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-Т2	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-Т2
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:

№	"ITware" (АйТиваре) жауапкершілігі шектеулі серіктестігі, 121040015817			
	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдамау себебі	Қабылдамау себептеріне негіздеме. Әлеуетті жеткізушінің өтініміндегі тендер талаптарына сәйкес келтірілуі тиіс құжаттар тізбесі
1	Комиссияның мүшесі	өткізілді		
2	Төраға	өткізілді		
3	Комиссияның мүшесі	өткізілді		
4	Комиссияның мүшесі	өткізілді		
5	Төрағаның орынбасары	өткізілді		
№	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "TRADE IT", 221140033126			
	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдамау себебі	Қабылдамау себептеріне негіздеме. Әлеуетті жеткізушінің өтініміндегі тендер талаптарына сәйкес келтірілуі тиіс құжаттар тізбесі
1	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып, әлеуетті өнім берушінің техникалық ерекшелігінің Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейтіндігіне байланысты, атап айтқанда: тендерлік өтінім беру шеңберінде әлеуетті өнім берушінің техникалық ерекшеліктің 13-бөлімінің 3) тармақшасының талаптарын бұза отырып, 13.03.2023 жылғы № 002.11.6-5685 және № 025.5 сертификаттары ұсынылды-13591 28.04.2023 жылы қолданылу мерзімі өткен (өндірушінің ресми сайтына сәйкес № 002.11.6-5685 сертификаты: 31.12.2023 жылға дейін жарамды, № 025.5-13591 сертификаты: 01.10.2024 жылға дейін жарамды).
2	Төраға	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып, әлеуетті өнім берушінің техникалық ерекшелігінің Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейтіндігіне байланысты, атап айтқанда: тендерлік өтінім беру шеңберінде әлеуетті өнім берушінің техникалық ерекшеліктің 13-бөлімінің 3) тармақшасының талаптарын бұза отырып, 13.03.2023 жылғы № 002.11.6-5685 және № 025.5 сертификаттары ұсынылды-13591 28.04.2023 жылы қолданылу мерзімі өткен (өндірушінің ресми сайтына сәйкес № 002.11.6-5685 сертификаты: 31.12.2023 жылға дейін жарамды, № 025.5-13591 сертификаты: 01.10.2024 жылға дейін жарамды).
3	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып, әлеуетті өнім берушінің техникалық ерекшелігінің Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейтіндігіне байланысты, атап айтқанда: тендерлік өтінім беру шеңберінде әлеуетті өнім берушінің техникалық ерекшеліктің 13-бөлімінің 3) тармақшасының талаптарын бұза отырып, 13.03.2023 жылғы № 002.11.6-5685 және № 025.5 сертификаттары ұсынылды-13591 28.04.2023 жылы қолданылу мерзімі өткен (өндірушінің ресми сайтына сәйкес № 002.11.6-5685 сертификаты: 31.12.2023 жылға дейін жарамды, № 025.5-13591 сертификаты: 01.10.2024 жылға дейін жарамды).
4	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып, әлеуетті өнім берушінің техникалық ерекшелігінің Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейтіндігіне байланысты, атап айтқанда: тендерлік өтінім беру шеңберінде әлеуетті өнім берушінің техникалық ерекшеліктің 13-бөлімінің 3) тармақшасының талаптарын бұза отырып, 13.03.2023 жылғы № 002.11.6-5685 және № 025.5 сертификаттары ұсынылды-13591 28.04.2023 жылы қолданылу мерзімі өткен (өндірушінің ресми сайтына сәйкес № 002.11.6-5685 сертификаты: 31.12.2023 жылға дейін жарамды, № 025.5-13591 сертификаты: 01.10.2024 жылға дейін жарамды).
5	Төрағаның орынбасары	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып, әлеуетті өнім берушінің техникалық ерекшелігінің Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейтіндігіне байланысты, атап айтқанда: тендерлік өтінім беру шеңберінде әлеуетті өнім берушінің техникалық ерекшеліктің 13-бөлімінің 3) тармақшасының талаптарын бұза отырып, 13.03.2023 жылғы № 002.11.6-5685 және № 025.5 сертификаттары ұсынылды-13591 28.04.2023 жылы қолданылу мерзімі өткен (өндірушінің ресми сайтына сәйкес № 002.11.6-5685 сертификаты: 31.12.2023 жылға дейін жарамды, № 025.5-13591 сертификаты: 01.10.2024 жылға дейін жарамды).
№	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "THERION", 170540022814			
	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдамау себебі	Қабылдамау себептеріне негіздеме. Әлеуетті жеткізушінің өтініміндегі тендер талаптарына сәйкес келтірілуі тиіс құжаттар тізбесі
1	Комиссияның мүшесі	өткізілді		
2	Төраға	өткізілді		
3	Комиссияның мүшесі	өткізілді		
4	Комиссияның мүшесі	өткізілді		
5	Төрағаның орынбасары	өткізілді		
№	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ADELINE", 070140016160			
	Комиссиядағы рөлі	Комиссия мүшесінің шешімі	Қабылдамау себебі	Қабылдамау себептеріне негіздеме. Әлеуетті жеткізушінің өтініміндегі тендер талаптарына сәйкес келтірілуі тиіс құжаттар тізбесі

1	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып жіберілмеді, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейді, атап айтқанда: 1) Әлеуетті жеткізушінің техникалық ерекшелігінің 4-бөлімінде мынадай тармақтар мен ұсыныстар жоқ: А) бағдарламалық құралда/вирусқа қарсы қорғаныс модулінде мынадай функционалдылық мүмкіндіктер жүзеге асырылуы тиіс: • жүктелетін Web беттеріндегі баннерлер мен қалқымалы терезелерді бұғаттау; • желілік сегменттерді санаттауға болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағиадалар құруға мүмкіндік беретін кіріктірілген желі экраны; • кез келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдардан қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартатын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory ішінен белгілі бір пайдаланушыларға тағайындау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау; • арнайы жүктеу агентін құрып, Single Sign On технологиясын қолдай отырып, толық дискіні шифрлау, UEFI жүйелерін қолдау; • жүктеу агенті немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қолдау; • шифрланатын контентті икемді көрсетуге болатын файлдарды шифрлау (орналасқан жері бойынша, кеңейту бойынша, файлды жасайтын қосымша бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ құпия сөздің көмегімен ұйымнан тыс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнатуға болатын алынбалы медиадағы деректерді шифрлау. Б) Windows серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • желілік сегменттерді санаттауға 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-қатерден қорғау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау. В) MacOS жұмыс станцияларына арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартатын белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі. Г) Linux жұмыс станциялары мен серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • Mageia 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • SkipPlainTextFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. Д) Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • пошталық қауіп-қатерден қорғау (Outlook плагині); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық түрде жаңартатын санатқа қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу. Е) Мобильді құрылғыларды вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қосымшаларды іске қосуды бақылау шеңберінде жүйелік қосымшаларды бұғаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарландыруларды жіберу; • Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды көрсету. Ж) Windows ОЖ негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар: • 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; • Postgres Pro 13.x (барлық редакция); • Postgres Pro 14.x (барлық редакция). • пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты вирусқа қарсы шешімнің баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар; • қайта бөлінетін триггерлердің иерархиялары; • клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу; • виртуалды машиналар желісін тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұйымның кез келген компьютерін көрсетуі; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, бұғаттау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді 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 таңдаған компьютерлерге, соның ішінде «жалаңаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жиынтығын қосу мүмкіндігі қамтамасыз етілуі тиіс; • дистрибутивтерден (WIM) операциялық жүйенің үлгісін импорттау мүмкіндігі; • лицензияны пайдаланудың бұзылғаны немесе лицензияның қолданылу мерзімінен асып кеткені туралы басқарушыға хабарлау мүмкіндігі бар компьютерде орнатылған бөгде БЖ лицензияларын бақылау жүйесінің болуы; • бөгде қосымшаларға арналған орнату пакеттерін автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалдығын қолдау; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрату мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; З) Linux ОЖ базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жоқ: Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек • 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; • қайта бөлінетін триггерлердің иерархиялары; • виртуалды машиналар желісінде тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын жұмысқа қабілеттілігі мен қателерді тексеру мүмкіндігі; • басты Сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелері бар серверлерді бағыныштылар ретінде басқару. И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар: • Агенттерден келетін оқиғаларды өзі арқылы проксиге арналған жекелеген бағдарламалық компоненттері, сенсорлары бар. Сенсорлар жүйенің негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компонентін Linux операциялық жүйесі негізінде орналастыруға болады; • Өңделетін сервердің компоненттерін KVM виртуализациясында агент орнатқан хосттардың шектеулі санын және пошта мен желілік трафик оқиғаларының шектеулі 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 көрсетілген параметрлерге сәйкес баптайды. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс – веб-интерфейс қолданылады. Егер жүйе кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларынан алынған файлдарды талдауға арналған YARA қағидаларын жүктеу мүмкіндігі; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға вендор не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді таңдау мүмкіндігі; • Құмсалғыштың объектілерді талдауға жіберудің пайдаланушы қағидаларын баптау арқылы зиянды мазмұнның бар-жоғына алынған файлдар мен сілтемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жүктеу және орнату мүмкіндігі болуы тиіс; • Құмсалғыштың пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтама құрамы сияқты параметрлерді баптау мүмкіндігі болуы тиіс; • Құмсалғышта табылған оқиғалар ағашын визуализациялау мүмкіндігі; • Талданатын контексті шығару мүмкіндігі: Трафиктің Pcap; Файлдардың сэмплдері; «Құмсалғыш» ортасындағы объект белсенділігінің логы; «Құмсалғыш» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоколы бойынша жүйенің негізгі компоненттерінің жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару серверін бір Құмсалғыш компоненттерінің серверлеріне қосу мүмкіндігі. 2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірушінің web-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, БЖ өндірушінің ресми web сайты (https://www.cynet.com/) шет тілінде орындалды, сондай-ақ осы сайтта Әлеуетті жеткізуші өзінің тендерлік өтінімін беру шеңберінде мәлімдеген «Cynet 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмайды. 3) техникалық ерекшеліктің 3-бөліміне сәйкес Әлеуетті жеткізуші Тапсырыс берушіге лицензия берілген күннен бастап кемінде 24 ай мерзімге вирусқа қарсы бақылайтын бағдарламалық жасақтаманы пайдалану және зиянды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС серіктесі 24 айға техникалық қолдаумен бірге лицензияға жылдық жазылымды жеткізетіні туралы өндірушіден авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынды. 4) Әлеуетті жеткізуші ұсынған Emir Saidov-тың атына 19.03.2025 жылғы сертификаттың (осы сертификаттың CCASP өткендігі үшін Саидов Эмирге берілгені туралы нотариалды куәландырылған аудармасымен) Тапсырыс берушінің техникалық ерекшелігінің 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтамаға ұсынылған сертификатталған маманның сертификатталған жүйелік инженерден төмен емес деңгейді қамтамасыз ету туралы ақпарат расталмайды.

2	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып жіберілмеді, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейді, атап айтқанда: 1) Әлеуетті жеткізушінің техникалық ерекшелігінің 4-бөлімінде мынадай тармақтар мен ұсыныстар жоқ: А) бағдарламалық құралда/вирусқа қарсы қорғаныс модулінде мынадай функционалдылық мүмкіндіктер жүзеге асырылуы тиіс: • жүктелетін Web беттеріндегі баннерлер мен қалқымалы терезелерді бұғаттау; • желілік сегменттерді санаттауға болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағиадалар құруға мүмкіндік беретін кіріктірілген желі экраны; • кез келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдардан қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартатын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory ішінен белгілі бір пайдаланушыларға тағайындау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау; • арнайы жүктеу агентін құрып, Single Sign On технологиясын қолдай отырып, толық дискіні шифрлау, UEFI жүйелерін қолдау; • жүктеу агенті немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қолдау; • шифрланатын контентті икемді көрсетуге болатын файлдарды шифрлау (орналасқан жері бойынша, кеңейту бойынша, файлды жасайтын қосымша бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ құпия сөздің көмегімен ұйымнан тыс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнатуға болатын алынбалы медиадағы деректерді шифрлау. Б) Windows серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • желілік сегменттерді санаттауға 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-қатерден қорғау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау. В) MacOS жұмыс станцияларына арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартатын белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі. Г) Linux жұмыс станциялары мен серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • Mageia 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • SkipPlainTextFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. Д) Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • пошталық қауіп-қатерден қорғау (Outlook плагині); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық түрде жаңартатын санатқа қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу. Е) Мобильді құрылғыларды вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қосымшаларды іске қосуды бақылау шеңберінде жүйелік қосымшаларды бұғаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарландыруларды жіберу; • Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды көрсету. Ж) Windows ОЖ негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар: • 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; • Postgres Pro 13.x (барлық редакция); • Postgres Pro 14.x (барлық редакция). • пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты вирусқа қарсы шешімнің баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар; • қайта бөлінетін триггерлердің иерархиялары; • клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу; • виртуалды машиналар желісін тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұйымның кез келген компьютерін көрсетуі; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, бұғаттау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді 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 бақсарушы таңдаған компьютерлерге, соның ішінде «жалаңаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жиынтығын қосу мүмкіндігі қамтамасыз етілуі тиіс; • дистрибутивтерден (WIM) операциялық жүйенің үлгісін импорттау мүмкіндігі; • лицензияны пайдаланудың бұзылғаны немесе лицензияның қолданылу мерзімінен асып кеткені туралы басқарушыға хабарлау мүмкіндігі бар компьютерде орнатылған бөгде БЖ лицензияларын бақылау жүйесінің болуы; • бөгде қосымшаларға арналған орнату пакеттерін автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалдығын қолдау; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрату мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; 3) Linux ОЖ базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жоқ: Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек • 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; • қайта бөлінетін триггерлердің иерархиялары; • виртуалды машиналар желісінде тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын жұмысқа қабілеттілігі мен қателерді тексеру мүмкіндігі; • басты Сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелері бар серверлерді бағыныштылар ретінде басқару. И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар: • Агенттерден келетін оқиғаларды өзі арқылы проксиге арналған жекелеген бағдарламалық компоненттері, сенсорлары бар. Сенсорлар жүйенің негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компонентін Linux операциялық жүйесі негізінде орналастыруға болады; • Өңделетін сервердің компоненттерін KVM виртуализациясында агент орнатқан хосттардың шектеулі санын және пошта мен желілік трафик оқиғаларының шектеулі 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 көрсетілген параметрлерге сәйкес баптайды. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс – веб-интерфейс қолданылады. Егер жүйе кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларынан алынған файлдарды талдауға арналған YARA қағидаларын жүктеу мүмкіндігі; • Шифрланған арихивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға вендор не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді таңдау мүмкіндігі; • Құмсалғыштың объектілерді талдауға жіберудің пайдаланушы қағидаларын баптау арқылы зиянды мазмұнның бар-жоғына алынған файлдар мен сілтемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жүктеу және орнату мүмкіндігі болуы тиіс; • Құмсалғыштың пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтама құрамы сияқты параметрлерді баптау мүмкіндігі болуы тиіс; • Құмсалғышта табылған оқиғалар ағашын визуализациялау мүмкіндігі; • Талданатын контекстті шығару мүмкіндігі: Трафиктің Pcap; Файлдардың сэмплдері; «Құмсалғыш» ортасындағы объект белсенділігінің логы; «Құмсалғыш» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоколы бойынша жүйенің негізгі компоненттерінің жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару серверін бір Құмсалғыш компоненттерінің серверлеріне қосу мүмкіндігі. 2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірушінің web-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, БЖ өндірушінің ресми web сайты (https://www.cynet.com/) шет тілінде орындалды, сондай-ақ осы сайтта Әлеуетті жеткізуші өзінің тендерлік өтінімін беру шеңберінде мәлімдеген «Cynet 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмайды. 3) техникалық ерекшеліктің 3-бөліміне сәйкес Әлеуетті жеткізуші Тапсырыс берушіге лицензия берілген күннен бастап кемінде 24 ай мерзімге вирусқа қарсы бақылайтын бағдарламалық жасақтаманы пайдалану және зиянды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС серіктесі 24 айға техникалық қолдаумен бірге лицензияға жылдық жазылымды жеткізетіні туралы өндірушіден авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынды. 4) Әлеуетті жеткізуші ұсынған Emir Saidov-тың атына 19.03.2025 жылғы сертификаттың (осы сертификаттың CCASP өткендігі үшін Саидов Эмирге берілгені туралы нотариалды куәландырылған аудармасымен) Тапсырыс берушінің техникалық ерекшелігінің 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтамаға ұсынылған сертификатталған маманның сертификатталған жүйелік инженерден төмен емес деңгейді қамтамасыз ету туралы ақпарат расталмайды.

3	Төраға	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып жіберілмеді, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейді, атап айтқанда: 1) Әлеуетті жеткізушінің техникалық ерекшелігінің 4-бөлімінде мынадай тармақтар мен ұсыныстар жоқ: А) бағдарламалық құралды/вирусқа қарсы қорғаныс модулінде мынадай функционалдық мүмкіндіктер жүзеге асырылуы тиіс: • жүктелетін Web беттеріндегі баннерлер мен қалқымалы терезелерді бұғаттау; • желілік сегменттерді санаттауға болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағидалар құруға мүмкіндік беретін кіріктірілген желі экраны; • кез келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдардан қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартатын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory ішінен белгілі бір пайдаланушыларға тағайындау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді күпия сөзбен қорғау; • интернетке қостығу шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау; • арнайы жүктеу агентін құрып, Single Sign On технологиясын қолдай отырып, толық дискіні шифрлау, UEFI жүйелерін қолдау; • жүктеу агенті немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қолдау; • шифрланатын контентті икемді көрсетуге болатын файлдарды шифрлау (орналасқан жері бойынша, кеңейту бойынша, файлды жасайтын қосымша бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ күпия сөздің көмегімен ұйымнан тыс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнатуға болатын алынбалы медиадағы деректерді шифрлау. Б) Windows серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • желілік сегменттерді санаттауға 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-қатерден қорғау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді күпия сөзбен қорғау; • егер интернетке қостығу шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау. В) MacOS жұмыс станцияларына арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартатын белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі. Г) Linux жұмыс станцияларын мен серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • Mageia 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • SkipPlainTextFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. Д) Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • пошталық қауіп-қатерден қорғау (Outlook плагині); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық түрде жаңартатын санатқа қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу. Е) Мобильді құрылғыларды вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қосымшаларды іске қосуды бақылау шеңберінде жүйелік қосымшаларды бұғаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарландыруларды жіберу; • Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды көрсету. Ж) Windows ОЖ негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар: • 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; • Postgres Pro 13.x (барлық редакция); • Postgres Pro 14.x (барлық редакция). • пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты вирусқа қарсы шешімнің баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар; • қайта бөлінетін триггерлердің иерархиялары; • клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу; • виртуалды машиналар желісін тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұйымның кез келген компьютерін көрсетуі; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, бұғаттау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді 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 бақсарушы таңдаған компьютерлерге, соның ішінде «жалаңаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жиынтығын қосу мүмкіндігі қамтамасыз етілуі тиіс; • дистрибутивтерден (WIM) операциялық жүйенің үлгісін импорттау мүмкіндігі; • лицензияны пайдалануды бұзылғаны немесе лицензияның қолданылу мерзімінен асып кеткені туралы басқарушыға хабарлау мүмкіндігі бар компьютерде орнатылған бөгде БЖ лицензияларын бақылау жүйесінің болуы; • бөгде қосымшаларға арналған орнату пакеттерін автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалдығын қолдау; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрату мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; 3) Linux ОЖ базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жоқ: Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек • 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; • қайта бөлінетін триггерлердің иерархиялары; • виртуалды машиналар желісінде тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын жұмысқа қабілеттілігі мен қателерді тексеру мүмкіндігі; • басты Сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелері бар серверлерді бағыныштылар ретінде басқару. И) Шабуылдарды анықтау модулінде қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар: • Агенттерден келетін оқиғаларды өзі арқылы проксиге арналған жекелеген бағдарламалық компоненттері, сенсорлары бар. Сенсорлар жүйенің негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компонентін Linux операциялық жүйесі негізінде орналастыруға болады; • Өңделетін сервердің компоненттерін KVM виртуализациясында агент орнатқан хосттардың шектеулі санын және пошта мен желілік трафик оқиғаларының шектеулі 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 көрсетілген параметрлерге сәйкес баптайды. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс – веб-интерфейс қолданылады. Егер жүйе кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларынан алынған файлдарды талдауға арналған YARA қағидаларын жүктеу мүмкіндігі; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға вендор не қолмен қалдырылған пайдалануы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді таңдау мүмкіндігі; • Құмсалғыштың объектілерді талдауға жіберудің пайдалануы қағидаларын баптау арқылы зиянды мазмұнның бар-жоғына алынған файлдар мен сілтемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдалануы үлгілерін жүктеу және орнату мүмкіндігі болуы тиіс; • Құмсалғыштың пайдалануы үлгілеріне компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтама құрамы сияқты параметрлерді баптау мүмкіндігі болуы тиіс; • Құмсалғышта табылған оқиғалар ағашын визуализациялау мүмкіндігі; • Талданатын контекстті шығару мүмкіндігі: Трафиктің Pcap; Файлдардың сэмплдері; «Құмсалғыш» ортасындағы объект белсенділігінің логы; «Құмсалғыш» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоколы бойынша жүйенің негізгі компоненттерінің жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару серверін бір Құмсалғыш компоненттерінің серверлеріне қосу мүмкіндігі. 2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірушінің web-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, БЖ өндірушінің ресми web сайты (https://www.cynet.com/) шет тілінде орындалды, сондай-ақ осы сайтта Әлеуетті жеткізуші өзінің тендерлік өтінімін беру шеңберінде мәлімдеген «Cynet 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмайды. 3) техникалық ерекшеліктің 3-бөліміне сәйкес Әлеуетті жеткізуші Тапсырыс берушіге лицензия берілген күннен бастап кемінде 24 ай мерзімге вирусқа қарсы бақылайтын бағдарламалық жасақтаманы пайдалану және зиянды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС сериктесі 24 айға техникалық қолдаумен бірге лицензияға жылдық жазылымды жеткізетіні туралы өндірушіден авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынды. 4) Әлеуетті жеткізуші ұсынған Emir Saidov-тың атына 19.03.2025 жылғы сертификаттың (осы сертификаттың CCASP өткендігі үшін Саидов Эмирге берілгені туралы нотариалды куәландырылған аудармасымен) Тапсырыс берушінің техникалық ерекшелігінің 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтамаға ұсынылған сертификатталған маманның сертификаттарға жүйелік инженерден төмен емес деңгейді қамтамасыз ету туралы ақпарат расталмайды.

4	Төрағаның орынбасары	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып жіберілмеді, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейді, атап айтқанда: 1) Әлеуетті жеткізушінің техникалық ерекшелігінің 4-бөлімінде мынадай тармақтар мен ұсыныстар жоқ: А) бағдарламалық құралда/вирусқа қарсы қорғаныс модулінде мынадай функционалдылық мүмкіндіктер жүзеге асырылуы тиіс: • жүктелетін Web беттеріндегі баннерлер мен қалқымалы терезелерді бұғаттау; • желілік сегменттерді санаттауға болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағиадалар құруға мүмкіндік беретін кіріктірілген желі экраны; • кез келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдардан қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартатын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory ішінен белгілі бір пайдаланушыларға тағайындау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау; • арнайы жүктеу агентін құрып, Single Sign On технологиясын қолдай отырып, толық дискіні шифрлау, UEFI жүйелерін қолдау; • жүктеу агенті немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қолдау; • шифрланатын контентті икемді көрсетуге болатын файлдарды шифрлау (орналасқан жері бойынша, кеңейту бойынша, файлды жасайтын қосымша бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ құпия сөздің көмегімен ұйымнан тыс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнатуға болатын алынбалы медиадағы деректерді шифрлау. Б) Windows серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • желілік сегменттерді санаттауға 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-қатерден қорғау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау. В) MacOS жұмыс станцияларына арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартатын белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі. Г) Linux жұмыс станциялары мен серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • Mageia 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • SkipPlainTextFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. Д) Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • пошталық қауіп-қатерден қорғау (Outlook плагині); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық түрде жаңартатын санатқа қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу. Е) Мобильді құрылғыларды вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қосымшаларды іске қосуды бақылау шеңберінде жүйелік қосымшаларды бұғаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарландыруларды жіберу; • Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды көрсету. Ж) Windows ОЖ негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар: • 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; • Postgres Pro 13.x (барлық редакция); • Postgres Pro 14.x (барлық редакция). • пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты вирусқа қарсы шешімнің баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар; • қайта бөлінетін триггерлердің иерархиялары; • клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу; • виртуалды машиналар желісін тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұйымның кез келген компьютерін көрсетуі; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, бұғаттау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді 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 таңдаған компьютерлерге, соның ішінде «жалаңаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жиынтығын қосу мүмкіндігі қамтамасыз етілуі тиіс; • дистрибутивтерден (WIM) операциялық жүйенің үлгісін импорттау мүмкіндігі; • лицензияны пайдаланудың бұзылғаны немесе лицензияның қолданылу мерзімінен асып кеткені туралы басқарушыға хабарлау мүмкіндігі бар компьютерде орнатылған бөгде БЖ лицензияларын бақылау жүйесінің болуы; • бөгде қосымшаларға арналған орнату пакеттерін автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалдығын қолдау; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрату мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; З) Linux ОЖ базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жоқ: Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек • 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; • қайта бөлінетін триггерлердің иерархиялары; • виртуалды машиналар желісінде тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын жұмысқа қабілеттілігі мен қателерді тексеру мүмкіндігі; • басты Сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелері бар серверлерді бағыныштылар ретінде басқару. И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар: • Агенттерден келетін оқиғаларды өзі арқылы проксиге арналған жекелеген бағдарламалық компоненттері, сенсорлары бар. Сенсорлар жүйенің негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компонентін Linux операциялық жүйесі негізінде орналастыруға болады; • Өңделетін сервердің компоненттерін KVM виртуализациясында агент орнатқан хосттардың шектеулі санын және пошта мен желілік трафик оқиғаларының шектеулі 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 көрсетілген параметрлерге сәйкес баптайды. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс – веб-интерфейс қолданылады. Егер жүйе кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларынан алынған файлдарды талдауға арналған YARA қағидаларын жүктеу мүмкіндігі; • Шифрланған архивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға вендор не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді таңдау мүмкіндігі; • Құмсалғыштың объектілерді талдауға жіберудің пайдаланушы қағидаларын баптау арқылы зиянды мазмұнның бар-жоғына алынған файлдар мен сілтемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жүктеу және орнату мүмкіндігі болуы тиіс; • Құмсалғыштың пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтама құрамы сияқты параметрлерді баптау мүмкіндігі болуы тиіс; • Құмсалғышта табылған оқиғалар ағашын визуализациялау мүмкіндігі; • Талданатын контексті шығару мүмкіндігі: Трафиктің Pcap; Файлдардың сэмплдері; «Құмсалғыш» ортасындағы объект белсенділігінің логы; «Құмсалғыш» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоколы бойынша жүйенің негізгі компоненттерінің жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару серверін бір Құмсалғыш компоненттерінің серверлеріне қосу мүмкіндігі. 2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірушінің web-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, БЖ өндірушінің ресми web сайты (https://www.cynet.com/) шет тілінде орындалды, сондай-ақ осы сайтта Әлеуетті жеткізуші өзінің тендерлік өтінімін беру шеңберінде мәлімдеген «Cynet 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмайды. 3) техникалық ерекшеліктің 3-бөліміне сәйкес Әлеуетті жеткізуші Тапсырыс берушіге лицензия берілген күннен бастап кемінде 24 ай мерзімге вирусқа қарсы бақылайтын бағдарламалық жасақтаманы пайдалану және зиянды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС серіктесі 24 айға техникалық қолдаумен бірге лицензияға жылдық жазылымды жеткізетіні туралы өндірушіден авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынды. 4) Әлеуетті жеткізуші ұсынған Emir Saidov-тың атына 19.03.2025 жылғы сертификаттың (осы сертификаттың CCASP өткендігі үшін Саидов Эмирге берілгені туралы нотариалды куәландырылған аудармасымен) Тапсырыс берушінің техникалық ерекшелігінің 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтамаға ұсынылған сертификатталған маманның сертификатталған жүйелік инженерден төмен емес деңгейді қамтамасыз ету туралы ақпарат расталмайды.

5	Комиссияның мүшесі	жіберілген жоқ	93 т. 1 т. тендерлік өтінім тендер талаптарына сәйкес келмеген	Қағидалардың 93-тармағының 1) тармақшасын басшылыққа ала отырып жіберілмеді, себебі Әлеуетті жеткізушінің техникалық ерекшелігі Тапсырыс берушінің техникалық ерекшелігінің талаптарына сәйкес келмейді, атап айтқанда: 1) Әлеуетті жеткізушінің техникалық ерекшелігінің 4-бөлімінде мынадай тармақтар мен ұсыныстар жоқ: А) бағдарламалық құралда/вирусқа қарсы қорғаныс модулінде мынадай функционалдылық мүмкіндіктер жүзеге асырылуы тиіс: • жүктелетін Web беттеріндегі баннерлер мен қалқымалы терезелерді бұғаттау; • желілік сегменттерді санаттауға болатын бағдарламалар үшін желілік пакеттік қағидалар мен желілік қағиадалар құруға мүмкіндік беретін кіріктірілген желі экраны; • кез келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран қағидаларын қолдана отырып, желілік шабуылдардан қорғау; • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық түрде жаңартатын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге мүмкіндік беру, сондай-ақ оны тек Active Directory ішінен белгілі бір пайдаланушыларға тағайындау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау; • арнайы жүктеу агентін құрып, Single Sign On технологиясын қолдай отырып, толық дискіні шифрлау, UEFI жүйелерін қолдау; • жүктеу агенті немесе Операциялық жүйелердің (бұдан әрі - ОЖ) файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI-жүйелерді қолдау; • шифрланатын контентті икемді көрсетуге болатын файлдарды шифрлау (орналасқан жері бойынша, кеңейту бойынша, файлды жасайтын қосымша бойынша); • таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ құпия сөздің көмегімен ұйымнан тыс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы; • ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнатуға болатын алынбалы медиадағы деректерді шифрлау. Б) Windows серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • желілік сегменттерді санаттауға 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-қатерден қорғау; • резервтік сақтау қоймасынан объектілерді қалпына келтіруді құпия сөзбен қорғау; • егер интернетке қостыру шектеулі болған жағдайда желілік трафиктің шектеулері; • пайдаланушылар үшін басып шығару құқықтарын баптау. В) MacOS жұмыс станцияларына арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші жасаған және динамикалық түрде жаңартатын белгілі бір ресурстарға немесе ресурстар санаттарына кіруге нақты тыйым салуды немесе рұқсатты қосу; • FileVault шифрлауды басқаруға болатын бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компонентті орталықтандырылған басқару; • дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және құқықтар берілгеннен кейін қажетті жүйелік кеңейтімдерді орнату мүмкіндігі. Г) Linux жұмыс станциялары мен серверлеріне арналған вирусқа қарсы қорғайтын бағдарламалық жасақтамаға қойылатын талаптар: • Mageia 4; • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • SkipPlainTextFiles параметрінің көмегімен бағдарламалардың жұмыс журналдарын тексеруді оңтайландыру. Д) Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қағидалардың бастапқы күйін қалпына келтіруге болатын операциялық жүйенің желілік экранын басқару; • пошталық қауіп-қатерден қорғау (Outlook плагині); • Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық түрде жаңартатын санатқа қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу. Е) Мобильді құрылғыларды вирусқа қарсы қорғайтын бағдарламалық құралдарға қойылатын талаптар: • қосымшаларды іске қосуды бақылау шеңберінде жүйелік қосымшаларды бұғаттау; • Firebase Cloud Messaging (GCM) сервисі арқылы пәрмендер мен хабарландыруларды жіберу; • Wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануға тыйым салу; • орнатуға міндетті қосымшаларды көрсету. Ж) Windows ОЖ негізіндегі орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар: • 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; • Postgres Pro 13.x (барлық редакция); • Postgres Pro 14.x (барлық редакция). • пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай OU немесе қандай қауіпсіздік тобына байланысты вирусқа қарсы шешімнің баптауларын қайта айқындайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар; • қайта бөлінетін триггерлердің иерархиялары; • клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу; • виртуалды машиналар желісін тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; • басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұйымның кез келген компьютерін көрсетуі; • Windows Failover Clustering қолдауы; • Windows Certificate Authority сервисімен интеграцияны қолдау; • пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы; • өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату, мобильді құрылғыларды қарау, бұғаттау пәрмендерін жіберу, құрылғыны іздеу және пайдаланушының мобильді 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 таңдаған компьютерлерге, соның ішінде «жалаңаш темірге» (bare metal) орнату; • бұрын жасалған үлгіге драйвер жиынтығын қосу мүмкіндігі қамтамасыз етілуі тиіс; • дистрибутивтерден (WIM) операциялық жүйенің үлгісін импорттау мүмкіндігі; • лицензияны пайдаланудың бұзылғаны немесе лицензияның қолданылу мерзімінен асып кеткені туралы басқарушыға хабарлау мүмкіндігі бар компьютерде орнатылған бөгде БЖ лицензияларын бақылау жүйесінің болуы; • бөгде қосымшаларға арналған орнату пакеттерін автоматты түрде құру (Adobe Reader, Mozilla Firefox, 7-zip және т.б.) және осы қосымшалар пакеттерін компьютерлерге автоматты түрде орталықтандыру; • деректерді шифрлауды басқару функционалдығын қолдау; • IPv6 және IPv4 мекенжайларымен жұмыс істеу және IPv6 мекенжайлары бар құрылғылары бар желілерді сұрату мүмкіндігі; • пайдаланушылардың компьютерлерінде орнатылған қосымшалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу; 3) Linux ОЖ базасында орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдарына қойылатын талаптар - Тармақтың атауы және оның мынадай мазмұны жоқ: Орталықтандырылған басқару, мониторингілеу және жаңарту бағдарламалық құралдары мынадай нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек • 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; • қайта бөлінетін триггерлердің иерархиялары; • виртуалды машиналар желісінде тану және егер бұл машиналар бір нақты серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; • жаңартуларды тексеру тапсырмасының көмегімен жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын жұмысқа қабілеттілігі мен қателерді тексеру мүмкіндігі; • басты Сервер ретінде әрекет ету және Linux немесе Windows операциялық жүйелері бар серверлерді бағыныштылар ретінде басқару. И) Шабуылдарды анықтау модуліне қойылатын талаптар: Жұмыс станцияларындағы шабуылдарды анықтау бағдарламалық құралына қойылатын талаптар: • Агенттерден келетін оқиғаларды өзі арқылы проксиге арналған жекелеген бағдарламалық компоненттері, сенсорлары бар. Сенсорлар жүйенің негізгі бөлігімен бөлек және біріктірілген орнату режимін қолдауы керек; • Шешімнің барлық компонентін Linux операциялық жүйесі негізінде орналастыруға болады; • Өңделетін сервердің компоненттерін KVM виртуализациясында агент орнатқан хосттардың шектеулі санын және пошта мен желілік трафик оқиғаларының шектеулі 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 көрсетілген параметрлерге сәйкес баптайды. • Масштабтау параметрлерін баптау үшін масштабтауды басқару үшін бөлек веб-интерфейс – веб-интерфейс қолданылады. Егер жүйе кластер түрінде орналастырылған болса, масштабтауды басқаруға арналған веб-интерфейсте сіз серверлер тізімін қарап, кластерді өшіре аласыз; • Жұмыс станцияларынан алынған файлдарды талдауға арналған YARA қағидаларын жүктеу мүмкіндігі; • Шифрланған арихивтерге, PDF, Word, Excel және PowerPoint форматындағы құжаттарға вендор не қолмен қалдырылған пайдаланушы тізімдері бойынша құпия сөз базасы бойынша құпия сөздерді таңдау мүмкіндігі; • Құмсалғыштың объектілерді талдауға жіберудің пайдаланушы қағидаларын баптау арқылы зиянды мазмұнның бар-жоғына алынған файлдар мен сілтемелерді тексеру мақсатында Windows операциялық жүйелерінің пайдаланушы үлгілерін жүктеу және орнату мүмкіндігі болуы тиіс; • Құмсалғыштың пайдаланушы үлгілерінде компьютер атауы, локализация, пайдаланушының есептік жазбалары және бағдарламалық жасақтама құрамы сияқты параметрлерді баптау мүмкіндігі болуы тиіс; • Құмсалғышта табылған оқиғалар ағашын визуализациялау мүмкіндігі; • Талданатын контекстті шығару мүмкіндігі: Трафиктің Pcap; Файлдардың сэмплдері; «Құмсалғыш» ортасындағы объект белсенділігінің логы; «Құмсалғыш» ортасындағы объект белсенділігінің скриншоттары; • SNMP протоколы бойынша жүйенің негізгі компоненттерінің жұмыс жағдайын мониторингілеу мүмкіндігі • Бірнеше орталықтандырылған басқару серверін бір Құмсалғыш компоненттерінің серверлеріне қосу мүмкіндігі. 2) техникалық ерекшеліктің 6-бөлімі 2) тармақшасының талаптарына сәйкес өндірушінің web-сайты орыс тілінде болуы, техникалық қолдауға арналған арнайы бөлімі, толықтырылатын білім базасы, сондай-ақ бағдарламалық жасақтаманы пайдаланушылар форумы болуы тиіс. Алайда, БЖ өндірушінің ресми web сайты (https://www.cynet.com/) шет тілінде орындалды, сондай-ақ осы сайтта Әлеуетті жеткізуші өзінің тендерлік өтінімін беру шеңберінде мәлімдеген «Cynet 360 Elite» деп аталатын бағдарламалық өнімнің болуы расталмайды. 3) техникалық ерекшеліктің 3-бөліміне сәйкес Әлеуетті жеткізуші Тапсырыс берушіге лицензия берілген күннен бастап кемінде 24 ай мерзімге вирусқа қарсы бақылайтын бағдарламалық жасақтаманы пайдалану және зиянды белсенділікті анықтау және зерделеу құқығына лицензия беруге тиіс. Алайда, Әлеуетті жеткізуші 2025 жылғы 9 сәуірден бастап «ADELINE» ЖШС серіктесі 24 айға техникалық қолдаумен бірге лицензияға жылдық жазылымды жеткізетіні туралы өндірушіден авторизациялық хаттың нотариалды куәландырылған аудармасын ұсынды. 4) Әлеуетті жеткізуші ұсынған Emir Saidov-тың атына 19.03.2025 жылғы сертификаттың (осы сертификаттың CCASP өткендігі үшін Саидов Эмирге берілгені туралы нотариалды куәландырылған аудармасымен) Тапсырыс берушінің техникалық ерекшелігінің 13-бөлімінің 3) тармақшасының талаптарына сәйкестігі туралы, атап айтқанда: ұсынылатын бағдарламалық жасақтамаға ұсынылған сертификатталған маманның сертификатталған жүйелік инженерден төмен емес деңгейді қамтамасыз ету туралы ақпарат расталмайды.

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-II 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-Т2	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-Т2
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:

№	"ITware" (АйТиваре) жауапкершілігі шектеулі серіктестігі, 121040015817			
	Роль в комиссии	Решение члена комиссии	Причина отклонения	Обоснование причин 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		
№	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "TRADE IT", 221140033126			
	Роль в комиссии	Решение члена комиссии	Причина отклонения	Обоснование причин отклонения. Перечень документов в заявке потенциального поставщика которые необходимо привести в соответствие с условиями тендера
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 допущен, 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).
№	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "THERION", 170540022814			
	Роль в комиссии	Решение члена комиссии	Причина отклонения	Обоснование причин 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		
№	ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ADELINE", 070140016160			
	Роль в комиссии	Решение члена комиссии	Причина отклонения	Обоснование причин отклонения. Перечень документов в заявке потенциального поставщика которые необходимо привести в соответствие с условиями тендера

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: 1) В разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения: А) в программном средстве\модуле антивирусной защиты должны быть реализованы следующие функциональные возможности: • блокировку 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 вычислетильных 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, категории 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 паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать 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. Б) Требования к программным средствам антивирусной защиты для серверов Windows: • встроенного сетевого экрана, позволяющего создавать сетевые пакетные 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 устройства; • защитить паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS: • 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 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. Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux: • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles. Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows: • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагин 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. Е) Требования к программным средствам антивирусной защиты мобильных устройств: • блокировка системных приложений, в рамках контроля запуска приложений; • отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows: • 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 переопределяют 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 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, 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 "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутивов (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, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; З) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux" - Отсутствует название пункта и следующее его содержание: Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий • 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 задачи 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. И) Требования к модулю обнаружения атак:Требования к программным средствам обнаружения атак на рабочих станциях: • Иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступаемых 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 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 и планируемый 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 система развернута 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 паролей к зашифрованным архивам, документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставляемой вендором либо по оставленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки получаемых файлов и ссылок 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 обеспечени; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность выгрузки анализируемого контекста: Pcap трафика; Сэмплы файлов; Лог активности объекта в среде «Песочницы»; 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. 2) Согласно требованиям подпункта 2) раздела 6 технической спецификации web-сайт производителя должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный web-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Cynet 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки. 3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя исходящее от 09 апреля 2025 г. о том, что партнёр ТОО"ADELINE" будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца. 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, представленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.

2	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: 1) В разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения: А) в программном средстве\модуле антивирусной защиты должны быть реализованы следующие функциональные возможности: • блокировку 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 вычислетильных 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, категории 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 паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать 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. Б) Требования к программным средствам антивирусной защиты для серверов Windows: • встроенного сетевого экрана, позволяющего создавать сетевые пакетные 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 устройства; • защитить паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS: • 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 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. Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux: • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles. Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows: • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагин 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. Е) Требования к программным средствам антивирусной защиты мобильных устройств: • блокировка системных приложений, в рамках контроля запуска приложений; • отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows: • 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 переопределяют 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 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, 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 "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутивов (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, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; З) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux" - Отсутствует название пункта и следующее его содержание: Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий • 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 задачи 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. И) Требования к модулю обнаружения атак:Требования к программным средствам обнаружения атак на рабочих станциях: • Иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступаемых 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 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 и планируемый 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 система развернута 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 паролей к зашифрованным архивам, документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставляемой вендором либо по оставленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки получаемых файлов и ссылок 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 обеспечени; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность выгрузки анализируемого контекста: Pcap трафика; Сэмплы файлов; Лог активности объекта в среде «Песочницы»; 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. 2) Согласно требованиям подпункта 2) раздела 6 технической спецификации web-сайт производителя должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный web-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Cynet 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки. 3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя исходящее от 09 апреля 2025 г. о том, что партнёр ТОО"ADELINE" будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца. 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, представленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.

3	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: 1) В разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения: А) в программном средстве\модуле антивирусной защиты должны быть реализованы следующие функциональные возможности: • блокировку 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, категории 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 паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать 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. Б) Требования к программным средствам антивирусной защиты для серверов Windows: • встроенного сетевого экрана, позволяющего создавать сетевые пакетные 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 устройства; • защитить паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS: • 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 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. Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux: • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles. Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows: • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагин 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. Е) Требования к программным средствам антивирусной защиты мобильных устройств: • блокировка системных приложений, в рамках контроля запуска приложений; • отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows: • 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 переопределяют 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 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, 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 "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутивов (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, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; 3) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux" - Отсутствует название пункта и следующее его содержание: Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий • 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 задачи 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. И) Требования к модулю обнаружения атак:Требования к программным средствам обнаружения атак на рабочих станциях: • Иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступаемых 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 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 и планируемый 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 система развернута 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 паролей к зашифрованным архивам, документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставляемой вендором либо по оставленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки получаемых файлов и ссылок 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 обеспечени; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность выгрузки анализируемого контекста: Pcap трафика; Сэмплы файлов; Лог активности объекта в среде «Песочницы»; 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. 2) Согласно требованиям подпункта 2) раздела 6 технической спецификации web-сайт производителя должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный web-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Cynet 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки. 3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя исходящее от 09 апреля 2025 г. о том, что партнёр ТОО"ADELINE" будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца. 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, представленный Потенцилным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.

4	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: 1) В разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения: А) в программном средстве\модуле антивирусной защиты должны быть реализованы следующие функциональные возможности: • блокировку 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 вычислетильных 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, категории 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 паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать 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. Б) Требования к программным средствам антивирусной защиты для серверов Windows: • встроенного сетевого экрана, позволяющего создавать сетевые пакетные 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 устройства; • защитить паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS: • 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 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. Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux: • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles. Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows: • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагин 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. Е) Требования к программным средствам антивирусной защиты мобильных устройств: • блокировка системных приложений, в рамках контроля запуска приложений; • отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows: • 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 переопределяют 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 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, 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 "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутивов (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, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; З) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux" - Отсутствует название пункта и следующее его содержание: Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий • 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 задачи 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. И) Требования к модулю обнаружения атак:Требования к программным средствам обнаружения атак на рабочих станциях: • Иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступаемых 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 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 и планируемый 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 система развернута 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 паролей к зашифрованным архивам, документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставляемой вендором либо по оставленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки получаемых файлов и ссылок 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 обеспечени; • Возможность визуализации дерева событий, обнаруженных в песочнице; • Возможность выгрузки анализируемого контекста: Pcap трафика; Сэмплы файлов; Лог активности объекта в среде «Песочницы»; 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. 2) Согласно требованиям подпункта 2) раздела 6 технической спецификации web-сайт производителя должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный web-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Cynet 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки. 3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя исходящее от 09 апреля 2025 г. о том, что партнёр ТОО"ADELINE" будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца. 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, представленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.

5	Член комиссии	отклонен	пп. 1 п. 93 несоответствие тендерной заявки условиям тендера	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: 1) В разделе 4 технической спецификации Потенциального поставщика отсутствуют следующие пункты и предложения: А) в программном средстве/модуле антивирусной защиты должны быть реализованы следующие функциональные возможности: • блокировку 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, категории 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 паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей; • полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем; • восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов Операционных систем (далее - ОС), поддержка UEFI-систем; • шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); • наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать 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. Б) Требования к программным средствам антивирусной защиты для серверов Windows: • встроенного сетевого экрана, позволяющего создавать сетевые пакетные 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 устройства; • защитить паролем восстановление объектов из резервного хранилища; • ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; • настроить права печати для пользователей. В) Требования к программным средствам антивирусной защиты для рабочих станций MacOS: • 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 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. Г) Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux: • Mageia 4; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles. Д) Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows: • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • защита от почтовых угроз (плагин 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. Е) Требования к программным средствам антивирусной защиты мобильных устройств: • блокировка системных приложений, в рамках контроля запуска приложений; • отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); • заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства; • указать обязательные к установке приложения. Ж) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows: • 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 переопределяют 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 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, 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 "голое железо" (bare metal); • должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ; • возможность импортировать образ операционной системы из дистрибутивов (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, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; • поддержка функциональности управления шифрованием данных; • возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; • автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; 3) Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux" - Отсутствует название пункта и следующее его содержание: Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий • 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 задачи 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. И) Требования к модулю обнаружения атак: Требования к программным средствам обнаружения атак на рабочих станциях: • Иметь отдельные программные компоненты, сенсоры, для проксирования через себя поступаемых 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 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 и планируемый 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 система развернута 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 паролей к зашифрованным архивам, документам формата PDF, Word, Excel и PowerPoint по базе паролей, поставляемой вендором либо по оставленным вручную пользовательским спискам; • Песочница должна иметь возможность загрузки и установки пользовательских образов операционных систем Windows с целью проверки получаемых файлов и ссылок 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 дерева событий, обнаруженных в песочнице; • Возможность выгрузки анализируемого контекста: Pcap трафика; Сэмплы файлов; Лог активности объекта в среде «Песочницы»; 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. 2) Согласно требованиям подпункта 2) раздела 6 технической спецификации web-сайт производителя должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке, пополняемую базу знаний, а также форум пользователей программного обеспечения. Однако, официальный web-сайт производителя ПО (https://www.cynet.com/) выполнен на иностранном языке, а также на данном сайте не подтверждается наличие программного продукта под названием «Cynet 360 Elite», заявленного Потенциальным поставщиком в рамках подачи своей тендерной заявки. 3) Согласно разделу 3 технической спецификации Потенциальный Поставщик должен предоставить лицензию на право использования программного обеспечения антивирусного контроля и обнаружения и изучения вредоносной активности на срок не менее 24 месяцев с даты предоставления лицензии Заказчику. Однако, Потенциальным поставщиком предоставлена нотариально засвидетельствованный перевод авторизационного письма от производителя исходящее от 09 апреля 2025 г. о том, что партнёр ТОО"ADELINE" будет поставлять годовую подписку на лицензию совместно с технической поддержкой на период на 24 месяца. 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, представленный Потенциальным поставщиком сертификат от 19.03.2025 г. на имя Emir Saidov не позволяет определить уровень его квалификации.

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 отображается, 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.