

Тауарларды, жұмыстарды, көрсетілетін қызметтерді сатып алу бойынша тендерға қатысуға алдын ала рұқсат беру хаттамасы № 80742-Т

23.04.2025 17:05:05

Тапсырыс беруші* «БІРЫҢҒАЙ ЖИНАҚТАУШЫ
ЗЕЙНЕТАҚЫ ҚОРЫ» АКЦИОНЕРЛІК
ҚОҒАМЫ

Тендер № 80742

Тендер атауы Бағдарламалық жасақтама қолдану
құқығына лицензия ұсыну бойынша
қызмет көрсетулер

Ұйымдастырушының атауы «БІРЫҢҒАЙ ЖИНАҚТАУШЫ
ЗЕЙНЕТАҚЫ ҚОРЫ» АКЦИОНЕРЛІК
ҚОҒАМЫ

Ұйымдастырушының мекенжайы Қазақстан, Алматы қ., Медеу
ауданы, Медеу ауданы, Самал- 2
ықшамауданы, дом №97, нежилое
помещение №13,

**Толықтырылған өтінімдерді
қабылдаудың аяқталу күні** 2025-04-29 10:00:00

Тендерлік комиссияның құрамы:

№	Т.А.Ә.	Ұйымдағы лауазымы	Комиссиядағы рөлі
1	Комиссияның мүшесі 1	Комиссия мүшесінің лауазымы 1	Төраға
2	Комиссияның мүшесі 2	Комиссия мүшесінің лауазымы 2	Төрағаның орынбасары
3	Комиссияның мүшесі 3	Комиссия мүшесінің лауазымы 3	Комиссияның мүшесі
4	Комиссияның мүшесі 4	Комиссия мүшесінің лауазымы 4	Комиссияның мүшесі
6	Комиссияның мүшесі 6	Комиссия мүшесінің лауазымы 6	Комиссияның мүшесі
7	Комиссияның мүшесі 7	Комиссия мүшесінің лауазымы 7	Хатшы

Жалпы сомасы көрсетілген сатып алынатын тауарлар, жұмыстар, көрсетілетін қызметтер тізбесі 84977196.42 теңге

№	Лоттың №	Лоттың атауы	Сатып алынатын тауарлар, жұмыстар, көрсетілетін қызметтердің сипаттамасы	Саны	Бірлік үшін бағасы, теңге	Сатып алу үшін бөлінген сома, теңге
1	238372-T2	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер	Антивирустық бақылау бағдарламалық қамтамасыз етуді пайдалану, зиянды әрекеттерді анықтау және зерттеу құқығына жазылу қызметтері	1.000	84977196.42	84977196.42

Лоттың № : 238372-T2

Лоттың атауы : Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Сатып алынатын тауарлар, жұмыстар, көрсетілетін қызметтердің сипаттамасы : Антивирустық бақылау бағдарламалық қамтамасыз етуді пайдалану, зиянды әрекеттерді анықтау және зерттеу құқығына жазылу қызметтері

Тендерлік комиссия мүшелерінің дауыс беру нәтижелері:

"ТWare" (АйТиваре) жауапкершілігі шектеулі серіктестігі, 121040015817			
№	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдама себебі
1	Комиссияның мүшесі	өткізілді	
2	Тараға	өткізілді	
3	Комиссияның мүшесі	өткізілді	
4	Комиссияның мүшесі	өткізілді	
5	Тарағандық орынбасары	өткізілді	
ТОВАРИШЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "TRADE IT", 22114003126			
№	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдама себебі
1	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген
2	Тараға	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген
3	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген
4	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген
5	Тарағандық орынбасары	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген
ТОВАРИШЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "THERION", 170540022814			
№	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдама себебі
1	Комиссияның мүшесі	өткізілді	
2	Тараға	өткізілді	
3	Комиссияның мүшесі	өткізілді	
4	Комиссияның мүшесі	өткізілді	
5	Тарағандық орынбасары	өткізілді	
ТОВАРИШЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ADELINE", 070140016160			
№	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдама себебі
1	Комиссияның мүшесі	өткізілді	

			<p>Кағидалардың 93-тармағының 1) тармақшасына басыпалық ала отырып жіберілме, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Талсырас берушінің техникалық ерекшелігін талаптарына сәйкес келмейді, атап айтқанда:</p> <p>1) Әлеуетті жеткізушінің техникалық ерекшелігін 4-бөлімде мынадай тармақтар мен ұсыныстар жок:</p> <p>A) Бағдарламалық құралды/вирусы қарсы қорғаныс модулінде мынадай функционалдық мүмкіндіктер жүзеге асқырау тиіс:</p> <ul style="list-style-type: none"> • жүктеушінің Web беттеріндегі баннерлер мен қалқымағы тереңдері бұтаттау; • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • көз көлпін тигізгі есептеу жолдарындағы қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдарды қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаптарды қосу, редакциялау, белгілі бір мазмұндық ресурстарға, өндіруші жасаған және динамикалық түрде жаңартылатын санақта, сондай-ақ ақпарат түріне (аудио, видео және т.б.) көп жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылауды ұяқат аралықтарына өлгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory үшін белгілі бір пайдаланушыларға таяғайлау; • резервті сақтау қоймасына объектілерді қалпына келтіруге құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құрыстарын баптау; • арнайы жүзеге ағачты құрал, Single Sign On технологиясын қолдай отырып, толық дерексіз шифрлау, UEFI жүзілерін қоллау; • жүзеге ағачты немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қоллау; • шифрланатын контентті әкемді қорғауға болатын файлдары шифрлау (орналасқан жері бойынша, көнеуі бойынша, файлды жасайтын қосымша бойынша); • таспадан қолданбалар тарапаны шифрланған файлдарға көп жеткізуге шектеу қиғтарыны болуы, сондай-ақ құпия сөздің көмегімен ұянымыз тиіс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұяны жеткізілетін тиіс файлдарды шифрлау және шифрлану шұға мүмкіндік беретін жұмыс ресшіні орнату болатын алмабыз медиадағы деректерді шифрлау. <p>B) Windows серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • қорғанысшы MAC мекенжайына үшін ARP-протоколдарды осалдықтырды пайдаланатын желілік қауіп-қатерлерді қорғау; • резервті сақтау қоймасына объектілерді қалпына келтіруге құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құрыстарын баптау. <p>C) MacOS жұмыс станцияларына арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар:</p> <ul style="list-style-type: none"> • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаптарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартылатын белгілі бір ресурстарға немесе ресурстар санаптарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірінші басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискеге толық көп жеткізу құралдарының пайда болуын ақауатты түрде бақылау және құралдар берілгеннен кейін жаңағы жүйеші көнеуілерді орнату мүмкіндігі. <p>D) Linux жұмыс станциялары мен серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар:</p> <ul style="list-style-type: none"> • Marea 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйені желілік экраны басқару; • SkipPain/GetFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. <p>E) Файлдық серверлерді, қаспоярған ауқымдағы серверлерді, Windows терминалдық серверлерін вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • мақилалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйені желілік экраны басқару; • топталық қауіп-қатерлерді қорғау (Сайфай тәуелсіз); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алды ала жасаған және динамикалық түрде жаңартылатын санақта көп жеткізуге нақты тыйым салуды немесе рұқсатты қосу. <p>F) Мобилді құрылғыларды вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • қосымшаларды іске қосуға бейімделуі жүйелік қосымшаларды бұтаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарламаларды жіберу; • Wi-Fi және bluetooth модульдерін, сондай-ақ мобилді құрылғы камерасын пайдалануға тыйым салу; • орнатуға мидетті қосымшаларды қорғау. <p>G) Windows OJ негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядты/64-разрядты; • MySQL Standard Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MySQL Enterprise Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MariaDB 10.1 (10.1.30 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.3 (10.3.22 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.4 (10.4.26 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.5 (10.5.17 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB Server InnoDB сақтау кіші жүйесі бар 10.3 32-разрядты/64-разрядты; • MariaDB Galera Cluster InnoDB сақтау кіші жүйесі бар 10.3 32-разрядты/64-разрядты; • PostgreSQL 13.x 64-разрядты; • PostgreSQL 14.x 64-разрядты; • PostgreSQL 13.x (барлық редакция); • PostgreSQL Pro 14.x (барлық редакция); <p>H) Пайдаланушы жүзеге кірген есептік жазбаға, ағындағы IPv4 мекенжайына және компьютердің қай ОУ немесе қандай қауіпсіздік тобына байланысты вирусы қарсы шешімін баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқалар:</p> <ul style="list-style-type: none"> • клиенттік машиналар тарапын бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тексілеу; • виртуалды машиналар желісіні таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобилді құрылғыларды серверлерден орыснату; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұянымыз көз көлпін компьютерлерді көрсетуі; • Windows Failover Clustering қоллауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталына болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобилді құрылғыға орнату, мобилді құрылғыларды қарау, бұтатуды пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобилді құрылғысында деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі тиіс; • ОЖ үлгілерімен жұмыс істеу құралдарының болуы: нақты немесе виртуалды машина негізінде мақсатты ОЖ үлгісін жасау, үлгіні басқарушы тандаған компьютерлерге, соның ішінде «Жалаңаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жинақталған қосу мүмкіндігі қамтамасыз етуі тиіс; • дистрибутивтерден (WIM) операциялық жүйені үлгісін импорттау мүмкіндігі; • лицензияны пайдалануды бұзылғаны немесе лицензияның қолдану мерзімінен асып кеткені туралы басқарушы хабарлау мүмкіндігі бар компьютерде орнатылған бөгет ЕЖ лицензияларын бақылау жүйесінің болуы; • бөгет қосымшаларға арналған орнату шапқартын автоматты түрде қосу (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалының қоллауы; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылар бар желілерді құрау мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; <p>I) Linux OJ базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жок:</p> <p>Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқаларын операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядты/64-разрядты; • Debian GNU/Linux 10.x (Buster) 32-разрядты/64-разрядты; • Debian GNU/Linux 11.x (Bullseye) 32-разрядты/64-разрядты; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядты; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядты; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядты; • CentOS 7.x 64-разрядты; • Red Hat Enterprise Linux Server 7.x 64-разрядты; • Red Hat Enterprise Linux Server 8.x 64-разрядты; • Red Hat Enterprise Linux Server 9.x 64-разрядты; • SUSE Linux Enterprise Server 12 (барлық жаңарту пакеті) 64-разрядты; • SUSE Linux Enterprise Server 15 (барлық жаңарту пакеті) 64-разрядты; • Oracle Linux 7 64-разрядты; • Oracle Linux 8 64-разрядты; • Oracle Linux 9 64-разрядты; • жайта бөлінегі триггерлердің неарақиялары; • виртуалды машиналар желісіне таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүктелетін жаңартуларды басқарылатын құрылғыларға орнатас бұрын жұмысқа қабылдануы мен қателерді тексеру мүмкіндігі; • басты сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйесі бар серверлерді бағындыру ретінде басқару; <p>II) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Агенттерден көптеген оқиғаларды өзі арқылы просигне арналған жөелген бағдарламалық компоненттері, сенсорларға бар. Сенсорлар жүйені негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компоненттері Linux негізінде орналастырылуы болуы; • Өңделетін сервердің компоненттері KVM виртуализациясына агент орнатқан хосттардың шектеулі санын және пошта мен желілік трафик оқиғаларының шектеулі санын бақылау үшін орналастыруға болуы; • Бағдарламаның масштабтау параметрлерін баптау мүмкіндігі болуы тиіс. Сіз хосттардың санын және жоспарланатын сақтау және оқиғалар базасының көлемін көрсете аласыз. Бағдарлама серверді қорғайтын параметрлерге сәйкес бағтайды. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс - веб-интерфейс қолданылады. Егер жеке кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларына алынған файлдары талдау арналған YARA қағидалары жұту мүмкіндігі; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға өңдер не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді тандау мүмкіндігі; • Құрылғының объектілерді талдау және жіберуді пайдаланушы қағидаларын баптау арқылы анықды мазмұнын бар-жоғына алынған файлдар мен сіттемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жұтқу және орнату мүмкіндігі болуы тиіс; • Құрылғының пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтама жұмыс сиксты параметрлерді баптау мүмкіндігі болуы тиіс; • Құрылғыға табылған оқиғалар ағышын визуализациялау мүмкіндігі; • Тапандың контексті шығару мүмкіндігі; <p>Трафикті Ресур:</p> <p>Файлдардың сәмделері:</p> <ul style="list-style-type: none"> • «Құрылғы» ортасындағы объект белсенділігінің лога; • «Құрылғы» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоқы бойынша жүйенің негізгі компоненттерін жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару сервері бір Құрылғыш компоненттерінің серверлеріне қосу мүмкіндігі. <p>2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірілуші веб-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, ЕЖ өндірілушінің ресми веб сайты (https://www.sputnik.com/) деп аталатын осындай сайтты сондай-ақ осы сайтты Әлеуетті жеткізуші өзінің төңіректері етіміне беруі шешімдеріне қолданылуы өзінің болуы расталмақдай.</p> <p>3) техникалық ерекшеліктің 3-бөліміне сәйкес: Әлеуетті жеткізуші Тапсырас беруші лицензия берген күннен бастап кемінде 24 ай мерзімге вирусы қарсы басқайтын бағдарламалық жасақтаманы пайдалану және анықды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖИШ сервисіне 24 айға техникалық қолдауды бірге лицензияға жылдық жалақымен жеткізетін тұрақты өндірілуші авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынады.</p> <p>4) Әлеуетті жеткізуші ұсынаған Elite Sudio-ның атауы 19.03.2025 жылғы сертификаттың (осы сертификаттың CASP өткендігі үшін Sudio Эмирге берілген тұрақты нотариалды куәландырылған аудармасымен) Тапсырас берушінің техникалық ерекшелігін 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтама ұсынылған сертификатталған жазықсыз сертификатталған жүйеші иеліктерден төмен емес, дөңгелегі қамтамасыз ету туралы ақпарат расталмақдай.</p>
--	--	--	---

		<p>Кағидалардың 93-тармағының 1) тармақшасына басшылыққа ала отырып жіберілмеі, себебі Әлеуметті жеткізушінің техникалық ерекшелігі Талсырсы берушінің техникалық ерекшелігін талаптарына сәйкес келмейді, атап айтқанда:</p> <p>1) Әлеуметті жеткізушінің техникалық ерекшелігін 4-бөлімдегі мынадай тармақтар мен ұсыныстар жок:</p> <p>A) Бағдарламалық құралды/вирусы қарсы қорғаныс модулінде мынадай функционалдық мүмкіндіктер жүзеге асырмауы тиіс:</p> <ul style="list-style-type: none"> • жүктеулетін Web беттеріндегі баннерлер мен қалқымағы тереңдері бұтаттау; • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • көз көлден тигенді есетуі желілердегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдарды қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санааттары қосу, редакциялау, белгілі бір мазмұндық ресурстарға, өндіруші жасаған және динамикалық түрде жанартағын санақта, сондай-ақ ақпарат түріне (аудио, видео және т.б.) көп жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылауды ұнатқ арналарын өңгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory үшін белгілі бір пайдаланушыларға таяғайлау; • резервті сақтау қоймасына объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құрыстарын баптау; • арнайы жүзеге ағачты құрал, Simple Sign On технологиясын қолдай отырып, толық дерексіз шифрлау, UEFI жүйелерін қоллау; • жүктеу ағачты немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қоллау; • шифрланатын контентті әкемеді қорғауға болатын файлдары шифрлау (орналасқан жері бойынша, көнеуі бойынша, файлды жасайтын қосымша бойынша); • тасқалған қолданбалар тарапаны шифрланған файлдарға көп жеткізуге шектеу қойылатын болуы, сондай-ақ құпия сөздің көмегімен ұйымның тасқалған транскрипциялауға мүмкіндік беретін технологияның болуы; • ұйым желісімен тасқалған файлдары шифрлау және шифрлануға мүмкіндік беретін жұмыс рөлінің орнатуы болатын алабына медициналық деректері шифрлау. <p>B) Windows серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • құралдығын MAC мекенжайына қолдану үшін ARP-протоколдағы осалдықтарды пайдаланатын желілік қауіп-қатерлерді қорғау; • резервті сақтау қоймасына объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құрыстарын баптау. <p>C) MacOS жұмыс станцияларына арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар:</p> <ul style="list-style-type: none"> • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санааттары қосу, редакциялау, өндіруші жасаған және динамикалық түрде жанартағын белгілі бір ресурстарға немесе ресурстар санаатарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірінші басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискеге толық көп жеткізу құралдарының пайда болуын ақауатты түрде бақылау және құралдар берілгеннен кейін жаңа желілік көнеуілерді орнату мүмкіндігі. <p>D) Linux жұмыс станциялары мен серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар:</p> <ul style="list-style-type: none"> • Marea 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйені желілік экраны басқару; • SkipPain/GetFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. <p>D) Файлдық серверлерді, қаспоярған ауқымдағы серверлерді, Windows терминалдық серверлерін вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • мақилалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйені желілік экраны басқару; • топталық қауіп-қатерлерді қорғау (Сайфок тәсілімен); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндық ресурстарға, өндіруші алдына ала жасаған және динамикалық түрде жанартағын санақта көп жеткізуге нақты тыйым салуды немесе рұқсатты қосу. <p>E) Мобилді құрылғыларды вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • қосымшаларды іске қосуға жүйелік қосымшаларды бұтаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарламаларды жіберу; • Wi-Fi және bluetooth модульдерін, сондай-ақ мобилді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды қорғау. <p>Ж) Windows OX негізіндегі орталықтандырылған басқару, мониторингілеу және жанарту бағдарламалық құралдарына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядты/64-разрядты; • MySQL Standard Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MySQL Enterprise Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MariaDB 10.1 (10.1.30 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.3 (10.3.22 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.4 (10.4.26 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.5 (10.5.17 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB Server InnoDB сақтау кіші жүйесі бар 10.3 32-разрядты/64-разрядты; • MariaDB Galera Cluster InnoDB сақтау кіші жүйесі бар 10.3 32-разрядты/64-разрядты; • PostgreSQL 13.x 64-разрядты; • PostgreSQL 14.x 64-разрядты; • PostgreSQL 13.x (барлық редакция); • PostgreSQL Pro 14.x (барлық редакция); <p>• пайдаланушы жүзеге кірген есетік жазбаға, ағындағы IPv4 мекенжайына және компьютердің қай ОУ немесе қандай қауіпсіздік тобына байланысты вирусы қарсы шешімін баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқалар;</p> <ul style="list-style-type: none"> • жайта бөлінегі триггерлердің неерархиялары; • клиенттік машиналар тараптағы бұрын орталықтандырылған басқару құралдарымен жүктелген жанартуларды тексілеу; • виртуалды машиналар желісіні таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын талсырмалардың жүктеме балансын бөлу; • басқарылатын мобилді құрылғыларды сервистермен оңтайландыру және оларды басқару; • басқару жүйесіне желілік жүктемені азайту үшін жанартуларды қайта жіберу орталығының ұйымның көз келген компьютерлерді көрсетуі; • Windows Failover Clustering қоллауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталына болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобилді құрылғыға орнату, мобилді құрылғыларды қарау, бұтатуды пәрмендерін жіберу, құралғыны іздеу және пайдаланушының мобилді құрылғысында деректері жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі тиіс; • ОЖ үлгілерімен жұмыс істеу құралдарының болуы: нақты немесе виртуалды машина негізінде мақсатты ОЖ үлгісін жасау, үлгіні басқарушы тандаған компьютерлерге, соның ішінде «жаланаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жинақталған қосу мүмкіндігі қамтамасыз етуі тиіс; • дистрибутивтерден (WIM) операциялық жүйені үлгісін импорттау мүмкіндігі; • лицензияны пайдалануды бұзылғаны немесе лицензияның қолдану мерзімінен асып кеткені туралы басқарушы хабарлау мүмкіндігі бар компьютерде орнатылған бөгет ЕЖ лицензияларын бақылау жүйесінің болуы; • бөгет қосымшаларға арналған орнату шапқартын автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлау басқару функционалының қоллауы; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылар бар желілерді құру мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; <p>3) Linux OX базасында орталықтандырылған басқару, мониторингілеу және жанарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жок:</p> <p>Орталықтандырылған басқару, мониторингілеу және жанарту бағдарламалық құралдары мынадай нұсқаларын операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядты/64-разрядты; • Debian GNU/Linux 10.x (Buster) 32-разрядты/64-разрядты; • Debian GNU/Linux 11.x (Bullseye) 32-разрядты/64-разрядты; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядты; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядты; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядты; • CentOS 7.x 64-разрядты; • Red Hat Enterprise Linux Server 7.x 64-разрядты; • Red Hat Enterprise Linux Server 8.x 64-разрядты; • Red Hat Enterprise Linux Server 9.x 64-разрядты; • SUSE Linux Enterprise Server 12 (барлық жанарту пакеті) 64-разрядты; • SUSE Linux Enterprise Server 15 (барлық жанарту пакеті) 64-разрядты; • Oracle Linux 7 64-разрядты; • Oracle Linux 8 64-разрядты; • Oracle Linux 9 64-разрядты; • жайта бөлінегі триггерлердің неерархиялары; • виртуалды машиналар желісіне таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын талсырмалардың жүктеме балансын бөлу; • жанартуларды тексеру талсырмасының көмегімен жүктеулетін жанартуларды басқарылатын құрылғыларға орнатас бұрын жұмысқа қабылдануы мен қателерді тексеру мүмкіндігі; • басты сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйесі бар серверлерді бағындыру ретінде басқару; <p>И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Агенттерден көптеген оқиғаларды өзі арқылы просигне арналған жөелген бағдарламалық компоненттері, сенсорларға бар. Сенсорлар жүйені негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компоненттері Linux негізінде орналастырылуы болуы; • Өңделетін сервердің компоненттері KVM виртуализациясына агент орнатқан хосттардың шектеулі санын пошта мен желілік трафик оқиғаларының шектеулі санын бақылау үшін орналастыруға болуы; • Бағдарламаның масштабтау параметрлерін баптау мүмкіндігі болуы тиіс. Сіз хосттардың санын және жоспарланатын сақтау және оқиғалар базасының көлемін көрсете аласыз. Бағдарлама серверді қорғайтын параметрлерге сәйкес баптауы; • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс - веб-интерфейс қолданылады. Егер жеке кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларына алынған файлдары талдауға арналған YARA қағидалары жұмыс істейді; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматтарындағы құжаттарға вендор не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді тандау мүмкіндігі; • Құрылғының объектілерді талдау және жіберуді пайдаланушы қағидаларын баптау арқылы анықды мазмұнын бар-жоғына алынған файлдар мен сіттемелерді тексеру мүмкіндігі болуы тиіс; • Құрылғының пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есетік жазбалары және бағдарламалық жасақтама жұмыс істейтін параметрлерді баптау мүмкіндігі болуы тиіс; • Құрылғыға табылған оқиғалар ағынын визуализациялау мүмкіндігі; • Тапандың контексті шығару мүмкіндігі; <p>Трафикті Ресур:</p> <p>Файлдардың сәмделері:</p> <ul style="list-style-type: none"> • «Құрылғы» ортасындағы объект белсенділігінің лога; • «Құрылғы» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоқы бойынша жүйенің негізгі компоненттерін жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару сервері бір Құрылғыш компоненттерінің серверлеріне қосу мүмкіндігі. <p>2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірілуші веб-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтама пайдаланушылар форумы болуы тиіс. Алайда, ЕЖ өндірілуші ресми веб сайты (https://www.sputnik.com/) деп аталатын осы сайтты өлеуметті жеткізуші өзінің төңірегіндегі өзінің бұры шабуылдарды қорғаушы «Спутник 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмақдай.</p> <p>3) техникалық ерекшеліктің 3-бөліміне сәйкес: Әлеуметті жеткізуші Талсырсы беруші лицензия берген күнінен бастап кемінде 24 ай мерзімге вирусы қарсы басқайтын бағдарламалық жасақтама пайдалану және анықды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуметті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС серіктесі 24 айға техникалық қолдаудымен бірге лицензияға жылдық жазбалымен жеткізілетін тұрақты өндірілуші авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынады.</p> <p>4) Әлеуметті жеткізуші ұсынағы Elite Sudio-ның атауы 19.03.2025 жылғы сертификаттың (осы сертификаттың CASP өткендігі үшін Судью Эмирге берілген тұрақты нотариалды куәландырылған аудармасымен) Талсырсы берушінің техникалық ерекшелігін 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтама ұсынылған сертификатталған жамансық сертификатталған жүйесінің иеліккерімен төмен емес деңгейде қамтамасыз ету туралы ақпарат расталмақдай.</p>	
d8e91b24072301dc973cf9a1e476b5d6	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. төңірегінде өзінің төңірегінде талаптарына сәйкес келмеген

3	Төраға	жәбірленген жок	<p>Қағидаларын 93-тармағының 1) тармақшасын басшылыққа ала отырып жәбірленген, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейді, атап айтқанда:</p> <p>1) Әлеуетті жеткізушінің техникалық ерекшелігін 4-бөлімде мынадай тармақтар мен ұсынымдар жок:</p> <p>A) бағдарламалық құралды/вирусы қарсы қорғаныс модуліне мынадай функционалдық мүмкіндіктер жүзеге асырмауы тиіс:</p> <ul style="list-style-type: none"> • жүктелетін Web беттеріндегі бағдарлар мен қалдымды түзетулерді бұзғанды; • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі ақыры; • көз көлген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдардан қорғау; <p>• пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санақтарды қосу, редакциялау, белгілі бір мазмұндығын жою, өндiрушi жасаған және динамикалық түрде жанаратын санақта, сондай-ақ ақпарат түрiне (аудио, видео және т.б.) кол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылауды уақыт аралықтарын өзгертуде мүмкіндік беру, сондай-ақ оны тек Active Directory ішінен белгілі бір пайдаланушыларға тыйым салу;</p> <ul style="list-style-type: none"> • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеуі болған жағдайда желілік трафикасты шектеуі; <p>• пайдаланушылар үшін баспан шығару құралдарына баулау;</p> <ul style="list-style-type: none"> • арнайы жүктеу агенті құрып, Simple Sign On технологиясын қолдай отырып, толық дискіні шифрлау, UEFI жүйелерін қолдау; • жүзеге асыру немесе Операциялық жүйелерін (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI жүйелерін қолдау; • шифрланатын контентті іскемді қорығуға болатын файлдарды шифрлау (орналасқан жері бойынша, көнегі бойынша, файлды жасайтын қосымша бойынша); • қосылған қосымшалар тараптарына шифрлануға қол жеткізуді шектеу тетіктерін болуы, сондай-ақ құпия сөздің қосымшасын ұстау файлының транскрипциялауға мүмкіндік беретін технологиясының болуы; • ұйым желісінен тыс файлдарды шифрлауға және шифрлануға мүмкіндік беретін жұмыс режимін орнатуға болатын алынбайтын медиадағы деректерді шифрлау. <p>B) Windows серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • құрылғының MAC мекенжайын қолдан жасау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіп-қатерлер қорғау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеуі болған жағдайда желілік трафикасты шектеуі; <p>• пайдаланушылар үшін баспан шығару құралдарына баулау;</p> <p>B) MacOS жұмыс станцияларына арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаларға қойылатын талаптар:</p> <ul style="list-style-type: none"> • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санақтарды қосу, редакциялау, өндiрушi жасаған және динамикалық түрде жанаратын белгілі бір ресурстарға немесе ресурстар санақтарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын біршағыр басқару жүйесі арқылы жоғарыда аталған барлық компонентті орнатқандардан басқару; • дискіге толық қол жеткізуді құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік көнегіштерді орнату мүмкіндігі; <p>J) Linux жұмыс станциялары мен серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаларға қойылатын талаптар:</p> <ul style="list-style-type: none"> • Mgrina 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экраны басқару; • SkipPlainTextFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. <p>D) Файлдық серверлерді, қосымша құрылғыларды серверлерін, Windows терминалдык серверлерін вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экраны басқару; • жоғалтылған қауіп-қатерден қорғау (Outlook плагины); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндығы ресурстарға, өндiрушi алдын ала жасаған және динамикалық түрде жанаратын санақта қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу. <p>E) Мобилді құрылғыларды вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • қосымшалармен іске қосуға бақылау шеңберінде жүйелік қосымшаларды бұзғанды; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарламаларды жіберу; • Wi-Fi және Bluetooth модульдерін, сондай-ақ мобилді құрылғы камерасын пайдалануға тыйым салу; • орнатуға мәжбүр қосымшаларды қорғау. <p>Ж) Windows OX негізіндегі орталықтандырылған басқару, мониторингілеу және жанарту бағдарламалық құралдарына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядты/64-разрядты; • MySQL Standard Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MySQL Enterprise Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MariaDB 10.1 (10.1.30 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.3 (10.3.22 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.4 (10.4.26 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.5 (10.5.17 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB Server InnoDB сәткіз кіші жүзесі бар 10.3 32-разрядты/64-разрядты; • MariaDB Galera Cluster InnoDB сәткіз кіші жүзесі бар 10.3 32-разрядты/64-разрядты; • PostgreSQL 13.x 64-разрядты; • PostgreSQL 14.x 64-разрядты; • PostgreSQL Pro 13.x (барлық редакция); • PostgreSQL Pro 14.x (барлық редакция). <p>• пайдаланушы жүзеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты вирусы қарсы шешімін баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқалар;</p> <ul style="list-style-type: none"> • клиенттік машиналар тарапынан бұрын орталықтандырылған басқару құралдарымен жүктелген жанартауларды тексілеу; • виртуалды машиналар желісіне таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобилді құрылғыларды серверлеріне орналастыруға орау; • басқару жүзесіне желілік жүктемені азайту үшін жанартауларды қайта жіберу орталығының ұйымның көз көлген компьютерлерді көрсетуі; <p>• Windows Failover Clustering қолдауы;</p> <p>• Windows Certificate Authority сервисімен интеграцияны қолдау;</p> <ul style="list-style-type: none"> • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобилді құрылғыға орнату, мобилді құрылғыларды қарау, бұзғанды пәрмендерін жіберу, құралғыны іздеу және пайдаланушының мобилді құрылғысында деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі тиіс; • OX үлгілерімен жұмыс істеу құралдарының болуы: нақты немесе виртуалды машина негізінде мақсатты OX үлгісін жасау, үлгіні басқарушы таңдаған компьютерлерге, соның ішінде «жаланыш темпіре» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жинақталған қосу мүмкіндігі қамтамасыз етуі тиіс; • дистрибутивтерден (WIM) операциялық жүйенің үлгісін импорттау мүмкіндігі; • лицензияны пайдалануды бұзылғаны немесе лицензияның қолдану мерзімінен асып кеткені туралы басқарушыға хабарлау мүмкіндігі бар компьютерде орнатылған бөгет EЖ лицензияларын бақылау жүйесінің болуы; • бөгет қосымшаларға арналған орнату шапқартып автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалының қолдауы; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылар бар желілерді құру мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; <p>З) Linux OX базасында орталықтандырылған басқару, мониторингілеу және жанарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жок:</p> <p>Орталықтандырылған басқару, мониторингілеу және жанарту бағдарламалық құралдары мынадай нұсқаларын операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядты/64-разрядты; • Debian GNU/Linux 10.x (Buster) 32-разрядты/64-разрядты; • Debian GNU/Linux 11.x (Bullseye) 32-разрядты/64-разрядты; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядты; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядты; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядты; • CentOS 7.x 64-разрядты; • Red Hat Enterprise Linux Server 7.x 64-разрядты; • Red Hat Enterprise Linux Server 8.x 64-разрядты; • Red Hat Enterprise Linux Server 9.x 64-разрядты; • SUSE Linux Enterprise Server 12 (барлық жанару пакеті) 64-разрядты; • SUSE Linux Enterprise Server 15 (барлық жанару пакеті) 64-разрядты; • Oracle Linux 7 64-разрядты; • Oracle Linux 8 64-разрядты; • Oracle Linux 9 64-разрядты; • Oracle Linux 9 64-разрядты; • жайта бөлінегі триггерлердің неарахиялары; • виртуалды машиналар желісіне таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жанартауларды тексеру тапсырмасының көмегімен жүктелетін жанартауларды басқарылатын құрылғыларға орнатқас бұрын жұмысқа қабілеттілігі мен қателерді тексеру мүмкіндігі; • Active Server ретінде әрекет ету және Linux немесе Windows операциялық жүйесі бар серверлерді бағындыру ретінде басқару. <p>И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Агенттерден көптеген оқиғаларды өзі арқылы проксиге арналған жөкейленген бағдарламалық компоненттері, сенсорлары бар. Сенсорлар жүйені негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдануы керек; • Шешімнің барлық компоненттері Linux негізінде орналастырыла бөлады; • Өңделетін сервердің компоненттері KVM виртуализациясында агент орнатқан хосттардың шектеуі санын және пошта мен желілік трафик оқиғаларының шектеуі санын бақылау үшін орналастыруға болады; • Бағдарламаның масштабтау параметрлерін баптау мүмкіндігі болуы тиіс. Сіз хосттардың санын және жоспарланатын сақтау және оқиғалар базасының көлемін көрсете аласыз. Бағдарлама серверді қорығатын параметрлерге сәйкес аласыз. Бағдарлама серверді қорығатын параметрлерге сәйкес аласыз. Бағдарлама серверді қорығатын параметрлерге сәйкес аласыз. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс - веб-интерфейс қолданылады. Егер жұмыс келетін түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейс сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларына алынған файлдары таңдауға арналған YARA қағидалары жұмыс мүмкіндігі; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға өңір не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді таңдау мүмкіндігі; • Құралдың объектілерді таңдау және жіберуді пайдаланушы қағидаларын баптау арқылы яғни мазмұнын бар-жоғына алынған файлдар мен сіттемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жұқтыру және орнату мүмкіндігі болуы тиіс; • Құралдың пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтаманы жұмыс саясаты параметрлерін баптау мүмкіндігі болуы тиіс; • Құралдың табылған оқиғалар ағашын визуализациялау мүмкіндігі; • Таңдалатын контекстті шығару мүмкіндігі; <p>Трафикасты Ретар:</p> <p>Файлдардың сәмделері:</p> <ul style="list-style-type: none"> • «Құралдың» ортасындағы объект белсенділігінің логы; • «Құралдың» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоколы бойынша жүйенің негізгі компоненттерін жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару сервері бір Құралдың компоненттерінің серверлеріне қосу мүмкіндігі. <p>2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндiрушi веб-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, ЕЖ өндiрушінің ресми веб сайты (https://www.sputnik.com/) деп аталатын осындай осы сайтты Әлеуетті жеткізуші өзінің төңірегінде өткізіп беру шеңберінде қолданған «Спутник 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмақдай.</p> <p>3) техникалық ерекшеліктің 3-бөліміне сәйкес Әлеуетті жеткізуші Тапсырыс берушіге лицензия берген күнінен бастап кемінде 24 ай мерзімге вирусы қарсы басқатытын бағдарламалық жасақтаманы пайдалану және яғни белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС серіктесті 24 айға техникалық қолдауды бірге лицензияға жылдық жазылымды жеткізетін тұрады өндiрушінің авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынады.</p> <p>4) Әлеуетті жеткізуші ұсынып Emsi Suite®-тың атаына 19.03.2025 жылғы сертификаттың (осы сертификаттың CoAS6 өткендігі үшін Судью Эмирге берілген тұрады нотариалды куәландырылған аудармасымен) Тапсырыс берушінің техникалық ерекшелігін 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтаманы ұсынылған сертификатталған жинақның сертификатталған жүйесінің иеліктерден төмен емес, дөңгелегі қамтамасыз ету туралы ақпарат расталмақдай.</p>
---	--------	-----------------	--

		<p>Қағидалардың 93-тармағының 1) тармақшасына басылымдық ала отырып жіберілме, себебі Әлеуметтік желінің техникалық ерекшелігі Талсырсы берушінің техникалық ерекшелігін талаптарына сәйкес келмейді, атап айтқанда:</p> <p>1) Әлеуметтік желінің техникалық ерекшелігін 4-бөлімде мынадай тармақтар мен ұсыныстар жазылған:</p> <p>А) Бағдарламалық құралды/вирусы қарсы қорғаныс модулінде мынадай функционалдық мүмкіндіктер жүзеге асырылуы тиіс:</p> <ul style="list-style-type: none"> • жүктеушінің Web беттеріндегі баннерлер мен қалқымағы тереңдеріне бұтаттау; • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • көз көрмеген тілдегі есептеу жолдарындағы қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдарды қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаптарды қосу, редакциялау, белгілі бір мазмұндық ресурстарға, өндіруші жасаған және динамикалық түрде жаңартылатын санақта, сондай-ақ ақпарат түріне (аудио, видео және т.б.) көп желілікке нақты тыйым салуды немесе рұқсатты қосу, бақылауды ұяқат аралықтарын өлшеуге мүмкіндік беру, сондай-ақ оны тек Active Directory үшін белгілі бір пайдаланушыларға таяғайлау; • резервті сақтау қоймасына объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құрыстарын баптау; • арнайы жүзеге ағачты құрал, Single Sign On технологиясын қолдай отырып, толық дерексіз шифрлау, UEFI жүзілерін қолдау; • жүзеге ағачты немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қолдау; • шифрланатын контентті әкемеді қорғауға болатын файлдары шифрлау (орналасқан жері бойынша, көнеуі бойынша, файлды жасайтын қосымша бойынша); • таспадан қолданбалар тарапаны шифрланған файлдарға көп желілік шектеу қолданушы болуы, сондай-ақ құпия сөздің көмегімен ұяқымды тас файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұяқым желісімен тас файлдарды шифрлау және шифрлануға мүмкіндік беретін жұмыс рөлінің орнатуы болатын алабына медициналық деректерді шифрлау. <p>Б) Windows серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • желілік сегменттерді санақтау болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • қорғанысшы MAC мекенжайына үшін ARP-протоколдағы осалдықтарды пайдаланатын желілік қауіп-қатерлерді қорғау; • резервті сақтау қоймасына объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құрыстарын баптау. <p>В) MacOS жұмыс станцияларына арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаларға қойылатын талаптар:</p> <ul style="list-style-type: none"> • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаптарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартылатын белгілі бір ресурстарға немесе ресурстар санаптарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірінші басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискеге толық көп желілік құрыстарының пайда болуын қауіпсіздігі тұрақ басқару және құралдар берілгеннен кейін жаңа желілік көнеуілерді орнату мүмкіндігі. <p>Г) Linux жұмыс станциялары мен серверлеріне арналған вирусы қарсы қорғайтын бағдарламалық жасақтамаларға қойылатын талаптар:</p> <ul style="list-style-type: none"> • Marea 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйені желілік экраны басқару; • SkipPain/GetFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. <p>Д) Файлдық серверлерді, қаспоярған ауқымдағы серверлерді, Windows терминалдық серверлерін вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • мақалалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйені желілік экраны басқару; • топталық қауіп-қатерлерді қорғау (Собой қолдану); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндық ресурстарға, өндіруші алды ала жасаған және динамикалық түрде жаңартылатын санақта көп желілікке нақты тыйым салуды немесе рұқсатты қосу. <p>Е) Мобилді құрылғыларды вирусы қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар:</p> <ul style="list-style-type: none"> • қосымшаларды іске қосуға бейімделуі жүйелік қосымшаларды бұтаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарламаларды жіберу; • Wi-Fi және bluetooth модульдерін, сондай-ақ мобилді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды қорғау. <p>Ж) Windows OX негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядты/64-разрядты; • MySQL Standard Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MySQL Enterprise Edition 8.0 (8.0.20 және одан да жоғары релиз) 32-разрядты/64-разрядты; • MariaDB 10.1 (10.1.30 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.3 (10.3.22 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.4 (10.4.26 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB 10.5 (10.5.17 және одан да жоғары құрастыру) 32-разрядты/64-разрядты; • MariaDB Server InnoDB сақтау кіші жүйесі бар 10.3 32-разрядты/64-разрядты; • MariaDB Galera Cluster InnoDB сақтау кіші жүйесі бар 10.3 32-разрядты/64-разрядты; • PostgreSQL 13.x 64-разрядты; • PostgreSQL 14.x 64-разрядты; • PostgreSQL 13.x (барлық редакция); • PostgreSQL Pro 14.x (барлық редакция); <p>• пайдаланушы жүзеге кірген есептік жазбаға, ағындағы IPv4 мекенжайына және компьютердің қай ОУ немесе қандай қауіпсіздік тобына байланысты вирусы қарсы шешімін баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқалар;</p> <ul style="list-style-type: none"> • жайта бөлінегі триггерлердің неерархиялары; • клиенттік машиналар тараптан бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тексілеу; • виртуалды машиналар желісіне таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобилді құрылғыларды орталықтандырылған басқаруға қосып алуға мүмкіндік беру; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұяқымды көз көлген компьютерлерді көрсетуі; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталына қолдау; • өзіне-өзі қызмет көрсету порталы басқару агентін мобилді құрылғыға орнату, мобилді құрылғыларды қарау, бұтатуды пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобилді құрылғысында деректерді жою мақсатында пайдаланушыларды қосу мүмкіндігін қамтамасыз етуі тиіс; • ОЖ үлгілерімен жұмыс істеу құралдарының болуы: нақты немесе виртуалды машина негізінде мақсатты ОЖ үлгісін жасау, үлгіні басқарушы тандаған компьютерлерге, соның ішінде «жаланаш темір» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жинақталған қосу мүмкіндігі қамтамасыз етуі тиіс; • дистрибутивтерден (WIM) операциялық жүйені үлгісі импорттау мүмкіндігі; • лицензияны пайдалануды бұзылғаны немесе лицензияның қолдану мерзімінен асып кеткені туралы басқарушы хабарлау мүмкіндігі бар компьютерде орнатылған бөгет ЕЖ лицензияларын бақылау жүйесінің болуы; • бөгет қосымшаларға арналған орнату шапқартын автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлау басқару функционалының қолдауы; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылар бар желілерді құру мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; <p>З) Linux OX базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жерек:</p> <p>Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқаларын операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядты/64-разрядты; • Debian GNU/Linux 10.x (Buster) 32-разрядты/64-разрядты; • Debian GNU/Linux 11.x (Bullseye) 32-разрядты/64-разрядты; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядты; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядты; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядты; • CentOS 7.x 64-разрядты; • Red Hat Enterprise Linux Server 7.x 64-разрядты; • Red Hat Enterprise Linux Server 8.x 64-разрядты; • Red Hat Enterprise Linux Server 9.x 64-разрядты; • SUSE Linux Enterprise Server 12 (барлық жаңарту пакеті) 64-разрядты; • SUSE Linux Enterprise Server 15 (барлық жаңарту пакеті) 64-разрядты; • Oracle Linux 7 64-разрядты; • Oracle Linux 8 64-разрядты; • Oracle Linux 9 64-разрядты; • жайта бөлінегі триггерлердің неерархиялары; • виртуалды машиналар желісіне таңу және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүзеге асырылатын жаңартуларды басқарылатын құрылғыларға орнатас бұрын жұмысқа қабылдануы мен қатерлерді тексеру мүмкіндігі; • басты сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйесі бар серверлерді бағындыру ретінде басқару; <p>И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар:</p> <ul style="list-style-type: none"> • Агенттерден көптеген оқиғаларды өзі арқылы проксиге арналған жөелген бағдарламалық компоненттері, сенсорларға бар. Сенсорлар жүйені негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компоненттері Linux негізінде орналастырылуы болуы; • Өңделетін сервердің компоненттері KVM виртуализациясына агент орнатқан хосттардың шектеулі санын пошта мен желілік трафик оқиғаларының шектеулі санын бақылау үшін орналастыруға болуы; • Бағдарламаның масштабтау параметрлерін баптау мүмкіндігі болуы тиіс. Сіз хосттардың санын және жоспарланатын сақтау және оқиғалар базасының көлемін көрсете аласыз. Бағдарлама серверді қорғайтын параметрлерге сәйкес баптауы. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс - веб-интерфейс қолданылады. Егер жеке кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларына алынған файлдары талдау арналған YARA қағидалары жұмыс істейді; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға вендор не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді тандау мүмкіндігі; • Құрылғының объектілерді талдау және жіберуді пайдаланушы қағидаларын баптау арқылы анықды мазмұнын бар-жоғына алынған файлдар мен сіттемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жүзеге асыру мүмкіндігі болуы тиіс; • Құрылғының пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтаманы жұмыс істейтін параметрлерді баптау мүмкіндігі болуы тиіс; • Құрылғыға табылған оқиғалар ағымын визуализациялау мүмкіндігі; • Тапданатын контексті шығару мүмкіндігі; <p>Трафикті Ресур:</p> <p>Файлдардың сәмделері:</p> <ul style="list-style-type: none"> • «Құрылғы» ортасындағы объект белсенділігінің лога; • «Құрылғы» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоқы бойынша жүйенің негізгі компоненттерін жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару сервері бар Құрылғыш компоненттерінің серверлеріне қосу мүмкіндігі. <p>2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірілуші веб-сайты осы тілде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, ЕЖ өндірілуші ресми веб сайты (https://www.sputnik.sputnik.ru) деп аталатын осы сайтты Әлеуметтік желінің өндірілуші жеткізуші өкілінің бұры шеңберінде қолмен «Спутник 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмайды.</p> <p>3) техникалық ерекшеліктің 3-бөліміне сәйкес: Әлеуметтік желінің Талсырсы беруші лицензия берілген күнінен бастап кемінде 24 ай мерзімге вирусы қарсы басқарылатын бағдарламалық жасақтаманы пайдалану және анықды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуметтік желінің 2025 жылғы 9 сәуірден бастап «ADELINE» ЖИШ серіктесі 24 айға техникалық қолдауды бірге лицензияға жылдық жазылымды жеткізетін түрде өндірілуші авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынады.</p> <p>4) Әлеуметтік желінің ұсыныс Emsi Sudo®-ның атауы 19.03.2025 жылғы сертификаттың (осы сертификаттың CASP өткендігі үшін Sudo® Эмиге берілгені туралы нотариалды куәландырылған аудармасымен) Талсырсы берушінің техникалық ерекшелігін 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтаманы ұсынылған сертификатталған жазылым сертификатталған жүйесінің иеліктерінен төмен емес, дөңгелегі қамтамасыз ету туралы ақпарат расталмайды.</p>
4	Төрағаның орманбасары жіберілген жоқ	93 т. 1 т. теңдерік өтінім төндер талаптарына сәйкес келмеген

Тендер талаптарына сәйкес келмейтін тендерлік өтінімдер: 2

№	Әлеуетті жеткізушінің атауы	БСН (ЖСН) / ССН / ТЕН	Комиссияның қорытынды шешімі
1	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "TRADE IT"	221140033126	жіберілген жоқ
2	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ADELINE"	070140016160	жіберілген жоқ

Тендер шарттарына сәйкес келетін тендерлік өтінімдер: 2

№	Әлеуетті жеткізушінің атауы	БСН (ЖСН) / ССН / ТЕН
1	"ITware" (АйТиваре) жауапкершілігі шектеулі серіктестігі	121040015817
2	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "THERION"	170540022814

Тендерлік өтінімдерді тендер талаптарына сәйкес келтіру мақсатында әлеуетті жеткізушілер ұсынатын қосымша құжаттарды берудің соңғы күні мен уақыты: осы Хаттама жарияланған сәттен бастап 3 жұмыс күнінен кешіктірмей.

Комиссияның құрамы	Қатысу белгісі/болмау себебі
Тендерлік комиссияның Төрағасы	Иә
Тендерлік комиссияның Төрағаның орынбасары	Иә
Комиссияның мүшелері	Иә
	Иә
	Иә
Тендерлік комиссияның хатшысы	Иә

Ескертпе:

* Тапсырыс берушілер туралы мәлімет, егер тапсырыс берушілер бірнешеу болса көрсетілмейді.

Аббревиатураларды таратып жазу:

БСН - бизнес-сәйкестендіру нөмірі;

ЖСН - жеке сәйкестендіру нөмірі;

ССН - салық төлеушінің сәйкестендіру нөмірі;

ТЕН - төлеушінің есеп нөмірі;

Т.А.Ә. - тегі, аты, әкесінің аты;

кк.аа.жжжж. – күні, айы, жылы.



Осы құжат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының 2003 жылғы 7 қаңтардағы N 370-ІІ Заңы 7 бабының 1 тармағына сәйкес қағаз тасығыштағы құжатпен бірдей.

Протокол предварительного допуска к участию в тендере по закупкам товаров, работ, услуг № 80742-Т

23.04.2025 17:05:05

Заказчик* АКЦИОНЕРНОЕ ОБЩЕСТВО "ЕДИНЫЙ
НАКОПИТЕЛЬНЫЙ ПЕНСИОННЫЙ
ФОНД"

№ тендера 80742

Наименование тендера Услуги по предоставлению лицензий на
право использования программного
обеспечения

Наименование организатора АКЦИОНЕРНОЕ ОБЩЕСТВО "ЕДИНЫЙ
НАКОПИТЕЛЬНЫЙ ПЕНСИОННЫЙ
ФОНД"

Адрес организатора Казахстан, г. Алматы, Медеуский
район, Медеуский район, микрорайон
Самал-2, дом №97, нежилое помещение
№13,

**Дата окончания приема дополненных
заявок** 2025-04-29 10:00:00

Состав тендерной комиссии:

№	Ф.И.О.	Должность в организации	Роль в комиссии
1	Член комиссии 1	Должность члена комиссии 1	Председатель
2	Член комиссии 2	Должность члена комиссии 2	Заместитель председателя
3	Член комиссии 3	Должность члена комиссии 3	Член комиссии
4	Член комиссии 4	Должность члена комиссии 4	Член комиссии
6	Член комиссии 6	Должность члена комиссии 6	Член комиссии
7	Член комиссии 7	Должность члена комиссии 7	Секретарь

Перечень закупаемых товаров, работ, услуг с указанием общей суммы 84977196.42 тенге

№	№ Лота	Наименование лота	Характеристика закупаемых товаров, работ и услуг	Количество	Цена за единицу, тенге	Сумма, выделенная для закупки, тенге
1	238372-T2	Услуги по предоставлению лицензий на право использования программного обеспечения	Услуги по подписке на право использования программного обеспечения антивирусного контроля, обнаружения и изучения вредоносной активности	1.000	84977196.42	84977196.42

№ лота: 238372-T2

Наименование лота: Услуги по предоставлению лицензий на право использования программного обеспечения

Характеристика закупаемых товаров, работ и услуг : Услуги по подписке на право использования программного обеспечения антивирусного контроля, обнаружения и изучения вредоносной активности

Результаты голосования членов тендерной комиссии:

"ТҮҮҮ" (АЙТҮҮ) ЖАУКАРҮПІНІ ШЕКТҮЛІ СЕРКІСТІНІ, 121040015817				
№	Роль в комиссии	Решение члена комиссии	Причина отклонения	Обоснование причины отклонения. Перечень документов в заявке потенциального поставщика которые необходимо привести в соответствие с условиями тендера
1	Член комиссии	допущен		
2	Председатель	допущен		
3	Член комиссии	допущен		
4	Член комиссии	допущен		
5	Заместитель председателя	допущен		
ТОВАРИШЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "TRADE IT", 221140033126				
1	Член комиссии	отклонен	пп. 1 п. 93 несоответствие тендерной заявки условиям тендера	не допущено, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно: в нарушение требования подпункта 3) раздела 13 технической спецификации Потенциальным поставщиком в рамках подачи тендерной заявки представлены сертификаты № 002.11.6-5685 от 13.03.2023 года и № 025.5-13591 от 28.04.2023 года с истекшими сроками действия (согласно официального сайта производителя ПО сертификат № 002.11.6-5685 действителен до: 31.12.2023 года, сертификат № 025.5-13591 действителен до: 01.10.2024 года).
2	Председатель	отклонен	пп. 1 п. 93 несоответствие тендерной заявки условиям тендера	не допущено, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно: в нарушение требования подпункта 3) раздела 13 технической спецификации Потенциальным поставщиком в рамках подачи тендерной заявки представлены сертификаты № 002.11.6-5685 от 13.03.2023 года и № 025.5-13591 от 28.04.2023 года с истекшими сроками действия (согласно официального сайта производителя ПО сертификат № 002.11.6-5685 действителен до: 31.12.2023 года, сертификат № 025.5-13591 действителен до: 01.10.2024 года).
3	Член комиссии	отклонен	пп. 1 п. 93 несоответствие тендерной заявки условиям тендера	не допущено, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно: в нарушение требования подпункта 3) раздела 13 технической спецификации Потенциальным поставщиком в рамках подачи тендерной заявки представлены сертификаты № 002.11.6-5685 от 13.03.2023 года и № 025.5-13591 от 28.04.2023 года с истекшими сроками действия (согласно официального сайта производителя ПО сертификат № 002.11.6-5685 действителен до: 31.12.2023 года, сертификат № 025.5-13591 действителен до: 01.10.2024 года).
4	Член комиссии	отклонен	пп. 1 п. 93 несоответствие тендерной заявки условиям тендера	не допущено, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно: в нарушение требования подпункта 3) раздела 13 технической спецификации Потенциальным поставщиком в рамках подачи тендерной заявки представлены сертификаты № 002.11.6-5685 от 13.03.2023 года и № 025.5-13591 от 28.04.2023 года с истекшими сроками действия (согласно официального сайта производителя ПО сертификат № 002.11.6-5685 действителен до: 31.12.2023 года, сертификат № 025.5-13591 действителен до: 01.10.2024 года).
5	Заместитель председателя	отклонен	пп. 1 п. 93 несоответствие тендерной заявки условиям тендера	руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно: в нарушение требования подпункта 3) раздела 13 технической спецификации Потенциальным поставщиком в рамках подачи тендерной заявки представлены сертификаты № 002.11.6-5685 от 13.03.2023 года и № 025.5-13591 от 28.04.2023 года с истекшими сроками действия (согласно официального сайта производителя ПО сертификат № 002.11.6-5685 действителен до: 31.12.2023 года, сертификат № 025.5-13591 действителен до: 01.10.2024 года).
ТОВАРИШЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "THERION", 170540022814				
1	Член комиссии	допущен		
2	Председатель	допущен		
3	Член комиссии	допущен		
4	Член комиссии	допущен		
5	Заместитель председателя	допущен		
ТОВАРИШЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ABELINE", 070140016160				
1	Член комиссии	допущен		

1	Член комиссии	отклонен	<p>по. пп. 1 п. 93 несоответствие тендерной заявки условиям тендера</p> <p>не допущено, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно:</p> <p>1) в разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения:</p> <p>А) в программном средстве/модуле антивирусной защиты должны быть реализованы следующие функциональные возможности:</p> <ul style="list-style-type: none"> • блокировка баннеров и всплывающих окон на загружаемых Web-страницах; • встроенного сетевого экрана, позволяющего создавать сетевые пакеты правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категория созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • подполосовочное шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановление зашифрованного содержимого в случае сбоя загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по созданию файла приложения); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расширивать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации. <p>Б) Требования к программным средствам антивирусной защиты для серверов Windows:</p> <ul style="list-style-type: none"> • встроенности сетевого экрана, позволяющего создавать сетевые пакеты правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройств; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. <p>В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS:</p> <ul style="list-style-type: none"> • контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категориям ресурсов, созданных и динамически обновляемых производителем; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; • возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены. <p>Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux:</p> <ul style="list-style-type: none"> • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра \$ZshPrintTextFile; <p>Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows:</p> <ul style="list-style-type: none"> • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагины для Outlook); • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. <p>Е) Требования к программным средствам антивирусной защиты мобильных устройств:</p> <ul style="list-style-type: none"> • блокировка системных приложений, в рамках контроля запуска приложений; • отправка команд и реагирование через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и Bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. <p>Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядная/64-разрядная; • MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная; • MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная; • MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная; • MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная; • MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • PostgreSQL 13.x 64-разрядная; • PostgreSQL 14.x 64-разрядная; • Postgres Pro 13.x (все редакции); • Postgres Pro 14.x (все редакции); • указания в политиках безопасности специальных триггеров, которые перераспределят настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • ведение триггеров, по которым происходит перераспределение; • генерация загрузочных образов операционной системы ПО централизованного управления перед распространением на клиентские машины; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • централизованная установка сертификатов на управляемые мобильные устройства; • указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие портала самообслуживания пользователей; • портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотра мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие инструментов работы с образами ОС: создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранное администратором компьютеры, в том числе на "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутива (WIM); • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышения срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv4 и IPv6-адресами и отправлять сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; <p>З) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux - Отсутствует название пункта и следующее его содержание:</p> <p>Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная; • Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная; • Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; • CentOS 7.x 64-разрядная; • Red Hat Enterprise Linux Server 7.x 64-разрядная; • Red Hat Enterprise Linux Server 8.x 64-разрядная; • Red Hat Enterprise Linux Server 9.x 64-разрядная; • SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная; • SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; • Oracle Linux 8 64-разрядная; • Oracle Linux 9 64-разрядная; • иерархия триггеров, по которым происходит перераспределение; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • возможность с помощью заданных проверок обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства; • выступать в качестве Главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных. <p>И) Требования к модулю обнаружения атак. Требования к программным средствам обнаружения атак на рабочих станциях:</p> <ul style="list-style-type: none"> • Иметь отдельные прозрачные компоненты, сенсоры, для проксирования через себя поступающих с агентов событий. Сенсоры должны поддерживать режим, как отдельный, так и совмещенной установки с основной частью системы; • Все компоненты решения могут быть развернуты на базе операционной системы Linux; • Компоненты обрабатывающего сервера могут быть развернуты на KVM-виртуализации для контроля ограниченного количества хостов с установленным агентом и ограниченного количества событий почтового и сетевого трафика; • Должна быть возможность настроить параметры масштабирования программы. Вы можете указать количество хостов в планировщик размер Хранилища и базы событий. Программа настроит сервера в соответствии с указанными параметрами. • Для настройки параметров масштабирования используется отдельный веб-интерфейс - веб-интерфейс для управления масштабированием. Если серверы возвращают в виде кластера, в веб-интерфейсе для управления масштабированием вы также можете просмотреть список серверов и выключить кластер; • Возможность загрузки собственных YARA-правил для анализа файлов, полученных с рабочих станций; • Возможность осуществлять подбор парочек к зашифрованным документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставленной верою либо по установленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки поведения файлов и ссылок на наличие вредоносного содержания, посредством настройки пользовательских правил отправки объектов на анализ; • В пользовательских образах песочницы должна быть возможность настройки таких параметров, как имя компьютера, локализация, учетные записи пользователей и состав программного обеспечения; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность загрузки анализируемого контекста; <p>Рear трафика;</p> <p>Смешта файлы;</p> <p>Лог активности объекта в среде «Песочница»;</p> <p>Скриншоты активности объекта в среде «Песочница»;</p> <ul style="list-style-type: none"> • Возможность мониторинга состояния работы основных компонентов системы по протоколу SNMP • Возможность подключения нескольких серверов централизованного управления к одним и тем же серверам компонентов Песочница. <p>2) Согласно требованиям подпункта 2) раздела 6 технической спецификации веб-сайт производителя должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный веб-сайт производителя ПО (https://www.cynet.net/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Супер 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки.</p> <p>3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и лицензия вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя изданные от 09 апреля 2025 г. о том, что партнер TOO 'ADELINE' будет поставлять годовую лицензию совместно с технической поддержкой на период на 24 месяца.</p> <p>4) Согласно требованиям подпункта 3) раздела 13 технической спецификации Заказчика вместе с тендерной заявкой Потенциальный поставщик должен предоставить: электронные копии действующих сертификатов на не менее чем 1 (одного) сертифицированного специалиста по предлагаемому программному обеспечению уровня не ниже сертифицированный системный инженер. Однако, предоставленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.</p>
---	---------------	----------	--

2	Член комиссии	отклонен	<p>пп. 1 п. 93 несоответствие тендерной заявки условиям тендера</p> <p>не допущено, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно:</p> <p>1) в разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения:</p> <p>А) в программном средстве/модуле антивирусной защиты должны быть реализованы следующие функциональные возможности:</p> <ul style="list-style-type: none"> • блокировка баннеров и всплывающих окон на загружаемых Web-страницах; • встроенного сетевого экрана, позволяющего создавать сетевые пакеты правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категория созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • подполосовое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановление зашифрованного содержимого в случае сбоя загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по созданию файла приложения); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расширивать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации. <p>Б) Требования к программным средствам антивирусной защиты для серверов Windows:</p> <ul style="list-style-type: none"> • встроенного сетевого экрана, позволяющего создавать сетевые пакеты правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройств; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. <p>В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS:</p> <ul style="list-style-type: none"> • контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категориям ресурсов, созданных и динамически обновляемых производителем; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; • возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены. <p>Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux:</p> <ul style="list-style-type: none"> • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра \$ZshPrintTextFile; <p>Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows:</p> <ul style="list-style-type: none"> • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагины для Outlook); • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. <p>Е) Требования к программным средствам антивирусной защиты мобильных устройств:</p> <ul style="list-style-type: none"> • блокировка системных приложений, в рамках контроля запуска приложений; • отправка команд и реагирование через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и Bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. <p>Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядная/64-разрядная; • MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная; • MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная; • MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная; • MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная; • MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • PostgreSQL 13.x 64-разрядная; • PostgreSQL 14.x 64-разрядная; • PostgreSQL Pro 13.x (все редакции); • PostgreSQL Pro 14.x (все редакции); • указания в политиках безопасности специальных триггеров, которые перераспределят настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • ведение триггеров, по которым происходит перераспределение; • генерация загрузочных образов операционной системы ПО централизованного управления перед распространением на клиентские машины; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • централизованная установка сертификатов на управляемые мобильные устройства; • указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие портала самообслуживания пользователей; • портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотра мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие инструментов работы с образами жесткого диска: создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранное администратором компьютеры, в том числе на "топое железо" (bare metal); • возможность импортировать образ операционной системы из дистрибутива (WIM); • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышения срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv4 и IPv6-адресами и отправлять сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; <p>З) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux - Отсутствует название пункта и следующее его содержание:</p> <p>Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная; • Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная; • Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; • CentOS 7.x 64-разрядная; • Red Hat Enterprise Linux Server 7.x 64-разрядная; • Red Hat Enterprise Linux Server 8.x 64-разрядная; • Red Hat Enterprise Linux Server 9.x 64-разрядная; • SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная; • SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; • Oracle Linux 8 64-разрядная; • Oracle Linux 9 64-разрядная; • иерархия триггеров, по которым происходит перераспределение; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • возможность с помощью заданных проверок обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства; • выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных. <p>И) Требования к модулю обнаружения атак. Требования к программным средствам обнаружения атак на рабочих станциях:</p> <ul style="list-style-type: none"> • Иметь отдельные прозрачные компоненты, сенсоры, для проксирования через себя поступающих с агентов событий. Сенсоры должны поддерживать режим, как отдельный, так и совмещенной установки с основной частью системы; • Все компоненты решения могут быть развернуты на базе операционной системы Linux; • Компоненты обрабатывающего сервера могут быть развернуты на KVM-виртуализации для контроля ограниченного количества хостов с установленным агентом и ограниченного количества событий почтового и сетевого трафика; • Должна быть возможность настроить параметры масштабирования программы. Вы можете указать количество хостов в планировщик размер Хранилища и базы событий. Программа настроит сервера в соответствии с указанными параметрами. • Для настройки параметров масштабирования используется отдельный веб-интерфейс - веб-интерфейс для управления масштабированием. Если серверы возвращают в виде кластера, в веб-интерфейсе для управления масштабированием вы также можете просмотреть список серверов и выключить кластер; • Возможность загрузки собственных YARA-правил для анализа файлов, полученных с рабочих станций; • Возможность осуществлять подбор парочек к зашифрованным документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставленной производителем либо по установленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образцов операционных систем Windows с целью проверки поведения файлов и ссылок на наличие вредоносного содержания, посредством настройки пользовательских правил отправки объектов на анализ; • В пользовательских образцах песочницы должна быть возможность настройки таких параметров, как имя компьютера, локализация, учетные записи пользователей и состав программного обеспечения; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность загрузки анализируемого контекста; <p>Рear трафика;</p> <ul style="list-style-type: none"> • Сметлы файлы; • Лог активности объекта в среде «Песочница»; • Скриншоты активности объекта в среде «Песочница»; • Возможность мониторинга состояния работы основных компонентов системы по протоколу SNMP • Возможность подключения нескольких серверов централизованного управления к одним и тем же серверам компонентов Песочница. <p>2) Согласно требованиям подпункта 2) раздела 6 технической спецификации веб-сайт производителя должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный веб-сайт производителя ПО (https://www.cynet.net/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Супер 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки.</p> <p>3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставлять лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и лицензия вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя изданные от 09 апреля 2025 г. о том, что партнер TOO 'ADELINE' будет поставлять годовую лицензию совместно с технической поддержкой на период на 24 месяца.</p> <p>4) Согласно требованиям подпункта 3) раздела 13 технической спецификации Заказчика вместе с тендерной заявкой Потенциальный поставщик должен предоставлять: электронные копии действующих сертификатов на не менее чем 1 (одного) сертифицированного специалиста по предлагаемому программному обеспечению уровня не ниже сертифицированный системный инженер. Однако, предоставленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emri Saidov не позволяет определить уровень его квалификации.</p>
---	---------------	----------	---

3	Председатель отклонен	п.п. 1, п. 53 несоответствие тендерной заявки условиям тендера	<p>не допущено, руководствуясь подпунктом 1) пункта 53 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно:</p> <p>1) в разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения:</p> <p>А) в программном средстве/модуле антивирусной защиты должны быть реализованы следующие функциональные возможности:</p> <ul style="list-style-type: none"> • блокировка баннеров и всплывающих окон на загружаемых Web-страницах; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категория созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • подполосковое шифрование с созданием специального загрузочного агента и поддержки технологии Single Sign On, поддержка UEFI-систем; • восстановление зашифрованного содержимого в случае сбоя загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого учета (по местоположению, по расширению, по создаваемому файлу приложения); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расширивать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации. <p>Б) Требования к программным средствам антивирусной защиты для серверов Windows:</p> <ul style="list-style-type: none"> • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защита от сетевых угроз, которая используетую узнаваемости и AM-протоколе для поддержки MAC-адреса устройств; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; <p>В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS:</p> <ul style="list-style-type: none"> • контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем; • централизованное управление всеми видеоподсистемами компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; • возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены. <p>Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux:</p> <ul style="list-style-type: none"> • MariaDB 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программы с возможностью параметра SkipPainTextFiles; <p>Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows:</p> <ul style="list-style-type: none"> • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (спам для Outlook); • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. <p>Е) Требования к программным средствам антивирусной защиты мобильных устройств:</p> <ul style="list-style-type: none"> • блокировка системных приложений, в рамках контроля запуска приложений; • отправка команд в реальном времени через сервис: Google Cloud Messaging (FCM); • заблокировать wi-fi и Bluetooth модули, а также использование камеры мобильного устройства; • указать обязательно к установке приложения. <p>Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядная/64-разрядная; • MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная; • MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная; • MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная; • MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная; • MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • PostgreSQL 13.x 64-разрядная; • PostgreSQL 14.x 64-разрядная; • Postgres Pro 13.x (все редакции); • Postgres Pro 14.x (все редакции); • указание в политике безопасности специальных триггеров, которые перераспределят настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • иерархии триггеров, по которым происходит перераспределение; • тестирование загрузочных образов средствами ПО централизованного управления перед распространением на клиентские машины; • расслоивание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • централизованная установка сертификатов на управляемые мобильные устройства; • указание любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие модуля самодиагностирования пользователей; • подпитка самообслуживания должна обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие инструментов работы с образами ОС. Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "топое железо" (bare metal); • должна быть обеспечена возможность добавления наборов ранее созданных образов; • возможность импортировать образ операционной системы из дистрибутива (WIM); • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и оприщать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установочных приложениях и операционной системе на компьютерах пользователей; <p>3) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux - Отсутствует название пункта и следующие его содержание:</p> <p>Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная; • Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная; • Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; • CentOS 7.x 64-разрядная; • Red Hat Enterprise Linux Server 7.x 64-разрядная; • Red Hat Enterprise Linux Server 8.x 64-разрядная; • Red Hat Enterprise Linux Server 9.x 64-разрядная; • SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная; • SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; • Oracle Linux 7 64-разрядная; • Oracle Linux 8 64-разрядная; • Oracle Linux 9 64-разрядная; • иерархии триггеров, по которым происходит перераспределение; • расслоивание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • возможность с помощью заданной проверки обновлений проверять загрузаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства; • выступать в качестве главного Сервера и управляемых системных Linux или Windows в качестве подчиненных. <p>И) Требования к модулю обнаружения атак. Требования к программным средствам обнаружения атак на рабочих станциях:</p> <ul style="list-style-type: none"> • Иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступающих с агентов событий. Сенсоры должны поддерживать режим, как отдельной, так и совмещенной установки с основной частью системы; • Все компоненты решения могут быть развернуты на базе операционной системы Linux; • Компоненты обрабатываемого сервера могут быть развернуты на KVM-виртуализации для контроля ограниченного количества хостов с установленными агентами и ограничением количества событий почтового и сетевого трафика; • Должна быть возможность настроить параметры масштабирования программы. Вы можете указать количество хостов и планируемый размер Хранилища и базы событий. Программы настроены сервера в соответствии с указанными параметрами. • Для настройки параметров масштабирования используется отдельный веб-интерфейс - веб-интерфейс для управления масштабированием. Если система развернута в виде кластера, а веб-интерфейс для управления масштабированием за также можете просмотреть список серверов и выключить кластер; • Возможность загрузки собственных YARA-правил для анализа файлов, полученных с рабочих станций; • Возможность осуществлять подбор парочек к зашифрованным картинкам, документов формата PDF, Word, Excel и PowerPoint по базе паролей, поставленной вездом либо по установленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки полученных файлов в ссылке на наличие вредоносного содержимого, посредством настройки пользовательских правил отправки объектов на анализ; • В пользовательских образах песочницы должна быть возможность настройки таких параметров, как имя компьютера, локализация, учетные записи пользователей и состав программного обеспечения; • Возможность визуализации обилия данных в песочнице; • Возможность загрузки анализируемого контекста; <p>Рear трафика;</p> <ul style="list-style-type: none"> • Сметлы файлы; • Лог активности объекта в среде «Песочница»; • Скриншоты активности объекта в среде «Песочница»; • Возможность мониторинга состояния работы основных компонентов системы по протоколу SNMP • Возможность подключения нескольких серверов централизованного управления к одним и тем же серверам компонента Песочница. <p>2) Согласно требованиям подпункта 2) раздела 6 технической спецификации веб-сайт производителя должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный веб-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Спут 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки.</p> <p>3) Согласно разделу 3 технической спецификации Потенциальных Поставщиков должно предоставлять лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяца с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизованного письма от производителя изданные от 09 апреля 2023 г. о том, что партнер TOO 'ADELINE' будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца.</p> <p>4) Согласно требованиям подпункта 3) раздела 13 технической спецификации Заказчика вместе с тендерной заявкой Потенциальному поставщику необходимо предоставить электронные копии действующих сертификатов на не менее чем 1 (одного) сертифицированного специалиста по предлагаемому программному обеспечению уровня не ниже сертифицированный системный инженер. Однако, предоставленный Потенциальным поставщиком сертификат от 19.03.2023 г. на имя Emil Saidov не позволяет определить уровень его квалификации.</p>
---	-----------------------	--	--

4	Заместитель председателя отклонен	п.п. 1, п. 93 несоответствие тендерной заявки условиям тендера	<p>руководствуется подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно:</p> <p>1) В разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и приложения:</p> <p>А) в программном средстве/модуле антивирусной защиты должны быть реализованы следующие функциональные возможности:</p> <ul style="list-style-type: none"> • блокировка баннеров и всплывающих окон на загружаемых Web-страницах; • встроенного сетевого экрана, позволяющего создавать сетевые пакеты правила в сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категория созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • подописковочное шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановление зашифрованного содержимого в случае сбоя загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по созданию файла приложения); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расширивать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации. <p>Б) Требования к программным средствам антивирусной защиты для серверов Windows:</p> <ul style="list-style-type: none"> • встроенного сетевого экрана, позволяющего создавать сетевые пакеты правила в сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройств; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. <p>В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS:</p> <ul style="list-style-type: none"> • контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категориям ресурсов, созданных и динамически обновляемых производителем; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; • возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены. <p>Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux:</p> <ul style="list-style-type: none"> • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра \$ZshPrintTextFile; <p>Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows:</p> <ul style="list-style-type: none"> • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагины для Outlook); • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. <p>Е) Требования к программным средствам антивирусной защиты мобильных устройств:</p> <ul style="list-style-type: none"> • блокировка системных приложений, в рамках контроля запуска приложений; • отправка команд и реагирование через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и Bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. <p>Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядная/64-разрядная; • MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная; • MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная; • MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная; • MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная; • MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • PostgreSQL 13.x 64-разрядная; • PostgreSQL 14.x 64-разрядная; • Postgres Pro 13.x (все редакции); • Postgres Pro 14.x (все редакции); • указания в политиках безопасности специальных триггеров, которые перераспределят настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • ведение журналов, по которым происходит перераспределение; • генерация загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • централизованная установка сертификатов на управляемые мобильные устройства; • указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие портала самообслуживания пользователей; • портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотра мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие инструментов работы с образами ОС: создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутива (WIM); • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышения срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv4 и IPv6-адресами и отправлять сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; <p>З) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux* - Отсутствует название пункта и следующее его содержание:</p> <p>Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная; • Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная; • Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; • CentOS 7.x 64-разрядная; • Red Hat Enterprise Linux Server 7.x 64-разрядная; • Red Hat Enterprise Linux Server 8.x 64-разрядная; • Red Hat Enterprise Linux Server 9.x 64-разрядная; • SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная; • SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; • Oracle Linux 8 64-разрядная; • Oracle Linux 9 64-разрядная; • иерархия триггеров, по которым происходит перераспределение; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • возможность с помощью задания проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства; • выступать в качестве Главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных. <p>И) Требования к модулю обнаружения атак. Требования к программным средствам обнаружения атак на рабочих станциях:</p> <ul style="list-style-type: none"> • Иметь отдельные прозрачные компоненты, сенсоры, для проскривания через себя поступающих с агентов событий. Сенсоры должны поддерживать режим, как отдельный, так и совмещенной установки с основной частью системы; • Все компоненты решения могут быть развернуты на базе операционной системы Linux; • Компоненты обрабатывающего сервера могут быть развернуты на KVM-виртуализации для контроля ограниченного количества хостов с установленным агентом и ограниченного количества событий почтового и сетевого трафика; • Должна быть возможность настроить параметры масштабирования программ. Вы можете указать количество хостов в планировщик размер Хранилища и базы событий. Программа настроит сервера в соответствии с указанными параметрами. • Для настройки параметров масштабирования используется отдельный веб-интерфейс - веб-интерфейс для управления масштабированием. Если серверы возвращают в виде кластера, в веб-интерфейсе для управления масштабированием вы также можете просмотреть список серверов и выключить кластер; • Возможность загрузки собственных YARA-правил для анализа файлов, полученных с рабочих станций; • Возможность осуществлять подбор парочек зашифрованных документов формата PDF, Word, Excel и PowerPoint по базе парочек, поставленной производителем или по установленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образцов операционных систем Windows с целью проверки поведения файлов и ссылок на наличие вредоносного содержания, посредством настройки пользовательских правил отправки объектов на анализ; • В пользовательских образцах песочницы должна быть возможность настройки таких параметров, как имя компьютера, локализация, учетные записи пользователей и состав программного обеспечения; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность загрузки анализируемого контекста; <p>Рear трафика;</p> <ul style="list-style-type: none"> • Сметлы файлы; • Лог активности объекта в среде «Песочница»; • Скриншоты активности объекта в среде «Песочница»; • Возможность мониторинга состояния работы основных компонентов системы по протоколу SNMP • Возможность подключения нескольких серверов централизованного управления к одним и тем же серверам компонентов Песочница. <p>2) Согласно требованиям подпункта 2) раздела 6 технической спецификации веб-сайт производителя должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный веб-сайт производителя ПО (https://www.cynet.net/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Супер 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки.</p> <p>3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и лицензия вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя изданные от 09 апреля 2025 г. о том, что партнер TOO 'ADELINE' будет поставлять годовую лицензию совместно с технической поддержкой на период на 24 месяца.</p> <p>4) Согласно требованиям подпункта 3) раздела 13 технической спецификации Заказчика вместе с тендерной заявкой Потенциальный поставщик должен предоставить: электронные копии действующих сертификатов на не менее чем 1 (одного) сертифицированного специалиста по предлагаемому программному обеспечению уровня не ниже сертифицированный системный инженер. Однако, предоставленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.</p>
---	-----------------------------------	--	--

5	Член комиссии	отклонен	<p>не допущен, руководствуясь подпунктом 1) пункта 93 Правил, в связи с тем, что техническая спецификация Потенциального поставщика не соответствует требованиям технической спецификации Заказчика, а именно:</p> <p>1) в разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения:</p> <p>А) в программном средстве/модуле антивирусной защиты должны быть реализованы следующие функциональные возможности:</p> <ul style="list-style-type: none"> • блокировка баннеров и всплывающих окон на загружаемых Web-страницах; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категория созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволить вводить временные интервалы контроля, а также назначать его только определенным пользователям и/или устройствам; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • подполосовиков шифрование с созданием специального загрузочного агента и поддержки технологии Single Sign On, поддержка UEFI-систем; • восстановление зашифрованного содержимого в случае сбоя загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого учета (по местоположению, по расширению, по создаваемому файлу приложения); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расширивать файлы за пределами организации с помощью пароля; • шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации. <p>Б) Требования к программным средствам антивирусной защиты для серверов Windows:</p> <ul style="list-style-type: none"> • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых угроз, которая используетую узнаваемости и AM-протоколе для поддержки MAC-адреса устройств; • защитить паролям восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; <p>В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS:</p> <ul style="list-style-type: none"> • контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем; • централизованное управление всеми видеонаблюдениями компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; • возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены. <p>Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux:</p> <ul style="list-style-type: none"> • MariaDB 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программы с помощью параметра SkipPainTextFiles. <p>Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows:</p> <ul style="list-style-type: none"> • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (спам для Outlook); • осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем. <p>Е) Требования к программным средствам антивирусной защиты мобильных устройств:</p> <ul style="list-style-type: none"> • блокировка системных приложений, в рамках контроля запуска приложений; • отправка команд в режим уведомлений через сервис: Firebase Cloud Messaging (FCM); • заблокировать wi-fi и Bluetooth модули, а также использование камеры мобильного устройства; • указать обязательно к установке приложения. <p>Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows:</p> <ul style="list-style-type: none"> • Microsoft Azure SQL Database; • MySQL 5.7 Community 32-разрядная/64-разрядная; • MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; • MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная; • MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная; • MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная; • MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная; • MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; • PostgreSQL 13.x 64-разрядная; • PostgreSQL 14.x 64-разрядная; • Postgres Pro 13.x (все редакции); • Postgres Pro 14.x (все редакции); • указание в политике безопасности специальных триггеров, которые перепределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • иерархии триггеров, по которым происходит перераспределение; • тестирование загрузочных образов средствами ПО централизованного управления перед распространением на клиентские машины; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • централизованная установка сертификатов на управляемые мобильные устройства; • указание любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие модуля самобслуживания пользователей; • подпитка самообслуживания должна обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие инструментов работы с образами ОС. Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "топое железо" (bare metal); • должна быть обеспечена возможность добавления наборов ранее созданных образов; • возможность импортировать образ операционной системы из дистрибутива (WIM); • наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии; • автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и оприщать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установочных приложениях и операционной системе на компьютерах пользователей; <p>3) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux - Отсутствует название пункта и следующее его содержание:</p> <p>Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий</p> <ul style="list-style-type: none"> • Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная; • Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная; • Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная; • Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; • Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; • CentOS 7.x 64-разрядная; • Red Hat Enterprise Linux Server 7.x 64-разрядная; • Red Hat Enterprise Linux Server 8.x 64-разрядная; • Red Hat Enterprise Linux Server 9.x 64-разрядная; • SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная; • SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; • Oracle Linux 7 64-разрядная; • Oracle Linux 8 64-разрядная; • Oracle Linux 9 64-разрядная; • иерархии триггеров, по которым происходит перераспределение; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • возможность с помощью заданной проверки обновлений проверять загрузяемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства; • выступать в качестве главного сервера и управлять Сервером с операционными системами Linux или Windows в качестве подчиненных. <p>И) Требования к модулю обнаружения атак. Требования к программным средствам обнаружения атак на рабочих станциях:</p> <ul style="list-style-type: none"> • иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступающих с агентов событий. Сенсоры должны поддерживать режим, как отдельной, так и совмещенной установки с основной частью системы; • Все компоненты решения могут быть развернуты на базе операционной системы Linux; • Компоненты обрабатываемого сервера могут быть развернуты на KVM-виртуализации для контроля ограниченного количества хостов с установленными агентами и ограничением количества событий почтового и сетевого трафика; • Должна быть возможность настроить параметры масштабирования программы. Вы можете указать количество хостов и планируемый размер Хранилища и базы данных. Программы настроит сервера в соответствии с указанными параметрами. • Для настройки параметров масштабирования используется отдельный веб-интерфейс - веб-интерфейс для управления масштабированием. Если система развернута в виде кластера, а веб-интерфейс для управления масштабированием за также можете просмотреть список серверов и выключить кластер. • Возможность загрузки собственных YARA-правил для анализа файлов, полученных с рабочих станций. • Возможность осуществлять подбор парочек к зашифрованным файлам, документом формата PDF, Word, Excel и PowerPoint по базе паролей, поставленной вендором либо по установленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки полученных файлов в связи на наличие вредоносного содержания, посредством настройки пользовательских правил отправки объектов на анализ; • Возможность визуализации информации о событиях, обнаруженных в песочнице; • Возможность загрузки анализируемого контекста; • Pcap трафика; • Сметки файлов; • Лог активности объекта в среде «Песочницы»; • Скриншоты активности объекта в среде «Песочницы»; • Возможность мониторинга состояния работы основных компонентов системы по протоколу SNMP • Возможность подключения нескольких серверов централизованного управления к одним и тем же серверам компонента Песочница. <p>2) Согласно требованиям подпункта 2) раздела 6 технической спецификации веб-сайт производителя должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный веб-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Супер 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки.</p> <p>3) Согласно разделу 3 технической спецификации Потенциальных Поставщиков должно предоставлять лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяца с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизованного письма от производителя изданные от 09 апреля 2023 г. о том, что партнер TOO «ADELINE» будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца.</p> <p>4) Согласно требованиям подпункта 3) раздела 13 технической спецификации Заказчик вводит с тендерной заявкой Потенциальному поставщику необходимо предоставить электронные копии действующих сертификатов на не менее чем 1 (одного) сертифицированного специалиста по предлагаемому программному обеспечению уровня не ниже сертифицированного системный инженер. Однако, предоставленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emil Saidov не позволяет определить уровень его квалификации.</p>
---	---------------	----------	---

Тендерные заявки, которые не соответствуют условиям тендера: 2

№	Наименование потенциального поставщика	БИН (ИИН) / ИНН / УНП	Итоговое решение комиссии
1	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "TRADE IT"	221140033126	отклонен
2	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ADELINE"	070140016160	отклонен

Тендерные заявки, которые соответствуют условиям тендера: 2

№	Наименование потенциального поставщика	БИН (ИИН) / ИНН / УНП
1	"ITware" (Айтиваре) жауапкершілігі шектеулі серіктестігі	121040015817
2	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "THERION"	170540022814

Окончательная дата и время предоставления дополнительных документов, предоставляемых потенциальными поставщиками, в целях приведения их тендерных заявок в соответствие условиям тендера: не позднее 3 рабочих дней с момента публикации данного протокола.

Состав комиссии	Признак присутствия/причина отсутствия
Председатель тендерной комиссии	Да
Заместитель Председателя тендерной комиссии	Да
Члены тендерной комиссии	Да
	Да
	Да
Секретарь тендерной комиссии	Да

Примечание:

* Сведения о заказчике не отображаются, если несколько заказчиков.

Расшифровка аббревиатур:

БИН - бизнес-идентификационный номер;

ИИН - индивидуальный идентификационный номер;

ИНН - идентификационный номер налогоплательщика;

УНП - учетный номер плательщика;

Ф.И.О. - фамилия имя отчество;

ДД.ММ.ГГГГ. - день, месяц, год.



Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года "Об электронном документе и электронной цифровой подписи" равнозначен документу на бумажном носителе.