ТЕХНИКАЛЫҚ СИПАТТАМА

1264050 сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 2 (3421-1 У, 4561504) 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	3421-1 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_Услуги по предоставлению лицензий на право использования ПО (Система раннего обнаружения кибер атак на основе сетевых ловушек). Срок лицензии 12 месяцев.
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

Желілік тұзақтар негізінде кибершабуылдарды ерте анықтау жүйесі.

1. **Бағдарламалық қамтамасыз етуге қойылатын талаптар**

Жеткізуші ұсынатын бағдарламалық қамтамасыз ету мынадай функционалдық мүмкіндіктерге ие болуы тиіс:

- Жүйенің толыққанды жұмыс істеуі үшін Тапсырыс берушіден Microsoft Windows бағдарламалық қамтамасыз етуін, жүйелік бағдарламалық қамтамасыз етуді және Жүйенің жұмысын қамтамасыз ететін мамандандырылған бағдарламалық қамтамасыз етуді қоса алғанда, қандай да бір қосымша бағдарламалық қамтамасыз етуді сатып алу талап етілмеуі тиіс.
- Жүйе мультитенанттылықты – бір басқару консолінде бір-бірінен оқшауланған аккаунттарды құру мүмкіндігін қолдауы тиіс. Бұл ретте жекелеген тенанттардың әкімшілері басқару консолінде тек өздерінің желі сегментіне қол жеткізе алады, ал бас әкімші барлық аккаунттарға қол жеткізе алады.
- Жүйе RBAC – жүйе әкімшілеріне құқықтар берудің рөлдік моделін қолдауы тиіс.
- Осы шешім басқару модулінде орындалған барлық әрекеттердің егжей-тегжейлі аудитін қолдауы тиіс. Өзгерістер енгізілген кезде аудит журналы өзгертілген параметрлердің бастапқы және соңғы мәндерін нақты көрсетуі тиіс.
- Осы шешім көп факторлы аутентификацияны (MFA) қолдауы тиіс. Уақытқа негізделген бір реттік пароль (TOTP) алгоритмін қолдау міндетті.
- Осы шешім техникалық мәселелерді Жеткізушінің қолдау қызметі автономды режимде жоюы үшін журналдар мұрағатын жасау мүмкіндігіне ие болуы тиіс.

- Осы шешім компоненттердегі ақауларды жоюға арналған құралдар жиынтығын қамтуы тиіс, оның ішінде ping, traceroute, htop, пакеттерді ұстап алу және т.б. болуы тиіс, бірақ олармен шектелмеуі керек.
- Осы шешім веб-интерфейсте тұзақтарды құру және жүйені жаңарту мәртебесі мен барысын көрсетуі тиіс.

1. **Жүйеге қойылатын талаптар**

Жүйе:

- VMWare және HyperV гипервизорларында орналастыру мүмкіндігін қолдауы тиіс;
- NetFlow немесе басқа трафик талдағыштарын пайдаланбай жұмыс істеуі тиіс;
- кез келген қосымша бағдарламалық қамтамасыз етуді (виртуализациялау БҚ-нан басқа), оның ішінде Microsoft Windows бағдарламалық қамтамасыз етуін, жүйелік бағдарламалық қамтамасыз етуді және жүйенің жұмысын қамтамасыз ететін мамандандырылған бағдарламалық қамтамасыз етуді сатып алуды талап етпеуі тиіс;
- қосымша лицензиялауды талап етпей, 20 VLAN шегінде кемінде 300 (үш жүз) белсенді тұзақты (операциялық жүйелердің, жабдықтың, сервистердің эмуляцияларын) имитациялау мүмкіндігіне ие болуы тиіс;
- әрбір тұзақ бірегей, өзіндік сипаттамалар жиынтығымен (MAC, IP, hostname, имитацияланатын сервистер және олардың баптаулары) болуы тиіс;
- тұзақтар IP-aliases негізіндегі масштабтау нұсқасын (әрбір тұзақтың бірнеше IP-мекенжайы болған кезде) пайдаланбауы тиіс, себебі бұл шабуылдаушыларға инфрақұрылымдағы бір типті алдамшы нысандарды анықтауды айтарлықтай жеңілдетеді;
- нақты желілік соңғы құрылғыларда қате деректерді (Breadcrumbs) – автоматты кірудің сақталған деректерін, имитацияланған дереккөздермен және желілік ресурстармен байланыстарды,
сақталған RDP және SSH сессияларын, дерекқорларды имитациялауға арналған есептік жазбалары бар конфигурациялық файлдарды және т.б. – 20 VLAN шегінде кемінде 5 (бес) мың жұмыс станциясына (компьютерлерге, ноутбуктерге, серверлерге және т.б.) қосымша лицензиялауды талап етпей құру және тарату мүмкіндігін ұсынуы тиіс;
- Ұсынылған шешім тұзақтарды мерзімді түрде:
    1. сыртқы веб-ресурстарға қосуы тиіс,
    2. DNS, mDNS, LLMNR және NetBIOS арқылы хост атаулары мен домендік атауларға сұрау жіберуі тиіс,
    3. SMB (Windows File Share) протоколы арқылы файлдық ресурстар тізімін сұратуы тиіс.

- нақты хосттарға жалған кэштелген деректерді тарату және құруға арналған ішкі утилиталарға ие болуы тиіс;
- SIEM/EDR-мен интеграциялану мүмкіндігіне ие болуы тиіс – SIEM-ге деректерді жіберу және одан алу;
- желілік шабуылдарды (bruteforce шабуылдарын, имитациялардағы сервистерге қосылу әрекеттерін анықтау) анықтауы, олардың критикалылық деңгейін және бағытталуын, қауіп түрі мен іске асырылу қағидатына қарамастан, санаттарға бөлуі тиіс;
- тұзақтарға қосылу тарихын және зиянкестің тұзақпен жасаған әрекеттерінің тарихын, бұзылған хосттың IP-мекенжайын, бұзылған есептік деректерді, өзара әрекеттесу протоколдарын/порттарын көрсете отырып көрсетуі тиіс;
- жүйенің жұмыс істеуі, оқиғалар және басқа да көрсеткіштер бойынша статистиканы көрсететін біріктірілген графикалық панельдерге ие болуы тиіс;
- жалған іске қосылулардың ең төмен деңгейін қамтамасыз ету үшін заңды сервистерді алып тастауға қосу мүмкіндігін қамтамасыз етуі тиіс. Пайдаланушы әрбір алып тастау үшін нақты уақыт аралығын көрсету мүмкіндігіне ие болуы тиіс;
- MiTM (man-in-the-middle) типіндегі шабуылдарды анықтауды жүзеге асыруы тиіс:
- ARP spoofing
- NBT/LLMNR/mDNS resolve poisoning
- HTTPS requests interception
- тұзақтарды толық автоматты режимде құру мүмкіндігіне ие болуы тиіс;
- киберқауіптерді анықтаудың сигнатурасыз әдісін қолдануы тиіс;
- Осы шешімде төменде көрсетілген тұзақтар (алдамшы нысандар) түрлерінің кемінде тізімі болуы тиіс.
    1. Microsoft Windows, RPC, WinRM, RDP-мен,
    2. Microsoft SMB file server,
    3. Linux OS серверлері,

4. QRadar web user interface,
5. VMware ESX web user interface,
6. FortiGate web user interface,
7. SCADA: HMI/PLC/Ethernet Processor/Modbus TCP Server,
8. DNS server,
9. Databases:
    - MySQL server,
    - PostgreSQL server.
10. FTP file server,
11. TFTP server,
12. Samba file server,
13. MQTT broker,
14. Telnet server,
15. Email servers:
    - Microsoft Outlook Web Access user interface,
    - Zimbra Collaboration Suite,
    - Kerio Connect Mail Server,
    - Roundcube Mail Server,
    - Vanilla Exim4 MTA,
16. VoIP:
    - Vanilla Asterisk PBX,
    - Asterisk with FreePBX Web UI,
    - 3CX Phone System,
    - Grandstream UCM6202 PBX

- Осы шешім дерекқор дамптары мен архивтерді тіркемелер ретінде пайдалана отырып, тұзақтарды пайдаланушы деректерімен автоматты түрде толтыру функционалын қамтуы тиіс.
- Осы шешім Windows тұзақтарын әртүрлі ОЖ нұсқаларымен және құрастыру нөмірлерімен, оның ішінде Windows Server 2003, Windows 8, Windows Server 2012 Datacenter, Windows Server 2008 R2 сияқты ескірген нұсқалармен құруды қолдауы тиіс.
- ОТ тұзақтары кемінде SIEMENS және Rockwell Automation PLC компаниясының Allen-Bradley веб-интерфейстерін эмуляциялауы тиіс.
- ОТ тұзақтары кемінде S7comm және Modbus TCP протоколдарын қолдауы тиіс.
- қолданыстағы желілік топология дизайнын қайта ұйымдастыруды талап етпей орналастырылуы тиіс;
- жүйе компоненттерін қайта орнатуды талап етпей масштабталуы тиіс;
- имитациялық тұзақтарды әртүрлі желілік сегменттерде орналастыру мүмкіндігіне ие болуы тиіс;
- Linux және Windows ОЖ басқаруындағы нақты желі хосттарында пассивті қате деректерді (Breadcrumbs) орналастыру мүмкіндігіне ие болуы тиіс;
- желілік активтердің өзара әрекеттесуін құру және визуализациялау мүмкіндігіне ие болуы тиіс;
- жүйенің барлық модульдерін орталықтандырылған басқаруды қамтамасыз етуі тиіс;
- интуитивті түсінікті интерфейске ие болуы және оны қызмет көрсету мен сүйемелдеуге мамандардың елеулі шығындарын талап етпеуі тиіс;
- өндірушінің техникалық қолдауымен қамтамасыз етілуі тиіс, оның құрамына:
- БҚ компоненттерінің, дерекқордың және Жүйенің толық әрі дұрыс жұмыс істеуі үшін қажетті басқа да БҚ-ның өзекті нұсқасына тегін жаңарту,
- БҚ іске пайдалануға енгізілгеннен кейін өндірушінің БҚ-ны жаңартуы және қолданыстағы қателерді түзетуі, жүйенің басқару компоненттерін қайта іске қоспай, проблемалық мәселелер туындаған жағдайда Орындаушыға немесе өндірушіге 12х5 режимінде жүгіну мүмкіндігімен;
- жүйеде бар базалық типтер негізінде желілік тұзақтардың өзіндік типтерін құру мүмкіндігіне ие болуы тиіс. Тұзақтардың жаңа типін жасағаннан кейін пайдаланушы қосымша әрекеттерсіз таңдалған типтегі бірнеше тұзақты бірден автоматты түрде құру мүмкіндігіне ие болуы тиіс. Тұзақтардың жаңа типтерінің конфигурациялары қарапайым және стандартталған мәтіндік түрде (YAML немесе JSON) болуы тиіс;
- Тапсырыс берушінің желісінде пайдаланылатын кез келген Web-сайт/Web-сервис негізінде желілік тұзақтар құру мүмкіндігіне ие болуы тиіс. Бұл тұзақтар Web-осалдықтарды қамтуы тиіс
- Веб-тұзақтарда конфигурациялауға арналған мынадай параметрлер болуы тиіс:
    - әртүрлі Web-серверлерді имитациялауға арналған Server-header
    - тұзаққа DoS-шабуылдарды болдырмауға арналған Rate-limit
    - рұқсат етілген HTTP-әдістер
    - Custom paths және осындай тұзақтардағы өзіндік файлдар, соның ішінде response

- өзінің еркін HTTP-headers қосу
- Web-тұзаққа арналған TLS-certificate

- Жүйе анықталған шабуылға байланысты оқиғаларды операторларды қарау және өңдеу үшін оқиғалардың көп санымен жүктемеу мақсатында бір Alert ретінде дәл жіктеп, біріктіруі тиіс;
- Жүйеде өңделген әрбір Alert бойынша мәртебелерді көрсете отырып, кіріктірілген IRMS-функционалы болуы тиіс;

- белсенді тұзақтар (high interaction honeypots) кемінде сканерлеуге жауап беру, есептік деректерді сұратуды орындау, графикалық және/немесе мәтіндік интерфейсті көрсету деңгейінде интерактивтілікті қамтамасыз етуі тиіс. Әрбір тұзақ бірегей, бір IP-мекенжайлы, IP-alias және full OS технологиясын пайдаланбайтын болуы тиіс.

- барлық компоненттерді толық орналастыру және жұмыс істеуі үшін аппараттық ресурстар мынадан аспауы тиіс:

1. 64 RAM
2. 16 vCPU
3. 2 Tb HDD

Қосымша функционал:

Жүйе инфрақұрылымның әлсіз тұстарын анықтау үшін әртүрлі тесттер мен симуляцияларды іске қосуға мүмкіндік беретін мониторинг функциясын қамтуы тиіс.

Мониторинг модулі желіні сканерлеу мүмкіндігіне ие болуы және алынған нәтижелер негізінде анықталған активтермен о дан әрі әрекеттерді орындауға мүмкіндік беруі тиіс.

Мониторинг модулі желілік сервистердің мынадай типтерін қамтуы тиіс: DNS, FTP, SSH, SAMBA, RDP, HTTP.

Мониторинг модулі Жүйеге интеграцияланған болуы және соңғы пайдаланушының қосымша компоненттерді қолмен неме се автоматты түрде орнатуын талап етпеуі тиіс.

Мониторинг модулінің тесттері MITRE матрицасындағы Reconnaissance және Initial
Access тактикаларын функционалы бойынша қамтуы тиіс.

Осы шешім қолжетімді Active Directory
(AD) инфрақұрылымына тұзақтар мен жалған пайдаланушыларды интеграциялау функционалын қамтуы тиіс.

Осы шешім AD ортасына қосылған компьютерлер үшін DNS-жазбаларды автоматты түрде құруды қолдауы тиіс.

Active
Directory инфрақұрылымына жалған ресурстарды қосуды желілік және қауіпсіздік әкімшілері алдын ала қарай алатын плат форма скрипттері арқылы автоматтандыру қажет.

Осы шешім жалған пайдаланушылардың белсенді мониторингін қамтамасыз етуі және Kerberoasting, AS-REP Roasting шабуылдарын және жалған пайдаланушыларды аутентификациялау үшін пайдалану әрекеттерін дәл анықтауы тиіс.

Шешім мониторинг үшін үш (3) немесе одан көп доменді қосу мүмкіндігін ұсынуы тиіс. Егер осы домендерге қатысты кез келген есептік деректер darknet-ке тарап кетсе, шешім дереу хабарлама беруі тиіс.

1. **Жеткізушіге қойылатын талаптар**

- жүйені орналастыру, әкімшілендіру және пайдалану бойынша техникалық құжаттаманы қазақ немесе орыс тілінде ұсыну;
- Жүйенің бағдарламалық қамтамасыз етуін Тапсырыс берушінің серверлерінде баптауды жүргізу және Тапсырыс берушіге Жүйе бойынша техникалық және пайдалану құжаттамасын ұсыну;
- Тапсырыс берушінің техникалық мамандарына (кемінде 3 адам) Жүйені әкімшілендіру және онымен жұмыс істеу мәселелері бойынша кеңес беру және оқыту қызметтерін (кемінде 40 сағат көлемінде) орыс тілінде ұсыну;
- Жүйеге қазақ және орыс тілдерінде 8х5 режимінде техникалық қолдаудың болуын қамтамасыз ету.
- Бағдарламалық қамтамасыз етуге қолжетімділікті ұсыну мерзімі – 12 (он екі) ай. Жеткізу мерзімі – шарт жасалған күннен бастап 30 (отыз) күнтізбелік күннен аспауы тиіс.

4. SLA (Service Level Agreement – Сервис деңгейі туралы келісім)
ақпараттық қауіпсіздік құралдарына техникалық қолдау көрсету қызметтері бойынша

4.1. Жалпы ережелер

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

4.1.2. Техникалық қолдау Тапсырыс берушіге техникалық спецификацияда сипатталған Өндірушінің техникалық қолдау сервистерін 24х7 режимінде пайдалану құқығын, оның ішінде техникалық қолдау порталына, жаңартуларға, сервистік келісімшартқа және техникалық қолдау қызметіне қолжетімділікті ұсынуды қамтиды.

4.2. Қызметтердің көрсетілгенін растау тәртібі

4.2.1. Қызметтер көрсету мерзімі ішінде Орындаушы ай сайын Тапсырыс берушіге техникалық қолдау көрсету қызметтері туралы мынадай ақпаратты қамтитын 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 болған жағдайда).
- Есепті кезеңдегі SLA көрсеткішін есептеу.

4.3. SLA талаптарының орындалуын бақылау

4.3.1. Орындаушы көрсеткен қызметтердің сапасына жалпы баға беру үшін «SLA орындалу деңгейі» көрсеткіші есептеледі.

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

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

4.3.4. SLA көрсеткіші осы құжатта белгіленген өтініштердің әрбір критикалылық деңгейі бойынша жеке есептеледі.

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

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

4.3.7. Тапсырыс берушінің жазбаша сұрауы бойынша Орындаушы көрсетілген кезеңдегі қызметтер көрсету нәтижелері бойынша қосымша талдамалық ақпарат ұсынады.

1-кесте. Өтініштерді өңдеудің басымдықтары және бақылау мерзімдері (24х7 режимі)

Басымдық (Критикалылық деңгейі)	**Бақылау мерзімі**	**Критерийлер**	**Күйдің сипаттамасы**
1-деңгей (Критикалық)	1 сағат	Критикалық жағдай	Жабдықтың немесе бағдарламалық қамтамасыз етудің ақаулығына байланысты жүйе толық қолжетімсіз. Мәселе Тапсырыс берушінің бизнес үшін критикалық сервистеріне әсер етеді.
2-деңгей (Жоғары)	2 сағат	Жұмыс қабілеттілігінің елеулі бұзылуы	Жабдықтың немесе бағдарламалық қамтамасыз етудің ақаулығына байланысты жүйенің жұмыс қабілеттілігі бұзылған немесе қауіпте тұр. Бұзушылық бизнес үшін критикалық сервистердің өнімділігіне әсер етеді.
3-деңгей (Орташа)	4 сағат	Критикалық емес бұзушылық	Функционалдың тиімділігінің төмендеуі. Өнімділік баяулауы мүмкін. Мәселе бизнес үшін критикалық сервистерге әсер етпейді.
	24 сағат	Консультациялық сұраулар	Жалпы сұрақтар. Өнімнің функционалдық

4-деңгей (Төмен)			мүмкіндіктері туралы ақпарат ұсыну жөніндегі сұраулар.

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

4.4. SLA көрсеткіштерін есептеу әдістемесі

4.4.1. SLA көрсеткіштерін есептеу ай сайын жүзеге асырылады.

4.4.2. Өтініштердің әрбір критикалылық деңгейі бойынша SLA орындалу көрсеткіші мынадай формула бойынша есептеледі:

SLAS= ((NT - NV) / NT) × 100 %

мұнда:

- SLAS - тиісті критикалылық деңгейі бойынша есепті айдағы SLA орындалу көрсеткіші;
- NT - есепті айдағы тиісті критикалылық деңгейі бойынша өтініштердің жалпы саны;
- NV - өңдеудің бақылау мерзімдері бұзылған тиісті критикалылық деңгейі бойынша өтініштер саны.

4.4.3. Егер тиісті критикалылық деңгейі бойынша есепті айдағы SLAS мәні 99,5 %-дан төмен болса, сервистік деңгей талаптары орындалмаған болып есептеледі.

5. ГОСТ

Орындаушы ГОСТ - СТ РК ISO/IEC 15408-3-2017 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялардың 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

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1264050
способом Открытый тендер на понижение

Лот № 2 (3421-1 У, 4561504) 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	3421-1 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_Услуги по предоставлению лицензий на право использования ПО (Система раннего обнаружения кибер атак на основе сетевых ловушек). Срок лицензии 12 месяцев.
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

Услуги по продлению лицензий на программное обеспечение «Многоуровневые ловушки»

1. **Требование к программному обеспечению**

Программное обеспечение, предоставленное Поставщиком, должно иметь следующие функциональные возможности:

- Для полноценного функционирования системы от Заказчика не требуется приобретение какого-либо дополнительного программного обеспечения, включая программное обеспечение Microsoft Windows, системное программное обеспечение и специализированное программное обеспечение, обеспечивающее работу Системы.
- Система должна поддерживать мультитенантность – возможность создания изолированных друг от друга аккаунтов, находящихся в одной консоли управления. При этом администраторы отдельных тенантов имеют доступ только к своему сегменту сети в консоли управления, а главный администратор имеет доступ ко всем аккаунтам.
- Система должна поддерживать RBAC – ролевую модель предоставления прав администраторам системы.
- Данное решение должно поддерживать подробный аудит всех действий, выполненных в модуле управления. Когда изменения изменяются, журнал аудита должен четко указывать исходное и конечное значение измененных настроек.
- Данное решение должно поддерживать многофакторную аутентификацию (MFA). Поддержка алгоритма одноразового пароля на основе времени (TOTP) обязательна.

- Данное решение должно иметь возможность создавать архив журналов для устранения технических проблем в автономном режиме службой поддержки поставщика.
- Данное решение должно включать набор инструментов для устранения неисправностей в компонентах, включающий, но не ограничивающийся, ping, traceroute, htop, захват пакетов и т.п.
- Данное решение должно отражать статус и ход создания приманок и обновления системы в веб-интерфейсе.

1. **Требования к системе**

Система должна:

- поддерживать возможность развертывания на гипервизорах VMWare и HyperV;
- функционировать без использования анализаторов трафика NetFlow или других анализаторов трафика;
- не требовать приобретения любого дополнительного программного обеспечения (кроме ПО виртуализации), в том числе программного обеспечения Microsoft Windows, системного программного обеспечения и специализированного программного обеспечения, обеспечивающего работу системы;
- иметь возможность имитировать не менее 300 трехсот активных ловушек (эмуляций операционных систем, оборудования, сервисов) в пределах 20 VLAN без необходимости их дополнительного лицензирования;
- каждая из ловушек должна быть уникальна, с собственным набором характеристик (MAC, IP, hostname, имитированные сервисы и их настройка);
- ловушки не должны использовать вариант масштабирования на основе IP-aliases (когда каждая ловушка имеет несколько IP-адресов), что существенно облегчает атакующим выявление однотипных приманок в инфраструктуре;
- предоставлять возможность создавать и распространять на реальных конечных устройствах сети ошибочные данные (Breadcrumbs) – сохраненные данные автовхода, связи с имитированными источниками данных, сетевыми ресурсами, сохраненные RDP и SSH-сессии, конфигурационные файлы с учетными записями под имитации баз данных и т.д. – для не менее 5 (пяти) тысяч рабочих станций (компьютеров, ноутбуков, серверов и т.п.) в пределах 20 VLAN без необходимости их дополнительного лицензирования;
- Предоставленное решение должно иметь возможность создавать приманки, периодически:
    1. подключаются к внешним веб-ресурсам,
    2. выполняют запросы имен хостов и доменных имен через DNS, mDNS, LLMNR и NetBIOS,
    3. запрашивают список файловых ресурсов через протокол SMB (Windows File Share).

- иметь внутренние утилиты для распространения и создания ложных кэшированных данных на реальные хосты;
- иметь возможность интеграции с SIEM/EDR – отправлять и получать SIEM;
- выявлять сетевые вмешательства (детектирование брутфорс атак, попытки подключения к сервисам на имитациях) категоризацию уровня их критичности, направленности, независимо от типа и принципа реализации угрозы;
- отображать историю подключений к ловушкам и историю манипуляции злоумышленника с ловушкой с указанием IP-адреса скомпрометированного хоста, скомпрометированных учетных данных, протоколов/портов взаимодействия;
- иметь интегрированные графические панели, отражающие статистику по функционированию системы, событиям и прочему;
- обеспечивать возможность добавления в исключение легитимных сервисов для обеспечения минимального уровня ложных срабатываний. Пользователь должен иметь возможность указать конкретные временные рамки для каждого из исключений;
- осуществлять детектирование MiTM (man-in-the-middle) типа атак:
- ARP spoofing
- NBT/LLMNR/mDNS resolve poisoning
- HTTPS requests interception
- возможность создания ловушек в полностью автоматическом режиме;
- без сигнатурный метод обнаружения киберугроз;
- Данное решение должно содержать по меньшей мере перечень типов ловушек (приманок) ниже.
    1. Microsoft Windows з RPC, WinRM, RDP,
    2. Microsoft SMB file server,
    3. Сервера на Linux OS,
    4. QRadar web user interface,
    5. VMware ESX web user interface,

6. FortiGate web user interface,
7. SCADA: HMI/PLC/Ethernet Processor/Modbus TCP Server,
8. DNS server,
9. Databases:
    - MySQL server,
    - PostgreSQL server.
10. FTP file server,
11. TFTP server,
12. Samba file server,
13. MQTT broker,
14. Telnet server,
15. Email servers:
    - Microsoft Outlook Web Access user interface,
    - Zimbra Collaboration Suite,
    - Kerio Connect Mail Server,
    - Roundcube Mail Server,
    - Vanilla Exim4 MTA,
16. VoIP:
    - Vanilla Asterisk PBX,
    - Asterisk with FreePBX Web UI,
    - 3CX Phone System,
    - Grandstream UCM6202 PBX

- Данное решение должно включать функциональность автоматического заполнения приманок пользовательскими данными с использованием дампов базы данных и архивов в качестве вложений..
- Данное решение должно поддерживать создание приманок Windows с различными версиями ОС и номерами сборок, включая устаревшие, такие как Windows Server 2003, Windows 8, Windows Server 2012 Datacenter, Windows Server 2008 R2.
- Приманки ОТ должны эмулировать веб-интерфейсы как минимум SIEMENS и Allen-Bradley от Rockwell Automation PLC.
- Приманки ОТ должны поддерживать как минимум протоколы S7comm и Modbus TCP.
- развертывание без необходимости реорганизации дизайна существующей сетевой топологии;
- масштабирование без необходимости переустановки компонентов системы;
- возможность размещения ловушек-имитаций в разных сетевых сегментах;
- возможность размещения пассивных ошибочных данных (Breadcrumbs) на реальных хостах сети под управлением ОС Linux и Windows;
- возможность построения и визуализации взаимодействия сетевых активов между собой;
- обеспечивать централизованное управление всеми модулями системы;
- иметь интуитивно понятный интерфейс и не требует существенных затрат специалистов на его обслуживание и сопровождение;
- обеспечиваться технической поддержкой производителя, включающей:
- бесплатное обновление до актуальной версии компонентов ПО, базы данных и другого ПО, необходимого для полного и корректного функционирования Системы,
- обновление ПО и исправление существующих ошибок производителем после запуска ПО в эксплуатацию, без перезапуска управляющих компонентов системы , с возможностью обращения к Исполнителю или производителю в случае возникновения проблемных вопросов в режиме 12x5;
- давать возможность создавать собственные типы сетевых ловушек на основе существующих в системе базовых типов. После создания нового типа ловушек пользователь должен иметь возможность автоматически создавать сразу более одной ловушки выбранного типа без дополнительных манипуляций. Конфигурации новых типов ловушек имеют буты в простом и стандартизированном текстовом виде (YAML или JSON);
- иметь возможность создавать сетевые ловушки на основе любого Web-сайта/Web-сервиса, используемого в сети Клиента. Эти ловушки должны включать в себя Web-уязвимости
- Веб-ловушки должны иметь следующие параметры для конфигурации:
    - Server-header для имитации разных Web-серверов
    - Rate-limit для предотвращения DoS-атак на ловушку
    - Разрешенными HTTP-методами
    - Custom paths и собственными файлами на таких ловушках, включая response
    - Добавление собственных произвольных HTTP-headers
    - TLS-certificate для Web-ловушки

- Система должна точно классифицировать и совмещать события, связанные с задетектированной атакой в один Alert, чтобы не перегружать операторов системы большим количеством событий для просмотра и обработки;
- Система должна иметь встроенный IRMS-функционал, с указанием статусов по каждому из проработанных Alerts;

- активные ловушки (high interaction honeypots) должны обеспечивать интерактивность на уровне по меньшей мере ответы на сканирование, выполнение запроса учетных данных, отображение графического и/или текстового интерфейса. Каждая ловушка должна быть уникальной, с одним IP-адресом, без использования IP-alias и full OS технологии.

- для полноценного развертывания и функционирования всех компонентов системы должно требоваться аппаратных ресурсов не более:

1. 64 RAM
2. 16 vCPU
3. 2 Tb HDD

Дополнительный функционал:

Система должна включать функцию мониторинга, позволяющую запускать разные типы тестов и симуляций для выявления слабых мест инфраструктуры.

Модуль мониторинга должен иметь возможность производить сканирование сети и на основе полученных результатов разрешать дальнейшие действия с выявленными активами.

Модуль мониторинга должен включать следующие типы сетевых сервисов: DNS, FTP, SSH, SAMBA, RDP, HTTP.

Модуль мониторинга должен быть интегрирован в Систему и не требовать ручной или автоматической установки конечным пользователем дополнительных компонентов.

Тесты модуля мониторинга должны покрывать своим функционалом тактики Reconnaissance и Initial Access с матрицы MITRE.

Данное решение должно включать в себя функциональность интеграции приманок и фальшивых пользователей в доступную инфраструктуру Active Directory (AD).

Данное решение должно поддерживать автоматическое создание DNS-записей для компьютеров, добавленных в среду AD.

Добавление фальшивых ресурсов в инфраструктуру Active Directory должно быть автоматизировано с помощью скриптов платформы, которые могут быть предварительно просмотрены сетевыми и администраторами безопасности.

Данное решение должно обеспечивать активный мониторинг фальшивых пользователей и точно выявлять атаки Kerberoasting, AS-REP Roasting и попытки использования фальшивых пользователей для аутентификации.

Решение должно предоставлять возможность добавления трех (3) или более доменов для мониторинга. Если любые учетные данные, связанные с этими доменами, оказываются утекающими в даркнете, решение должно немедленно вызвать уведомление.

1. **Требования к Поставщику**

- предоставить техническую документацию по развертыванию, администрированию и использованию системы на казахском либо русском языке;
- провести настройки программного обеспечения Системы на серверах Заказчика и предоставить Заказчику техническую и эксплуатационную документацию на Систему;
- предоставить услуги по вопросам консультирования и обучения технических специалистов Заказчика (не менее 3 человек) администрированию и работе с Системой (в объеме не менее 40 часов) на русском языке;
- обеспечить наличие технической поддержки Системы в режиме 8х5 на казахском и русском языках.
- Срок предоставления доступа к программного обеспечения – 12 (двенадцать) месяцев. Срок поставки – не более 30 (тридцати) календарных дней с даты заключения договора.

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

4.1. Общие положения

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

4.1.2. Техническая поддержка включает предоставление Заказчику права пользования сервисами технической поддержки Производителя описанных в технической спецификации в режиме 24х7, включая доступ к порталу технической поддержки, обновлениям, сервисному контракту и службе технической поддержки.

4.2. Порядок подтверждения оказания услуг

4.2.1. 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.

4.3. Контроль выполнения SLA

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

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

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

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

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

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

4.3.7. 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.

4.4. Методика расчета показателей SLA

4.4.1. Расчет показателей SLA осуществляется ежемесячно.

4.4.2. 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.

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

5. 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