-деңгей протоколдарын мониторингтеуді қолдау (HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP, SMTP, POP3, IMAP және MS SQL (TDS)); • OT/ICS-орталарының трафигін мониторингтеуді қолдау, оның ішінде IEC 61850 (GOOSE, MMS), DLMS, CoAP, IEC 104, Modbus, DNP3, S7COMM және MQTT протоколдары; • L3/L4 ISO OSI кеңейтілген мониторингін қолдау (TTL, TCP Window Size, NAT анықтау үшін TCP SYN пакет өлшемі); • Бір көздің әртүрлі интерфейстерінен

	ағындарды семплирлеудің әртүрлі деңгейлерін қолдау; • Скрипттер (сценарийлер) жазу тілін қолдау. Скрипттер жазу тілі Python тілінің жалпы қабылданған командаларын қолдайды; • Басқа коллекторларда өңдеу үшін алынған мониторинг трафигін форвардинг мүмкіндігін қолдау; • Трафикті қайта жіберу кезінде Flow форматтарын конвертациялау мүмкіндігі (NetFlow v5/v9, IPFIX); • IPv4 және IPv6, VLAN, MPLS деректер трафигін өңдеу және оны коллекторға беру мүмкіндігі; • QinQ трафигін өңдеуді қолдау, сыртқы S-TAG және ішкі C-TAG шығарумен; • GRE, VxLAN, ESP, 4in6, DS-Lite және OTV туннельдеріндегі трафикті мониторингтеу мүмкіндігі (декапсуляция); • Қайталанатын пакеттерді анықтау және жою мүмкіндігі; • Прокси арқылы өтетін трафикті корреляциялау мүмкіндігі; • HTTP-трафиктен X-Forwarded-For атрибутын шығаруды қолдау; • Желідегі құрылғыларды профильдеу мүмкіндігі: ОС идентификациясы, оның ішінде нұсқасы. Браузер идентификациясы, оның ішінде нұсқасы; • Ағынның аяқталу уақытын орнату мүмкіндігі (RFC 3954); • RFC 7011 стандартына сәйкес TCP/TLS қосылымдарын пайдалана отырып IPFIX трафигін сенімді және қауіпсіз беру мүмкіндігін қолдау; • Шифрланған (SSL/TLS) трафикті мониторингтеуді қолдау; • Flow статистикасы көзін автоматты идентификациялау; • Flow деректерін сыртқы ақпарат қоймасына резервтік көшіру және қалпына келтіру мүмкіндігі; • Жергілікті желідегі пайдаланушылар туралы деректерді жинау және көрсету, оның ішінде Active Directory, Cisco ISE және ұқсас сыртқы деректер қоймаларынан; • ISO OSI моделінің 7-деңгей өрістерінен ақпарат негізінде көрсетілетін деректерді сүзу мүмкіндіктері; • Берілген опциялар мен атрибуттар бойынша ТОП-Х статистикасын көрсету; • Пайдаланушыларға email, SNMP traps және Syslog арқылы жедел хабарламаларды қолдау; • Пайдаланушылар міндеттеріне жеке анықталған трафик профильдерін қолдау; • Жергілікті желідегі белсенді құрылғыларды анықтау және мониторингтеу; • IP мекенжайларына негізделген автоматты геолокацияны қолдау; • Ашық интеграциялық API интерфейсі; • SNMP бойынша Flow ақпараты көздерінің қолжетімділігін мониторингтеу; • Периметрді қорғаудың үшінші тарап шешімдерімен интеграцияны қолдау, FortiNet, Checkpoint (Тапсырыс берушіде бар); • Лицензияланған деректер қоймасының көлемі 1 (бір) Тб. Деректерді жинау және сақтау жүйесі (коллектор) өңдейтін көлем — секундына 75 мың ағын; • Ішкі диск квотасын басқару тетіктерін қолдау; • Жүйені біртіндеп тік масштабтау мүмкіндігі; • Деректер базасында жинақталатын деректерді семплирлеудің (кесудің) болмауы; • Жүйені қайта орнату қажеттілігінсіз тік модернизациялау мүмкіндігі; • Орталық / агрегациялайтын мониторинг контроллерін пайдалануды қолдау; • Орталық / агрегациялайтын контроллер басқаруындағы бірнеше бөлінген мониторинг контроллерлерінің бірлескен жұмысын қолдау; • Пайдаланушылардың жүйеге веб-интерфейс арқылы және клиенттік БҚ орнатпай қол жеткізуін қолдау; • HTTP/HTTPs негізіндегі бірыңғай жалпы графикалық веб-басқару интерфейсінің болуы; • Пайдаланушылардың құқықтары мен артықшылықтарын бөлу

	тетігін қолдайтын көпдеңгейлі рөлдік модельді қолдау; • HTTP/HTTPs басқаруды қолдау; • SSHv2/Secure Copy қолдау; • SNMP v1/v2c/v3 протоколын қолдау; • TACACS+ аутентификация протоколын қолдау; • LDAP (Active Directory) бойынша аутентификацияны қолдау; • Құрылғыда резервтік конфигурацияны сақтауды және алдыңғы конфигурацияға қайтаруды қолдау; • Талап бойынша сақталатын шектеусіз конфигурациялар саны; • Қашықтан қол жеткізуді сүзу және шектеу функционалын қолдау; • Басқару интерфейсін кастомизациялауды қолдау; • Виртуалды машинаның қашықтағы түйіндермен өзара әрекеттесуін сүзетін кіріктірілген желіаралық экранды қолдау; • Flow-деректерді сақтау баптауларын өзгертпей, талдау мен визуализациялаудың уақыттық егжей-тегжейлеуін қолмен таңдау мүмкіндігі; • Трафик туралы ақпаратқа негізделген статистиканы, есептерді, графиктерді визуализациялау; • Желі өнімділігі метрикаларын визуализациялау; • Деректерді талдау және PDF және CSV-ге экспорттау мүмкіндігі; • PDF немесе CSV-ге деректерді экспорттау мүмкіндігімен, сондай-ақ электрондық поштаға автоматты жіберу мүмкіндігімен кіріктірілген есептер тетігі; Аномалияларды анықтау жүйесіне қойылатын талаптар: 6 Аномалияларды анықтау жүйесіне қойылатын талаптар • NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream желілік трафигіндегі аномалияларды анықтау тетіктерін қолдау; • Желілік ағындарды дедупликациялау тетіктерін қолдау; • Желілік ағындар деңгейінде трафикті семплирлеу; • Трафик көздерінің домен атауларын тану және сақтауды қолдау; • Желілік ағындарды, ақпараттық қауіпсіздік оқыс оқиғаларын және желілік аномалияларды талдау үшін пайдаланылатын алдын ала орнатылған ережелер мен алгоритмдердің болуы; • Қолтаңбасыз әдістерді пайдалана отырып, желілік шабуылдарды анықтау (порттарды сканерлеу, құпия сөздерді іріктеу шабуылдары, DoS/DDoS, SSH, RDP, Telnet желілік протоколдарына шабуылдар және т.б.); • Желілік трафиктегі аномалияларды анықтау, оның ішінде DNS, DHCP, SMTP, multicast және т.б.; • JA3 саусақ іздері көмегімен шифрланған трафикті талдауды қолдау; • Заңсыз протоколдар мен қолданбаларды анықтау, оның ішінде P2P-желілер, DNS-over-HTTPS (DoH), QUIC протоколдары, сондай-ақ анонимизация сервистері (TOR қоса) және басқа да қалаусыз трафик түрлері; • IP мекенжайлары мен елдердің репутациялық тізімдеріне негізделген ақпараттық қауіпсіздік оқыс оқиғалары мен желілік аномалияларды анықтау; • Жүйелік қызметтердің (DNS қоса) жұмыс істеуіне байланысты операциялық проблемаларды анықтау, сондай-ақ желідегі жаңа түйіндер мен сервистерді анықтау; • Жергілікті желідегі түйіндердің мінез-құлық моделі негізінде ақпараттық қауіпсіздік оқыс оқиғалары мен желілік аномалияларды автоматты анықтау; • Машиналық оқыту алгоритмдерін пайдалана отырып, желілік трафикті талдау негізінде OT-ортадағы зиянды, ақаулы, дұрыс бапталмаған және жаңа құрылғыларды анықтау; • Ақпараттық қауіпсіздік оқыс оқиғалары мен желілік аномалияларды анықтау әдістерін баптауды автоматтандыру үшін алдын ала орнатылған процедуралардың болуы; • MISP

	платформасын қолдау; • MITRE ATT&CK; жүйесін қолдау және контекстті ескере отырып көрсету; • Әртүрлі IP мекенжайлары, сегменттер, сервистер және қызметтер үшін ақпараттық қауіпсіздік оқыс оқиғалары мен желілік аномалияларды анықтау әдістерін пайдаланушылық баптау; • Желідегі белсенді хосттар үшін қатер дәрежесін бағалау тетігін қолдау; • ISO OSI моделінің 7-деңгей ақпараты негізінде пайдаланушының өз анықтау әдістерін баптау мүмкіндігі; • ISO OSI моделінің 3 және 4 деңгей ақпараты негізінде NAT анықтау; • Оқиғаларды сүзу тетігі, оның ішінде кірістірілген сүзгілер. CSV файлдары арқылы сүзгілерді импорттау және экспорттау мүмкіндіктері; • Жалған іске қосылуларды басқару (ерекшеліктерді қолмен баптау); • ASN, FQDN, IP диапазондары және басқа белгілер негізінде шарттарды пайдалана отырып, жалған іске қосылуларды басқаруды қолдау; • IP мекенжайлары, оқиға түрлері және оқиғалардың географиялық белгіге байланыстырылуы негізінде оқиғаларды пайдаланушылық басымдықтау; • CEF форматында Syslog протоколы бойынша пайдаланушыларға хабарламалар; • SNMP Trap тетігі арқылы пайдаланушыларға хабарламалар; • E-mail арқылы пайдаланушыларға хабарламалар (HTML немесе TXT форматында); • Оқиға анықталған кезде пайдаланушы скрипттерін автоматты немесе қолмен іске қосу мүмкіндігі; • Ақпарат ағындарын өңдеу — 100 ағын / с; • Мінез-құлық үлгілерін өңдеу — 100 ағын / с; • Flow статистикасын байыту мақсатында сыртқы ақпараттық сервистермен интеграция тетіктерін қолдау, оның ішінде DNS, WHOIS, геолокациялық сервистер, каталогтар жүйесі (AD, LDAP); • Жүйе пайдаланушыларының оқиғаларды санаттау және түсініктеме беруі; • Оқиға түрі, оқиға көзінің IP мекенжайы, оқиға санаты, оқиға ID және т.б. негізінде оқиғаларды іздеу тетіктерін қолдау; • Қатысатын IP мекенжайларын, олардың арасындағы байланыстарды, желілік алмасу статистикасын көрсететін оқиғаларды интерактивті визуализациялау; • Алдын ала анықталған үлгілер мен пайдаланушы баптауларына негізделген PDF-ке есептілік және экспорт тетігінің болуы; • Оқиғаларды CSV форматына экспорттау; • Ашық API интерфейсі бойынша интеграцияны қолдау; • Жүйе конфигурацияларының өзгеру оқиғаларын Syslog бойынша сыртқы SIEM жүйесіне журналдау; • Оқиғалардың келесі түрлерін визуализациялауды қолдау: Оқиғалар ағашы, Уақыттық график, Егжей-тегжейлеу, Растаулар, Интерактивті режим; • Келесі үшінші тарап өнімдерімен интеграцияны қолдау: IBM QRadar App, LDAP/AD (Тапсырыс берушіде бар) Берілген лицензияның түрі мен құрамы: Жеткізуші Тапсырыс берушіге 12 ай мерзімге жазылу форматында лицензия береді.

Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	- Өнім беруші шарт жасалған күннен бастап 3 жұмыс күні ішінде қайтарып алынбаған, толық төленген және қолданыстағы лицензияны растайтын, оны лицензияның бүкіл қолданылу мерзімі ішінде үшінші тұлғалардың кері қайтарып алу, тоқтата тұру немесе шектеу мүмкіндігін болдырмайтын құжатты ұсынуға міндетті. Орындалатын жұмыстарға, көрсетілетін қызметтерге қойылатын талаптар: Өнім беруші шарт жасалған күннен бастап күнтізбелік 30 (отыз) күн ішінде Бағдарламалық қамтамасыз етуді енгізуді толық көлемде орындауға міндеттенеді - Жеткізуші лицензияның қолданылу мерзімі ішінде жүйеге техникалық қолдау көрсетеді. Техникалық қолдау электрондық пошта, телефон арқылы және Қазақстан Республикасының уақыты бойынша жұмыс күндері сағат 08:00-ден 17:00-ге дейін қашықтан қол жеткізу арқылы ұсынылады. Электрондық пошта немесе билет жүйесі арқылы өтініштерді қабылдау тәулік бойы, тәулігіне 24 сағат, аптасына 7 күн қамтамасыз етілуі тиіс. Техникалық қолдау жүйені орнату, баптау, пайдалану, сондай-ақ жеткізуші ұсынатын қызметтер шегінде техникалық ақауларды анықтау және жою мәселелері бойынша консультацияларды қамтиды. Өтініштерді тіркеу тәртібі, Алғашқы жауап беру мерзімдері және ақауларды жою мерзімдері Шартпен не оған қосымшамен айқындалады. - Өнім беруші Тапсырыс берушіге жеткізілетін жүйеге пайдалану және техникалық құжаттама жиынтығын электрондық түрде береді. Құжаттамада жүйені орнату, конфигурациялау, басқару және пайдалану, есептік жазбалар мен қол жеткізу құқықтарын басқару, есептерді қалыптастыру, параметрлердің сақтық көшірмесін жасау және қалпына келтіру, сондай-ақ типтік ақауларды жою үшін қажетті мәліметтер болуы керек.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Республиканское государственное предприятие на праве хозяйственного ведения «Национальный центр качества дорожных активов» Комитета автомобильных дорог Министерства транспорта Республики Казахстан
Наименование организатора	Республиканское государственное предприятие на праве хозяйственного ведения «Национальный центр качества дорожных активов» Комитета автомобильных дорог Министерства транспорта Республики Казахстан
№ конкурса:	№ 17891305-1
Наименование конкурса:	Услуги по предоставлению лицензий на право использования программного обеспечения
Номер лота:	№ 88092853-ОК1
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:	8586206
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	8586206
Срок оказания услуги:	Согласно требованиям технической спецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Функциональные требования: • Поддержка анализа трафика flow (потоков), отправленных с сетевых устройств инфраструктуры Заказчика на сервер-коллектор. Типы поддерживаемых протоколов перечислены ниже, в разделе «Функциональные требования». • В случае если сетевое оборудование инфраструктуры Заказчика не имеет функционала генерации и отправки поддерживаемых flow протоколов, должна быть предусмотрена возможность генерации flow трафика специальным устройством – зондом, путем приема SPAN трафика на скорости 1 Гб/с и инкапсуляции в поддерживаемый системой flow протокол. В рамках поставки должен быть предусмотрен 1 (один) зонд, встроенный в коллектор. • Поддержка анализа трафика на нескольких интерфейсах • Поддержка мониторинга «сырого» SPAN трафика • Поддержка протокола мониторинга NetFlow v5 • Поддержка протокола мониторинга NetFlow v9 • Поддержка протокола мониторинга jFlow • Поддержка протокола мониторинга IPFIX • Поддержка протокола мониторинга sFlow v2/4/5 RFC 3176 • Поддержка протокола мониторинга NetStream • Поддержка протокола мониторинга cFlowd • Поддержка протокола мониторинга NetFlow Lite • Поддержка стандартов Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2 • Поддержка сбора, хранения и визуализации Flow статистики из облачных инфраструктур: Amazon AWS (VPC FlowLogs), Microsoft Azure (VNet Flow Logs), Google Cloud Platform (VPC FlowLogs), включая возможность фильтрации, детализации и отображения облачного трафика в едином интерфейсе; • Поддержка мониторинга проприетарных полей OneAccess, IXIA, VMware, Gigamon, Cisco Systems по протоколу IPFIX • Поддержка IPFIX записей переменной длины • Поддержка IPFIX модификаций сторонних производителей, включая VMware NSX, Gigamon и Ixia IPFIX Extensions • Возможность анализа и контроля сетевых взаимодействий с поддержкой подхода drill-down (углубление в данные) для получения детальной статистики по каждому сетевому подключению (сетевому потоку); • Поддержка структурированных многошаговых расследований с возможностью объединения отдельных аналитических запросов в единый процесс, сохранения, повторного использования, совместного доступа и документирования результатов анализа. • Поддержка динамических фильтров и повторно используемых переменных в рамках расследований, включая возможность передачи значений, полученных на одном шаге, в последующие аналитические запросы. • Поддержка синхронизации системного времени по протоколу NTP; • Поддержка DNS кэш; • Поддержка обогащения Flow-записей доменными именами, полученными из DNS, для более точного определения сервисов и приложений, в том числе использующих общую сетевую инфраструктуру. • Поддержка стандарта Cisco AVC, включая метрики производительности сети (AVC ART) и значения HTTP (имя хоста и URL); • Поддержка мониторинга сетевой производительности. Сбор и анализ RTT, SRT, delay, jitter, retransmission, out-of-order пакетов; • Поддержка мониторинга протоколов 7 уровня ISO OSI (HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP, SMTP, POP3, IMAP и MS SQL

	(TDS)); • Поддержка мониторинга трафика OT/ICS-сред, включая протоколы IEC 61850 (GOOSE, MMS), DLMS, CoAP, IEC 104, Modbus, DNP3, S7COMM и MQTT, с передачей полученных атрибутов в составе IPFIX. • Поддержка расширенного мониторинга L3/L4 ISO OSI (TTL (Time To Live), TCP Window Size, TCP SYN размер пакета для NAT обнаружения); • Поддержка различных уровней семплирования потоков с разных интерфейсов одного источника; • Поддержка языка написания скриптов (сценариев). Язык написания скриптов будет поддерживать общепринятые команды языка Python; • Поддержка возможности форвардинга получаемого трафика мониторинга для обработки на других коллекторах, включая возможность семплирования трафика; • Возможность конвертирования Flow форматов при пересылке трафика (NetFlow v5/v9, IPFIX); • Возможность обработки трафика данных IPv4 и IPv6, VLAN, MPLS и передача его коллектору; • Поддержка обработки трафика QinQ с извлечением внешнего S-TAG и внутреннего C-TAG и передачей соответствующих атрибутов в составе Flow-статистики. • Возможность мониторинга трафика в туннелях GRE, VxLAN, ESP,4in6, DS-Lite и OTV (декапсуляция); • Возможность обнаружения и удаления дублированных пакетов • Возможность корреляции трафика, проходящий через прокси • Поддержка извлечения атрибута X-Forwarded-For из HTTP-трафика для определения исходного IP-адреса клиента при прохождении соединения через прокси-сервер или балансировщик нагрузки. • Возможность профилирования устройств в сети: идентификация ОС, включая ее версию. Идентификация браузера, включая его версию; • Возможность установки времени истечения потока: настройки таймаута для активного и неактивного истечения потоков (RFC 3954); • Поддержка возможности надежной и безопасной передачи IPFIX трафика с использованием TCP/TLS подключений согласно стандарту RFC 7011; • Поддержка мониторинга зашифрованного (SSL/TLS) трафика: определение версии протокола, алгоритма шифрования, набора шифров, данных сертификата; • Автоматическая идентификация источника Flow статистики, включая имя источника данных, наименование интерфейса и его параметры; • Резервное копирование, с возможностью дальнейшего восстановления, Flow данных на внешнее хранилище информации; • Сбор и отображение данных о пользователях в ЛВС, включая IP адрес хоста и ID пользователя, получаемых из внешних хранилищ данных, как Active Directory, Cisco ISE и аналогичные; • Наличие возможностей по фильтрации отображаемых данных на основании информации из полей 7 уровня модели ISO OSI с поддержкой запросов на основании регулярных выражений (AND, OR, NOT); • Отображение ТОП-Х статистики по заданным опциям и атрибутам: включая количество переданных байт, пакетов, потоков, максимальное RTT и среднее SRT; • Поддержка оперативных уведомлений пользователей по email, SNMP traps и Syslog; • Поддержка профилей трафика, определенных под задачи пользователей индивидуально; • Обнаружение и мониторинг активных устройств

	в ЛВС, а также хранение истории, включая информацию о MAC адресах, VLAN, OS и идентификационные данные пользователей; • Поддержка автоматической геолокации, основанной на IP адресах с возможностью фильтрации трафика по странам; • Открытый интеграционный интерфейс API; • Мониторинг доступности источников Flow информации по SNMP. • Поддержка интеграции со сторонними решениями защиты периметра, FortiNet, Checkpoint (имеются у заказчика); • Объем лицензированного хранилища данных 1 (один) Тб. Объем обрабатываемых системой сбора и хранения данных (коллектором) - 75 тысяч потоков в секунду; • Поддержка механизмов управления внутренней дисковой квотой; • Возможность постепенного вертикального масштабирования системы; • Отсутствие семплирования (урезания) накапливаемых данных в базе данных. • Возможность вертикальной модернизации системы без необходимости переустановки системы; • Поддержка использования центрального / агрегирующего контроллера мониторинга (для схем с распределенной архитектурой); • Поддержка совместного функционирования нескольких распределенных контроллеров мониторинга под управлением центрального / агрегирующего контроллера; • Поддержка доступа пользователей к системе через веб-интерфейс и без установки какого бы то ни было клиентского ПО. Допускается использование любого ПО, входящего в состав операционной системы, и стандартных библиотек. • Наличие единого общего графического веб-интерфейса управления, основанного на HTTP/HTTPs с возможностью персонализации разделов для каждого пользователя • Поддержка многоуровневой ролевой модели с поддержкой механизма разделения прав и привилегий пользователей • Поддержка HTTP/HTTPs управления • Поддержка SSHv2/Secure Copy • Поддержка протокола SNMP v1/v2c/v3; • Поддержка протокола аутентификации TACACS+; • Поддержка аутентификации по LDAP (Active Directory); • Поддержка хранения на устройстве резервной конфигурации устройства, а также возврат устройства на предыдущую конфигурацию; • Неограниченное количество сохраняемых по требованию конфигураций, на которые можно осуществить возврат в любое время; • Поддержка функционала по фильтрации и ограничению удаленного доступа; • Поддержка кастомизации интерфейса управления (настройка панелей и виджетов, их расположения и типов отображаемой информации); • Поддержка встроенного межсетевого экрана, фильтрующего взаимодействие виртуальной машины с удаленными узлами • Возможность ручного выбора временной детализации анализа и визуализации данных, от долгосрочного представления до интервала 30 секунд, без изменения настроек хранения Flow-данных. • Визуализация статистики, отчетов различных типов, графиков, основанных на информации о трафике (количество переданных байт, потоков, пакетов); • Визуализация метрик производительности сети; • Анализ данных и возможность экспорта в PDF и CSV • Встроенный механизм отчетов с возможностью экспорта данных в PDF или CSV, а также возможностью автоматической отправки на электронную почту; Требования к системе

	детектирования аномалий: • Поддержка механизмов выявления аномалий в сетевом трафике NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream; • Поддержка механизмов дедупликации сетевых потоков; • Семплирование трафика на уровне сетевых потоков; • Поддержка распознавания и хранения доменных имен источников трафика; Тип и состав предоставляемой лицензии: Поставщик предоставляет Заказчику лицензию в формате подписки сроком на 12 месяцев. Поставщик обязан предоставить документ, в течение 3 рабочих дней с даты заключения договора, подтверждающий безотзывную, полностью оплаченную и действующую лицензию, исключающую возможность её отзыва, приостановки или ограничения третьими лицами в течение всего срока действия лицензии. Требования к выполняемым работам, оказываемым услугам: Поставщик обязуется в течение 30 (тридцати) календарных дней со дня заключения договора выполнить внедрение Программного обеспечения в полном объеме • Наличие предустановленных правил и алгоритмов, используемых для анализа сетевых потоков, инцидентов информационной безопасности и сетевых аномалий; • Обнаружение сетевых атак (включая сканирование портов, атаки перебора паролей, DoS / DDoS, атаки на сетевые протоколы SSH, RDP, Telnet и прочие) с использованием безсигнатурных методов; • Обнаружение аномалий в сетевом трафике, включая DNS, DHCP, SMTP, multicast и прочее; • Поддержка анализа зашифрованного трафика с помощью отпечатков пальцев JA3; • Обнаружение нелегитимных протоколов и приложений, включая P2P-сети, протоколы DNS-over-HTTPS (DoH), QUIC, а также сервисы анонимизации (включая TOR) и прочие нежелательные типы трафика; • Обнаружение инцидентов информационной безопасности и сетевых аномалий, основанное на репутационных списках IP адресов и стран; • Обнаружение операционных проблем, связанных с функционированием системных служб (включая DNS), а также выявление новых узлов и сервисов в сети; • Автоматическое обнаружение инцидентов информационной безопасности и сетевых аномалий, на основании модели поведения узлов в ЛВС; • Обнаружение вредоносных, неисправных, неправильно настроенных и новых устройств в OT-среде на основании анализа сетевого трафика с использованием алгоритмов машинного обучения. • Наличие предустановленных процедур для автоматизации настройки методов обнаружения инцидентов информационной безопасности и сетевых аномалий; • Поддержка платформы MISP; • Поддержка системы MITRE ATT&CK; и отображение с учетом контекста; • Пользовательская настройка методов обнаружения инцидентов информационной безопасности и сетевых аномалий для разных IP адресов, сегментов, сервисов и служб; • Поддержка механизма оценки степени угрозы для активных хостов в сети на основе числового индекса с возможностью ранжирования и визуализации по уровню риска; • Возможность настройки пользователем собственных методов обнаружения инцидентов информационной безопасности и сетевых аномалий на основании информации 7 уровня модели ISO OSI; • Обнаружение NAT на основании

	информации 3 и 4 уровня модели ISO OSI; • Механизм фильтрации событий, включая вложенные фильтры. Возможности импорта и экспорта фильтров через CSV файлы; • Управление ложными срабатываниями (ручная настройка исключений) • Поддержка управления ложными срабатываниями с использованием условий на основе ASN, FQDN, диапазонов IP и других признаков; • Пользовательская приоритезация событий, основанная на IP адресах, типах событий и привязанности событий к географической метке; • Уведомления пользователей по протоколу Syslog, в формате CEF; • Уведомления пользователей через механизм SNMP Trap; • Уведомления пользователей через E-mail (в формате HTML или TXT); • Возможность автоматического или ручного запуска пользовательских скриптов при обнаружении события, в том числе для передачи информации о событии и запуска ответных действий во внешних системах. • Обработка потоков информации - 100 потоков / с; • Обработка поведенческих шаблонов - 100 потоков / с; • Поддержка механизмов интеграции со внешними информационными сервисами в целях обогащения Flow статистики, включая DNS, WHOIS, геолокационные сервисы, систем каталогов (AD, LDAP) и прочие пользовательские сервисы, основанные на HTTP протоколе; • Категоризация и комментирование событий пользователями системы; • Поддержка механизмов поиска событий, основанных на типе событий, IP адресе источника событий, категории событий, ID событий и т.д); • Интерактивная визуализация событий с отображением участвующих IP-адресов, связей между ними, статистики сетевого обмена, а также других узлов, взаимодействовавших с участниками события в период его регистрации. • Наличие механизма отчетности и экспорта в PDF, основанного на предопределенных шаблонах и пользовательских настройках, с поддержкой передачи по e-mail; • Экспорт событий в CSV формат; • Поддержка интеграции по открытому API интерфейсу; • Журналирование событий изменения конфигураций системы по Syslog во внешнюю SIEM систему; • Поддержка визуализации событий следующих видов: Дерево событий, Временной график, Детализация, Подтверждения, Интерактивный режим; • Поддержка интеграции со следующими сторонними продуктами: IBM QRadar App, LDAP/AD (имеются у заказчика) Тип и состав предоставляемой лицензии: Поставщик предоставляет Заказчику лицензию в формате подписки сроком на 12 месяцев.

Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	- Поставщик обязан предоставить документ, в течение 3 рабочих дней с даты заключения договора, подтверждающий безотзывную, полностью оплаченную и действующую лицензию, исключающую возможность её отзыва, приостановки или ограничения третьими лицами в течение всего срока действия лицензии. Требования к выполняемым работам, оказываемым услугам: Поставщик обязуется в течение 30 (тридцати) календарных дней со дня заключения договора выполнить внедрение Программного обеспечения в полном объеме. - Поставщик обеспечивает техническую поддержку Системы в течение срока действия лицензии. Техническая поддержка предоставляется по электронной почте, телефону и посредством удалённого доступа в рабочие дни с 08:00 до 17:00 по времени Республики Казахстан. Приём обращений посредством электронной почты или тикетной системы должен обеспечиваться круглосуточно, 24 часа в сутки, 7 дней в неделю. Техническая поддержка включает консультации по вопросам установки, настройки, эксплуатации Системы, а также выявления и устранения технических неисправностей в пределах предоставляемых поставщиком услуг. Порядок регистрации обращений, сроки первичного ответа и сроки устранения неисправностей определяются договором либо приложением к нему. - Поставщик передаёт Заказчику комплект эксплуатационной и технической документации на поставляемую Систему в электронном виде. Документация должна содержать сведения, необходимые для установки, настройки, администрирования и эксплуатации Системы, управления учётными записями и правами доступа, формирования отчётов, резервного копирования и восстановления настроек, а также устранения типовых неисправностей.