ТЕХНИКАЛЫҚ СИПАТТАМА

1273696 сатып алу бойынша
Төмендету баға ұсыныстарын сұрату тәсілімен

Лот № 1 (35 У, 4591167) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: "Kazakhstan Petrochemical Industries Inc." Жауапкершілігі шектеулі серіктестігі.

Ұйымдастырушы: "Kazakhstan Petrochemical Industries Inc." Жауапкершілігі шектеулі серіктестігі.

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	35 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	Антивирустық бағдарламаға жазылу
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Атырау облысы, г Атырау, трасса Атырау-Доссор, строение 295
Жеткізу шарттары	-
Жеткізу мерзімі	01.2027 бастап 01.2028 дейін (қоса алғанда)
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

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

Соңғы құрылғыларды (компьютерлер мен серверлерді) қауіптерден қорғауға арналған бағдарламалық қамтылымға қойылатын техникалық талаптар

Модуль	Талаптар	Бар болуы

		• Басқару консолін орналастыру тапсырыс берушіден бағдарламалық және аппараттық ресурстар бөлуді талап етпеуге тиіс. • Басқару консолі және жиналған деректерді өңдеу шешім өндірушісінің бұлтында іске асырылуға тиіс. • Қол жеткізу құқықтарын егжей-тегжейлі бөліп беру мүмкіндігімен басқару консоліне рөлдік қол жеткізу көзделуге тиіс. • Басқару консолі пайдаланушыларының есептік жазбалары үшін екі факторлы аутентификацияны қолдау. • Басқару консолі мен соңғы құрылғылардағы модульдер арасындағы деректер алмасу TLS 1.2 көмегімен қорғалуға тиіс.	

- Инциденттерді және/немесе маркерлерді талдау, оларға ден қою және олардың басымдығын айқындау операцияларын жеделдету үшін консольдің барлық бөлімдері бойынша икемді іздеу тетігінің болуы.
- Соңғы құрылғылар топтарына саясаттарды тағайындау мүмкіндігі.
- Консоль соңғы құрылғыларды статикалық түрде де, төмендегі динамикалық өлшемшарттар бойынша да топтастыруға мүмкіндік беруге тиіс:
    - ОЖ түрі
    - Жүйенің желілік параметрлері
- Жұмыс станциясы /сервер
- Қорғаныс күйі
- Клиенттік модуль нұсқасы

	• Шешімде барлық әкімшілендіру функциялары үшін бірыңғай пайдаланушы интерфейсі болуға тиіс. Инциденттерді талдау және оларға ден қою жөніндегі барлық операциялар бір консоль шеңберінде орындалуға тиіс. • Басқару консолінде әкімшілердің /талдаушылардың санына шектеу болмауға тиіс. • Басқару консолі аудиттің мынадай түрлерін қолдауға тиіс: • Хосттар аудиті • Пайдаланушы әрекеттерінің аудиті • API арқылы қосылулар аудиті • Саясаттар аудиті • Real Time Response аудиті • Файлдарға арналған ерекшеліктер аудиті	

Басқару консолі	• Консоль соңғы құрылғыларда орналастырылған модульдерді VPN немесе корпоративтік желіге қол жеткізудің өзге құралдарын пайдаланбай басқару мүмкіндігін қолдауға тиіс (корпоративтік периметрден тыс орналасқан жүйелерді қорғау). • Консоль талдаушылар тобының инциденттермен бірлесіп жұмыс істеуін, инциденттерді басқа талдаушыларға тапсыру және олардың мәртебесін өзгерту мүмкіндігін қолдауға тиіс.	

- Басқару консолі инциденттерді төрт негізгі түрде көрсетуді және олардың арасында дереу ауысу мүмкіндігін қамтамасыз етуге тиіс:

- Әрбір хост бойынша жалпы ақпарат
- Шабуыл векторы көрсетілген кестелік көрініс
- Шартты белгілері және шабуылдың өрбу барысы көрсетілген байланыстар графы
- Әрбір оқиғаның сипаттамасы бар оқиғалар уақыт шкаласы

	• Алынған деректерді көрнекі көрсетуді жеңілдету және шешім қабылдауды жеделдету үшін іске қосылған процестердің байланыстар графтарының масштабын интуитивті түрде өзгерту мүмкіндігі. • Инцидент деректерін қарау кезінде мынадай әрекеттерді дереу орындау мүмкіндігі: • Ден қою әрекеттерін орындау үшін жүйеге интерактивті қосылу • Желілік оқшаулау • Инцидентті топтың нақты мүшесіне бекіту • Инцидент мәртебесін өзгерту • Жүйе, хэш және процесс атауы бойынша деректерді іздеу	

	• Басқару консолінде бизнес-процестерді автоматтандыруға арналған қосымша WorkFlow функционалы болуға тиіс. • WorkFlow модулінде скриптті жасау және оған жұмыс барысында өзгерістер енгізу үшін икемді тетік, сондай-ақ әрекеттерді автоматтандырудың дайын үлгілері болуға тиіс. • Төменде көрсетілген барлық модульдер үшін басқару консолі бірыңғай болуға тиіс. Басқару консоліне қол жеткізу қосылатын модульдердің лицензиялары қолданылатын бүкіл кезеңге берілуге тиіс.	

		• Модульді орналастыру ОЖ-ні қайта жүктеуді талап етпеуге тиіс. • Қауіптерді анықтау кезінде модуль сигнатуралар дерекқорларын пайдаланбауға тиіс. • Соңғы құрылғының 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 етуге тиіс.	

Антивирустық модуль	• Модуль өз жұмысына араласудан және рұқсатсыз жойылудан қорғауды қолдауға тиіс. • Кіріктірілген желіаралық экранды жеке саясаттар арқылы басқару мүмкіндігі (Windows және Mac жүйелері үшін). Бір жерден басқару. • Шешім бұрын белгісіз/бірегей зиянды бағдарламалық қамтылымды анықтай алуға тиіс. • Скрипттер қолданылатын шабуылдарды анықтауды жақсарту үшін Microsoft AMSI-мен интеграцияны қолдау. • Белгісіз немесе қайта қапталған зиянды кодты анықтауды жақсарту үшін машиналық оқыту мүмкіндіктерін пайдалану.	

		• Файлдар мен олардың атрибуттарын талдау үшін бұлттық бедел дерекқорын пайдалану. • Жүйелерді жұқтыру үшін пайдаланылатын жүйелік құралдардың күмәнді шақырылуларын тану. • Эксплойттардан және процестер жадысымен манипуляциялардан қорғау. • Есептік деректердің ұрлануынан немесе есептік жазбалармен манипуляциялардан қорғау. • Модуль файлдарды өндірушінің бұлттық «құмсалғышына» жіберу мүмкіндігін қолдауға тиіс.	

		• Модуль файлдарды өндірушінің бұлттық «құмсалғышына» жіберуді өшіру мүмкіндігін қолдауға тиіс. • Жеткізуші бір күнтізбелік жылға 700 лицензия ұсынуға тиіс.	
		• Модульді орналастыру ОЖ-ні қайта жүктеуді талап етпеуге тиіс. • Модуль өз жұмысына араласудан және рұқсатсыз жойылудан қорғауды қолдауға тиіс. • Жеткізілетін модуль құрамына желілік трафикті талдау модулі кіруге тиіс.	

		• Соңғы құрылғыларда іске қосылған процестер, желілік белсенділік және файлдық жүйедегі операциялар туралы метадеректерді жинау. • Аномалиялар мен ықтимал зиянды операцияларды анықтау үшін жүйедегі өзгерістердің реттілігін қадағалау. • Іске қосылған процестерді олардың иелерімен және пайдаланушы әрекеттерімен корреляциялау. • Жүйеге араласуға ден қою үшін мынадай әрекеттерді қолдану:	

	• Карантинге орналастыру • Файлды, каталогті жою • Процесті, процестер ағашын тоқтату • ОЖ пәрменін орындау • Еркін скрипттерді орындау • Нақты файлдардың файлдық жүйеде орналасқан жері бойынша оларды шешім өндірушісінің бұлтына жіберуге тыйым салу мүмкіндігі. Саясатты қолданар алдында таңдалған үлгіні тексеру мүмкіндігі көзделуге тиіс. • Соңғы құрылғылардан алынатын барлық телеметрия мен метадеректер шифрланған арна арқылы беріліп, тек шешім өндірушісінің бұлтында өңделуге тиіс.	

		• Жүйе инциденттерге қатысты деректерді инцидент анықталған сәттен бастап кемінде 90 күн сақтауды қолдауға тиіс. • Жүйе телеметрия деректерін (метадеректердің толық тізбесін) өндірушінің бұлтына берілген сәттен бастап соңғы 7 күн үшін сақтауды қолдауға тиіс. Тапсырыс берушінің немесе реттеуші органның талабы бойынша сақтау мерзімін ұзарту мүмкіндігі көзделуге тиіс.	

Мінез-құлықты қадағалау және қауіптерге ден қою модулі	• Жүйе қауіпті немесе оның жүйеде болу іздерін жою үшін соңғы құрылғыларда пәрмендер мен скрипттерді интерактивті орындау мүмкіндігін қолдауға тиіс. PowerShell, Bash, CMD, BAT қолдауы, таңдалған скрипттің орындалу нәтижелерін қадағалау, сондай-ақ аналитика мен графикалық талдауды қосу мүмкіндігі көзделуге тиіс.	

		• Жүйе инциденттерге ден қоюды жеделдету үшін жиі қолданылатын пайдаланушы скрипттерінің кітапханасын қалыптастыру және таңдаулы пәрмендерді (бұрын қолданылған пәрмендерді) сақтау мүмкіндігін қолдауға тиіс. • Жүйе таңдалған жүйелерді желілік оқшаулау мүмкіндігін қолдауға тиіс. Карантиндегі жүйелерге өндіруші консолінен басқа қолжетімді болатын нақты желілерді баптау мүмкіндігі көзделуге тиіс.	

		• Желілік оқшаулау (карантин) қолданылатын жүйелер жедел әрекеттерді орындау үшін басқару консолімен (шешім өндірушісінің бұлтымен) байланыста қалуға тиіс. • Жүйе нысаналы жүйені қайта жүктемей түзету әрекеттерін (пәрмендер мен скрипттерді орындауды) жүргізуге мүмкіндік беруге тиіс. • Модуль ОЖ-де іске қосылған процестердің кемінде 600 параметрін жинау мүмкіндігін қолдауға тиіс.	

		• Соңғы құрылғылардан алынатын телеметрия индекстелуге және басқару консолінің іздеу сұраулары арқылы іздеу мүмкіндігін қолдауға тиіс. • Соңғы құрылғылардың телеметриясын экспорттау/жүктеу мүмкіндігі болуға тиіс. • Таңдалған процестің жады дампын жасау мүмкіндігі.	
		• Шешім соңғы 5 жыл ішінде Gartner Magic Quadrant for Endpoint Protection Platforms есебінің көшбасшылар квадрантында болуға тиіс.	

		• Шешімде соңғы 3 жыл үшін MITRE ATT&CK® evaluation бағалауына сәйкестігін растау болуға тиіс. • Шешім жүйенің ағымдағы күйін сұрату, инциденттерді және компрометация маркерлерін іздеу, оқиғалар аудитін жүргізу және саясаттарды басқару үшін бұлттық API-ді қолдауға тиіс. • Бұлттық API жүйеден деректерді оқуды да, оларды жазуды /өзгертуді де қолдауға тиіс. • Бұлттық API OAuth 2.0 аутентификация хаттамасын қолдауға тиіс.	

Жалпы талаптар	• Үшінші тарап шешімдерімен интеграция модульдерін басқару мүмкіндігі. Интеграция пакеттерін тікелей бұлттық басқару консолінен қосу мүмкіндігі. • SIEM модулінің және SIEM жүйелерімен интеграцияның болуы. • Басқару консолімен байланыс болмаған немесе өзге техникалық қиындықтар туындаған жағдайда клиенттік модульдерді толық жоюға арналған утилитаның болуы. • Жиналған деректерді басқа қорғау модульдерінде одан әрі пайдалану үшін жүйеден тыс JSON форматында беруге мүмкіндік беретін құралдың болуы.	

	• Жүйе анықталған араласу тәсілдері мен бұғатталған мінез-құлық бойынша интерактивті анықтаманы қолдауға тиіс.	
	• Жүйе жергілікті инфрақұрылымға барынша аз тәуелді бола отырып, бұлтта орналастыру мүмкіндігін қолдауға тиіс. • Модульдің базалық функционалы жеткізілім құрамына енгізілуге және қосымша лицензияларсыз жұмыс істеуге тиіс. • Тәулігіне 1 петабайтқа дейінгі деректерді өңдеу үшін масштабтау мүмкіндігін қолдау.	

		• Жүйені орналастыру уақыты қол жеткізу берілген сәттен бастап 48 сағаттан аспауға тиіс. • SIEM модуліне қол жеткізу негізгі консольден жүзеге асырылуға тиіс. • Жүйе модулі лицензияны кеңейту арқылы қосымша корреляциялық ережелерді қосып, өз мүмкіндіктерін кеңейтуді қолдауға тиіс. • Жүйе модулі әртүрлі көздерден, оның ішінде төмендегілерден деректер жинауды қолдауға тиіс: • Соңғы құрылғылардағы қауіптерді анықтау және оларға ден қою жүйелері (Endpoint Detection and Response, EDR), • осалдықтарды басқару шешімдері,	

		• желілік құрылғылар (IDS /IPS, желіаралық экрандар), • бұлттық платформалар (AWS, Azure, Google Cloud), • дерекқорлар мен қолданбалар. • JSON, Syslog, CEF және LEEF форматтарындағы деректерді өңдеу мүмкіндігі болуға тиіс. • Жүйе деректер ағындарын қалыпқа келтіру мен біріктіруді қолдай отырып, оларды орталықтандырылған басқаруды қамтамасыз етуге тиіс. • Жүйе мінез-құлықты талдау және жасанды интеллект (AI) негізінде аномалиялар мен қауіптерді автоматты түрде анықтауды қолдауға тиіс.	

		• Білім базасын кемінде әр 15 минут сайын жаңарту мүмкіндігімен MITRE ATT&CK негізінде қауіптерді жіктеуді қолдау. • Оқиғалар туралы егжей-тегжейлі ақпаратты, оның ішінде қауіптің мәнмәтінін, таралу жолдарын және жою жөніндегі ұсынымдарды ұсыну мүмкіндігі. • Жүйе деректерді өңдеу және іздеу жылдамдығын секундына кемінде 10 000 оқиға деңгейінде қамтамасыз етуге тиіс. • Жүйе инциденттерді өңдеуге арналған автоматты жұмыс процестерін (playbooks) жасауды қолдауға тиіс.	

SIEM және SOAR модулі	• Құрылғыларды оқшаулауды, IP-мекенжайларды бұғаттауды және қауіпсіздік саясаттарын жаңартуды қоса алғанда, оқиғаларға автоматты түрде ден қою мүмкіндігі. • SIEM модулінің базалық функционалы қосылған көздерден келіп түсетін журнал жазбаларын нақты уақыт режимінде іздеу мүмкіндігін қамтамасыз етуге тиіс. • SIEM модулінің базалық функционалы пайдаланушының өз корреляциялық ережелерін жасау мүмкіндігін қамтамасыз етуге тиіс. • SOAR функционалы базалық жеткізілім құрамына кіруге тиіс.	

		• Жүйе архитектурасы ISO 27001, SOC 2 және GDPR стандарттарына сәйкес келетін бұлттық платформа негізінде құрылуға тиіс. • Жүйе MFA (көп факторлы аутентификация) қолдауымен веб-интерфейс арқылы қол жеткізуді қамтамасыз етуге тиіс. • Жүйе танымал SIEM платформаларымен (Splunk, QRadar, ArcSight) API арқылы интеграцияны қолдауға тиіс. • STIX/TAXII форматында компрометация индикаторларын (IOC) импорттау мүмкіндігі.	

		• Жүйе деректерді үшінші тараптың талдау құралдарына экспорттауды қолдауға тиіс. • Жүйе деректерді беру және сақтау кезінде шифрлауды қамтамасыз етуге тиіс. • Қол жеткізуді басқарудың рөлдік моделін пайдалана отырып, рұқсатсыз қол жеткізуден қорғау іске асырылуға тиіс. • Жүйедегі барлық әрекеттер бойынша аудитті орталықтандырылған басқаруды және журналдарды жүргізуді қолдау.	

		• Лицензиялау API шақыруларының шектеусіз санын және қосымша шығындарсыз жүйенің барлық функцияларын қолдауды қамтуға тиіс. • Лицензиялау қосылған көздердің санына емес, өңделетін деректер көлеміне негізделуге тиіс. • Модульге қол жеткізу антивирустық модульдің және мінез-құлықты қадағалау мен қауіптерге ден қою модулінің лицензиялары қолданылатын бүкіл кезеңге берілуге тиіс.	

Клиенттік модульдердің ОЖ-лерді қолдауы	• Windows • Клиенттік ОЖ-лер – Windows 11, 10, 8.1, 7 SP1. • Серверлік ОЖ-лер – 2008 R2 SP1, 2012 (R2), 2016 (Core нұсқасын қоса алғанда), 2019 (Core нұсқасын қоса алғанда), • 2022 (Core нұсқасын қоса алғанда Mac OS – 10.14.x, 10.15.x және одан жоғары). • 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.x, Oracle 6–9, Debian 9.x–11.x, Alma Linux 8.x–9.x,	

	• VDI жүйелері – AWS, Azure, GCP • Лицензиялар 1 жылға жарамды.	
Техникалық талаптар	Агенттің қатты дискіде алатын көлемі 75 МБ-тан аспауға тиіс. Агент пайдаланатын жедел жад көлемі қалыпты жұмыс режимінде 50 МБ-тан, ал ең жоғары жүктеме кезінде 70 МБ-тан аспауға тиіс.	

Қол қойған Соловьев Сергей Юрьевич
Қол қойылған күні 26.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1273696
способом Запрос ценовых предложений на понижение

Лот № 1 (35 У, 4591167) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Kazakhstan Petrochemical Industries Inc." /"Казахстан Петрокемикал Индастриз Инк."/

Организатор: Товарищество с ограниченной ответственностью "Kazakhstan Petrochemical Industries Inc." /" Казахстан Петрокемикал Индастриз Инк."/

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	35 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Подписка на Антивирусное ПО
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Атырауская область, г Атырау, трасса Атырау-Доссор, строение 295
Условия поставки	-
Срок поставки	с 01.2027 по 01.2028 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

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

Модуль	Требования	Наличие

		• Развертывание консоли управления не должно требовать от заказчика выделения программных и аппаратных ресурсов • Консоль управления и обработка собранных данных должна быть реализована в облаке производителя решения • Наличие ролевого доступа к консоли управления с возможностью гранулированного делегирования прав доступа • Поддержка двухфакторной аутентификации для учетных записей пользователей консоли управления	

		• Обмен данными между консолью управления и модулями на конечных точках должен быть защищен с помощью TLS 1.2 • Наличие гибкого механизма поиска по всем разделам консоли для ускорения операций анализа, реагирования и тиража (приоритетизации) инцидентов и/или маркеров • Возможность назначения политик на группы конечных устройств • Консоль должна позволять объединять конечные устройства как в статическом порядке, так и по динамическим критериям, среди которых: • • Тип ОС • Сетевые параметры системы	

		• Рабочая станция /Сервер • Статус защиты • Версия клиентского модуля • Решение должно иметь единый пользовательский интерфейс для всех функций администрирования – все операции по анализу инцидентов и реагирование на них должны осуществляться в пределах одной консоли • Консоль управления не должна иметь ограничения по количеству администраторов /аналитиков • Консоль управления должна поддерживать аудиты следующих типов:	

	• Аудит хостов • Аудит действий пользователя • Аудит подключений по API • Аудит политик • Аудит Real Time Response • Аудит исключений файлов	
Консоль управления	• Консоль должна поддерживать возможность управления развернутыми модулями на конечных точках без необходимости использования VPN или других средств доступа к корпоративной сети (защита систем, находящихся за пределами корпоративного периметра)	

		• Консоль должна поддерживать совместную работу над инцидентами для команды аналитиков с возможностью делегации инцидентов и изменения их статуса • Консоль управления должна обеспечивать отображение инцидентов в четырех основных формах с возможностью немедленного переключения между ними: • Общая информация по каждому хосту • Табличная с отображением вектора атаки • Граф связей с отображением легенды и указанием развития атаки • Временная шкала событий с описание каждого события	

	• Возможность интуитивного масштабирования графов связей запущенных процессов для облегчения визуали зации полученных данных и ускорения принятия решений • Возможность мгновенного выполнения следующих действий при просмотре данных инцидента: • Интерактивное подключение к системе для выполнения реакций • Сетевая изоляция • Закрепление инцидента за конкретным членом команды • Изменение статуса инцидента • Поиск данных за системой, хэшем, именем процесса	

		• В консоле управления должен присуствовать дополнительный функционал по автоматизации бизнес процесов WorkFlow. • Модуль WorkFlow должен обладать гибким процессом создания скрипта с возможностью внесения в него изменений на «лету» и готовые шаблоны автоматизации действий. • Консоль управления должна одна для всех нижеперечисленных модулей	

	Доступ в консоль управления должен быть предоставлен на весь период действий лицензий подключаемых модулей	
	• Развертывание модуля не должно требовать перезагрузки ОС • При обнаружении угроз модуль не должен использовать базы данных сигнатур	

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

Антивирусный модуль	• Возможность управления встроенным брандмауэром с помощью отдельных политик (для Windows, Mac систем). Управление с одного места. • Решение должно уметь выявлять ранее неизвестное /уникальное вредоносное ПО • Поддержка интеграции с Microsoft AMSI для улучшенного обнаружения атак с использованием скриптов • Использование возможностей машинного обучения для улучшения обнаружения неизвестного или перепакованного вредоносного кода • Использование облачной базы репутации для анализа файлов и их атрибутов

		• Распознавание подозрительных вызовов системных инструментов, используемых для инфицирования систем • Защита от эксплойтов, защита от манипуляций с памятью процессов • Защита от кражи учетных данных или манипуляции с учетными записями • Модуль должен поддерживать возможность отправки файлов в облачную «песочницу» производителя • Модуль должен поддерживать возможность деактивации отправки файлов в облачную «песочницу» производителя • Поставщик должен предоставить 700 лицензий на один календарный год.	

		• Развертывание модуля не должно требовать перезагрузки ОС • Модуль должен поддерживать защиту от вмешательства и несанкционированной деинсталляции • В поставляемый модуль должен входить модуль по анализу трафика сети и его анализ • Сбор метаданных по запущенным процессам, сетевой активности, операциям на файловой системе на конечных точках • Отслеживание последовательности изменений в системе для выявления аномалий и потенциально вредных операций • Корреляция запущенных процессов с их владельцами и действиями пользователей	

- Использование следующих реакций по реагированию на вмешательство:

- Карантин
- Удаление файла, каталога
- Остановка процесса, дерева процессов
- Выполнение команды ОС
- Выполнение произвольных скриптов

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

		• Вся телеметрия и метаданные с конечных точек должны обрабатываться только в облаке производителя решения по зашифрованному каналу. • Система должна поддерживать хранение данных, связанных с инцидентами не менее 90 дней с момента обнаружения • Система должна поддерживать сохранение данных телеметрии (полный перечень метаданных) за последние 7 дней с момента их передачи в облако производителя с возможностью расширения по требования заказчика или регулируемого органа	

Модуль отслеживания поведения и реагирования на угрозы	• Система должна поддерживать возможность интерактивного выполнения команд и скриптов на конечных точках для нейтрализации угрозы или следов ее пребывания в системе с поддержкой PowerShell, Bash, CMD, BAT с возможностью отслеживания результатов выполнения выбранного скрипта, с возможностью подключения аналитики и графического анализа • Система должна поддерживать возможность формирования библиотеки часто используемых пользовательских скриптов для ускорения реагирования на инциденты и сохранения избранных (ранее примененных команд)	

		• Система должна поддерживать возможность сетевой изоляции выбранных систем с возможностью настройки конкретных сетей, которые будут доступны для систем в карантине, кроме консоли производителя • Системы, для которых применяется сетевая изоляция (так называемый карантин), должны оставаться на связи с консолью управления (облаком производителя решения) для проведения оперативных манипуляций. • Система должна разрешать проведение корректировки (выполнение команд и скриптов) без необходимости перезагрузки целевой системы	

		• Модуль должен поддерживать возможность сбора не менее 600 параметров запущенных процессов ОС • Телеметрия с конечных точек должна индексироваться и поддерживать возможность поиска через поисковые запросы консоли управления • Телеметрия конечных точек должна иметь возможность экспорта/загрузки • Возможность создания дампа памяти выбранного процесса	

		• Решение должно быть в квадранте лидеров отчета Gartner Magic Quadrant for Endpoint Protection Platforms за последние 5 лет • Решение должно иметь подтверждение соответствия MITRE ATT&CK® evaluation за последние 3 года • Решение должно поддерживать облачный API для запроса текущего состояния системы, поиска инцидентов, маркеров компрометации, аудита событий и управления политиками • Облачный API должен поддерживать как возможность считывания данных из системы, так и их записи /модификации	

Общие требования	• Облачный API должен поддерживать протокол аутентификации OAuth 2.0 • Возможность управления модулями интеграции с посторонними решениями. Возможность подключения пакетов интеграции непосредственно с облачной консоли управления • Наличие модуля SIEM и интеграции с SIEM системами • Наличие утилиты для полного удаления клиентских модулей в случае отсутствия связи с консолью управления или других технических усложнений	

	• Наличие инструмента, позволяющего передавать накопленные данные за пределы системы в формате JSON для дальнейшего их использования в других модулях защиты. • Система должна поддерживать интерактивную справку по выявленным способам вмешательства и заблокированному поведению.	
	• Система должна поддерживать возможность облачного развертывания с минимальной зависимостью от локальной инфраструктуры.	

		• Базовый функционал модуля должен быть включен и работать без дополнительных лицензий • Поддержка масштабируемости для обработки до 1 петабайта данных в сутки. • Время развертывания системы не должно превышать 48 часов с момента предоставления доступа. • Доступ в модуль SIEM должен осуществляться из основной консоли • Модуль системы должен поддерживать расширение возможностей за счет подключения дополнительных корреляционных правил за счет расширение лицензии	

		• Модуль системы должен поддерживать сбор данных из различных источников, включая: • Endpoint Detection and Response (EDR), • решения по управлению уязвимостями, • сетевые устройства (IDS/IPS, фаерволы), • облачные платформы (AWS, Azure, Google Cloud), • базы данных и приложения. • Должна быть возможность обработки данных в форматах JSON, Syslog, CEF и LEEF. • Система должна обеспечивать централизованное управление потоками данных с поддержкой их нормализации и агрегирования.	

		• Система должна поддерживать автоматическое выявление аномалий и угроз на основе анализа поведения и искусственного интеллекта (AI). • Поддержка классификации угроз на основе MITRE ATT&CK с возможностью обновления базы знаний не реже чем раз в 15 минут. • Возможность предоставления детализированной информации о событиях, включая контекст угрозы, пути распространения и рекомендации по устранению. • Система должна обеспечивать скорость обработки и поиска данных не менее 10 000 событий в секунду.	

Модуль SIEM и SOAR	• Система должна поддерживать создание автоматических рабочих процессов (playbooks) для обработки инцидентов. • Возможность автоматического реагирования на события, включая изоляцию устройств, блокировку IP-адресов и обновление политик безопасности. • Базовый функционал модуля SIEM должен иметь возможность поиска логов от поступающих источников в режиме реального времени • Базовый функционал модуля SIEM должен иметь возможность создания собственных корреляционных правил

		• Функционал SOAR должен входить базовой поставку. • Архитектура системы должна быть построена на облачной платформе, соответствующей стандартам ISO 27001, SOC 2 и GDPR. • Система должна обеспечивать доступ через веб-интерфейс с поддержкой MFA (многофакторной аутентификации) • Система должна поддерживать интеграцию через API с популярными SIEM-платформами (Splunk, QRadar, ArcSight). • Возможность импорта индикаторов компрометации (IOC) в формате STIX/TAXII.	

		• Система должна поддерживать экспорт данных в сторонние аналитические инструменты. • • Система должна обеспечивать шифрование данных при передаче и в состоянии покоя. • Должна быть реализована защита от несанкционированного доступа с использованием ролевой модели управления доступом. • Поддержка централизованного управления аудитом и ведения логов для всех действий в системе.	

		• Лицензирование должна включать неограниченное количество вызовов API и поддержку всех функций системы без дополнительных затрат. • Лицензирование должно основываться на объемах обрабатываемых данных, а не на количестве подключенных источников. • Доступ к модулю должен быть предоставлен на весь период действий лицензий антивирусного модуля и модуля отслеживания поведения и реагирования на угрозы	

Поддержка ОС клиентскими модулями	• Windows • • Клиентские – Windows 11, 10, 8.1, 7 SP1. • Серверные – 2008 R2 SP1, 2012 (R2), 2016 (включительно с версией core), 2019 (включительно с версией core), 2022 (включительно с версией) • coreMac OS - 10.14.x, 10.15. x и выше • 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.x, Oracle 6-9, Debian 9.x-11.x, Alma Linux 8.x-9.x,	

	• VDI системы – AWS, Azure, GCP • Срок действия лицензий - 1 год.	
Технические Требования	Агент не должен превышать 75 мб на жестком диске. Объем оперативной памяти, используемой агентом, не должен превышать 50 МБ в штатном режиме работы и 70 МБ при пиковых нагрузках.	

Подписал Соловьев Сергей Юрьевич
Дата подписания 26.11.2026