



Ақпараттық қауіпсіздіктің жедел орталығы қызметінің техникалық ерекшелігі

Осы техникалық ерекшелік ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер кешенін (бұдан әрі – «Қызмет») көрсетуге қойылатын жалпы және жеке талаптарды қамтиды.

Қызмет шеңберінде мынадай міндеттер шешілуге тиіс:

- Тапсырыс берушінің инфрақұрылымында қажетті құрамдастарды өрістетуді қоса алғанда, АҚ оқиғаларына мониторинг жүргізуді және АҚ инциденттерін өңдеуді ұйымдастыру әрі жүзеге асыру (бұдан әрі – АҚ инциденттеріне мониторингті ұйымдастыру);
- Өнім берушінің SIEM жүйесіне қосылған Тапсырыс берушінің серверлік жабдығында, желілік құрылғыларында және ақпараттық жүйелерінде тіркелген АҚ оқиғаларына тәулік бойы мониторинг жүргізу (бұдан әрі – Мониторинг аймағы);
- Мониторинг аймағында орын алған АҚ инциденттерін анықтау;
- Тапсырыс берушіге анықталған инциденттер, оларға ден қою тәсілдері туралы ақпарат және оларды жою жөніндегі ұсынымдар беру;
- АҚ инциденттеріне ден қою барысында сараптамалық қолдау көрсету;
- АҚ инциденттерін тергеп-тексеруге көмек көрсету. Егер Мониторинг аймағында оған кірмейтін жүйелерге қатысты күмәнді оқиға анықталса, бұл туралы Тапсырыс берушіге хабарланады. Одан әрі тергеп-тексеруді Тапсырыс беруші дербес жүргізеді, ал Өнім беруші қажет болған жағдайда сындарлылық дәрежесін айқындау және қосымша талдау жүргізу, мәселе көзін анықтау әрі Тапсырыс беруші мамандарының инцидентті жоюына жәрдемдесу үшін консультация береді;

1. Қызмет көрсету шекаралары және АҚ ахуалдық орталығына қосылу:

Жалпы алғанда Қызмет көрсету шекарасына ақпараттық жүйелер орналастырылған Тапсырыс берушінің мынадай алаңдары кіреді

Қызметтер Өнім берушінің орналасқан жерінен қашықтан көрсетіледі. Қажет болған жағдайда Өнім берушінің қызметкерлері Тапсырыс берушінің аумағына барып Қызмет көрсете алады (жабдықты монтаждау, баптау және т.б.). Тапсырыс беруші Өнім берушінің қызметкерлеріне қажетті қолжетімділікті қамтамасыз етуге тиіс, оның тәртібі шарт жасалғаннан кейін келісіледі.

Қызмет шеңберінде Өнім беруші қажетті аппараттық және бағдарламалық қамтылымды ескере отырып, Қызметтің мақсаттары мен міндеттерін орындауға арналған 2-кестеде көрсетілген мамандандырылған жүйелер мен қызметтерді ұсынады:

№2 кесте. Қызмет құрамы

№	Құрамдастың атауы	Сипаттамасы
1	АҚ ахуалдық орталығының қызметі	АҚ оқиғаларын мониторингтеу және талдау, АҚ инциденттеріне ден қоюға көмек көрсету, сондай-ақ АҚ ахуалдық орталығының технологиялық стегін басқару қызметтерін қамтиды.
2	АҚ ахуалдық орталығының платформасы	АҚ ахуалдық орталығының қызметі көрсетілетін платформа; ол ақпараттық қауіпсіздік оқиғаларын жинау, мониторингтеу және талдау жүйесінің, инциденттерді

№	Құрамдастың атауы	Сипаттамасы
2	АҚ ахуалдық орталығының платформасы	АҚ ахуалдық орталығының қызметі көрсетілетін платформа; ол ақпараттық қауіпсіздік оқиғаларын жинау, мониторингтеу және талдау жүйесінің, инциденттерді басқару мен автоматтандыру және қатерлерді талдау жүйесінің функционалын қамтиды.
3	АҚ ахуалдық орталығы платформасының оқиға коллекторлары	Тапсырыс беруші жағында орналастырылады (қажет болған жағдайда).
4	VPN-шлюз	Тапсырыс берушінің жабдығы пайдаланылады

2. Қызмет көрсету мерзімі және ақы төлеу тәртібі

Қызметтер шарт жасалған сәттен бастап 2027 жылғы 31 желтоқсанға дейін көрсетіледі. Шарт сомасы 12 айға есептелген. Шарт 2027 жылғы 1 қаңтардан кейін жасалған жағдайда, оның сомасы қалған кезеңге пропорционалды түрде түзетіледі.

3. Көрсетілетін қызметтерге қойылатын функционалдық талаптар

Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер шеңберінде тиісті функционалдық сипаттамалары бар мынадай сервистер мен жүйелер ұсынылады.

5.1. АҚ ахуалдық орталығының қызметі

АҚ ахуалдық орталығы қызметінің құрамы

АҚ ахуалдық орталығы қызметінің құрамына қойылатын талаптар 4 кезеңнен тұрады, әр кезеңде мақсат және оған қол жеткізуге арналған міндеттер белгіленген.

1-кезең. Зерттеп-қарау:

Кезеңнің мақсаты – қызмет көрсету мониторингі аймағын және дереккөздер тізбесін айқындау.

Мақсатқа қол жеткізу үшін шешілуге тиіс міндеттер:

Тапсырыс беруші толтырған сауалнама парағы және оның өкілдерімен жүргізілген сұхбат негізінде Өнім беруші Тапсырыс берушінің АТ-инфрақұрылымына талдау жүргізеді, соның нәтижесінде:

- қосылатын АҚ оқиғалары дереккөздерінің (бұдан әрі – дереккөздер) құрамы мен басымдығы жөнінде ұсынымдар беріледі;
- қолданыстағы шабуылдарды анықтау сценарийлерін қосу және жаңаларын әзірлеу бөлігінде Тапсырыс берушінің қажеттіліктері айқындалады. Ол үшін Тапсырыс берушіге толтыруға арналған талдамалық сауалнама парағы жіберіледі;
- қызмет көрсету мониторингі аймағы және Қызмет құрамдастарын Тапсырыс берушінің алаңында өрістету тәртібі бойынша ұйымдастырушылық-техникалық шешімдер әзірленеді;
- оқиғаларды Тапсырыс берушінің АТ-инфрақұрылымында 3 (үш) ай бойы ықтимал сақтау үшін файлдық қоймалардың сыйымдылығын есептеуді қоса алғанда, Тапсырыс беруші бөлетін есептеу ресурстарының техникалық сипаттамалары мен оларға қойылатын талаптар айқындалады;
- Тапсырыс беруші алаңындағы Қызмет құрамдастары мен Киберқауіптерді мониторингтеу және оларға ден қою орталығы арасындағы желіаралық өзара іс-қимылдың тәртібі мен ұйымдастырылуы айқындалады;

• осы кезең шеңберінде кемінде мынадай мәліметтер жиналуға тиіс:

- дереккөздің атауы;
- дереккөз функционалының сипаттамасы (ақпараттық жүйеге тиесілігі);
- орналастыру алаңы;
- өндіруші/маркасы/моделі;

Қосылатын инфрақұрылым объектілерінің (оқиға көздерінің) саны – 11 физикалық сервер, 24 виртуалды, 30 соңғы құрылым, 2 Palo Alto брандмауэрі.

2-кезең. Енгізу:

Кезеңнің мақсаты – Қызмет құрамдастарын Тапсырыс берушінің алаңында өрістету және Тапсырыс беруші мен Өнім берушінің алаңдары арасында VPN-туннель құру:

Мақсатқа қол жеткізу үшін шешілуге тиіс міндеттер:

Таралған алаңдар арасында L3 байланысы болмаған жағдайда Өнім беруші мен Тапсырыс беруші өз алаңдарының арасында VPN-туннель ұйымдастырады, бұл ретте Тапсырыс беруші өз АТ-инфрақұрылымының шекарасына дейінгі қосылысты қамтамасыз етеді.

- Өзара іс-қимыл кезінде пайдаланылатын көлік хаттамасын бұғаттау арқылы трафикті сүзгілеуге жол берілмеуге тиіс;
- Өнім берушінің сұрауына сәйкес Қызмет құрамдастары мен оқиғалар дереккөздері арасында желілік қолжетімділікті ұйымдастыру;
- Өнім беруші қажет болған жағдайда Қызмет құрамдастарын Тапсырыс берушінің АТ-инфрақұрылымына енгізу бойынша орнату жұмыстарын орындайды;
- қажет болған жағдайда Тапсырыс берушіге қосымша Қызмет құрамдастарын орнату үшін есептеу ресурстарына, сақтау кіші жүйесіне (жүйелеріне) қойылатын талаптар мен конфигурациялау жөніндегі ұсынымдарды беру;
- Өнім беруші Қызмет құрамдастарының жұмыс қабілеттілігін мониторингке қояды, сондай-ақ Тапсырыс берушімен VPN-қосылыс ұйымдастырылған белсенді желілік жабдықтың үздіксіз жұмысын қамтамасыз етеді;

3-кезең. Қосу:

Кезеңнің мақсаты – оқиғалар дереккөздерін қосу және оқиғалардың SIEM жүйесіне дұрыс түсетініне көз жеткізу, сондай-ақ Өнім берушінің сұрауы негізінде (қажет болған жағдайда) АҚ бұзушылықтары мен инциденттерін анықтаудың жаңа сценарийлерін әзірлеу:

Мақсатқа қол жеткізу үшін шешілуге тиіс міндеттер:

- 1-кезеңде айқындалған дереккөздер тізбесіне сәйкес Өнім беруші оларды қосу жөніндегі нұсқаулықтарды ұсынады;
- Өнім беруші қажет болған жағдайда стандартты емес дереккөздерге арналған жеке адаптерлерді әзірлейді;
- дереккөздер қосылғаннан кейін Өнім беруші түсетін оқиғалардың толықтығын тексереді және қажет болған жағдайда оларды оңтайландырады;
- Өнім беруші Тапсырыс беруші толтырған талдамалық сауалнама парағы негізінде SIEM жүйесін оның АТ-инфрақұрылымына бейімдеп конфигурациялайды және профильдейді. Бұл жұмыстар АҚ бұзушылықтары мен инциденттерін анықтау сценарийлерінің жұмыс қабілеттілігіне кепілдік береді;
- Өнім беруші Тапсырыс берушінің арнайы сұраулары және/немесе осалдықтарды талдау нәтижелері негізінде жаңа сценарийлерді, атап айтқанда инциденттер санаттары мен корреляция қағидаларын кеңейтуді әзірлейді;
- Өнім беруші Қызметті мониторингтеу үшін Тапсырыс берушінің уәкілетті өкілдеріне SOAR жүйесіне қолжетімділік береді;
- Тапсырыс беруші Өнім берушіге АҚ инциденттері туралы ақпарат жіберілуге тиіс қызметкерлердің тізімін береді, содан кейін Өнім беруші тиісті хабарландыру топтарын баптайды.

4-кезең. Операциялық жұмыс:

Кезеңнің мақсаты – SIEM жүйесін Тапсырыс берушінің мониторинг аймағына бейімдеу және SLA талаптарына сәйкес АҚ инциденттері туралы хабарландыруларды жіберуді баптау:

Мақсатқа қол жеткізу үшін шешілуге тиіс міндеттер:

АҚ ахуалдық орталығының қызметін көрсету шеңберінде Өнім беруші мыналарды орындауға тиіс:

- әртүрлі оқиға дереккөздерінен түсетін АҚ оқиғаларын Өнім берушінің бірыңғай «кіру нүктесі» болып табылатын бірінші желі талдаушыларының күшімен 24x7 режимінде талдау. Бірінші желі талдаушылары АҚ инциденттерін өңдеуді, жалған іске қосылуды тексеруді, бастапқы талдау жүргізуді және инциденттер санаттары мен қағидалары негізінде АҚ инциденттерін бөліп көрсетуді, сондай-ақ ITIL стандарттарына сәйкес инцидентті тіркеуді және кейіннен сүйемелдеуді (санаттау, басымдық беру, SLA және т.б.) қамтамасыз етуге тиіс. АҚ инциденттері туралы хабарлау режимі:
- Өнім берушінің екінші желі талдаушыларының күшімен АҚ инциденттерін 8x5 режимінде өңдеу, әртүрлі мамандандырылған құралдарды қолдана отырып тереңдетілген талдау жүргізу; корреляция қағидаларын Тапсырыс берушінің АТ-инфрақұрылымындағы өзгерістерге сәйкес бейімдеу; Тапсырыс берушінің талабы бойынша да, оның профилін дербес талдау негізінде де корреляция қағидаларына ерекшеліктер қосу;
- Тапсырыс беруші оқиғаның АҚ инциденті екенін растаған кезде инцидент тиісті мәртебеге ауыстырылады және онымен одан әрі жұмысты екінші және үшінші желі талдаушылары жүргізеді. Талдаушылар АҚ инцидентіне алып келген ретроспективалық оқиғаларға тереңдетілген талдау жүргізеді;
- АҚ инцидентін бастапқы тергеп-тексеру ұсынымдар беру және инцидентке ден қою жөніндегі нұсқаулықтарды дайындау арқылы жүргізіледі; олар оқиғаларды тікелей дереккөзден жинауға арналған конфигурациялық файлдарды да қамтуы мүмкін;

Қызметтер шеңберінде виджеттер және/немесе дашбордтар (Жеке кабинет) арқылы АҚ инциденттері жөніндегі талдамалық ақпаратты визуалдау мүмкіндігі іске асырылуға тиіс.

Жеке кабинетте Тапсырыс берушіге мынадай функциялар қолжетімді болуы керек:

- әрбір АҚ инцидентінің карточкасын қарау және оның мәртебесін дербес басқару;
- орын алған АҚ инциденттерінің статистикасын қарау;
- өтініштерді/АҚ инциденттерін тіркеу және олардың мәртебесін нақты уақыт режимінде қадағалау;
- SLA орындалуын қоса алғанда, Қызмет көрсету параметрлері туралы көрнекі ақпарат алу;
- анықталған шабуыл техникаларының сипаттамасы берілген әрбір АҚ инциденті туралы ақпаратты қарау;
- әрбір анықталған АҚ инциденті бойынша бірыңғай үлгідегі инцидент карточкасын ұсыну;
- Жеке кабинеттен бірыңғай есептерді жүктеп алу.

АҚ ахуалдық орталығының қызметін көрсетуге қойылатын талаптар

Осы талаптар АҚ ахуалдық орталығының қызметін қамтамасыз ету тәртібін белгілейді және АҚ инциденттерін анықтау мен оларға ден қоюға байланысты өзара іс-қимыл рәсімдерін сипаттайды.

Өнім берушінің есепке алу жүйесінде инцидент карточкасын толтыру арқылы АҚ инцидентін тіркеу және оны Тапсырыс берушіге жіберу іске асырылуға тиіс. Сындарлы, жоғары, орта және төмен деңгейдегі инциденттер туралы хабарлау Жеке кабинетте инцидент карточкасын көрсету және/немесе электрондық хат жіберу және/немесе Тапсырыс берушінің жауапты маманына расталған қоңырау шалу арқылы жүзеге асырылады.

Тапсырыс беруші инцидентті анықтаған жағдайда ол Өнім берушіге оның техникалық қызметінің байланыс деректері бойынша хабарлайды.

Инцидент карточкасында мынадай міндетті ақпарат болуға тиіс:

Жалпы ақпарат:

- тіркелген инциденттің нөмірі (Өнім берушінің есепке алу жүйесінде);
- инциденттің басымдығы;

- тіркеу уақыты;
- тақырыбы (қысқаша сипаттамасы);
- инцидент туралы ақпарат (ағымдағы мәртебе, осы мәртебеге түсініктеме);

Негізгі ақпарат (анықтау мүмкіндігі болған кезде):

- инцидент кезінде зардап шеккен хосттар мен олардағы белсенді есептік жазбалардың тізімі;
- инцидент анықталған АҚ оқиғаларының дереккөзі/дереккөздері;
- анықталған компрометация индикаторларының тізімі;
- инциденттің хронологиялық тәртіптегі сипаттамасы;
- инцидентке тіркелетін қосымша файлдарға сілтемелер;

Ұсынымдар:

- АҚ инцидентінің алдын алу немесе оның салдарын барынша азайту үшін қандай бастапқы әрекеттер жасалуға тиіс не Өнім берушінің инцидентті одан әрі талдауы үшін қандай қосымша ақпарат қажет;
- Қызмет көрсету шартына қол қойылғаннан кейін Өнім беруші мен Тапсырыс беруші көрсетілетін қызметтер шеңберіндегі барлық АҚ инциденттері, жаңартулар мен ұсынымдар ескерілетін есеп нысанын бірлесіп әзірлеуге тиіс. Есепті екі тарап ұйымдарының басшылығы ай сайын бекітеді.

Қызмет талаптарын орындау шеңберінде Өнім беруші АҚ инциденттерінің негізгі санаттарын анықтай алуға тиіс:

- **Unauthorized Access/Compromised.** Қорғалатын желіге/жүйеге/қосымшаға/деректерге рұқсатсыз физикалық немесе логикалық қолжетімділік алуға байланысты инциденттер.
- **Scans/Probes/Attempted Access.** Қолжетімді хосттар, ашық порттар, осалдықтар, орнатылған бағдарламалық қамтылым немесе нысана туралы бұзушы шабуылды одан әрі жоспарлау және дамыту үшін пайдалана алатын өзге де мәліметтерді алуға бағытталған белсенділікке байланысты инциденттер.
- **Brute Force.** Қорғалатын жүйелердің құпиясөздерін сәтті және сәтсіз іріктеу әрекеттеріне байланысты инциденттер.
- **Vulnerability.** Осалдықтарды сәтті пайдалануға, сондай-ақ пайдаланылуы ақпараттық қауіпсіздік қатерлерінің іске асуына әкелуі мүмкін сындарлы осалдықтарды (іске асыру осалдықтарын) сканерлер арқылы анықтауға байланысты инциденттер.
- **Malware.** Зиянды бағдарламалық қамтылымның белсенділігіне байланысты инциденттер (мысалы, шифрлаушы бағдарламаны іске қосу, троянды автоматты жүктеуге тіркеу және т.б.).
- **Malware C&C Communication.** Қорғалатын инфрақұрылым хосттарының белгілі командалық орталықтармен өзара іс-қимылын анықтауға байланысты инциденттер.
- **Malicious Host.** Зиянды бағдарламалық қамтылымды тарататын ресурстарға қол жеткізуге (ботнет желілерінің белгілі командалық орталықтарын қоспағанда) немесе осындай ресурстарды Интернет желісінде орналастыруға байланысты инциденттер.
- **Spam.** Ақпараттық/жарнамалық сипаттағы сұратылмаған электрондық поштаны таратуға байланысты инциденттер.
- **Fraud.** Қорғалатын ақпараттық жүйе пайдаланушыларының алаяқтық әрекеттеріне байланысты инциденттер.
- **Social Engineering.** Қорғалатын ақпараттық жүйе пайдаланушыларын алдау немесе сенімін теріс пайдалану арқылы бұзушының мақсаттарына жетуге бағытталған әрекеттерді жасауға (ақша аудару, зиянды сілтемеге өту, құпиясөз ақпаратын жария ету және т.б.) итермелеуге байланысты инциденттер.

- **Improper Usage.** АҚ саясатының/регламенттерінің/нұсқаулықтарының талаптарын бұзуға байланысты инциденттер (мысалы, ргоху-ді айналып өтіп Интернетке шығу, жалпыға ортақ Wi-Fi желілеріне қосылу, тыйым салынған хостта домен әкімшісінің есептік жазбасын пайдалану және т.б.).
- **Suspicious Process Activity.** Заңды процестердің қалыптан тыс мінез-құлқына байланысты инциденттер.

АҚ ахуалдық орталығы қызметін көрсету деңгейінің нысаналы көрсеткіштері:
АҚ инциденттері оларды шешудің шұғылдық дәрежесі бойынша №3 кестеде көрсетілген басымдықтарға бөлінуге тиіс.

№3 кесте. Басымдық көрсеткіштері

Басымдық	Басымдық сипаттамасы	Мысал
Сындарлы	Тапсырыс берушінің барлық қорғалатын ресурстарының 15 минуттан астам уақыт бойы толық қолжетімсіз болуына не Тапсырыс берушіге елеулі залал келтіруі мүмкін көптеген қорғалатын ресурстардың компрометациялануына әкелетін инцидент. Сондай-ақ инцидент нысаналы сипатта болуы мүмкін.	Домен әкімшісінің есептік жазбасы компрометацияланған нысаналы шабуыл
Жоғары	Тапсырыс берушінің қорғалатын ресурстарының 15 минуттан аспайтын ішінара қолжетімсіздігіне және сағатына бір реттен жиі емес қайталануына не қорғалатын ресурстарды компрометациялау мүмкіндігіне немесе жағдайының жасалуына әкелетін инцидент: зиянды белсенділік алдын алу АҚҚ-мен бұғатталмаған.	Пайдаланылатын антивирустық қорғау құралдары анықтамайтын зиянды бағдарламалық қамтылым белсенділігі
Орта	Қазіргі кезде Тапсырыс берушінің қорғалатын ресурстарының қолжетімсіздігіне әкелмейтін, бірақ болашақта басымдығы жоғары инцидентке әкелу ықтималдығы жоғары инцидент. Зиянды белсенділік оқшауланып, алдын алу АҚҚ-мен бұғатталған.	Браузер осалдығын сәтті пайдаланып, кейін хостты зиянды бағдарламалық қамтылыммен жұқтыру әрекетінің пайдаланылатын антивирустық қорғау құралдарымен бұғатталуы
Төмен	Тапсырыс берушіге ешқандай залал келтірілмеген, қолда бар қолжетімділік құқықтары шеңберінде жүйе туралы ақпарат жиналған инцидент.	Қорғалатын периметр туралы ақпарат жинау

Қызметтің нысаналы көрсеткіштеріне қойылатын талап:
Қызмет №4 кестеде келтірілген нысаналы көрсеткіштерге сәйкес көрсетілуге тиіс.

№4 кесте. Қызмет көрсету деңгейінің көрсеткіштері

№	Көрсеткіш	Басымдық	Көрсеткішті орындау уақыты	Кесте	Тапсырыс берушінің Өнім беруші сұрауларына ден қою уақыты
1.	АҚ инцидентін анықтау, АҚ инцидентін тіркеу	1 — Сындарлы	30 минутқа дейін	24x7	Қатысы жоқ
		2 — Жоғары	30 минутқа дейін	24x7	Қатысы жоқ
		3 — Орта	30 минутқа дейін	24x7	Қатысы жоқ
		4 — Төмен	60 минутқа дейін	24x7	Қатысы жоқ
2.	АҚ инциденті тіркелген сәттен бастап Өнім беруші жалған іске қосылуды тексереді және инцидентті санаттайды, Тапсырыс берушіге АҚ инциденті туралы хабарлайды	1 — Сындарлы	60 минутқа дейін	24x7	30 минутқа дейін
		2 — Жоғары	90 минутқа дейін	24x7	45 минутқа дейін
		3 — Орта	120 минутқа дейін	24x7	60 минутқа дейін
		4 — Төмен	240 минутқа дейін	24x7	120 минутқа дейін
3.	Тапсырыс беруші АҚ инцидентін растаған жағдайда Өнім беруші қарсы іс-қимыл жөніндегі ұсынымдарды береді	1 — Сындарлы	тіркелген сәттен бастап 2 сағат	24x7	Қатысы жоқ
		2 — Жоғары	тіркелген сәттен бастап 4 сағат	24x7	Қатысы жоқ
		3 — Орта	тіркелген сәттен бастап 6 сағат	24x7	Қатысы жоқ
		4 — Төмен	тіркелген сәттен бастап 24 сағат	24x7	Қатысы жоқ
4.	АҚ инцидентін тергеп-тексеру және Тапсырыс беруші Өнім берушіге ұсынған оқиғалар журналдарын талдау уақыты	1 — Сындарлы	Қатысы жоқ	24x7	Қатысы жоқ
		2 — Жоғары	Қатысы жоқ	24x7	Қатысы жоқ
		3 — Орта	Қатысы жоқ	8x5	Қатысы жоқ
		4 — Төмен	Қатысы жоқ	8x5	Қатысы жоқ

Қызметтерді Өнім беруші Тапсырыс берушінің сұрауларын №5 кестеде көрсетілген көрсеткіштерге сәйкес өңдеуге тиіс.

№5 кесте. Бір ай ішінде өзгерістер енгізудің нысаналы көрсеткіштері

№	Көрсеткіш		Өтініштер саны
1.	Өзгертуге сұрау	Қызмет конфигурациясын өзгертуге байланысты өтінімдер (АҚ оқиғалары дереккөзін қосу/жою, сценарийді бейімдеу)	8-ден аспайды
2.	Ақпараттық сұрау	Қызмет бойынша консультациялық мәселелерге байланысты өтінімдер (Шарт бойынша сұрақтар және т.б.)	5-тен аспайды
3.	АҚ инцидентіне күдік	Тапсырыс берушінің АҚ инцидентіне күдігіне байланысты өтінім. Бастапқыда бұл өтінішке «төмен» басымдық беріледі. Қажет болған жағдайда Тапсырыс беруші басымдықты көтере алады. Осы сұрау түрі бойынша жұмыс №4 кестеге сәйкес жүргізіледі.	Шектеусіз

5.2. Ақпараттық қауіпсіздікті қамтамасыз етуге арналған техникалық талаптар.

Қызмет Өнім беруші ұсынатын технологиялық шешімнің негізінде көрсетілуге тиіс.

Көрсетілетін қызметтердің тиімділігі мен сенімділігін арттыру мақсатында шешім АҚ ахуалдық орталығының бірыңғай платформасы (бұдан әрі – Платформа) түрінде ұсынылуға тиіс.

Платформа ақпараттық қауіпсіздік оқиғаларын жинау, мониторингтеу және талдау жүйесінің, инциденттерді басқару мен автоматтандыру және қатерлерді талдау жүйесінің функционалын қамтуға тиіс.

Платформаға қойылатын функционалдық талаптар:

- Платформа SIEM, SOAR және Threat Intelligence функционалын бірыңғай интерфейсте және ортақ дерекқормен біріктіретін, бөгде құрамдастарды орнатуды немесе интеграциялауды қажет етпейтін бірыңғай интеграцияланған жүйе болуға тиіс.
- Платформа SIEM, SOAR және TI арасындағы деректердің кросс-корреляциясын коннекторларсыз қамтамасыз ете отырып, оқиғалардың, инциденттердің және қатер индикаторларының бірыңғай қоймасын қамтамасыз етуге тиіс.
- Платформа SIEM, SOAR немесе TI үшін жекелеген лицензияларды сатып алуды қажет етпейтін бірыңғай лицензиялау жүйесін қолдауға тиіс.
- Платформа TI талдамасы мен SIEM корреляция қағидалары арасындағы жіксіз интеграцияны қамтамасыз етуге тиіс, бұл қатерлердің жаңа индикаторларын анықтау қағидаларында автоматты түрде пайдалануға мүмкіндік береді.
- Платформа SOAR инциденттері мен SIEM оқиғалары арасындағы екіжақты синхрондауды нақты уақыт режимінде қолдауға тиіс.
- Платформа барлық құрамдастарды бірыңғай интерфейс арқылы орталықтандырылған жаңартуды және басқаруды қолдауға тиіс.
- Платформа көлденең масштабтау мүмкіндігі бар толық контейнерленген архитектурада (Docker/Kubernetes) жұмыс істеуге тиіс.
- Платформа Интернетке қолжетімділігі жоқ оқшауланған (air-gapped) желілерде орнатуды қолдауға тиіс.
- Платформада тұтастықты бақылаудың және әкімшілердің барлық әрекеттерін аудиттеудің кіріктірілген құралдары болуға тиіс.

- Платформа бөгде қосымшаларды, қосымша терезелерді, интерфейстерді немесе скрипттерді пайдалануды қажет етпей, өзінің барлық құрамдастары мен функционалын бірыңғай веб-интерфейс арқылы орталықтандырылған басқаруды қамтамасыз етуге тиіс.
- Платформа бөгде құралдарды пайдаланбай-ақ оқиғалар дереккөздерінің негізгі түрлерін автоматты түрде анықтауға тиіс.
- Платформа бапталатын дашбордтарды (dashboards) жасауды қолдауға тиіс.
- Платформа пайдаланушылардың есептік жазбалары мен олардың рөлдерін басқару функционалын ұсынуға тиіс.
- Платформада конфигурацияның резервтік көшірмесін автоматты түрде жасау тетігі болуға тиіс.
- Платформада өзін-өзі диагностикалаудың кіріктірілген құралдары болуға және ақаулар туындаған кезде пайдаланушыға хабарлауға тиіс.
- Платформа оның өндірушісі әзірлеген инциденттерге ден қою және оларды тергеп-тексеру процестерін үйлестіру және автоматтандыру модулін қамтуға тиіс.
- Платформа масштабталатын болуға және Тапсырыс берушінің инфрақұрылымына жаңа құрылғылар, кеңселер мен қосымшалар қосылған кезде функционалды кеңейтуді қамтамасыз етуге тиіс.
- Платформа оқиғаларды сақтау үшін таратылған дерекқорларды пайдалануды және оларға бірыңғай пайдаланушы интерфейсі арқылы қол жеткізуді қолдауға тиіс.
- Платформа өнімділік қорымен жұмыс істеуге және есептік мәндерден асатын қысқа мерзімді жүктеме шарықтауларына төтеп беруге тиіс.
- Платформа жиналатын және өңделетін деректердің тұтастығын қамтамасыз етуге тиіс.
- Платформа оқиғалар мен өрістердің кеңейтілген таксономиясын қолдап, пайдаланушыға оларға өз атауларын беру мүмкіндігін ұсынуға тиіс.
- Платформа пайдаланушы саясатына сәйкес оқиғаларды маңыздылық дәрежесі бойынша автоматты жіктеуді баптау мүмкіндігін беруге тиіс.
- Платформа деректерді айқын алуды, біріктіруді, сүзгілеуді, сұрыптауды және талдауды қамтамасыз етуге тиіс.
- Платформада деректерді қысқа мерзімді (online) және ұзақ мерзімді (offline) сақтауды қолдайтын оқиғалар журналдарын жинау және архивтеу модулі болуға тиіс.
- Платформа оқиғаларды жинаудың стандартты хаттамаларын қолдауға және техникалық мүмкіндік болған жерде деректерді агентсіз жинауды қамтамасыз етуге тиіс.
- Платформа тергеп-тексеру мен талдау жүргізу үшін оқиғалар туралы ұзақ кезеңдегі тарихи деректерге қолжетімділік беруге тиіс.
- Платформа әртүрлі құрылғылардан түсетін оқиғалар өрістерін қосымша баптаусыз автоматты түрде қалыпқа келтіруге тиіс.
- Платформа оқиғаларды алдын ала конфигурациялаусыз стандартты санаттауды қамтамасыз етуге тиіс.
- Платформа оқиғаларды кейіннен талдау үшін бастапқы және қалыпқа келтірілген түрде сақтауға тиіс.
- Платформа бастапқы баптауларда болмаған стандартты емес өрістерді өңдеп, қалыпқа келтіре алуға тиіс.
- Платформа оқиғаларды нақты уақыт режимінде де, пайдаланушы таңдаған уақыт кезеңдері бойынша да талдауды қамтамасыз етуге тиіс.
- Платформа пайдаланушы сүзгілері негізінде оқиғаларды жинау және талдау мүмкіндігін ұсынуға, сондай-ақ сұрау бойынша қосымша ақпарат алуды қамтамасыз етуге тиіс.

- Платформа оқиғаларды веб-интерфейс арқылы сүзгілерді лезде қолдану мүмкіндігімен нақты уақыт режимінде көрсетуге тиіс.
- Платформа оқиғалар бойынша пайдаланушыларға веб-интерфейс арқылы қолжетімді есептілікті қалыптастыруды қамтамасыз етуге тиіс.
- Платформа пайдаланушыларға есептілік параметрлерін дербес баптау және өз есептерін жасау мүмкіндігін беруге тиіс.
- Платформа графикалық интерфейсті пайдалана отырып, қалыпқа келтірілген және бастапқы деректер бойынша іздеу параметрлерін SQL-тәрізді сұрау тіліне түрлендіруді қамтамасыз етуге тиіс.
- Платформа корреляция қағидаларының санын кеңейтуді қолдауға тиіс.
- Платформа пайдаланушылар мен жалға алушылар арасындағы қолжетімділік құқықтарын ажырата отырып, көп жалға алушылықты (multitenancy) қамтамасыз етуге тиіс.
- Платформа қажет болған жағдайда қалыпқа келтірілетін өрістер санын ұлғайтуды қолдауға тиіс.
- Платформа MITRE ATT&CK, NIST және ISO/IEC 27035 әдіснамалары бойынша есептер мен визуалдауды қамтамасыз етуге тиіс.
- Платформа Тапсырыс берушінің Service Desk жүйесімен (мысалы, Jira) API арқылы интеграциялануды қолдауға тиіс.
- Платформа MITRE ATT&CK Framework талаптарына сәйкес типтік қатерлерді визуалдауды, сондай-ақ MITRE тактикалары мен техникалары бойынша қатерлерді анықтау қағидаларының қамту деңгейін бағалауды қамтамасыз етуге тиіс.
- Платформа лицензиялауға қосымша шығынсыз, деректерді берудің қорғалған хаттамаларын пайдалана отырып, қашықтағы желілерден оқиғаларды жинауға арналған құрамдастардың шектеусіз санын орнату мүмкіндігін қамтамасыз етуге тиіс.
- Платформа машиналық оқыту әдістерін қолданатын және бөлек лицензиялауды талап етпейтін мінез-құлықты талдау модулін (UBA) қамтуға тиіс.
- Платформада талданатын есептік жазбалар мен пайдаланушылар саны бойынша шектеулер болмауға, ал мінез-құлықты талдау модулі белсенділіктің кемінде 10 санатын қолдауға тиіс.
- Платформа жоғарыда аталған барлық модульдер мен құрамдастарды бірыңғай веб-интерфейс арқылы орталықтандырылған басқаруды қамтамасыз етуге тиіс.
- Платформа барлық құрамдастарды бірыңғай бағдарламалық образдан өрістетуді қамтамасыз етуге тиіс, бұл ретте қажетті функционал бөгде өндірушілердің қосымша бағдарламалық қамтылымын орнатуды немесе лицензиялауды қажет етпей, лицензия арқылы белсендірілуге тиіс.
- Платформа дереккөзден оқиғалар алынған сәттен бастап 1 секундтан аспайтын кідіріспен бірыңғай дерекқордағы деректердің өзектілігін және синхронды корреляциясын қамтамасыз етуге тиіс.
- Платформа барлық модульдерінің ақпаратты сақтауы мен өңдеуі үшін бірыңғай дерекқорды пайдалануға тиіс.
- Платформа техникалық мүмкіндік болған кезде оқиғаларды жинау үшін серверлер мен жұмыс станцияларына агенттер орнатуды қамтамасыз етуге тиіс.
- Платформа Тапсырыс берушінің ақпараттық инфрақұрылым көздерінен оқиғаларды (тіркеу журналдарын) Syslog хаттамасы бойынша агентсіз қабылдауды, өңдеуді және қалыпқа келтіруді қамтамасыз етуге тиіс. Платформа UDP және TCP хаттамалары арқылы деректерді қабылдауды, оның ішінде TLS пайдалану арқылы қорғалған түрде беруді қолдауға тиіс. Функционалдық мүмкіндік Қызметті баптау барысында оқиғаны ақпарат көзінен тестілік жіберу және оның Платформа интерфейсінде көрсетілуі арқылы тексеріледі.

- Платформа шарттың қолданылу мерзімі аяқталғаннан кейін Тапсырыс берушіге оқиғалардың архивтік дерекқорын және жедел қолжетімділік дерекқорын беруді, содан кейін Өнім беруші жағындағы деректерді толық жоюды қамтамасыз етуге тиіс.
- Платформа оқиғаларды корреляциялау мен ден қою әрекеттерін оркестрациялаудың бірыңғай қозғалтқышын пайдаланатын кіріктірілген SOAR модулін қамтуға тиіс.
- Платформа код жазуды қажет етпейтін визуалды құрастырғыш арқылы ден қою сценарийлерін (playbooks) жасауды қолдауға тиіс.
- Платформа анықталған инциденттер негізінде ахуалдық орталыққа арналған міндеттерді автоматты түрде қалыптастыруды және оларды рөлдер бойынша бағыттауды қамтамасыз етуге тиіс.
- Платформа Өнім беруші мен Тапсырыс берушінің қызметкерлеріне нақты уақыт режимінде хабарлау үшін мессенджерлермен және пошта жүйелерімен интеграциялануды қолдауға тиіс.
- Платформа талдаушы автоматты әрекеттерді мақұлдайтын немесе күшін жоятын «human-in-the-loop» сценарийлерін қолдауға тиіс.
- Платформа тіркелген ақпараттық қауіпсіздік инциденттерінің мәртебесі туралы нақты уақытқа жақын режимде өзекті ақпарат беруге тиіс.
- Платформа Тапсырыс берушінің кіріктірілген интерфейстер арқылы ақпараттық қауіпсіздік инциденттерін дербес тіркеу мүмкіндігін қамтамасыз етуге тиіс.
- Платформа өңделген және ағымдағы инциденттер туралы статистикалық деректерді интерактивті мониторинг панельдері (Dashboard) түрінде визуалдау функционалын ұсынуға тиіс.
- Платформа бекітілген өзара іс-қимыл регламентіне сәйкес Өнім беруші қалыптастыратын қолжетімді есептер мен хабарландыруларды пайдаланушылардың алуын қамтамасыз етуге тиіс.
- Платформа ақпараттық қауіпсіздік инциденттерін басқару және оларға ден қою процестерін, оның ішінде тіркеуді, жіктеуді, эскалациялауды, тергеп-тексеруді және жабуды автоматтандыруды қамтамасыз етуге тиіс.
- Платформа инциденттерді өңдеуге байланысты міндеттерді, оның ішінде ағымдағы мәртебені, орындау мерзімдерін және орындалу нәтижелерін бақылау мүмкіндігін қамтамасыз етуге тиіс.
- Платформа компрометация индикаторларын (IoC) және инцидентке байланысты өзге де объектілерді әртүрлі кейстер мен инциденттер арасында корреляциялау мүмкіндігімен мониторингтеуді қамтамасыз етуге тиіс.
- Платформа ден қоюдың техникалық, уақыттық және ұйымдастырушылық метрикаларын қоса алғанда, белгіленген көрсеткіштер бойынша есептер қалыптастыруды қамтамасыз етуге тиіс.
- Платформа IP-мекенжайларды, домендерді, зиянды файлдардың сигнатураларын және шабуыл сценарийлерін қоса алғанда, қатерлердің техникалық индикаторларын жинауды қамтамасыз етуге тиіс.
- Платформа ішкі сенсорлардан (XDR, EDR, SIEM), құмсалғыштардан, даркнет дереккөздерінен, инфрақұрылымнан және сыртқы фидтерден алынатын деректерді интеграциялауды қамтамасыз етуге тиіс.
- Платформа автоматты түрде жаңартылатын және қорғау жүйелеріне берілетін құрылымдалған Threat Intelligence Feeds (TI Feeds) қалыптастыру үшін бастапқы деректерді тазартуды, атрибуттауды және байытуды қамтамасыз етуге тиіс.
- Платформа индикаторлар, шабуылдаушылардың тактикалары, топтар және шабуыл мақсаттары арасындағы өзара байланысты белгілеуді қоса алғанда, талдаманы қалыптастыруды қамтамасыз етуге тиіс.

- Платформа SIEM, SOAR және басқа қорғау құралдарымен интеграциялану арқылы қатерлерді анықтауды, оларға ден қоюды және бұғаттауды автоматтандыруды қамтамасыз етуге тиіс.
- Платформа соңғы нүктені оқшаулауды, талдаушыларға хабарлауды және инциденттерді тергеп-тексеру мен талдауға арналған міндеттер жасауды қоса алғанда, нақты ден қою сценарийлерін іске асыруды қамтамасыз етуге тиіс.
- Платформаның құжаттамасы, интерфейсі және оқыту материалдары қазақ, орыс және ағылшын тілдерінде болуға тиіс.
- Платформа өндірушіден жергілікті техникалық қолдауға ие болуға тиіс.
- Платформа мемлекеттік тілді қолдауға және отандық әзірлеме болуға тиіс.

Әлеуетті өнім беруші тендерлік құжаттама шеңберінде Платформаға қолжетімділігінің бар екенін растайтын өндірушінің немесе оның Қазақстан Республикасындағы өкілдігінің авторизациялық хатын ұсынуға тиіс. Хат Тапсырыс берушінің атына сатып алу атауы мен Тапсырыс берушінің атауы көрсетіле отырып берілуге тиіс. Атаулар толық көрсетілуге тиіс. Хат мәтіні мемлекеттік немесе орыс тілінде ұсынылады.

Платформаның сапасы мен функционалын тексеру үшін өнім беруші өтінім құрамында Платформаға қол жеткізу сілтемелері көрсетілген ресми хат ұсынуға тиіс.

Платформаның сапасы мен функционалын тексеру үшін Әлеуетті өнім беруші тендерлік өтінім құрамында Платформаға сілтеме ұсынуға тиіс.

Шартқа қол қойылған күннен бастап 3 күнтізбелік күн ішінде Әлеуетті өнім беруші ұсынылатын шешімдердің осы техникалық ерекшелік талаптарына сәйкестігін растауға, сондай-ақ көрсетілген жүйелерді жеткізуге және сүйемелдеуге арналған рұқсат құжаттарын (өндірушінің немесе оның жергілікті өкілінің хатын) ұсынуға тиіс.

5.3. Желілік қауіпсіздікті қамтамасыз ету жүйесін ұсыну қызметіне қойылатын талаптар.

Жүйенің сипаттамасы:

Қызмет көрсету шеңберінде Өнім беруші Тапсырыс берушіге бағдарламалық шешімді тек ақпараттық қауіпсіздік қызметін көрсету мақсатында уақытша пайдалану құқығын береді.

Жүйе Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V «Ақпараттандыру туралы» Заңының 54-бабының 3-1-тармағына және Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» қаулысының 2-параграфының 29-тармағына сәйкес сенімді бағдарламалық қамтылым және электрондық өнеркәсіп өнімдері тізілімінде болуға тиіс.

Бағдарламалық қамтылым ҚР СТ ISO/IEC 15408-3-2017F талаптарына сәйкес сәйкестік сертификатына және сенімнің 4-бағалау деңгейіне ие болуға тиіс.

Конкурстық өтінім құрамында Өнім беруші сатып алу атауы мен Тапсырыс берушінің атауын көрсете отырып, Тапсырыс берушіге бағдарламалық қамтылымды пайдалану құқығын беру қызметін көрсетуге рұқсат ететін өндірушінің рұқсат хатын ұсынуға тиіс.

Жүйенің сапасын, функционалын тексеру және осы ерекшелік талаптарына сәйкестігін растау үшін Әлеуетті өнім беруші тендерлік өтінім құрамында бланкідегі хатпен жүйеге сілтеме мен есептік деректерді ұсынуға тиіс.

Желіаралық экран қауіпсіз желіаралық өзара іс-қимылды, Интернет ғаламдық желісі ресурстарының пайдаланылуын есепке алуды және бақылауды қамтамасыз етуге арналған.

Бағдарламаны пайдалану құқығы (лицензия) мына құқықтары бар жазылымды қамтуға тиіс:

- бағдарлама жаңартуларын алу (өнімнің жаңа нұсқаларын және сигнатура жаңартуларын алу мүмкіндігі);
- бағдарламаға техникалық қолдау алу;
- басып кіруді болдырмау модулін пайдалану (модульді пайдалану және оның жаңартуларын алу мүмкіндігі);
- қосымшаларды бақылау модулін пайдалану (модульді пайдалану және оның жаңартуларын алу мүмкіндігі);
- контентті сүзгілеу модулін пайдалану (модульді пайдалану және оның жаңартуларын алу мүмкіндігі).

Желіаралық экранның функционалдық, техникалық, сапалық және пайдалану сипаттамалары:

- Жұмыс параметрлері белгіленген шектерден шыққан кезде қызметтердің жұмысы бұзылуының алдын алатын жүйені тұрақты бақылау модулінің болуы
- Сервердің ақауға төзімді кластер режимінде жұмыс істеу мүмкіндігі
- Жүктеу кезінде жүйенің жабдықтың барлық параметрлерін, файлдық жүйе мен дерекқорлардың жай-күйін, сондай-ақ барлық өзгермейтін файлдардың бақылау сомасын тексеруі
- Бағдарламалық қамтылымның жаңа нұсқаларына уақтылы өтуге мүмкіндік беретін автоматты жаңарту жүйесі
- Барлық жүктелетін файлдарды электрондық цифрлық қолтаңбамен тексеру
- Әрбір пайдаланушыны логин мен құпиясөз бойынша WEB арқылы, VPN PPTP, IKEv2/IPSec, L2TP/IPSec, SSTP арқылы Интернетке кіруге авторизациялау, IP-мекенжай, MAC-мекенжай және IP + MAC бойынша сәйкестендіру
- VPN пайдаланушыларын RADIUS сервері арқылы аутентификациялау
- Терминал серверінің пайдаланушыларын прокси-сервер арқылы авторизациялау мүмкіндігі
- VPN арқылы авторизациялау кезінде трафикті тыңдаудан және IP-мекенжайды алмастырудан қорғауды қамтамасыз ету
- HTTPS, HTTP, SSH және RDP ресурстарын жариялау мүмкіндігі бар SSL VPN порталы
- Active Directory және Samba DC пайдаланушыларын синхрондау мүмкіндігі
- Kerberos хаттамасы бойынша ашық (Single Sign-On) авторизация
- Active Directory қауіпсіздік журналы арқылы сәйкестендіру
- Бірнеше тәуелсіз Active Directory доменімен интеграциялану мүмкіндігі
- Пайдаланушылар туралы барлық ақпаратты SQLite дерекқорында сақтау
- Әрбір пайдаланушы мен әрбір топтың егжей-тегжейлі статистикасын сақтау
- NetFlow коллекторына ақпарат беруге арналған NetFlow сенсоры
- NetFlow нұсқаларын қолдау
- Кез келген уақытта пайдаланушының немесе бүкіл топтың қандай Интернет ресурстарына кіргенін есеп түрінде қарау мүмкіндігі
- Интернет ресурстарына кіру статистикасын мегабайтпен жүргізу
- Контентті сүзгілеу модулінің жұмысын оқиғалар журналынан қарау мүмкіндігі
- Басып кіруді болдырмау, қосымшаларды бақылау және желіаралық экран модульдерінің жұмысын бірыңғай оқиғалар журналынан қарау мүмкіндігі
- Дерекқор мен конфигурациялық файлдардың резервтік көшірмесін жергілікті қоймаға автоматты түрде жасау және оларды FTP серверіне немесе ортақ SMB қалтасына жіберу жүйесі
- Серверді қайта жүктемей конфигурация саясаттарын қалпына келтіру мүмкіндігі

- Файлдық жүйе мен жүйелік командаларға толық қолжетімділікпен жергілікті консольден басқарудың кіріктірілген мүмкіндігі (оның ішінде сенімді желіден SSH хаттамасы бойынша қашықтан қол жеткізу)
- VPN арқылы Интернеттен қосылу және қашықтан басқару мүмкіндігі (IKEv2/IPsec, L2TP/IPsec, SSTP, PPTP)
- VPN пайдаланушыларына берілетін маршруттардан мекенжайларды алып тастау мүмкіндігі
- WEB интерфейсі арқылы әкімшілендіру үшін әкімшілерге әртүрлі рөлдер тағайындау мүмкіндігімен бірнеше әкімші есептік жазбасын пайдалану мүмкіндігі
- Microsoft AD және RADIUS серверінен әкімшілер топтарын импорттау мүмкіндігі
- VPN пайдаланушыларының әртүрлі топтарына әртүрлі ішкі желілерден IP-мекенжайлар беру мүмкіндігі
- Әкімшілер әрекеттерінің аудиті
- Интерфейстердің (жергілікті де, сыртқы да) шектеусіз санын қолдайтын маршрутизатор функциялары
- Виртуалды 802.1q VLAN интерфейстерін, PPTP және PPPoE интерфейстерін қолдау мүмкіндігі
- Loopback интерфейстерін қолдау
- Трафикті айнада көрсету үшін SPAN интерфейстерін жасау мүмкіндігі
- L2 және L3 деңгейлерінде WCCP хаттамасын қолдау
- Маршруттарды дереккөз бойынша көрсету мүмкіндігі (оның ішінде пайдаланушыларды немесе желілерді дереккөз ретінде пайдалану)
- OSPF және BGP хаттамалары бойынша динамикалық маршруттау
- Пайдаланушылардың әртүрлі провайдерлер арқылы Интернетке шығуын толық бөлу немесе арналар арасында трафикті теңгеру мүмкіндігімен бірнеше провайдер арнасын және бірнеше сыртқы желіні қолдау
- Өткізу қабілетін арттыру және сенімділікті жоғарылату үшін арналарды біріктіру мүмкіндігі
- Провайдермен байланысты автоматты түрде тексеру және қажет болған жағдайда балама провайдерге ауысу
- PPTP VPN, PPPoE және L2TP хаттамалары бойынша провайдерге қосылу мүмкіндігі
- Белгілі санаттардағы сайттарға қолжетімділікті басқаруға мүмкіндік беретін контент-сүзгі функциясын қосу мүмкіндігі
- Контент-сүзгідегі санаттар саны
- Контент-сүзгідегі URL мекенжайлар саны
- Жүктелетін файлдарды кеңейтімі бойынша сүзгілеу мүмкіндігі
- HTTP әдістері бойынша сүзгілеу мүмкіндігі (get, post, put, delete, head, options, patch, trace)
- Трафикті MIME түрлері бойынша сүзгілеу мүмкіндігі
- Тандалған санаттарға сұрауларды көрсетілген URL мекенжайына қайта бағыттау мүмкіндігі
- Сайт санаттарына сәйкес пайдаланушылар трафигі бойынша веб-есептілікті қалыптастыру мүмкіндігі
- Контент-сүзгінің HTTP және HTTPS трафигін шифрын ашып та, шифрын ашпай да (SNI мен сертификат деректерін талдау арқылы) сүзгілеу мүмкіндігі
- Сайттарға морфологиялық талдау жүргізу мүмкіндігі
- Контент-сүзгі дерекқорын автоматты түрде жаңарту мүмкіндігі
- NAT технологиясы мен қосылыстар күйін бақылайтын желіаралық экранды пайдалана отырып, компьютерлерді Интернет шабуылдарынан қорғау

- Белгіленген шарттар бойынша IP-мекенжайлар мен хаттамаларды бұғаттау мүмкіндігі
- IP-мекенжайларды олардың орналасқан жері бойынша бұғаттау мүмкіндігі (Geo IP)
- DoS шабуылдарынан қорғау және шамадан тыс белсенділікті бұғаттау
- DNAT (portmapper) технологиясы арқылы ресурстарды жариялау
- Мекенжайлар мен порттарды басқа мекенжайға ашық қайта бағыттау мүмкіндігі
- Бір немесе бірнеше интерфейсті қамтитын аймақтарды пайдаланып желіаралық экран қағидаларын жасау мүмкіндігі (Zone Based Firewall)
- Желіаралық экранда дереккөз портын көрсету мүмкіндігі
- FORWARD және INPUT кестелері қағидаларының жұмысын тексеру мүмкіндігі
- Арнайы кестенің шарттарына сәйкес келетін барлық трафикті желіаралық экран кестелерін қарағанға дейін бұғаттау мүмкіндігі (алдын ала сүзгілеу)
- SNAT үшін IP-мекенжайлар пулын пайдалану мүмкіндігі
- Трафикті MAC-мекенжайлар бойынша аппараттық сүзгілеу мүмкіндігі
- Белгілі бір қолданылу уақыты бар қағидаларды жасау мүмкіндігі
- Қызметкерлердің Интернет арқылы қорғалған арнамен қашықтан қосылу арқылы ішкі жергілікті есептеу желісіне қол жеткізу мүмкіндігі
- Барлық қашықтағы бөлімшелерді шифрланған IKEv2/IPsec хаттамасы бойынша бірыңғай платформада ортақ желіге біріктіру мүмкіндігі
- Қашықтағы бөлімшелерді ортақ желіге біріктіру үшін GRE туннелін жасау мүмкіндігі. Құрылғылар арасында IPsec пайдаланып шифрланбаған да, шифрланған да байланыс арнасын жасау мүмкіндігі.
- Пайдаланушылар мен топтар үшін Интернет ресурстарына өткізу жолағын шектеу мүмкіндігі (трафик шейпері)
- SYSLOG хаттамасы және CEF форматы бойынша SIEM жүйелерімен интеграциялану және TCP/UDP беру хаттамасын таңдау мүмкіндігін қамтамасыз ету
- SNMP хаттамасы бойынша мониторинг жүйелерімен интеграциялану мүмкіндігін қамтамасыз ету
- ICAP хаттамасы бойынша DLP жүйелерімен интеграциялану мүмкіндігін қамтамасыз ету
- Белсенді және пассивті екі режимде жұмыс істейтін кіріктірілген Zabbix агенті
- Пайдаланушыларды IKEv2/IPSec, PPTP, L2TP/IPSec және SSTP хаттамалары бойынша қосу мүмкіндігі бар VPN сервері; VPN серверіне қосылатын пайдаланушылардың екі факторлы аутентификациясын пайдалану мүмкіндігі
- Екі факторлы аутентификация үшін «Мультифактор» сервисімен интеграциялану мүмкіндігі
- Қауіпті трафик пен серверге жасалған шабуылдарды талдап, бұғаттайтын, бұғатталған трафик пен ескертулер туралы ақпаратты журналдарда кемінде үш ай сақтайтын басып кіруді болдырмау қызметін пайдалану мүмкіндігі; қызметтің сигнатуралар базасы әкімшінің қатысуынсыз автоматты түрде жаңартылады
- Басып кіруді болдырмау модуліне өз сигнатураларын қосу мүмкіндігі
- Қосымшалар трафигін шектеу мүмкіндігі бар қосымшаларды бақылау қызметін пайдалану мүмкіндігі
- Қосымшаларды бақылау қызметіндегі хаттамалар мен қосымшалар саны
- TУ АБЖ хаттамаларын анықтау мүмкіндігі (EtherSIO, FINS, HART-IP, Modbus, OPC-UA, UMAS)
- HTTP және HTTPS сайттарын жариялауға арналған кері прокси-сервер
- Кері прокси-сервер арқылы бірнеше серверге трафикті теңгеру

- Жарияланған веб-сайттарға жасалатын SQL Injection, XSS және басқа шабуылдарды бұғаттау мүмкіндігі бар веб-қосымшалар деңгейіндегі кіріктірілген желіаралық экранды пайдалану мүмкіндігі
- Басып кіруді болдырмау, қосымшаларды бақылау және веб-қосымшалар деңгейіндегі желіаралық экран қызметтері үшін әртүрлі профильдер жасау және қолдану мүмкіндігі
- Кері прокси-сервер жариялайтын ресурстар үшін DoS шабуылдарынан қорғауды қосу мүмкіндігі
- IGMP Proху қолдауы
- Forward DNS аймақтарын қолдау, жергілікті желіден DNS сұрауларын кәштеу, сыртқы DNS серверлеріне сұрауларды ұстап қалу және домендік атауларды кіріктірілген сервер арқылы мәжбүрлі түрде шешу мүмкіндіктері бар толық функционалды DNS сервері
- Динамикалық домендік атауларды (DDNS) қолдауды іске асыру
- Жергілікті желіде IP-мекенжайларды автоматты түрде таратуға арналған DHCP сервері
- DHCP арқылы еркін шлюзді және кез келген опцияларды беру мүмкіндігі
- IP-мекенжайды компьютердің MAC-мекенжайына тұрақты түрде байланыстыру мүмкіндігі
- DHCP клиенттеріне DNS, DNS суффиксін және WINS беру мүмкіндігі
- DHCP клиенттеріне маршруттар беру және берілген мекенжайларды жалға алуды мониторингтеу мүмкіндігі
- Берілген мекенжайларды жалға алуды мониторингтеу мүмкіндігі
- Әртүрлі интерфейстер мен VLAN үшін әртүрлі ауқымдарды көрсету мүмкіндігі
- DHCP-Relay режимінде жұмыс істеу мүмкіндігі
- Виртуалды контекстерді жасау мүмкіндігі: VCE / VDOM / VSX
- Пошта трафигін сүзгілеу мүмкіндігі бар пошта релесі
- IMAP және POP3 хаттамаларын қолдайтын пошта серверін баптау мүмкіндігі
- Кәдімгі браузер арқылы шифрланған арнамен әлемнің кез келген нүктесінен жеке поштамен жұмыс істеуге мүмкіндік беретін веб-интерфейсті баптау мүмкіндігі
- Орталық басқару консолі арқылы серверлер тобын орталықтандырылған басқару мүмкіндігі
- Процессор жұмысының үнемді режимін пайдалану мүмкіндігі
- Жергілікті желі құрылғыларының уақытын серверлермен синхрондауға арналған дәл уақыт NTP сервері
- Сыртқы серверлерге жіберілетін NTP сұрауларын ұстап қалуды қосу мүмкіндігі
- Веб-интерфейс тілін таңдау (орыс, ағылшын, қазақ)

Әлеуетті өнім беруші тендерлік құжаттама шеңберінде Платформаға қолжетімділігінің бар екенін растайтын өндірушінің немесе оның Қазақстан Республикасындағы өкілдігінің авторизациялық хатын ұсынуға тиіс. Хат Тапсырыс берушінің атына сатып алу атауы мен Тапсырыс берушінің атауы көрсетіле отырып берілуге тиіс. Атаулар толық көрсетілуге тиіс. Хат мәтіні мемлекеттік немесе орыс тілінде ұсынылады.

Платформаның сапасы мен функционалын тексеру үшін өнім беруші өтінім құрамында Платформаға қол жеткізу сілтемелері көрсетілген ресми хат ұсынуға тиіс.

Шартқа қол қойылған күннен бастап 3 күнтізбелік күн ішінде Әлеуетті өнім беруші ұсынылатын шешімдердің осы техникалық ерекшелік талаптарына сәйкестігін растауға, сондай-ақ көрсетілген жүйелерді жеткізуге және сүйемелдеуге арналған рұқсат құжаттарын (өндірушінің немесе оның жергілікті өкілінің хатын) ұсынуға тиіс.

5.4.Қосымша қызметтер

Сындарлы инциденттер бойынша компьютерлік криминалистика (форензика) қызметтері.

Рұқсатсыз қол жеткізуге, деректерді жоюға немесе өзгертуге, арнайы зиянды бағдарламалық қамтылымның енуі мен жұқтыру фактілерін анықтауға байланысты сындарлы инциденттерді тергеп-тексеру қызметін көрсету. Қызметтер шеңберінде желілік белсенділікті, логтарды және баптаулардағы өзгерістерді талдау, жойылған ақпаратты қалпына келтіру, шабуыл векторын іздеу және оқшаулау жұмыстары жүргізіледі.

6. Өзге ережелер

6.1.Қызметті тиісінше көрсету шарттары:

Өнім беруші төменде көрсетілген себептердің кез келгенінен туындаған, Қызмет көрсетудің үзілуіне әкеп соққан инциденттер мен өзге де мән-жайлар үшін жауапты болмайды:

- Тапсырыс берушіге хабарлай отырып, Қызмет көрсетуге қатысатын жабдықта жоспарлы және авариялық жөндеу жұмыстарын жүргізу;
- Тапсырыс берушінің Қызмет көрсету деңгейімен айқындалған мерзімде инциденттерді анықтау және жою кезінде Өнім берушіге жәрдем көрсетуден бас тартуы немесе жәрдем көрсетуге қабілетсіздігі;
- Тапсырыс берушінің осы Регламент талаптарына сәйкес Қызмет көрсету шеңберінде бағдарламалық қамтылымды немесе жабдықты баптауға қажетті деректерді 5 жұмыс күніне дейінгі мерзімде беруден бас тартуы немесе беруге қабілетсіздігі;
- Шартта айқындалған еңсерілмейтін күш мән-жайлары туындаған жағдайда.

Өнім беруші Тапсырыс берушіден шабуылды анықтау сценарийін іске асыруға қажетті ақпаратты (АТ-инфрақұрылым, ақпараттық активтер туралы) сұратуға, сондай-ақ жалған іске қосылуларды барынша азайту үшін осы ақпаратты пайдалануға құқылы. Өнім беруші Тапсырыс берушінің уәкілетті тұлғасына электрондық пошта арқылы сұрау жібереді; сұрауда өтініштің негізделген себебі көрсетілуге тиіс. Тапсырыс беруші осы сұрау бойынша 5 жұмыс күні ішінде кері байланыс береді, қажет болған жағдайда бұл мерзімдер түзетілуі мүмкін. Мынадай ақпарат сұратылуы мүмкін:

- DNS серверлерінің тізімі;
- қауіпсіздік сканерлерінің IP-мекенжайлары;
- Интернет желісінен қолжетімді ресурстар тізімі;
- Тапсырыс берушіге тиесілі ақ тізімдегі IP-мекенжайлар;
- ақпараттық жүйелер мен ресурстардың иелері;
- IP-мекенжайдың пайдаланушыға немесе жүйеге тиесілігі туралы ақпарат.

Шарт жасалғаннан кейін 15 (он бес) жұмыс күні ішінде Өнім беруші өзара іс-қимыл регламентін ұсынады, ал Тапсырыс беруші оны келіседі.

Ай сайынғы есептерді Өнім беруші есепті айдан кейінгі айдың 5 (бесінші) күнінен кешіктірмей ұсынады. Егер көрсетілген күн демалыс немесе мереке күніне сәйкес келсе, есеп осы күннің алдындағы жұмыс күнінен кешіктірмей ұсынылады. Тараптар қол қойған есептер көрсетілген қызметтер актісін ресімдеу және оған қол қою үшін негіз болып табылады.

Көрсетілген қызметтер актісі ай сайын ресімделеді.

6.2.Жоспарлы техникалық қызмет көрсету:

Өнім беруші Қызмет көрсетілетін кіші жүйелерге жоспарлы техникалық қызмет көрсетуі, оларды жаңартуы немесе жетілдіруі мүмкін. Бұл жұмыстар жоспарлы жөндеу жұмыстары ретінде айқындалады және Қызмет көрсетуде үзілістер тудыруы мүмкін. Жоспарлы жөндеу жұмыстары Тапсырыс берушімен келісілген Қызмет көрсетуді тоқтату кезеңінде жүргізіледі.

Өнім беруші Қызметтің жұмысында үзіліс тудыруы мүмкін кез келген жоспарлы жөндеу жұмыстары туралы Тапсырыс берушіге жұмыстар басталғанға дейін кемінде 1 (бір) күн бұрын хабарлауға міндетті. Жұмыстар Тапсырыс берушінің сұрауы бойынша орындалатын жағдайлар, сондай-ақ Өнім берушінің желісіндегі жоспарлы жөндеу жұмыстары мемлекеттік органдардың немесе Қазақстанның телекоммуникация саласындағы құзыретті органдарының талабы бойынша жүргізілуіне байланысты Өнім беруші көрсетілген мерзімді сақтай алмайтын жағдайлар бұған жатпайды.

Тапсырыс беруші қажет болған жағдайда жұмыстарды жүргізу мерзімдерін түзету жөніндегі ұсыныстарды жібереді, олар Өнім берушінің техникалық мүмкіндігіне қарай ескеріледі. Өнім берушіге жіберілетін хабарламада мыналар көрсетіледі:

- жоспарлы жөндеу жұмыстарын жүргізу уақыты;
- жоспарлы жөндеу жұмыстарын жүргізу күні;
- жоспарлы жөндеу жұмыстарының ұзақтығы;
- жүргізілетін жұмыстар туралы ақпарат беруге жауапты тұлғаның байланыс деректері;
- Тапсырыс беруші қызметкерлерінің жоспарлы жөндеу жұмыстарына, мысалы, Тапсырыс берушінің ақпараттық жүйесінің жұмыс қабілеттілігін тексеруге қатысу қажеттілігі туралы ақпарат.

Тапсырыс беруші жұмыстарға қатысу үшін жауапты қызметкерлерді бөлуге міндетті. Қызметкерді көрсетілген күні жұмыстарға тарту мүмкін болмаған жағдайда Тапсырыс беруші жұмыстарды жүргізу мерзімдерін түзету жөніндегі ұсыныстарды жібереді.

Жоспарлы жұмыстар жойылған кезде Өнім беруші шешім қабылданғаннан кейін мүмкіндігінше қысқа мерзімде Тапсырыс берушіге хабарлайды.

Тапсырыс беруші өзінің жабдығында қорғалатын ресурстардың уақытша қолжетімсіздігіне және соның салдарынан Қызмет көрсетудің үзілуіне әкелуі мүмкін кез келген жоспарлы жұмыстар туралы Өнім берушіге жұмыстар басталғанға дейін кемінде 1 (бір) тәулік бұрын хабарлауға тиіс.

Хабарламада жоспарлы жұмыстарды жүргізу уақыты, күні, ұзақтығы және жүргізілетін жұмыстар туралы ақпарат беруге жауапты тұлғаның байланыс деректері көрсетілуге тиіс.

Жоспарлы жұмыстарды жүргізу мерзімдері өзгерген кезде Тапсырыс беруші шешім қабылданғаннан кейін мүмкіндігінше қысқа мерзімде, бірақ жұмыстар басталғанға дейін кемінде 1 (бір) тәулік бұрын Өнім берушіге хабарлайды.

Тапсырыс берушінің немесе Өнім берушінің барлық хабарламалары уәкілетті өкілдердің электрондық мекенжайына жіберілуге тиіс.

6.3.Авариялық жөндеу жұмыстары:

Қызмет көрсетілетін кіші жүйелердің жұмысында мерзімді үзілістер байқалған немесе Қызмет сапасының параметрлері елеулі түрде нашарлап, бұл кейіннен авариялық жағдайға әкелуі мүмкін болған кезде авариялық жөндеу жұмыстары жүргізіледі.

Өнім беруші Тапсырыс берушіге авариялық жөндеу жұмыстарының жүргізілетіні туралы олар басталғанға дейін кемінде 4 (төрт) сағат бұрын хабарлауға тиіс.

Тапсырыс беруші өзінің жабдығында қорғалатын ресурстардың уақытша қолжетімсіз болуына және соның салдарынан Қызмет көрсетудің үзілуіне әкеп соғуы мүмкін кез келген авариялық жөндеу жұмыстары туралы Өнім берушіге жұмыстар басталғанға дейін кемінде 2 (екі) сағат бұрын хабарлауға тиіс.

Хабарламада мыналар көрсетілуге тиіс:

- авариялық жөндеу жұмыстарының басталу уақыты, күні және ұзақтығы;
- жүргізілетін жұмыстар туралы ақпарат беруге жауапты тұлғаның байланыс деректері;

- Тапсырыс беруші қызметкерлерінің авариялық жөндеу жұмыстарына қатысу қажеттілігі туралы ақпарат (Өнім беруші жұмыстар жүргізген кезде ғана).

Қызметтің құрамдас бөліктеріндегі негізгі жабдықты, оның функционалдық модульдерін, қосалқы бөлшектерді және қосымша лицензияларды сатып алуды немесе ауыстыруды талап етпейтін ақауларды Өнім беруші өз күшімен және өз қаражаты есебінен Қызмет құны шеңберінде жояды.

Тапсырыс берушінің жабдығында оны жою үшін жабдықты немесе оның функционалдық модульдерін ауыстыру, қосалқы бөлшектерді, қосымша лицензияларды сатып алу не жаңғырту жұмыстарын жүргізу қажет ақау анықталған жағдайда, Өнім беруші ақау анықталған сәттен бастап 1 (бір) жұмыс күнінен кешіктірмей Тапсырыс берушіге ақау актісін немесе техникалық қорытындыны ұсынады. Құжатта ақаудың сипаттамасы, болжамды себебі, қажетті жұмыстар мен материалдардың тізбесі, сондай-ақ ұсынылатын уақытша шаралар көрсетілуге тиіс.

Тапсырыс берушінің жабдығын жөндеу немесе ауыстыру туралы шешімді Тапсырыс беруші қабылдайды. Техникалық ерекшелікте және Шарттың құнында көзделмеген жұмыстар мен сатып алулар Қазақстан Республикасының мемлекеттік сатып алу туралы заңнамасына сәйкес бөлек мемлекеттік сатып алу рәсімін өткізу арқылы не өзге де заңды негізде жүзеге асырылады.

Өнім берушіге тиесілі не Қызмет көрсету үшін ол ұсынған жабдықты, бағдарламалық қамтамасыз етуді және өзге де құрамдастарды жөндеу және ауыстыру жұмыстарының көлеміне қарамастан, Өнім берушінің қаражаты есебінен орындалады және Қызмет құнына кіреді.

6.4.АҚЖО қызметін көрсету кезеңіндегі жауапкершілік аймақтары:

№7 кесте. Қызметтер кешеніне қатысушылардың жауапкершілік аймақтары.

№	Параметр	Тапсырыс беруші	Өнім беруші
АҚ оқиғаларын мониторингтеу және талдау қызметін көрсету			
1.1	Мониторинг аймағына кіретін Клиенттер инфрақұрылымының элементтеріне қатысты тіркелген АҚ оқиғаларын мониторингтеу және талдау (инциденттерге ден қою жөніндегі ұсынымдарды ұсынуды қоса алғанда).		+
1.2	Тапсырыс берушінің жабдығының жұмыс қабілеттілігін қамтамасыз ету, қалпына келтіру және мониторингтеу.	+	
1.3	Мониторинг аймағына кірмейтін Клиенттер инфрақұрылымының элементтеріне қатысты тіркелген АҚ оқиғаларын мониторингтеу және талдау.	+	
1.4	Тапсырыс берушінің алаңында да, Өнім берушінің алаңында да орнатылған АҚ оқиғаларын басқару кіші жүйесі құрамдастарының жай-күйін мониторингтеу.		+
1.5	АҚ оқиғаларын басқару кіші жүйесінің дұрыс жұмыс істеуін қамтамасыз ету.		+
1.6.	Логтарды жіберу үшін дереккөздерге агенттер орнату.	+	
1.7	Өнім берушінің ұсынымдарына сәйкес оқиғалар/ағындар коллекторларын және АҚ оқиғаларын басқару кіші жүйесінің өзге де инфрақұрылымдық элементтерін өрістетуге қажетті технологиялық қуаттарды ұсыну. Тиісті инфрақұрылымның ақауға төзімділігі мен қолжетімділігін қолдау.	+	
1.8	Дереккөздерден желілік ағындарды коллекторларға жіберу.	+	
1.9	Өнім беруші ұсынған ұсынымдарға сәйкес АҚ	+	+

№	Параметр	Тапсырыс беруші	Өнім беруші
	инциденттеріне ден қою, оларды оқшаулау, салдарын жою және штаттық жұмыс режимін қалпына келтіру.		
1.10	АҚЖО ұсынымдарын орындау және АҚ инциденттеріне уақтылы ден қою.	+	
1.11	Мониторинг аймағына кіретін серверлік, коммуникациялық және компьютерлік жабдықтың, сондай-ақ ақпараттық жүйелердің өзекті тізбесін ұсыну.	+	
1.12	Тапсырыс беруші мен Өнім берушінің алаңдары арасындағы қорғалған ақпарат беру арналарының жұмыс қабілеттілігін қамтамасыз ету.		+
1.13	Қайталама инциденттің туындау ықтималдығын болдырмау мақсатында Өнім берушінің ұсынымдарын қолдану.	+	
1.14	Мониторинг аймағындағы барлық өзгерістер туралы, оның ішінде жаңа желілік құрылғылар, IP-мекенжайлау, сыртқы авторизацияланған қосылыстар және т.б. туралы ақпаратты жедел ұсыну.	+	
1.15	Шарттың қолданылу кезеңінде Тапсырыс берушіден алынатын деректерді (оқиғалар, желілік ағындар) сақтау.	+	
1.16	«АҚ инциденттерін тергеп-тексеру бойынша кеңейтілген сараптама» қызметін пайдаланып толыққанды тергеп-тексеруді бастау жөнінде ұсыным беру.		+

7. Заңдармен және стандарттармен реттелетін талаптар

Қызметтер Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V «Ақпараттандыру туралы» Заңына (2024 жылғы 11 ақпандағы жағдай бойынша өзгерістермен және толықтырулармен), Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» қаулысына (2023 жылғы 25 ақпандағы жағдай бойынша өзгерістермен және толықтырулармен), сондай-ақ ISO/IEC 27001 «Ақпараттық технологиялар — Қауіпсіздікті қамтамасыз ету әдістері — Ақпараттық қауіпсіздікті басқару жүйелері» ақпараттық қауіпсіздік стандартының ұсынымдарына сәйкес көрсетілуге тиіс.

Тапсырыс берушінің деректері Қазақстан Республикасының аумағында орналасқан дерекқорларда сақталады (Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V «Дербес деректер және оларды қорғау туралы» Заңының 12-бабының талаптары, Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» қаулысы).

Қазақстан Республикасының 2015 жылғы 24 қарашадағы «Ақпараттандыру туралы» Заңының 7-2-бабының 2-тармағына сәйкес Әлеуетті өнім беруші Қазақстан Республикасының Ұлттық қауіпсіздік комитеті беретін «Ақпараттың таралып кетуінің техникалық арналарын және жедел-ізвестіру іс-шараларын жүргізуге арналған арнайы техникалық құралдарды анықтау жөніндегі қызметтерді көрсету» лицензиясы негізінде қызметті жүзеге асыруға тиіс және оны ұсынуға тиіс.

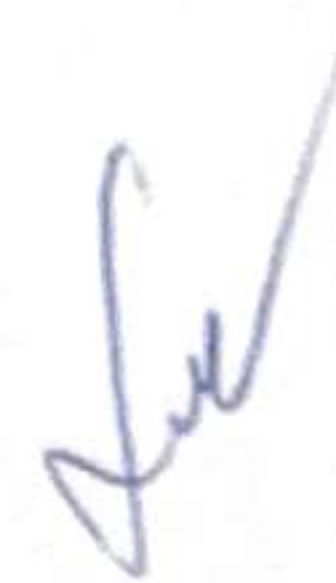
Ішкі бақылау басқармасының басшысы

Цифрландыру департаментінің басшысы

Жексембаев Е.К.

Альчимбаев А.Б.

Сатып алу және мониторинг департаментінің
басшысы



Бейсенова С.А.

Талап қою-шағым жұмысы басқармасы
басшысының міндетін атқарушы



Мадихан М.М.

Мониторинг басқармасының
басшысы



Кенесбеков Н.Н.