БЕКІТЕМІН
Қазақстан Республикасының
Мәдениет және ақпарат
вице-министрі
_____ Е. Тоқтағұлов
«__» _____ 2026 жыл

Конкурстық құжаттамаға 16-қосымша

«Құжаттардың бірыңғай электрондық архиві» ақпараттық жүйесі үшін ақпараттық қауіпсіздіктің жедел орталығының қызметтеріне арналған Техникалық ерекшелік

Тапсырыс берушінің атауы	«Қазақстан Республикасының Мәдениет және ақпарат министрлігі» мемлекеттік мекемесі
Ұйымдастырушының атауы	«Қазақстан Республикасының Мәдениет және ақпарат министрлігі» мемлекеттік мекемесі
Конкурстың №	-
Конкурстың атауы	«Құжаттардың бірыңғай электрондық архиві» ақпараттық жүйесі үшін ақпараттық қауіпсіздіктің жедел орталығының қызметтері
Лоттың №	-
Лоттың атауы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы	801019.000.000010

Қызметтің атауы:	«Құжаттардың бірыңғай электрондық архиві» ақпараттық жүйесі үшін ақпараттық қауіпсіздіктің жедел орталығының қызметтері
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есепке алмағандағы бірлік бағасы	-
Қосылған құн салығын есепке алмағанда, сатып алу үшін бөлінген жалпы сома	-
Қызмет көрсету мерзімі	Шарт күшіне енген күннен бастап 2027 жылғы 31 желтоқсанды қоса алғанда, бірақ кемінде 15 күнтізбелік күннен кем болмауы тиіс.
Аванстық төлем мөлшері	-
Кепілдік мерзімі (айлармен)	12 ай

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы:	**1. Жалпы талаптар** 1.1. Сатып алынатын қызметтердің атауы: «Құжаттардың бірыңғай электрондық архиві» ақпараттық жүйесі үшін ақпараттық қауіпсіздіктің жедел орталығының қызметтері (бұдан әрі - АҚЖО) 1.2. Сатып алу нысанасы ақпараттық қауіпсіздіктің жедел орталығының (АҚЖО) қызметтері болып табылады, олар ақпараттық қауіпсіздік инциденттерін мониторингтеу, талдау және оларға ден қоюды қамтамасыз етуге бағытталған. Жабдықты, бағдарламалық қамтамасыз етуді және лицензияларды жеткізу көрсетілген қызметтерді көрсету үшін қажетті көлемде ғана жүзеге асырылады және сатып алудың негізгі нысанасына — АҚЖО қызметтерін көрсетуге қатысты қосалқы сипатта болады. 1.3. Қызмет көрсету орны: «Қазақстан Республикасының Мәдениет және ақпарат министрлігі» мемлекеттік мекемесі, Астана қаласы, «Есіл» ауданы, Мәңгілік Ел даңғылы 8, 14 кіреберіс 1.4. Сатып алынатын қызметтердің сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары:

1.4. **Негізгі терминдер мен анықтамалар:**

– **АҚ** – ақпараттық қауіпсіздік.

– **SIEM** (Security Information and Event Management) – қауіпсіздік оқиғалары туралы ақпаратты жинауға және талдауға арналған бағдарламалық өнімдердің сыныбы.

– **АТ** – ақпараттық технологиялар.

– **ITIL** – АТ-мен байланысты бизнес-үдерістерді басқару, баптау және үздіксіз дұрыстау әдіснамасы.

– **SLA** – қызмет көрсету деңгейі туралы келісім.

– **FQDN** – толық домендік атау.

– **Байланыстылық** – компьютерлер арасындағы өзара әрекеттесу мүмкіндігі.

– **АЖ** – ақпараттық жүйе.

– **VPN** – виртуалды жеке желі.

– **АҚҰҰО** – «Мемлекеттік техникалық қызмет» АҚ Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы.

– **Оқиға** – стандартты қызметтердің бір бөлігі болып табылмайтын және қызметтер сапасының үзілуіне немесе төмендеуіне әкелуі мүмкін кез келген оқиға.

▪ **ТЕ** – техникалық ерекшелік.

Қызметтер көрсету Тапсырыс берушінің АТ-инфрақұрылымының АҚ-ның қазіргі заманғы қатерлерінен қорғалу деңгейін арттыруға, сондай-ақ ақ АҚ оқиғаларының туындау тәуекелдерін барынша азайту бойынша алдын алу шараларын жүргізуге бағытталған.

Қызметтер көрсету шеңберінде мынадай міндеттер шешілуі тиіс:

• Тапсырыс берушінің инфрақұрылымында Қызметтер компоненттерін өрістетуді қоса алғанда, оқиғалар мониторингін және АҚ оқиғаларын өңдеуді ұйымдастыру және жүзеге асыру.

Осы техникалық ерекшелік (бұдан әрі – ТЕ) жоғарыда көрсетілген міндеттерді шешуді қамтамасыз ететін Қызметтерді көрсетуге қойылатын жалпы және жеке талаптарды қамтиды.

Ақпарат таралып кететін техникалық арналарды және арнайы техникалық құралдарды ақпараттық қауіпсіздіктің жедел орталығымен анықтау бойынша көрсетілетін қызметтер, оның ішінде:

- қосылатын оқиға көздерінің жиынтық саны 50-ден (елуден) аспайтын оқиғалар мен желілік ағындар коллекторларын (LOG/FLOW Collector) ұсыну;

Өнім беруші АҚЖО-ның техникалық құралдарын жеткізуді, орнатуды, қосуды және баптауды жеткізу мен енгізудің нақты көлемін ескере отырып, 15 күнтізбелік күн ішінде, бірақ Мемлекеттік сатып алуды жүзеге асыру қағидаларының 569-тармағында белгіленген ең төменгі мерзім өткеннен ерте емес жүзеге асырады.

Орнату, қосу және баптау фактісі Тапсырыс беруші мен Өнім беруші қол қойған жазбаша актімен ресімделеді.

1.5. Тапсырыс беруші осы ТЕ-нің 3.6-тармағында белгіленген мерзімде қажетті ресурстарды ұсынады және көздердің қосылуын қамтамасыз етеді.

2. Қызметтерге қойылатын талаптар

2.1. Қызметтер көрсету шеңберінде мынадай функциялар мен қосымша сервистер қолжетімді болады:

1) Өнім берушінің SIEM жүйесіне қосылған Тапсырыс берушінің серверлік жабдықтарында және желілік құрылғыларында тіркелген АҚ оқиғаларын мониторингілеу;

2) Мониторинг аймағында АҚ оқиғаларын анықтау;

3) Тапсырыс берушіні анықталған оқиғалар, оларға ден қою әдістері туралы хабардар ету, сондай-ақ оларды жою жөнінде ұсынымдар беру;

4) Оқиғаларға ден қою үдерісінде сараптамалық қолдау көрсету;

5) Тапсырыс берушінің АТ-инфрақұрылымын осалдықтардың бар-жоғына сканерлеу — айына кемінде 1 (бір) рет (кемінде 512 бірегей IP-мекенжай);

6) Тапсырыс берушінің өтінімі бойынша Қызметтер көрсету мерзімі ішінде 2 (екі) рет Тапсырыс берушінің АТ-инфрақұрылымына енуге тестілеу және оның қорғалуын талдау (кемінде 128 бірегей IP-мекенжай);

7) АҚ сыни оқиғаларын тексеру кезінде кеңес беру;

8) Ақпараттық қауіпсіздік талаптарына сәйкестікті растау сынақтарынан өту бойынша көмек көрсету және консультациялар ұсыну;

9) «Құжаттардың бірыңғай электрондық архиві» АЖ үшін ақпараттық қауіпсіздіктің жедел орталығы қызметін көрсету шеңберінде ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарға сәйкестігіне ақпараттық қауіпсіздік аудитін жүргізу (шарттың қолданылу мерзімі ішінде 1 (бір) рет), жазбаша есеп пен ұсынымдар ұсыну;

10) Мониторинг аймағына кірмейтін жүйелерге қатысты күдікті оқиғалар анықталған жағдайда, одан әрі тергеп-тексеруді Тапсырыс беруші дербес жүзеге асырады. Өнім беруші қажет болған жағдайда сындылық дәрежесін айқындау үшін Тапсырыс берушіге консультация береді, мәселенің көзін анықтау мақсатында қосымша талдау жүргізеді және Тапсырыс берушінің мамандарына инцидентті жоюға жәрдемдеседі;

11) Есептік деректерді орталықтандырылған сақтауды, қол жеткізу құқықтарының аражігін ажыратуды, артықшылықты сеанстарды басқаруды, сеанстарды жазуды және пайдаланушылардың әрекеттерін журналға тіркеуді қамтамасыз ететін артықшылықты қол жеткізуді басқару және мониторингтеу сервисі (3 (үш) пайдаланушыға);

2.2. Кеңейтілген сараптама

Тапсырыс берушінің сұрау салуы бойынша ТЕ-ке 6-қосымшаға сәйкес мониторинг аймағының қосымша кеңейтілген сараптамасы ұсынылуы мүмкін.

2.3. Қызметтер осы техникалық ерекшелікке сәйкес ақпараттық қауіпсіздік инциденттерін мониторингтеу мен оларға ден қоюдың мынадай құралдарын пайдалана отырып көрсетіледі::

- ақпараттық қауіпсіздік оқиғаларын басқару жүйесі (SIEM);
- басқару және артықшылықты қолжетімділік мониторингі сервисі;
- осалдықтар сканері (Vulnerability Scanner).

2.4. Ұсынылатын қаражат шарттың қолданылу мерзіміне шешімдерді өндірушілердің техникалық қолдауымен сүйемелденуі тиіс, бұл тапсырыс берушіге ұсынылатын веб-ресурстарға (бар болса) сілтемелері бар өндірушінің немесе оның ресми өкілінің (дистрибьютордың) ресми хатымен расталуы тиіс.

2.5. Қызметтер көрсету шеңберінде туындауы мүмкін оқиғалар шегінің деңгейі.

Әрбір АҚ оқиғасы үшін техникалық ерекшелікке осы ТЕ-ке № 2 қосымшаға сәйкес басымдық белгіленеді. АҚ оқиғаларына ден қою техникалық ерекшелікке осы ТЕ-ке № 3 қосымшада келтірілген уақытша сипаттамалармен айқындалған мерзімде жүзеге асырылады.

3. Өнім беруші міндетті:

3.1. Төмендегіні қоса алғанда, Тапсырыс беруші толтырған сауалнама парағының негізінде қосылатын ақпараттық жүйелер (АЖ) бөлігінде Тапсырыс берушінің АТ-инфрақұрылымына талдау (зерттеу) жүргізу:

1) ақпараттық қауіпсіздік оқиғаларының қосылатын көздерінің (бұдан әрі - көздер) құрамы бойынша ұсынымдар беру;
2) Өнім берушінің білім базасына сәйкес стандартты және стандартты емес көздерді типтеу;
3) Тапсырыс берушінің шабуылдарды анықтаудың қолданыстағы сценарийлерін қосуға және жаңа сценарийлерін әзірлеуге қажеттілігін айқындау;
4) талап етілетін лицензиялардың көлемін анықтау.

Осы кезеңде мынадай мәліметтер жинақталуы тиіс:

1) көздің атауы;
2) көздің функционалын сипаттау (АЖ-ге қатыстылығы);
3) орналастыру алаңы;
4) өндіруші/марка/модель;
5) ОЖ түрі/нұсқасы;
6) БЖ түрі/нұсқасы;
7) FQDN;
8) IP-мекенжай.

3.2. Осы техникалық ерекшелікке сәйкес ұйымдастырушылық-техникалық шешімдер айқындалуы және әзірленуі тиіс:

1) Қызметтер көрсетудің нысаналы архитектурасы;
2) файлдық сақтау орындарының сыйымдылығын есептеуді қоса алғанда, Тапсырыс беруші бөлетін есептеу ресурстарына қойылатын техникалық ерекшеліктер мен талаптар;
3) Қызметтер компоненттерін өрістету тәртібі, оның ішінде Тапсырыс берушінің алаңында;
4) Тапсырыс беруші мен киберқатерлерге мониторинг және ден қою орталығының алаңында Қызметтер құрауыштарының желіаралық өзара іс-қимылының тәртібі мен ұйымдастырылуы.

	3.3. Өнім беруші көздерді қосуды орындауы керек: 1) Тапсырыс беруші мен Өнім берушінің алаңы арасында келісілген параметрлер бойынша Өнім берушінің жабдығында қорғалған VPN-қосылуды (бұдан әрі - VPN-қосылыс) ұйымдастыру. Бөлінген алаңдар арасында L3 байланысы болмаған жағдайда олардың әрқайсысымен VPN-қосылыстарды орнатуды қамтамасыз ету қажет; 2) SIEM-жүйе компоненттерін орнатуды жүргізу. Қажет болған жағдайда Тапсырыс берушіге есептеу ресурстарына, сақтаудың кіші жүйелеріне қойылатын талаптарды және Қызметтердің қосымша компоненттерін орнату үшін конфигурациялау жөніндегі ұсынымдарды ұсыну; 3) Тапсырыс берушінің АТ-инфрақұрылымына SIEM конфигурациялауды және бейіндеуді орындау, бұл ақпараттық қауіпсіздіктің бұзушылықтары мен оқиғаларын анықтау сценарийлерінің жұмыс қабілеттілігіне кепілдік береді; 4) көздерді ақпараттық қауіпсіздік оқиғаларын мониторингілеу және талдау сервисіне қосу жөніндегі нұсқаулықтарды жіберу; 5) стандартты емес көздер үшін 3 (үш) жеке адаптерге дейін әзірлеу; 6) Тапсырыс берушінің Өнім берушімен келісілген ерекше сұрау салулары негізінде оқиғалар мен корреляция қағидаларының санаттарын кеңейтуді қоса алғанда, шабуылдарды анықтаудың жаңа сценарийлерін әзірлеу; 7) осы техникалық ерекшелікке сәйкес SIEM-жүйесінің компоненттері, көздер мен өнім берушінің алаңы арасындағы желілік байланысты тексеруді жүргізу. **3.4.** Мониторинг және киберқатерлерге ден қою орталығының базасында Өнім беруші міндетті: 1) барлық түрлі оқиға көздерінен келіп түсетін бірыңғай «кіру нүктесі» болып табылатын кезекші ауысымның бірінші желісі талдаушыларының күшімен 24/7 режимінде ақпараттық қауіпсіздік оқиғаларын талдауды қамтамасыз етуге. Бірінші желінің талдаушылары ақпараттық қауіпсіздік оқиғаларын өңдеуді, жалған іске қосылуларды бастапқы тексеруді, бастапқы талдау жүргізуді және оқыс оқиғалар санаттары мен қағидалар негізінде ақпараттық қауіпсіздік оқиғаларын бөліп көрсетуді, ITIL стандарттарына сәйкес (санаттау, басымдық беру, SLA) оқиғаларды тіркеуді және кейіннен сүйемелдеуді қамтамасыз етуге тиіс; 2) Тапсырыс берушінің алаңында да, Өнім берушінің алаңында да орнатылған SIEM-жүйе компоненттерінің жай-күйінің мониторингі; 3) VPN-арнасының жай-күйіне мониторинг жүргізу; 4) 8/5 режимінде екінші желі талдаушыларының күшімен оқиғаларды өңдеу бойынша ұсынымдар беру, сондай-ақ ақпараттық қауіпсіздіктің типтік оқиғаларын шешу. Осы үрдіс шеңберінде мамандандырылған құралдарды пайдалана отырып тереңдетілген талдау жүргізу, сондай-ақ Тапсырыс берушінің инфрақұрылымындағы өзгерістерге сәйкес корреляция қағидаларын бейімдеу қамтамасыз етілуге тиіс. Қажет болған жағдайда, Тапсырыс берушінің сұрау салуы бойынша корреляция қағидаларына ерекшеліктер қосу;

5) үшінші сараптамалық желінің күшімен сыни деңгейдегі оқиғаларды тергеп-тексеруді жүргізу, расталған оқиғаларды жою жөнінде ұсынымдар беру, сондай-ақ ретроспективті талдау жүргізу және релевантты қауіп-қатерлер мен шабуылдар, оларды анықтау және қарсы іс-қимыл тәсілдері туралы ақпаратты өзектендіру;

6) Киберқауіпсіздік инциденттері мен қатерлерін сараптау, техникалық тергеп-тексеру;

7) Киберқауіпсіздік инциденттері мен қатерлеріне сараптама жүргізу, техникалық тергеп-тексеру;

8) Киберқауіпсіздік қатерлерін мониторингтеу, талдау және болжау;

9) Киберқауіпсіздік инциденттерінің салдарын оқшаулау және бейтараптандыру;

10) Тапсырыс берушінің инфрақұрылымында оқиға анықталған жағдайда, оқиға туралы ақпаратты АҚҰҰО-ға беруді қамтамасыз етуге;

11) әрбір анықталған ақпараттық қауіпсіздік оқиғасы бойынша бір байланыс арнасы бойынша есептілікті ұсыну: электрондық пошта, телефон қоңырауы.

3.5. Тапсырыс берушіге ден қою және ақпараттық қауіпсіздік оқиғаларын басқару жүйелерінің интерфейсіне қол жеткізуді ұсыну қамтамасыз етілуі тиіс. Жеке кабинеттің функционалы мыналарды қамтуы тиіс:

1) оқиғалардың мәртебесі бойынша өзекті ақпаратқа қол жеткізу;
2) оқиғаларды дербес тіркеу мүмкіндігі;
3) орын алған оқиғалар бойынша статистиканы қарау;
4) әрбір анықталған оқиға бойынша есептілік;
5) Өнім берушіден есептер мен хабарламалар алу.

3.6. Тапсырыс беруші шарт күшіне енген күннен бастап 14 (он төрт) жұмыс күні ішінде Қызметтерді енгізу үшін Өнім беруші сұратқан қажетті ресурстарды ұсынуға және бөлуге, сондай-ақ көрсетілген мерзімде барлық қажетті көздердің SIEM жүйесіне қосылуын қамтамасыз етуге міндетті.

3.7. Өнім беруші Тапсырыс берушінің көмегімен қызмет көрсету үшін қажетті компоненттер мен Тапсырыс берушінің АТ-инфрақұрылымы арасындағы желілік байланысты ұйымдастыруға міндетті.

3.8. Өнім беруші Тапсырыс берушімен келісілген параметрлер бойынша Тапсырыс берушінің алаңы мен Өнім берушінің алаңы арасында Тапсырыс берушінің жабдығында қорғалған VPN-қосылысын ұйымдастыруға тиіс.

3.9. Өнім беруші ай сайын, есепті айдан кейінгі айдың 3 (үшінші) күнінен кешіктірмей, ал желтоқсан айының есебін 2027 жылғы 20 желтоқсаннан кешіктірмей Тапсырыс берушіге жабдық орналастырылған әрбір алаң бойынша көрсетілген Қызметтер туралы егжей-тегжейлі есептерді ілеспе хатпен бірге, Тапсырыс берушінің кеңсесінде міндетті түрде тіркей отырып ұсынуға міндетті.

4. Өнім беруші мен Тапсырыс берушінің өзара әрекеттесуі

4.1. АҚ қамтамасыз ету мәселелері бойынша Өнім беруші мен Тапсырыс беруші арасындағы өзара әрекеттесу тәртібін белгілейтін және АҚ оқиғаларын анықтауға және оларға ден қоюға байланысты рәсімдерді сипаттайтын Регламент әзірленеді.

4.2. Өнім беруші мен Тапсырыс берушінің мониторинг орталығының өзара әрекеттесуі:

1) көрсетілетін қызметтердің талап етілетін сапа параметрлеріне сәйкес келмеуіне өтінімдерді тіркеу;

2) сервисті қалпына келтіру үрдісін ұйымдастыру;

3) екі тараптың жауапты басшыларын қызметтердің талап етілетін сапасын қалпына келтіруге байланысты мәселелерді шешу барысы туралы өзара хабардар ету.

4.3. Өнім беруші тәулігіне 24 сағат, аптасына 7 күн қызмет көрсетуге міндетті.

4.4. АҚЖО қызметін көрсету кезеңінде Өнім беруші мен Тапсырыс беруші арасындағы жауапкершілік аймақтарының аражігін ажырату техникалық ерешелікке осы ТЕ-ке №5 қосымшада көрсетілген.

4.5. Оқиғаларды анықтау кезіндегі Тараптардың өзара әрекеттесу рәсімі

Оқиғаны Тапсырыс беруші анықтаған жағдайда, ол регламентте көрсетілген Өнім берушінің техникалық қызметінің байланыс деректері бойынша Өнім берушіні хабардар етеді. Өнім беруші оқиғаны тіркейді және Тапсырыс берушіге мынадай деректерді хабарлайды:

1) тіркелген оқиғаның нөмірі;

2) тіркеу уақыты;

3) тақырып (қысқаша сипаттама);

4) оқиға туралы ақпарат;

5) оны жою жөніндегі ұсынымдар.

4.6. Тапсырыс берушіден оқиға туралы хабарлама Өнім берушіге электрондық пошта арқылы жіберіледі.

АҚ оқиғасына ден қою деп оқиғаның тетіктерін анықтауға, зиянды барынша азайтуға және оқиғаның болашақта қайталануын болдырмауға бағытталған іс-қимылдардың құрылымдалған жинағы түсініледі. АҚ оқиғаларын анықтау және оларға ден қою жөніндегі іс-қимылдар, сондай-ақ олардың реттілігі техникалық ерекшелікке осы ТЕ-ке № 1 қосымшада берілген.

4.7. Тапсырыс берушінің өтініштерін тіркеу кезінде Тараптардың өзара әрекеттесу рәсімі

Тапсырыс берушіге техникалық ерекшелікке осы ТЕ-ке № 4 қосымшада көрсетілген көрсеткіштерге сәйкес сұрау салуларды жіберу мүмкіндігі беріледі. Бұл үшін Тапсырыс берушінің уәкілетті өкілі хат тақырыбында сәйкестендіргішті көрсете отырып, Өнім берушінің электрондық мекенжайына мынадай пішімде сұрау салу жіберуі тиіс:

1) Хат тақырыбы: сәйкестендіргіш (сервис-менеджер ұсынады), сұраудың қысқаша мәні.

2) Хат денесі: сұрау салудың егжей-тегжейлі сипаттамасы, сұрау салудың басымдығын көрсету.

5. Қызметтерді тиісінше көрсету шарттары

5.1. Қызметтер көрсетуде үзілістерге әкеп соққан оқиғалар мен басқа да мән-жайлар үшін, егер олар мынадай себептердің бірінен туындаса, Өнім беруші жауапты болмайды:

1) Тапсырыс берушіні алдын ала хабардар ете отырып, Қызметтер көрсетуге қатысатын жабдықта жоспарлы немесе апаттық жөндеу жұмыстарын жүргізу;
2) Тапсырыс берушінің сұрауы бойынша Тапсырыс беруші немесе Өнім беруші жүргізетін Қызметтерді көрсетуге қатысатын жабдықтардағы жұмыстар;
3) Ешқандай оқыс оқиғалар анықталмаған жағдайда Тапсырыс берушінің сұрау салуы бойынша Қызметтерді тестілік көрсету;
4) Тапсырыс берушінің Қызметтер көрсету деңгейінде белгіленген мерзімде Өнім берушіге оқиғаларды анықтауға және жоюға жәрдемдесуді қамтамасыз етуден бас тартуы немесе қабілетсіздігі;
5) Тапсырыс берушінің регламент талаптарына сәйкес қызмет көрсету шеңберінде бағдарламалық жасақтаманы немесе жабдықты баптау үшін қажетті деректерді 5 (бес) жұмыс күнінен аспайтын мерзімде ұсынудан бас тартуы немесе қабілетсіздігі;
6) Өнім берушіні хабардар етпей, Тапсырыс берушінің қорғалатын ресурстардың құрамына және конфигурациясына олардың уақытша қол жетімсіздігіне және соның салдарынан Қызметтер көрсетудегі үзіліске әкелуі мүмкін өзгерістер енгізу жөніндегі жұмыстарды жүргізуі;
7) Тапсырыс берушінің бағдарламалық және/немесе бағдарламалық-аппараттық жасақтамасының көрсетілетін Қызметтермен жұмысқа қабілетсіздігі немесе үйлеспеушілігі;
8) Шарттың талаптарына сәйкес еңсерілмейтін күш жағдайларының басталуы.

6. Өнім берушінің құқықтары.

6.1. Өнім беруші шабуылдарды анықтау сценарийін іске асыру үшін Тапсырыс берушіден қажетті ақпаратты (оның ішінде АТ-инфрақұрылымы туралы ақпаратты) сұратуға, сондай-ақ бұл ақпаратты жалған іске қосылуларды барынша азайту мақсатында Шарт бойынша өз міндеттемелерін орындау үшін ғана пайдалануға құқылы.

6.2. Сұрау салу Өнім берушімен қалыптастырылады және Тапсырыс беруші тарапынан уәкілетті тұлғаға электрондық пошта арқылы жіберіледі. Сұрау салуда өтініштің себебі көрсетілуге тиіс. Тапсырыс беруші осы сұрау салу бойынша кері байланысты 3 (үш) жұмыс күні ішінде беруге міндетті, қажет болған жағдайда мерзім тараптардың келісімі бойынша түзетілуі мүмкін.

Сұратылған ақпараттың мысалдары мыналарды қамтуы мүмкін, бірақ олармен шектелмейді:
1) DNS-серверлер тізімі;
2) қауіпсіздік сканерлерінің IP-мекенжайлары;
3) интернет желісінен қол жетімді ресурстар тізімі;
4) Тапсырыс берушіге тиесілі жаһандық IP-мекенжайлар тізімі;
5) ақпараттық жүйелер әкімшілерінің есептік жазбаларының тізімі;
6) ақпараттық жүйелер мен ресурстардың иелері туралы ақпаратты;
7) IP-мекенжайдың пайдаланушыға немесе жүйеге тиесілігі туралы деректер.

Ақпарат Тапсырыс берушінің Қызметтерді қосу және Тапсырыс берушінің уәкілетті өкілдерімен сұхбат жүргізу үшін тиісті сауалнама парақтарын толтыру жолымен ұсынылады.

7. Өнім берушінің жабдықтарына жоспарлы техникалық қызмет көрсету

7.1. Өнім беруші Қызметтер көрсетілетін кіші жүйелерге жоспарлы техникалық қызмет көрсетуді немесе жетілдіруді жүргізуге құқылы. Бұл жұмыстар жоспарлы жөндеу жұмыстары болып саналады және Қызметтер көрсетуде үзілістерге әкелуі мүмкін. Жоспарлы жөндеу жұмыстары 19:00-ден 08:00-ге дейінгі аралықта (Астана қаласының уақыты) не Тапсырыс берушімен келісілген басқа уақытта Қызметтер көрсетуде ықтимал үзіліспен жүргізіледі.

7.2. Өнім беруші Тапсырыс берушіні жұмыстар басталғанға дейін 1 (бір) жұмыс күнінен кешіктірмей Қызметтер көрсетуде үзілістер тудыруы мүмкін жоспарлы жөндеу жұмыстарын жүргізу туралы хабардар етуге міндеттенеді. Жұмыстар Тапсырыс берушінің сұрауы бойынша орындалатын жағдайлар, сондай-ақ егер жоспарлы жөндеу жұмыстары Қазақстан Республикасының мемлекеттік органдарының немесе құзыретті телекоммуникациялық органдарының талабы бойынша жүргізілсе, Өнім беруші көрсетілген мерзімде хабарлай алмайтын жағдайлар бұған жатпайды.

7.3. Тапсырыс беруші қажет болған жағдайда техникалық мүмкіндік болған кезде Өнім беруші ескеретін жұмыстарды жүргізу мерзімдерін түзету жөнінде ұсыныстар жібере алады. Өнім беруші жіберген хабарламада мынадай ақпарат көрсетіледі:

жоспарлы жөндеу жұмыстарын жүргізу уақыты;

1) жұмыстарды жүргізу күні;
2) жұмыстың ұзақтығы;
3) жұмыстар туралы ақпарат беретін жауапты тұлғаның байланыс деректері;
4) Тапсырыс беруші қызметкерлерінің жұмыстарға, мысалы, Тапсырыс берушінің ақпараттық жүйелерінің жұмысқа қабілеттілігіне тексеру жүргізу үшін қатысу қажеттілігі.

7.4. Тапсырыс беруші жұмыстарға қатысу үшін жауапты қызметкерлер бөлуге міндеттенеді. Қызметкерді көрсетілген мерзімде тарту мүмкін болмаған жағдайда, Тапсырыс беруші жұмыстарды жүргізу мерзімдерін түзету жөнінде ұсыныстар жібереді.

7.5. Егер жоспарлы жұмыстар тоқтатылса, Өнім беруші Тапсырыс берушіні шешім қабылданғаннан кейін қысқа мерзімде хабардар етеді.

7.6. Тапсырыс беруші, сондай-ақ, егер бұл жұмыстар қорғалатын ресурстардың уақытша қол жетімсіздігіне және соның салдарынан Қызметтер көрсетудегі үзіліске әкеп соғуы мүмкін болса, Өнім берушіні ол өз жабдығында жоспарлы жұмыстар жүргізілетіні туралы хабардар етуге міндетті. Хабарлама жұмыс басталғанға дейін 1 (бір) жұмыс күнінен кешіктірілмей жіберілуге тиіс.

Тапсырыс берушінің хабарламасында келесі ақпарат көрсетілуі тиіс:

1) жоспарлы жұмыстарды жүргізу уақыты мен күні;
2) жұмыстың ұзақтығы;
3) жұмыстар туралы ақпарат беретін жауапты тұлғаның байланыс деректері.

7.7. Жоспарлы жұмыстарды жүргізу мерзімдері өзгерген жағдайда Тапсырыс беруші Өнім берушіні қысқа мерзімде, бірақ жұмыс басталғанға дейін 1 (бір) жұмыс күнінен кешіктірмей хабардар етуге міндетті. Жоспарлы жұмыстарды тоқтату кезінде Тапсырыс беруші Өнім берушіні қысқа мерзімде хабардар етуге міндетті.

7.8. Тапсырыс берушіден немесе Өнім берушіден барлық хабарламалар регламентте көрсетілген уәкілетті өкілдердің электрондық мекенжайларына жіберілуі тиіс.

8. Өнім берушінің жабдықтарындағы апаттық жөндеу жұмыстары

8.1. Базасында Қызметтер көрсетілетін кіші жүйелердің апаттық жөндеу жұмыстары Қызметтер көрсетуде кезеңдік үзілістер немесе болашақта апаттық жағдайға әкеп соғуы мүмкін сапа параметрлерінің едәуір нашарлауы тіркелген жағдайларда жүргізіледі.

8.2. Өнім беруші Тапсырыс берушіні апаттық жөндеу жұмыстарын жүргізу туралы олар басталғанға дейін кемінде 4 (төрт) сағат бұрын хабардар етуге міндетті.

8.3. Тапсырыс беруші, өз кезегінде, егер олар қорғалатын ресурстардың уақытша қол жетімсіздігіне және соның салдарынан Қызметтер көрсетудегі үзіліске әкеп соғуы мүмкін болса, Өнім берушіні өз жабдығында апаттық жөндеу жұмыстарын жүргізу туралы хабардар етуге міндетті. Хабарлама жұмыс басталғанға дейін кемінде 2 (екі) сағат бұрын жіберілуге тиіс.

8.4. Хабарламалар осы техникалық регламентте көрсетілген уәкілетті өкілдердің электрондық мекенжайларына жіберіледі. Хабарламада мыналар көрсетілуі тиіс:

1) апаттық жөндеу жұмыстарының уақыты, күні және ұзақтығы;
2) жүргізілетін жұмыстар туралы ақпарат беретін жауапты тұлғаның байланыс деректері;
3) Тапсырыс беруші қызметкерлерінің апаттық жөндеу жұмыстарына қатысу қажеттілігі туралы ақпарат (егер жұмыстарды Өнім беруші жүргізсе).

9. Тапсырыс берушіде бар зиянды немесе күдікті объектілерді талдау:

9.1. Зерттеу объектісі: бір күдікті файл. Құрамдас файлдарды (архивтерді) талдау жағдайында жалпы архив емес, архив құрамына кіретін әрбір жеке файл зерттеу объектісі болып табылады. Егер құрамдас орындалатын файлдар (өздігінен ашылатын архивтер, инсталляторлар) талданса, зерттеу объектісі осы архивтердің немесе инсталляторлардың функционалы (сценарийі) болып табылады. Егер алынған файлдардың функционалын зерттеу қажет болса, олардың әрқайсысы жеке зерттеу объектісі ретінде қарастырылады.

9.2. Зерттеу көлемі: Тапсырыс берушінің талабы бойынша.

	9.3. Зерттеулерді жүргізудің негізгі ықтимал кезеңдері (кезеңдер олардың орындылығына, қолданылуына қарай, файлдың пішімімен құрылымын, сондай-ақ зерттеу міндеттерін шешу қажеттілігін ескере отырып жүргізіледі. Бұл нақты файлды талдау кезінде барлық көрсетілген кезеңдер орындалмауы мүмкін, бірақ зерттеу мақсаттарына қол жеткізуге мүмкіндік беретін кезеңдер орындалуы тиіс дегенді білдіреді: **9.4.** Объектіні базалық статистикалық зерттеу: 1) Файл пішімі мен өлшемін анықтау; 2) Хэш-сомаларды есептеу (MD5, SHA-256); 3) Цифрлық қолтаңбаның болуын айқындау; 4) Файлдағы жолдарды алу және талдау; 5) Файлды компиляциялау құралдарын сәйкестендіру; 6) Импортталған функцияларды, секцияларды, компиляция уақытын және басқа да уақыт белгілерін қоса алғанда, файл тақырыбын талдау (егер мұндай деректер бар болса). **9.5.** Ашық көздер бойынша деректерді іздеу: 1) Google.com және Virustotal.com көмегімен объектіні сәйкестендіретін хэш-сомаларды іздеу (Тапсырыс берушінің келісімі бойынша объектіні ресурсқа жүктеумен немесе жүктеусіз); 2) Google.com және басқа да сервистерді пайдалана отырып, объектіде қамтылған ерекше жолдарды іздеу. Мұндай жолдардың тізімін зерттеу объектісінің ерекшеліктеріне байланысты талдаушы таңдайды. **9.6.** Тереңдетілген статикалық және қажет болған жағдайда динамикалық талдау: 1) Талдау объектісінің дизассемблирленген, декомпилирленген немесе өзге де қолжетімді кодын зерттеу (файл пішіміне байланысты); 2) Қажет болған жағдайда және техникалық мүмкіндік болған кезде - объектіні оқшауланған виртуалды ортада, интернетке қол жеткізумен немесе қол жеткізусіз дұрыстауды жүргізу (Тапсырыс берушінің келісімі бойынша). **9.7.** Компрометация сәйкестендіргіштерін бөлу (зиянды функционал анықталған жағдайда): 1) Жинақталған ақпаратты құрылымдау және зерттелетін объект жұққан жүйеде анықталуы мүмкін индикаторлардың мынадай ықтимал топтарын бөліп анықтау: мьютекстердің, файлдардың, тізілім кілттерінің, процестердің атаулары, IP-мекенжайлар, домендік атаулар, есептік деректер, зиянды БҚ жасайтын пайдаланушылардың аттары мен құпия сөздері. **9.8.** Зерттелетін объектінің функционалдық сипаттамасы: 1) Объектіні оның таралу мүмкіндіктері мен орындайтын функциялары бойынша жіктеу (мысалы: троян, құрт, вирус, бэкдор, тиегіш және т.б.). Зиянды функционал анықталған жағдайда бұл сипатталады немесе егер зерттеу оның бар екенін растамаса, оның жоқтығы көрсетіледі. **9.9.** Объектіні бейтараптандыру үшін ұсынымдар дайындау: 1) Егер объектіде зиянды функционал болса, объектінің жұқтыруын анықтау, оны бейтараптандыру және жүйелерді (жұмыс станцияларын, серверлерді немесе басқа жабдықтарды) қалпына келтіру үшін ұсынымдар қалыптастыру. Егер зиянды функционал анықталмаса, бұл да көрсетіледі.

10. Желілер арасындағы экранға қойылатын техникалық талаптар

Құрылғылар саны – 1 дана.

- Next Generation Firewall (NGFW) функционалы;
- Қолданбаларды бақылау және веб-трафикті сүзгілеу (Application Control & URL Filtering);
- Шешім Ену әрекеттерінің алдын алу жүйесінің (IPS) функционалын қамтамасыз етуі тиіс;
- IPS жүйесі төмендегі механизмдер негізінде қауіптерді анықтауды қамтамасыз етуі керек:
- Белгілі шабуылдар мен эксплойттарды анықтау үшін сигнатуралық талдау (Signature Analysis);
- Стандартқа сай емес немесе зиянды трафикті анықтау үшін протоколдар аномалияларын бақылау және талдау (Protocol Anomaly Analysis);
- Қолданбалардың қажетсіз белсенділігін бақылау және бұғаттау үшін қолданба басқаруы (Application Control);
- Бұрын белгісіз шабуылдар мен аномалды әрекеттерді анықтау үшін мінез-құлық талдауына негізделген анықтау (Behavior Analysis);
- Қауіптерді проактивті анықтау мүмкіндігі бар антивирустық қорғау (Antivirus);
- Антивирустық шешім зиянды веб-сайттарға қолжетімділікті болдырмауы, сондай-ақ кіріс зиянды файлдарды анықтап, бұғаттауы тиіс (Anti-virus);
- Боттар мен зиянды бағдарламалардан қорғау (Anti-Bot);
- Anti-Bot қосымшасы бірнеше деңгейлі анықтау механизмін қолдануы тиіс, оған IP, URL және DNS мекенжайларының беделі, байланыс протоколдарының үлгілері бойынша боттарды анықтау, сондай-ақ DNS хаттамасындағы шабуылдардан автоматты қорғауға арналған зерделі аналитика механизмдері, соның ішінде DGA-дан қорғау тетіктері кіреді;
- Электрондық поштаны спамнан қорғау (Anti-Spam) зияткерлік талдау негізінде;
- Оқшауланған ортада орындалуын эмуляциялау мүмкіндігімен файлдарды талдау және нөлдік күн қатерлерін анықтауға арналған песочница (sandbox) функционалы;
- Қауіпсіздік шлюзі қосылыстардың күйін бақылау үшін трафиктің егжей-тегжейлі талдауы және қолданбалар жағдайын пайдаланып желілік ағындарды басқаруды қамтамасыз етуі тиіс;
- Шешім DHCP сервері және ретранслятор (relay) режимдерінде жұмыс істеуді қолдауы тиіс;
- Шешім Transparent (Bridge) режимінде жұмыс істеу мүмкіндігін қолдауы тиіс;
- Жергілікті желіге қолжетімділікті шектеу үшін MAC мекенжайларының ақ тізіміне негізделген саясатты қолдау;
- QoS механизмдеріне негізделген саясатты қолдау;
- Белгілі бір IP-дереккөз, IP-мекенжай немесе сервис үшін өткізу қабілетін шектеу немесе кепілдендіру, сондай-ақ кідірістерді басқару мүмкіндігі;

	– VPN-трафик үшін QoS ережелерін икемді баптау мүмкіндігі, оның ішінде артықшылықтарды, өткізу қабілетінің шектеуін немесе кепілдендірілуін орнату; – Шешім веб-қолданбаларды зиянды кодтар мен шабуылдардан қорғау үшін кіріктірілген ену әрекеттерінің алдын алу жүйесінің (IPS) функционалын қамтамасыз етуі тиіс. Жүйе желілік червьтерді, буферді толтыру шабуылдарын, SQL-инъекцияларды, командалық инъекцияларды, сайт аралық скриптингті (XSS) бұғаттауы, сондай-ақ HTTP-червьтерін бұғаттауға арналған баптауға болатын модульді қолдауы тиіс. Сонымен қатар, жүйе каталогтарды айналып өту (Directory Traversal), зиянды немесе дұрыс емес HTTP тақырыптарын (Header Rejection), сондай-ақ зиянды HTTP кодтарын қорғауды қамтамасыз етуі керек; – Шешім HTTP/3 over QUIC протоколын қолдауы тиіс; – Лицензия бар жағдайда құмсалғыш (Sandboxing) функционалы (бұлтта немесе жергілікті бөлінген құрылғыда инспекция) қамтамасыз етілуі тиіс; – Шешім пайдаланушыларды сәйкестендіру және бақылау (Identification & User Control) функционалын қамтамасыз етуі тиіс; – Райдаланушылар идентификаторларын Microsoft Active Directory қауіпсіздік оқиғаларын талдау арқылы алу мүмкіндігі; – Домен құрамына кірмейтін құрылғылар мен пайдаланушылар үшін браузер арқылы идентификатор бойынша аутентификацияны қолдау; – Пайдаланушылар компьютерлеріне саясат бойынша орнатылатын және идентификаторларды қауіпсіздік шлюзіне жіберетін арнайы агент болуы тиіс; – Кіріктірілген VPN қолдауы (Site-to-Site VPN, Remote Access VPN); – Райдаланушыларды Active Directory, RADIUS, LDAP арқылы аутентификациялау; – IP/MAC-мекенжай бойынша пайдаланушыларды аутентификациялау және икемді қауіпсіздік ережелерін қолдау; – Қазақстан Республикасының ақпаратты қорғау саласындағы заңнамасының талаптарына сәйкес келетін заманауи криптографиялық шифрлау және аутентификациялау алгоритмдерін қолдау; – Шешім кемінде келесі Diffie-Hellman топтарын қолдауы тиіс: Топ 1 (768 бит), Топ 2 (1024 бит), Топ 5 (1536 бит), Топ 14 (2048 бит), Топ 19 және Топ 20; – Шешім кіріктірілген сертификаттау орталығын (CA) да, сыртқы үшінші тарап сертификаттау орталықтарын да қолдануды қолдауы тиіс; – Шешім кемінде келесі деректер тұтастығын қамтамасыз ету механизмдерін қолдауы тиіс: MD5, SHA-1, SHA-256, SHA-512 және AES-XCBC алгоритмдерін пайдалану; – Құзыреттерді тиімді бөлу үшін рөлдік қолжетімділікті басқару (RBAC) қолдауы; – Шешім екі факторлы аутентификацияны қамтамасыз етуі тиіс, соның ішінде сыртқы екі факторлы аутентификация жүйелерімен интеграция арқылы немесе өндірушінің кіріктірілген механизмі арқылы;

	– Пайдаланушылар, топтар, IP-мекенжайлар, қолданбалар, қолданба санаттары және басқа параметрлер бойынша қауіпсіздік саясаттарын баптау мүмкіндігі; – Саясаттарды кесте бойынша белсендіру мүмкіндігі, оның ішінде уақыттық шектеулер мен қолжетімділік шарттары; – Қауіпсіздік саясаты бұзылған кезде автоматты түрде есептерді қалыптастыру; – Қолданбаларды басқару дерекқоры кемінде 10 000 белгілі қолданбаны қамтуы тиіс; – Шешім кемінде 250000 Web 2.0 виджетіне егжей-тегжейлі қауіпсіздік бақылауын қамтамасыз етуі тиіс; – Сыртқы интеграциясыз кіріктірілген екі факторлы аутентификация жүйесі;; – 200 миллионнан астам URL-ді қамтитын URL-категоризацияны қамтамасыз ету; – Лицензия бар жағдайда құмсалғыш (Sandboxing) функционалы (инспекция – бұлтта немесе жергілікті бөлінген құрылғыда). Желілік функциялар және істен шығуға төзімділік – Жүктемені басымдыққа қарай интеллектуалды басқару үшін SD-WAN қолдауы (SD-WAN); – Жүктемені теңгеру үшін өткізу қабілетін басқару (Traffic Shaping); – Сыртқы телеметрия және осалдық мониторинг жүйелерімен интеграция; – Маршрутизация протоколдарын қолдау: OSPFv2, BGPv4, RIP, PIM (SM, DM, SSM), IGMP; – IPv6 және dual-stack туннелдеу IPv4-over-IPv6 қолдауы; – Ақау кезінде автоматты ауысу мүмкіндігі бар Active/Passive кластерлеу; – Бұлттық портал арқылы орталықтандырылған басқару; – Сыртқы интеграциясыз кіріктірілген екі факторлы аутентификация жүйесі; – Желілік қосылыстарды егжей-тегжейлі визуализациялау және пайдаланушылардың аномалды әрекеттерін талдау мүмкіндігі.. Өнімділік – NGFW өткізу қабілеті: кемінде 1,2 Gbps; – Threat Prevention (Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot және бұлттық Sandbox функционалы қосылғанда): кемінде 750 Mbps; – IPS өткізу қабілеті: кемінде 1,7 Gbps; – Firewall өткізу қабілеті: кемінде 2,2 Gbps; – VPN AES-128 өткізу қабілеті: кемінде 1,4 Gbps; – Жаңа қосылыстарды орнату жылдамдығы: кемінде 16 000 қосылыс/сек; – Бір мезгілдегі максималды қосылыстар саны: кемінде 1 000 000; – Процессор және желілік интерфейстер жүктемесін кеңейтілген мониторингтеу мүмкіндігі; – Өндірушінің қолдауы/жазылымы 12 айға ұсынылады және актімен расталатын лицензияны белсендіру/пайдалануға енгізу күнінен бастап есептеледі. 12 айлық кепілдік мерзімі жабдықты/БҚ-ны

пайдалануға енгізу (қабылдау) актісіне қол қойылған күннен бастап есептеледі. Жеткізілген жабдық/БҚ бойынша кепілдік міндеттемелер/қолдау қызметтер көрсету мерзімі аяқталған кезде тоқтатылмайды және кепілдік кезеңі ішінде қолданылады.

Аппараттық сипаттамалар

- WAN порты: кемінде 1× 10/100/1000Base-T RJ-45;
- LAN порттары: кемінде 6× 10/100/1000Base-T RJ-45;
- Консоль порты: кемінде 1× USB-C;
- USB порттары: кемінде 2× USB 3.0;
- Жұмыс температурасының диапазоны: 0°C-тан 40°C-қа дейін

Қосымша талаптар

- Мобильді қосымша арқылы басқаруды қолдау;
- Саясаттарды орталықтандырылған басқару мүмкіндігі;
- Жылдам енгізу (Zero Touch Deployment) қолдауы;
- Нақты уақыт режимінде есеп беру және лог жүргізу мүмкіндігі;
- Бір интерфейс арқылы бірнеше қауіпсіздік шлюзін басқару мүмкіндігі;
- Қауіпсіздік сертификаттауларын қолдау: CB 62368-1, UL 62368-1, FCC IC Class B, CE, VCCI, RoHS, REACH, WEEE;
- Осы Техникалық ерекшелікте көрсетілген жабдықтар, бағдарламалық қамтамасыз ету және лицензиялар жеткізуші тарапынан тек АҚЖО қызметтерін көрсету мақсатында жеткізіледі және өздігінен сатып алу нысаны болып табылмайды. Көрсетілген элементтердің құны қызметтердің құнына кіреді және бөлек есептелмейді.

11. EDR класты бағдарламалық қамтамасыз етуге қойылатын талаптар

EDR (Endpoint Detection and Response) ақпараттық қауіпсіздік құралдарына лицензия талаптары бағдарламалық қамтамасыз ету Қазақстан Республикасы Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 2026 жылғы 2 маусымдағы № 279/НҚ бұйрығына сәйкес, сенімді бағдарламалық қамтамасыз ету және электрондық өнеркәсіп өнімдері тізіліміне енгізілуі тиіс.

Жалпы (жүйелік) талаптар:

11.1. Архитектура талаптары

11.1.1. Орталықтандырылған архитектура:

Жүйе біртұтас деректер өңдеу орталығында орналастырылған.

Барлық деректерді өңдеу және басқару орталықтандырылған түрде жүзеге асырылады.

11.1.2. Істен шығуға төзімділік және деректерді сақтық көшірмелеу:

Деректерді сақтық көшірмелеу және автоматты қалпына келтіруді қолдау.

Жоғары қолжетімділікті қамтамасыз ету үшін түйіндерді баптау.

	11.1.3. Деректер қауіпсіздігі: Деректерді тасымалдау кезінде (TLS 1.2/1.3) және сақтау кезінде шифрлау. Рөлдік қолжетімділікті басқару (RBAC) негізінде қолжетімділікті бақылау. 11.1.4. Өнімділік және жүктеме: Үлкен көлемдегі телеметрияны нақты уақыт режимінде өңдеу. Инфрақұрылымға минималды талаптар: процессор – 4 ядродан, ЖЖҚ – 16 ГБ, SSD-дискілер. 11.1.5. Интеграция және үйлесімділік: Стандартты API интерфейстерін қолдау (REST, JSON). SIEM, SOAR және басқа киберқауіпсіздік құралдарымен интеграция. 11.1.6. Мониторинг және басқару: Веб-консоль арқылы орталықтандырылған басқару. Жүйенің күйін нақты уақыт режимінде мониторингтеу. Журнал жүргізу және есеп беру мүмкіндігі. Журналдағы оқиғаларды сүзгілеу, корреляциялау және ақпараттық қауіпсіздік оқиғаларын талдауды қамтамасыз ететін аналитикалық сұраулар тілдерін және іздеу механизмдерін қолдау. Оқиғалар журналынан ақпарат іздеу үшін KQL/ES|QL сұраныс тілін қолдау. Қосымша талаптар - Жүйенің on-premise, қоғамдық бұлттар және гибридті нұсқаларда жұмыс істеу мүмкіндігі. - Локалды және мультиоблачное орналастыруды қолдайтын, ашық деректер схемасы бар масштабталатын іздеу платформасы. - Функционалдық талаптар бір шешім аясында да, бірнеше шешімді біріктіру арқылы да орындалуы мүмкін, бастысы осы Техникалық ерекшеліктегі барлық талаптардың сақталуы. - Сыртқы шешімдермен интеграция модульдерін басқару және консоль арқылы интеграция пакеттерін қосу мүмкіндігі. - Инциденттерді іздеу, талдау, жауап беру және приоритизациялау үшін AI-ассистентті қолдау; ассистент LLM чат-бот түрінде ұсынылуы тиіс. - Соңғы құрылғылар топтарына саясаттар тағайындау мүмкіндігі. - Рөлдік қолжетімділік (RBAC) және консоль операторларының әрекеттерін аудиттеу қолдауы - Консоль аналитиктердің инциденттер бойынша бірлесіп жұмыс жасауын қолдауы, соның ішінде делегирование және статустарды өзгерту мүмкіндігі. - Корпоративтік периметрден тыс жүйелерді қорғау үшін VPNсыз соңғы нүктелерді басқару мүмкіндігі. - Оқиғаларды талдау үшін алдын ала орнатылған және бапталатын дашбордтардың болуы. - Іске қосылған процестер арасындағы байланыстарды масштабталатын визуализациялау. - Шектеусіз әкімшілер санын қолдау.

	- Басқару консолі мен модульдер арасындағы деректер алмасуы TLS 1.2 арқылы жүзеге асуы тиіс. - Өнім отандық өндірістен не өзге өндірістен болуы, тапсырыс берушінің Қазақстан Республикасының аумағында пайдалануына құқық беретін құқық иеленушінің қолданыстағы лицензиясы болуы және Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының талаптарына сәйкес келуі тиіс («Киберқауіпсіздік туралы» Қазақстан Республикасы Заңының 61-бабы 3-тармағының 2) тармақшасы). - Осы Техникалық ерекшелікте көрсетілген жабдықтар, бағдарламалық қамтамасыз ету және лицензиялар жеткізуші тарапынан тек АҚЖО қызметтерін көрсету мақсатында жеткізіледі және өздігінен сатып алу нысаны болып табылмайды. Көрсетілген элементтердің құны қызметтердің құнына кіреді және бөлек есептелмейді. **Функционалды талаптар** **11.2.** Операциялық жүйелерді қолдау 11.2.1.Жұмыс станциялары: -Windows: Windows 10, Windows 11 (x64). -macOS: macOS 11 Big Sur және одан жоғары нұсқалары. - Linux: Ubuntu 18.04 LTS және одан жоғары, Debian 10 және одан жоғары. 11.2.2.Серверлер: -Windows Server 2016, 2019, 2022. - Linux: Red Hat Enterprise Linux 8, CentOS 7.9-2009 және одан жоғары. 11.2.3.Мобильді құрылғылар: - Android: Android 9.0 және одан жоғары нұсқалары. - iOS: iOS 13 және одан жоғары нұсқалары. 11.2.4.Виртуалды орта: -VMware, Hyper-V, KVM-де виртуализацияны қолдау. **11.3.** Сканерлеу түрлері 11.3.1.Қол жетімділікті сканерлеу (On-access): - Файлдарды жасау, ашу, өзгерту немесе орындау кезінде оларды автоматты түрде сканерлеу. 11.3.2.Сұраныс бойынша сканерлеу (d-demand): - Сканерлеуді агент интерфейсі арқылы қолмен іске қосыңыз. 11.3.3.Алынбалы медианы сканерлеу: -Қосылған USB құрылғыларын, сыртқы қатты дискілерді және басқа алынбалы медианы тексеріңіз. 11.3.4.Жоспарлы сканерлеу: - Кесте бойынша реттелетін сканерлеу тапсырмалары (күнделікті, апта сайын, ай сайын). 11.3.5.Жедел жадты сканерлеу: - Жедел жадтағы процестер мен деректерді зиянды бағдарлама белгілерінің бар-жоғын тексеру. 11.3.6.Жүйені терең сканерлеу:

	- Мазмұнын егжей-тегжейлі талдай отырып, бүкіл файлдық жүйені сканерлеу. **11.4**. Сканерленетін Архив форматтары 11.4.1.Қолдау көрсетілетін Архив форматтары: -7zip, ace, arj, bzip2, cab, gz, gzip, jar, rar, tar, tgz, xz, zip, zipx. 11.4.2.Сканерлеу ерекшеліктері: - Ішкі архивтерді ашу. - Көп томдық архивтерді қолдау. - Барлық қолдау көрсетілетін форматтарда зиянды мазмұнды сканерлеу. Сканерленетін желілік протоколдар Қолдау көрсетілетін хаттамалар: -HTTP, HTTPS -FTP, FTPS -IMAP, IMAPS -SMTP, SMTPS -POP3, POP3S -DNS Сканерлеу ерекшеліктері: - Кіріс және шығыс трафикті талдау. - Деректерді беру хаттамаларында зиянды элементтерді анықтау. - TLS қолдауымен шифрланған трафикті тексеру. Сканерленетін желілік ресурстар Қолдау көрсетілетін ресурстар: SMB (Windows Shares), NFS (Network File System), WebDAVСканерлеу ерекшеліктері: - Желілік ресурстардың мазмұнын қауіп-қатерге талдау. - Файлдардың қол жетімділігі мен өзгеруін тексеру. - Рұқсатсыз кіруді анықтау. Ақпараттың тұтастығы мен қолжетімділігін қамтамасыз етуге қойылатын талаптар Жергілікті деректерді сақтау: антивирустық агент графикалық интерфейс арқылы көруге болатын жергілікті есептер қоймасына ие болуы керек. - Қосымша талдау үшін есептерді файлға экспорттауға қолдау болуы керек. Карантин: анықталған зиянды файлдарды жергілікті қоймаға жылжыту мүмкіндігі (карантин), содан кейін қажет болған жағдайда қалпына келтіру. Қауіптерді анықтаудағы әрекеттер: - Процестерді аяқтау.

	- Файлдарды жою. - Пайдаланушы ережелеріне негізделген жалған позитивтерді елемеу. Мінез-құлықты талдау: - Зиянды белсенділікті анықтау үшін процестердің мінез-құлқын талдау мүмкіндігі. -Осалдықтарды пайдалану әрекеттерін анықтау. Араласудан қорғау: - Процестерді тоқтатудан және антивирустық агент файлдарын жоюдан қорғау. -Параметрлерді рұқсатсыз өзгертуден қорғау үшін құпия сөзді орнату мүмкіндігі. Антивирустық компоненттерді жаңарту: - Интернет, Жергілікті сервер немесе желілік каталог арқылы жаңарту. - Қолтаңбалар мен қауіп-қатер базасын автоматты түрде жаңарту. **11.5.** Компоненттің тұтастығы мен қолжетімділігін қамтамасыз етуге қойылатын талаптар 11.5.1.Рұқсатсыз араласудан қорғау: - Агент процестерін тоқтатудан немесе жоюдан қорғау. - Авторизациясыз параметрлердің өзгеруін бұғаттау. - Әкімшілік консоль арқылы кіру құқығын орнату. 11.5.2.Өзін-өзі емдеу механизмдері: - Апаттар кезінде сыни қызметтерді автоматты түрде қайта іске қосыңыз. - Файлдық жүйелер мен компоненттер конфигурацияларының тұтастығын бақылау. 11.5.3.Қол жеткізуді басқару және аутентификация: - Жүйе конфигурациясының барлық өзгерістерін журналға жазу. 11.5.4.Өнімділік мониторингі: - Ескертулермен жүйенің жай-күйін үздіксіз бақылау. - Нақты уақыттағы компоненттердің күйі туралы есептер. 11.5.5.Жаңартулар мен түзетулер: - Тұрақты жаңартулар мен қауіпсіздік патчтары. - Қорғалған байланыс арналары арқылы қолтаңба базалары мен қауіпсіздік саясатын жаңарту. **11.6. Антивирустық компоненттер мен қолтаңба жиынтығын жаңарту көздері** 11.6.1.Қашықтағы көздер: - Интернет арқылы қол жетімді өндірушінің сервері (https). -Бұлтты сақтау. 11.6.2.Жаңартуларды автоматтандыру: - Реттелетін автоматты жаңарту кестесі. - Веб-консоль арқылы жаңартуларды қолмен іске қосуды қолдау.

	11.6.3.Қорғалған деректерді беру: - Жаңартуларды қауіпсіз тасымалдау үшін TLS пайдалану. - Орнату алдында компоненттердің сандық қолтаңбаларын тексеру. Орталықтандырылған басқару мүмкіндіктері Орталықтандырылған орнату және жаңарту: - Орталық консольден жүйе компоненттерін орнату, жаңарту және жою. - Барлық соңғы нүктелердегі қауіпсіздік саясатын басқару. Мониторинг және бақылау: - Нақты уақыт режимінде жүйенің жұмысын орталықтандырылған бақылау. - Оқиғалар журналдарын және жаңарту тарихын қарау. Конфигурацияны басқару: - Топтық саясатты қолдана отырып, жүйе параметрлерін теңшеу. - Пайдаланушылардың қол жеткізу құқықтары мен рөлдерін басқару. Оқиғаларға жауап беру: - Құрылғыларды оқшаулауға командалар жіберу. - Процестерді, файлдарды және желілік қосылымдарды бұғаттау. - Соңғы нүктелерде қашықтағы командаларды орындау. Есептер мен хабарламалар: - Қауіпсіздік туралы егжей-тегжейлі есептер шығару. - Қауіпсіздік оқиғалары мен жүйенің жаңартулары туралы реттелетін хабарламалар. Сыртқы жүйелермен Интеграция: - Siem, SOAR және басқа қауіпсіздік жүйелерімен Интеграция. -Басқа ат шешімдерімен өзара әрекеттесуге арналған API. **11.7. Оқиғаларға жауап беру** 11.7.1.Инциденттерге ден қою жөніндегі іс-қимылдар: - Процесті аяқтаңыз; - Файлды жою; - Файлды жұмыс станциясынан аналитиктің компьютеріне немесе ДК қоймасына жүктеңіз; - Жүйелік артықшылықтары бар Операциялық жүйе пәрменін орындаңыз; - Автоматты түрде іске қосылатын нысандарды/сценарийлерді алыңыз; - Орындалатын файлдарды бұғаттау (хэш, Файл атауы); - Оқиғаларға жауап беру үшін Playbook құру функциясы. Басқа жүйелермен Интеграция 11.7.2.SIEM жүйелерімен Интеграция:

	- Деректерді алмасудың стандартты протоколдары мен интерфейстері (API, syslog, REST, webhook және басқалары) арқылы өндірістік SIEM жүйелерімен интеграцияны қолдау. - Нақты уақыттағы оқиғалар мен анықталған қауіптер туралы деректерді беру. 11.7.3.SOAR интеграциясы: - Soar платформалары арқылы жауап беру процестерін автоматтандыруды қолдау (мысалы, IBM Resilient, ServiceNow). 11.7.4.Осалдықтарды басқару жүйелерімен Интеграция: -Осалдықты сканерлеу жүйелерімен байланыс (мысалы, Tenable, Qualys). 11.7.5.Қол жеткізуді басқару жүйесімен Интеграция: - Есептік жазбаларды басқаруға арналған LDAP, Active Directory интеграциясы. -SAML арқылы SSO қолдау. 11.7.6.API және веб-ілмектер: - Оқиғалар, қауіптер мен оқиғалар туралы деректерді алу үшін REST API. -Ескерту жүйелеріне деректерді жіберуге арналған Веб-ілмектер. 11.7.7.Бұлтты интеграция: - Amazon AWS, Microsoft Azure, Google Cloud бұлтты қызметтерін қолдау. -Бұлтты ресурстарды басқару және деректерді қорғау үшін кіріктірілген интеграциялар. 11.7.8.Техникалық интеграция: - Күдікті хаттарды талдауға арналған пошта жүйелерімен Интеграция (SMTP/IMAP). - Киберқауіптер туралы деректерді бөлісу үшін STIX/TAXII есеп форматтарын қолдау. **11.8. Техникалық қолдау** Жеке техникалық менеджерге қойылатын талаптар Өнім беруші жеке техникалық менеджерді бөледі, ол: 11.8.1. Тапсырыс берушінің сұраныстарын өңдеумен айналысады. 11.8.2. Техникалық қолдау жұмыстарын ұйымдастырады. 11.8.3. Тапсырыс берушіні сұрау салуларды шешудің ағымдағы жай-күйі туралы хабардар етеді. 11.8.4. Жұмыс күндері Астана уақыты бойынша дүйсенбіден жұмаға дейін сағат 9.00-ден 18.00 дейінгі телефон және электрондық пошта арқылы қолжетімді. Техникалық қолдаудың реакция уақытына қойылатын талаптар Техникалық қолдау демалыс және мереке күндерін қоса алғанда, интернет-портал және (немесе) телефон және (немесе) электрондық пошта арқылы тәулік бойы қолжетімді болуы тиіс. Жауап беру уақыты: - Сыни деңгей-30 минуттан аспайды - Жоғары деңгей-4 жұмыс сағатынан аспайды

	- Орташа деңгей-6 жұмыс сағатынан аспайды - Төмен деңгей-8 жұмыс сағатынан аспайды "Сыни деңгей" -бүкіл жергілікті желі (немесе желінің маңызды бөлігі) жұмыс істемейді, бұл негізгі бизнес-процестерді тоқтатады. "Жоғары деңгей" - өнім толығымен істен шыққан, бірақ негізгі бизнес-процестердің үздіксіздігі бұзылмайды. "Орта деңгей" - өнім ішінара істен шыққан (сәйкес емес жұмыс істейді), бірақ өнімнің жұмысының нәтижесінде пайдаланушының басқа бағдарламалық жасақтамасы істен шыққан жоқ. "Төмен деңгей" - басқа маңызды емес қызмет сұрауларын білдіреді. Жоғарыда айтылмаған барлық оқиғалар осы сыни деңгейге жатады. Техникалық қолдау сұрауларының түрлері - Өнімді орнату, конфигурациялау және жұмыс істеу процесінде оқиғаларды шешу бойынша кеңес беру. - Зиянды бағдарламалармен жұқтырылған файлдарды емдеу бойынша кеңестер; - Антивирустық қолтаңбалар жиынтығын басымдықпен шығаруды жүзеге асыру, оның ішінде: - берілген жиынтықтан жекелеген зиянды заттарды анықтау, осындай жиынтықтың зиянды заттарының әрқайсысы үшін қолтаңбалардың дайындығына қарай; - осы жиынтыққа қолтаңбалар дайын болғаннан кейін бір уақытта зиянды заттар жиынтығын анықтау. - Антивирустық бағдарламалық қамтамасыз етуді өндірушінің білікті мамандарымен (вирустық талдаушылар, компьютерлік криминалистика және инциденттерге ден қою жөніндегі мамандар), зиянды кодты зерттеу, Компьютерлік криминалистика және компьютерлік инциденттерге ден қою мәселелері бойынша қажеттілігіне қарай, бірақ жыл ішінде 50 сағаттан аспайтын консультациялар; Бағдарламалық жасақтаманы жаңартуға қойылатын талаптар – Антивирустық қолтаңбалар жиынтығын жаңарту жиілігі-аптасына кемінде бір рет. - "Орталықтандырылған басқарылатын антивирустық қорғау ДК" және 'Sandbox компоненті бар ақпараттық қауіпсіздік инциденттерін анықтау және орталықтандырылған әрекет ету ДК" агенттерін жаңарту кезеңділігі – тоқсанына кемінде бір рет. - Өнім беруші анықталған осалдықты сипаттайтын Тапсырыс берушінің сұранысы бойынша компоненттердің бағдарламалық жасақтамасына түзетулер (патчтар) шығаруды қамтамасыз етуі керек. Жабдықтың ақаулыққа төзімділігін қамтамасыз етуге қойылатын талаптар Өнім берушіде компоненттердің серверлік жабдықтарына арналған қосалқы бөлшектер, құралдар, керек-жарақтар мен материалдар болуы керек және жабдық істен шыққан жағдайда олардың сыни деңгейге сәйкес тұрақты жұмысын қалпына келтіруі керек. Деректерді сақтауға және өңдеуге қойылатын талаптар: - 7 күнге дейін сақталатын толық телеметрия. - TLS протоколы арқылы қорғалған байланыс арнасы арқылы барлық деректер мен метадеректерді шифрлау.

	Жеткізу талаптары Жабдықтар мен бағдарламалық қамтамасыз етуді жеткізу бір жолғы түрде жүзеге асырылады, бірақ Қазақстан Республикасы мемлекеттік сатып алуды жүзеге асыру қағидаларының 569-тармағында белгіленген ең төменгі мерзім аяқталғаннан кейін ғана. Өнімділікті тексеруге қойылатын талаптар Тапсырыс берушінің аумағында шарт талаптарына сәйкес тауардың жұмыс қабілеттілігі мен толықтығын тексеру және тексеру үшін жеткізуді жүзеге асыру. Жұмыс қабілеттілігін тексеру іске қосу және сынамалық қосу, зақымданулардың, ақаулардың, жарықтардың, коррозияның болмауын көзбен шолып тексеру жолымен жүзеге асырылады. **12. Ақпараттық қауіпсіздік саласындағы шешімдердің архитектуралық принциптері мен жіктелуіне қойылатын талаптар** **1.** Шешімдер сыныбына сәйкестік қағидаты Ақпараттық қауіпсіздікке (АҚ) қойылатын әрбір функционалдық Талап АҚ архитектурасы мен әдіснамасында белгіленген шешімдердің жеке, нақты айқындалған сыныбына сәйкес келетін шешіммен іске асырылуға тиіс **2.** Функционалдық талаптар бір шешім шеңберінде де, бірнеше шешімді біріктіру арқылы да жүзеге асырылуы мүмкін, бастысы осы Техникалық ерекшеліктегі барлық талаптардың орындалуы. **3.** Дербестік өлшемшарты Әрбір енгізілген шешім ақпараттық қауіпсіздікті қамтамасыз етудің дербес және тәуелсіз функциясын орындауға міндетті.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді	Әлеуетті өнім беруші оны жеңімпаз деп анықтаған және Мемлекеттік сатып алу туралы шарт жасасқан жағдайда мыналарды ұсынуға міндетті: Техникалық ерекшелікте көзделген өнімдерді жеткізуге (ұсынуға) Өнім берушінің құқығын растайтын құқық иеленушінің (өндірушінің) немесе оның ресми өкілінің хаттары (сертификаттары) шарт күшіне енген күннен бастап 10 (он) жұмыс күні ішінде ұсынылады. Көрсетілген хат Техникалық ерекшелікке енгізілген әрбір өнім үшін бөлек ұсынылуы керек және мыналарды қамтуы керек: **1.** Вендор құрастырған және ресми растаған техникалық ерекшелік талаптары мен тиісті өнімнің/шешімнің сипаттамаларын егжей-тегжейлі салыстыратын кесте. **2.** Вендордан осы өнімнің сертификатталғандығы және / немесе тиісті бағдарламалық қамтамасыз етуді пайдалану үшін өзекті нұсқада қолдау көрсетілетіндігі туралы растау;

көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

Техникалық ерекшелікке
1-қосымша

АҚ қатерлері мен оқиғаларына ден қоюдың базалық үдерісі

№	Іс-қимыл	Қысқаша сипаттамасы	Жауапты	SLA
1	**Ақпараттық қауіпсіздік (АҚ) оқиғаларының мониторингі және талдау**			
1.1		Ақпараттық қауіпсіздік оқиғаларының мониторингі мен талдауы әлеуетті оқиғаларды анықтауды және оларды жалған оң нәтижелерге бағалауды көздейді. Бұл қатерлерді уақтылы анықтауға және ақпараттық жүйелерді қорғау тиімділігін арттыра отырып, қате оқиғаларға қажетсіз ден қою санын азайтуға көмектеседі.	SOC желісінің 1/2 талдаушылары	ТЕ-ке № 3 қосымшасына сәйкес
1.2.		Оқиға туралы қосымша ақпарат беру және іс-әрекеттің заңдылығын растау/теріске шығару Өнім берушінің 1-ші және 2-ші желісі талдаушыларының сұрау салуы шеңберінде жүзеге асырылады. Бұл үдеріс оқиғаны неғұрлым терең талдауға, оның бөлшектерін нақтылауға және анықталған іс-қимылдардың заңды болып табылатынын немесе олардың ақпараттық қауіпсіздікке қатер төндірумен байланысты екенін анықтауға бағытталған.	Тапсырыс берушінің жауапты қызметкері	ТЕ-ке № 3 қосымшасына сәйкес
2	**АҚ қатерлері мен оқиғаларын талдау**			
2.1		АҚ әлеуетті оқиғаларын талдау, олардың басымдықтарын бағалау және бастапқы ден қою бойынша ұсынымдар әзірлеу	SOC желісінің 1/2 талдаушысы	ТЕ-ке № 3 қосымшасына сәйкес
3	**Тапсырыс берушінің АҚ-ның анықталған қатері мен оқиғасы туралы хабарлама**			
3.1		**Өнім берушінің есепке алу жүйесінде ақпараттық қауіпсіздік оқиғасын (АҚ) ашу оқиға карточкасын толтыру және оны Тапсырыс берушіге** жіберу жолымен жүзеге асырылады. Оқиға карточкасында мынадай ақпарат болуы мүмкін: **Жалпы ақпарат:** • АҚ оқиғасының тақырыбы; • Өнім берушінің есепке алу жүйесіндегі АҚ оқиғасының нөмірі; • UTC пішіміндегі АҚ оқиғасын тіркеу уақыты;	SOC желісінің 1/2/3 талдаушысы	ТЕ-ке № 3 қосымшасына сәйкес

	• Оқиғаның басымдығы; **Негізгі ақпарат:** • оқиға кезінде қозғалған хосттар мен олардың белсенді тіркеулік жазбалардың тізімі (осы ақпарат болған жағдайда); • АҚ оқиғасы анықталған АҚ оқиғаларының көзі (дереккөзі); • Анықталған компромат индикаторларының тізімі (мысалы, файл хэш-сомасы, файл атауы, C&C серверінің мекенжайы, домендік атаулар және т.б.); • Оқиғаға қоса берілетін қосымша файлдарға сілтемелер; **Ұсынымдар:** • АҚ оқиғасын болдырмау немесе оның салдарларын барынша азайту үшін қабылдануы тиіс бастапқы іс-қимылдар; • Өнім берушінің АҚ инцидентін одан әрі талдауы үшін Тапсырыс берушіден талап етілуі мүмкін қосымша ақпарат.		
4	**Тапсырыс берушінің АҚ оқиғасы бойынша кері байланысты ұсынуы**		
4.1	Оқиға карточкасын алғаннан кейін Тапсырыс беруші Өнім беруші ұсынған ұсынымдарға, Оқиғаның түрі мен басымдығына байланысты АҚ Оқиғасына тиісті реакцияны қамтамасыз етеді.	Тапсырыс берушінің жауапты қызметкері	ТЕ-ке № 3 қосымшасына сәйкес

Техникалық ерекшелікке
2-қосымша

АҚ анықталған қатерлер мен оқиғалардың сындылығын жіктеу

Деңгей	Сындылық деңгейінің сипаттамасы	Мысал
Сыни	Тапсырыс берушінің барлық қорғалатын ресурстарына не ұзақтығы 15 минуттан асатын толық қол жетімсіздікке, не Тапсырыс берушіге елеулі залал келтіруі мүмкін Тапсырыс берушінің қорғалатын ресурстарының көп мөлшерін ымыраландыру фактілеріне әкелетін тосын оқиға. Немесе оқиға таргеттелген сипатта болады.	Домен әкімшісінің тіркеулік жазбасы әшкерленген таргеттелген шабуыл
Жоғары	Тапсырыс берушінің қорғалатын ресурстарының ішінара қол жетімсіздігіне, 15 сағатта 1 реттен аспайтын кезеңділікпен туындайтын ұзақтығы 1 минуттан аспайтын оқиғаға не Тапсырыс берушінің қорғалатын ресурстарының әшкереленуі үшін мүмкіндікке немесе жағдай жасауға әкеп соғатын оқиға: қасақана белсенділікке ескертпелі АҚҚ тосқауыл қойылмаған	Пайдаланылатын вирусқа қарсы қорғау құралдарымен анықталмайтын зиянды бағдарламалық жасақтаманың белсенділігі
Орташа	Қазіргі сәтте Тапсырыс берушінің қорғалатын ресурстарының қолжетімсіздігіне әкелмейтін, бірақ болашақта неғұрлым жоғары басымдықты оқиғаға әкелу ықтималдығы жоғары оқиға. Қасақана белсенділікті ескертпелі АҚҚ оқшаулады және бұғаттады.	Пайдаланылатын антивирустық қорғау құралдарымен бұғатталған зиянды бағдарламалық жасақтаманы кейіннен хостқа жұқтыру әрекетімен шолғыштың осалдығын сәтті пайдалану
Төмен	Оның шеңберінде Тапсырыс берушіге қандай да бір залал келтірілмеген оқиға, қолда бар қол жеткізу құқықтары шеңберінде жүйе туралы ақпарат жинау жүзеге асырылды.	Қорғалатын периметр туралы ақпарат жинау

Техникалық ерекшелікке
3-қосымша

АҚ оқиғаларының мониторингі қызметін ұсыну деңгейінің нысаналы көрсеткіштері

№	Көрсеткіш	Басымдық	Көрсеткішті орындау уақыты *	Табель*	Тапсырыс берушінің Өнім берушінің сұрауларына жауап беру уақыты **
1.	АҚ оқиғасын анықтау,	1 — Сыни	30 минутқа дейін	24x7	Қолданылмайды
		2 — Жоғары	30 минутқа дейін	24x7	Қолданылмайды
		3 — Орташа	30 минутқа дейін	24x7	Қолданылмайды
		4 — Төмен	60 минутқа дейін	24x7	Қолданылмайды
2.	АҚ оқиғасын тіркеу АҚ оқиғасы тіркелген сәттен бастап Өнім беруші тосын оқиғаның жалған іске қосылуын тексеруді және санаттауды жүргізеді, АҚ оқиғасы туралы Тапсырыс берушіні хабардар етеді	1 — Сыни	60 минутқа дейін	24x7	30 минутқа дейін
		2 — Жоғары	90 минутқа дейін	24x7	45 минутқа дейін
		3 — Орташа	120 минутқа дейін	24x7	60 минутқа дейін
		4 — Төмен	240 минутқа дейін	24x7	120 минутқа дейін
3.	Егер Тапсырыс беруші АҚ оқиғасын растаған жағдайда, Өнім беруші қарсы іс-қимыл бойынша ұсынымдар береді	1 — Сыни	Тіркелген сәттен бастап 2 сағат	24x7	Қолданылмайды
		2 — Жоғары	Тіркелген сәттен бастап 4 сағат	24x7	Қолданылмайды
		3 — Орташа	Тіркелген сәттен бастап 6 сағат	24x7	Қолданылмайды
		4 — Төмен	Тіркелген сәттен бастап 24 сағат	24x7	Қолданылмайды

** Үшінші тұлғалардың бағдарламалық қамтамасыз етуін өндірушінің техникалық қолдауына (техникалық қолдаудың үшінші желісі) жүгіну және (немесе) Тапсырыс берушіден қосымша ақпарат алу талап етілетін кезеңде АҚ инцидентін қалпына келтіру және шешу мерзімі тоқтатыла тұрады. Осы кезеңде АҚ инциденті «Күту» мәртебесіне ауыстырылады. ** Тапсырыс берушінің ден қою уақыты Өнім беруші сұрау салуды жіберген сәттен бастап есептеледі.*

Техникалық ерекшелікке
4-қосымша

Айына өзгерістер жүргізудің нысаналы көрсеткіштері

№	Көрсеткіш		Жүгінулер саны
1.	Өзгертуге сұрау салу	Қызмет конфигурациясын өзгертуге байланысты өтінімдер (АҚ оқиғалар көзін қосу/жою, сценарийді бейімдеу)	8-ден артық емес
2.	Ақпараттық сұрау	Қызмет бойынша консультациялық мәселелерге байланысты өтінімдер (Шарт бойынша мәселелер және т.б.)	4-тен артық емес
3.	АҚ оқиғасына күдік	Тапсырыс берушінің АҚ оқиғасына күдіктенуіне байланысты өтінім. Бастапқыда бұл өтінішке «төмен» басымдық беріледі. Қажет болған жағдайда Тапсырыс беруші басымдықты жоғарылата алады. Сұрау салудың осы түрі бойынша жұмыс ТЕ-ге № 3 қосымшаға сәйкес жүргізіледі.	Шектелмеген

Техникалық ерекшелікке
5-қосымша

АҚ Оқиғаларының мониторингі қызметін көрсету кезеңінде жауапкершілік аймақтарының аражігін ажырату

№	Параметрі	Тапсырыс беруші	Өнім беруші
АҚ Оқиғаларына мониторинг және талдау қызметін көрсету			
1.1	Мониторинг аймағына кіретін Тапсырыс беруші инфрақұрылымының элементтеріне қатысты тіркелген АҚ оқиғаларын мониторингтеу және талдау (инциденттерге ден қою жөніндегі ұсынымдарды ұсынуды қоса алғанда).		+
1.2	Мониторинг аймағына кірмейтін Клиенттердің тіркелген немесе инфрақұрылым элементтеріне қатысты АҚ оқиғаларын мониторингілеу және талдау.	+	
1.3	Тапсырыс берушінің алаңында да, Өнім берушінің алаңында да орнатылған АҚ оқиғаларын басқару кіші жүйесі компоненттерінің жай-күйін мониторингтеу		+
1.4	АҚ оқиғаларын басқару кіші жүйесінің дұрыс жұмыс істеуін қамтамасыз ету		+
1.5	Логтарды жіберу үшін көздерге агенттерді орнату	+	
1.6.	Өнім берушінің ұсынымдарына сәйкес оқиғалар/ағындар коллекторларын және АҚ оқиғаларын басқару кіші жүйесінің өзге де инфрақұрылымдық элементтерін өрістету үшін қажетті технологиялық қуаттарды ұсыну. Тиісті инфрақұрылымның істен шығуға төзімділігі мен қол жетімділігін қолдау	+	
1.7	Көздерден коллекторларға желілік ағындарды бағыттау	+	
1.8	Орындаушы ұсынған ұсынымдарға сәйкес АҚ оқиғаларына ден қою, оларды оқшаулау, зардаптарын жою және штаттық жұмыс режимін қалпына келтіру	+	
1.9	Тапсырыс беруші мен Өнім берушінің алаңдары арасында ақпаратты берудің қорғалған арналарының жұмыс қабілеттілігін қамтамасыз ету	+	+
1.10	АҚЖО ұсынымдарын орындау және АҚ оқиғаларына уақтылы ден қою	+	
1.11	Мониторинг аймағына кіретін серверлік, коммуникациялық және компьютерлік жабдықтардың, сондай-ақ ақпараттық жүйелердің өзекті тізбесін ұсыну	+	
1.12	Қайталанған оқиғаның туындау ықтималдығын болдырмау мақсатында Орындаушының ұсынымдарын қолдану	+	

№	Параметрі	Тапсырыс беруші	Өнім беруші
1.13	Мониторинг аймағындағы барлық өзгерістер туралы ақпаратты, жаңа желілік құрылғылар, IP мекенжайлары, сыртқы авторландырылған қосылулар және т.б. туралы ақпаратты қоса алғанда, бірақ олармен шектелмей, жедел ұсыну.	+	
1.14	Шарттың қолданылу кезеңінде Тапсырыс берушіден алынатын деректерді (оқиғалар, желілік ағындар) сақтау		+

Техникалық ерекшелікке
6-қосымша

Тапсырыс берушінің АТ-инфрақұрылымының кеңейтілген сараптамасы

Сұрау түрі	Қысқаша сипаттамасы	Көрініс бірлігі
Осалдықтардың болуына мониторинг аймағын сканерлеу	Қосымшалар мен операциялық жүйелердегі қауіптерді анықтау үшін, осалдықтар мен оларды жою бойынша ұсынымдар бойынша егжей-тегжейлі есеп бере отырып, мониторинг аймағына кіретін тораптар мен ақпараттық жүйелерді аспаптық сканерлеу.	Бекітілген жұмыс жоспарына сәйкес тоқсанына кемінде 1 рет кемінде 512 бірегей IP-мекенжай.
Периметрді осалдыққа сканерлеу (сыртқы)	Қосымшалар мен операциялық жүйелердегі қауіптерді анықтау үшін, осалдықтар мен оларды жою бойынша ұсынымдар бойынша егжей-тегжейлі есеп бере отырып, мониторинг аймағына кіретін тораптар мен ақпараттық жүйелерді аспаптық сканерлеу.	Бекітілген жұмыс жоспарына сәйкес тоқсанына 1 реттен кем емес 256 бірегей IP-мекен-жай.
Тапсырыс берушінің инфрақұрылымына сырттан кіруге арналған тестілеулер	Интернет желісінен Тапсырыс берушінің инфрақұрылымына енулерге тесттер жүргізу. Тестілеудің сценарийлері мен әдістері Тапсырыс берушімен келісіледі. Тестілеу қорытындысы бойынша Өнім беруші есеп береді.	Кем дегенде 128 бірегей IP, жылына кемінде 2 тест. Сервис Тапсырыс берушінің сұранысы бойынша ұсынылады.
Нысаналы кибершабуылдарды еліктеу (Red Teaming)	Кейіннен талдау және ақпараттық жүйелердің қорғалу деңгейін арттыру бойынша ұсынымдар бере отырып, нысаналы кибершабуылдарды еліктеуді жүргізу. Енуге тесттерден айырмашылығы, Red Teaming мақсаты - Тапсырыс берушінің максималды осалдықтардын табу емес, басып кіруді анықтау және болдырмау қабілеттерін бағалау.	Кемінде 128 бірегей IP-мекенжай, Тапсырыс берушінің өтінімі бойынша Қызметтер көрсету мерзімі ішінде 2 (екі) тест; құны Шарт бағасына енгізілген.

- - Форензия жөніндегі мамандарды тарта отырып, сындарлы оқиғаларға кеңейтілген тексеру жүргізу қажет болған кезде (Тапсырыс берушінің алаңында ден қою жөніндегі іс-шараларды, қатты дискілердің үлгілерін жинау және зерттеуді, зиянды бағдарламалық жасақтаманы талдауды, сондай-ақ оқиғалардың салдарын жоюға көмек көрсетуді қоса алғанда), бұл сервис Тапсырыс берушінің сұрау салуы бойынша ғана ұсынылады.