ТЕХНИКАЛЫҚ СИПАТТАМА

1265848 , Ақпараттық қауіпсіздікті қамтамасыз етуді ұзарту қызметі (антивирус және серверлерді қорғау) сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 1 (60-1 У, 4566892) Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер

Тапсырыс беруші: ЖШС "Тау-Кен Алтын"

Ұйымдастырушы: ЖШС "Тау-Кен Алтын"

1. ТЖҚ қысқаша сипаттамасы

Атауы	Мәні
Жол нөмірі	60-1 У
Атауы және қысқаша сипаттамасы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер, Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Қосымша сипаттама	Тиістілігі: ИБ / Сипаттамасы: Ақпараттық қауіпсіздікті қамтамасыз етуді ұзарту жөніндегі қызмет (антивирус және серверлерді қорғау)
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., г. Астана, Индустриальный парк, СЭЗ "Астана-Новый город", ул. А194, д. 1
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 365 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0%

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

1. Соңғы нүктелер мен серверлердің қорғанысын басқарудың бірыңғай консоліне қойылатын талаптар

1.1. Басқару консолін өрістету тапсырыс берушіден бағдарламалық және аппараттық ресурстар бөлуді талап етпеуі тиіс

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

1.3. Қол жеткізу құқықтарын егжей-тегжейлі беру мүмкіндігі бар басқару консоліне рөлдік қол жеткізудің болуы

1.4. Басқару консолі пайдаланушыларының есептік жазбалары үшін екі факторлы аутентификацияны қолдау

1.5. Басқару консолі мен соңғы нүктелердегі модульдер арасындағы деректер алмасу TLS 1.2 арқылы қорғалуы тиіс

1.6. Инциденттерді және/немесе маркерлерді талдау, оларға ден қою және басымдығын айқындау операцияларын жеделдету үшін консольдің барлық бөлімдері бойынша икемді іздеу тетігінің болуы

1.7. Соңғы құрылғылар топтарына саясаттарды тағайындау мүмкіндігі

1.8. Консоль соңғы құрылғыларды статикалық тәртіппен де, төмендегі динамикалық өлшемшарттар бойынша да біріктіруге мүмкіндік беруі тиіс:

1.8.1. ОЖ түрі

1.8.2. Жүйенің желілік параметрлері

1.8.3. Жұмыс станциясы/Сервер

1.8.4. Қорғаныс күйі

1.8.5. Клиенттік модуль нұсқасы

1.9. Шешімнің барлық әкімшілендіру функциялары үшін бірыңғай пайдаланушы интерфейсі болуы тиіс – инциденттерді талдау және оларға ден қою жөніндегі барлық операциялар бір консоль шегінде орындалуы тиіс

1.10. Басқару консолінде әкімшілердің/талдаушылардың санына шектеу болмауы тиіс

1.11. Басқару консолі аудиттің мынадай түрлерін қолдауы тиіс:

1.11.1. Хосттар аудиті

1.11.2. Пайдаланушы әрекеттерінің аудиті

1.11.3. API арқылы қосылымдар аудиті

1.11.4. Саясаттар аудиті

1.11.5. Real Time Response аудиті

1.11.6. Файлдарға қатысты ерекшеліктер аудиті

1.12. Консоль VPN немесе корпоративтік желіге қол жеткізудің басқа құралдарын пайдаланбай, соңғы нүктелерде өрістетілген модульдерді басқару мүмкіндігін қолдауы тиіс (корпоративтік периметрден тыс орналасқан жүйелерді қорғау)

1.13. Консоль инциденттерді басқа талдаушыларға тапсыру және олардың мәртебесін өзгерту мүмкіндігімен талдаушылар тобының инциденттер бойынша бірлесіп жұмыс істеуін қолдауы тиіс

1.14. Басқару консолі инциденттерді олардың арасында дереу ауысу мүмкіндігімен төрт негізгі нысанда көрсетуді қамтамасыз етуі тиіс:

1.14.1. Әрбір хост бойынша жалпы ақпарат

1.14.2. Шабуыл векторы көрсетілген кестелік нысан

1.14.3. Шартты белгілер түсіндірмесі мен шабуылдың дамуы көрсетілген байланыстар графы

1.14.4. Әрбір оқиғаның сипаттамасы бар оқиғалардың уақыт шкаласы

1.15. Алынған деректерді көрнекі көрсетуді жеңілдету және шешім қабылдауды жеделдету үшін іске қосылған процестердің байланыс графтарының масштабын интуитивті түрде өзгерту мүмкіндігі

1.16. Инцидент деректерін қарау кезінде мынадай әрекеттерді дереу орындау мүмкіндігі:

1.16.1. Ден қою әрекеттерін орындау үшін жүйеге интерактивті қосылу

1.16.2. Желілік оқшаулау

1.16.3. Инцидентті топтың нақты мүшесіне бекіту

1.16.4. Инцидент мәртебесін өзгерту

1.16.5. Жүйе, хэш, процесс атауы бойынша деректерді іздеу

1.17. Басқару консолінде бизнес-процестерді автоматтандыруға арналған қосымша WorkFlow функционалы болуы тиіс

1.18. WorkFlow модулінде скриптті жұмыс барысында өзгертуге мүмкіндік беретін икемді құру процесі және әрекеттерді автоматтандырудың дайын үлгілері болуы тиіс

1.19. Басқару консолі төменде көрсетілген барлық модульдер үшін бірыңғай болуы тиіс

1.20. Басқару консоліне қол жеткізу қосылатын модульдер лицензияларының бүкіл қолданылу мерзіміне берілуі тиіс

2. Вирусқа қарсы модульге қойылатын талаптар

Лицензиялар саны кемінде 75 болуы тиіс.

2.1. Модульді өрістету ОЖ-ні қайта жүктеуді талап етпеуі тиіс

2.2. Қауіптерді анықтау кезінде модуль сигнатуралар дерекқорларын пайдаланбауы тиіс

2.3. Соңғы нүктенің басқару консолімен байланысы болмаған жағдайда, шешім орталық консольге қосылғанға дейін 90 күн бойы мінез-құлықты талдау және белгілі ықтимал зиянды операцияларды (жүйені жұқтыру үшін ОЖ-нің кіріктірілген функционалын пайдалану және т.б.) бұғаттау арқылы базалық қорғанысты қамтамасыз етуі тиіс.

2.4. Модуль оның жұмысына араласудан және рұқсатсыз жоюдан қорғауды қолдауы тиіс

2.5. Жеке саясаттар арқылы кіріктірілген желіаралық экранды басқару мүмкіндігі (Windows, Mac жүйелері үшін). Бір жерден басқару.

2.6. Шешім бұрын белгісіз/бірегей зиянды бағдарламалық қамтылымды анықтай алуы тиіс

2.7. Скрипттер қолданылатын шабуылдарды анықтауды жақсарту үшін Microsoft AMSI-мен интеграцияны қолдау

2.8. Белгісіз немесе қайта қапталған зиянды кодты анықтауды жақсарту үшін машиналық оқыту мүмкіндіктерін пайдалану

2.9. Файлдар мен олардың атрибуттарын талдау үшін бедел туралы бұлттық дерекқорды пайдалану

2.10. Жүйелерді жұқтыру үшін пайдаланылатын жүйелік құралдардың күмәнді шақырылуын тану

2.11. Эксплойттардан және процестер жадына манипуляциялар жасаудан қорғау

2.12. Есептік деректерді ұрлаудан немесе есептік жазбаларға манипуляциялар жасаудан қорғау

2.13. Модуль файлдарды өндірушінің бұлттық «құмсалғышына» жіберу мүмкіндігін қолдауы тиіс

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

3. Мінез-құлықты қадағалау және қауіптерге ден қою модуліне қойылатын талаптар

3.1. Модульді өрістету ОЖ-ні қайта жүктеуді талап етпеуі тиіс

3.2. Модуль оның жұмысына араласудан және рұқсатсыз жоюдан қорғауды қолдауы тиіс

3.3. Жеткізілетін модуль құрамына желілік трафикті талдауға арналған модуль кіруі тиіс (host-based network visibility)

3.4. Соңғы нүктелердегі іске қосылған процестер, желілік белсенділік және файлдық жүйедегі операциялар туралы метадеректерді жинау

3.5. Аномалиялар мен ықтимал зиянды операцияларды анықтау үшін жүйедегі өзгерістер реттілігін қадағалау

3.6. Іске қосылған процестерді олардың иелерімен және пайдаланушылардың әрекеттерімен корреляциялау

3.7. Араласуға ден қоюдың мынадай әрекеттерін пайдалану:

3.7.1. Карантин

3.7.2. Файлды, каталогті жою

3.7.3. Процесті, процестер ағашын тоқтату

3.7.4. ОЖ командасын орындау

3.7.5. Еркін скрипттерді орындау

3.8. Саясатты қолданар алдында таңдалған үлгіні тексеру мүмкіндігімен, нақты файлдардың файлдық жүйедегі орналасуына қарай оларды шешім өндірушісінің бұлтына жіберуді болдырмау (тыйым салу) мүмкіндігі

3.9. Соңғы нүктелерден алынатын барлық телеметрия мен метадеректер шифрланған арна арқылы беріліп, тек шешім өндірушісінің бұлтында өңделуі тиіс.

3.10. Жүйе инциденттерге қатысты деректерді олар анықталған сәттен бастап кемінде 90 күн сақтауды қолдауы тиіс

3.11. Жүйе телеметрия деректерін (метадеректердің толық тізбесін) өндірушінің бұлтына берілген сәттен бастап соңғы 7 күн үшін сақтауды, тапсырыс берушінің немесе реттеуші органның талаптары бойынша сақтау мерзімін ұзарту мүмкіндігімен қолдауы тиіс

3.12. Жүйе қауіпті немесе оның жүйеде болу іздерін бейтараптандыру үшін соңғы нүктелерде командалар мен скрипттерді интерактивті орындау мүмкіндігін қолдауы тиіс. PowerShell, Bash, CMD, BAT қолдауы, таңдалған скрипттің орындалу нәтижелерін қадағалау, аналитика мен графикалық талдауды қосу мүмкіндіктері қамтамасыз етілуі тиіс

3.13. Жүйе инциденттерге ден қоюды жеделдету үшін жиі қолданылатын пайдаланушы скрипттерінің кітапханасын қалыптастыру және таңдаулыларды (бұрын қолданылған командаларды) сақтау мүмкіндігін қолдауы тиіс

3.14. Жүйе таңдалған жүйелерді желілік оқшаулау мүмкіндігін, өндіруші консолінен бөлек карантиндегі жүйелерге қолжетімді болатын нақты желілерді баптау мүмкіндігімен қолдауы тиіс

3.15. Желілік оқшаулау (карантин деп аталатын) қолданылатын жүйелер жедел әрекеттерді орындау үшін басқару консолімен (шешім өндірушісінің бұлтымен) байланыста қалуы тиіс.

3.16. Жүйе нысаналы жүйені қайта жүктемей түзетулер енгізуге (командалар мен скрипттерді орындауға) мүмкіндік беруі тиіс

3.17. Модуль ОЖ-нің іске қосылған процестерінің кемінде 600 параметрін жинау мүмкіндігін қолдауы тиіс

3.18. Соңғы нүктелерден алынатын телеметрия индекстелуі және басқару консолінің іздеу сұраулары арқылы іздеу мүмкіндігін қолдауы тиіс

3.19. Соңғы нүктелер телеметриясын экспорттау/жүктеу мүмкіндігі болуы тиіс

3.20. Таңдалған процестің жад дампын жасау мүмкіндігі

4. Жалпы талаптар

4.1. Шешім жүйенің ағымдағы күйін сұрату, инциденттерді және компрометация маркерлерін іздеу, оқиғалар аудитін жүргізу және саясаттарды басқару үшін бұлттық API-ді қолдауы тиіс

4.2. Бұлттық API жүйеден деректерді оқуды да, оларды жазуды/өзгертуді де қолдауы тиіс

4.3. Бұлттық API OAuth 2.0 аутентификация хаттамасын қолдауы тиіс

4.4. Үшінші тарап шешімдерімен интеграция модульдерін басқару мүмкіндігі. Интеграция пакеттерін тікелей бұлттық басқару консолінен қосу мүмкіндігі

4.5. SIEM модулінің және SIEM жүйелерімен интеграцияның болуы

4.6. Басқару консолімен байланыс болмаған немесе басқа техникалық қиындықтар туындаған жағдайда клиенттік модульдерді толық жоюға арналған утилитаның болуы

4.7. Жиналған деректерді басқа қорғаныс модульдерінде әрі қарай пайдалану үшін жүйеден тыс жерге JSON пішімінде беруге мүмкіндік беретін құралдың болуы

4.8. Жүйе анықталған араласу тәсілдері және бұғатталған мінез-құлық бойынша интерактивті анықтаманы қолдауы тиіс

5. SIEM және SOAR модуліне қойылатын талаптар

5.1. Жүйе жергілікті инфрақұрылымға барынша аз тәуелділікпен бұлтта өрістету мүмкіндігін қолдауы тиіс.

5.2. Модульдің базалық функционалы қосылған болуы және қосымша лицензияларсыз жұмыс істеуі тиіс

5.3. Тәулігіне 1 петабайтқа дейінгі деректерді өңдеу үшін ауқымдауды қолдау.

5.4. Жүйені өрістету уақыты қол жеткізу берілген сәттен бастап 48 сағаттан аспауы тиіс.

5.5. SIEM модуліне қол жеткізу негізгі консольден жүзеге асырылуы тиіс

5.6. Жүйе модулі лицензияны кеңейту арқылы қосымша корреляция ережелерін қосу есебінен мүмкіндіктерді кеңейтуді қолдауы тиіс

5.7. Жүйе модулі әртүрлі көздерден, соның ішінде төмендегілерден деректер жинауды қолдауы тиіс:

5.7.1. Endpoint Detection and Response (EDR),

5.7.2. осалдықтарды басқару шешімдері,

5.7.3. желілік құрылғылар (IDS/IPS, желіаралық экрандар),

5.7.4. бұлттық платформалар (AWS, Azure, Google Cloud),

5.7.5. дерекқорлар мен қолданбалар.

5.8. JSON, Syslog, CEF және LEEF пішімдеріндегі деректерді өңдеу мүмкіндігі болуы тиіс.

5.9. Жүйе деректер ағындарын қалыпқа келтіруді және біріктіруді қолдай отырып, оларды орталықтандырылған басқаруды қамтамасыз етуі тиіс.

5.10. Жүйе мінез-құлықты талдау мен жасанды интеллект (AI) негізінде аномалиялар мен қауіптерді автоматты түрде анықтауды қолдауы тиіс.

5.11. Білім қорын кемінде әрбір 15 минут сайын жаңарту мүмкіндігімен MITRE ATT&CK негізінде қауіптерді жіктеуді қолдау.

5.12. Қауіптің мәнмәтінін, таралу жолдарын және жою жөніндегі ұсынымдарды қоса алғанда, оқиғалар туралы егжей-тегжейлі ақпарат беру мүмкіндігі.

5.13. Жүйе деректерді өңдеу және іздеу жылдамдығын секундына кемінде 10 000 оқиға деңгейінде қамтамасыз етуі тиіс.

5.14. Жүйе инциденттерді өңдеу үшін автоматты жұмыс процестерін (playbooks) құруды қолдауы тиіс.

5.15. Құрылғыларды оқшаулауды, IP-мекенжайларды бұғаттауды және қауіпсіздік саясаттарын жаңартуды қоса алғанда, оқиғаларға автоматты түрде ден қою мүмкіндігі.

5.16. SIEM модулінің базалық функционалы дереккөздерден келіп түсетін журнал жазбаларын нақты уақыт режимінде іздеу мүмкіндігін қамтамасыз етуі тиіс

5.17. SIEM модулінің базалық функционалы жеке корреляция ережелерін құру мүмкіндігін қамтамасыз етуі тиіс

5.18. SOAR функционалы базалық жеткізілім құрамына кіруі тиіс.

5.19. Жүйенің архитектурасы ISO 27001, SOC 2 және GDPR стандарттарына сәйкес келетін бұлттық платформа негізінде құрылуы тиіс.

5.20. Жүйе MFA (көп факторлы аутентификация) қолдауымен веб-интерфейс арқылы қол жеткізуді қамтамасыз етуі тиіс

5.21. Жүйе танымал SIEM платформаларымен (Splunk, QRadar, ArcSight) API арқылы интеграцияны қолдауы тиіс.

5.22. Компрометация индикаторларын (IOC) STIX/TAXII пішімінде импорттау мүмкіндігі.

5.23. Жүйе деректерді үшінші тараптың аналитикалық құралдарына экспорттауды қолдауы тиіс.

5.24. Жүйе деректерді беру кезінде және сақталған күйінде шифрлауды қамтамасыз етуі тиіс.

5.25. Қол жеткізуді басқарудың рөлдік моделін пайдалана отырып, рұқсатсыз қол жеткізуден қорғау іске асырылуы тиіс.

5.26. Жүйедегі барлық әрекеттер бойынша аудитті орталықтандырылған басқаруды және журнал жүргізуді қолдау.

5.27. Лицензия API шақыруларының шектеусіз санын және қосымша шығындарсыз жүйенің барлық функцияларын қолдауды қамтуы тиіс.

5.28. Лицензиялау қосылған дереккөздер санына емес, өңделетін деректер көлеміне негізделуі тиіс.

5.29. Модульге қол жеткізу вирусқа қарсы модуль мен мінез-құлықты қадағалау және қауіптерге ден қою модулі лицензияларының бүкіл қолданылу мерзіміне берілуі тиіс

6. Клиенттік модульдердің операциялық жүйелерді қолдауына қойылатын талаптар

6.1. Windows

6.1.1. Клиенттік – Windows 11, 10, 8.1, 7 SP1.

6.1.2. Серверлік – 2008 R2 SP1, 2012 (R2), 2016 (core нұсқасын қоса алғанда), 2019 (core нұсқасын қоса алғанда), 2022 (core нұсқасын қоса алғанда), 2025.

6.2. Mac OS – 10.14.x, 10.15.x және одан жоғары

6.3. Linux – Amazon Linux 2, Amazon Linux AMI 2018.03, 2017.09, CentOS 7.x-8.x, RHL 6.x-9.x, RHL CoreOs 4.x, SUSE 12. x, SUSE 15, Ubuntu 16.04/18.04/20.04/22.04/24.04, Oracle 6-9, Debian 9.x-12.x, Alma Linux 8.x-9.x,

6.4. VDI жүйелері – AWS, Azure, GCP

7. Техникалық талаптар

7.1. Агенттің қатты дискіде алатын көлемі 75 МБ-тан аспауы тиіс.

7.2. Агент пайдаланатын жедел жад көлемі 50 МБ-тан аспауы тиіс. Критикалық жағдайларда – 70 МБ.

8. Орындаушы өндірушіден бірегей кодтары бар жаңа түпнұсқа лицензияларды жеткізуді қамтамасыз етуі керек.

9. Қызмет күн сайын орындалуын талап етеді.

Қол қойған	Карменова Лэйла Нуралиевна
Қол қойылған күні	28.10.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1265848 , Услуга по продлению обеспечения информационной безопасности (Антивирус и защита серверов)
способом Открытый тендер на понижение

Лот № 1 (60-1 У, 4566892) Услуги по обеспечению информационной безопасности

Заказчик: Товарищество с ограниченной ответственностью "Тау-Кен Алтын"
Организатор: Товарищество с ограниченной ответственностью "Тау-Кен Алтын"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	60-1 У
Наименование и краткая характеристика	Услуги по обеспечению информационной безопасности, Услуги по обеспечению информационной безопасности
Дополнительная характеристика	Принадлежность: ИБ /Описание: Услуга по продлению обеспечения информационной безопасности (Антивирус и защита серверов)
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, г. Астана, Индустриальный парк, СЭЗ "Астана-Новый город", ул. А194, д. 1
Условия поставки	-
Срок поставки	С даты подписания договора в течение 365 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

1. Требования к единой консоли управления защитой конечных точек, серверов

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

1.2. Консоль управления и обработка собранных данных должна быть реализована в облаке производителя решения

1.3. Наличие ролевого доступа к консоли управления с возможностью гранулированного делегирования прав доступа

1.4. Поддержка двухфакторной аутентификации для учетных записей пользователей консоли управления

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

1.6. Наличие гибкого механизма поиска по всем разделам консоли для ускорения операций анализа, реагирования и тиража (приоритетизации) инцидентов и/или маркеров

1.7. Возможность назначения политик на группы конечных устройств

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

1.8.1. Тип ОС

1.8.2. Сетевые параметры системы

1.8.3. Рабочая станция/Сервер

1.8.4. Статус защиты

1.8.5. Версия клиентского модуля

1.9. Решение должно иметь единый пользовательский интерфейс для всех функций администрирования – все операции по анализу инцидентов и реагирование на них должны осуществляться в пределах одной консоли

1.10. Консоль управления не должна иметь ограничения по количеству администраторов/аналитиков

1.11. Консоль управления должна поддерживать аудиты следующих типов:

1.11.1. Аудит хостов

1.11.2. Аудит действий пользователя

1.11.3. Аудит подключений по API

1.11.4. Аудит политик

1.11.5. Аудит Real Time Response

1.11.6. Аудит исключений файлов

1.12. Консоль должна поддерживать возможность управления развернутыми модулями на конечных точках без необходимости использования VPN или других средств доступа к корпоративной сети (защита систем, находящихся за пределами корпоративного периметра)

1.13. Консоль должна поддерживать совместную работу над инцидентами для команды аналитиков с возможностью делегации инцидентов и изменения их статуса

1.14. Консоль управления должна обеспечивать отображение инцидентов в четырех основных формах с возможностью немедленного переключения между ними:

1.14.1. Общая информация по каждому хосту

1.14.2. Табличная с отображением вектора атаки

1.14.3. Граф связей с отображением легенды и указанием развития атаки

1.14.4. Временная шкала событий с описание каждого события

1.15. Возможность интуитивного масштабирования графов связей запущенных процессов для облегчения визуализации полученных данных и ускорения принятия решений

1.16. Возможность мгновенного выполнения следующих действий при просмотре данных инцидента:

1.16.1. Интерактивное подключение к системе для выполнения реакций

1.16.2. Сетевая изоляция

1.16.3. Закрепление инцидента за конкретным членом команды

1.16.4. Изменение статуса инцидента

1.16.5. Поиск данных за системой, хэшем, именем процесса

1.17. В консоле управления должен присуствовать дополнительный функционал по автоматизации бизнес процесов WorkFlow

1.18. Модуль WorkFlow должен обладать гибким процессом создания скрипта с возможностью внесения в него изменений на «лету» и готовые шаблоны автоматизации действий

1.19. Консоль управления должна одна для всех нижеперечисленных модулей

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

2. Требования к антивирусному модулю

Количество лицензий не менее 75.

2.1. Развертывание модуля не должно требовать перезагрузки ОС

2.2. При обнаружении угроз модуль не должен использовать базы данных сигнатур

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

2.4. Модуль должен поддерживать защиту от вмешательства и несанкционированной деинсталляции

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

2.6. Решение должно уметь выявлять ранее неизвестное/уникальное вредоносное ПО

2.7. Поддержка интеграции с Microsoft AMSI для улучшенного обнаружения атак с использованием скриптов

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

2.9. Использование облачной базы репутации для анализа файлов и их атрибутов

2.10. Распознавание подозрительных вызовов системных инструментов, используемых для инфицирования систем

2.11. Защита от эксплойтов, защита от манипуляций с памятью процессов

2.12. Защита от кражи учетных данных или манипуляции с учетными записями

2.13. Модуль должен поддерживать возможность отправки файлов в облачную «песочницу» производителя

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

3. Требования к модулю отслеживания поведения и реагирования на угрозы

3.1. Развертывание модуля не должно требовать перезагрузки ОС

3.2. Модуль должен поддерживать защиту от вмешательства и несанкционированной деинсталляции

3.3. В поставляемый модуль должен входить модуль по анализу трафика сети и его анализ (host-based network visibility)

3.4. Сбор метаданных по запущенным процессам, сетевой активности, операциям на файловой системе на конечных точках

3.5. Отслеживание последовательности изменений в системе для выявления аномалий и потенциально вредных операций

3.6. Корреляция запущенных процессов с их владельцами и действиями пользователей

3.7. Использование следующих реакций по реагированию на вмешательство:

3.7.1. Карантин

3.7.2. Удаление файла, каталога

3.7.3. Остановка процесса, дерева процессов

3.7.4. Выполнение команды ОС

3.7.5. Выполнение произвольных скриптов

3.8. Возможность исключения (запрета) передачи конкретных файлов в облако производителя решения по их расположению на файловой системе, с возможностью проверки выбранного шаблона перед применением политики

3.9. Вся телеметрия и метаданные с конечных точек должны обрабатываться только в облаке производителя решения по зашифрованному каналу.

3.10. Система должна поддерживать хранение данных, связанных с инцидентами не менее 90 дней с момента обнаружения

3.11. Система должна поддерживать сохранение данных телеметрии (полный перечень метаданных) за последние 7 дней с момента их передачи в облако производителя с возможностью расширения по требования заказчика или регулируемого органа

3.12. Система должна поддерживать возможность интерактивного выполнения команд и скриптов на конечных точках для нейтрализации угрозы или следов ее пребывания в системе с поддержкой PowerShell, Bash, CMD, BAT с возможностью отслеживания результатов выполнения выбранного скрипта, с возможностью подключения аналитики и графического анализа

3.13. Система должна поддерживать возможность формирования библиотеки часто используемых пользовательских скриптов для ускорения реагирования на инциденты и сохранения избранных (ранее примененных команд)

3.14. Система должна поддерживать возможность сетевой изоляции выбранных систем с возможностью настройки конкретных сетей, которые будут доступны для систем в карантине, кроме консоли производителя

3.15. Системы, для которых применяется сетевая изоляция (так называемый карантин), должны оставаться на связи с консолью управления (облаком производителя решения) для проведения оперативных манипуляций.

3.16. Система должна разрешать проведение корректировки (выполнение команд и скриптов) без необходимости перезагрузки целевой системы

3.17. Модуль должен поддерживать возможность сбора не менее 600 параметров запущенных процессов ОС

3.18. Телеметрия с конечных точек должна индексироваться и поддерживать возможность поиска через поисковые запросы консоли управления

3.19. Телеметрия конечных точек должна иметь возможность экспорта/загрузки

3.20. Возможность создания дампа памяти выбранного процесса

4. Общие требования

4.1. Решение должно поддерживать облачный API для запроса текущего состояния системы, поиска инцидентов, маркеров компрометации, аудита событий и управления политиками

4.2. Облачный API должен поддерживать как возможность считывания данных из системы, так и их записи /модификации

4.3. Облачный API должен поддерживать протокол аутентификации OAuth 2.0

4.4. Возможность управления модулями интеграции с посторонними решениями. Возможность подключения пакетов интеграции непосредственно с облачной консоли управления

4.5. Наличие модуля SIEM и интеграции с SIEM системами

4.6. Наличие утилиты для полного удаления клиентских модулей в случае отсутствия связи с консолью управления или других технических усложнений

4.7. Наличие инструмента, позволяющего передавать накопленные данные за пределы системы в формате JSON для дальнейшего их использования в других модулях защиты

4.8. Система должна поддерживать интерактивную справку по выявленным способам вмешательства и заблокированному поведению

5. Требования к модулю SIEM и SOAR

5.1. Система должна поддерживать возможность облачного развертывания с минимальной зависимостью от локальной инфраструктуры.

5.2. Базовый функционал модуля должен быть включен и работать без дополнительных лицензий

5.3. Поддержка масштабируемости для обработки до 1 петабайта данных в сутки.

5.4. Время развертывания системы не должно превышать 48 часов с момента предоставления доступа.

5.5. Доступ в модуль SIEM должен осуществляться из основной консоли

5.6. Модуль системы должен поддерживать расширение возможностей за счет подключения дополнительных корреляционных правил за счет расширение лицензии

5.7. Модуль системы должен поддерживать сбор данных из различных источников, включая:

5.7.1. Endpoint Detection and Response (EDR),

5.7.2. решения по управлению уязвимостями,

5.7.3. сетевые устройства (IDS/IPS, фаерволы),

5.7.4. облачные платформы (AWS, Azure, Google Cloud),

5.7.5. базы данных и приложения.

5.8. Должна быть возможность обработки данных в форматах JSON, Syslog, CEF и LEEF.

5.9. Система должна обеспечивать централизованное управление потоками данных с поддержкой их нормализации и агрегирования.

5.10. Система должна поддерживать автоматическое выявление аномалий и угроз на основе анализа поведения и искусственного интеллекта (AI).

5.11. Поддержка классификации угроз на основе MITRE ATT&CK с возможностью обновления базы знаний не реже чем раз в 15 минут.

5.12. Возможность предоставления детализированной информации о событиях, включая контекст угрозы, пути распространения и рекомендации по устранению.

5.13. Система должна обеспечивать скорость обработки и поиска данных не менее 10 000 событий в секунду.

5.14. Система должна поддерживать создание автоматических рабочих процессов (playbooks) для обработки инцидентов.

5.15. Возможность автоматического реагирования на события, включая изоляцию устройств, блокировку IP-адресов и обновление политик безопасности.

5.16. Базовый функционал модуля SIEM должен иметь возможность поиска логов от поступающих источников в режиме реального времени

5.17. Базовый функционал модуля SIEM должен иметь возможность создания собственных корреляционных правил

5.18. Функционал SOAR должен входить базовой поставку.

5.19. Архитектура системы должна быть построена на облачной платформе, соответствующей стандартам ISO 27001, SOC 2 и GDPR.

5.20. Система должна обеспечивать доступ через веб-интерфейс с поддержкой MFA (многофакторной аутентификации)

5.21. Система должна поддерживать интеграцию через API с популярными SIEM-платформами (Splunk, QRadar, ArcSight).

5.22. Возможность импорта индикаторов компрометации (IOC) в формате STIX/TAXII.

5.23. Система должна поддерживать экспорт данных в сторонние аналитические инструменты.

5.24. Система должна обеспечивать шифрование данных при передаче и в состоянии покоя.

5.25. Должна быть реализована защита от несанкционированного доступа с использованием ролевой модели управления доступом.

5.26. Поддержка централизованного управления аудитом и ведения логов для всех действий в системе.

5.27. Лицензия должна включать неограниченное количество вызовов API и поддержку всех функций системы без дополнительных затрат.

5.28. Лицензирование должно основываться на объемах обрабатываемых данных, а не на количестве подключенных источников.

5.29. Доступ к модулю должен быть предоставлен на весь период действий лицензий антивирусного модуля и модуля отслеживания поведения и реагирования на угрозы

6. Требования к поддержке операционных систем клиентскими модулями

6.1. Windows

6.1.1. Клиентские – Windows 11, 10, 8.1, 7 SP1.

6.1.2. Серверные – 2008 R2 SP1, 2012 (R2), 2016 (включительно с версией core), 2019 (включительно с версией core), 2022 (включительно с версией core), 2025.

6.2. Mac OS - 10.14.x, 10.15.x и выше

6.3. Linux – Amazon Linux 2, Amazon Linux AMI 2018.03, 2017.09, CentOS 7.x-8.x, RHL 6.x-9.x, RHL CoreOs 4.x, SUSE 12. x, SUSE 15, Ubuntu 16.04/18.04/20.04/22.04/24.04, Oracle 6-9, Debian 9.x-12.x, Alma Linux 8.x-9.x,

6.4. VDI системы – AWS, Azure, GCP

7. Технические требования

7.1. Агент не должен привышать 75 мб на жестком диске.

7.2. Агент не должен привышать объем оперативной памяти в размере 50 мб. В критических ситуациях 70мб.

8. Исполнитель должен обеспечить поставку новых оригинальных лицензий от производителя с уникальным кодом.

9. Услуга требует ежедневного исполнения.

Подписал	Карменова Лэйла Нуралиевна
Дата подписания	28.10.2026