ТЕХНИКАЛЫҚ СИПАТТАМА

1264050 сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 1 (3422-1 У, 4561505) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: "Қазақтелеком" АҚ

Ұйымдастырушы: "Қазақтелеком" акционерлік қоғамының филиалы "Телеком Жинақтау" дирекциясы"

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	3422-1 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	ДЦБ_Доступ к программному обеспечению для защиты конечных устройств (компьютеров и серверов) от угроз EDR
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Алматы қ., г.Алматы, ул.Чайковского 39 (ДЦБ)
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 30 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

Құрылғыларды (компьютерлер мен серверлерді) қауіп-қатерлерден қорғауға арналған бағдарламалық қамтамасыз етуге қойылатын техникалық талаптар

1. **Басқару консолі**

• Басқару консолін орналастыру Тапсырыс берушіден бағдарламалық және аппараттық ресурстар бөлуді талап етпеуі тиіс

• Басқару консолі және жиналған деректерді өңдеу шешім өндірушісінің бұлтында іске асырылуы тиіс

• Қолжетімділік құқықтарын түйіршіктеп делегаттау мүмкіндігімен басқару консоліне рөлдік қолжетімділіктің болуы

• Басқару консолі пайдаланушыларының есептік жазбалары үшін екі факторлы аутентификацияны қолдау

• Басқару консолі мен соңғы нүктелердегі модульдер арасындағы деректер алмасу TLS 1.2 көмегімен қорғалуы тиіс

• Инциденттерді және/немесе маркерлерді талдау, әрекет ету және триаждау (басымдықтарын айқындау) операцияларын жеделдету үшін консольдің барлық бөлімдері бойынша икемді іздеу тетігінің болуы

• Соңғы құрылғылар топтарына саясаттарды тағайындау мүмкіндігі

• Консоль соңғы құрылғыларды статикалық тәртіпте де, динамикалық критерийлер бойынша да біріктіруге мүмкіндік беруі тиіс, олардың ішінде:

• ОЖ түрі

- Жүйенің желілік параметрлері
- Жұмыс станциясы/Сервер
- Қорғау мәртебесі
- Клиенттік модуль нұсқасы
- Шешімде барлық әкімшілендіру функциялары үшін бірыңғай пайдаланушы интерфейсі болуы тиіс – инциденттерді талдау және оларға әрекет ету бойынша барлық операциялар бір консоль шегінде орындалуы тиіс
- Басқару консолінде әкімшілер/талдаушылар санына шектеу болмауы тиіс
- Басқару консолі аудиттің мынадай түрлерін қолдауы тиіс:
- Хосттар аудиті
- Пайдаланушы әрекеттерінің аудиті
- API арқылы қосылулар аудиті
- Саясаттар аудиті
- Real Time Response аудиті
- Файл ерекшеліктерінің аудиті
- Консоль корпоративтік желіге VPN немесе басқа да қолжетімділік құралдарын пайдаланбай, соңғы нүктелерде орналастырылған модульдерді басқару мүмкіндігін қолдауы тиіс (корпоративтік периметрден тыс орналасқан жүйелерді қорғау)
- Консоль талдаушылар тобының инциденттер бойынша бірлесіп жұмыс істеуін, инциденттерді делегаттау және олардың мәртебесін өзгерту мүмкіндігін қолдауы тиіс
- Басқару консолі инциденттерді олардың арасында дереу ауысу мүмкіндігімен төрт негізгі нысанда көрсетуді қамтамасыз етуі тиіс:
- Әрбір хост бойынша жалпы ақпарат
- Шабуыл векторын көрсететін кестелік нысан
- Аңызын көрсете отырып және шабуылдың даму барысын белгілей отырып байланыстар графигі
- Әрбір оқиғаның сипаттамасы бар оқиғалар уақыт шкаласы
- Алынған деректерді визуализациялауды жеңілдету және шешім қабылдауды жеделдету үшін іске қосылған процестер байланыстарының графиктерін интуитивті масштабтау мүмкіндігі
- Инцидент деректерін қарау кезінде мынадай әрекеттерді лезде орындау мүмкіндігі:
- Әрекет ету шараларын орындау үшін жүйеге интерактивті қосылу
- Желілік оқшаулау
- Инцидентті нақты команда мүшесіне бекіту
- Инцидент мәртебесін өзгерту
- Жүйе, хэш және процесс атауы бойынша деректерді іздеу
- Басқару консолінде Workflow бизнес-процестерін автоматтандыру бойынша қосымша функционал болуы тиіс.
- Workflow модулі автоматтандыру сценарийлерін икемді түрде құруды, оларды «нақты уақытта» өзгерту мүмкіндігін қамтамасыз етуі және автоматтандырылған әрекеттердің дайын үлгілерін ұсынуы тиіс.

- Басқару консолі төменде көрсетілген барлық модульдер үшін бірыңғай болуы тиіс

- Модульді орналастыру ОЖ-ны қайта жүктеуді талап етпеуі тиіс

- Қауіптерді анықтау кезінде модуль сигнатуралар дерекқорларын пайдаланбауы тиіс

- Соңғы нүктенің басқару консолімен байланысы болмаған жағдайда шешім мінез-құлықты талдауды және белгілі ықтимал зиянды операцияларды (жүйені жұқтыру үшін ОЖ-ның кіріктірілген функционалдығын пайдалану және т. б.) бұғаттауды қолдана отырып, орталық консольге қосылғанға дейін 90 күн ішінде базалық қорғауды қамтамасыз етуі тиіс.

- Модуль араласудан және рұқсатсыз деинсталляциядан қорғауды қолдауы тиіс

- Кіріктірілген брандмауэрді жеке саясаттар арқылы басқару мүмкіндігі (Windows, Mac жүйелері үшін). Бір жерден басқару.

- Шешім бұрын белгісіз/бірегей зиянды БҚ-ны анықтай алуы тиіс

- Скрипттерді пайдалана отырып жасалған шабуылдарды жақсартылған анықтау үшін Microsoft AMSI интеграциясын қолдау

- Белгісіз немесе қайта оралған зиянды кодты анықтауды жақсарту үшін машиналық оқыту мүмкіндіктерін пайдалану

- Файлдар мен олардың атрибуттарын талдау үшін бұлттық бедел дерекқорын пайдалану

- Жүйелерді жұқтыру үшін пайдаланылатын жүйелік құралдардың күдікті шақыруларын тану

- Эксплойттерден қорғау, процестер жадына манипуляция жасаудан қорғау

- Есептік деректердің ұрлануынан немесе есептік жазбаларға манипуляция жасаудан қорғау

- Беделі белгісіз файлдарды статикалық және динамикалық талдау үшін өндірушінің бұлтына «құмсалғыш» сыныбындағы жүйеге жіберу мүмкіндігі

- Модуль өндірушінің бұлттық «құмсалғышына» файлдарды жіберуді өшіру мүмкіндігін қолдауы тиіс

Басқару консоліне қолжетімділік қосылатын модульдер лицензияларының бүкіл қолданылу мерзіміне берілуі тиіс

1. **Антивирустық модуль**

- Модульді орналастыру ОЖ-ны қайта жүктеуді талап етпеуі тиіс

- Қауіптерді анықтау кезінде модуль сигнатуралар дерекқорларын пайдаланбауы тиіс

- Соңғы нүктенің басқару консолімен байланысы болмаған жағдайда шешім мінез-құлықты талдауды және белгілі ықтимал зиянды операцияларды (жүйені жұқтыру үшін ОЖ-ның кіріктірілген функционалдығын пайдалану және т. б.) бұғаттауды қолдана отырып, орталық консольге қосылғанға дейін 90 күн ішінде базалық қорғауды қамтамасыз етуі тиіс.

- Модуль араласудан және рұқсатсыз деинсталляциядан қорғауды қолдауы тиіс

- Кіріктірілген брандмауэрді жеке саясаттар арқылы басқару мүмкіндігі (Windows, Mac жүйелері үшін). Бір жерден басқару.

- Шешім бұрын белгісіз/бірегей зиянды БҚ-ны анықтай алуы тиіс

- Скрипттерді пайдалана отырып жасалған шабуылдарды жақсартылған анықтау үшін Microsoft AMSI интеграциясын қолдау

- Белгісіз немесе қайта оралған зиянды кодты анықтауды жақсарту үшін машиналық оқыту мүмкіндіктерін пайдалану

- Файлдар мен олардың атрибуттарын талдау үшін бұлттық бедел дерекқорын пайдалану
- Жүйелерді жұқтыру үшін пайдаланылатын жүйелік құралдардың күдікті шақыруларын тану
- Эксплойттерден қорғау, процестер жадына манипуляция жасаудан қорғау
- Есептік деректердің ұрлануынан немесе есептік жазбаларға манипуляция жасаудан қорғау
- Беделі белгісіз файлдарды статикалық және динамикалық талдау үшін өндірушінің бұлтына «құмсалғыш» сыныбындағы жүйеге жіберу мүмкіндігі
- Модуль өндірушінің бұлттық «құмсалғышына» файлдарды жіберуді өшіру мүмкіндігін қолдауы тиіс

1. **Мінез-құлықты бақылау және қауіптерге әрекет ету модулі**

- Модульді орналастыру ОЖ-ны қайта жүктеуді талап етпеуі тиіс
- Модуль араласудан және рұқсатсыз деинсталляциядан қорғауды қолдауы тиіс
- Жеткізілетін модуль құрамына желілік трафикті талдау модулі және оны талдау функциясы кіруі тиіс
- Соңғы нүктелердегі іске қосылған процестер, желілік белсенділік, файлдық жүйедегі операциялар бойынша метадеректерді жинау
- Аномалиялар мен ықтимал зиянды операцияларды анықтау үшін жүйедегі өзгерістердің реттілігін бақылау
- Іске қосылған процестерді олардың иелерімен және пайдаланушылардың әрекеттерімен корреляциялау
- Араласуға әрекет ету үшін мынадай реакцияларды пайдалану:
- Карантин
- Файлды, каталогты жою
- Процесті, процестер ағашын тоқтату
- ОЖ командасын орындау
- Ерікті скрипттерді орындау
- Файлдық жүйедегі орналасуына қарай нақты файлдарды шешім өндірушісінің бұлтына жіберуге ерекшелік (тыйым салу) қою мүмкіндігі, саясатты қолданар алдында таңдалған үлгіні тексеру мүмкіндігімен
- Соңғы нүктелерден алынған барлық телеметрия мен метадеректер тек шифрланған арна арқылы шешім өндірушісінің бұлтында өңделуі тиіс.
- Жүйе анықталған сәттен бастап инциденттерге байланысты деректерді кемінде 90 күн сақтауды қолдауы тиіс
- Жүйе өндірушінің бұлтына жіберілген сәттен бастап соңғы 7 күндегі телеметрия деректерін (метадеректердің толық тізбесін) сақтауды қолдауы тиіс, Тапсырыс берушінің немесе реттеуші органның талабы бойынша сақтау мерзімін ұзарту мүмкіндігімен
- Жүйе қауіп-қатерді немесе оның жүйеде болу іздерін бейтараптандыру үшін соңғы нүктелерде командалар мен скрипттерді интерактивті орындау мүмкіндігін қолдауы тиіс: PowerShell, Bash, CMD, BAT қолдауымен, таңдалған скрипттің орындалу нәтижелерін бақылау және аналитика мен графикалық талдауды қосу мүмкіндігімен
- Жүйе инциденттерге әрекет етуді жеделдету және таңдаулы (бұрын қолданылған командаларды) сақтау үшін жиі пайдаланылатын пайдаланушы скрипттерінің кітапханасын қалыптастыру мүмкіндігін қолдауы тиіс

- Жүйе таңдалған жүйелерді желілік оқшаулау мүмкіндігін қолдауы тиіс, бұл ретте карантиндегі жүйелер үшін өндірушінің консолінен басқа қолжетімді болатын нақты желілерді баптау мүмкіндігі болуы тиіс
- Желілік оқшаулау қолданылатын жүйелер (яғни карантин) жедел манипуляциялар жүргізу үшін басқару консолімен (шешім өндірушісінің бұлтымен) байланысты сақтауы тиіс.
- Жүйе нысаналы жүйені қайта жүктеуді қажет етпей түзету жүргізуге (командалар мен скрипттерді орындауға) рұқсат беруі тиіс
- Модуль ОЖ-да іске қосылған процестердің кемінде 600 параметрін жинау мүмкіндігін қолдауы тиіс
- Соңғы нүктелер телеметриясы индекстелуі және басқару консолінің іздеу сұраулары арқылы іздеу мүмкіндігін қолдауы тиіс
- Соңғы нүктелер телеметриясын экспорттау/жүктеу мүмкіндігі болуы тиіс
- Таңдалған процестің жады дампын жасау мүмкіндігі

1. **Active Directory қорғау модулі**

Шешім Active Directory автоматты аудитін қамтамасыз етуі тиіс:

- Артықшылықты пайдаланушылар және олардың артықшылықтары
- Құпиясөздері компрометацияланған есептік жазбалар
- Жасырын әкімші есептік жазбалары және олардың артықшылықтары
- Ортақ есептік жазбаларды анықтау
- Компрометацияланған есептік жазбаларды анықтау
- Қайталанатын есептік жазбалар
- NTLMv2 үйлесімділігін тексеру
- Артықшылықты SID бар есептік жазбалар
- SPNs бар әлсіз қорғалған есептік жазбалар
- Артықшылықсыз пайдаланушылардың құқықтарын эскалациялау

Шешім Threat Hunting функциясын қамтамасыз етуі тиіс:

- Жұмыс станциялары арасындағы SMB-қосылымдарды анықтау
- Критикалық серверлерге SMB-қолжетімділікті анықтау
- Артықшылықты есептік жазбаларды пайдалана отырып RDP-сессияларды анықтау
- Құпиясөздері компрометацияланған пайдаланушылардың SMB және RDP-трафигін анықтау
- Active Directory Reconnaissance
- Бүйірлік жылжудың кең таралған техникалары – PsExec, PAExec, WMI, RDP, Scheduled Tasks, CrackMapExec

Шешім қолжетімділіктерге рұқсат беруге/тыйым салуға тиіс:

- Бүйірлік жылжу әрекеттері мен техникаларын бұғаттау
- Егер олар PAM-шешімдерімен (CyberArk, senhasegura және т. б.) бастамаланса, серверлерге RDP-сессияларға рұқсат беру

- Критикалық серверлерге қосылған кезде қосымша MFA-аутентификацияны сұрату
- Сервистік есептік жазбалар бастамалаған RDP-сессияларды бұғаттау
- Пайдаланушы бұрын қосылмаған жүйелерге қосылған кезде MFA-аутентификацияны сұрату (пайдаланушының мінез-құлқын үйрету кезеңі 14 күнтізбелік күннен аспауы тиіс)
- AD есептік жазбаларын пайдаланатын критикалық веб-қосымшаларға қосылған кезде MFA-аутентификацияны сұрату (мысалы, VMware vCenter/vSphere)

Шешім пайдаланушының мінез-құлқының базалық профилін (baseline) қалыптастыруы, аномалды мінез-құлық туралы сигнал беруі, оның алдын алуы немесе пайдаланушыдан MFA-аутентификацияны сұратуы тиіс.

1. **Жалпы талаптар**

- Шешім өндірушісі MITRE ATT&CK® Enterprise Evaluations бағдарламасына қатысуы тиіс; соңғы аяқталған бағалау нәтижелері MITRE Engenuity ресми ресурсында жариялануы тиіс.
- Шешім жүйенің ағымдағы жай-күйін сұрату, инциденттерді, компрометация индикаторларын іздеу, оқиғалар аудитін жүргізу және саясаттарды басқару үшін бұлттық API-ді қолдауы тиіс
- Бұлттық API жүйеден деректерді оқу, сондай-ақ оларды жазу/өзгерту мүмкіндігін қолдауы тиіс
- Бұлттық API OAuth 2.0 аутентификация хаттамасын қолдауы тиіс
- Үшінші тарап шешімдерімен интеграция модульдерін басқару мүмкіндігі. Интеграция пакеттерін тікелей бұлттық басқару консолінен қосу мүмкіндігі
- SIEM модулінің және SIEM-жүйелерімен интеграцияның болуы
- Басқару консолімен байланыс болмаған немесе басқа техникалық қиындықтар туындаған жағдайда клиенттік модульдерді толық жоюға арналған утилитаның болуы
- Жинақталған деректерді жүйеден тыс JSON форматында басқа қорғау модульдерінде одан әрі пайдалану үшін беруге мүмкіндік беретін құралдың болуы
- Жүйе анықталған араласу тәсілдері және бұғатталған мінез-құлық бойынша интерактивті анықтаманы қолдауы тиіс
- Жеткізуші бір күнтізбелік жылға 4 000 лицензияны ұсынуы және бес жылға ұзарту мүмкіндігін қамтамасыз етуі тиіс

1. **SIEM және SOAR модулі**

- Жүйе жергілікті инфрақұрылымға тәуелділікті барынша азайта отырып, бұлттық орналастыру мүмкіндігін қолдауы тиіс.
- Модульдің базалық функционалдығы стандартты жеткізілім құрамына енгізілуі, бірыңғай консольден қолжетімді болуы және қосымша лицензияларсыз жұмыс істеуі тиіс
- Тәулігіне 1 петабайтқа дейінгі деректерді өңдеу үшін масштабталуды қолдау.
- Жүйені орналастыру уақыты қолжетімділік берілген сәттен бастап 48 сағаттан аспауы тиіс.
- SIEM модуліне қолжетімділік негізгі консольден жүзеге асырылуы тиіс
- Жүйе модулі әртүрлі көздерден деректер жинауды қолдауы тиіс, оның ішінде:
- Endpoint Detection and Response (EDR),
- осалдықтарды басқару шешімдері,
- желілік құрылғылар (IDS/IPS, фаерволдар),
- бұлттық платформалар (AWS, Azure, Google Cloud),
- дерекқорлар мен қосымшалар.

- Деректерді JSON, Syslog, CEF және LEEF форматтарында өңдеу мүмкіндігі болуы тиіс.
- Жүйе деректер ағындарын орталықтандырылған басқаруды, оларды нормализациялау және агрегаттау мүмкіндігін қамтамасыз етуі тиіс.
- Жүйе мінез-құлықты талдау және жасанды интеллект (AI) негізінде аномалиялар мен қауіптерді автоматты анықтауды қолдауы тиіс.
- MITRE ATT&CK негізінде қауіптерді жіктеуді қолдау, білім базасын кемінде әр 15 минут сайын жаңарту мүмкіндігімен.
- Модульдің функционалдығы қосымша лицензияларды пайдалану есебінен кеңейтілетін болуы тиіс
- Модуль функционалдығы кеңейтілген кезде жүйе қолда бар және көздерден келіп түсетін оқиғаларды талдауға арналған корреляциялық қағидаларды қамтуы тиіс
- Оқиғалар туралы қауіп контекстін, таралу жолдарын және жою жөніндегі ұсынымдарды қоса алғанда, егжей-тегжейлі ақпарат ұсыну мүмкіндігі.
- Жүйе деректерді өңдеу және іздеу жылдамдығын секундына кемінде 10 000 оқиға деңгейінде қамтамасыз етуі тиіс.
- Өнімділікті төмендетпей үлкен көлемдегі деректерді өңдеу үшін көлденең масштабтауды қолдау.
- Жүйе инциденттерді өңдеу үшін автоматты жұмыс процестерін (playbooks) құруды қолдауы тиіс.
- Құрылғыларды оқшаулау, IP-мекенжайларды бұғаттау және қауіпсіздік саясаттарын жаңарту сияқты әрекеттерді қоса алғанда, оқиғаларға автоматты түрде әрекет ету мүмкіндігі.
- SIEM модулінің базалық функционалы келіп түсетін көздерден логтарды нақты уақыт режимінде іздеу мүмкіндігін қамтамасыз етуі тиіс
- SIEM модулінің базалық функционалы пайдаланушының жеке корреляциялық қағидаларын құру мүмкіндігін қамтамасыз етуі тиіс
- SOAR функционалдығы базалық жеткізілім құрамына кіруі тиіс.
- Жүйе архитектурасы ISO 27001, SOC 2 және GDPR стандарттарына сәйкес келетін бұлттық платформада құрылуы тиіс.
- Жүйе MFA (көп факторлы аутентификация) қолдауы бар веб-интерфейс арқылы қолжетімділікті қамтамасыз етуі тиіс
- Деректер 90 күн ішінде талдау үшін қолжетімді болуы тиіс, инфрақұрылымға қосымша шығындарсыз ұзақ мерзімді сақтауды (1 жылға дейін) қамтамасыз ету мүмкіндігімен.
- Жүйе танымал SIEM-платформаларымен (Splunk, QRadar, ArcSight) API арқылы интеграцияны қолдауы тиіс.
- Компрометация индикаторларын (IOC) STIX/TAXII форматында импорттау мүмкіндігі.
- Жүйе деректерді үшінші тараптың аналитикалық құралдарына экспорттауды қолдауы тиіс.
- Жүйе деректерді беру кезінде және сақталған күйінде шифрлауды қамтамасыз етуі тиіс.
- Рөлдік қолжетімділікті басқару моделін пайдалана отырып, рұқсатсыз қолжетімділіктен қорғау іске асырылуы тиіс.
- Жүйедегі барлық әрекеттер үшін аудитті және логтарды жүргізуді орталықтандырылған басқаруды қолдау.
- Лицензия API шақыруларының шектеусіз санын және қосымша шығындарсыз жүйенің барлық функцияларын қолдауды қамтуы тиіс.
- Лицензиялау қосылған көздердің санына емес, өңделетін деректер көлеміне негізделуі тиіс.
- SIEM модуліне қолжетімділік антивирустық модуль мен мінез-құлықты бақылау және қауіптерге әрекет ету модульдерінің лицензиялары қолданылатын бүкіл кезеңге берілуі тиіс

1. **ОЖ қолдауы**

- Windows
  - Клиенттік жүйелер – Windows 11 (25H2, 24H2, 23H2, 22H2, 21H2); Windows 10 (22H2, 21H2, 1809, 1607, 1507); Windows 7 SP1; Windows 10/11 ARM64.
  - Серверлік жүйелер – Windows Server 2025, 2022/Core, 2019/Core, 2016/Core, 2012 R2, Storage Server 2012 R2, 2012, 2008 R2 SP1, Azure Local.
  - Ескірген жүйелер – Windows 8/8.1 және Falcon for Legacy Systems пайдаланылған кездегі өзге нұсқалар.
  - macOS – Tahoe 26, Sequoia 15, Sonoma 14 (Intel және Apple silicon).
  - Linux – AlmaLinux, RHEL және Rocky Linux 9.6–10.0; SLES 15 SP6; openSUSE Leap 15.6; Ubuntu 24.04.
  - Linux-тың өзге дистрибутивтеріне, архитектураларына және ядро нұсқаларына қолдау өндірушінің қолданыстағы үйлесімділік матрицасымен расталуы тиіс.

Бұлттық және виртуалдандырылған орталар – AWS, Microsoft Azure, Google Cloud Platform (GCP) және өндіруші қолдайтын VDI-орталар

1. **Техникалық талаптар**

Агент дискіде 75 МБ-тан артық орын алмауы тиіс.

Агент жедел жадтың 50 МБ-тан артық көлемін пайдаланбауы тиіс; сыни жағдайларда 70 МБ-қа дейін ұлғайтуға жол беріледі.

9. Ақпараттық қауіпсіздік құралдарына техникалық қолдау көрсету қызметтері бойынша SLA (Service Level Agreement – Қызмет көрсету деңгейі туралы келісім)

9.1. Жалпы ережелер

9.1.1. Осы Қызмет көрсету деңгейі туралы келісім (бұдан әрі – SLA) Орындаушының Тапсырыс берушіге ұсынатын ақпараттық қауіпсіздік құралдарына техникалық қолдау көрсету қызметтерінің сапа көрсеткіштерін айқындайды.

9.1.2. Техникалық қолдау Тапсырыс берушіге техникалық спецификацияда сипатталған Өндірушінің техникалық қолдау сервистерін 24x7 режимінде пайдалану құқығын беруді, оның ішінде техникалық қолдау порталына, жаңартуларға, сервистік келісімшартқа және техникалық қолдау қызметіне қолжетімділікті қамтиды.

9.2. Қызметтердің көрсетілгенін растау тәртібі

9.2.1. Қызмет көрсету мерзімі ішінде Орындаушы Тапсырыс берушіге ай сайын мынадай мәліметтерді қамтитын техникалық қолдау көрсету қызметтері туралы есеп ұсынады:

• өндірушілердің техникалық қолдау платформаларына қолданыстағы қолжетімділік туралы ақпарат;

• есепті кезеңде тіркелген өтініштердің тізбесі;

• өтініштерді қарау мәртебесі;

• өтініштерді өңдеудің бақылау мерзімдерінің сақталуы туралы мәліметтер;

• өндірушілер ұсынған жаңартулар мен хабарламалар туралы ақпарат (бар болса).

• Есепті кезеңдегі SLA көрсеткішін есептеу.

9.3. SLA орындалуын бақылау

9.3.1. Көрсетілген қызметтердің сапасын жалпы бағалау үшін Орындаушының қызметтерінің «SLA орындау деңгейі» көрсеткіші есептеледі.

9.3.2. Орындаушы Тапсырыс берушіге қолжетімділік коэффициенті кемінде 99,5 % болатын қызметтерді ұсынады.

9.3.3. SLA көрсеткішін есептеуді Орындаушы есепті айдың қорытындылары бойынша ай сайын жүзеге асырады.

9.3.4. SLA көрсеткіші осы құжатта белгіленген өтініштердің әрбір сыни деңгейі бойынша жеке есептеледі.

9.3.5. Егер есепті айда тиісті сыни деңгей бойынша SLA көрсеткіші 99,5 %-дан төмен болса, қызмет көрсету деңгейіне қойылатын талаптар орындалмаған болып есептеледі.

9.3.6. Тапсырыс беруші көрсетілген қызметтердің көлемі мен сапасын Орындаушының ай сайынғы есебі негізінде бақылайды.

9.3.7. Тапсырыс берушінің жазбаша сұрауы бойынша Орындаушы көрсетілген кезеңдегі қызмет көрсету нәтижелері бойынша қосымша талдамалық ақпарат ұсынады.

1-кесте. Өтініштерді өңдеудің басымдықтары мен бақылау мерзімдері (24x7 режимі)

Басымдық (Сыни деңгей)	**Бақылау мерзімі**	**Критерийлер**	**Жай-күйінің сипаттамасы**
1-деңгей (Сыни)	1 сағат	Сыни жағдай	Аппараттық немесе бағдарламалық қамтамасыз етудің ақаулығына байланысты жүйе толық қолжетімсіз. Мәселе Тапсырыс берушінің бизнес үшін сыни сервистеріне әсер етеді.
2-деңгей (Жоғары)	2 сағат	Жұмыс қабілеттілігінің елеулі бұзылуы	Аппараттық немесе бағдарламалық қамтамасыз етудің ақаулығына байланысты жүйенің жұмыс қабілеттілігі бұзылған немесе қауіп төнген. Бұзушылық бизнес үшін сыни сервистердің өнімділігіне әсер етеді.
3-деңгей (Орташа)	4 сағат	Сыни емес бұзушылық	Функционал тиімділігінің төмендеуі. Өнімділік баяулауы мүмкін. Мәселе бизнес үшін сыни сервистерге әсер етпейді.
4-деңгей (Төмен)	24 сағат	Консультациялық сұраулар	Жалпы мәселелер. Өнімнің функционалдық мүмкіндіктері туралы ақпарат ұсыну жөніндегі сұраулар.

Өтінішті жұмысқа қабылдаудың бақылау мерзімі – тіркелген сәттен бастап 15 минуттан аспайды.

9.4. SLA көрсеткіштерін есептеу әдістемесі

9.4.1. SLA көрсеткіштерін есептеу ай сайын жүргізіледі.

9.4.2. Өтініштердің әрбір сыни деңгейі бойынша SLA орындау көрсеткіші мынадай формула бойынша есептеледі:

SLAS= ((NT - NV) / NT) × 100 %

мұнда:

- SLAS - тиісті сыни деңгей бойынша есепті айдағы SLA орындау көрсеткіші;
- NT - есепті айдағы тиісті сыни деңгей бойынша өтініштердің жалпы саны;
- NV - есепті айда өңдеудің бақылау мерзімдері бұзылған тиісті сыни деңгей бойынша өтініштер саны.

9.4.3. Егер тиісті сыни деңгей бойынша есепті айдағы SLAS мәні 99,5 %-дан төмен болса, сервис деңгейіне қойылатын талаптар орындалмаған болып есептеледі.

10. ГОСТ

Орындаушы **ГОСТ** – СТ РК ISO/IEC 15408-3-2017 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялар қауіпсіздігін бағалау критерийлері» стандартымен танысуы тиіс. Сондай-ақ Орындаушы «Қазақтелеком» АҚ-ның ақпараттық қауіпсіздік саясатымен танысуы тиіс. СТ РК ISO/IEC 20000 стандартына сәйкес, Қоғамға тауарларды, жұмыстарды және қызметтерді ұсыну кезінде үшінші тұлғалардың «Қазақтелеком» АҚ-ның ақпараттық қауіпсіздік саясатымен танысуы қажет.

Қол қойған	Аубакир Улан Нурланулы
Қол қойылған күні	30.10.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1264050
способом Открытый тендер на понижение

Лот № 1 (3422-1 У, 4561505) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Акционерное общество "Казахтелеком"

Организатор: "Дирекция "Телеком Комплект" - филиал Акционерного общества "Казахтелеком"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	3422-1 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	ДЦБ_Доступ к программному обеспечению для защиты конечных устройств (компьютеров и серверов) от угроз EDR
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Алматы, г.Алматы, ул.Чайковского 39 (ДЦБ)
Условия поставки	-
Срок поставки	С даты подписания договора в течение 30 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Технические требования к программному обеспечению для защиты конечных устройств (компьютеров и серверов) от угроз

1. **Консоль управления**

• Развертывание консоли управления не должно требовать от заказчика выделения программных и аппаратных ресурсов

• Консоль управления и обработка собранных данных должны быть реализованы в облаке производителя решения

• Наличие ролевого доступа к консоли управления с возможностью гранулированного делегирования прав доступа

• Поддержка двухфакторной аутентификации для учетных записей пользователей консоли управления

• Обмен данными между консолью управления и модулями на конечных точках должен быть защищен с помощью TLS 1.2

• Наличие гибкого механизма поиска по всем разделам консоли для ускорения операций анализа, реагирования и триажа (приоритизации) инцидентов и/или маркеров

• Возможность назначения политик на группы конечных устройств

• Консоль должна позволять объединять конечные устройства как в статическом порядке, так и по динамическим критериям, среди которых:

- Тип ОС
- Сетевые параметры системы
- Рабочая станция/Сервер
- Статус защиты
- Версия клиентского модуля
- Решение должно иметь единый пользовательский интерфейс для всех функций администрирования – все операции по анализу инцидентов и реагированию на них должны осуществляться в пределах одной консоли
- Консоль управления не должна иметь ограничения по количеству администраторов/аналитиков
- Консоль управления должна поддерживать аудиты следующих типов:
- Аудит хостов
- Аудит действий пользователя
- Аудит подключений по API
- Аудит политик
- Аудит Real Time Response
- Аудит исключений файлов
- Консоль должна поддерживать возможность управления развернутыми модулями на конечных точках без необходимости использования VPN или других средств доступа к корпоративной сети (защита систем, находящихся за пределами корпоративного периметра)
- Консоль должна поддерживать совместную работу над инцидентами для команды аналитиков с возможностью делегации инцидентов и изменения их статуса
- Консоль управления должна обеспечивать отображение инцидентов в четырех основных формах с возможностью немедленного переключения между ними:
- Общая информация по каждому хосту
- Табличная с отображением вектора атаки
- Граф связей с отображением легенды и указанием развития атаки
- Временная шкала событий с описанием каждого события
- Возможность интуитивного масштабирования графов связей запущенных процессов для облегчения визуализации полученных данных и ускорения принятия решений
- Возможность мгновенного выполнения следующих действий при просмотре данных инцидента:
- Интерактивное подключение к системе для выполнения действий реагирования
- Сетевая изоляция
- Закрепление инцидента за конкретным членом команды
- Изменение статуса инцидента
- Поиск данных по системе, хэшу и имени процесса
- В консоли управления должна присутствовать дополнительная функциональность по автоматизации бизнес-процессов Workflow.

- Модуль Workflow должен обеспечивать гибкое создание сценариев автоматизации с возможностью внесения изменений «на лету» и предоставлять готовые шаблоны автоматизированных действий.

- Консоль управления должна быть единой для всех нижеперечисленных модулей

- Развертывание модуля не должно требовать перезагрузки ОС

- При обнаружении угроз модуль не должен использовать базы данных сигнатур

- В случае отсутствия связи конечной точки с консолью управления решение должно обеспечивать базовую защиту с применением анализа поведения и блокирования известных потенциально вредных операций (использование встроенной функциональности ОС для инфицирования системы и т. п.) до момента подключения к центральной консоли в течение 90 дней.

- Модуль должен поддерживать защиту от вмешательства и несанкционированной деинсталляции

- Возможность управления встроенным брандмауэром с помощью отдельных политик (для Windows, Mac систем). Управление с одного места.

- Решение должно уметь выявлять ранее неизвестное/уникальное вредоносное ПО

- Поддержка интеграции с Microsoft AMSI для улучшенного обнаружения атак с использованием скриптов

- Использование возможностей машинного обучения для улучшения обнаружения неизвестного или перепакованного вредоносного кода

- Использование облачной базы репутации для анализа файлов и их атрибутов

- Распознавание подозрительных вызовов системных инструментов, используемых для инфицирования систем

- Защита от эксплойтов, защита от манипуляций с памятью процессов

- Защита от кражи учетных данных или манипуляции с учетными записями

- Возможность передачи файлов с неизвестной репутацией в облако производителя для их статического и динамического анализа в системе класса «песочница»

- Модуль должен поддерживать возможность деактивации отправки файлов в облачную «песочницу» производителя

Доступ в консоль управления должен быть предоставлен на весь период действий лицензий подключаемых модулей

1. **Антивирусный модуль**

- Развертывание модуля не должно требовать перезагрузки ОС
- При обнаружении угроз модуль не должен использовать базы данных сигнатур
- В случае отсутствия связи конечной точки с консолью управления решение должно обеспечивать базовую защиту с применением анализа поведения и блокирования известных потенциально вредных операций (использование встроенной функциональности ОС для инфицирования системы и т. п.) до момента подключения к центральной консоли в течение 90 дней.
- Модуль должен поддерживать защиту от вмешательства и несанкционированной деинсталляции
- Возможность управления встроенным брандмауэром с помощью отдельных политик (для Windows, Mac систем). Управление с одного места.
- Решение должно уметь выявлять ранее неизвестное/уникальное вредоносное ПО
- Поддержка интеграции с Microsoft AMSI для улучшенного обнаружения атак с использованием скриптов
- Использование возможностей машинного обучения для улучшения обнаружения неизвестного или перепакованного вредоносного кода
- Использование облачной базы репутации для анализа файлов и их атрибутов
- Распознавание подозрительных вызовов системных инструментов, используемых для инфицирования систем

- Защита от эксплойтов, защита от манипуляций с памятью процессов
- Защита от кражи учетных данных или манипуляции с учетными записями
- Возможность передачи файлов с неизвестной репутацией в облако производителя для их статического и динамического анализа в системе класса «песочница»
- Модуль должен поддерживать возможность деактивации отправки файлов в облачную «песочницу» производителя

1. **Модуль отслеживания поведения и реагирования на угрозы**

- Развертывание модуля не должно требовать перезагрузки ОС
- Модуль должен поддерживать защиту от вмешательства и несанкционированной деинсталляции
- В поставляемый модуль должен входить модуль по анализу трафика сети и его анализ
- Сбор метаданных по запущенным процессам, сетевой активности, операциям на файловой системе на конечных точках
- Отслеживание последовательности изменений в системе для выявления аномалий и потенциально вредных операций
- Корреляция запущенных процессов с их владельцами и действиями пользователей
- Использование следующих реакций по реагированию на вмешательство:
- Карантин
- Удаление файла, каталога
- Остановка процесса, дерева процессов
- Выполнение команды ОС
- Выполнение произвольных скриптов
- Возможность исключения (запрета) передачи конкретных файлов в облако производителя решения по их расположению на файловой системе, с возможностью проверки выбранного шаблона перед применением политики
- Вся телеметрия и метаданные с конечных точек должны обрабатываться только в облаке производителя решения по зашифрованному каналу.
- Система должна поддерживать хранение данных, связанных с инцидентами не менее 90 дней с момента обнаружения
- Система должна поддерживать сохранение данных телеметрии (полный перечень метаданных) за последние 7 дней с момента их передачи в облако производителя с возможностью расширения по требованию заказчика или регулирующего органа
- Система должна поддерживать возможность интерактивного выполнения команд и скриптов на конечных точках для нейтрализации угрозы или следов ее пребывания в системе с поддержкой PowerShell, Bash, CMD, BAT с возможностью отслеживания результатов выполнения выбранного скрипта, с возможностью подключения аналитики и графического анализа
- Система должна поддерживать возможность формирования библиотеки часто используемых пользовательских скриптов для ускорения реагирования на инциденты и сохранения избранных (ранее примененных команд)
- Система должна поддерживать возможность сетевой изоляции выбранных систем с возможностью настройки конкретных сетей, которые будут доступны для систем в карантине, кроме консоли производителя
- Системы, для которых применяется сетевая изоляция (так называемый карантин), должны оставаться на связи с консолью управления (облаком производителя решения) для проведения оперативных манипуляций.
- Система должна разрешать проведение корректировки (выполнение команд и скриптов) без необходимости перезагрузки целевой системы
- Модуль должен поддерживать возможность сбора не менее 600 параметров запущенных процессов ОС
- Телеметрия с конечных точек должна индексироваться и поддерживать возможность поиска через поисковые запросы консоли управления
- Телеметрия конечных точек должна иметь возможность экспорта/загрузки
- Возможность создания дампа памяти выбранного процесса

1. **Модуль защиты Active Directory**

Решение должно обеспечивать автоматический аудит Active Directory:

- Привилегированных пользователей и их привилегии
- Учетные записи с компрометированными паролями
- Скрытые учетные записи администраторов и их привилегии

- Выявление общих учетных записей
- Выявление скомпрометированных учетных записей
- Дублирующиеся учетные записи
- Проверка совместимости с NTLMv2
- Учетные записи с привилегированными SID
- Слабо защищенные учетные записи с SPNs
- Эскалация привилегий непривилегированных пользователей

Решение должно обеспечивать Threat Hunting:

- Выявлять SMB-соединения между рабочими станциями
- Выявлять SMB-доступ к критическим серверам
- Выявлять RDP-сессии с использованием привилегированных учетных записей
- Выявлять SMB- и RDP-трафик пользователей с компрометированными паролями
- Active Directory Reconnaissance
- Распространенные техники латерального перемещения – PsExec, PAExec, WMI, RDP, Scheduled Tasks, CrackMapExec

Решение должно разрешать/запрещать доступы:

- Блокировать попытки и техники латерального перемещения
- Разрешать RDP-сессии к серверам, если они инициированы PAM-решениями (CyberArk, senhasegura и др.)
- Запрашивать дополнительную MFA-аутентификацию при подключении к критическим серверам
- Блокировать RDP-сессии, инициированные сервисными учетными записями
- Запрашивать MFA-аутентификацию при подключении к системам, к которым пользователь ранее не подключался (период обучения поведению пользователя не должен превышать 14 календарных дней)
- Запрашивать MFA-аутентификацию для критических веб-приложений, использующих учетные записи AD (например, VMware vCenter/vSphere)

Решение должно создавать базовый профиль поведения пользователя (baseline), иметь возможность сигнализировать об аномальном поведении, предотвращать его или запрашивать MFA-аутентификацию пользователя.

1. **Общие требования**

- Производитель решения должен участвовать в MITRE ATT&CK® Enterprise Evaluations; результаты последней завершенной оценки должны быть опубликованы на официальном ресурсе MITRE Engenuity.
- Решение должно поддерживать облачный API для запроса текущего состояния системы, поиска инцидентов, маркеров компрометации, аудита событий и управления политиками
- Облачный API должен поддерживать как возможность считывания данных из системы, так и их записи /модификации
- Облачный API должен поддерживать протокол аутентификации OAuth 2.0
- Возможность управления модулями интеграции со сторонними решениями. Возможность подключения пакетов интеграции непосредственно из облачной консоли управления
- Наличие модуля SIEM и интеграции с SIEM-системами
- Наличие утилиты для полного удаления клиентских модулей в случае отсутствия связи с консолью управления или других технических затруднений
- Наличие инструмента, позволяющего передавать накопленные данные за пределы системы в формате JSON для дальнейшего их использования в других модулях защиты
- Система должна поддерживать интерактивную справку по выявленным способам вмешательства и заблокированному поведению
- Поставщик должен предоставить 4 000 лицензий на один календарный год с возможностью продления на пять лет
- Срок действия ТП устанавливается с даты предоставления лицензии и действует в течение 365 (триста шестьдесят пять) календарных дней.

1. **Модуль SIEM и SOAR**

- Система должна поддерживать возможность облачного развертывания с минимальной зависимостью от локальной инфраструктуры.
- Базовая функциональность модуля должна быть включена в стандартную поставку, доступна из единой консоли и работать без дополнительных лицензий
- Поддержка масштабируемости для обработки до 1 петабайта данных в сутки.
- Время развертывания системы не должно превышать 48 часов с момента предоставления доступа.
- Доступ в модуль SIEM должен осуществляться из основной консоли
- Модуль системы должен поддерживать сбор данных из различных источников, включая:
- Endpoint Detection and Response (EDR),
- решения по управлению уязвимостями,
- сетевые устройства (IDS/IPS, фаерволы),
- облачные платформы (AWS, Azure, Google Cloud),
- базы данных и приложения.
- Должна быть возможность обработки данных в форматах JSON, Syslog, CEF и LEEF.
- Система должна обеспечивать централизованное управление потоками данных с поддержкой их нормализации и агрегирования.
- Система должна поддерживать автоматическое выявление аномалий и угроз на основе анализа поведения и искусственного интеллекта (AI).
- Поддержка классификации угроз на основе MITRE ATT&CK с возможностью обновления базы знаний не реже чем раз в 15 минут.
- Функциональность модуля должна быть расширяемой за счет использования дополнительных лицензий
- При расширении функциональности модуля система должна включать корреляционные правила для анализа имеющихся и поступающих от источников событий
- Возможность предоставления детализированной информации о событиях, включая контекст угрозы, пути распространения и рекомендации по устранению.
- Система должна обеспечивать скорость обработки и поиска данных не менее 10 000 событий в секунду.
- Поддержка горизонтального масштабирования для обработки больших объемов данных без ухудшения производительности.
- Система должна поддерживать создание автоматических рабочих процессов (playbooks) для обработки инцидентов.
- Возможность автоматического реагирования на события, включая изоляцию устройств, блокировку IP-адресов и обновление политик безопасности.
- Базовый функционал модуля SIEM должен иметь возможность поиска логов от поступающих источников в режиме реального времени
- Базовый функционал модуля SIEM должен иметь возможность создания собственных корреляционных правил
- Функциональность SOAR должна входить в базовую поставку.
- Архитектура системы должна быть построена на облачной платформе, соответствующей стандартам ISO 27001, SOC 2 и GDPR.
- Система должна обеспечивать доступ через веб-интерфейс с поддержкой MFA (многофакторной аутентификации)
- Данные должны быть доступны для анализа в течение 90 дней, с возможностью долгосрочного хранения (до 1 года) без дополнительных затрат на инфраструктуру.
- Система должна поддерживать интеграцию через API с популярными SIEM-платформами (Splunk, QRadar, ArcSight).
- Возможность импорта индикаторов компрометации (IOC) в формате STIX/TAXII.
- Система должна поддерживать экспорт данных в сторонние аналитические инструменты.
    - Система должна обеспечивать шифрование данных при передаче и в состоянии покоя.
    - Должна быть реализована защита от несанкционированного доступа с использованием ролевой модели управления доступом.
    - Поддержка централизованного управления аудитом и ведения логов для всех действий в системе.
- Лицензия должна включать неограниченное количество вызовов API и поддержку всех функций системы без дополнительных затрат.
- Лицензирование должно основываться на объемах обрабатываемых данных, а не на количестве подключенных источников.
- Доступ к модулю SIEM должен быть предоставлен на весь период действия лицензий антивирусного модуля и модуля отслеживания поведения и реагирования на угрозы.

1. **Поддержка ОС**

- Windows

- Клиентские системы – Windows 11 (25H2, 24H2, 23H2, 22H2, 21H2); Windows 10 (22H2, 21H2, 1809, 1607, 1507); Windows 7 SP1; Windows 10/11 ARM64.
- Серверные системы – Windows Server 2025, 2022/Core, 2019/Core, 2016/Core, 2012 R2, Storage Server 2012 R2, 2012, 2008 R2 SP1, Azure Local.
- Устаревшие системы – Windows 8/8.1 и иные версии при использовании Falcon for Legacy Systems.
- macOS – Tahoe 26, Sequoia 15, Sonoma 14 (Intel и Apple silicon).
- Linux – AlmaLinux, RHEL и Rocky Linux 9.6–10.0; SLES 15 SP6; openSUSE Leap 15.6; Ubuntu 24.04.
- Поддержка иных дистрибутивов Linux, архитектур и версий ядер должна подтверждаться актуальной матрицей совместимости производителя.

Облачные и виртуализированные среды – AWS, Microsoft Azure, Google Cloud Platform (GCP) и VDI-среды, поддерживаемые производителем

1. **Технические требования**

Агент не должен занимать более 75 МБ на диске.

Агент не должен использовать более 50 МБ оперативной памяти; в критических ситуациях допускается увеличение до 70 МБ.

9. SLA (Service Level Agreement – Соглашение об уровне сервиса)
по услугам технической поддержки средств информационной безопасности

9.1. Общие положения

9.1.1. Настоящее Соглашение об уровне сервиса (далее – SLA) определяет показатели качества оказания услуг технической поддержки средств информационной безопасности, предоставляемых Исполнителем Заказчику.

9.1.2. Техническая поддержка включает предоставление Заказчику права пользования сервисами технической поддержки Производителя описанных в технической спецификации в режиме 24x7, включая доступ к порталу технической поддержки, обновлениям, сервисному контракту и службе технической поддержки.

9.2. Порядок подтверждения оказания услуг

9.2.1. В течение срока оказания услуг Исполнитель ежемесячно предоставляет Заказчику отчет об оказании услуг технической поддержки, включающий:

- информацию о действующем доступе к платформам технической поддержки производителей;
- перечень зарегистрированных обращений за отчетный период;
- статус рассмотрения обращений;
- сведения о соблюдении контрольных сроков обработки обращений;
- информацию о предоставленных обновлениях и уведомлениях производителей (при наличии).
- Расчет показателя SLA за отчетный период.

9.3. Контроль выполнения SLA

9.3.1. Для проведения общей оценки качества оказанных Исполнителем услуг производится расчёт показателя «Уровень выполнения SLA».

9.3.2. Исполнитель предоставляет Заказчику услуги с коэффициентом доступности не менее 99,5 %.

9.3.3. Расчет показателя SLA осуществляется Исполнителем на ежемесячной основе по итогам отчетного месяца.

9.3.4. Показатель SLA рассчитывается отдельно по каждому уровню критичности обращений, установленному настоящим документом.

9.3.5. В случае если показатель SLA по соответствующему уровню критичности за отчетный месяц составляет менее 99,5 %, требования по уровню сервиса считаются невыполненными.

9.3.6. Заказчик осуществляет контроль объема и качества оказанных услуг на основании ежемесячного отчета Исполнителя.

9.3.7. По письменному запросу Заказчика Исполнитель предоставляет дополнительную аналитическую информацию по результатам оказания услуг за указанный период.

Таблица 1. Приоритеты и контрольные сроки обработки обращений (режим 24x7)

Приоритет (Уровень критичности)	**Контрольный срок**	**Критерии**	**Описание состояния**
Уровень 1 (Критичный)	1 час	Критическая ситуация	Система полностью недоступна вследствие неисправности оборудования или программного обеспечения. Проблема влияет на бизнес-критичные сервисы Заказчика.
Уровень 2 (Высокий)	2 часа	Значительное нарушение работоспособности	Работоспособность системы нарушена либо находится под угрозой вследствие неисправности оборудования или программного обеспечения. Нарушение влияет на производительность бизнес-критичных сервисов.
Уровень 3 (Средний)	4 часа	Некритичное нарушение	Снижение эффективности функционала. Производительность может быть замедлена. Проблема не оказывает влияния на бизнес-критичные сервисы.
Уровень 4 (Низкий)	24 часа	Консультационные запросы	Общие вопросы. Запросы на предоставление информации по функциональным возможностям продукта.

Контрольный срок принятия обращения в работу – не более 15 минут с момента регистрации.

9.4. Методика расчета показателей SLA

9.4.1. Расчет показателей SLA осуществляется ежемесячно.

9.4.2. Показатель выполнения SLA по каждому уровню критичности обращений рассчитывается по следующей формуле:

SLAS= ((NT - NV) / NT) × 100 %

где:

- SLAS - показатель выполнения SLA за отчетный месяц по соответствующему уровню критичности;
- NT - общее количество обращений по соответствующему уровню критичности за отчетный месяц;
- NV - количество обращений по соответствующему уровню критичности, по которым были нарушены контрольные сроки обработки.

9.4.3. В случае если значение SLAS за отчетный месяц по соответствующему уровню критичности составляет менее 99,5 %, считается, что требования по уровню сервиса не выполнены.

10.ГОСТ

Исполнитель должен ознакомится с **ГОСТ** - СТ РК ISO/IEC 15408-3-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». А так же Исполнитель должен ознакомится с Политикой информационной безопасности в АО "Казахтелеком". Согласно стандарта СТ РК ISO /IEC 20000, необходимо ознакомление с Политикой информационной безопасности в АО "Казахтелеком" третьими лицами при предоставлении Обществу товаров, работ и услуг.

Подписал	Аубакир Улан Нурланулы
Дата подписания	30.10.2026