**Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер**

**техникалық ерекшелігі**

**(ТЖҚ БНА бойынша коды 801019.000.000010)**

|  |  |
| --- | --- |
| **№ р/с** | **Талаптар** |
| 1 | 2 |
| 1 | **Сатып алынатын тауарлардың, жұмыстар мен қызметтердің сипаттамасы** |
|  | Ақпараттық қауіпсіздікті басқару жүйесі (бұдан әрі – АҚБЖ) қызметтерін көрсетуді Қазақстан Республикасының ақпараттандыру саласындағы заңнамасына сәйкес ақпараттың жайылып кетуінің техникалық арналарын және жедел-іздестіру іс-шараларына арналған арнайы құралдарды анықтау жөніндегі қызмет көрсету туралы лицензияның негізінде өз қызметін жүзеге асыратын ақпараттық қауіпсіздіктің жедел орталығы (АҚЖО) жүзеге асырады.  Негізгі мақсаттары мен міндеттері:   * Мақсатты шабуылдарды анықтау және алдын алу үшін қазіргі заманғы қорғау механизмдерін енгізу; * Деректердің жайылып кетуін анықтау және алдын алу механизмдерін жетілдіру; * АТ-инфрақұрылымы мен сервистерінің қолжетімділігін арттыру; * «ҚТЖ» ҰК» АҚ-тың ақпараттық қауіпсіздік деңгейін арттыру; * Ақпараттық қауіпсіздік тәуекелдерін қысқарту және өзекті қатерлердің санын азайту; * Ақпараттық қауіпсіздік процестерінің толығуын арттыру, ақпараттық қауіпсіздік құралдарын интеграциялау және орталықтандыру; * Ақпараттық қауіпсіздік жүйелеріне орталықтандырылған бақылау жасауды, процестерді мониторингтеу мен қауіпсіздікті басқаруды жүзеге асыру үшін ақпараттық қауіпсіздіктің ахуалдық орталығын құру болып табылады. |
| 2 | **Сатып алынатын тауарлардың, жұмыстар мен қызметтердің талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары.** |
|  | Орындаушы ақпараттық қауіпсіздікті басқару жөніндегі қызметтер көрсету шеңберінде келесілерге міндеттенеді:  1. Тапсырыс берушіге бағдарламалық және аппараттық қамтамасыз етуді пайдалану құқығын бере отырып, шартқа қол қойылған күннен бастап 5 жұмыс күні ішінде енгізілетін қызметтер бойынша бағдарламалық/бағдарламалық-аппараттық сервистерді пайдалану құқығына лицензияларды орнатуды және іске қосуды жүргізуге.  2. АҚБЖ қызметін көрсету үшін берілген лицензияларға сәйкес жабдықтың және бағдарламалық жасақтаманың қауіпті деректер базасын жаңартуды және өзекті сипат беруді қамтамасыз етуге;  3. Енгізілетін қызметті «ҚТЖ» ҰК» АҚ-тың қолданыстағы және енгізілген жүйелерімен баптауға және интеграциялауға;  4. «ҚТЖ» ҰК» АҚ ақпараттық қауіпсіздік қызметі қызметкерлерінің сұрау салуы бойынша «ҚТЖ» ҰК» АҚ корпоративтік қауіпсіздік қызметі қызметкерлерімен келісе отырып, сондай-ақ олардың сұрау салуы бойынша бекітілген сервистік регламенттерге сәйкес АҚБЖ қызметінің баптаулары мен қауіпсіздік саясаттарына өзгерістер енгізуге;  5. «ҚТЖ» ҰК» АҚ АТ-инфрақұрылымының қауіпсіздігіне қатер төндіретін анықталған осалдықтар туралы «ҚТЖ» ҰК» АҚ жауапты қызметкерлерін хабардар етуге;  6. 24\*7 режимінде толық көлемде қызмет көрсету үшін қажетті техникалық мамандар бөлуге (24\*7 тәулік бойы режимінде бірінші желідегі 2 қызметкерден кем емес);  7. АҚБЖ қызметтерінің шеңберінде қажетті аппараттық және бағдарламалық жасақтаманы ұсынумен қатар АҚБЖ қызметінің мақсаттары мен міндеттерін орындау үшін мамандандырылған жүйелерді пайдалану және 1-кестеде келтірілген қызметтерді көрсетуге міндеттенеді:  **1-кесте:** АҚБЖ қызметтерін көрсету кезінде қолданылатын міндетті жүйелер мен қызметтердің тізбесі.   |  |  |  |  | | --- | --- | --- | --- | | **Жүйе атауы** | **Сыни көрсеткіші (1-5), 1-макс.** | **Сандық көрсеткіштер** | **Жылына Тапсырыс берушінің қызметкерлерін жүйемен оқытуға арналған ең аз сағат саны** | | Ахуалдық орталық қызметі (SOC) | 1 | 1 қызмет |  | | Оқиғаларды жинау және талдау жүйесі (SIEM) | 1 | Секундына 30 000 оқиға (EPS), максимал мән | 80 | | Активтер мен инциденттерді басқару жүйесі | 1 | 1 қызмет, 12 000 активтер үшін | 80 | | Желілік периметрді қорғау жүйесі және желі сегменттері арасындағы қол жеткізуді бақылау жүйесі (Firewall and network security) | 1 | 2 алаң:  A) Периметрлік: ыстық резервті (серверлік сегмент, клиенттік сегмент, DMZ) ұйымдастырумен интернет желісіне қосылу;  B) Ішкі: ыстық резервті ұйымдастырумен (серверлік сегмент, клиенттік сегмент).  VPN – 2 факторлы аутентификацияны пайдаланатын кемінде 5000 қосылым. | 160 | | Екі факторлы аутентификация | 1 | 1 қызмет (кемінде 5000 қосылым) |  | | Соңғы жұмыс станцияларын бақылаудың антивирустық жүйесі (Endpoint malware protection) | 1 | embedded жүйесі бар 1500 объектіні қоса алғанда, 18000 қорғалатын объект | 160 | | Таргеттелген шабуылға қарсы қорғау жүйесі (APT defense) | 1 | 1 қызмет | 160 | | Деректердің жайылып кетуін анықтау және алдын алу жүйесі (DLP); | 3 | 11 000 қорғалатын объектілер | 80 | | Желі трафигін және байланыс арналарын талдау жүйелері | 2 | 1 қызмет, корпоративтік орталық және 12 өңір үшін | 80 | | Почталық трафикті фильтрациялау жүйесі (Mail gateway) | 2 | 18 000 қорғалатын объектілер | 80 | | Осалдыққа сканерлеу жүйесі (Vulnerability scanner) | 4 | 1 қызмет | 80 | | Бастапқы кодты талдау жүйесі (Source code analyzer) | 4 | 1 қызмет | 80 | | Ерекше артықшылығы бар қолжетімділікті басқару және мониторингтеу жүйесі (PAM - Privileged Acccess Management) | 1 | Пайдаланушыларды шектеусіз 1000 ресурстар | 160 | | Ішіне кіруге тестілеу жүргізу (Penetration testing, pentest) | 5 | жылына 1 рет |  | | Пайдаланушының хабардар болуын арттыру қызметтері | 5 | 1 қызмет |  | | Компьютерлік криминалистика қызметтері (форензика) | 4 | 1 қызмет |  | | Консалтингтік қызметтер | 5 | 1 қызмет |  | | «Қызмет көрсетуден бас тарту» шабуылын тазалау жүйесі (Anti-DDOS) | 1 | Кемінде 5 ақпараттық ресурстар  Трафикті тазалау қуаты кемінде 5 Гбит/c | 80 | | Веб-қосымшалар трафигін фильтациялау (WAF) жүйесі | 1 | 1 қызмет, кемінде 5 ақпараттық ресурстар | 80 |   Ескерту: барлық жүйелерге қызметтерді тиімді көрсету үшін жеткілікті қажетті есептеу қуатымен қамтамасыз етуді Орындаушы жүзеге асырады, сондай-ақ аталған жүйелердің басқару орталықтары мен серверлерін Тапсырыс берушінің жергілікті желісінің шектерінде орналастыруды қамтамасыз ету қажет.  8. «ҚТЖ» ҰК» АҚ қызметкерлеріне сервистің ағымдағы жай-күйін және есептілігін көру, сондай-ақ қағидалар мен саясаттарды дербес баптауды орындау үшін сервистік қызметтерді басқару жүйелерінің интерфейсіне қолжетімділікті қамтамасыз етуге:   * Оқиғаларды жинау және талдау жүйесі; * Активтер мен инциденттерді басқару жүйесі; * Желілік периметрді қорғау және желілік сегменттер арасындағы қол жеткізуді бақылау жүйесі; * Соңғы жұмыс станцияларын бақылау жүйесі (вирусқа қарсы қорғау); * Таргеттелген шабуылдардан қорғау жүйесі; * Деректердің жайылып кетуін анықтау және алдын алу жүйесі; * Желілік трафикті және байланыс арналарын талдау жүйелері; * Почталық трафикті фильтрациялау жүйесі; * Осалдықтарды сканерлеу жүйесі; * Бастапқы кодты талдау жүйесі; * Ерекше артықшылығы бар қолжетімділікті басқару және мониторингтеу жүйесі; * Күдікті оқиғалар мен ақпараттық қауіпсіздік инциденттері туралы ақпарат алмасу жүйесі.   9. Апаттық жағдайда да жедел әрекет ету және Тапсырыс берушінің объектісіне бару үшін Орындаушының техникалық қолдау қызметі Астана қаласында орналасуы тиіс.  **2.3 Жалпы талаптар**  10. Орындаушы Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 қаулысымен бекітілген бірыңғай талаптарға, сондай-ақ «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы Заңының талаптарын сәйкес болуы тиіс.  11. Орындаушының Қазақстан Республикасының Ақпараттандыру туралы Заңының 7-2-баптарына сәйкес жедел-іздестіру іс-шараларын жүргізуге арналған ақпараттың жайылып кетуінің техникалық арналарын және арнайы техникалық құралдарды анықтау бойынша қызметтер көрсетуге қолданыстағы лицензиясы болуы тиіс.  12. Ақпаратты қауіпсіздіктің жедел орталығымен ақпараттың жайылып кетуінің техникалық арналарын анықтау бойынша қызметтерді көрсету әдістемесінің болуы.  13. Ақпаратты қауіпсіздіктің жедел орталығымен ақпараттың жайылып кетуінің техникалық арналарын және СТС анықтау бойынша көрсетілетін қызметтер туралы ай сайынғы/тоқсан сайынғы электрондық есепті ұсыну.  14. Оларда жұмыс істейтіндердің ақпараттық жүйелерге қолжетімділігіні дербес шектеу мүмкіндігі.   * 1. **SLA деңгейінің талабы**   15. Тапсырыс берушіге қызмет көрсету Тапсырыс берушімен алдын ала келісілген (кемінде 2 жұмыс күні) жоспарлы регламенттік жұмыстарды жүргізу уақытын қоспағанда, үздіксіз, күн тәулігіне 24 сағат ішінде толық көлемде жүзеге асырылады.  16. Орындаушы қызметінің қолжетімсіздігі мыналармен байланысты болуы мүмкін:   * Апаттық жағдаймен. * үзіліс басталғанға дейін кем дегенде 48 (қырық сегіз) сағат бұрын Тапсырыс берушімен келісілген, жиынтық ұзақтығы айына 8 (сегіз) сағаттан аспайтын жоспарлы регламенттік жұмыстармен. * Тапсырыс берушімен келісілген шұғыл жұмыстармен.   17. Қызметтер толық көлемде көрсетілмеген жағдайда (Инцидент) Тапсырыс беруші қызмет көрсетуге арналған өтінімдер мен сұрау салуларды келесі тәсілдердің бірімен Орындаушының Қолдау қызметіне (ServiceDesk) жібереді:   * Сұрау салуларды есепке алу жүйесі арқылы электрондық өтінімдер; * Белгіленген нөмірге телефон бойынша; * Электрондық почта арқылы.   Сұрау салу оны дұрыс тіркеу және орындау үшін қажетті ақпаратты қамтуы тиіс:   * Сұрау салу бастамашысының Т.А.Ә.; * Сұрау салу бастамашысының телефон нөмірі және корпоративтік электрондық почта мекенжайы; * Туындаған ақаудың сипаттамасы немесе қызмет көрсетуге немесе өзгертуге сұрау салу болған жағдайда орындауға қойылатын талаптардың сипаттамасы;   Сұрау салу келіп түскеннен кейін ServiceDesk қызметкерлері:   * Сұрау салуларды есепке алу жүйесінде сұрау салуды тіркеуге; * Ақпарат алмасуды жеңілдету үшін қолдау туралы әрбір сұрау салуға бірегей нөмір тағайындауға; * Сұрау салу басымдығын орнатуға; * Сұрау салуды орындауға кірісуге міндеттенеді.   Тіркеу ақпараты жеткіліксіз және (немесе) дұрыс болмаса, ServiceDesk сервисінің мамандарының:   * Қосымша ақпарат алу үшін Сұрау салу бастамашысына хабарласуға. * Сұрау салу бастамашысы сұрау салуды тіркеу үшін қажетті ақпаратты беруден бас тартса, сұрау салуды қабылдамауға құқығы бар.   Сұрау салуларды өңдеу уақыты және Тапсырыс берушінің сұрау салулары бойынша жұмыс уақыты түрге байланысты және 2-кестеге сәйкес анықталады.  **2-кесте.** Сұрау салуларды басымдық деңгейі және жауап беру уақыты бойынша жіктеу   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Сыни деңгейі** | **Жүйенің сыни көрсеткіші** | **Проблеманы сипаттау** | **Жою жұмыстарының басталу уақыты** | **Жою уақыты** | | 1-деңгей (Сыни қате) | 1 | Қызметтің – инфрақұрылымның функционалдығын айтарлықтай бұзуға әкеп соғуы мүмкін инциденттер, соның ішінде Тапсырыс берушінің бизнес-процестері жұмыс істемейтін болады. | 30 минутқа дейін | 1 сағатқа дейін | | 2-деңгей (Маңызды қате) | 1-2 | Клиенттің бизнес-процестері жұмыс істейтін, бірақ олардың жұмысы өте қиын немесе ақпараттық қауіпсіздік тәуекелі жоғары болатын инциденттер. Инциденттердің бұл түрлері жалпы алғанда клиенттің бизнес процесіне айтарлықтай теріс әсер етеді. | 1 сағатқа дейін | 4 сағатқа дейін | | 3-деңгей (Шағын қате) | 1-3 | Бизнес-процестердің функционалдығын ішінара жоғалтуға әкелетін инциденттер. Проблема жұмысқа ішінара ғана кедергі келтіреді, жалпы бизнес-процесс дұрыс жұмыс істеуін жалғастырады; | 3 сағатқа дейін | 12 сағатқа дейін | | 4-деңгей (Кеңес беру) | 1-4 | Ақпаратты жинау және талдау бойынша Тапсырыс берушіге қызмет көрсетуге арналған кез келген сұрау салулар; | 6 сағатқа дейін | 1 жұмыс күніне дейін | | 5-деңгей (Өзгерту мен пысықтау) | 1-5 | Конфигурацияларды өзгерту бойынша Тапсырыс берушіге қызмет көрсетуге арналған кез келген сұрау салулар | 24 сағатқа дейін | Тапсырыс берушінің келісімі бойынша |   Кестеде проблеманы шешу мерзімдері көрсетілген. Проблеманы шешумен айналысатын қызметкерлер шешімді мүмкіндігінше тезірек ұсынуы тиіс.  18. Орындаушы бұзушылықтың себептерін талдауға және SLA бұзылған жағдайда, SLA бұзушылығының қайталануын болдырмау үшін түзету шараларын әзірлеуге міндетті.  19. Орындаушы Тапсырыс берушіге апаттық жағдайды жойғаннан кейін 3 (үш) жұмыс күні ішінде жұмыстың аяқталғаны туралы актіні және апаттық жағдайды жою кезінде қабылданған шаралар туралы есепті ұсынуға міндетті.  20. Қызметтердің қолжетімсіздігі үшін және/немесе Техникалық қолдау көрсету мерзімінен асып кеткені үшін Тапсырыс берушіге барлық өтемақылар тиісті Есептік кезеңде Тапсырыс берушіге Есепті кезеңдегі қызметтерді көрсету құнынан шегерім түрінде ғана ұсынылады. Бұл ретте «Есепті кезең» деп Тараптар қызмет көрсету айы, «Қызметтердің қолжетімсіздігі кезеңінің басы», Өтінімді (хат, хабарлама немесе басқа құжат) алуды түсінеді. Тапсырыс берушіден Қызметтердің қолжетімсіздігінің басталу уақытын көрсететін «Қызметтің қолжетімсіздігі кезеңінің аяқталуы» деп Тараптар Орындаушының Өтінімді (Өтінімнің статусы – Орындалды) толтыру уақытын түсінуге келісті, ал «Техникалық қолдау көрсету мерзімінен асып кету» деп – Орындаушының Тапсырыс беруші таңдаған осы Келісімнің техникалық қолдау деңгейінде көзделген жауап беру немесе шешім қабылдау мерзімдерін бұзуы түсініледі.  21. Орындаушы 3-кестеге сәйкес Тапсырыс берушіге SLA бұзылу жағдайын өтеуге міндеттенеді.  **3-кесте.** Өтемақы түрлері мен мөлшері:   |  |  |  | | --- | --- | --- | | **Реакция уақытынан асып кетті** | **Орындау уақытынан асып кету** | **Өтемақы сомасы** | | 1 минуттан 2 сағатқа дейін | 1 минуттан 4 сағатқа дейін | Есепті кезең сомасынан 1% | | 2 сағат 1 минуттан 4 сағатқа дейін | 4 сағат 1 минуттан 8 сағатқа дейін | Есепті кезең сомасынан 3% | | 4 сағат 1 минуттан 6 сағатқа дейін | 8 сағат 1 минуттан 12 сағатқа дейін | Есепті кезең сомасынан 5% | | 6 сағат 1 минуттан 9 сағатқа дейін | 12 сағат 1 минуттан 1 сағатқа дейін | Есепті кезең сомасынан 7% | | 9 сағат 1 минут немесе одан да көп | 18 сағат 1 минут немесе одан да көп | Есепті кезең сомасынан 10% |   22. Тапсырыс беруші Орындаушының келісімінсіз баптауларды немесе конфигурацияларды өзгертуден туындаған қызметтердің қолжетімсіздігі және/немесе техникалық қолдау көрсету мерзімдерін асырғаны үшін Орындаушыға өтемақы талап етпейді және айыппұл салмайды.  23. Тапсырыс беруші тойтарылмас күш жағдайларының салдарынан туындаған қызметтердің қолжетімсіздігі және/немесе техникалық қолдау көрсету мерзімдерінің өтіп кеткені үшін Орындаушыдан өтемақыны талап етпейді және айыппұл салмайды. Көрсетілетін қызметтерге қойылатын функционалдық талаптарАхуалдық орталық (SOC) қызметі Ахуалдық орталықтың қызметі Орындаушыдағы ақпараттық қауіпсіздікті мониторингтеу жөніндегі бағдарламалық-аппараттық кешендер арқылы жүзеге асырыладыі.  Ахуалдық орталық қызметі келесі функцияларды қамтамасыз етуі тиіс:   * осы Шарттың шеңберінде ұсынылатын жүйелерде тіркелген ақпараттық қауіпсіздік оқиғаларының тәулік бойы мониторингтеу; * Орындаушының SIEM-жүйесіне (бұдан әрі – Мониторингтеу аймағы) қосылған Тапсырыс берушінің серверлік, клиенттік және желілік жабдықтарда, операциялық жүйелерде, ақпараттық жүйелерде және бағдарламалық жасақтамада тіркеліп жазылған ақпараттық қауіпсіздік оқиғаларын тәулік бойы мониторингтеу; * Жалған іске қосылуларды және күдікті оқиғалардың дубликаттарын (бұдан әрі – ЖО) алып тастау; * 24/7 режимінде қызмет немесе сыртқы көздер шеңберінде ұсынылатын жүйелерден қосымша деректермен ЖО туралы ақпаратты байыту; * Зиянды бағдарламалық жасақтама мен цифрлық артефактілерді талдауды қоса алғанда, инцидентке техникалық талдау жүргізу, ұсынымдар беру және инцидентке қашықтан, ал қажет болған жағдайда Тапсырыс берушінің алаңында ден қоюға қатысу; * Мониторингтеу аймағында орын алған ақпараттық қауіпсіздік инциденттерін анықтау; * Инциденттерге ден қою процесінде сараптамалық қолдау көрсету; * Артефакттарды жинау бойынша нұсқаулық пен бағдарламалық жасақтама; * Маңызды осалдықтар мен қауіптер туралы ақпарат беру; * Инциденттерді тергеп-тексеру шеңберінде жиналған артефактілерді беру үшін Орындаушыға тиесілі ресурсты ұсыну; * Ақпараттық қауіпсіздік инциденттерін тергеп-тексеру кезінде консультациялар беру; * Анықталған сыни осалдықтар туралы ақпаратты оларды жою бойынша егжей-тегжейлі ұсынымдармен Тапсырыс беруші қызметкерлерінің корпоративтік электрондық пошта мекенжайларына ұсыну; * Тапсырыс беруші үшін кем дегенде 10 бірегей шабуылды анықтау сценарийін әзірлеу; * Тапсырыс беруші оқиғаларының типтік көздеріне және жылына кемінде 5 типтік емес (бар болса) шектеусіз қосылу; * Тапсырыс берушінің ақпараттандыру объектілерінің Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының талаптарына сәйкестігіне талдау жүргізу; * Оқиғаларды жинау және талдау жүйесіне Тапсырыс берушінің көздерін қосу бойынша консультациялық көмек, ұсыныстар мен нұсқаулар беру; * Мониторингтеу аймағында егер Мониторингтеу аймағына кірмейтін жүйелерге қатысты күдікті оқиға анықталса - Тапсырыс берушіге бұл оқиға туралы хабарланады. Тапсырыс беруші одан әрі тергеуді өз бетінше жүзеге асырады; Орындаушы қажет болған жағдайда проблеманың көзін анықтау және Тапсырыс беруші мамандарына инцидентті шешуге көмектесу мақсатында маңыздылық дәрежесін анықтау және қосымша талдау бойынша кеңестер береді; * Қазақстан Республикасы заңнамасының талаптарына сәйкес НКЦИБ-пен өзара іс-қимыл жасау; * Деректер форматы келісілген жағдайда «Самұрық-Қазына» АҚ компаниялар тобының орталықтандырылған ақпараттық қауіпсіздік жүйесіне орын алған ақпараттық қауіпсіздік инциденттері туралы деректерді жіберу; * Келесі жаңа сценарийлерді және тиісті қағидаларды және шабуылды анықтау сигнатураларын әзірлеу:   + жеке аналитиканың негізінде Purple Teaming әдістерін қолдануды қоса алғанда, шабуылдау техникаларын, тактикаларын және рәсімдерін (TTP);   + Cyber ​​​​threat Intelligence жинау және талдау негізінде - CTI (CTI бойынша есептерді және шабуылдар туралы есептерді, сондай-ақ жаңа қауіптерді, осалдықтарды және зерттеулерді қоса алғанда, киберқауіпсіздік саласындағы жаңалықтарды жинау, өңдеу және талдау);   + Тапсырыс берушінің сұрау салуы бойынша; * Жалған мақсаттарды - ішкі және сыртқы «кибер-тұзақтарды» енгізу:   + Тапсырыс беруші сервистерінің цифрлық клондарын - стандартты және егжей-тегжейлі «кибер-тұзақтарын» құру және мониторингтеу;   + зиянкестердің белсенділігін анықтау және оған әрекет ету үшін «кибер-тұзақтарды» пайдалану;   + қорғалатын активтерге зиянткестердің қол жеткізуін периметрлік құрылғыларда автоматты түрде блоктау;   + Threat Intelligence:   + әшкерелеу индикаторларының сыртқы көздерімен интеграциялау (IoC);   + кибер-тұзақ инфрақұрылымына жасалған шабуылдарды талдау нәтижелері бойынша нақты уақыт режимінде әшкерелеу индикаторларын (IoC) анықтау;   + нақты уақыт режимінде әшкерелеу индикаторлары (IoC) болуының оқиғалары журналдарын талдау;   + әшкерелеу индикаторлары (IoC) болуының оқиғалары журналын мерзімді ретроспективті талдау;   + TI коммерциялық көздеріне (арналар, есептер және т.б.) қосылу мүмкіндігі (бөлек тариф бойынша); * Threat Hunting – нақты уақыт режимінде алдын ала қорғау құралдарымен және анықтау тетіктерімен анықталмаған Тапсырыс берушінің АТ-инфрақұрылымында әшкерелеу іздерін іздестіру:   + қолмен жұмыс режимінде Орындаушының талдаушыларымен;   + қауіпсіздік оқиғаларының автоматтандырылған ретроспективті корреляциясын қолдану;   + шабуылдарды анықтау және мамандандырылған сараптама жүргізу процесін оңайлату үшін өзара байланысты оқиғалардың күрделі тізбектерін визуалды қайта құруды қолдану; * Орындаушының SOC технологиялық платформасын әкімшілендіру (SIEM серверлері, оқиғаларды жинау және сақтау жүйелері, ақпараттық қауіпсіздіктің күдікті оқиғалары/инциденттері, кибер-тұзақтар туралы ақпарат алмасу жүйелері). * Анықталған инциденттер және оларға ден қою әдістері туралы ақпаратты Тапсырыс берушіге жіберу және SLA белгіленген мерзімдерде олардың таралуын тоқтату, ақпараттық қауіпсіздік инциденттерін жою және алдын алу бойынша ұсыныстар беру (2.5.1.1-бөлім). * Тапсырыс беруші АҚЖО қызметтерін пайдаланудан бас тартқан жағдайда немесе Шарттың қолданылу мерзімі аяқталғаннан кейін Орындаушы 14 күнтізбелік күн ішінде Орындаушы ресурстарында орналасқан барлық жинақталған деректерді (оқиғаларды, желі ағындарын) мұрағаттауы керек. Тапсырыс берушіге деректер мұрағатын қауіпсіз арна арқылы жүктеп алу немесе оны өзінің алынбалы тасымалдағышына көшіру мүмкіндігі берілуі керек. Мәліметтерді беру қабылдау-беру актісімен ресімделуі керек. Тапсырыс беруші берілген деректерді 3 (үш) жыл бойы сақтауға міндетті. Орындаушы Шарт тоқтатылғаннан кейін Тапсырыс берушінің деректерін өз ресурстарында 30 (отыз) күнтізбелік күн ішінде тегін сақтауға міндеттенеді. Мәліметтерді 30 (отыз) күнтізбелік күннен артық сақтау кезінде Тапсырыс беруші Орындаушының ресурстары туралы Тапсырыс берушінің ақпаратын сақтау мерзімі ішінде келісілген тарифтер бойынша Орындаушы қызметтерінің құнын төлейді. * Сұраныс болмаған жағдайда жинақталған деректер, оның ішінде мұрағатталған деректер Тапсырыс берушінің алдын ала хабардар болуы және ықтимал қатысуы бойынша күнтізбелік 45 (қырық бес) күннен кешіктірмей жойылатын болады.   + - 1. **Ахуалдық орталық (SOC) қызметтерін ұсыну деңгейінің мақсатты көрсеткіштері** * Ахуалдық орталық қызметін ұсыну деңгейінің мақсатты көрсеткіштері тек Тапсырыс берушінің көздерінен келіп түсетін оқиғаларға ғана қолданылады және 4-кестеге сәйкес анықталады.   4-кесте   | **№** | **Көрсеткіш** | **Сыни деңгейі** | **Орындаушының әрекет ету уақыты** | **Табель** | **Тапсырыс берушінің әрекет ету уақыты** | | --- | --- | --- | --- | --- | --- | |  | Орындаушының Тапсырыс берушінің SIEM-де тіркелген сәттен бастап, алғашқы талдау, жалған іске қосу белгісіне тексеру, санаттау жүргізгеннен кейін, алғашқы ден қою бойынша ұсынымдар бере отырып, ЖО/ ақпараттық қауіпсіздік инциденті туралы хабардар ету уақыты | 4 – сыни | 30 минут | 24х7 | Қолданылмайды | | 3 – Жоғары | 45 минут | 24х7 | Қолданылмайды | | 2 – Орташа | 2 сағат | 24х7 | Қолданылмайды | | 1 – Төмен | 6 сағат | 24х7 | Қолданылмайды | |  | Ақпараттық қауіпсіздік инцидентін Тапсырыс беруші растаған сәттен бастап ақпараттық қауіпсіздік инцидентіне қарсы іс-қимыл бойынша ұсынымдар беру | 4 – Сыни | 1 сағат | 24х7 | Қолданылмайды | | 3 – Жоғары | 2 сағат | 24х7 | Қолданылмайды | | 2 – Орташа | 4 сағат | 24х7 | Қолданылмайды | | 1 – Төмен | 18 сағат | 24х7 | Қолданылмайды |  * ЖО/инциденттің сыни деңгейі 5-кесте бойынша анықталады.   **5-кесте. ЖО/Ақпараттық қауіпсіздік инцидентінің сыни деңгейлері**   | **Сыни деңгейі** | **Сипаттама** | | --- | --- | | |  | | 4  (Critical - Сыни) | Нәтижесінде жүйенің/жүйелердің әшкереленуімен байланысты Тапсырыс берушінің бизнес-процестері жұмысқа қабілетсіз болған немесе Тапсырыс берушіге айтарлықтай зиян келтірілген сыни ресурспен байланысты инцидент | | 3  (High - Жоғары) | Жүйенің/жүйелердің әшкереленуіне немесе Тапсырыс берушіге зақым келтіруге әкелуі мүмкін немесе әкелетін ЖО немесе инцидент. Клиенттің бизнес-процестері жұмыс істейді, бірақ олардың жұмысы өте қиын немесе ақпараттық қауіпсіздік қаупі жоғары. Инциденттердің бұл түрлері жалпы алғанда клиенттің бизнес процесіне айтарлықтай теріс әсер етеді. | | 2  (Medium - Орташа) | Жүйенің/жүйелердің әшкереленуіне немесе Тапсырыс берушіге шектеулі зақым келтіруге әкелуі мүмкін немесе әкелетін сыни емес ресурстармен байланысты ЖО немесе инцидент. Проблема жұмысқа ішінара ғана кедергі келтіреді, жалпы алғанда бизнес-процесс дұрыс жұмыс істеуін жалғастырады. | | 1  (Low - Төмен) | Сәтсіз шабуыл әрекеті, қорғау құралдарымен тоқтатылған шабуылды куәландыратын не болмаса Тапсырыс берушінің инфрақұрылымын барлау кезеңін көрсететін ЖО. |  * ЖО-ға ден қою уақытын есепке алу осы уақытқа әсер ететін жағдай Орындаушының жауапкершілік аймағынан тыс болған кезде тоқтатылады, мысалы, байланыс арналарындағы ақаулар, Тапсырыс беруші бақылайтын оқиғаларды жеткізу жүйелерінің серверлерінің ақаулары және т.б. * Тапсырыс беруші Орындаушыны ЖО/инцидентке ден қоюдың жай-күйі туралы 5-кестеде көрсетілген мерзімдерде хабарлайды. * Тапсырыс беруші 5 жұмыс күні ішінде ЖО/инцидентке жауап берудің түпкілікті нәтижесі туралы Орындаушыға хабарлайды, осыдан кейін Орындаушы өз тарапынан ЖО-ны автоматты түрде жабуға құқылы (егер Тапсырыс беруші Шарттың мерзімін ұзарту туралы дәлелді өтініш алмаса) жауап беру мерзімі 5 жұмыс күні ішінде). * SLA «Threat Hunting» сценарийіне қолданылмайды (Threat Hunting принципінің өзі Тапсырыс берушінің АТ-инфрақұрылымында профилактикалық қауіпсіздік шараларымен анықталмаған компромисс іздерін жартылай автоматты және қолмен іздеуді көздейтіндіктен және нақты уақытта анықтау механизмдері).      * + - 1. **Мониторингтеу қызметінің шеңберінде SLA орындалу деңгейін есептеу.** * SLA орындау сапасын жалпы бағалау мақсатында Орындаушы жыл сайын «SLA сәйкестік деңгейі» көрсеткішін есептейді. * Орындаушы Тапсырыс берушінің бағдарламалық жасақтамасы мен жабдығының кез келген ақаулары үшін, соның ішінде Тапсырыс беруші Мониторингтеу аймағына енгізілген көздерді конфигурациялау кезінде орын алған, сондай-ақ Орындаушы өз бетінше жұмыс істейтін жағдайды қоспағанда, Қызметті көрсету кезінде туындаған ақауларға жауапты емес. оның мамандарын пайдалана отырып, Тапсырыс берушінің АЖ бойынша жұмыс жүргізді (мысалы, брокерлерді баптау және басқару кезінде). Бұл ретте Орындаушы көздерден оқиғалар журналдарын жинау үшін Орындаушы ұсынған мониторингтеу платформасы мен бағдарламалық жасақтаманың дұрыс жұмыс істеуін қамтамасыз ету үшін консультациялық көмек көрсетуге өз құзыреті шегінде бар күш-жігерін салады. * Қызмет көрсету кезінде Орындаушы тек 4-кестеде көрсетілген көрсеткіштер шеңберінде ғана жауапты болады. Инцидентке ден қою және АЖ функционалдығын қалпына келтіру бойынша тікелей жұмысты Тапсырыс беруші жүргізеді және Тапсырыс берушінің АЖ-ның кез келген істен шығуы немесе тоқтап қалуы SLA есептеуге ешқандай әсер етпейді. * Ақпараттық қауіпсіздік оқиғаларының тәулік бойы мониторингтеу қызметін есептеу келесі формула бойынша жүзеге асырылады:   Тәулік бойы мониторингтеу қызметін орындау деңгейі = = ((R-S)/R)\*100%  , мұндағы   * R – тәулік бойы мониторингтеу арқылы анықталған маңызды және жоғары басымдықтағы күдікті оқиғалардың саны; * S – 5-кестеге сәйкес көрсетілген мерзімде өңделмеген маңызды және жоғары басымдықтағы күдікті оқиғалардың саны. Шекті бағалау көрсеткіші 100%-ды құрайды. * Қызмет көрсету деңгейі мәлімделген 99,5%-дан төмендесе, Тапсырыс беруші 6-кестеге сәйкес айыппұл санкцияларын қолдануға құқылы.   **6-кесте**   |  |  | | --- | --- | | **SLA % мәні** | **Салынатын айыппұл деңгейі SLA қолданылу кезеңіндегі төлем сомасынан пайызбен алынады** | | 98-99,(4)% | 0,3%-ға дейін | | 95-97,(9)% | 0,5%-ға дейін | | 95%-дан кем | 1%-ға дейін |    Оқиғаларды жинау және талдау жүйесі Қауіптердің алдын алу, оқиғаларды анықтау және оларға нақты уақыт режимінде әрекет ету мақсатында ұйымдағы ақпараттық қауіпсіздік оқиғаларын сенімді және жедел басқаруды қамтамасыз ету.  Тапсырмалар:  Қауіпсіздік оқиғалары туралы мәліметтерді орталықтандырылған жинауды және талдауды қамтамасыз ету.  Қауіпсіздік оқиғаларын автоматты түрде анықтау және жіктеу.  Оқиғаға қарсы әрекет етудің автоматтандырылған процестерін енгізу.  Нормативтік талаптарға және киберқауіпсіздік стандарттарына сәйкес келу.  Негізгі функционалдық талаптар  - Ақпараттық қауіпсіздік оқиғаларын жинау, өңдеу және корреляциялау Тұтынушыда орналастырылған ақпараттық қауіпсіздік оқиғаларын басқару (SIEM) жүйесі арқылы орындалуы керек.  - Жүйе үшінші тарап қосымшаларын, қосымша интерфейстерді, терезелерді немесе сценарийлерді іске қосуды қажет етпей, бір веб-интерфейс арқылы оның барлық компоненттері мен функционалдығын орталықтандырылған басқаруды қамтамасыз етуі керек;  - Жүйе деректерді автоматты түрде импорттауды қамтамасыз етуі керек: Басқа өнімдермен дайын интеграциялар. Бірнеше минут ішінде әртүрлі көздерден деректерді автоматты түрде импорттау мүмкіндігі.  - Әр түрлі деректер пішімдерін қолдау: кез келген түрдегі құрылымсыз деректер.  - Жүйе SOC (Security Operations Center) және NOC (Network Operations Center) іске асыруларында пайдалану үшін пайдаланушы интерфейсі арқылы бақылау тақталарын бөлу мүмкіндігін қолдауы керек;  - Жүйе пайдаланушы тіркелгілерін және олардың рөлдерін басқарудың икемді процесін қамтамасыз етуі керек;  - Жүйе компоненттер арасындағы байланысты шифрлай алуы керек;  - Жүйе конфигурацияларды Интернетте немесе ұйымның жергілікті желісінде орналасуы мүмкін жаңарту серверінен автоматты түрде жүктеп алу арқылы жүйе пайдаланушысы тарапынан қосымша уақыт шығынынсыз автоматты жаңартуды қамтамасыз етуі керек. Мысалы, жеке жүйелер мен үшінші тарап өндірушілерінің құрылғылары үшін қалыпқа келтіру модульдері мен қосқыштарын жаңарту;  - жүйе ақауларға төзімді архитектураны жүзеге асыру мүмкіндігін қолдауы керек;  - Жүйе жүйенің кез келген бөлігі істен шыққан жағдайда жүйенің жеке құрамдастарының жұмысына кепілдік беруі керек. (Мысалы, орталық консоль істен шығады, бірақ журнал жинағыштары жұмысын жалғастырады);  - Жүйеде конфигурацияның автоматты сақтық көшірме жасау процесі (Сақтық көшірме жасау) және графикалық пайдаланушы интерфейсінен конфигурацияны қалпына келтіру (қалпына келтіру) мүмкіндігі болуы керек;  - Жүйеде оның күйін талдау және проблемалар туындаған кезде пайдаланушыны хабардар ету үшін кірістірілген процесс болуы керек;  - Жүйе қажет болған жағдайда Жүйені өндірушіден инциденттерге ден қою және тергеу процестерін үйлестіру және автоматтандыру үшін ішкі жүйені енгізу мүмкіндігін қамтамасыз етуі керек;  - жүйе оңай масштабталатын және ұйымның талаптарын қанағаттандыру үшін функционалдық мүмкіндіктерін кеңейтуі керек (жаңа құрылғыларды, кеңселерді, тұтынушы желісіне қосымшаларды қосқанда);  - Жүйе оқиғаларды іздеу және тергеу мүмкіндігін сақтай отырып, шығындарды азайту үшін ыстық, жылы және суық деректерге бөлу арқылы деректерді ұзақ мерзімді икемді сақтауды қамтамасыз ете алуы керек.  - Жүйе деректерді жергілікті серверлерде, жалпыға қолжетімді бұлттарда және гибридті нұсқада бөлек сақтау және іздеу мүмкіндігі болуы керек.  - Жүйе өнімділік резервімен орналастырылуы және берілген жүйе үшін жобалық жүктемелерден асатын қысқа мерзімді жүктеме шыңдары кезінде жұмыс істеуі керек;  - жүйе жиналған ақпараттың тұтастығын қамтамасыз етуі керек;  - Жүйе барлық коллекторлардан корреляция үшін бөлінген үлгіні қолдауы керек. (Мысалы, 25 сәтсіз аутентификация әрекеті үшін, 25 оқиға 1 коллекторға емес, бірнешеге келгенде);  - Жүйе оқиғалар мен өрістер үшін кеңейтілген пайдаланушы таксономиясын қолдауы керек. Пайдаланушы оқиғаларға кез келген атауларды тағайындай алуы керек;  - Жүйе пайдаланушының қалауына сәйкес оқиғаларды маңыздылығы бойынша автоматты түрде белгілеу арқылы мінез-құлықты өзгерту мүмкіндігін қамтамасыз етуі керек;  - Жүйеде SOAR функциясы болуы керек.  - Жүйе жүйенің барлық таратылған құрамдас бөліктері бойынша мөлдір қабылдауды, жинақтауды, сұрыптауды, сүзуді және деректерді талдауды қамтамасыз етуі керек;  - Жүйе осы мүмкіндіктерді белсендіру үшін қосымша лицензияларды сатып алуды қажет етпей, оқиғалар журналдарын сыртқы жадта сақтауды қолдауы керек;  - Жүйе оқиғалар журналдарын жинаудың стандартты әдістерін қолдауы керек (мысалы, syslog, WMI, JDBC, SNMP, Checkpoint LEA және т.б.);  - Жүйе мүмкіндігінше оқиғалар журналдарын агентсіз жинауды қолдауы керек;  - Жүйе оқиғалар журналдарын сақтауды және оларды Жүйенің архитектурасында өңдеуді тарату мүмкіндігі болуы керек;  - Жүйе одан әрі тергеулер үшін ұзақ уақыт кезеңіндегі (мысалы, 12 ай) оқиғалар туралы барлық ақпаратқа қол жеткізуді қамтамасыз етуі керек;  - Жүйе стандартты оқиға өрістерін (пайдаланушы аттары, IP мекенжайлары, хост атаулары, оқиға көзі құрылғылары) көп жеткізушілер желісіндегі әртүрлі құрылғылардан қалыпқа келтіруі керек. Нормалау қосымша параметрлерсіз жүзеге асырылуы керек (қораптан тыс);  - Жүйе алдын ала қосымша баптауларсыз оқиғалардың стандартты категорияларын қамтамасыз етуі керек;  - Жүйе оқиғалар туралы ақпаратты өзінің бастапқы түрінде де, әрі қарай тергеуде пайдалану үшін нормаланған түрінде де сақтай алуы керек;  - Жүйе бастапқыда қолдау көрсетілмейтін және қораптан тыс параметрлермен қамтамасыз етілмеген өрістердегі деректерді өңдеу және қалыпқа келтіру мүмкіндігі болуы керек;  - Жүйе нақты уақыт режимінде оқиғаларды талдауды қамтамасыз етуі керек;  - жүйе белгілі бір уақыт аралығындағы оқиғаларды талдауды қамтамасыз етуі керек;  - Жүйе пайдаланушы орнатқан сүзгілерді пайдаланып оқиғаларды жинау және талдау мүмкіндігін қамтамасыз етуі керек;  - Жүйе қажет болған жағдайда оқиғалар туралы қосымша ақпарат алу мүмкіндігін қамтамасыз етуі керек (бұрғылау);  - Жүйе сүзуді қамтамасыз етуі керек, сонымен қатар пайдаланушы саясаттар мен сүзгілерді дереу қолдана алатын интерфейс арқылы оқиғаларды нақты уақыт режимінде көрсетуі керек;  - Жүйе барлық оқиғалар туралы есеп беруді қамтамасыз етуі керек, есеп беру шешімді пайдаланушылар үшін веб-интерфейс арқылы қолжетімді болуы керек;  - Жүйе пайдаланушыға есептілікті дербес конфигурациялауға және өз есептерін құруға мүмкіндік беруі керек;  - Жүйе қосымшаларды/интеграцияларды орнату арқылы өзінің функционалдығын кеңейте алуы керек, оларды жүйе өндірушісі растауы керек;  - Жүйе ES|QL сұрау тілін қолдауды қамтамасыз етуі керек;  - жүйе корреляциялық ережелердің санын (мысалы, жаңа қауіптерді анықтау үшін), есептер мен жүйе өндірушісі тексеруі тиіс қосымшаларды/интеграцияларды орнату арқылы кеңейте алуы керек;  - Жүйе көрсетілген пайдаланушылар үшін деректерге қол жеткізуді және жасыру (маскировка) шектеу мүмкіндігімен көптендікті қолдауы керек;  - Жүйе қосымшаларды/интеграцияларды орнату арқылы жүйемен қалыпқа келтірілген өрістер санын көбейте алуы керек, оны жүйе өндірушісі тексеруі керек;  - Жүйе алдын ала анықталған анықтау ережелерін қамтамасыз етуі керек: MITER ATT&CK негізіндегі кемінде 800 алдын ала анықталған анықтау ережелерінің болуы  - Жүйе пайдаланушыға MITER ATT & CK Framework сәйкес белгілі тактикалар мен әдістердің қауіпті анықтау ережелерін қамту деңгейін бағалауға мүмкіндік беруі керек;  - Жүйе «кодты» пайдаланбай өзіңіздің анықтау ережелеріңізді жасау мүмкіндігін қамтамасыз етуі керек.  - Жүйе үшінші тараптың қауіпті анықтау арналарын (Threat Intelligence) қоса алуы керек. Оларды шабуылдарды, соның ішінде тарихи контекстте анықтау үшін пайдаланыңыз  - Жүйе ықтимал қауіптерді анықтау мақсатында корреляция ережелері бойынша әрі қарай талдау үшін веб-интерфейс арқылы оқиғаларды қолмен жүктеп алу мүмкіндігін қамтамасыз етуі керек;  - Жүйе жалпыға ортақ желілер арқылы қосылу мүмкіндігімен қауіпсіз деректерді беру хаттамаларын пайдалана отырып, қашықтағы желілерден оқиғаларды жинауды қамтамасыз ету үшін қосымша лицензиялық шығындарды қажет етпейтін компоненттердің шектеусіз санын орнату мүмкіндігін қамтамасыз етуі керек;  - Жүйе күрделі модельдер мен қауіптерді анықтау алгоритмдерін құру процесін жеңілдету үшін корреляция ережелерінің, корреляция ережелерінің топтары мен динамикалық тізімдердің өзара әрекеттесуінің диаграммасы түріндегі графикалық талдау және визуализация мүмкіндігін қамтамасыз етуі керек;  - Жүйе аномалиялар мен белгісіз қауіптерді анықтау үшін машиналық оқыту алгоритмдерін пайдалануды қолдауы керек;  - Жүйе пайдаланушының өзінің машиналық оқыту үлгілерін пайдалану мүмкіндігін қолдауы керек;  - Жүйе пайдаланушы әрекетінің мінез-құлық талдауының функционалдығын қамтамасыз етуі керек (UBA);  - Мінез-құлықты талдау модулі машиналық оқыту үлгілерін пайдалануы және қосымша лицензиялауды қажет етпеуі керек;  - Мінез-құлықты талдау модулінде қызметі талдауға болатын тіркелгілер мен пайдаланушылар санына шектеулер болмауы керек;  - Жүйе үшінші тараптың AI қосу мүмкіндігін қолдауы керек.  - Жүйе қосылған оқиғалар көздері туралы ақпарат негізінде қосымша қолданбаларды/интеграцияларды орнату бойынша ұсыныстар жасауы керек;  - Жүйе DNS деңгейінде қауіптерді анықтау мүмкіндігін қамтамасыз етуі керек (домендік атауларды генерациялау алгоритмдерін (DGA) пайдалану, деректерді DNS сұраулары арқылы беру (DNS Tunneling), қосалқы домендік атауларға қол жеткізу әрекеттерін анықтау (DNS Squatting)). DNS серверлерінен, прокси-серверлерден немесе BIND технологиясын қолдайтын басқа жүйелерден алынған деректер;  - Жүйе бір веб-интерфейс арқылы жоғарыда аталған барлық компоненттерді және олардың функционалдығын орталықтандырылған басқаруды қамтамасыз етуі керек;  - Жүйе бірыңғай дерекқорда жиналған және өңделген деректердің өзектілігіне кепілдік беруі керек - жүйе оқиғалар көзінен деректерді алғаннан кейін 1 секундтан аспайтын кешіктірумен оқиғалар журналынан (журналдардан) мәліметтерді өңдеуді және корреляциясын қамтамасыз ету;  - Жүйенің жоғарыда аталған барлық құрамдас бөліктері ақпаратты сақтау және өңдеу үшін бірыңғай деректер қоры болуы керек.  Интеграция талаптары  - Деректер көздерімен интеграция: желілік құрылғылар (маршрутизаторлар, коммутаторлар, желіаралық қалқандар); серверлер мен жұмыс станциялары (соның ішінде Microsoft OS, Linux/Unix және т. қолданбалар мен мәліметтер базасы (соның ішінде SAP, Web, Oracle, MySQL және т.б.); басқа қауіпсіздік жүйелері (IPS, IDS, DLP және т.б.); интеграцияға арналған стандартты хаттамаларды қолдау (LDAP, Netflow, J-Flow, S-Flow Syslog, SNMP, API, WMI, JDBC, Checkpoint LEA және т.б.); стандартты емес журнал пішімдері үшін өзіңіздің жеке талдаушыларыңызды жасау мүмкіндігі.  Оқыту және қолдау талаптары  - Жүйені пайдалану бойынша қызметкерлерді оқыту: негізгі және жоғары деңгейлі.  - Жүйенің жұмысы кезінде техникалық қолдау көрсету.  - Жүйе үшін жаңартулар мен қауіпсіздік патчтарын жеткізу.  Лицензиялау талаптары  - Лицензиялау үлгісі (1-кестеде көрсетілген EPS көлемін жазуға және өңдеуге мүмкіндік беретін деректер көлеміне немесе көздер санына немесе секундтағы оқиғалар санына негізделген).  - Негізгі өнімді ауыстырусыз жүйенің функционалдығын кеңейту және кеңейту мүмкіндігі, соның ішінде. қосымша коллекторларды орналастыру арқылы.   * + 1. **Активтер мен инциденттерді басқару жүйесі**   Жүйе келесі компоненттерді қамтуы керек:  - ақпараттық қауіпсіздікті басқарудың орталық сервері;  - мәліметтер базасының сервері;  - Коллектор(лар).  Жүйені басқарудың орталық сервері активтермен жұмысты, осалдықтарды, ақпараттық қауіпсіздік инциденттерін, тәуекелдерді, аудиттерді, визуализацияны және есептерді қалыптастыруды, сондай-ақ Жүйенің басқа модульдерімен өзара әрекеттесуді қоса алғанда, Жүйенің негізгі функцияларын іске асыруды қамтамасыз етуі тиіс.  Жүйе коллекторы АТ-инфрақұрылымының жекелеген сегменттерін түгендеуді, соның ішінде бағдарламалық қамтамасыз етудің осал тұстарын іздеу үшін сканерлеуді және ақпаратты негізгі серверге(лерге) беруді, әртүрлі байланысты ақпараттық жүйелермен және ақпараттық қауіпсіздік жүйелерімен интеграцияны қамтамасыз етуі керек, сондай-ақ техникалық жауап беру функцияларын жүзеге асыру мүмкіндігі,  Жүйе қосымша үшінші тараптың коммерциялық бағдарламалық құралын, соның ішінде ДҚБЖ пайдалануды немесе сатып алуды қамтымауы керек.  Жүйе архитектурасы оның құрамдас бөліктерін бірнеше сайттарға/есептеу ресурстарына орналастыру мүмкіндігін қамтамасыз етуі және Тұтынушы желісінің әртүрлі сегменттерінде орналасқан жабдықпен біріктірілуі керек.  Тұтынушы басқаратын жұмыс станциялары Пайдаланушының және Әкімшінің жұмыс станциялары ретінде пайдаланылуы тиіс.  Функцияға қойылатын талаптар  Ақпараттық қауіпсіздікті басқарудың орталық ішкі жүйесіне қойылатын талаптар  Ішкі жүйені басқару әдістері мен құралдарына, сондай-ақ ішкі жүйе модульдері арасында ақпарат алмасуға қойылатын талаптар  Ішкі жүйенің құрамдас бөліктері арасындағы үйлесімділік, сондай-ақ оның Тұтынушы басқаратын және біріктіру үшін қолжетімді өзара байланысты телекоммуникациялық және автоматтандырылған жүйелермен үйлесімділігі қамтамасыз етілуге ​​тиіс.  Ішкі жүйені пайдаланушылар арасындағы өзара әрекеттестік графикалық веб-интерфейс арқылы жүзеге асырылуы керек.  Бағдарлама құрамдас бөліктер арасында қауіпсіз деректерді тасымалдау протоколдарын пайдалануды қолдауы керек.  Ішкі жүйе ішкі жүйе құрамдастарын Интернетке қосылмай жергілікті жаңарту мүмкіндігін қамтамасыз етуі керек.  Ішкі жүйені диагностикалауға қойылатын талаптар  Жүйені диагностикалау аудит журналдарында қызмет көрсету оқиғалары мен ақаулар туралы ақпаратты жазу арқылы орындалуы керек. Журнал жазбаларында ақаулықтың себебін анықтау үшін жеткілікті ақпарат болуы керек. Жүйе құрамдастарының журналдарын бақылау серверіне syslog протоколы арқылы жіберу мүмкіндігі болуы керек.  Ішкі жүйені масштабтау  Ішкі жүйе пайдаланылатын аппараттық кешеннің қосымша құрамдастарын қосу және лицензияны ұзарту арқылы өнімділік пен өңделген ақпарат көлемін масштабтауды қамтамасыз етуі керек. Масштабтау кезінде ішкі жүйе коммерциялық ДҚБЖ қоса алғанда, үшінші тараптың қосымша коммерциялық бағдарламалық құралын пайдалануды қамтымауы керек.  Ақпаратты рұқсатсыз кіруден қорғауға қойылатын талаптар  Ішкі жүйе келесі функцияларды қолдауы керек:  • Пайдаланушылардың авторизациясы мен аутентификациясын қамтамасыз ету.  • Ішкі жүйелерді көрші АЖ немесе ақпараттық қауіпсіздік жүйелеріне қосу үшін пайдаланылатын аутентификация деректері ішкі жүйеде шифрланған түрде сақталуы керек.  • Рөлге негізделген қол жеткізу үлгісінің болуы, ішкі жүйе пайдаланушыларының белгілі бір функционалды блоктарға қол жеткізуін шектеу мүмкіндігі.  • API ішкі жүйесі арқылы жұмыс істеу үшін таңбалауышты пайдаланып пайдаланушы авторизациясы. Токенді пайдалана отырып, пайдаланушы өзінің тіркелгісінде көрсетілген құқықтармен API ішкі жүйесі арқылы жұмыс істей алады.  Орталық басқару кіші жүйесінің активтерді басқару модуліне қойылатын талаптар  Түгендеу функционалдығына қойылатын талаптар  • Соңғы хосттарда жұмыс істейтін WMI, WinRM, SMB немесе VBS сценарийлерін пайдаланып Windows хосттарын түгендеу мүмкіндігі.  • Соңғы хосттарда жұмыс істейтін SSH, SNMP немесе bash сценарийлері арқылы Linux хосттарын түгендеу мүмкіндігі.  • SSH немесе SNMP протоколы арқылы қосылу арқылы желілік жабдықты түгендеу мүмкіндігі (OID MIB-II қолдайтын жабдық инвентаризацияланған).  • Жабдықтың техникалық параметрлері мен қауіпсіздік параметрлерін қоса алғанда, негізгі түгендеу ақпаратын жинаңыз.  • Келесі функцияларды қоса алғанда, объектілерді түгендеу жиілігін орнату арқылы түгендеу саясатын құру мүмкіндігі:  o IP мекенжайларының/желілердің/құрылғы атауларының ерікті диапазондарын сканерлеу;  o құрылғы атаулары бойынша хосттарды және АТ активтер топтарын сканерлеу;  o сканерлеуден IP мекенжайларын/желілерді/құрылғы атауларын алып тастау;  o сканерлеу аймағын орнату мүмкіндігі - барлық жабдық немесе тек жаңа нысандар;  o әрбір саясат үшін шоттардың тізімін көрсету мүмкіндігі;  o Есептік жазбасыз сканерлеуге арналған «Анықтау» режимі;  o сканерлеу параметрлерін конфигурациялау мүмкіндігі;  o Интерфейстегі сканерлеу журналы мен күйді қараңыз.  o TCP/UDP порттарының берілген диапазоны үшін ашық порттар туралы ақпаратты жинау.  Сыртқы жүйелермен интеграцияға қойылатын талаптар  • Вирусқа қарсы қорғаныс жүйелерімен интеграция:  o Түйіндер туралы инвентарлық ақпаратты импорттау.  • Басқа жүйелермен интеграция:  o Active Directory-мен интеграцияның болуы. AD жүйесінде тіркелген пайдаланушылар туралы ақпаратты, жабдықты, құрылымдық элементтер туралы ақпаратты - құрылымдық бөлімшелер туралы немесе АТ активтерінің топтары туралы ұйымдық бірлік AD немесе пайдаланушы/жабдық атрибутынан импорттаңыз. Жүйеге жабдықтың немесе AD пайдаланушыларының импортталған қосымша атрибуттарының теңшелетін тізімі;  o актив деректерін импорттау үшін файлдармен әмбебап интеграцияны құру мүмкіндігі. xlsx, csv, json, xml пішіміндегі файлдардан ақпаратты импорттауды қолдау. Excel файлдарынан импорттау кезінде жабдықты доменге байланыстыру мүмкіндігі: жүйе дерекқорда доменнің бар-жоғын тексереді: егер мұндай домен бар болса, доменде болмаса, жүйе жабдықты осы доменге автоматты түрде байланыстырады; дерекқор, жүйе жаңа домен қосады және оған жабдықты байланыстырады;  o мәліметтер базасымен әмбебап интеграцияның болуы: Microsoft SQL Server, Oracle, PostgreSQL, MySQL. Келесі актив түрлерін импорттау: жабдық, ұйым, бизнес-процестер, ақпарат, АТ активтер топтары, желілер, персонал, үй-жайлар, сондай-ақ реттелетін активтер түрлері. Жабдықты сыртқы дерекқорлардан импорттау кезінде жабдықта орнатылған бағдарламалық құрал туралы тиісті ақпаратты Жүйеге импорттау қажет.  • Келесі функцияларды қолдайтын интеграциялық дизайнердің болуы:  o өз кезегінде Python бағдарламалау тілін пайдаланып кез келген активтерді импорттай алатын теңшелетін интеграцияны құру;  o негізгі параметрлерді конфигурациялау үшін біріктіру үлгілерін пайдалану мүмкіндігі;  o қажет болса, біріктіру сценарийін іске қосу үшін виртуалды ортаны конфигурациялау мүмкіндігі, стандартты әдепкі виртуалды ортаға қосылмаған кітапханаларды жүктеңіз.  • Сыртқы жүйелермен біріктіру кестесін орнату мүмкіндігі.  • Жүйені «донорлық жүйе» - «реципиент жүйесі» үлгісіне сәйкес Жүйенің басқа қондырғысымен стандартты интеграциялау мүмкіндігі. Интеграцияның бөлігі ретінде келесі деректер синхрондалады:  o Активтер бөліміндегі каталогтар: Тегтер, Пайдаланушы каталогтары, Актив сипаттамасы өрістері, Жабдық күйлері, Жабдық түрлері, Бағдарламалық құрал топтары;  o Жалпы бөлімнен анықтамалық: Орындар;  o актив түрлері үшін: АТ активтер топтары, Жабдық, Персонал, Желілер, Бизнес бөлімшелер, Бизнес-процестер, Үй-жайлар;  o АТ активтерінің топтарын санаттау арқылы.  Активтерді есепке алу талаптары  • Материалдық және материалдық емес активтерді және олардың өзара байланыстарын есепке алу (бизнес-процестер, ақпарат, желілер, жабдықтар, үй-жайлар, персонал, бөлімдер, АТ активтерінің топтары, пайдаланушы активтері).  • Бірнеше сыртқы көздермен біріктіру кезінде актив деректерін қалыпқа келтіріңіз және қайталаңыз.  • Актив туралы жалпы ақпаратты, жауапты тұлғалар мен байланысты активтер тізімін, байланысты оқиғалар мен қосымша ақпаратты, сондай-ақ кез келген байланысты актив үшін картаны бөлек терезеде көру мүмкіндігін қамтитын актив карталарын ұстаңыз.  • Активті басқа жүйе нысандарымен байланыстыру мүмкіндігі (қолмен немесе автоматты түрде):  • жүйеде конфигурацияланған басқа түрдегі активтер (бизнес-процестер, ақпарат, АТ активтерінің топтары, жабдық, құрылымдық бөлімшелер, персонал, бағдарламалық қамтамасыз ету, пайдаланушы активтері және активтердің басқа түрлері);  • қарапайым қосылу немесе иерархиялық принципке негізделген бір типті активтер (АТ активтерінің топтары, жабдық және пайдаланушы активтері сияқты активтер үшін);  • тапсырмалар (бизнес-процестер, АТ активтерінің топтары, жабдық, құрылымдық бөлімшелер, пайдаланушы активтері сияқты активтер үшін);  • оқиғалар (бизнес-процестер, ақпарат, АТ активтерінің топтары, жабдық, құрылымдық бөлімшелер, персонал, бағдарламалық қамтамасыз ету сияқты активтер үшін);  • осалдықтар (осалдықтар туралы статистиканы көрсету мүмкіндігі бар жабдық түрінің активтері және АТ активтері топтары үшін және ауырлық деңгейі бойынша, жабдық түрі бойынша, эксплуатацияның болуы бойынша, порттар бойынша, қолжетімділік векторы бойынша сүзгіден өткізу);  • талаптар (бизнес-процестер, АТ активтерінің топтары, жабдықтар, құрылымдық бөлімшелер, үй-жайлар сияқты активтерге);  • аудиттер (бизнес-процестер, АТ активтерінің топтары, жабдықтар, құрылымдық бөлімшелер, үй-жайлар сияқты активтер үшін);  • құжаттар (бизнес-процестер, АТ активтерінің топтары, жабдық, құрылымдық бөлімшелер, үй-жайлар, ақпарат, бағдарламалық қамтамасыз ету, желілер, персонал, пайдаланушы активтері сияқты активтер үшін).  • Активтің әрбір түрін бөлек қойындыда ұстау мүмкіндігі (жабдық, персонал, бағдарламалық қамтамасыз ету, үй-жайлар және т.б.).  • Активтер тізімімен жұмыс істеу мүмкіндігі:  o жабдықтар мен персонал тізімдері бар кестелер арқылы іздеу;  o тізімді әрбір актив түрі үшін кез келген өріс бойынша сұрыптау;  o әрбір актив түрі үшін тізімді бір немесе бірнеше өрістер бойынша сүзу;  o пайдаланушының тізім сүзгісін сақтауы;  o активтер тізімі үшін көрсетілетін өрістерді орнату;  o берілген сүзгіге сәйкес активтерді көрсетудің бірнеше режимдерін құру және олардың арасында жылдам ауысу (Жүйенің әрбір жергілікті пайдаланушысы үшін).  o негізгі және еншілес активтерді жылдам сәйкестендіру мүмкіндігімен сызықтық тізім түрінде де, иерархиялық құрылым түрінде де активтер тізімдерін (бөлімшелер, үй-жайлар, бизнес-процестер, АТ активтерінің топтары, бағдарламалық қамтамасыз ету, желілер) көрсету;  o активтерді топтық жою.  • Жеке карта өрістері бар өзіңіздің (арнаулы) актив түрлерін жасау және мұндай активтер үшін дисплей белгішесін таңдау мүмкіндігі. Пайдаланушы активтері мен активтердің басқа түрлерімен байланыс орнату мүмкіндігі.  • Бірдей адрестелген желілердегі жабдықтарды автоматтандырылған есепке алу мүмкіндігі. Мекенжай кеңістігінің қажетті санын жасау және олар бойынша барлық қайталанатын желілерді тарату мүмкіндігі.  • Теңшелетін ережелер арқылы түйін түрін автоматты түрде анықтау.  • Осы топтың түйіндерін қамтитын АТ активтерінің топтарына желілерді автоматты түрде байланыстыру.  • Конфигурацияланған ережелерге сәйкес бағдарламаларды топтарға автоматты түрде қосу мүмкіндігі. Бағдарламалық жасақтама топтары үшін ерекше жағдайларды конфигурациялау мүмкіндігі. Бағдарламалық құрал атауы бойынша топтастырылуы керек және бір топтың бірнеше элементтерін өңдеу мүмкіндігі болуы керек.  • Активтердің критикалық дәрежесін түс схемасы түрінде көрсету.  • Тиісті сипаттама өрістерін толтыра отырып, АТ активтерінің топтарын санаттауды басқару мүмкіндігі (процесті басқару жүйесі, GIS, CII, ISPDn және т.б.). Жеке өрістер жинағы бар АТ активтері топтарының жеке санаттарын жасау мүмкіндігі.  • Өзгерістер көзіне қарамастан (пайдаланушы, интеграция) пайдаланушы интерфейсінде активтермен әрекеттер тарихын (қосу, өзгерту, жою) жүргізу.  • Пайдаланушыларды электрондық пошта арқылы немесе активтердегі жазылған өзгерістер туралы хабарландыру тақтасындағы қалқымалы терезеде хабарлау мүмкіндігі (жаңа жабдықты табу, жаңа ашық аппараттық портты, жаңа бағдарламалық құралды немесе пайдаланушыны табу, жаңа осалдықтарды, жаңа желілерді, осалдықтарды жою, жабдықтың жоғалғаны туралы хабарлау (жабдықты жою), АТ активтерінің жаңа тобын табу, пайдаланушы активін құру/өзгерту/жою, түйіннің инвентарлық күйінің өзгеруі).  • Үлгі арқылы желілер, жабдық, АТ активтерінің топтары, бөлімдер, үй-жайлар, қызметкерлер, бизнес-процестер және пайдаланушы активтері туралы Excel файлдарынан деректерді қолмен импорттау мүмкіндігі. Жүйе файлдан активтерді импорттау кезінде қажетті өрістердің толтырылғанын тексеруі керек.  • Бағандардың, қолданылатын сүзгілердің және сұрыптаулардың ағымдағы параметрлерін ескере отырып, актив деректерін .xlsx кестесіне экспорттау мүмкіндігі.  • Құпиялылық, тұтастық және қолжетімділік параметрлері, сондай-ақ оларды өңдеу негізінде актив құнының бастапқы бағасын (АТ активтерінің тобы, бизнес-процестер, ақпарат сияқты активтер үшін) жүргізу мүмкіндігі.  Өрістерге және актив карталарына қойылатын талаптар  • Келесі өріс түрлерін қосу мүмкіндігімен активтің әрбір түрі үшін актив карталарын бөлек құрастыру мүмкіндігі: ашылмалы тізім, күн, бірнеше мәтін жолдары, мәтін өрісі, құсбелгі ұясы, сандық өріс, валюта белгісі бар сандық өріс , пайдаланушы таңдауы (жүйе пайдаланушыларының тізімінен пайдаланушыны таңдау мүмкіндігі), IP мекенжайы/желі мекенжайы. Дизайнер берілген актив түріне арналған картадағы өрістер жиынтығы мен ретін теңшеуге мүмкіндік беруі керек.  • IP мекенжайы/желі мекенжайы сияқты мәтіндік өрістер мен өрістер үшін тұрақты өрнекті тексеруді конфигурациялау мүмкіндігі  • «Күн» түріндегі кез келген өрістердің жарамдылық мерзімін интерфейсте көрсету және хабарламаларды жіберу арқылы бақылау мүмкіндігі: пошта арқылы да, хабарландыру тақтасында да.  • Актив өрістерін топтық өңдеу мүмкіндігі.  • Жабдық картасында түгендеу күйін көрсететін, түгендеу қатесінің сипаттамасын немесе оның сәтті аяқталу күйін қамтитын өрістің болуы.  • Географиялық картада активтер мен қатысты инциденттер мен осалдықтар туралы ақпаратты көрсету үшін пайдаланылатын активті орналасу каталогындағы елді мекенге немесе нысанға байланыстыру мүмкіндігі бар орынды көрсету үшін актив картасында өрістің болуы.  Өмірлік циклге қойылатын талаптар  • Ұйымда көрсетілген процедураларға сәйкес активтің күй үлгісін енгізу мүмкіндігі.  • Ақпараты белгілі бір уақыт аралығында жаңартылмаған персонал түріндегі активтерді және жүйе жабдығын автоматты түрде белгілеу және жою мүмкіндігі.  • Ақпарат белгілі бір уақыт аралығында жаңартылмаған жабдық немесе персонал сияқты активтер санының диаграммалар түріндегі визуализациясы.  Автоматтандыруға қойылатын талаптар  • Актив өрістері автоматты түрде толтырылатын ережелерді жасау мүмкіндігі.  • Құрастырушы түйіндерден алынған ақпарат негізінде АТ активтері мен желілер тобы үшін «Орналасу» өрісін автоматты түрде толтыру.  • Активтердің күйін есептеу мүмкіндігі  диаграмма түріндегі бизнес-процестердің ресурстық-қызметтік моделін автоматтандырылған құру;  o олармен байланысты инциденттер негізінде ресурстық-қызметтік модель активтерінің жай-күйін автоматты түрде есептеу;  o дерекқордағы соңғы ақпаратқа сәйкес өзара байланыс диаграммасын автоматты түрде жаңарту опциясы;  o активтердің жағдайын есептеу схемасынан тиісті активтерге немесе инциденттерге көшу;  o активтердің бір-біріне және бизнес-процестің жай-күйіне әсерін есептеу, активтердің жай-күйін ескере отырып, жабдықты кластерге біріктіру, әсер ету коэффициентін анықтау мүмкіндігімен, сондай-ақ шектеу шегін шектеу; инциденттердің актив жағдайына әсері;  o оқиғаның бизнес үдерісіне тікелей әсерін анықтау мүмкіндігі;  o активтерге «виртуалды инциденттерді» қосуға және өзгерту нүктесінен күй есептеулерін жүргізуге мүмкіндік беретін активтердің өзара қосылу схемасы үшін тестілеу режимінің болуы;  o бір уақытта тек бір пайдаланушыға деректерді өзгертуге мүмкіндік беретін диаграмманы өңдеу режимінің болуы, сонымен қатар өзара байланыс диаграммасын өңдейтін пайдаланушының көрсеткішін көрсетеді;  o диаграммаға таңдалған активтің барлық қосылымдарын бір деңгейге жүктеу және активтер тізбегін таңдалғанға қысқарту мүмкіндігі;  o көрсетілген бизнес-процестің өзара байланыс үлгісі өзгерген кезде хабарландыруларды жіберу мүмкіндігі;  o активтердің өзара қосылу схемасындағы өзгерістер тарихын қарау.  • Жүйемен инвентаризацияланған хосттарда автоматтандыру сценарийлерін орындау мүмкіндігі.  • Түрлері бойынша топтастырылған кемінде 50 дайын әртүрлі автоматтандыру сценарийлерінің болуы.  • Python, java, powershell, bash тілдерінде жазылған өзіңіздің автоматтандыру сценарийлеріңізді қосу мүмкіндігі (егер сәйкес бағдарламалық құрал хостта орнатылған болса).  Орталық басқарудың ішкі жүйесінің инциденттерді басқару модуліне қойылатын талаптар  Сыртқы жүйелермен интеграцияға қойылатын талаптар  Сыртқы көздерден инциденттерді қабылдауға қатысты  • Кері күйді синхрондау арқылы ескертулерді генерациялау нәтижелеріне негізделген инциденттерді алу үшін оқиғаларды басқару модулімен интеграция.  • Деректер базасымен әмбебап интеграцияның болуы: Microsoft SQL Server, Oracle, PostgreSQL.  • Белгіленген өрістерді автоматты түрде толтыру мүмкіндігі бар электрондық пошта хабарларынан оқиғаларды жасау.  • API арқылы оқиғаларды жасау:  o сыртқы жүйеден таңдалған деректермен көрсетілген оқиға өрістерін толтыру мүмкіндігі;  o екі жақты деректер алмасу мүмкіндігі – оқиға күйін синхрондау.  • Сыртқы жүйелермен біріктіру кестесін орнату мүмкіндігі.  Оқиғаларды сыртқы жүйелерге жіберуге қатысты:  • Оқиғалар туралы ақпаратты электрондық пошта арқылы жіберу мүмкіндігі (IMAP, SMTP протоколдары).  • REST API интерфейсімен әрекеттесу арқылы кездейсоқ сыртқы жүйелерге оқиға деректерін тасымалдау мүмкіндігі.  Оқиғаларды тіркеуге қойылатын талаптар  • Бір жүйеде әртүрлі көздерден ақпараттық қауіпсіздіктің барлық инциденттері туралы ақпаратты жинау, тіркеу және байыту.  • Оқиғалар туралы ақпаратты, тіркелген файлдарды және қосымша ақпаратты қамтитын оқиға карталарын жүргізу.  • Оқиғаны сыртқы көздерден автоматты түрде немесе қолмен жасау мүмкіндігі (соның ішінде алдын ала толтырылған үлгілерді пайдалану).  • Кез келген оқиғалардың санаттары мен түрлерін өзгерту мүмкіндігімен оқиғаларды санаттар мен түрлер бойынша жіктеу.  • Критикалық деңгейлердің теңшелетін каталогына сәйкес оқиғаға сын деңгейін тағайындау мүмкіндігі.  • Оқиғаның жасалған күні мен уақытын автоматты түрде жазу.  • Оқиғаға файлдарды тіркеу мүмкіндігі (осы файлдардың бақылау сомасын автоматты түрде есептеумен (MD5, SHA-1)) және оларға метадеректерді қосу, оқиға үшін барлық файлдарды мұрағат түрінде жүктеп алу мүмкіндігі. Файлдарды тіркеу үшін файлды картаның жұмыс кеңістігіне жылжытуға арналған құралға (сүйреп апару) қолдау көрсету керек.  • Оқиғаны басқа жүйе нысандарымен байланыстыру мүмкіндігі (қолмен немесе автоматты түрде):  o активтер (бизнес-процестер, ақпарат, АТ активтерінің топтары, жабдық, құрылымдық бөлімшелер, персонал, пайдаланушы активтері және жүйеде конфигурацияланған активтердің басқа түрлері);  o тапсырмалар;  o басқа оқиғалар.  • Оқиғаға жұмсалған уақытты бақылау:  o оқиға картасына конфигурацияланатын уақыт есептегіштерін қосу;  o уақыт шектеуінің есептегішінің мақсаты;  o мерзімнен асып кетуді көрсету;  o жауап сценарийлері деңгейінде қарсы бақылау: тоқтату, бастау, шектеу тағайындау;  o бақылау тақталарындағы графиктердегі инциденттерде конфигурацияланған уақыт есептегіштеріндегі жиынтық ақпаратты көрсету мүмкіндігі.  • Оқиғалар тізімімен жұмыс істеу мүмкіндігі:  o тізімде іздеу;  o тізімді бір немесе бірнеше өрістер бойынша сұрыптау және сүзу;  o пайдаланушының тізім сүзгісін қайта пайдалану үшін сақтауы;  o жалпы тізімде көрсетілетін өрістер тізімін орнату;  o берілген сүзгіні пайдаланып инциденттерді көрсетудің бірнеше режимдерін жасау және олардың арасында жылдам ауысу мүмкіндігі.  • Оқиға картасына енгізілген өзгерістер өзгертулер көзіне (пайдаланушы, сценарий) және олар енгізілген интерфейске (UI, API) қарамастан тіркелуі керек.  • Оқиға деректерін \*.xlsx пішіміндегі файлға экспорттау/импорттау мүмкіндігі. Оқиға деректерін экспорттау кезінде өрістерді таңдау мүмкіндігі.  • Белгіленген критерийлерге сәйкес келетін оқиғаларда өзгерістер болған кезде пайдаланушыларды хабардар ету мүмкіндігі. Оқиғаға жаңа түсініктеме қосылғанда пайдаланушыға хабарлау мүмкіндігі.  • Пошта жүйесімен біріктірілген кезде хатты жіберушінің пошталық мекен-жайына оқиғаның категориясы мен түрін тағайындау мүмкіндігі.  • Ақпараттық қауіпсіздік инциденттерінен залал деңгейін есепке алу мүмкіндігі.  Өрістерге және оқиға карталарына қойылатын талаптар  • Оқиғалардың әрбір санаты (түрі) үшін оқиға картасын жеке конфигурациялау мүмкіндігі.  • Картаға келесі түрлердің теңшелетін өрістерін қосу мүмкіндігі: сандық өріс, мәтіндік өріс, көп жолды мәтін өрісі, ашылмалы тізім, валюта таңбасы бар сандық өріс, күн мен уақыт, уақыт есептегіші, құсбелгі ұясы, пайдаланушы таңдау.  • Карточкаға кестелерді қосу мүмкіндігі, мұнда бағандар аталған түрлердің өрістері болып табылады: мәтіндік өріс, сандық өріс, бірнеше мәтіндік жолдар, ашылмалы тізім, ақша белгісі бар сандық өріс, күн, құсбелгі, пайдаланушы таңдауы.  • «Ашылмалы тізім» түріндегі өрістер үшін өзіңіздің анықтамалықтарыңызды жасау және өңдеу.  • Мәтіндік өрістерге енгізілген мәндер үшін тексеруді орнату. Алдын ала конфигурацияланған және жеке анықтамалық кітапқа енгізілген тексеру үшін тұрақты өрнектерді пайдалану мүмкіндігі.  • Күн түрінің өрістері үшін енгізілген мән үшін тексеру ережесін орнату мүмкіндігі: тек болашақ немесе тек өткен күндерді енгізуге рұқсат беріңіз.  • Өрістерге алдын ала орнатылған мәндерді орнатыңыз.  • Өрістерге арналған кеңестерді орнату.  • Мәтін өрістерін теңшелетін сілтеме мекенжайы және сынақ шығысы бар гиперсілтемелер ретінде көрсету.  • Таңдалған сценарийді іске қосу үшін оқиға картасына түймені қосу мүмкіндігі.  • Келесі функцияларды қолдайтын оқиға картасын қарау дизайнерінің болуы:  o теңшелетін өрістердің мәндеріне, пайдаланушы рөліне немесе осы критерийлердің жиынтығына қатысты көрсетілген критерийлерге байланысты оқиға картасының әртүрлі дисплейін орнату;  o өрістерді теңшеу: жасыру, көрсету, өңдеуді өшіру, бос жасыру, өрісті міндетті ету, алдын ала орнатылған мәнді орнату, «ашылмалы тізім» түріндегі өрістер үшін анықтамалықты конфигурациялау, көрсетілген өріс мәндерін таңдау үшін қолжетімсіз ету.  o оқиға өрістерін логикалық ұйымдастыру үшін өрістерді атаулы топтарға біріктіру мүмкіндігі, әдепкі бойынша топтың дисплейін басқаруды қолдау - жиырылған немесе кеңейтілген пішінде.  o оқиға картасының бөлімдерін жасыру немесе көрсету мүмкіндігі;  o басқа көрініс тағайындалмаған жағдайда картаға қолданылатын әдепкі көріністі тағайындау мүмкіндігі.  o бір өрістің мәнін басқасының мәніне байланысты көрсетуге мүмкіндік беретін көріністердегі тәуелділіктерді конфигурациялау мүмкіндігі.  • Өнім интерфейсіндегі барлық қойындыларға қатынаусыз нақты пайдаланушы рөлдері үшін оқиғаларды хабарлау үшін жеңіл Жүйе беті көрінісін жасау мүмкіндігі.  Оқиғаның өмірлік цикліне қойылатын талаптар  • Ұйымда көрсетілген процедураларға сәйкес оқиға күйінің үлгісін енгізу мүмкіндігі.  • Оқиғаның өмірлік циклінің икемді конфигурациясы:  o өмірлік циклге ерікті күйлерді қосу;  o өмірлік цикл күйлері арасында еркін ауысуларды орнату;  o жеке пайдаланушылар мен пайдаланушылар топтары үшін өту құқықтарын орнату;  o пайдаланушы интерфейсінде толтырылуы бір күйден екіншісіне өту үшін міндетті болып табылатын оқиға өрістерін орнату;  o оқиғалардың әртүрлі санаттары үшін әртүрлі өмірлік циклдерді орнату.  Оқиғаның бірлескен жұмысына қойылатын талаптар  • Оқиғаларға қол жеткізуді шектеу:  o үлгі;  o дискрециялық қол жеткізу құқығы;  o оқиға өрісінің мәндері.  • Оқиғаларды жасау, жою, оқу және өзгерту үшін жеке құқықтарды конфигурациялау мүмкіндігі.  • Пайдаланушы жасай алатын оқиғалар санаттарына (түрлеріне) шектеу қою мүмкіндігі.  • Оқиғаға жауапты пайдаланушыны тағайындау:  o оқиға өрістерінде көрсетілген критерийлер негізінде жауапты тұлғаны автоматты түрде тағайындауды орнату;  o ағымдағы жүктеме негізінде жергілікті пайдаланушылардың белгілі бір тобынан жауапты тұлғаны автоматты түрде тағайындауды орнату.  • Жеке кірістірілген чатта әрбір оқиға бойынша байланысу мүмкіндігі:  o мәтіндік хабарламада жүйе пайдаланушысын кейінгі хабарландырумен атап өту мүмкіндігі;  o нақты уақыттағы жүйеде пайдаланушының жүйедегі жұмысының күйін көрсету: «белсенді», «белсенді емес».  • Картадағы оқиға бойынша пошталық хат алмасуды жүргізу мүмкіндігі, оның аясында жүйе пайдаланушылары электрондық пошта арқылы хабарламалар жіберіп, жауап ала алады, бұл ретте барлық хаттар жүйеде сақталуы және оқиға картасынан көруге болатын болуы керек.  Макрокорреляцияға және топтастыруға қойылатын талаптар  • Оқиғаларды топтастыру:  o бір оқиға ата-ана, қалғандары балалар болып табылатын оқиғаларды топтарға біріктіру;  o оқиғаны бар топқа қосу және топтан оқиғаны жою мүмкіндігі;  o топқа енгізілген инциденттер тізімін ыдырату/кеңейту мүмкіндігімен пайдаланушы интерфейсінде оқиғалар тобын көрсету;  o атаулы топ түрлерін құру. Топ түріне, топ ішіндегі өрістерді ата-ана оқиғасынан еншілес оқиғаға мұраға алуға және еншілес өрістерден ата-аналық өрістерді толтыруға теңшеуге болады.  • Сәйкес өріс мәндерінің критерийі негізінде ұқсас оқиғаларды іздеу.  • Табылған оқиғаларды ағымдағы оқиғамен байланыстыру және оларды топқа біріктіру мүмкіндігі.  Автоматтандыруға қойылатын функционалдық талаптар  Оқиғаға қолданылатын конфигурацияланатын сценарийлерді (ойын кітаптарын) қосу мүмкіндігі.  • Сценарий берілген ретпен орындалатын әрекеттерден тұруы керек.  • Сценарий «тармақтауға» (әртүрлі әрекеттер тізбегін параллель орындау) және «тармақтарды» біріктіруге (екі немесе одан да көп тармақтарды аяқтағаннан кейін әрекетті орындау - барлығы немесе кез келген), оның ішінде пайдаланушы әрекеттеріне, нәтижелерге байланысты болуы керек. алдыңғы әрекеттердің немесе айнымалылардың мәні (оқиға картасындағы өріс мәні).  • Сценарий "if-else" және "case" сияқты шартты мәлімдемелерді пайдалана алуы керек.  • Бір сценарийден басқа сценарийді іске қосу мүмкіндігі болуы керек.  • Сценарийдегі әрекеттердің кешіктірілген бастау опциясы болуы керек.  • Сценарийдегі әрекеттер әрекет іске қосылған кездегі оқиға өрістерінің мәндерінде жұмыс істеуі керек (яғни нақты уақытта).  • Жүйенің бөлігі ретінде берілген әрекеттер келесі мүмкіндіктерді қамтамасыз етуі керек:  - пайдаланушы мазмұны бар электрондық хаттарды автоматты түрде жіберу, соның ішінде оқиға өрістеріндегі мәндерді пайдалану: жауапты күту және оның мазмұнын сақтау мүмкіндігімен; оқиға туралы есепті автоматты түрде жасау және хатқа тіркеу мүмкіндігімен; оқиға шеңберінде жіберілген және алынған барлық хаттарды картаның тиісті бөлімінде сақтау мүмкіндігімен; әрекетті автоматты түрде аяқтау шарттарын конфигурациялау мүмкіндігімен – хат жібергеннен кейін немесе алушыдан жауап алғаннан кейін; хабарлама жібермес бұрын жүйедегі пайдаланушы тіркелгісінің күйін тексеру керек;  - инциденттер бойынша тапсырмаларды орындаушылар ретінде оқиғаға жауапты пайдаланушыларды көрсету мүмкіндігімен берілген мазмұндағы тапсырма жүйесінде автоматты түрде құру;  - жауапты тұлғаны автоматты түрде тағайындау немесе ауыстыру және оқиғаға еркін қол жеткізу құқығын беру;  - оқиға өрістерін автоматты түрде өзгерту (оның ішінде басқа өрістердің мазмұнын мәтіндік өрістерге жазу мүмкіндігі), оның ішінде әрекет орындалған кездегі ағымдағы күнді немесе өріс мәні ретінде ағымдағы күннен ығыстыруды көрсету мүмкіндігі «күн» түріндегі;  - оқиғаға қатысты жабдықты сканерлеуді іске қосу;  - пайдаланушы әзірлеген сыртқы жүйелерге сценарийлер мен қосқыштарды іске қосу (оркестрлеу механизмдерінің функционалдық талаптарын қараңыз), оның ішінде белгіленген тоқтату критерийіне жеткенше циклде жұмыс істеу мүмкіндігі;  • Сценарийді қолмен іске қосу.  • Оқиғаның реттелетін өрістерінің мәндері үшін көрсетілген критерийлер сәйкес келсе, оқиға жасалғанда немесе өзгертілгенде сценарийді автоматты түрде іске қосыңыз.  • Сценарийді іске қосу және оның ішінде әрекеттерді орындау журналда болуы керек.  • Сценарийдің орындалуын кідірту опциясы болуы керек. Сценарий кідіртілгеннен кейін оны жалғастыру мүмкіндігі болуы керек.  • Сценарийдегі бір әрекеттің де, бүкіл сценарийдің де орындалуын үзу мүмкіндігі болуы керек.  • Сценарий үшін оны оқиғаға қолдану мүмкіндігі конфигурациялануы керек - бір реттік қолданба немесе бірнеше рет пайдалану.  • Хабарландыруды жіберу немесе ақпаратты электрондық пошта арқылы сұрау (соның ішінде жауап күту мүмкіндігі), сценарийлер мен қосқыштарды іске қосу, қатысты жабдықты сканерлеу, сценарий жасауды қажет етпестен тікелей оқиға картасынан тапсырмаларды орнату әрекеттерін қолмен іске қосу мүмкіндігі бұл үшін.  • Мәні оқиға өрістерінен ақпаратты немесе мәтін пішіміндегі теңшелетін ақпаратты қамтитын айнымалы мәндерді жасау және оларды жауап әрекеттерінде, соның ішінде қосқыштарды пайдалану мүмкіндігі.  Оркестрлік механизмдерге қойылатын функционалдық талаптар  • Ерікті сыртқы жүйелермен өзара әрекеттесу үшін қосқыштарды графикалық жобалау мүмкіндігі.  • Жүйені тоқтатпай жаңа қосқыштарды орнату және іске қосу мүмкіндігі.  • Қосқыштар технологияларды қолдауы керек: Powershell және cmd.exe; SSH; REST API; LDAP; MS SQL; MySQL; PostgreSQL; SNMP; SOAP.  • Қосқыш корпусында оқиға өрісінің мәндерін пайдалану мүмкіндігі.  • Коннекторды орнату сатысында сыртқы жүйеге қосылымды тексеру мүмкіндігі.  • Сұрау жіберу және оның нәтижесін көрсету арқылы конфигурациялау кезінде коннекторды жөндеу мүмкіндігі.  • Қосқыш конструкторымен жұмыс істеу кезінде бар қосқышты көшіру мүмкіндігі.  • Қосқышты өзгерту әсер етуі мүмкін қатысты нысандарды (скрипттер және басқа қосқыштар) көру мүмкіндігі.  • REST қосқыштарын прокси серверлер арқылы басқару мүмкіндігі.  • REST API қосқышы арқылы екілік файлдарды сыртқы жүйелерге жіберу мүмкіндігі.  • Бөлек қашықтағы коллектордағы қосқыштың орындалуын конфигурациялау мүмкіндігі.  • Бастапқы орындау кезінде қате орын алса, «Қосқышты іске қосу» әрекетінің көрсетілген күту уақытымен қайта орындалуын конфигурациялау мүмкіндігі, сценарийді орындауды кідірту немесе үзу.  • Тұрақты өрнектерді пайдаланып қосқыштың нәтижелерін өңдеу және өңдеу нәтижелерін бір немесе бірнеше оқиға өрісінде жазу мүмкіндігі.  • REST және SOAP қосқыштары үшін SSL сертификатының аутентификациясын тексеру мүмкіндігі.  Пайдаланушы интерфейсінде сценарийлермен жұмыс істеуге қойылатын талаптар  • Графикалық режимде сценарийлерді құру және өңдеу.  • Бір уақытта барлық сценарийлерді де, таңдалған сценарийді де көру мүмкіндігімен графикалық пішінде оқиға бойынша орындалатын сценарийлерді көрсету.  • Оқиға кезінде іске қосылған сценарийлерді олардың іске қосылу уақыт белгілерімен байланыстырылған уақыт шкаласы түрінде көрсету.  • «Кірістірілген» сценарийдің әрекеттерін көру мүмкіндігі және бір сценарийді екіншісінен іске қосу кезінде оларды шағын блокқа жинаудың кері мүмкіндігі.  • Іске қосылған сценарийді қарау кезіндегі әрекеттердің көрсеткіші: орындалған, қазіргі уақытта іске қосылған, жоспарланған және қатемен орындалған әрекеттер, ол үшін оның дұрыс емес аяқталуына әкелген қатенің мәтінін көру мүмкіндігі болуы керек.  • Оқиға кезінде орындалған сценарийлер диаграммасын сурет ретінде сақтау мүмкіндігі.  Орталық басқарудың ішкі жүйесінің осалдықтарын басқару модуліне қойылатын талаптар  Сыртқы жүйелермен интеграцияға қойылатын талаптар  • осалдықтар мен осал бағдарламалық құрал туралы ақпаратты импорттау.  • Осалдық сканерлерімен біріктіру кестесін орнату мүмкіндігі.  Осалдықтарды тіркеуге қойылатын талаптар  • Осалдық сканерлерінен және (немесе) осалдықтар туралы ақпаратты қамтамасыз ететін қызметтерден алынған ақпарат негізінде сканерлеу нәтижелерін есепке алу және көрсету, сондай-ақ кірістірілген сканерлеу функционалдығы.  • Жүйеде тіркелген осалдықтар бойынша статистиканы көрсету, ауырлық деңгейі, жабдық түрі, эксплуатацияның болуы, порттар, қолжетімділік векторы бойынша сүзу мүмкіндігімен.  • осалдықтар тізімімен жұмыс істеу мүмкіндігі:  • осалдықтар тізімін іздеу;  • тізімді бір немесе бірнеше өрістер бойынша сұрыптау және сүзу;  • пайдаланушының осалдықтардың сүзгі тізімін сақтауы;  • осалдықтардың жалпы тізімінде көрсетілетін өрістер тізімін теңшеу;  • берілген сүзгіге сәйкес осалдықтарды көрсетудің бірнеше режимдерін құру және олардың арасында жылдам ауысу мүмкіндігі (әрбір Жүйе пайдаланушысы үшін).  • Осалдықты қолмен жасау және осал жабдықпен байланысты конфигурациялау, сондай-ақ осындай осалдықтарды өңдеу мүмкіндігі.  • Осалдық деректерін \*.xlsx пішіміндегі файлға экспорттау мүмкіндігі.  • Мыналарды көрсететін бірегей осалдықтар тізімінің болуы:  • бірегей осалдықтың осал жабдықпен қосылымдар саны;  • жабдықтың ашық осалдықтарының жалпы рейтингі;  • Жабдықтағы ашық осалдықтарды ауырлық деңгейі бойынша бөлу.  • Бірегей осалдықтардың тізімімен жұмыс істеу мүмкіндігі:  • осалдықтар тізімін іздеу;  • тізімді сұрыптау;  • осалдықтардың жалпы тізімінде көрсетілетін өрістер тізімін теңшеу;  • ауырлық деңгейі мен күйі бойынша алдын ала сүзгілеу арқылы осалдықтар тізіміне көшу.  Өрістерге және осалдық карталарына қойылатын талаптар  • Картадағы әрбір осалдық туралы жалпы ақпаратты көрсету.  • Осалдық рейтингіне байланысты осалдықтардың критикалық деңгейін көрсету, деңгейлер үшін рейтинг мәндерінің ауқымдарын өзгерту мүмкіндігі.  • «Осалдық» бөліміндегі осалдықтар туралы түсініктеме жазу мүмкіндігі.  • Картаға келесі түрлердің теңшелетін өрістерін қосу мүмкіндігі: сандық өріс, мәтіндік өріс, көп жолды мәтін өрісі, ашылмалы тізім. Пайдаланушы өрістерін өңдеу мүмкіндігі.  • «Ашылмалы тізім» түріндегі өрістер үшін өзіңіздің анықтамалықтарыңызды жасау және өңдеу.  Өмірлік циклге қойылатын талаптар  • Осалдықтардың келесі күйлерін есепке алу: ашық, жабық, қабылданған тәуекел және жалған позитив, сондай-ақ күйлерді қолмен өзгертуге қолдау көрсету.  • Жеке осалдықтың өмірлік циклінің күйлерін жасау мүмкіндігі.  • Күйдің жарамдылық мерзімін көрсете отырып, таңдалған осалдықтың күйін өзгерту мүмкіндігі.  • Осалдықтардың күйін топтастыру мүмкіндігі.  Автоматтандыруға қойылатын талаптар  • Осалдықты автоматтандырылған басқару: тапсырмаларды немесе инциденттерді жасау, күйді өзгерту, көрсетілген критерийлерге сәйкес осалдықтарды жою (осалдық атрибуттары, осал құрылғының атрибуттары, АТ активтері тобының сынилігі немесе осал құрылғы).  • Саясат қолданылмайтын ерекшелік критерийлерін көрсету мүмкіндігі.  • Пайдаланушы осалдық рейтингі негізінде осалдықтарға басымдық беріңіз. Рейтингті есептеу үшін осалдықтың атрибуттарын, аппараттық құралды және аппараттық құралмен байланысты АТ активтер тобын пайдалану мүмкіндігі болуы керек. Рейтинг күніне кемінде бір рет автоматты түрде қайта есептелуі керек.  • Жүйе базасындағы бар осалдықтарға осалдықтарды басқару саясаттарын қолдану мүмкіндігі.  Орталық бақылау кіші жүйесінің тәуекелдерді басқару модуліне қойылатын талаптар  Кірістірілген каталогтарға қойылатын талаптар  • Алдын ала орнатылған қауіп каталогтарының болуы (меншікті стандартты дерекқор).  • Алдын ала орнатылған қорғаныс шараларының каталогының болуы (меншікті стандартты деректер базасы).  • Алдын ала анықталған тәуекелдерді бағалау схемаларының болуы.  Теңшеу мүмкіндігіне қойылатын талаптар  • Ұйымда қолданылатын нақты әдістемеге бейімделуі мүмкін тәуекелді бағалау схемасының икемді конфигурациясының мүмкіндігі. Сандық есептеу параметрлерін (қолмен толтырылады, формула арқылы есептеледі немесе өзара байланысты параметрдің мәндеріне негізделеді) және сапалық (мәндер қолмен, тізімнен немесе кесте негізінде толтырылады) құру мүмкіндігі.  • Қауіпсіздік қатерлерінің ықтимал тізімін, сондай-ақ олардың байланысты көздерін, іске асырудың алғышарттарын, қорғаныс шараларын және әсер ететін қауіпсіздік атрибуттарын сипаттайтын қауіп каталогтарын конфигурациялау мүмкіндігі.  • Қауіп көздерінің әлеуетін конфигурациялау мүмкіндігі, іске асыру үшін алғышарттардың жеткіліктілігі және каталогтағы әрбір қауіпке қатысты қорғаныс шараларының тиімділігі.  • Жүйедегі бар қауіп каталогтарын көшіру мүмкіндігі.  • Актив құнын бағалау критерийлері мен деңгейлерін теңшеу мүмкіндігі.  • Қолмен немесе Excel бағдарламасынан импорттау арқылы каталогтарды құруға қолдау көрсететін қорғаныс шаралары каталогтарының дерекқорын жүргізу мүмкіндігі.  • АТ активтерінің топтарымен, ақпараттық активтермен және олар іске асырылатын бизнес-процестермен байланыстыру мүмкіндігімен енгізілген қорғаныс шараларының деректер қорын жүргізу мүмкіндігі.  Тәуекелді бағалауды жүргізуге қойылатын талаптар  • Тәуекелді бағалау саласына кіретін активтердің тізімін жасау, құпиялылық, тұтастық және қолжетімділік параметрлері негізінде олардың құнын анықтау, сондай-ақ оларды редакциялау. Активтердің тәуекелдік аппетитін анықтау.  • Олардың біреуінің қауіпсіздік атрибуттарының ықтимал бұзылуы контекстінде қатысты активтердің бір-біріне әсерін көрсету мүмкіндігі.  • АТ активтерінің топтары, сондай-ақ байланысты бизнес-процестер және өңделген ақпарат үшін ақпараттық қауіпсіздік тәуекелдерін бағалау мүмкіндігі.  • Ағымдағы көздер мен алғышарттар туралы сауалнаманы толтыру негізінде бағалаудың берілген саласына қатысты тәуекелдерді каталогтан автоматты түрде іздеу мүмкіндігі.  • Берілген бағалау схемасына (әдістемесіне) сәйкес ықтималдық, зақымдану және/немесе басқа параметрлер негізінде тәуекел деңгейін автоматты түрде есептеу.  • Тәуекелдерді бағалау кезінде актив құнын, бұзушылардың әлеуетін, енгізілген қорғаныс шаралары және олардың тиімділігі туралы ақпараттарды есепке алу мүмкіндігі.  • Ұйымда анықталған тәуекелге байланысты оқиғалардың тізімін көру мүмкіндігі.  • Актив үшін белгіленген рұқсат етілген деңгейден асатын тәуекелдерді визуалды таңбалау.  • Туынды тәуекелдерді есепке алу (бір активтің құны басқа активтің құнына әсер еткен жағдайда).  Тәуекелді емдеу талаптары  • Белгілі бір кезеңге тәуекелдерді емдеу жоспарын құру және оны ақпараттық қауіпсіздікке арналған қолданыстағы бюджетпен салыстыру мүмкіндігі.  • Өңдеу жоспарына ұйымның каталогынан қорғау шараларын енгізу шараларын енгізу мүмкіндігі.  • Іс-шаралардың тиімділігін бағалау үшін тәуекелдің бастапқы (ағымдағы) деңгейімен салыстыру мақсатында емдеу жоспары құрылатындықтан мақсатты тәуекел деңгейін автоматты түрде қайта есептеу.  • Тәуекелді емдеудің әртүрлі сценарийлерін салыстыру мүмкіндігі.  • Тәуекелдерді емдеу жөніндегі іс-шараларға (бағалау шеңберінде және тәуекелді емдеудің жалпы жоспарында) құжаттарды қосу және ескертулер жасау мүмкіндігі.  Тәуекелдерді бағалау нәтижелерімен жұмыс істеуге қойылатын талаптар  • Қалыптасқан тәуекелдер картасын және оларды өңдеу жоспарын бекіту үшін ақпараттық қауіпсіздік тәуекелдерін бағалауды жазу мүмкіндігі, сондай-ақ уақыт бойынша жеке тәуекелдердің өзгерістерін талдауды қамтамасыз ету.  • Тәуекелдер туралы жиынтық ақпаратты көру мүмкіндігі – бағалау кезінде анықталған барлық тәуекелдердің (соның ішінде қауіп көздері мен алғышарттардың) тізімі.  • Тәуекелдерді бағалау нәтижелерін тіркейтін құжаттарды дайындау (тәуекелдердің жиынтық тізілімі, тәуекелдерді емдеу жоспары және т.б.).  • Ұйымның тәуекелдер картасына енгізілген тәуекелдерді талдау мүмкіндіктері: оның пайда болуына себеп болған тәуекел факторларының тізімінің болуы; тәуекелге қатысты қазірдің өзінде енгізілген қорғаныс шараларының тізбесі; жоспарланған өңдеу жұмыстарының тізбесі; орын алған тәуекелмен байланысты оқиғалардың тізбесі; тарихи бағалау негізінде тәуекел деңгейіндегі өзгерістерді қадағалау мүмкіндігі.  • Ұйымның активтеріне қатысты барлық тәуекелдерге қатысты шараларды қоса алғанда, олардың мәртебесі мен мерзімдерін қадағалау мүмкіндігі бар тәуекелдерді емдеудің бірыңғай жоспарының болуы.  • Тәуекелдерді жою шараларының мұрағатын жүргізу мүмкіндігі.  • Жаңасын жасау кезінде активтердің тәуекелін бұрынғы бағалау нәтижелерін есепке алу: ұйымның Тәуекелдер картасынан бұрыннан анықталған тәуекелдерді автоматты түрде қосу, тәуекел факторлары бойынша сауалнаманы алдын ала толтыру, аяқталмаған тәуекелдерді өңдеу шараларын қосу.  • Ағымдағы ақпараттық қауіпсіздік тәуекелдері және тәуекелдерді өңдеу схемалары (графиктері) туралы ақпаратты көрнекі түрде көрсету.  Ынтымақтастыққа қойылатын талаптар  • Қатысушылардың рөлдерін көрсете отырып, бағалау жүргізу үшін жұмыс тобын тағайындау мүмкіндігі: Қатысушы немесе Бақылаушы.  • Оларға жүктелген жеке тәуекелдерді бағалау үшін сарапшыларды тарту мүмкіндігі.  • Бірнеше сарапшылардың тәуекел параметрлерін бағалауды өңдеу принципін теңшеу мүмкіндігі.  Орталық басқару ішкі жүйесінің аудитті басқару модуліне қойылатын талаптар  Кірістірілген каталогтарға қойылатын талаптар  • Ақпараттық қауіпсіздік саласында алдын ала белгіленген нормативтік құқықтық актілер мен стандарттардың болуы:  - ISO 27001:2013  - ISO 27001:2022  - ISO/IEC 27001:2013/DAM 1:2022  - ISO/IEC 27002:2022  Аудиторлармен жұмыс істеуге қойылатын талаптар  • АТ активтерінің, бизнес-процестердің, бөлімдердің, үй-жайлар мен жабдықтардың топтарына аудит жүргізу мүмкіндігі.  • Бірнеше аудитті біріктіретін кешенді аудиттер (консолидацияланған аудиттер) жүргізу мүмкіндігі: әртүрлі активтерге қатысты және/немесе әртүрлі стандарттар бойынша. Жиынтық интерфейстен қарапайым аудиттерді басқару мүмкіндігі: күйді өзгерту, жұмыс тобын өңдеу, талаптарды бағалау. Аудит картасынан аудитті бағалау аймағына енгізілген актив карталарын көру мүмкіндігі. Кірістірілген бақылау тақтасының көмегімен кіріс тексерулерінің нәтижелерін талдау мүмкіндігі, оған мыналар кіреді: сәйкестік деңгейінің есептеулері туралы ақпарат, жасалған есептер, анықталған бұзушылықтар статистикасы және оларды өңдеу деректері.  • Аудиттің уақытын, жай-күйін және барысын бақылауға, сондай-ақ жоспарланған және нақты күндерді салыстыруға мүмкіндік беретін динамикалық аудит жоспарының жүйесінде болуы.  • Тексеру тізілімімен жұмыс істеу мүмкіндігі: тізімді бір немесе бірнеше өрістер бойынша сұрыптау және сүзу, тексерулердің жалпы тізімінде көрсетілетін өрістер тізімін теңшеу, пайдаланушының қайта пайдалануы үшін сүзгіні сақтау, тізілімге негізделген бірнеше тізілімді көрсету режимдерін жасау. берілген сүзгі және олардың арасында жылдам ауысу мүмкіндігі.  • Активтердің қасиеттерінде оларға қатысты қолданыстағы нормативтік құжаттар тізбесін жүргізу мүмкіндігі, соның ішінде. автоматты түрде актив атрибуттарына негізделген.  • Активтер тізілімінен динамикалық тексеру жоспарын құру мүмкіндігі: актив картасында жоспарлауға қажетті ақпараттың болуы (қазіргі жоспарланған тексерулер тізімі, мерзімі мен мәртебесі, бұрын анықталған ескертулер, жоспарланған жұмыстар); актив қасиеттерінен аудитті жылдам құру режимі; байланысты активтердің аудитін оларға қатысты қолданыстағы құжаттарды ескере отырып, кешенді аудитке автоматты түрде қосу мүмкіндігі (қосымша жүйелерге, кіріс жабдықтарға және т.б. аудиттер).  • Жаңа аудиттерді құру, жоспарлы тексерулердің жақындауы, жоспарланған тексеру мерзімдерін бұзу, сондай-ақ аудит мәртебесін өзгерту туралы хабарламалар жіберу мүмкіндігі.  • Көшірілген сәйкестікті қайта бағалау үшін қолданыстағы сәйкестікті бағалауды көшіру мүмкіндігі.  • Аудитордың активтің құжатқа сәйкестік деңгейін кейін автоматты түрде қайта есептеу арқылы шкала бойынша жауапты таңдау арқылы талаптарды бағалау мүмкіндігі.  • Активке қолданылмайтын талаптарды белгілеу, содан кейін оларды сәйкестік деңгейін есептеуден шығару мүмкіндігі.  • Excel файлдарынан аудит бағалау нәтижелерін импорттау мүмкіндігі.  • Нормативтік құжаттың бағаланатын талаптарына тексеру сертификаттарын қосу мүмкіндігі.  • Аудит аясындағы талаптарға тіркелген барлық дәлелдемелерді файлдарды аудит мәселелеріне сәйкес қалталарға автоматты түрде бөлу арқылы бір рет басу арқылы жүктеп алу мүмкіндігі.  • Ақпараттық қауіпсіздік жүйесінің жай-күйі туралы, сондай-ақ сәйкестікті бағалау және ақпараттық қауіпсіздік аудитінің нәтижелері бойынша есеп беру құжаттарының пакетін қалыптастыру (жиынтық және егжей-тегжейлі есептер, белгіленген нысандардағы есептер, бағалау дәлелдемелерінің тізбесі және т.б.); оның ішінде аудит аясындағы жұмыс тобына қатысушылардың ескертулері бар есептер және бірнеше таңдалған аудиттер үшін өнімділікті бағалаудағы өзгерістерді бағалауға мүмкіндік беретін есеп).  • Ақпараттық қауіпсіздік аудитіне есептерді және басқа құжаттарды қосу мүмкіндігі (мысалы, сыртқы аудит нәтижелері бойынша аудиторлық есеп).  • «Аяқталды» күйіне көшкеннен кейін чек ішіндегі кез келген өзгерістерді блоктау.  Түсініктемемен жұмыс істеуге қойылатын талаптар  • Орындалмаған талаптарға қатысты ескертулер жасау мүмкіндігі, оларды жоюдағы ілгерілеуді бақылаудың маңыздылығын, жауапкершіліктерін және мерзімдерін көрсету.  • Жаңа түсініктемелерді тексерілетін активпен, түсініктеме авторымен, бұзылған талаппен және аудитпен автоматты түрде байланыстыру.  • Алдыңғы тексерулердің бөлігі ретінде жасалған тарихи пікірлерді қарау мүмкіндігі, оларды жоюдың сәттілігін талдау және қайталанатын ескертулерді анықтау.  • Орындаушыларға беру жоспары негізінде тапсырмаларды автоматты түрде құруды қоса алғанда, аудиторлық бақылауларды жою жоспарын құру мүмкіндігі.  • Деректерді жүйелеу және статистикалық мәліметтерді жинау мақсатында шаблондарды пайдалана отырып, ескертулер мен оларды жою шараларын енгізу мүмкіндігі.  • Талаппен бар байланыс негізінде үлгіні пайдаланып оқиғаны жасау кезінде оқиға қамтылған түсініктемелерді автоматты түрде іздеу.  • Әрекеттерді түзету жоспарынан қосалқы тапсырмаларға бөлу мүмкіндігі, соның ішінде барлық зардап шеккен активтер үшін бөлек ішкі тапсырмаларды жылдам жасау мүмкіндігі.  • Шешім жоспарына енгізілген тапсырмалар аяқталған кезде түсініктемелерді автоматты түрде жабу.  • Excel файлдарынан түсініктемелерді импорттау мүмкіндігі.  • Пікірлер тізілімімен және оларды өңдеу жоспарымен жұмыс істеу мүмкіндігі: тізімді бір немесе бірнеше өрістер бойынша сұрыптау және сүзу, тексерулердің жалпы тізімінде көрсетілетін өрістер тізімін теңшеу, пайдаланушының қайта пайдалануы үшін сүзгіні сақтау, құру берілген сүзгіге сәйкес регистрді көрсетудің бірнеше режимдері және олардың арасында жылдам ауысу мүмкіндігі.  Ынтымақтастыққа қойылатын талаптар  • Аудит менеджерлері (жауапты) ретінде бірден бірнеше пайдаланушыны көрсету мүмкіндігі, сонымен қатар кешенді аудит пен оның аудитіне әртүрлі менеджерлерді тағайындау мүмкіндігі.  • Жұмыс топтарының икемді қалыптасуы: сарапшыларға олардың құзырет саласына қатысты тексеру сауалнамасының жеке бөліктеріне қол жеткізу мүмкіндігі; тексерудің белгілі бір кезеңдерінде ғана сарапшыларға қолжетімділікті қамтамасыз ету мүмкіндігі.  Бақылау тексерулерінің функционалдығына қойылатын талаптар  • Әртүрлі нормативтік құжаттардың ұқсас талаптары арасындағы байланыстарды қадағалау мүмкіндігі.  • Басқару тексерулерінің жеке жиынтықтарын жасау және олардың қосылымдарын біріктіретін талаптармен теңшеу мүмкіндігі - қолмен немесе Excel арқылы импорттау арқылы.  • Бақылау тексерулерін бағалау үшін таразыларды теңшеу мүмкіндігі.  • Активтерге қатысты қолданыстағы нормативтік құжаттар негізінде бақылау тексерулерінің тізімін автоматты түрде қалыптастыру.  • Активтің оған тағайындалған бақылау тексерулеріне сәйкестігін жүйелі түрде бағалау және орындалатын бақылау жиілігін орнату мүмкіндігі.  • Бақылауды тексеру үшін жұмыс тобын (жауаптылар/аудиторлар) құру мүмкіндігі.  • Жұмыс тобының мүшелеріне алдағы қарау мерзімдері туралы автоматты түрде хабарлау.  • Жұмыс тобының қатысушылары берген бағалардың негіздемесін міндетті түрде жазып алу.  • Бағалауды растайтын құжаттарды қоса беру мүмкіндігі.  • Аудитпен қамтылған талаптардың аудиті кезінде анықталған ескертулерді қарастыру мүмкіндігі.  • Бұрын шығарылған бағалардың тарихын қарау мүмкіндігі, соның ішінде: бағалау күні, растайтын құжаттар тізімі және үлгерімнің автоматты түрде көрсетілуі (алдыңғы бағамен салыстырғанда нашарлау немесе жақсарту).  • Әртүрлі нормативтік құжаттарда кездесетін ұқсас талаптарды жылдам бағалау үшін бақылау тексерулерін бағалау нәтижелерін автоматты түрде аудитке ауыстыру мүмкіндігі.  • Бақылау тексеру баллдарын автоматты түрде беру кезінде талаптардың коэффициенттерін, олардың рейтингтік шкаласындағы айырмашылықтарды және аудитордың бағалауы үшін өрістер санын есепке алу.  • Басқа аудиттер кезінде анықталған ұқсас талаптарға түсініктемелерді көру мүмкіндігі.  Орталық басқарудың ішкі жүйесінің тапсырмаларды басқару модуліне қойылатын талаптар  Теңшеу мүмкіндігіне қойылатын талаптар  • Әр түрлі тапсырмалар түрлері үшін өрістердің құрамы мен ретін теңшеу мүмкіндігі.  • Тапсырма жасау үшін қажетті өрістерді, сондай-ақ бір күйден екіншісіне ауысқанда толтыру қажет өрістерді конфигурациялау мүмкіндігі  Тапсырмалармен жұмыс істеуге қойылатын талаптар  • Тапсырмалар тізілімімен жұмыс істеу мүмкіндігі: тапсырмалар тізімін бір немесе бірнеше өрістер бойынша сұрыптау және сүзу, пайдаланушының тапсырмалар тізімі сүзгісін қайта пайдалану үшін сақтау, тапсырмалар тізілімінде көрсетілетін өрістер тізімін теңшеу, көрсетілген тізілім сүзгісін сақтау және қайта пайдалану берілген сүзгіге негізделген бірнеше тізілімді көрсету режимдерінің тапсырмаларын жасау және олардың арасында жылдам ауысу.  • Тапсырмалар мен активтер, оқиғалар, осалдықтар және құжаттар арасында байланыстың болуы. Осы нысандар арасындағы бар қарым-қатынастарды көру және жаңаларын құру мүмкіндігі.  • Тапсырма картасынан онымен байланысты нысандарға (активтер, инциденттер және осалдықтар) өту мүмкіндігі.  • Тапсырмаларды орындау мерзімдерін бақылау. Мерзімі біткен тапсырмалар мен мерзімі өтіп кеткен тапсырмалар үшін хабарландыруларды орнату мүмкіндігі.  • Тапсырмалардың күйін визуализациялау, тапсырмалардың маңыздылығын (сындылығын) көрсету, сонымен қатар мерзімі өткен тапсырмалар.  • Тапсырманың орындалу тарихын есепке алу және қарау.  • Тапсырманы бекітуге де, оның орындалу нәтижелеріне де қатысты құжаттарды сақтау және есепке алу.  • Негізгі тапсырмаға сілтеме жасай отырып, оның күйіне автоматты түрде әсер ететін қосалқы тапсырмаларды қолмен жасау мүмкіндігі.  • Әртүрлі жүйе объектілерінің карталарынан тапсырмаларды қолмен жасау мүмкіндігі (пайдаланушы активтері, құжаттар, ескертулерді жою әрекеттері, инциденттер)  • Топтағы активтерді таңдау кезінде контекстік мәзірден бірнеше бағдарламалық түрдегі активтер үшін немесе бірнеше реттелетін активтер үшін тапсырма жасау мүмкіндігі.  • Excel файлдарынан тапсырмаларды импорттау мүмкіндігі.  • Microsoft Excel пішіміндегі файлға тапсырма ақпаратын экспорттау мүмкіндігі.  • осалдықтарды жоюға қатысты тапсырмалар түрі үшін осалдықтарды жою барысын көрсететін көрсеткіштің болуы (прогресс жолағы).  • Оқиғаға қатысты тапсырмалар үшін иерархия мен теңшелетін өрістерді көрсету мүмкіндігі.  Ынтымақтастыққа қойылатын талаптар  • Пайдаланушы рөліне байланысты тапсырмаларды көрсету.  • Тапсырмаға қатысатын пайдаланушылар тобының мүшелері арасында хабар алмасу үшін чаттың болуы.  Орталық басқару кіші жүйесінің құжат айналымы модуліне қойылатын талаптар  Теңшеу мүмкіндігіне қойылатын талаптар  • Құжаттардың әртүрлі түрлерін (бұйрықтар, нұсқаулар, саясаттар және т.б.) жасау және құжаттың әрбір түрі үшін өрістердің құрамын жеке конфигурациялау мүмкіндігі.  Құжаттарды тіркеуге қойылатын талаптар  • Ақпараттық қауіпсіздік құжаттамасын бір репозиторийде жүргізу мүмкіндігі.  • Құжаттар тізімімен жұмыс істеу мүмкіндіктері: құжат тізілімімен жұмыс істеу кезінде пайдаланушыға көрсетілетін бағандарды орнату, құжаттар тізімі бойынша іздеу, тізімді бір немесе бірнеше өрістер бойынша сұрыптау және сүзу, пайдаланушыны сақтау және көрсетілген тізілімді қайта пайдалану. сүзу шарты, берілген сүзу шарты бар қойындыларды жасау.  • Құжаттарды қолмен немесе Excel бағдарламасынан импорттау арқылы жасау мүмкіндігі.  • Құжат картасына кез келген пішімдегі қосымшаларды жүктеп алу мүмкіндігі (жүктелген файл үшін бақылау сомасын автоматты түрде есептеумен).  • Құжат картасынан бір уақытта бір файлды немесе бір мұрағаттағы барлық тіркемелерді жүктеп алу мүмкіндігі.  • Құжаттың өмірлік циклін басқару мүмкіндігі. Құжаттың жарамдылық мерзімін көрсету, сондай-ақ құжатты қайта қараудың белгіленген күні туындаған кезде жауапты пайдаланушыларды автоматты түрде хабардар ету мүмкіндігі.  • Құжаттарды әртүрлі типтегі активтермен байланыстыру мүмкіндігі (АТ активтерінің топтары, ақпарат, бизнес-процестер, бөлімшелер).  • Активтерге, инциденттерге, қорғау шараларына, тапсырмаларға, тәуекелдерді бағалауға, аудиттерге, ескертулерге және ескертулерді жою шараларына ортақ дерекқордан құжаттарды қосу мүмкіндігі.  • Құжат(тар) мен активтер арасындағы байланыстарды топтық өңдеу мүмкіндігі.  • Құжат картасында дәлел ретінде қолданылатын талаптарды көрсетіңіз.  • Құжат картасына бұрын енгізілген өзгерістердің тарихын қарау мүмкіндігі.  Құжаттармен жұмыс істеуге қойылатын талаптар  • Құжатқа жауапты пайдаланушылардың жұмыс тобын конфигурациялау мүмкіндігі. Әрбір қатысушы қол жеткізу деңгейін конфигурациялай алуы керек (оқу, өзгерту).  • Ұйымның барлық қызметкерлеріне оқу үшін құжатқа қол жеткізуді жылдам қамтамасыз ету мүмкіндігі.  Орталық басқарудың ішкі жүйесінің деректерін визуализациялау және көрсету модуліне қойылатын талаптар  Бақылау тақталарымен жұмыс істеуге қойылатын талаптар  • Карталарды, желілерді, еден жоспарларын және активтерді визуализациялау диаграммаларын, оқиға статистикасын көрсететін әртүрлі панельдерден тұратын қойындыларды жасау мүмкіндігі және панельдер арасында жылдам ауысу мүмкіндігі.  • Диаграммалар, графиктер және интерактивті диаграммалар түріндегі ақпаратты визуализациялау. Бақылау тақтасындағы графиктердің санын, өлшемін және орнын теңшеу мүмкіндігі.  • Соңғы жаңарту уақытын көру мүмкіндігімен бақылау тақталарындағы пайдаланушы диаграммаларын автоматты және қолмен жаңарту.  • Активтер мен оқиғаларды геокартада визуализациялау (әлемдік карта). АТ активтері топтарын барлық топтарды бөлек терезеде қарау мүмкіндігімен қысқа тізім ретінде қарау мүмкіндігі.  • OSI моделінің L3 желілік диаграммасында активтерді визуализациялау.  • Геокартадан L3 схемасына көшу мүмкіндігі (интерактивтілік).  • Активтерді қабат жоспарларында көрсету, еден жоспарларын графикалық форматта Жүйеге жүктеу мүмкіндігі.  • Деректерді ұсынудың ресурстық-қызметтік моделін көрсету, физикалық және ақпараттық активтер арасындағы байланыстарды көрсету, оларды жүйедегі бар қосылымдар негізінде диаграммалар бойынша автоматты түрде салу.  • АТ активтерінің топтары үшін желілік карталарды (АТ активтерінің тобын құрайтын жабдық пен желілерді көрсететін диаграммалар) және байланыс диаграммаларын (байланысты активтерді көрсететін диаграммалар) көру мүмкіндігі.  • Ақпараттық қауіпсіздік инциденттерін олардың Жүйенің әртүрлі элементтерімен (мысалы, АТ активтерімен) байланысын көрсетуге мүмкіндік беретін диаграммаларда визуализациялау мүмкіндігі, сонымен қатар жеке өрістердің мағынасын ұсыну.  • L3 диаграммасында және осалдықтар анықталған активтердің қабат жоспарында көрсету, олардың сыни күйін ескере отырып, оқиғалар тіркелген активтер (критикалық дәрежесіне қарай әртүрлі түстермен бөлектеу).  • Объектілерді топтастыру, белгішелердің кескіндері бар алдын ала конфигурацияланған каталогтан топқа белгішелерді тағайындау мүмкіндігі.  • Диаграммаға графикалық элементтерді (сызықтар, шеңберлер, тіктөртбұрыштар) сала білу.  • Көрнекілік панельдеріндегі элементтермен интерактивті әрекеттесу мүмкіндігі: түйіндер туралы қосымша ақпаратты көрсету, оларды топтау, желілік карталарда сүзу, диаграммаларға қатысты элементтерді қосу, графиктер мен диаграммаларды басу арқылы тиісті бөлімге өту мүмкіндігі (төмен қарай жылжыту) .  • Актив туралы қосымша ақпаратты желілік диаграммада немесе ресурс-қызмет диаграммасында (ақпарат пен физикалық активтер арасындағы байланыс диаграммасы) екі рет басу арқылы көрсету мүмкіндігі. Кем дегенде келесі ақпарат көрсетілуі керек: (құрылғы атауы, ОЖ түрі, домен, IP мекенжайы, ОЖ-ға соңғы рет кіру күні туралы ақпарат бар ОЖ пайдаланушыларының тізімі, орнатылған бағдарламалық қамтамасыз ету тізімі, ОЖ қауіпсіздік параметрлері, оқиғалар, осалдықтар туралы ақпарат).  • Графиктерді логикалық топтастыру үшін топтар құру мүмкіндігі. Жүйе графиктерді іздеу, қысқаша сипаттау және алдын ала қарау үшін қолжетімді болуы керек.  Алдын ала анықталған диаграмма үлгілеріне қойылатын талаптар  Жүйеде келесі кестелер тізімі алдын ала орнатылуы керек:  • ұйымның бизнес-процестерінің жай-күйінің жалпы кестесі.  • бөлім бойынша персоналды қорғау;  • жабдықтың тарихы (АТ активтерінің тобы бойынша);  • ашық осалдықтар тарихы (АТ-активтер тобы бойынша);  • ашық осалдықтардың саны (активтер топтары, желілер бойынша);  • желілердегі ашық осалдықтардың саны;  • бағдарламалық қамтамасыз ету топтары бойынша орнатулар санының статистикасы;  • активтер топтары бойынша жабдық көлемінің статистикасы;  • желілердегі жабдықтар санының статистикасы;  • операциялық жүйелердің статистикасы;  • жабдық түрі бойынша статистика;  • артықшылықтар бойынша пайдаланушылар санының статистикасы;  • өндірістегі оқыс оқиғалар;  • өңдеу күйі бойынша оқиғалар;  • жауапкершілік бойынша инциденттер (сындық/мәртебе деңгейін көрсету);  • түрлері бойынша оқиғалар;  • инфрақұрылым объектілеріне қатысты оқиғалар;  • департаменттер бойынша оқиғалар;  • оқиғалар тарихы;  • жауап беру уақытына сәйкес келетін оқиғалардың үлесі;  • оқиғалардан залалдың алдын алу;  • оқиғаларға орташа жауап беру уақыты;  • оқиғалардан залал.  • актив үшін тәуекелді бөлу (сапалық/сандық бағалау).  • актив үшін тәуекелді өңдеу схемасы (сапалық/сандық бағалау).  • тәуекелді емдеу қызметінің күйі.  • актив бойынша тәуекелдер деңгейінің өзгеру тарихы (сапалық/сандық бағалау).  • объектілердің нормативтік талаптарға сәйкестік деңгейін қарау.  • нысан бойынша нормативтік құжат талаптарын орындау.  • элемент бойынша ашық пікірлерді қарау.  • нысан бойынша сәйкестік көрсеткіштерінің өзгеру тарихы.  Диаграммалармен бірлесіп жұмыс істеуге қойылатын талаптар  • Диаграммасы қолжетімді бақылау тақталары мен нысандарға пайдаланушының кіру құқықтарын конфигурациялау мүмкіндігі.  • Әр түрлі пайдаланушы топтары үшін әртүрлі визуализация тақталарын көрсету мүмкіндігі.  • Бір топтың әртүрлі пайдаланушылары үшін визуализация тақталарын теңшеу мүмкіндігі.  • Әрбір пайдаланушы үшін теңшелген карта/желі/басқа элементтер дисплейін сақтау мүмкіндігі.  Орталық басқару кіші жүйесінің есептілікті басқару модуліне қойылатын талаптар  Есептермен жұмыс істеуге қойылатын талаптар  • Жүйеде жинақталған тарихи деректер негізінде есептерді дайындау, құру және қарау;  • Жүйенің негізгі функцияларына сәйкес келетін алдын ала анықталған есептердің болуы.  • Жаңа есептерді құру және бар есептерді өзгерту үшін кіріктірілген құралдардың болуы;  • HTML белгілеуін немесе бағдарламалау тілдерін пайдаланбай кірістірілген есеп үлгілерін өзгерту мүмкіндігі.  • Белгіленген кестеге сәйкес есептерді қолмен және автоматты түрде жасау.  • Жүйедегі құжат деректер базасына есептерді автоматты түрде қосу мүмкіндігі.  • Есептерді портативті деректер пішімі (PDF), DOCX сияқты әртүрлі пішімдегі файлдарға экспорттау;  • Карталарды, еден жоспарларын графикалық форматта экспорттау.  • Жасалған есептерді корпоративтік электрондық пошта арқылы тұтынушылардың белгілі топтарына автоматты түрде тарату мүмкіндігі.  Алдын ала анықталған есептерге қойылатын талаптар  Жүйе келесі есептерді қамтуы керек:  • АТ активтері тобының қысқаша мазмұны – есепте таңдалған АТ активтер тобының ішіндегі аппараттық құралдардың, желілердің, пайдаланушылардың және бағдарламалық құралдың қысқаша мазмұны болуы керек;  • Желілік қорытынды – есепте таңдалған желіде табылған аппараттық құралдардың, пайдаланушылардың және бағдарламалық құралдың қысқаша мазмұны болуы керек;  • Бағдарламалық қамтамасыз ету тізімі – есепте барлық бағдарламалық құралдың немесе бағдарламалық жасақтаманың белгілі бір тобының бағдарламалық құралының қысқаша мазмұны болуы керек;  • Ақпараттық активтер тізбесі – ақпараттық активтердің (ақпараттардың) қысқаша мазмұнын қамтуы тиіс, сондай-ақ олардың бизнес-процестермен және АТ активтерінің топтарымен байланысын көрсететін есеп;  • Бизнес-процестердің тізімі – есепте олардың ақпаратпен және АТ активтерінің топтарымен байланысын көрсететін бизнес-процестердің тізімі болуы керек;  • АТ активтерінің тобына арналған осалдық туралы есеп – есепте АТ активтерінің белгілі бір тобы үшін қауіпсіздік сканері анықтаған осалдықтардың тізімі болуы керек;  • Желінің осалдығы туралы есеп – есепте белгілі бір желі үшін сканер анықтаған осалдықтардың тізімі болуы керек;  • Хосттың осалдығы туралы есеп – есепте белгілі бір хост үшін қауіпсіздік сканері анықтаған осалдықтар болуы керек;  • Бөлме есебі – есепте таңдалған бөлмеде орналасқан жабдықтың, пайдаланушылардың және бағдарламалық қамтамасыз етудің қысқаша мазмұны болуы керек;  • Хост есебі – есепте белгілі бір хосттың қысқаша мазмұны және орнатылған бағдарламалық құрал, ақпараттық қауіпсіздік құралдары, пайдаланушылар, байланысты құжаттар және бар осалдықтар (қауіпсіздік талдауының сканері қосылған болса) туралы ақпаратты қамтуы керек;  • Ақпараттық қауіпсіздік инциденттерінің қысқаша мазмұны – есепте Жүйеде орын алған және тіркелген ақпараттық қауіпсіздік инциденттері туралы жалпы ақпарат болуы керек;  • Ағымдағы оқиға туралы есеп – есепте таңдалған ақпараттық қауіпсіздік оқиғасы туралы толық ақпарат болуы керек;  • АТ активтерінің топтары бойынша оқиғалар – есепте таңдалған кезеңдегі АТ активтері топтары бойынша оқиғалардың таралуы көрсетілуі керек;  • Құрылымдық бөлімшелер бойынша есеп – есепте таңдалған кезеңдегі оқиғаларды құрылымдық бөлімшелер бойынша бөлу көрсетілуі керек;  • Аумақтық бөлімшелер бойынша есеп – есепте таңдалған кезеңдегі барлық аумақтық бөлімшелер бойынша оқиғалардың статистикасы болуы тиіс;  • Белгілі бір уақыт аралығындағы оқиғалардың саны, орындалып жатқандар, жабылған оқиғалар, олардың ауырлық деңгейлері, санаттары мен түрлері бойынша бөлінуі туралы деректерді қамтитын есеп;  • Тапсырманың қысқаша мазмұны – есепте тапсырмалар туралы ақпараттың толық тізбесі, оның ішінде олардың мәртебесінің көрінісі болуы керек;  • Жеке қызметкерлер жауапты болатын ашық және жабық оқиғалардың санын көрсететін есеп. Барлық немесе жекелеген бөлімдер үшін есеп құрастыру мүмкіндігі;  • АТ активтер тобының жаңарту есебі;  • IT активтер тобының бағдарламалық қамтамасыз ету есебі, хост бағдарламалық құралы туралы есеп.  • Талаптардың орындалуын бағалау нәтижелері туралы егжей-тегжейлі есеп – есепте таңдалған аудит бойынша орындалу дәрежесін көрсететін бағаланатын талаптар/критерийлер тізімі болуы керек.  • Жиынтық аудиторлық есеп – есепте анықталған бақылауларды көрсете отырып, таңдалған аудиттер мен бағалау бағыттарының сәйкестігін бағалау нәтижелері туралы толық ақпарат болуы керек.  • Аудиттердің кестесі.  • Сәйкестік туралы жиынтық есеп – есепте таңдалған бағалау аймағына қойылатын әртүрлі талаптарға сәйкестік туралы жалпы ақпарат болуы керек.  • Салыстырмалы аудит есебі – есепте таңдалған талаптың барлық аудиттерінің салыстырмалы сипаттамалары болуы керек.  • Тәуекелдердің егжей-тегжейлі тізілімі – есепте егжей-тегжейлі ақпарат болуы керек – ақпараттық қауіпсіздік тәуекелдерінің анықталған тізімі бар активтердің сипаттамасы.  • Тәуекелді емдеу жоспары.  • Тәуекелдердің шоғырландырылған тізілімі – есепте таңдалған активтер үшін анықталған тәуекелдер тізілімі болуы керек.  API арқылы жүйемен әрекеттесу модуліне қойылатын талаптар  • Жүйе GET және POST сұрау әдістерін қолдауы керек.  • Жүйе API жүйесінде авторизациялау үшін таңбалауыштарды пайдалануы керек.  Жүйе API-де пайдалану үшін келесі сұраулар жинағын қолдауы керек:  Диаграммалармен жұмыс істеуге арналған сұраныстарға қойылатын талаптар: пайдаланушы диаграммаларының тізімін алу, пайдаланушы диаграммасының деректерін алу.  • Жүйе туралы ақпаратты сұрау.  Пайдаланушы активтерімен жұмыс істеуге арналған сұрауларға қойылатын талаптар: пайдаланушы активтерінің түрлерінің тізімін алу, соның ішінде. пайдаланушы активін сүзуді, құруды және өңдеуді, пайдаланушы активтерінің тарихын алуды ескере отырып.  Бөлімшелермен жұмыс істеуге қойылатын талаптарды сұрау  Ұйымдармен жұмыс істеуге қойылатын талаптар:  Рөлдермен және пайдаланушылармен жұмыс істеуге қойылатын сұрау талаптары  Персоналмен жұмыс істеуге сұранысқа қойылатын талаптар  Бизнес-процестермен жұмыс істеуге қойылатын талаптарды сұрау  Жабдықпен жұмыс істеуге қойылатын талаптарды сұрау  Оқиғалармен жұмыс істеуге қойылатын талаптарды сұрау  Оқиға түсініктемелерімен жұмыс істеуге қойылатын талаптар:  Осалдықтармен жұмыс істеуге қойылатын талаптарды сұрау  Тапсырмалармен жұмыс істеуге арналған сұраныстарға қойылатын талаптар  Құжаттармен жұмыс істеуге арналған сұраныстарға қойылатын талаптар   * + 1. **Желілік периметрін қорғау және желілік сегменттер арасындағы қол жеткізуді бақылау жүйесі**   **Желінің қорғау құралдарына қойылатын талаптар:**  Ұсынылған бағдарламалық-аппараттық өнімдер әр алаң үшін (сыртқы және ішкі периметрдегі) қауіптерді анықтау және алдын алу мүмкіндігі бар (Intrusion Detection/ Prevention Systems - IDS/IPS) екі бағдарламалық-аппараттық желілік экрандардан (Next-Generation Firewall - NGFW) тұруы керек.  Бағдарламалық-аппараттық желілік экрандар ақауларға төзімділікті қолдауы керек  Ұсынылған NGFW ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, FedRAMP, Германия C5, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSFNE, USGV6C, USGV6C стандарттарына сәйкес болуы керек.  Жабдық ағымдағы, қолдаудан тыс емес және өндірушінің зауыттарында сыналған болуы керек. Барлық қажетті техникалық құжаттама мен пайдаланушы нұсқаулығы өндіруші ұсынған толық көлемде берілуі керек. Жеткізу пакетінде жеткізілетін Жабдықтың жұмыс істеуін қамтамасыз ету үшін барлық қажетті керек-жарақтар болуы керек.    **Өнімділікке қойылатын талаптар:**  **Ішкі алаң үшін:**  Қосымшалар мен пайдаланушыларды сәйкестендіруді қамтамасыз ететін желілік экрандау режиміндегі құрылғының өткізу қабілеті кемінде 43,5 Гбит/с құрайды.  Қауіпті ескерту және қорғау режиміндегі құрылғының өткізу қабілеті (Application Control, IPS, Anti-Virus, Anti-spyware немесе Anti-bot, Zero Day Attacks Detection және Analysis және құрылғыда логтау) кемінде 26,7 Гбит/с; Бұл көрсеткішті appmix пакеттерімен өлшеу керек. Бұл деректер өндірушінің ресми сайтында жариялануы керек.  IPsec VPN функциясының өткізу қабілеті кемінде 21 Гбит/сек болуы керек.  Құрылғы кем дегенде 10 000 site to site туннельдерін қолдауы керек.  Секундына жаңа сеанстардың максималды саны - кемінде 270 000.  Қолдау көрсетілетін сеанстардың ең көп саны - кемінде 3 600 000.  Жүйе кемінде 6 ай журналды сақтауға мүмкіндік беретін, ол қолдайтын жадтың максималды көлемімен жеткізілуі керек.  Құрылғы бағдарламалық және аппараттық құралдармен бөлінген екі құрамдас бөліктен тұруы керек - құрылғыны басқару құрамдастары және трафикті өңдеу компоненттері. Әрбір компоненттің өз процессорлары (CPU), оперативтік жады (RAM) және интерфейстері (Ethernet порты) болуы керек. Трафикті басқару және өңдеу компоненттері трафиктің маңызды жүктемесі жағдайында, атап айтқанда DoS/DDoS шабуылдары кезінде құрылғыны басқару мүмкіндігін қамтамасыз ету үшін бір-бірінен тәуелсіз болуы керек.  Құрылғыда келесі интерфейстер болуы керек:  100/1000/10G Мыс стандартының кемінде 8 мыс порты.  1/10G SFP/SFP+ стандартының кемінде 12 оптикалық порты.  Кемінде 4 оптикалық порт стандартты 25G SFP28.  Кемінде 4 оптикалық порт стандартты 40/100G QSFP+/QSFP28  Басқару порты бағдарламалық құралдан оқшауланған және трафикті өңдеу үшін желілік порттардан аппараттық құралда бөлек орналасуы керек. Басқару порты құрылғыдағы ақауларға төзімділікті (Management HA порты) қолдауы керек.  Виртуалды маршрутизаторларды қолдау – кемінде 20 дана.  Кемінде 10 виртуалды желіаралық қалқанға лицензияның болуы, кеңейту мүмкіндігімен - 20 және одан да көп.  Ұсынылған жүйеде кемінде 480 ГБ өлшемі бар SSD қатты дискілері болуы керек.  IPv4/IPv6 статикалық маршруттауын және BGPv4, OSPFv2/v3, RIP v2 динамикалық маршруттау хаттамаларын қолдайды. Бұл функция лицензияны қажет етсе, ол ұсынысқа қосылуы керек.  Коммутациялық жабдықтың қосылған Span порттарынан (TAP) «қайталанатын» трафикті тыңдау режимдерінде, MAC және IP мекенжайын (Virtual Wire) өзгертпей мөлдір режимде, трафикті ауыстыру режимінде (Layer 2) желілік интерфейстердің жұмысын қолдау, трафикті бағыттау режимінде (Layer 3).  Бір виртуалды желілік экран шеңберінде шектеусіз кез келген комбинацияда аталған режимдердің кез келгенінде әртүрлі желілік интерфейстердің бір уақытта жұмыс істеуін қолдайды.  Құрылғыны қайта жүктемей-ақ порттың жұмыс режимін өзгертуді (Layer 2, Layer 3, мөлдір режим және тыңдау режимі) қолдайды.  Static және Dynamic (Hide) NAT қолдауы.  Айқын режимде NAT қолдауы.  IPV6 қолдауы, соның ішінде қосымшалар мен пайдаланушы идентификациясы.  Мультихастты маршруттауды және хаттамаларды қолдау – PIM-SM, PIM-SSM, IGMP v1, v2, v3.  Желілік экранда ұйымдастырылған VLAN желілері арасындағы маршруттауды қолдау.  Құрылғы кемінде 4000 вланға қолдау көрсетуі керек.  NAT мекенжайын аудару функциясын, DHCP серверін және DHCP релесін қолдау.  802.1 кадрлық тегтеуді қолдау.  802.3ad арқылы интерфейсті біріктіруге қолдау көрсету (LACP қолдауы).  Үлкенірек пакеттерді тасымалдауға қолдау көрсету (Jumbo жақтаулары).  SNMPv3 қолдауы.  Netflow қолдауы. Netflow профилі физикалық порттар негізінде анықталуы керек.  LLDP (Link Layer Discovery Protocol) қолдайды. Осылайша, құрылғы басқа құрылғылар (MAC мекенжайы, жүйе атауы, оған қосылған порт) туралы ақпаратты бере алуы керек.  IPv4 және IPv6 хаттамалары үшін саясатқа негізделген қайта жіберу саясатын қолдау.  BFD (Bidirectional Forward detection) қолдауы. Бұл маршруттау деңгейіндегі кез келген өзгерістерге жылдам бейімделуге мүмкіндік береді.  Виртуалды маршрутизаторларды қолдау – кемінде 20 дана.  20 дейін кеңейтілетін 10 виртуалды желіаралық қалқанға лицензияның болуы.  Қауіпсіздік аймақтарын қолдау – кемінде 4000 дана.  Сайттан сайтқа және клиенттен сайтқа IPSec VPN қолдауы.  Ең көп мүмкін болатын Client SSL VPN саны кемінде 15 000.  Ең көп мүмкін болатын Clientless VPN желісінің саны кемінде 2500.  IPSEC VPN туннельдерінің саны (сайттан сайтқа) кемінде 10 000 құрайды.  Бір уақыттағы SSL шифрын шешу сеанстарының саны кемінде 360 000 құрайды.  Қауіптерді сканерлеуді және туннель хаттамаларының мазмұнын тексеруді қолдайды: 2-деңгейге дейін GRE, GTP-U, шифрланбаған IPSEC: ESP-null немесе AH.  **Сыртқы алаң үшін:**  Қосымшалар мен пайдаланушыларды сәйкестендіруді қамтамасыз ететін желіаралық экран режиміндегі құрылғының өткізу қабілеті кемінде 20,5 Гбит/с құрайды.  Қауіптерді ескерту және қорғау режимінде құрылғының өткізу қабілеті (Application Control, IPS, Anti-Virus, Anti-spyware или Anti-bot, Zero Day Attacks Detection and Analysis и логирование на устройстве) – кем дегенде 10,5 Гбит/с; Бұл көрсеткішті appmix пакеттерімен өлшеу керек. Бұл деректер өндірушінің ресми сайтында жариялануы керек.  IPsec VPN функцияналының өткізу қабілеті кемінде 12 Гбит/с болуы керек.  Құрылғы кем дегенде 10 000 торап туннельдерін қолдауы керек.  Секундына жаңа сессиялардың максималды саны - кемінде 240 000.  Қолдау көрсетілетін сессиялардың ең көп саны - кемінде 2 500 000.  Жүйе кемінде 6 ай журналды сақтауға мүмкіндік беретін, ол қолдайтын жадтың максималды көлемімен жеткізілуі керек.  Құрылғы бағдарламалық және аппараттық бөлінген екі компоненттен тұруы керек - құрылғыны басқару компоненттері және трафикті өңдеу компоненттері. Әрбір компоненттің өз процессорлары (CPU), жедел жады (RAM) және интерфейстері (Ethernet порты) болуы керек. Трафикті басқару және өңдеу компоненттері трафиктің маңызды жүктемесі жағдайында, атап айтқанда DoS/DDoS шабуылдары кезінде құрылғыны басқару мүмкіндігін қамтамасыз ету үшін бір-бірінен тәуелсіз болуы керек.  Құрылғыда келесі интерфейстер болуы керек:  Кемінде 12 100/1000/10G Мыс стандартты мыс порттары.  1/10G SFP/SFP+ стандартының кемінде 10 оптикалық порты.  Кемінде 4 оптикалық порт стандартты 25G SFP28.  Кемінде 2 оптикалық порт стандартты 40/100G QSFP+/QSFP28  Басқару порты (Management HA порты) бағдарламалық оқшауланған және трафикті өңдеу үшін желілік порттардан аппараттық құралда бөлек орналасуы керек. Басқару порты құрылғыдағы ақауларға төзімділікті қолдауы керек.  Виртуалды маршрутизаторларды қолдау – кемінде 11 дана.  11 немесе одан да көп кеңейту мүмкіндігі бар - кемінде 1 виртуалды файерволдар лицензиясының болуы.  Ұсынылған жүйеде кемінде 480 ГБ өлшемі бар SSD қатты дискілері болуы керек.  **Қолдау көрсетілетін хаттамалар мен ПАК жұмыс істеу режимдеріне қойылатын талаптар:**  - IPv4/IPv6 статикалық маршруттауын және BGPv4, OSPFv2/v3, RIP v2 динамикалық маршруттау хаттамаларын қолдау. Егер бұл функционал лицензияны қажет етсе, онда ол ұсынысқа енгізілуі тиіс.  - Коммутациялық жабдықтың (TAP) қосылған Span-порттарынан «қайталанатын» трафикті тыңдау режимдерінде, MAC және IP-мекенжайын (Virtual Wire) өзгертпей айқын режимде, трафикті коммутациялау режимінде (Layer 2), трафикті маршруттау режимінде (Layer 3) желілік интерфейстердің жұмысын қолдау.  - Бір виртуалды желілік экран ішінде шектеусіз кез келген комбинацияда аталған режимдердің кез келгенінде әртүрлі желілік интерфейстердің бір уақытта жұмыс істеуін қолдайды.  - Құрылғыны қайта жүктемей-ақ порттың жұмыс режимін өзгертуді (2-қабат, 3-қабат, мөлдір режим және тыңдау режимі) қолдайды.  - Статикалық және динамикалық (жасыру) NAT қолдауы.  - NAT қолдауы мөлдіррежимі.  - IPV6 қолдауы, соның ішінде қолданба мен пайдаланушы идентификациясы.  - Мультихастты маршруттауды және протоколдарды қолдау – PIM-SM, PIM-SSM, IGMP v1, v2, v3.  - VLAN аралық бағыттауды қолдау,желілік экранда ұйымдастырылған.  - Құрылғы кемінде 4000 вланға қолдау көрсетуі керек.  - NAT мекенжайын аудару функциясын, DHCP серверін және DHCP релесін қолдау.  - 802.1 кадрлық тегтеуді қолдау.  - 802.3ad арқылы интерфейсті біріктіруге қолдау көрсету (LACP қолдауы).  - Үлкенірек пакеттерді тасымалдауға қолдау көрсету (Jumbo жақтаулары).  - SNMPv3 қолдауы.  - Netflow қолдауы. Netflow профилі физикалық порттар негізінде анықталуы керек.  - LLDP (Link Layer Discovery Protocol) қолдайды. Осылайша, құрылғы басқа құрылғылар (MAC мекенжайы, жүйе атауы, оған қосылған порт) туралы ақпаратты бере алуы керек.  - IPv4 және IPv6 хаттамалары үшін саясатқа негізделген қайта жіберу саясатын қолдау.  - BFD (екі бағытты алға анықтау) қолдауы. Бұл маршруттау деңгейіндегі кез келген өзгерістерге жылдам бейімделуге мүмкіндік береді.  - Қолдау виртуалды маршрутизаторлар – кемінде 11 дана.  - 1 үшін лицензияның болуы виртуалды желілік экран, 11-ге дейін кеңейтіледі.  - Қауіпсіздік аймақтарын қолдау – кемінде 200 дана.  - Сайттан сайтқа және клиенттен сайтқа IPSec VPN қолдауы.  - Максималды сан ықтимал Client SSL VPN – кемінде 2000.  - Максималды сан мүмкін Клиентсіз VPN – кемінде 200.  - IPSEC VPN туннельдерінің саны (сайттан сайтқа) кемінде 8000 құрайды.  - Бір уақыттағы SSL шифрын шешу сеанстарының саны кемінде 250 000 құрайды.  - Қауіптерді сканерлеуді және туннель хаттамаларының мазмұнын тексеруді қолдайды: 2-деңгейге дейін GRE, GTP-U, шифрланбаған IPSEC: ESP-null немесе AH.  **ПАК істен шығуына тұрақтылыққа қойылатын талаптар:**  High-Availability (HA) – Active/Passive қолжетімділігі жоғары істен шығуларға тұрақты кластерді құруға және – Active/Active белсенді режиміндегі кластердің екі желіаралық экранының бір уақытта жұмыс істеуіне қолдау көрсету.  Қолжетімділігі жоғары (HA) кластеріндегі желілік экрандар арасындағы сессиялардың жай-күйін үндестіру арқылы HA Clustering жұмыс режимін қолдау.  HA Clustering жұмыс режимі NGFWs 8 құрылғыға дейін көлденең масштабтауға қолдау көрсетуі керек, сонымен қатар бірнеше таратылған деректер орталықтарымен жұмыс істеуі керек.  Кластер құрамдастары арасында ауысу үшін интерфейсті бақылау және жолды бақылау орындалуы керек.  **ПАК жүйесінің функционалдығына қойылатын талаптар:**  Құрылғы пакетті фильтрлеу және қолданбаны идентификациялау арқылы сеанстардың күйін бақылауы керек (Қызметтік тексеру).  Құрылғы аймаққа негізделген желілік экран болуы керек. Бір немесе бірнеше интерфейстер немесе ішкі интерфейстер бір аймаққа тиесілі болуы мүмкін. Қауіпсіздік ережелері мен NAT саясаттары аймаққа негізделген болуы керек.  NAT саясаттарында қатынау саясаттарынан (қауіпсіздік ережелерінен) тәуелсіз ережелер жиынтығы болуы керек.  желілік экран арқылы өтетін трафик негізінде OSI моделінің жетінші деңгейінде желілік қосымшаларды тану және блоктау, соның ішінде жалпы портты пайдаланатын барлық қосымшалар үшін жеке; динамикалық TCP/UDP порттарын қолданатын 80 және 443.  Layer-7 OSI үлгісінде тексерілген трафикті қолтаңбалар, келесі бағдарламалық жасақтама (қосымшалар), хаттамалар немесе қызметтер арқылы тану:  - аутентификация қызметтері, соның ішінде Microsoft Active Directory, LDAP, RADIUS, TACACS+, Kerberos, SAML, Syslog Monitoring/Parser (Syslog хабарламаларын өңдеу кезінде құрылғы пайдаланушыдан IP салыстыруды қолдауы керек);  - МҚБЖ, соның ішінде Microsoft SQL, Oracle және т.б.;  - файлдық қызметтер, соның ішінде Microsoft SMB;  - электрондық құжат айналымы және хабар алмасу жүйелері, соның ішінде Microsoft Sharepoint, Exchange, Office 365, Google Docs;  - электрондық почта алмасу хаттамалары: SMTP, POP3, IMAP;  - VOIP және аудио-бейне конференция хаттамалары, соның ішінде SIP, H.323, H.245, H.225, Webex, ағынды аудио-бейне (веб-сайттан тәуелсіз), HTTP арқылы аудио және бейне;  - бағдарламалық жасақтаманы жаңарту қызметтері, соның ішінде Microsoft Update, антивирустық бағдарламалық жасақтама, Adobe, Java;  - резервтік көшіру қызметтері;  - виртуализация және терминалға қол жеткізу қызметтері, соның ішінде Vmware, Microsoft RDP;  - қашықтан қол жеткізу хаттамалары, соның ішінде Telnet, SSH, VNC, Radmin;  - желілік хаттамалар, соның ішінде динамикалық маршруттау хаттамалары және SSL/IPSec VPN;  - әлеуметтік желілер, жедел хабар алмасу;  - жұмыс үстеліндегі жариялау құралдары және қашықтан қол жеткізу, соның ішінде Team-Viewer;  - сыртқы прокси-серверлер мен анонимизаторлар, соның ішінде Tor, Ultrasurf, Freegate, SOCKS, PHP Proxy;  - Freenet, Open-vpn, Vtun, RDP-to-TCP, TCP-over-Dns қоса алғанда, басқа қосымшалар арқылы VPN және туннельдерді құруға арналған құралдар.  Шешім YouTube үшін қауіпсіз іздеу режимін және CIPA-үйлесімді Google іздеуін қолдауы керек (прокси режимінде жұмыс істемеуі керек).  HTTP(S), FTP, SMB, SMTP, RPC және т.б. декодерлерді пайдалана отырып, тұрақты өрнектерді пайдалана отырып, сонымен қатар TCP/UDP пакеттерінің мазмұнына масканы пайдалану арқылы жеке қосымша қолтаңбаларын жасау үшін кірістірілген желіаралық қалқан құралдарын қамтамасыз ету;  Шифрланған SSL (2048 битке дейінгі RSA кілттерін қолдау) және желіаралық қалқан арқылы өтетін SSHv2 трафигі (SSL шифрын шешу, SSHv2) арқылы желілік қосымшаларды тану - кіріс және шығыс қосылымдар үшін, домендегі пайдаланушылар үшін мөлдір, басқару мүмкіндігі бар қосымшалардың жеке функциялары, соның ішінде әлеуметтік желілерде хабарламалар жіберу, файлдарды ортақ пайдалану, аудио, бейне ағыны;  Бір сессия ішінде қолданылатын әртүрлі қосымшаларды дәйекті тану;  Қолжетімділікті басқару ережелері осындай қол жеткізудің уақытын, күнін, күнін және кезеңін есепке алу мүмкіндігін қолдауы керек.  Microsoft Active Directory, Microsoft Exchange, LDAP, Novell eDirectory сияқты корпоративтік пайдаланушы аутентификация қызметтерімен біріктіру арқылы желілік қосымшаларды пайдаланатын пайдаланушыларды тану;  Microsoft Active Directory бағдарламасымен біріктіру Active Directory қызметіне өзгертулерсіз жасалуы керек және доменнің Active Directory әкімші есепке алуын пайдаланбауы керек.  Ашық XML API арқылы басқа аутентификация қызметтерімен (мысалы, сымсыз желі контроллерлері) біріктіру мүмкіндігі;  Пайдаланушыларды аутентификациялаған жүйе жіберген жүйе хабарламаларын талдау арқылы пайдаланушы-IP картасын жасау мүмкіндігі.  Ережелерде динамикалық пайдаланушы топтарын құру және пайдалану мүмкіндігі. Динамикалық пайдаланушы топтары сәйкес каталогқа өзгертулер қажетсіз (мысалы, Active Directory) және саясаттарды орнатусыз пайдаланушыны топтан жылдам жоюға (пайдаланушыны топқа қосу) мүмкіндік береді. Бұл рұқсат етілген әкімшілерге немесе сыртқы жүйелерге пайдаланушыны динамикалық пайдаланушылар тобынан жоюға мүмкіндік береді, мысалы, егер қарастырылып отырған пайдаланушы бұзылған болса.  Жіберушінің, алушының, пайдаланылатын қызметтердің (TCP/UDP порттары) IP мекенжайы, пайдаланушы аттары, пайдаланушы топтары және пайдаланушы немесе пайдаланушылар тобы немесе белгілі бір санаттар пайдаланатын қосымшалар туралы ақпаратты жіктеуіштер ретінде пайдалана отырып, бірыңғай қауіпсіздік саясатында ережелерді құру.  Құрылған саясаттар келесі әрекеттерді жүзеге асыруға қабілетті болуы керек:  Рұқсаттар немесе тыйымдар;  Арнайы қолданбаға немесе қосымшалар санатына стандартты немесе қатаң анықталған TCP/UDP порттарын ғана пайдалануға рұқсат беру. Дегенмен, бұл порттарды басқа қосымшалар мұндай өзара іс-қимылге нақты рұқсат беретін саясатсыз пайдаланбауы керек;  Кестеге, пайдаланушыға немесе пайдаланушы тобына негізделген рұқсаттар немесе шектеулер;  Қосымшаларға, IP мекенжайларына, DSCP, пайдаланушылар мен пайдаланушы топтарына негізделген QOS саясаттарын пайдаланып, DSCP таңбалауын және трафик шектеулерін орындау;  Қолданба деңгейінде анықталған нақты уақыттағы трафик үшін QOS енгізу;  IP мекенжайы (көз және/немесе тағайындау), пайдаланушы, қолданба немесе URL мекенжайы негізінде саясатқа негізделген бағыттауды қолдану мүмкіндігі;  Қосымшалар да белгілі бір функционалдылыққа тыйым салу мүмкіндігі;  Жоғарыда аталған әрекеттердің кез келген комбинациясын қолдану мүмкіндігі;  Жеке пайдаланушылар үшін ақ тізім/қара тізім саясаттарын құру мүмкіндігі.  Хаттама трафигінің мазмұнын тексеру:  Жалпы бағыттау инкапсуляциясы;  Шифрланбаған IPsec трафигі (IPsec үшін NULL шифрлау алгоритмі және AH IPsec тасымалдау режимі).  Құрылғы саясатты оңтайландыру функционалдығын қамтамасыз етуі керек, атап айтқанда қосымшаларды пайдалануға негізделген; пайдаланылмаған саясат ережелерін анықтау және жою:  Неғұрлым қатаң ережелер жасау және саясаттарды оңтайландыру үшін құрылғыны басқару интерфейсінде келесі мүмкіндіктер қолжетімді болуы керек:  Анықталмаған қосымшалары бар ережелерді хабарлаңыз, осы ережелер арқылы өтетін қосымшаларды анықтаңыз және тізімдегі қосымшалардан қалағандарын таңдау арқылы ережеде белсендіріңіз.  Жүйе соңғы 7, 15, 30 күн ішінде ережелерде анықталған және пайдаланылмаған қосымшалар туралы есеп бере алады.  Жүйе ережеде анықталған қолданбаның бірінші және соңғы сәйкестендіру күні және оның соңғы 30 күнде қанша өткізу қабілетін пайдаланғаны туралы ақпаратты хабарлау мүмкіндігіне ие.  Жүйе соңғы 30 күнде және 90 күнде пайдаланылмаған ережелерді анықтайды.  Қауіпсіздік ережелері географиялық аймақтарға сәйкес қолданылуы мүмкін; Ережеге бірнеше географиялық аймақтарды қосуға болады.  Өткізу қабілетінің шегі пайдаланушы/топ атауы, мақсатты/көз IP мекенжайы және бағдарлама негізінде қолданылуы мүмкін.  Бұл пакеттер негізгі процессордың немесе виртуалды NGFW буферінің ресурстарын пайдаланбас бұрын, желіаралық қалқанның бөлек бөлігі арқылы белгілі бір көздерден трафикті автоматты түрде блоктау мүмкіндігі.  Microsoft Windows ортасындағы жаңа ықтимал зиянды файлдарды, соның ішінде желі арқылы тасымалданатын орындалатын файлдарды (EXE, DLL, SCR, BAT және т.б.), SMTP/POP3 электрондық почта хабарларында, соның ішінде SSL арқылы шифрланған хабарларды сканерлеу қызметінің болуы, жеке немесе сыртқы бұлтта («құмсалғыш») күдікті файлдар мен сілтемелердің әрекетін қамтамасыз ету, жаңа зиянды бағдарламаны анықтау және 24 сағат ішінде антивирустық қолтаңбаны автоматты түрде жасау және 30 минут ішінде URL беделінің дерекқорын жаңарту.  Визуализация функциялары әзірленді: желілік қосымшалардың белсенділігінің қарапайым және ыңғайлы форматында визуализация, пайдаланушылар пайдаланатын қосымшалардың анықталған және блокталған желілік қауіптері. Әртүрлі сүзгілер арқылы ақпаратты фильтрлеу мүмкіндігі (қолданба бойынша, қауіп бойынша, пайдаланушы, IP мекенжайы, TCP/UDP порты, қауіпсіздік аймағы, қауіп түрі және т.б.).  Есептерді құра білу. Желілік экранда жасалған есептерді қолмен орнату үшін әртүрлі тақырыптық функциялар бойынша есептерді және жоспарланған есептерді автоматты түрде жасау функциялары болуы керек. Есептерді тікелей желіаралық қалқан веб-негізделген графикалық интерфейсі (GUI) арқылы және есептерді PDF және CSV пішіміне экспорттау мүмкіндігі арқылы көру мүмкіндігі болуы керек.  Бір өндірушінің орталықтандырылған басқару, журнал жүргізу, есеп беру және желілік экран бағдарламалық құралын жаңарту ішкі жүйесімен біріктіру мүмкіндігі бар.  Орталықтандырылған тіркеу ішкі жүйесінің қысқа мерзімді қолжетімсіздігі жағдайында журналдарды арнайы виртуалды машина дискі кеңістігіне жергілікті түрде буферлеу мүмкіндігі.  Жергілікті әкімшілер үшін рөлге негізделген қатынасты басқару мүмкіндігі бар:  жалпы виртуалды құрылғы, сондай-ақ жеке виртуалды жүйелер (контекстер) деңгейінде қарау және басқару аймағын шектеу мүмкіндігі;  Тек оқуға арналған өңдеу режимінде қол жеткізуді қамтамасыз ету немесе желіаралық қалқан веб-интерфейсінің кез келген бөліміне кіруге тыйым салу мүмкіндігі;  Тек оқуға арналған өңдеу режимінде қатынасты қамтамасыз ету немесе CLI желілік экраніне кіруге тыйым салу мүмкіндігі.  Қауіпсіздік саясаттары мен желі параметрлері әкімшінің жұмыс станциясында кез келген қосымша басқару бағдарламалық құралын орнатудың қажетінсіз HTTPS және SSH хаттамалары арқылы басқарылуы керек.  Желілік экранды басқару интерфейсі (веб және CLI) орталықтандырылған басқару, журнал жүргізу, есеп беру және бағдарламалық құралды жаңарту үшін ішкі жүйемен біріктірілген болуы керек; [Жүйе болашақта орталықтандырылған басқару серверін қосуға мүмкіндік беруі керек].  Қауіпсіздік саясаттарын орнату қажеттілігінсіз XML API арқылы қауіпсіздік ережелеріндегі осындай топтарды динамикалық түрде жаңартуға мүмкіндік беретін динамикалық мекенжай тобына және динамикалық пайдаланушы тобына қолдау көрсету.  Ішкі қосымшалар үшін мәжбүрлі көп факторлы аутентификацияны қолдау.  **ПАК жүйесіне зиянды немесе тыйым салынған трафиктің енуін болдырмау, тану және бұғаттау мүмкіндіктеріне қойылатын талаптар:**  Құрылғыларда архитектуралық тексеру, IP пакеттерін фильтрлеу және қосымшаларды тану мүмкіндіктері болуы керек және келесі қауіпсіздік қызметтері болуы керек: Келесі ұрпақ желілік экраны (NGFW), IPSEC VPN, SSL VPN, қосымшаларды басқару, вирусқа қарсы/антивирустық бағдарлама, шабуылдан қорғау қызметтері (IPS) ), Анти-шпиондық бағдарлама (антиспад/антибот), DNS хаттамасы (DNS қауіпсіздігі) арқылы шабуылдарды блоктау, URL фильтрлеу, Пайдаланушы идентификациясы үшін каталогтармен интеграция (Identity Awareness).  Желілік экран арқылы нақты уақыт режимінде қолтаңбалар мен мінез-құлыққа негізделген ағында трафик мазмұнын тексеру мүмкіндігі, осалдықтардан, желілік шабуылдардан және зиянды бағдарламалардан қорғау, қолтаңбалары бойынша файл түрлерін тану, веб, электрондық почта, FTP арқылы берілетін вирустарды анықтау. SMB, шпиондық бағдарлама, желі құрттары, белгілі бір мазмұнды тұрақты өрнектерді, соның ішінде SSL және SSHv2 шифрлауын қолданатын қосымшалар арқылы жіберуді блоктау.  Вирусқа қарсы қорғау, шпиондық бағдарламадан қорғау, осалдықтар мен желілік шабуылдардан қорғау (интрузияны анықтау және алдын алу жүйесі), динамикалық бедел базасын пайдаланып URL фильтрлеу, бір веб-сайттың әртүрлі бөлімдері үшін санаттарды қолдау, соның ішінде әртүрлі веб-сайттар санаттарына қолдау көрсету тілдер, түрі бойынша файлдарды тасымалдауды блоктау, арнайы қолтаңбалар.  Вирусқа қарсы қорғаныстан, шпиондық бағдарламадан қорғаудан, осалдықтардан және желілік шабуылдардан қорғаудан, қауіптерден және 0-күндік вирустардан қорғаудан алынған ақпаратты пайдаланатын жаңартылған корреляция объектілерін пайдалана отырып, желіаралық қалқандағы ақпараттық қауіпсіздік оқиғаларының автоматты корреляциясы жүйелерімен біріктіру мүмкіндігі.  Бір сеанс ішінде жасалған әртүрлі типтегі журналдардың автоматты корреляциясы (желілік экран, қауіптен қорғау, файлдарды жіберуді басқару, URL фильтрлеу).  Құрылғыда келесі кіруді болдырмау жүйесінің (IPS) мүмкіндіктері болуы керек:  Әртүрлі пайдаланушылар немесе пайдаланушы топтары үшін әртүрлі IPS саясаттарын жасау мүмкіндігі.  CVE, маңыздылық деңгейлері және хост түрі (клиент/сервер) арқылы құрылғыда IPS қолтаңбаларын іздеу мүмкіндігі.  Төмендегідей шабуылдарға жауап беру үшін IPS жүйесінің қолтаңбаларын жеке конфигурациялау мүмкіндігі: Рұқсат ету, Ескерту, Бас тарту, қалпына келтіру-екеуін, қалпына келтіру-клиент, қалпына келтіру-сервер, Блок-IP. IP негізіндегі блоктау бастапқы IP негізінде және бастапқы және тағайындалған IP екеуінде орындалуы керек.  Шабуылдарға қарсы қолданылатын IPS сүзгілері жаңарту файлынан немесе Интернет арқылы жаңартылуы керек. Сонымен қатар, қажет болған жағдайда қолтаңбалар пайдаланушының араласуынсыз автоматты түрде жаңартылуы керек.  Ұсынылған IPS функционалдығы қолданыстағы қолтаңбаларға сүйенбестен шабуылдарды блоктауға мүмкіндік беретін қолданылған аномалиялардағы ауытқуларды анықтау технологиясын қамтуы керек (Protocol Anomaly Detection).  IPS функционалдығы келесі шабуылдарға төтеп беруі керек:  (Қатыгез күш, код/команданы орындау, Sql-инъекция, эксплуатация жинағы, қызмет көрсетуден бас тарту, ақпараттың жайылып кетуі, толып кету, сканерлеу және т.б.)  Құрылғыда келесі мүмкіндіктермен антишпиондық/анти-ботты анықтау және блоктау функциясы болуы керек:  Бұл функция порт пен хаттамаға қарамастан жұмыс істеуі керек және Интернетке барлық IP-трафикті тексеруі керек;  Botnet командалық және басқару орталықтарының IP мекенжайлары үшін рұқсат сұрауларын анықтау және оларды DNS сұраулары арқылы блоктау;  DNS Sinkhole функциясы зиянды домендік атауды сұрау кезінде әкімші тағайындаған IP мекенжайын қайтаруы керек. Осылайша жұқтырған жүйелерді оңай анықтауға болады;  Қолтаңбаларды пайдаланып белгілі ботнеттерді блоктау функционалдығы. Жүйе әкімшіге ботнет қолтаңбаларын конфигурациялауға рұқсат беруі керек;  Қолтаңба әрекеттері үшін келесі әрекеттер қолжетімді болуы керек: Рұқсат ету, Ескерту, Бас тарту, ысыру-екеуін, қалпына келтіру-клиент, қалпына келтіру-сервер, Блок-ip;  Әртүрлі пайдаланушылар мен пайдаланушы топтары үшін шпиондық бағдарламаға қарсы әртүрлі саясаттар жасалуы керек;  Шпиондық бағдарламаға қарсы функция келесі шабуылдарды анықтауды және блоктауды қамтуы керек: жарнамалық бағдарлама, ботнеттер, бэкдор, браузерты ұрлау, деректерді ұрлау, клавиатура, шпиондық бағдарлама, желі құрты, p2p-коммуникация.  Құрылғыда келесі мүмкіндіктері бар антивирусты анықтау және ескерту функциясы болуы керек:  Белгілі зиянды бағдарламаларды қолтаңба негізінде блоктау;  Ағынды сканерлеу мүмкіндігі болуы керек. Мұрағатталған файлдарды сканерлеу керек;  Антивирустық архитектура Active Directory-мен біріктіру мүмкіндігі болуы керек, осылайша Антивирус ережелері Active Directory ішіндегі пайдаланушы немесе пайдаланушы тобы негізінде анықталуы мүмкін;  Қолтаңба деректер базасынан антивирустық қолтаңбаларды алып тастау мүмкіндігі (ерекшеліктерді орнату мүмкіндігі);  Әртүрлі пайдаланушылар мен пайдаланушы топтары үшін әртүрлі антивирустық саясаттар жасалуы керек;  Антивирус FTP, HTTP, SMB, POP3, IMAP, SMTP хаттамалары арқылы жіберілетін зиянды файлдарды блоктауы керек.  Құрылғыда URL фильтрлеу функциясы болуы керек.  Құрылғыда пайдаланушы идентификациясын басқару функциясы арқылы фишингтік шабуылдардан қорғаныс болуы керек. Ұсынылған шешім HTTP/HTTPS POST деңгейінде пайдаланушы (логин) және құпия сөз ақпаратын жіберуді/ұрлауды болдырмауға қабілетті болуы керек. Ол Active Directory интеграциясында пайдаланушы есепке алу деректерін басқара алуы керек. Ұсынылған шешімге тиісті лицензия қосылуы керек.  Құрылғылар SSL/TLS және SSH шифрын шеше алуы керек. TLS 1.0, TLS 1.1, TLS 1.2 және TLS 1.3 хаттамаларының шифрын шешуге қолдау көрсету.  Құрылғы HTTPS трафигін тексеріп, IPS, қолданбаны басқару, URL сүзгісін және антивирустық қорғауды қолдана алуы керек.  Құрылғы кіріс және шығыс бағытта HTTPS шифрын ашуы керек.  Құрылғы сандық кілттерді басқару үшін HSM (Аппараттық қауіпсіздік модулі) интеграциясын қолдауы керек.  VxLAN туннельдерін тексеруді қолдау  HTTPS трафикті тексеру (шифрын шешу) ережелері пайдаланушы аты/пайдаланушы тобы, бастапқы IP/желі/аймақ, тағайындалған IP/тағайындалған желі/тағайындалған аймақ және URL санаты негізінде құрылуы керек.  Құрылғы HTTPS трафигінің мазмұны көрінбейтін жағдайда (банктік транзакциялар және т.б.) шифрды шешуді болдырмайтын ережелерді жасау мүмкіндігін қамтамасыз етуі керек.  HTTPS сеанстарының сертификатын тексеру және мерзімі өткен, сенімсіз немесе күші жойылған сертификаттары бар сеанстарды болдырмау мүмкіндігі болуы керек.  Құрылғы SSL веб-трафикінің шифрын шеше алуы және трафикті көрсету функциясын пайдаланып, шифры шешілген трафиктің көшірмесін сыртқы аналитикалық құрылғыларға жіберуі керек. Ұсынысқа тиісті лицензия қосылуы керек.  Жүйе бірнеше географиялық аймақтармен бір ережені құру мүмкіндігімен географиялық аймаққа сәйкес қауіпсіздік ережелерін қолдана алуы керек.  Ұсынылған NGFW мүмкіндіктері бар Windows, Mac OS, Linux, IOS және Android үшін қашықтағы VPN пайдаланушы агентін ұсынуы керек:  СІМ қолдауы;  Құрылғы негізіндегі қауіпсіздік саясатының орындалуын қолдау;  AirWatch немесе MobileIron сияқты үшінші тарап MDM шешімдерімен интеграцияны қолдайды;  IP мекенжайлары, домендері және қосымшалары негізінде бөлінген туннельді қолдайды;  Cookie файлдары арқылы VPN аутентификациясын қайта анықтауды қолдау;  Қашықтағы пайдаланушының негізгі VPN туннелінен бейне трафигін алып тастауды қолдау;  SSL жүктеу сияқты мүмкіндіктерді қосуға көмектесу үшін қашықтағы VPN пайдаланушы құрылғыларына сенімді түбірлік сертификаттарды жіберуге қолдау көрсету;  Бастапқы пайдаланушы идентификаторы, аймақ, операциялық жүйе және IP мекенжайы негізінде VPN шлюзін таңдауды қолдау.  **NGFW қойылатын қосымша міндетті талаптар:**  Құрылғы сыртқы динамикалық IP/URL/домен блоктау тізімдерін жасауды қолдауы керек. Құрылғы бұл тізімге HTTP арқылы кіруі керек. Осы тізімге өзгертулер енгізген кезде, құрылғы саясаттарды құрылғының өзінде орнатпай (қолданбай) осы IP/URL/домендерді автоматты түрде блоктауы (немесе саясат жиынтығына байланысты рұқсат беруі) керек. Тізімдердің сыйымдылығы кемінде 150 000 IP және URL мекенжайларын және кемінде 4 000 000 домен атауларын қамтуы керек.  Өндірушінің кибер барлау қызметі анықтаған зиянды IP мекенжайларының тізімі құрылғыда үнемі жаңартылып отыруы керек. Осылайша, бұл IP мекенжайларына кіру блокталуы мүмкін.  Жүйеде SYN Flood, UDP Flood, ICMP Flood қарсы тұру үшін бір уақыттағы сеанстардың шекті санын конфигурациялау мүмкіндігі болуы керек.  Жүйе портты сканерлеуді анықтау және блоктау мүмкіндігі болуы керек: TCP портын сканерлеу, UDP порттарын сканерлеу және сканерлеу.  Сақтық көшірме жасау ережелерін қайта жүктеуді қажет етпестен жалғастыру және белсендіру қажет.  NGFW пайдаланатын барлық қызметтер NGFW белсендірілген күннен бастап 31.12.2025ж. дейін бағдарламалық құрал жаңартуларын және қауіпсіздік қолтаңбаларын (мысалы, қосымшаларды басқару, деректерді фильтрлеу, IPS, антивирус, антишпиондық бағдарлама, SSL шифрын шешу) алу мүмкіндігіне ие.  Ұсынылған NGFW әзірлеу құралдарына, құралдарына, сценарийлеріне және үлгілеріне қол жеткізу үшін төлемдік қабырғасыз (жазылымсыз) үздіксіз ашық API қолдауы керек.  **NGFW сервистік қолдауға қойылатын талаптар:**  бағдарламалық қамтамасыз ету қызметін қолдау, мүмкіндігі бар:  Сертификатталған инженерлермен Қазақстандағы NGFW өндірушісінің бірінші желілік қолдауына жергілікті қолжетімділік;  Телефон немесе онлайн байланыс (чат және электрондық почта);  Жүктеп алу жаңартуларына, түзетулеріне қол жеткізу;  Құжаттамаға қол жеткізу.  **Көші-қон қызметтері жүйесін өрістетуге қойылатын талаптар**  Орындаушының техникалық тобы жүйені бастапқы орналастыруға және көшіру қызметтеріне, соның ішінде:  АТ архитектурасын талқылау және жоспарлау, құрылғыларды тіркеу, барлық лицензияларды белсендіру, операциялық жүйенің таңдаулы нұсқасын және динамикалық жаңартулардың соңғы нұсқасын орнату, құрылғылардың High Availability функционалдығын конфигурациялау.  Ағымдағы «сол қалпында» конфигурациясын бар жабдықтан жаңа жабдыққа ауыстыру, оның ішінде: Қауіпсіздік аймақтары; Интерфейс конфигурациясы; Маршруттау; NAT саясаты; Қауіпсіздік саясаты; Қауіпсіздік профильдері; Адрес нысандары және мекенжай топтары; Zone Protection конфигурациясы; Аутентификация қызметтерімен интеграция; Пайдаланушыны сәйкестендіру конфигурациясы; Әкімшілер мен әкімшілік рөлдердің конфигурациясы; VPN конфигурациясы;  Техникалық топ сертификаттаудың ең жоғары деңгейіне ие болуы керек  **Желіні қорғауға арналған бағдарламалық-аппараттық кешендерге (ПАК) арналған басқару жүйесі.**  Желілік экранның орталықтандырылған басқару жүйесіне, журналға, есеп беруге және бағдарламалық қамтамасыз етуді жаңартуға (бұдан әрі – Орталықтандырылған басқару жүйесі) қойылатын талаптар:  - Барлық үлгілер мен нұсқаларды қолдайдыЖелілік экран бағдарламалық жасақтамасы бағдарламалық және аппараттық желілік экранмен бірдей өндірушіден;  - Бір өндірушінің NGFW-мен веб-интерфейстің унификациясы - ұқсас басқару элементтерібасқару элементтері, бөлімдер, бетбелгілер және графикалық дизайн;  - CLI бір өндірушінің NGFW-мен біріздендіру - ұқсас командалар;  - Орталықтандырылған басқару жүйесінің веб-интерфейсінің веб-басқару интерфейсіне ауысу мүмкіндігінақты NGFW және керісінше;  - Орталықтандырылған басқару жүйесіне лицензия 25 NGFW құрылғысын басқаруға мүмкіндік беруі керек  **Орталықтандырылған басқару функцияларына қойылатын талаптар:**  - Басқарылатын NGFW-ларды топтарға біріктіру мүмкіндігі - физикалық құрылғылар да, жеке виртуалды жүйелер де (контекстер);  - жергілікті мүмкіндіктерді ескере отырып, біркелкі ақпараттық қауіпсіздік параметрлерін қолдану және желі мен жүйе параметрлерін кейінгі түзетулермен қайталау мүмкіндігі;  - Құрылғылар топтарына орталықтандырылған нысан параметрлерін қолдану мүмкіндігі:Адрес объектілері (IP мекенжайлары, FQDN) және топтар; кірістірілген NGFW құралдарымен жасалған қолданба және қауіп қолтаңбалары; статикалық және динамикалық қолданбалы топтар; жасалған URL санаттары; динамикалық URL сүзгісін, енуді анықтау және алдын алу жүйелерін (IDS/IPS), антивирустық қорғауды, шпиондық бағдарламалардан (соның ішінде ботнеттерді) және DoS шабуылдарынан қорғауды орнатуға арналған профильдер; журнал жіберу профильдері; саясат кестесі.  - Құрылғылар топтарына орталықтандырылған саясат параметрлерін қолдану мүмкіндігі: Ақпараттық қауіпсіздік (желілік экран және қауіптен қорғау); SSL және SSHv2 шифрын шешу; QoS; Қолданбаны қайта анықтау; DoS шабуылдарынан қорғау.  - Саясаттарды топтағы жеке құрылғыларға, сондай-ақ барлығына таңдап қолдану мүмкіндігі, кейбіреулерін қоспағанда.  - Құрылғыда орталықтандырылған және жергілікті саясаттарды біріктіру мүмкіндігі. Бұл жағдайда орталықтандырылған саясаттар мен нысандар тек оқуға арналған режимде жергілікті әкімшіге қолжетімді болуы керек.  - Барлық желі және жүйе параметрлері үшін конфигурация үлгілерін құрылғылар топтарына қолдану мүмкіндігі, соның ішінде: NGFW қолдауына байланысты виртуалды жүйелерді (контексттерді) құру; Әкімші рөлдерін орнату, сәйкестендіруAI және пайдаланушының аутентификациясы; Қауіпсіздік аймақтарын конфигурациялау, желі интерфейсінің параметрлерін (түрі, IP мекенжайы), маршруттау, VLAN, IPsec/SSL VPN, QoS; Желілік экран аймақтарын L3-L4 шабуылдарынан қорғауды конфигурациялау, соның ішінде су тасқыны, желіні сканерлеу және TCP/UDP тақырыптарын өзгерту.  - Үлгілерді орталықтан қолданғаннан кейін жергілікті әкімшіге желі мен жүйе параметрлерін таңдаулы түрде реттеуге рұқсат беру.  - Журналдарды қабылдау және сақтауБір өндірушінің NGFW пішімі.  - Екі деңгейлі тіркеу және есеп беру жүйесін қолдау: Журналға тіркеу серверінің рөлі қосылған ME журналдарын сақтау болып табылады; Басқару серверінің рөлі орталықтандырылған конфигурациялау және тіркеу серверлерінде тарату арқылы сақталған деректер негізінде есептерді құру, есептерді біріктіру; Бір құрылғыда басқару және тіркеу серверінің рөлдерін біріктіру мүмкіндігі.  - Трафик пен қауіптердің визуализациясы, бірдейбөлек NGFW-ге, бірақ жинақталған журналдар мен статистикаға негізделген.  - Есептердің барлық түрлерін құру мүмкіндігі, бірдейбөлек NGFW-ге, бірақ жинақталған журналдар мен статистикаға негізделген.  - Әрбір модель үшін орталықтандырылған бағдарламалық жасақтаманы жаңарту мүмкіндігіNGFW басқарады.  - Қолданба мен қауіп қолтаңбаларын орталықтан жаңарту мүмкіндігі.  - Лицензиялардың, жазылымдар мен өндірушінің техникалық қолдау келісім-шарттарының қолжетімділігі мен өзектілігін орталықтан басқару мүмкіндігі.  - Рөлге негізделген әкімші қатынасын басқару: Басқарылатын МС топтары деңгейінде қарау және басқару аймағын, сондай-ақ жеке құрылғыларды шектеу мүмкіндігі; Тек оқу үшін өңдеу режимінде қол жеткізуді қамтамасыз ету немесе бағдарламалық қамтамасыз етуді басқару, тіркеу, есеп беру және жаңарту веб-интерфейсінің кез келген бөліміне кіруге тыйым салу мүмкіндігі; Өңдеу режимінде тек оқуға рұқсатты қамтамасыз ету немесе CLI-ге кіруге тыйым салу опциясы.  - Cisco ACI контроллерімен біріктіру мүмкіндігі, NGFW желілік экранын қызмет ретінде 4-деңгейден 7-деңгейге дейін EPG арасында енгізуге мүмкіндік береді, осы EPG-лердегі бағдарлама деңгейлері арасындағы Шығыс-Батыс трафикті және пайдаланушылар мен бағдарламалар арасындағы Солтүстік-Оңтүстік трафикті тексеруге мүмкіндік береді.  - NGFW басқаратын IPS ішкі жүйелері үшін Snort және Suricata қолтаңбаларын түрлендіру мүмкіндігі.  **Басқару жүйесін сервистік қолдауға қойылатын талаптар:**  Кемінде 12 ай бойы бағдарламалық жасақтаманың сервистік қолдауы, келесі мүмкіндігімен: Қазақстандағы басқару жүйесін өндірушіден сертификатталған инженерлермен қолдаудың бірінші желісіне жергілікті қолжетімділік; Телефон немесе онлайн байланыс (чат және электрондық почта); Жаңартуларды, түзетулерді және құжаттаманы жүктеп алу мүмкіндігі.  **Жүйені өрістетуге қойылатын талаптар**  Орындаушының техникалық тобы жүйені бастапқы орналастыруға көмектесуі керек, соның ішінде: Таңдалған виртуалдандыру жүйесінде басқару жүйесінің кескінін орналастыру (тапсырыс беруші береді), Құрылғыны тіркеу; Барлық лицензияларды белсендіру; Операциялық жүйенің таңдаулы нұсқасын және динамикалық жаңартулардың соңғы нұсқасын орнату; Басқару жүйесіне барлық қажетті NGFW қосу; Әкімшілер мен әкімшілік рөлдерін құру;  Техникалық топ сертификаттаудың ең жоғары деңгейіне ие болуы керек  **Желілік периметрді қорғау және желілік сегменттер арасындағы қол жеткізуді басқару жүйесінің құрамдас бөліктері бойынша оқытуға қойылатын талаптар**  Тапсырыс беруші тарапынан оффлайн оқытуды өткізу мүмкіндігі.  **Желілік периметрді қорғау және желілік сегменттер арасындағы кіруді басқару жүйесіне екі факторлы аутентификация**  **Екі факторлы аутентификацияға қойылатын талап**  Интернетке қосылуды қажет етпейтін екі факторлы аутентификацияны қамтамасыз ету.  Мобильді қосымша, push-хабарлама, SMS хабарлама немесе белгі арқылы бір реттік парольді алу мүмкіндігі.  Бір реттік құпия сөздерді жеткізу жолдарын көрсету мүмкіндігі.  Әрбір пайдаланушы үшін құпия сөздерді жасаудың бірегей алгоритмі.  Active Directory-мен интеграция.  Доменсіз инфрақұрылымда пайдалану мүмкіндігі.  LDAP және MAC Open Directory қолдауы.  Жергілікті есепке алу үшін де, жұмыс істеп тұрған жүйе үшін домен есепке алу үшін де қауіпсіз кіру үшін 2FA қосу мүмкіндігі: Microsoft Windows, Linux немесе MAC OS X.  OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence сияқты бұлттық қызметтерге (қызмет провайдеріне) және сәйкестендіру провайдеріне 2FA қамтамасыз ету үшін Identity Provider Connector қолжетімділігі.  Сақтық көшірме құпия сөзін пайдалану мүмкіндігі (басты қалпына келтіру кілті).  OATH, HOTP, TOTP, FIDO, FIDO2 стандарттарына сәйкес жұмыс істейтін аппараттық токендерді қолдау.  VPN және VDI жүйелерін қорғау, мысалы: Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC, Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, Nesqta , VMware Horizon View және Citrix XenApp, Cyberoam.  VPN қосылымдарын қорғау үшін екі факторлы аутентификацияны пайдалану мүмкіндігі, Қашықтағы жұмыс үстелі хаттамасы , ОЖ-дағы авторизация, Microsoft ADFS 3 немесе 4 пайдаланатын веб-қызметтері, Microsoft Web Apps, Microsoft Exchange сервері, Microsoft Share Point Server, қашықтағы жұмыс үстелі веб-қатынауы, Microsoft Dynamics CRM, VMware Horizon View, RADIUS негізіндегі қызметтер.  Office 365 немесе Azure жүйесіне кіру үшін SSO және Microsoft Active Directory Федерациясы қызметтері арқылы қауіпсіздік.  Windows Safe Mode және PC Locked Mode режимінде екі факторлы аутентификацияны пайдалану.  UAC қатынасын екі факторлы аутентификация арқылы қорғау.  Linux/Mac OS үшін RADIUS PAM, (SSH қорғау, cli кіру, GUI кіру). (AD мүшелігіне байланысты).  Екі факторлы аутентификацияны қажет етпейтін IP мекенжайларының ақ тізімдерін жасау мүмкіндігі; Кез келген пайдаланушы қолданбасымен екі факторлы аутентификацияны пайдалануға мүмкіндік беретін API және SDK пакеттерінің болуы  Белсенді/Пассивті режимде бірнеше серверлердің ақауларға төзімді конфигурациясын пайдалану мүмкіндігі.  Пайдаланушыға аутентификацияны растау немесе қабылдамау опциясы бар авторизация әрекеті туралы хабарлау.  Бақылау тақтасы үшін де, есептерді шығару үшін де пайдалануға болатын есеп беру жүйесінің болуы.  Екі факторлы аутентификация қызметінің конфигурациясына, іске қосылуына және тоқтауына қатысты барлық өзгерістерді жазатын және қадағалайтын аудит журналының болуы.  SIEM және басқа бақылау, талдау және жауап беру жүйелерімен интеграциялау мүмкіндігі.  Пайдаланушының таңбалауышқа немесе мобильді қосымшаға кіру мүмкіндігі болмаған жағдайда әкімшінің бір реттік балама OTP құпия сөзін ұсыну мүмкіндігі.  CSV немесе LDF арқылы пайдаланушыларды теңшелетін аймақтарға импорттау мүмкіндігі.  2FA серверіне қосылмаған компьютерлер үшін бір реттік құпия сөздерді пайдалануды шектеу мүмкіндігі.  Пайдаланушыны блоктау арқылы бір реттік парольді болжаудан қорғаудың болуы.  Таңдалған әрекеттер түрлері туралы хабарландыру жүйесінің болуы.   * + 1. **Соңғы жұмыс станцияларын бақылау жүйесі (антивирустық қорғау)**   Соңғы жұмыс станцияларын басқару жүйесі келесі функцияларды қамтамасыз етуі керек:  **Басқару сервері**  - Бүкіл желілік инфрақұрылымды антивирустық қорғауды орталықтандырылған басқару мүмкіндігі.  - Негізгі сервер мен бағынышты серверлерден тұратын иерархиялық басқару құрылымын құру мүмкіндігі, ол негізгі және аймақтық бөлімдерге де жататын жұмыс станцияларын, серверлерді және мобильді құрылғыларды антивирустық қорғауды орталықтан басқаруға мүмкіндік береді.  - Жеке желілік экран, нақты уақыттағы қорғау, электрондық почта клиентін қорғау, Интернетке кіруді қорғау, құрылғыны басқару, веб-бақылау, бір клиентте спамнан қорғау сияқты қорғау модульдерін қашықтан қосу және өшіру мүмкіндігі.  - Қашықтан басқару құралының көмегімен қосымша желілік әрекеттерді орындау мүмкіндігі, мысалы: өшіру және қайта жүктеу, компьютерді ояту сигналын жіберу, хабарламаларды жіберу, клиенттік компьютерде пәрмен жолы бойынша арнайы нұсқауларды орындау, клиенттік компьютердің жаңартуын бастау. операциялық жүйе.  - Соңғы нүктелерде антивирустық өнімді қашықтан басқаруға, сондай-ақ жұмыс станцияларындағы антивирустық қорғау деңгейін және операциялық жүйенің күйін бақылауға мүмкіндік беретін тәуелсіз агентті пайдалану.  - Мына дерекқорларды қашықтан басқаруды қолдау: MS SQL Server, MySQL.  - Үшінші тарап HTTP серверлері негізінде жаңарту айнасын жасау мүмкіндігі.  - Журнал мен есеп параметрлерін теңшеу немесе әртүрлі жүйелер/клиенттер үшін 50-ден астам үлгіні таңдау мүмкіндігі.  - Жұмыс станциясында орнатылған бағдарламалық құралды бақылау, сондай-ақ таңдаған орнатылған бағдарламалық құралды жою мүмкіндігі.  - Тіпті физикалық немесе қашықтан қол жеткізу мүмкіндігі жоқ жұмыс станцияларында да антивирус өнімдерінің лицензиясын өшіру мүмкіндігі.  - Лицензияның сәйкес бөлігі бар сайттың немесе филиалдың әкімшісін анықтау функционалдығының болуы.  - VDI жүйелерімен қате конфигурацияланған интеграция туралы хабарлауға мүмкіндік беретін клондалған машиналарды қате сәйкестендіру туралы хабарлау үшін хабарлама жүйесінде алдын ала анықталған үлгілердің болуы.  - VDI жүйелерінде көшіру немесе клондау үшін қай виртуалды машинаның көзі болатынын анықтау мүмкіндігі.  - Жеке филиалдарға лицензияның белгілі бір бөлігін тағайындауға мүмкіндік беретін компанияның филиалдарына сәйкес сайттарды құру функционалдық мүмкіндіктерінің болуы.  - Клиенттік машиналардағы барлық дискілерді қашықтан толық дискімен шифрлау/шифрын шешу мүмкіндігі.  - Клиенттік машиналарда тек жүктеу дискісін қашықтан толық дискілік шифрлау/шифрды шешу мүмкіндігі.  - Басқару серверінің консолінде әкімшіге қашықтағы жұмыс станциясы үшін қажетті параметрлері бар сәйкес саясатты өте ыңғайлы және жылдам таңдауға және дискіні шифрлау процесін бастауға мүмкіндік беретін басқару серверінің консолінде шифрлауды қосу шеберінің болуы.  - Әрбір жұмыс станциясының пайдаланушылары үшін жүктеуге дейінгі жеке кіру құпия сөзін жасау мүмкіндігі.  - Әкімшінің жүктеу алдындағы құпия сөзге әртүрлі критерийлерді орнату мүмкіндігі, мысалы: құпия сөздің күрделілігі, енгізу әрекеттерінің саны, жарамдылық мерзімі.  - Әкімшінің жүктеу алдындағы құпия сөзді қашықтан құлыптау мүмкіндігі, бұл кейінгі қайта жүктеуден кейін алдын ала жүктеу логинін өшіруге әкеледі және құлыпты ашу үшін қалпына келтіру құпия сөзін пайдаланып жаңа алдын ала жүктеу құпия сөзін орнатуды талап етеді.  - Әкімшінің жүктеу алдындағы құпия сөзді қашықтан өшіру мүмкіндігі, бұл қашықтағы жұмыс станциясын дереу құлыптауға әкеледі және пайдаланушыға экранда көк экранның маңызды қате туралы хабары көрсетіледі. Осыдан кейін дискілердегі ақпаратқа жүктелетін қалпына келтіру дискісін пайдаланып шифрды шешкеннен кейін ғана қол жеткізуге болады.  **Жұмыс станцияларын қорғау**  - Зиянды бағдарламадан қорғауды қамтамасыз ету – компьютердегі файлдар кодының басына немесе соңына қосылатын арнайы зиянды код. Зиянды бағдарламалық жасақтаманы анықтау машиналық оқыту құрамдас бөлігімен біріктірілген анықтау қозғалтқышы арқылы орындалуы керек.  - Вирустар немесе троян аттары сияқты анық зиянды бағдарламалар сияқты зиянды бағдарлама ретінде анық жіктелмейтін ықтимал қалаусыз бағдарламалардан қорғауды қамтамасыз ету, бірақ бұл бағдарламалар қосымша қажетсіз бағдарламалық құралды орнатуы, жүйе параметрлерін өзгертуі және күтпеген әрекеттерді немесе әрекеттерді орындауы мүмкін. пайдаланушы растамаған.  - Интернеттен шабуылдаушыларға жүйеге шектеусіз қол жеткізуді қамтамасыз ететін қауіпті руткит бағдарламаларынан қорғауды қамтамасыз ету, сонымен бірге олардың операциялық жүйеде болуын жасыру.  - Зиянды емес, бірақ сканерлеу ауытқуларға әкелуі немесе жүйе өнімділігіне әсер етуі мүмкін кейбір файлдарды сканерлеуден ерекше жағдай жасау мүмкіндігі.  - Нақты уақытта антивирустық қорғауды қамтамасыз ету.  - Пайдаланушының немесе әкімшінің сұранысы бойынша және кестеге сәйкес антивирустық сканерлеу.  - Зиянды мінез-құлық пен зиянды бағдарламалық құралдың сипаттамаларын анықтау үшін кодты тереңірек талдау үшін машиналық оқыту технологияларын пайдалану мүмкіндігі.  - Рұқсат етілген немесе тыйым салынған сыртқы құрылғылардың топтарын құру мүмкіндігі.  - Conficker, Sirefef, Necurs және басқалар сияқты күрделі тұрақты қауіптердің қалдықтарын тазарту үшін бірнеше утилиталарды біріктіретін кіріктірілген құралдың болуы  - Браузердің жад аймағына және оның терезелерінің мазмұнына кедергі жасау әрекеттерін блоктау үшін браузерлерді қорғалған режимде іске қосуға мүмкіндік беретін қосымша модульдің болуы, сондай-ақ Интернет төлемдері және Интернет төлемдері сияқты маңызды Интернет қосылымдарын қосымша қорғау. Интернет-банкинг және т.б.  - қашықтағы компьютерде іске қосылған процестер мен қызметтерді тоқтатуға, тізілім тармақтарын жоюға және желілік қосылымдарды блоктауға мүмкіндік беретін сценарийлерді жасау және қашықтан орындау мүмкіндігі.  - Барлығы үшін де, жеке пайдаланушылар немесе Windows топтары немесе домен үшін де сыртқы құрылғыларды қосуға тыйым салу немесе рұқсат беру мүмкіндігі.  - Барлық қол жетімді желілік қосылымдар туралы барлық егжей-тегжейлі ақпаратты көруге, сондай-ақ пайдаланушыны қорғалмаған Wi-Fi желісіне қосылу туралы ескертуге мүмкіндік беретін жеке желілік экранның қосымша функционалдығының болуы.  - ДК-де блокталған IP мекенжайларының тізімін көруге мүмкіндік беретін жеке желіаралық қалқанның қосымша функционалдығының болуы, қара тізімге ену себептері туралы ақпарат береді және нақты қауіпсіз мекенжайлар үшін ерекшеліктер жасауға мүмкіндік береді.  - Әкімшіге желілік қосымшалар мен жабдықтарға рұқсат беретін ережелерді қашықтан конфигурациялауға мүмкіндік беретін жеке желіаралық қалқанда оқыту режимінің болуы.  - белгісіз қауіпті желілерге рұқсатсыз компьютер қосылымдарын болдырмау үшін жеке желіаралық қалқанда қосымша желі аутентификациясын пайдалану мүмкіндігі.  - Жаңа рұқсат етілмеген желі қосылымдарына әкеліп соқтырған желілік бағдарламалардағы өзгерістерді анықтауға қабілетті жеке желілік экранның қосымша мүмкіндіктерінің болуы.  - Интернетке кіру мүмкіндігі жоқ жабық, оқшауланған желілерде антивирустық қорғауды жаңартуға мүмкіндік беретін сервердегі жергілікті жадтан клиенттік жаңартуларды алу.  - Тұрақты, сынақ және кейінге қалдырылған жаңартуларды алу режимінде жаңарту мүмкіндігі.  - Жүйе әкімшісіне антивирустық бағдарламалық құралды икемді түрде конфигурациялау үшін саясатпен тағайындалған және өңдеуге болмайтын антивирустық бағдарламалық құрал параметрлерін дербес компьютерде өзгертуге уақытша мүмкіндік беретін саясатты қайта анықтау режимінің болуы. нақты орта.  - Ағымдағы антивирус өнімдерінің ДК ресурстарының төмен тұтынуы (барлық процестермен бірге: графикалық интерфейс, кешенді қорғау процесі, қашықтан басқару қызметі): 50-100 МБ жедел жады, орталық процессордың 2-35%.  - Компьютерді белсенді емес күйде сканерлеңіз.  - Жүйеге жүктемені азайтатын және ең жылдам және тиімді сканерлеуді жасауға мүмкіндік беретін сканерлеу үшін 64 биттік ядроны пайдалану.  - ЖЖҚ сканерлеу модулі, ол күдікті іске қосылған процестердің жұмысын бақылауға қабілетті, ол тіпті мұқият шифрланған және жасырын қауіптермен инфекцияны болдырмауға мүмкіндік береді.  - Операциялық жүйедегі рұқсат етілмеген және қауіпті өзгерістерді анықтау үшін операциялық жүйенің әртүрлі параметрлерінің мәндерінің сыни деңгейін (қауіпті, белгісіз, аз белгілі, қауіпсіз) анықтау мүмкіндігі.  - ОЖ қолдауы: Microsoft Windows Vista (Кәсіби немесе одан жоғары); Microsoft Windows 7 (кәсіби немесе одан жоғары); Microsoft Windows 8 (кәсіби немесе одан жоғары); Microsoft Windows 8.1 (кәсіби немесе одан жоғары); Microsoft Windows 10 және Microsoft Windows 11.  - Басқарылатын Windows жұмыс станцияларында толық дискіні шифрлауды басқаруды жүктеу алдында жүйеге кіру кезінде қосымша қорғаныс деңгейімен қосыңыз.  - Шифрлау үшін жабдық өндірушілерінің қосымша технологияларын пайдалану мүмкіндігі: сенімді платформа модулі (TPM) немесе өзін-өзі шифрлайтын дискілер (OPAL).  - Графикалық пайдаланушы интерфейсінің әртүрлі режимдері: қалыпты, графикалық интерфейстің барлық функционалдығы қолжетімді болады немесе минималды, тек хабарландырулар көрсетіледі.  - Шифрлауға қатысты барлық хабарларды жасыру мүмкіндігі бар толық экран режимінде жұмыс істейтін бағдарламаларды қолдау.  - Ағымдағы құпия сөзді пайдаланып пайдаланушының жүктеу алдындағы құпия сөзін өзгерту мүмкіндігі  - Пайдаланушы өзінің құпия сөзін ұмытып қалған жағдайда әкімшінің қалпына келтіру құпия сөзін жасау мүмкіндігі.  - Шифрланған дискідегі деректерге стандартты құралдарды қолдану арқылы қол жеткізу мүмкін болмаған жағдайда, әкімшінің дискінің жедел шифрын шешу үшін жүктеу дискісін немесе USB дискісін жасау мүмкіндігі.  - Әкімшінің жүктелу алдындағы құпия сөзді қашықтан қайтарып алу мүмкіндігі, бұл пайдаланушыдан парольді өзгертуге және ОЖ кейіннен қайта жүктелген кезде құпия сөзді өзгертуге мәжбүрлеуге әкеледі.  **Серверді қорғау**  - Сервердің операциялық жүйесінің жұмысына әсерін азайтуға мүмкіндік беретін нақты файлдар, қалталар, қосымшалар үшін автоматты ерекшеліктерді жасау үшін сервер рөлдерін автоматты түрде анықтау.  - Қосымша бағдарламалық өнімдерді орнатуды қажет етпестен жұмыс станциялары мен серверлерді бұлттық құмсалғышпен (қосымша лицензиямен) қорғауды біріктіру мүмкіндігі.  - UEFI интерфейсін сканерлеу - негізгі жүктеу жазбасында зиянды бағдарламаны тексереді.  - сканерлеу кезінде эвристикалық технологияларды қолдану.  - Зиянды бағдарламалардан, трояндық аттардан, клавиатурадан, жарнамалық бағдарламадан, фишингтен, шпиондық бағдарламадан, руткиттерден, сценарийлерден, ықтимал қалаусыз және қауіпті бағдарламалық құралдан қорғауды қамтамасыз етеді.  - Күніне кемінде 24 рет вирустық дерекқорларды жүйелі түрде жаңарту.  - Негізгі серверге қосымша сақтық көшірмелерді басқару серверлерін көрсету мүмкіндігі.  - Құрылғы түрі, қол жеткізу деңгейі, өндіруші, модель немесе құрылғының сериялық нөмірі бойынша қол жеткізу ережелерін құру арқылы перифериялық құрылғыларды жұмыс станциясына қосуды басқара алатын құралдың болуы. Ережелер барлығына немесе жеке Windows пайдаланушылары немесе топтары үшін жасалуы мүмкін.  - Операциялық жүйенің әртүрлі аспектілерін, соның ішінде іске қосылған процестерді, тізілім мазмұнын, орнатылған бағдарламалық қамтамасыз етуді, желілік қосылымдарды одан әрі терең талдау үшін операциялық жүйе күйінің суретін жасай алатын жүйелік диагностикалық құралдың болуы. Жүйенің әртүрлі суреттерін салыстыру мүмкіндігінің арқасында бұл құрал жүйеде болған өзгерістерді анықтай алады. Ол сондай-ақ іске қосылған процестерді тоқтатуға, тізілім тармақтарын жоюға және желілік қосылымдарды блоктауға мүмкіндік беретін сценарийлерді жасай және орындай алады.  - Белгіленген кеңейтімді пайдаланып Интернеттен файлдарды жүктеуді блоктау мүмкіндігі.  - Тұрақты, сынақ және кейінге қалдырылған жаңартуларды алу режимінде жаңарту мүмкіндігі.  - Виртуалды жұмыс станцияларына, сондай-ақ тұтастай алғанда гипервизорға жүктемені айтарлықтай төмендететін арнайы технологияның болуы.  - терминалды пайдаланушылар үшін графикалық интерфейсті өшіру арқылы іске қосу режимін теңшеу мүмкіндігі, бұл терминал сервері режимінде жұмыс істейтін серверге жүктемені азайтады.  **Жетілдірілген анықтау және әрекет ету**  - Корпоративтік желіде орын алған қалыптан тыс оқиғалар туралы өзекті ақпаратты бақылау үшін бақылау панелінің болуы.  - Ережелер негізінде бағдарламалық жасақтаманың жұмысында орын алатын аномальды оқиғалар туралы ескертулерді алу.  - Әдепкі ережелер тізімі және бағдарламалық жасақтама әрекетін аномальды деп сипаттайтын өз ережелеріңізді жасау мүмкіндігі.  - Қауіптілік деңгейі бойынша ескертулерді автоматты түрде жіктеу маңызды оқиғаларды жылдам анықтауға және оларға жауап беруге мүмкіндік береді.  - Оқиғаларды икемді сұрыптау және фильтрлеу үшін ескертулер үшін басымдықты орнату мүмкіндігі.  - Түр, компьютер, ереже, процесс, файл сияқты әртүрлі критерийлер бойынша ескертулерді топтау мүмкіндігі.  - Оқиға туралы жиынтық ақпаратты (ол қашан және қайда болғаны (компьютер), қай пайдаланушыдан, қандай орындалатын файл іске қосылды, тіпті қандай нақты процесс іске қосылды) қамтитын дабылдарды анықтауды жасау арқылы ақпараттық қауіпсіздік инциденттерін жазу мүмкіндігі. тізімделген параметрлердің әрқайсысы үшін толық ақпарат.  - Әрбір дабылды анықтауда ережені тудырған оқиғаның егжей-тегжейлі сипаттамасын, ықтимал себептердің тізбесін, ықтимал тәуекелдер мен салдарларды және оқиғаны одан әрі талдау үшін қажетті әрекеттерге қатысты ұсыныстарды беретін арнайы ақпараттық бөлімнің болуы. .  - Интерактивті дабылды анықтау интерфейсінің болуы жиынтық дабылды анықтауда қолжетімді негізгі параметрлер үшін ақпараттық қауіпсіздік оқиғасын егжей-тегжейлі шолуға мүмкіндік береді.  - Процесс ағашы, файлдық жүйе және ОЖ тізілімінің өзгерістері, желілік белсенділік, URL мекенжайларына қосылу, қосымша жүктелген орындалатын файлдар және ОЖ-дағы ең егжей-тегжейлі оқиғалар журналы сияқты триггерді іске қосқан процесс туралы толық ақпаратты ұсыну.  - EXE/DLL файлдарының ауырлық деңгейі бойынша автоматты түрде жіктелуі қалыпты емес файл әрекетін жылдам анықтауға және жауап беруге мүмкіндік береді.  - Сценарийлердің сыни деңгейі бойынша автоматты түрде жіктелуі аномальды мінез-құлықты тез анықтауға және оған жауап беруге мүмкіндік береді.  - Орындалатын файлдардың бақылау сомасы, олардың орналасқан жері, электрондық цифрлық қолтаңба және басқа ақпарат туралы ақпаратты қамтуы тиіс жеке оқиғалар үшін егжей-тегжейлі ерекшеліктерді жасау мүмкіндігі.  - EXE/DLL файлдарын сенімді немесе қауіпсіз деп белгілеу мүмкіндігі.  - EXE/DLL файлдарын тексерілген немесе талданған деп белгілеу мүмкіндігі.  - Тексерілген сценарийлерді сенімді немесе қауіпсіз деп белгілеу мүмкіндігі.  - Әрі қарай талдау мақсатында жұмыс станциялары мен серверлердегі барлық EXE/DLL файлдарының тізімін жасау.  - Толығырақ талдау үшін оларды қалпына келтіру, жою және жүктеп алу мүмкіндігі бар блокталған EXE/DLL файлдарының тізімі.  - Әрі қарай талдау үшін соңғы нүктелерден күдікті файлдарды жүктеп алу мүмкіндігі.  - Одан әрі талдау үшін соңғы нүктелерден күдікті сценарий файлдарын (скрипттерді) жүктеп алу мүмкіндігі.  - Жұмыс станциялары мен серверлерде орындалатын барлық сценарийлердің, сценарийлердің тізімін құру.  - Сценарийлерді негізгі процесс, бірінші еншілес процесс, пәрмен жолы сияқты әртүрлі критерийлер бойынша топтау мүмкіндігі.  - Оқиғалар, EXE/DLL файлдары, сценарийлер туралы толық ақпараты бар компьютерлер тізімін жасау.  - Жұмыс станциясын қашықтан қайта жүктеу немесе оны толық өшіру мүмкіндігі.  - қашықтағы жұмыс станциясында операциялық жүйенің суретін лезде жасау мүмкіндігі, ол қазіргі уақытта барлық іске қосылған процестер, желілік қосылымдар туралы ақпаратты жазады, сонымен қатар ОЖ тізілімінің маңызды мазмұны, ОЖ жоспарлаушысындағы тапсырма туралы ақпаратты береді, ОЖ пайдаланушылары және олардың артықшылықтары, «хосттар», «win.ini» және басқалар сияқты маңызды ОЖ файлдарының мазмұны және ОЖ және орнатылған бағдарламалық қамтамасыз ету туралы барлық толық ақпарат.  - Орталықтандырылған басқару серверіне рұқсатсыз қосылулардың алдын алуға көмектесетін әкімші есепке алулары үшін екі факторлы аутентификацияны пайдалану мүмкіндігі.  - Барлық кең ауқымды антивирустық қорғау жүйелерін орталықтандырылған бақылау және басқару үшін конфигурацияланған бар әкімшілік серверлермен басқарылатын жағдайда, EDR шешімін пайдалану мүмкіндігі.   * + 1. **Таргеттелген шабуылдардан қорғау жүйесі:**   Мақсатты шабуылдардан қорғау жүйесі келесі функцияларды қамтамасыз етуі керек:   * Активтерді агенттік бақылау 1-кестеде көрсетілген саннан кем емес; * АТ-инфрақұрылымына кіріктірудің келесі әдістерін қолдайды:   + POP3 хаттамасы арқылы почта серверінен алынған электрондық почта хабарларының көшірмелерін өңдеу үшін почта серверімен интеграция (егер почта серверінде техникалық мүмкін болса);   + Іске қосылған процестер, ашық желі қосылымдары және өзгертілген файлдар, соның ішінде үйлесімді антивирустық бағдарламалық құрал агентін пайдалану туралы деректерді қабылдау және өңдеу үшін жұмыс станцияларымен және серверлермен интеграция. * Жиналған ақпарат негізінде ауытқулар мен қауіптерді анықтау; * Сыни инциденттер болған жағдайда, әрекеттер туралы толығырақ ақпаратты таба алатын MITER ATT&CK ресурсының тиісті бөлімдеріне сілтемелермен ұқсас жағдайда шабуылдаушылар бұрын пайдаланған белгілі әдістер мен құралдардың тізімі туралы ақпаратты беру мүмкіндігі. * Вирусқа қарсы дерекқорды пайдалана отырып, деректерді вирустарға және басқа қауіпті бағдарламаларға тексеру; * Құм жәшігіндегі күдікті орындалатын файлдар мен сценарийлерді талдау; * Статистикалық талдау және компьютерлік желінің белсенділігін желідегі типтік емес мінез-құлық белгілеріне тексеру; * Файлдар мен URL сілтемелерінің беделін талдау; * Қолданушы әрекеттерінің мінез-құлық талдауы; * Фишинг пен зиянды сілтемелерді анықтау; * Тарихи оқиға деректерін сақтау; * Өз қолтаңбаңызды жасау мүмкіндігі; * Анықталған қауіптердің тәуекел деңгейі бойынша басымдылығы; * Статистикалық деректер мен есептілікке қол жеткізу үшін графикалық басқару жүйесінің болуы.   + 1. **Деректердің жайылып кетуін анықтау және алдын алу жүйесі**   **Жалпы талаптар**  Жалпы талаптар  Сатып алынған бағдарламалық қамтамасыз ету қызметі (бұдан әрі – бағдарламалық қамтамасыз ету) пайдаланушының әрекеті туралы ақпаратты жинауға, сақтауға, талдауға және көруге арналған.  Бағдарламалық жасақтама келесі талаптарға сай болуы керек:  Серверге қауіпсіз қосылым арқылы қосылыңыз;  Клиенттен серверге қосылуды қамтамасыз ететін кез келген желілік инфрақұрылымда қолдау жұмысы: VPN, NAT және басқа қосылу арналары арқылы;  Агент бағдарламасы Windows, Linux және macOS тобының операциялық жүйелері бар жұмыс станцияларында немесе терминалдық серверлерде жұмыс істеуі, пайдаланушының өз компьютеріндегі әрекеттері мен оқиғаларын бақылауы, оларды серверге тасымалдауы керек;  Жергілікті желіге кіру мүмкіндігіне қарамастан (қашықтағы компьютерде) агент серверге одан әрі жіберу үшін пайдаланушы әрекеттері туралы ақпараттың жинақталуын қамтамасыз етеді;  Бағдарламалық құрал жүйелердің корпоративтік сыныбына (Enterprise DLP, соның ішінде Gartner Magic Quadrant есебінде) тиесілі болуы және соңғы нүктелерде орнатылған агентті (EndPoint DLP) пайдаланып, соңғы нүктелерді құпия деректердің ағып кетуінен қорғау функциясына және функционалдығына ие болуы керек. желілік арналар арқылы ағып кетуді бақылау құпия деректерінің (Network DLP).  Бағдарламалық қамтамасыз ету жұмыс станцияларында және файлдық серверлерде орналасқан құпия ақпаратты іздеу мүмкіндігін қамтамасыз етуі керек (табылған файлдарды карантинге жылжыту және мұндай жылжыту себептері туралы ақпаратты / мәтіндік файлдарды / орнында қалдыру мүмкіндігімен).  Бағдарламалық қамтамасыз ету құпия ақпараттың ықтимал ағып кетуі үшін келесі арналарды бақылауы керек:  - шығыс SMTP қосылымдары;  - шығыс HTTP қосылымдары;  - шығыс HTTPS қосылымы;  - шығыс IM қосылымдары;  - ақпаратты сыртқы сақтау құралдарына және ақпараттық ресурстарға көшіру;  - жергілікті/желілік принтерде ақпаратты басып шығару.  Бағдарламалық қамтамасыз ету келесі функцияларды қамтамасыз етуі керек:  - корпоративтік электрондық пошта жүйесі арқылы құпия ақпараттың ашылуына жол бермеу;  - құпия ақпаратты қамтитын шығыс хаттарды блоктау мүмкіндігі;  - Интернетке корпоративтік қол жеткізу жүйесі арқылы құпия ақпараттың ашылуына жол бермеу;  - HTTP/HTTPS трафигінен құпия ақпаратты шығару мүмкіндігі;  - HTTP/HTTPS трафигін блоктау мүмкіндігі;  - құпия ақпаратты ашуды болдырмау және ағып кету арналарын бақылау, атап айтқанда: құпия ақпаратты желілік қалтадан жергілікті қатты дискілерге көшіру, құпия ақпаратты алынбалы тасымалдағышқа көшіру, құпия ақпаратты жергілікті және желілік басып шығаруға, сондай-ақ факс арқылы жіберу, ақпаратты қорғау. көшіру/қою операциялары кезінде алмасу буферінің мазмұны;  - табылған файлдарды жылжыту мүмкіндігімен құпия ақпаратқа желінің соңғы түйінінің жергілікті қатты дискілерін сканерлеу мүмкіндігі (соның ішінде белгіленген кесте бойынша);  - графикалық объектілерде (pdf файлдар, суреттер және т.б.) қамтылған мәтіндік ақпаратты, сондай-ақ мұндай объектілердегі графикалық бейнелерді (жауапты тұлғалардың қолдары, мөртабандар, логотиптер және т.б.) тану мүмкіндігі;  - құпия деректерді сканерлеу және одан «сандық саусақ іздерін» алу мүмкіндігі;  - корпоративтік желіден соңғы түйін ажыратылған немесе желіге қосылу жоғалған жағдайда, клиенттердің және бағдарламалық модульдердің (анықтау серверлерінің) автономды жұмыс істеу мүмкіндігі;  - қауіпсіздік саясатын орталықтандырылған басқару мүмкіндігі;  - бағдарламалық қамтамасыз етудің қауіпсіздік саясатына нақты уақытта жылдам өзгерістер енгізу, қолданыстағы ережелер мен параметрлерді өзгерту және жаңаларын қосу мүмкіндігі;  - бағдарламалық қамтамасыз ету саясатының бұзылуы туралы автоматты хабарламаларды орнату;  - қауіпсіздік саясатының бұзылуына әрекет етудің әртүрлі нұсқаларын орнату;  - қауіпсіздік саясатын бұзудың даталары мен фактілері туралы есептерді құру және қалыптастыру;  - басқару консолімен орыс немесе ағылшын тілінде жұмыс істеу мүмкіндігі;  - басқару консолінде аутентификация үшін бар Active Directory тіркелгілерін пайдалану мүмкіндігі;  - AD тіркелгісінің атрибуттарын (аты, телефоны, бөлімі, лауазымы және т.б.) тікелей бағдарламалық құрал консолінен көру мүмкіндігі.  Техникалық талаптар  Операцияларды басқару мүмкіндігі:  - алынбалы тасымалдағышқа (USB, CompactFlash, SD) құпия ақпаратты (бұдан әрі - CI) жазу;  - қосымша модульдерді орналастыруды (орнатуды) қажет етпейтін кірістірілген «Құрылғыны басқару» функционалдығы;  - CI басып шығару (желілік және жергілікті принтерлер);  - CI алмасу буферіне көшіру;  - жергілікті дискілерге CI жазу;  - қолданбаның CI-ге қол жеткізуін бақылау (оның ішінде CI бар файлдарды Skype және Teams арқылы тасымалдау);  - HTTP протоколы арқылы CI деректерін жіберу;  - HTTPS протоколы арқылы CI деректерін жіберу;  - электрондық пошта клиенті деңгейінде SMTP басқару;  - CI файлдарын желілік ресурстарға, соның ішінде Office 365 ресурстары мен қызметтеріне көшіру;  - соңғы нүкте деңгейінде орталықтандырылған блоктау мүмкіндігімен PrintScreen функциясын басқару;  - саясаттар мен конфигурацияларды агентке олардың орналасқан жеріндегі соңғы нүктелерде - корпоративтік желіде немесе корпоративтік желіден тыс конфигурациялау және қолдану мүмкіндігі;  - құжаттарды сыртқы тасымалдағышқа жаппай көшіруді бақылау мүмкіндігі жүйе белгілі бір уақыт ішінде пайдаланушы сыртқы тасымалдағышқа көшіре алатын файлдардың санын бақылауы керек;  - сыртқы тасымалдағышқа көшіру кезінде құжаттарды шифрлау мүмкіндігі, пайдаланушының немесе бағдарламалық қамтамасыз ету әкімшісінің құпия сөзді орнату мүмкіндігі;  - MTP хаттамасын бұғаттау мүмкіндігі, басқару көрсетілген саясаттарға сәйкес CI анықтау және CI блоктау (берілуге ​​кедергі жасау) мүмкіндігін білдіреді.  Windows және Linux ОЖ-де жүйенің барлық анықтау модульдерін орналастыру (орнату) мүмкіндігі.  Оқиғаларға жауап беру мүмкіндігі: жауапты тұлғаны немесе ақпарат иесін автоматты түрде хабардар ету, электрондық пошта арқылы жіберуді блоктау, веб-формалар арқылы деректерді жіберуді блоктау, сценарийді орындау, құпия ақпаратты жою.  Оқиғаны күшейту және қосымша әрекеттерді іске қосу мүмкіндігі (мысалы, CI шифрлау, CI қозғалысы және т.б.).  OCR (Таңбаларды оптикалық тану) сканерлеуі қосымша үшінші тарап бағдарламалық құралын пайдаланбай, кірістірілген технология/механизм арқылы қамтамасыз етілуі керек.  Мәтінді тану ағылшын, орыс және қазақ тілдерін қолдау арқылы латын және кириллица әліпбиін қолдауы керек.  Сканерленген кескіндерді тану және түрлендіру келесі құжат пішімдерін қолдауы керек: PDF, BMP, JPEG, PNG, TIFF.  OCR сканерлеу келесі сканерлеу түрлерін қолдауы керек:  - жергілікті сканерлеу;  - сыртқы тасымалдағыштарға CI сканерлеу және көшіру;  - CI файлын серверге сканерлеу және көшіру;  - HTTP / HTTPS арқылы CI жіберулерді сканерлеу;  - Webmail протоколы арқылы CI жіберулерді сканерлеу;  - SMTP хаттамасы арқылы жіберулерді сканерлеу.  Пайдаланушының USB-ге қол жеткізу деңгейін реттеу мүмкіндігі.  Соңғы нүкте модулін Ubuntu және Centos жүйелерінде қолдану мүмкіндігі:  - тыныштықтағы CI анықтау;  - алынбалы тасымалдағыштағы ақпараттың ағып кетуін бақылау, оның ішінде мұндай ақпаратты блоктау және тіркеу;  - HTTP / HTTPS арналары арқылы CI ағуын бақылау;  - Webmail протоколы арқылы CI ағуын бақылау.  Бағдарламалық құрал пайдаланушы компьютерге сенімсіз USB дискісін салған кезде әкімшіге алдын ала хабарлау мүмкіндігін қолдауы керек.  Бағдарламалық құрал агенті жасырын режимде жұмыс істеуге қолдау көрсетуі керек, барлық процестер соңғы пайдаланушыдан жасырылуы керек.  Интерфейс талаптары  Бағдарлама келесі интерфейс тілдерін қолдауы керек: ағылшын, орыс.  Бағдарлама жүйені басқару және инциденттермен жұмыс істеу үшін бірыңғай веб-интерфейсті қолдауы керек.  Шешім интерфейсін пайдаланып соңғы нүкте агенттерін жою мүмкіндігі болуы керек.  Шешім интерфейсін пайдаланып соңғы нүкте агенттерін жаңарту мүмкіндігі болуы керек.  Классификацияға қойылатын талаптар  Бағдарламалық құрал Microsoft Office файлдарының классификациясын қолдауы керек.  Жіктеу файл жабылған кезде емес, сақталған кезде жасалуы керек.  Нақты уақыттағы деректерді алу кезінде бағдарламалық жасақтама мәтіндік құжаттар мен суреттердің тыныштықтағы классификациясын қолдауы керек.  Бағдарлама деректерді жіктеу кезінде құжатқа су таңбасын қою мүмкіндігін қолдауы керек.  Бағдарламалық қамтамасыз ету желілік жадты тексеру мүмкіндігін қолдауы керек, файлдардың ашылуы, өзгертілуі, жойылуы және атын өзгерту бақылануы керек.  Бағдарламалық құрал басып шығару операциялары кезінде құжаттарды жіктей алуы керек.  Бағдарламалық жасақтама позицияны таңдау мүмкіндігімен, көріну мүмкіндігімен және су таңбасын бүкіл экранға қою мүмкіндігімен пайдаланушы экранында су таңбасын орналастыру мүмкіндігі болуы керек.  Бағдарлама нақты уақытта файлдар мен қалталарды жіктеуі керек.  Бағдарламалық қамтамасыз ету алмасу буферінде файлдарды көшіруді басқаруы және файлдың жіктелу деңгейіне байланысты мұндай операцияны блоктай алуы керек.  Қосымша талаптар  Бағдарламалық құрал мамандандырылған стандартты хаттамаларды (MTA) пайдалана отырып, үшінші тарап электрондық пошта қызметтерімен интеграцияны қолдауы керек.  Бағдарламалық құрал мамандандырылған стандартты хаттамаларды (ICAP) пайдалана отырып, үшінші тарап веб-қызметтерімен (шлюздар) интеграцияны қолдауы керек.  Бағдарламалық құрал орталықтандырылған бағдарламалық құрал консолінде осындай ортадағы CI-ға қатысты оқиғаларды көру мүмкіндігімен Office 365 бұлттық ортасымен интеграцияны қолдауы керек. Оның ішінде OneDrive және Бизнеске арналған OneDrive ішіндегі файлдармен жұмыс істеу мүмкіндігі.  Қатысушы техникалық қолдау (ТС) шеңберінде жүйені және оның құрамдас бөліктерін пайдалану және әкімшілендіру бойынша консультациялық қолдау көрсете отырып, Тұтынушыда жүйені енгізу мен конфигурациялауды толық көлемде қамтамасыз ете алуы керек.  TP жүйесіне қойылатын талаптар:  - ТП 24x7 қамтамасыз етілуі керек;  - ТА ағылшын және орыс тілдерінде берілуі керек;  - Тапсырыс берушінің кем дегенде үш маманына жүйені және оның құрамдас бөліктерін пайдалану және басқару бойынша консультациялық қолдау көрсете отырып, жүйені Тұтынушыда толық көлемде енгізу және конфигурациялау;  - құпия ақпараттың ағып кетуін болдырмау үшін орнату және конфигурациялау (жүйелер) бойынша Тапсырыс берушінің персоналымен (кемінде 3 адам) техникалық консультациялар жүргізу.  Агентті пайдаланып трафикті ұстап алу пайдаланушы браузерінде плагинді орнатпай жүзеге асырылуы керек.  Жүйе әрбір функция үшін файлды сканерлеудің максималды уақытын бөлек орнату мүмкіндігіне ие болуы керек.  Active Directory-ге қосылмай-ақ өзіңіздің пайдаланушы топтарыңызды құру мүмкіндігі болуы керек.  Бағдарламалық қамтамасыз ету белгілі бір сайттар/ресурстар үшін пакеттік тексерусіз толық тексеруді айналып өтуді жүзеге асыра алуы керек.  Корпоративтік ресурстарды теріс пайдалану жағдайларын анықтау, бұзушыларды іздестіру және дәлелдемелік базаны қалыптастыру үшін жалпы көлемі кемінде соңғы 6 айдағы ақпарат қозғалысының бағыттарын қадағалау үшін ұсталған барлық ақпараттың мұрағатын сақтау.  SIEM жүйесімен интеграция.  Техникалық қолдау 12 ай мерзімге, Шарт бойынша қызметтерді көрсету кезеңінде көрсетілуі тиіс.   * + 1. **Желілік трафикті және байланыс арналарын талдау жүйелері Жалпы талаптар**   Функционалдық талаптар:  • Тұтынушы инфрақұрылымының желілік құрылғыларынан коллекторлық серверге жіберілетін трафик ағындарын талдауды қолдау. Қолдау көрсетілетін протокол түрлері төменде Функционалдық талаптар бөлімінде берілген.  • Тұтынушы инфрақұрылымының желілік жабдығында қолдау көрсетілетін ағын хаттамаларын жасау және жіберу мүмкіндігі болмаса, SPAN трафикті қабылдау және оны қолдау көрсетілетін ағын хаттамасына инкапсуляциялау арқылы арнайы құрылғы - зонд арқылы ағын трафигін генерациялау мүмкін болады. жүйесі бойынша. Коллекторға біріктірілген бір зонд жеткізу бөлігі ретінде қосылуы керек.  • Бірнеше интерфейстерде трафик талдауын қолдайды  • «шикі» SPAN трафигін бақылауға қолдау көрсету  • NetFlow v5 бақылау протоколын қолдау  • NetFlow v9 бақылау протоколын қолдау  • jFlow бақылау протоколын қолдау  • IPFIX бақылау протоколын қолдау  • sFlow v2/4/5 RFC 3176 бақылау протоколын қолдау  • NetStream бақылау протоколын қолдау  • cFlowd бақылау протоколын қолдау  • NetFlow Lite бақылау протоколын қолдау  • Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2 стандарттарын қолдайды  • IPFIX протоколы арқылы OneAccess, IXIA, VMware, Gigamon, Cisco жүйелерінің меншік өрістерін бақылауға қолдау көрсету  • IPFIX айнымалы ұзындық жазбаларын қолдау  • VMware NSX, Gigamon және Ixia IPFIX кеңейтімдерін қоса, үшінші тараптың IPFIX модификацияларына қолдау көрсету  • Әрбір желі қосылымы (желі ағыны) үшін егжей-тегжейлі статистиканы алу үшін егжей-тегжейлі тәсілді (деректерді тереңдету) қолдауымен желілік өзара әрекеттесуді талдау және бақылау мүмкіндігі;  • NTP протоколы арқылы жүйелік уақытты синхрондауды қолдау;  • DNS кэшті қолдау;  • Cisco AVC стандартты қолдауы, соның ішінде желі өнімділігі көрсеткіштері (AVC ART) және HTTP мәндері (хост аты және URL мекенжайы);  • Желінің өнімділігін бақылауды қолдау. RTT, SRT, кідіріс, діріл, ретрансляция, ретсіз пакеттерді жинау және талдау;  • ISO OSI деңгейінің 7 хаттамаларының мониторингін қолдау (HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP, SMTP, POP3, IMAP және MS SQL (TDS));  • Жетілдірілген L3/L4 ISO OSI мониторингін қолдау (TTL (Time To Live), TCP Window Size, NAT анықтау үшін TCP SYN пакет өлшемі);  • Бір көздің әртүрлі интерфейстерінен іріктеу ағындарының әртүрлі деңгейлерін қолдау;  • Сценарий тілін қолдау. Сценарий тілі жалпы Python пәрмендерін қолдайды;  • Қабылданған бақылау трафигін басқа коллекторларға өңдеуге жіберу мүмкіндігін қолдау, соның ішінде трафикті таңдау мүмкіндігі;  • Трафик жіберу кезінде Flow форматтарын түрлендіру мүмкіндігі (NetFlow v5/v9, IPFIX);  • IPv4 және IPv6 деректер трафигін, VLAN, MPLS өңдеу және оны коллекторға беру мүмкіндігі;  • GRE, VxLAN, ESP, 4in6, DS-Lite және OTV туннельдеріндегі трафикті бақылау мүмкіндігі (декапсуляция);  • Қайталанатын бумаларды анықтау және жою мүмкіндігі  • Желідегі құрылғыларды профильдеу мүмкіндігі: ОЖ сәйкестендіру, оның нұсқасын қоса. Браузердің идентификациясы, оның ішінде оның нұсқасы;  • Жіптің жарамдылық мерзімін орнату мүмкіндігі: белсенді және белсенді емес ағынның жарамдылық мерзімінің күту уақыты параметрлері (RFC 3954);  • RFC 7011 стандартына сәйкес TCP/TLS қосылымдарын пайдалана отырып, IPFIX трафикті сенімді және қауіпсіз тасымалдау мүмкіндігін қолдау;  • Шифрланған (SSL/TLS) трафикті бақылауды қолдау: протокол нұсқасын, шифрлау алгоритмін, шифрлар жиынтығын, сертификат деректерін анықтау;  • Деректер көзінің атын, интерфейс атауын және оның параметрлерін қоса алғанда, Flow статистикасының көзін автоматты түрде анықтау;  • Сақтық көшірме жасау, әрі қарай қалпына келтіру мүмкіндігімен, Деректерді сыртқы ақпарат қоймасына жіберу;  • Active Directory сияқты сыртқы деректер қоймаларынан алынған хосттың IP мекенжайын және пайдаланушы идентификаторын қоса, жергілікті желідегі пайдаланушылар туралы деректерді жинау және көрсету;  • Тұрақты өрнектерге (ЖӘНЕ, НЕМЕСЕ, ЕМЕС) негізделген сұрауларды қолдаумен ISO OSI үлгісінің 7-деңгейіндегі өрістердегі ақпарат негізінде көрсетілетін деректерді сүзгілеу мүмкіндігі;  • Көрсетілген опциялар мен атрибуттар үшін TOP-X статистикасын көрсету: байттардың, пакеттердің, тасымалданатын ағындардың, максималды RTT және орташа SRT санын қоса;  • Электрондық пошта, SNMP тұзақтары және Syslog арқылы пайдаланушының жедел хабарландыруларын қолдау;  • Пайдаланушы тапсырмалары үшін жеке анықталған трафик профильдерін қолдау;  • Жергілікті желідегі белсенді құрылғыларды анықтау және бақылау, сонымен қатар MAC мекенжайлары, VLAN, ОЖ және пайдаланушы идентификация деректері туралы ақпаратты қоса алғанда, тарихты сақтау;  • Ел бойынша трафикті сүзу мүмкіндігімен IP мекенжайлары негізінде автоматты геолокацияны қолдау;  • Ашық API интеграциялық интерфейсі;  • SNMP арқылы Flow ақпарат көздерінің қолжетімділігін бақылау.  • Үшінші тараптың периметрді қорғау шешімдерімен, атап айтқанда FortiNet, Checkpoint-пен интеграцияны қолдау;  • Лицензияланған деректерді сақтау көлемі 3 (үш) ТБ. Деректерді жинау және сақтау жүйесі (коллектор) өңдейтін деректер көлемі секундына 75 мың ағынды құрайды;  • Ішкі дискілік квоталарды басқару механизмдерін қолдау;  • Жүйені біртіндеп тік масштабтау мүмкіндігі;  • Дерекқорда жинақталған деректердің сынамаларын алу (қию) жоқ.  • Жүйені қайта орнату қажеттілігінсіз тік жүйені жаңғырту мүмкіндігі;  • Орталық/агрегациялық бақылау контроллерін пайдалануды қолдау (үлестірілген архитектурасы бар схемалар үшін);  • Орталық/агрегациялық контроллердің бақылауындағы бірнеше бөлінген бақылау контроллерінің бірлескен жұмысын қолдау;  • Пайдаланушының жүйеге веб-интерфейс арқылы және кез келген клиенттік бағдарламалық құралды орнатусыз кіруіне қолдау көрсету. Сіз операциялық жүйеге және стандартты кітапханаларға кіретін кез келген бағдарламалық құралды пайдалана аласыз.  • Әрбір пайдаланушы үшін бөлімдерді жекелендіру мүмкіндігі бар HTTP/HTTP негізіндегі бірыңғай жалпы графикалық веб-басқару интерфейсінің болуы.  • Пайдаланушы құқықтары мен артықшылықтарын бөлу механизмін қолдауы бар көп деңгейлі рөлдік үлгіні қолдау  • HTTP/HTTP басқаруына қолдау көрсету  • SSHv2/Secure Copy қолдауы  • SNMP v1/v2c/v3 протоколын қолдау;  • TACACS+ аутентификация протоколын қолдау;  • LDAP (Active Directory) аутентификациясын қолдау;  • Құрылғының сақтық көшірме конфигурациясын құрылғыда сақтауға, сондай-ақ құрылғыны алдыңғы конфигурацияға қайтаруға қолдау көрсету;  • Сұраныс бойынша сақталған конфигурациялардың шектеусіз саны, оларды кез келген уақытта қайтаруға болады;  • Қашықтан қол жеткізу мүмкіндігін сүзу және шектеуді қолдау;  • Басқару интерфейсін теңшеуге қолдау көрсету (панельдер мен виджеттерді орнату, олардың орналасуы және көрсетілетін ақпарат түрлері);  • Виртуалды машинаның қашықтағы хосттармен әрекеттесуін сүзетін кірістірілген брандмауэрді қолдау  • Статистиканы, әртүрлі типтегі есептерді, трафик ақпаратына негізделген графиктерді визуализациялау (жіберілген байттар, ағындар, пакеттер саны);  • Желінің өнімділік көрсеткіштерін визуализациялау;  • Деректерді талдау және PDF және CSV файлдарына экспорттау мүмкіндігі  • Деректерді PDF немесе CSV форматына экспорттау мүмкіндігі, сондай-ақ электрондық пошта арқылы автоматты түрде жіберу мүмкіндігі бар кірістірілген есеп беру механизмі;  Аномалияларды анықтау жүйесіне қойылатын талаптар:  • NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream желілік трафиктегі ауытқуларды анықтау механизмдерін қолдау;  • Желілік ағынды қайталау механизмдерін қолдау;  • Желілік ағындар деңгейінде трафикті іріктеу;  • Трафик көздерінің домендік атауларын тану және сақтауды қолдау;  • Желілік ағындарды, ақпараттық қауіпсіздік инциденттерін және желідегі ауытқуларды талдау үшін қолданылатын алдын ала анықталған ережелер мен алгоритмдердің болуы;  • қолтаңбасыз әдістерді қолдану арқылы желілік шабуылдарды анықтау (соның ішінде портты сканерлеу, құпия сөзді дөрекі шабуылдар, DoS/DDoS, желілік протоколдар SSH, RDP, Telnet және т.б. шабуылдар);  • желілік трафиктегі ауытқуларды анықтау, соның ішінде DNS, DHCP, SMTP, мультикаст және т.б.;  • JA3 саусақ іздері арқылы шифрланған трафикті талдауды қолдау;  • Заңсыз хаттамалар мен қосымшаларды, соның ішінде P2P желілерін, «анонимизация» қызметтерін (соның ішінде TOR) және т.б. анықтау;  • IP мекенжайлар мен елдердің репутация тізімдері негізінде ақпараттық қауіпсіздік инциденттері мен желілік ауытқуларды анықтау;  • Жүйелік қызметтердің (соның ішінде DNS) жұмысына байланысты операциялық ақауларды анықтау, сондай-ақ желідегі жаңа түйіндер мен қызметтерді анықтау;  • LAN желісіндегі түйіндердің мінез-құлық моделіне негізделген ақпараттық қауіпсіздік инциденттері мен желілік ауытқуларды автоматты түрде анықтау;  • Ақпараттық қауіпсіздік инциденттері мен желідегі ауытқуларды анықтау әдістерін орнатуды автоматтандыру үшін алдын ала анықталған процедуралардың болуы;  • MISP платформасын қолдау;  • MITER ATT&CK жүйесін және контекстке сезімтал дисплейді қолдау;  • Әртүрлі IP мекенжайлары, сегменттері, қызметтері мен қызметтері үшін ақпараттық қауіпсіздік инциденттері мен желілік ауытқуларды анықтау әдістерін теңшеу;  • Пайдаланушының ISO OSI үлгісінің 7-деңгейіндегі ақпарат негізінде ақпараттық қауіпсіздік инциденттері мен желілік ауытқуларды анықтаудың өз әдістерін конфигурациялау мүмкіндігі;  • ISO OSI үлгісінің 3 және 4 деңгейлеріндегі ақпарат негізінде NAT анықтау;  • Оқиғаларды сүзу механизмі, оның ішінде кірістірілген сүзгілер. CSV файлдары арқылы сүзгілерді импорттау және экспорттау мүмкіндігі;  • Жалған позитивтерді басқару (ерекшеліктерді қолмен орнату)  • IP мекенжайларына, оқиға түрлеріне және оқиғалардың геолокациясына негізделген реттелетін оқиға басымдылығы;  • CEF пішіміндегі Syslog протоколы арқылы пайдаланушы хабарландырулары;  • SNMP Trap механизмі арқылы пайдаланушы хабарландырулары;  • Электрондық пошта арқылы пайдаланушы хабарламалары (HTML немесе TXT пішімінде);  • Алдын ала анықталған пайдаланушы сценарийлеріне негізделген жүйелік оқиғаларға автоматтандырылған жауап;  • Ақпараттық ағындарды өңдеу – 5000 ағын/с;  • Мінез-құлық үлгілерін өңдеу – 5000 жіп/с;  • Сыртқы ақпараттық қызметтермен, соның ішінде DNS, WHOIS, геолокация қызметтерімен және HTTP хаттамасына негізделген басқа пайдаланушы қызметтерімен интеграциялық механизмдерді қолдау;  • Жүйе пайдаланушылары бойынша оқиғаларды санаттау және түсініктеме беру;  • Оқиға түріне, оқиға көзінің IP мекенжайына, оқиға санатына, оқиға идентификаторына және т.б. негізделген оқиғаларды іздеу механизмдерін қолдау;  • Пайдаланушы интерфейсінің графиктері мен кестелері негізінде оқиғаларды интерактивті визуализациялау;  • Электрондық пошта арқылы жіберуге қолдау көрсететін алдын ала анықталған шаблондар мен пайдаланушы параметрлеріне негізделген есеп беру және PDF форматына экспорттау механизмінің болуы;  • Оқиғаларды CSV пішіміне экспорттау;  • Ашық API интерфейсі арқылы интеграцияны қолдау;  • Сыртқы SIEM жүйесіне Syslog арқылы жүйе конфигурациясын өзгерту оқиғаларын тіркеу;  • Келесі түрдегі оқиғаларды визуализациялауды қолдау: Оқиғалар ағашы, Уақыт кестесі, Мәліметтер, Растаулар, Интерактивті режим;  • Келесі үшінші тарап өнімдерімен интеграцияны қолдайды: IBM QRadar қолданбасы, LDAP/AD  Жүйе мыналарды қамтамасыз етуі керек:  - 10Гб/с жоғары жылдамдықты деректер желілеріндегі байланыс арнасына қосылған пайдаланушы таңдайтын желілік интерфейстен (максималды, мүмкін жаңартуларды ескере отырып, бір сілтемеге 40Гб/с дейін), барлық желілік трафикті түсіру;   * + 1. **Почта трафигін фильтрлеу жүйесі**   Почта трафигін фильтрлеу жүйесі келесі функцияларды қамтамасыз етуі керек:  - жіберушінің IP мекенжайын Sender Policy Framework (SPF) технологиясы арқылы домен үшін рұқсат етілген мекенжайлар тізіміне сәйкестігін тексеру; DKIM/DMARC технологияларын қолдау;  - кіріс және шығыс электрондық почта хабарламаларының ағынындағы вирустардың, құрттардың, трояндардың және басқа да зиянды бағдарламалардың барлық түрлерін нақты уақыт режимінде іздеу және жою, спам-хабарламалардың, соның ішінде тіркемелердің бақылау сомасын тексеру;  - хат мәтініндегі зиянды және фишингтік сілтемелерді анықтау;  - эвристикалық анықтау әдістерін қамтамасыз ету;  - репутацияның бұлттық қызметтерін қосуды және пайдалануды қамтамасыз ету керек;  - кіріс электрондық хаттарды спамға тексеру;  - бұрын белгісіз қауіптерді блоктау үшін аномалияларға құрама файлдарды орамнан шығаруға және талдауға мүмкіндік беретін қорғаныс компонентінің толық жұмыс істеуін қамтамасыз ету;  - аты, түрі және қосымшалардың өлшемі бойынша электрондық почта хабарламаларының мазмұнын фильтрлеу;  - Active Directory және Open LDAP каталог қызметтерімен біріктіру;  - IPv6 хаттамасы арқылы жұмыс істеу;  - хатты жіберушінің мекенжайы (электрондық почта және/немесе IP мекенжайы) бойынша өзінің «қара» және «ақ» тізімдері бойынша хабарламаны фильтрлеу немесе сүзгіден шығару;  - сұр тізімге негізделген спамға қарсы механизмді қолдау («сұр тізімдер»);  - DNS негізіндегі нақты уақыттағы қара нүктелер тізімінде (DNSBL) жіберушінің IP мекенжайының болуын тексеру;  - хаттың негізгі бөлігінде орналасқан сайттардың мекенжайлары мен сілтемелерін тексеру, хат мәтініндегі сілтемелердің URL мекенжайларын тексеру және қайта жазуды қолдау;  - белгілі спам-хабарлама қолтаңбалары бар графикалық тіркемелердің сәйкестігін тексеру;  - вирус жұққан, күдікті және зақымдалған почта трафигі объектілерін карантиндік каталогқа көшіру, парольмен қорғалған файлдарды анықтау;  - жалпы және жеке карантиннің болуы;  - жеке қара және ақ тізімдерді құру;  - сұраныс бойынша объектілерді вирусқа қарсы сканерлеуді орындау;  - жіберушілер мен алушылар топтары үшін белгіленген ережелерге сәйкес почта трафигін өңдеу;  - тіркелген файлдардың атаулары мен түрлері бойынша хабарламалардың почталық ағынын қосымша фильтрлеуді ұйымдастыру және сүзгіден өткен хабарламаларға жеке өңдеу ережелерін қолдану;  - фильтрлеу ережелерін құру кезінде тұрақты тіркестерді қолдану;  - жіберушіге, алушыға және сервер әкімшісіне вирус жұққан және күдікті объектілері бар электрондық хабарлама туралы хабарламалар;  - бағдарламаны басқару пәрмен жолы (SSH) арқылы және браузерлерде жұмыс істейтін арнайы веб-интерфейс арқылы жүзеге асырылуы керек: Internet Explorer, Google Chrome, Yandex;  - анық зиянды ғана емес, сонымен қатар ықтимал қауіпті қосымшаларды анықтау және жою, мысалы: жарнамалық бағдарламалар, ақпарат жинау бағдарламалары, ақылы сайттарға автоматты терулер және шабуылдаушылар өз мақсаттарында пайдалана алатын басқа да утилиталар;  - мақсатты шабуылдардан қорғау: корпоративтік электрондық почта компромиссі (BEC), жіберушінің спуфингінен көп деңгейлі қорғаныс, қос домендерден қорғау;  - жоғары қолжетімділікті қолдау (HA): Белсенді-Пассивті; құрылғының ақаулығын анықтау және хабарлау;  - карантиндік және почталық кезектерді синхрондау;  - карантиннен хат «босатылған» кезде қайта тексеру;  - PDF файлдары мен кескіндерді спамға талдау;  - жақында тіркелген домендерді анықтау.   * + 1. **Осалдықты сканерлеу жүйесі**   Жалпы жүйелік талаптар  Жүйе келесі опцияларды қоса, бірақ олармен шектелмей, қамтамасыз етілуі керек:  • VMware немесе Hyper-V үшін дайын виртуалды құрылғы (VA - Virtual Appliance);  • Linux ОЖ үшін орнату пакеті.  • Орталық басқару  • Жүйе бір веб-интерфейс арқылы оның барлық компоненттері мен функционалдығын орталықтандырылған басқаруды қамтамасыз етуі керек.  • Жүйе есептерді жасауға және өзгерістер хронологиясына мүмкіндік беру үшін сканерлеу және активтерді бағалау нәтижелерін дерекқорда сақтауы керек.  • Деректер базасы келесі критерийлерге сай болуы керек:  • Нәтижелерді сақтау үшін үшінші тарап дерекқорларын пайдалануды талап етпеңіз  • Нәтижеге байланысты репозитарийлерде сканерлеу деректерінің бөлек сақталуын қамтамасыз етіңіз (осалдықтардың түрлері, ресурстар топтары және т.б.), деректерді талдау немесе сұрау кезінде нәтижелерді кез келген комбинацияда біріктіріңіз.  • Деректерді белгілі және конфигурацияланатын уақыт кезеңіне сақтаңыз, содан кейін дерекқор ескірген ақпараттан автоматты түрде тазартылады.  • Жүйе пайдаланушылары  • Жүйе рөлдік басқаруды және қол жеткізу құқықтарын саралауды қолдауы керек: Сканерлерді құру; Агентті синхрондау тапсырмаларын жасау; Агенттік сканерлеуді құру; Рөлді басқару; Топты басқару; Топтық байланыстарды басқару; Деректер базасын тексеруді жаңарту; Сканерлеу саясатына немесе оның болмауына байланысты кез келген сканерлеуді орындау; Пайдаланушыны басқару; Осалдық деректерін қарауға қол жеткізу; Активтер тізімдерін анықтау, құру және ортақ пайдалану; Аудиторлық файлдарды қосу; Ескертулерді құру; Тіркелгі деректерін қамтамасыз ету арқылы сканерлеу тіркелгі деректерін анықтаңыз және бөлісіңіз; Сканерлеу саясаттарын жасау және бөлісу; Билеттерді басқару (жұмыс процесі); Пайдаланушы әрекеттерінің аудиті.  • Жүйе пайдаланушыға анықталған осалдық қаупін қабылдауға немесе жеткізуші нені анықтайтынына қарамастан, оны қажетті деңгейге дейін қайта анықтауға мүмкіндік беруі керек.  • Жүйе осалдықтарды зерттеу және түзету үшін жұмыс үрдісінің билетін басқаруды қолдауы керек.  • Жүйе билеттерді жеке тағайындауға мүмкіндік беруі керек.  • Жүйе билетке қатысты осалдықтардың тізімін жүргізуі керек.  • Жүйе пайдаланушыға платформаның негізгі қауіпсіздік және кіру параметрлерін конфигурациялауға мүмкіндік беруі керек, мысалы:  • Құпия сөз саясаты;  • Әрекеттерді тіркеу;  • Сеанс күту уақыты.  • Жүйе Жүйе пайдаланушыларының шектеусіз санын жасау мүмкіндігін қамтамасыз етуі керек.  • Берілген деректерді шифрлау  • Жүйе Жүйе құрамдастары/модульдері арасындағы байланысты шифрлау үшін қажет.  • Жүйе пайдаланушылар мен Жүйе арасындағы байланысты шифрлауды қамтамасыз етуі керек.  • Сыртқы аутентификация мен авторизацияны қолдау  • Ішкі пайдаланушылар үшін аутентификация мен авторизацияны қамтамасыз ету үшін жүйе үшінші тарап жүйелерімен (LDAP, AD) біріктірілуі керек.  • Жүйе өнімділігі  • Жүйе ITS жүйесінде кемінде 500 IP мекенжайын сканерлеу мүмкіндігін қамтамасыз етуі керек.  • Жүйе коммутациялық жабдықты, маршрутизаторларды, брандмауэрлерді және енуді болдырмау жүйелерін жинау, талдау және тексеру мүмкіндігін қамтамасыз етуі керек.  • Активтерді басқару  • Жүйе активтерді анықтау, портты сканерлеу немесе ОЖ сәйкестендіру үшін сыртқы сканерлерге сенбеуі керек.  • Жүйеде активтерді қолмен қосу мүмкіндігі болуы керек.  • Жүйе трафикті талдау негізінде белсенді немесе агент сканерлеуін қолданбай, желідегі жаңа активтердің көрінісін анықтай алуы керек. Бұл ретте жүйе, кем дегенде, келесі түрлер бойынша активтерді анықтауы керек: Серверлер, Жұмыс станциялары, Қолданбалар, Операциялық жүйелер, Желілік құрылғылар, Виртуалды және бұлттық жүйелер, BYOD құрылғылары, Ұялы телефондар, IOS жүйесі бұзылған құрылғылар.  • Жүйе жоспарлы да, сұраныс бойынша да желілік түгендеуді шектеусіз сканерлеу мүмкіндігіне ие болуы керек.  • Жүйе сканерлеу нәтижелерін IP мекенжайлары өзгеруі мүмкін DHCP ортасындағы активтермен байланыстыра алуы керек.  • Жүйе әртүрлі критерийлер мен ережелер негізінде активтерді динамикалық түрде қосу мүмкіндігі болуы керек.  • Жүйеде желідегі белгілі бір активтерді автоматты түрде жіктеу және динамикалық таңбалау үшін кіріктірілген функционалдылық болуы керек, соның ішінде, бірақ олармен шектелмей, келесі критерийлер: IP ішкі желісіне жататындығы бойынша; NetBIOS және FQDN атауына негізделген; Операциялық жүйеге негізделген; Ашық порттар/қызметтер арқылы; Белгілі бір осалдықтың болуына негізделген; Сканерлеу уақытына негізделген; Жоспарланған сканерлеуді өткізіп алған активтер және т.б.  • Жүйе сканерлеу тапсырмалары кезінде тұтынушы арналарының шамадан тыс жүктелуін болдырмау үшін инфрақұрылымға жүктемені конфигурациялауға мүмкіндік беруі керек.  • Артықшылықты сканерлеуді орындау кезінде жүйе Windows жүйелерінде қашықтағы тіркеу қызметтерін автоматты түрде іске қосуы керек, содан кейін сканерлеу аяқталғаннан кейін бұл қызметтерді автоматты түрде тоқтатуы керек.  • Қолдау көрсетілетін операциялық жүйе және сканерлеуге арналған дерекқор  • Жүйе келесі операциялық жүйелерді сканерлеуді қоса, бірақ олармен шектелмей қолдауы керек: Microsoft Windows; AIX; Solaris; HP/UX; Linux; Желілік бағдарламалық қамтамасыз ету; MacOS.  • Жүйе келесі дерекқорларды сканерлеуді қоса, бірақ олармен шектелмей қолдауы керек: MS SQL; IBM DB2; Informix/DRDA; MySQL; Oracle деректер базасы; PostgreSQL; Sysbase ASE.  Деректерді визуализациялау (бақылау тақтасы)  • Жүйеде деректерді визуализациялауға арналған кірістірілген панельдер жинағы болуы керек (бақылау тақтасы).  • Жүйе пайдаланушы деректерді визуализациялау тақталарын жасауға мүмкіндік беруі керек.  • Визуализация тақталарында автоматты жаңарту мүмкіндігі болуы керек.  • Жүйе визуализация панелінің элементтерін бөлек терезеге «төмендетуге» қолдау көрсетуі керек (үздіксіз мониторинг пен оқиғаны тергеуді жүзеге асыру үшін).  • Жүйе деректерді визуализациялау тақталарын ортақ пайдалануды қолдауы керек.  • Визуализация тақталары таңдауларды, тегтерді, активтерді, уақытты және т.б. пайдаланып ақпаратты сүзуге мүмкіндік беруі керек.  • Жүйе көрсетілген деректерді визуализациялау тақталары негізінде есептерді жасауға және жүктеп алуға мүмкіндік беруі керек.  API қолдауы  • Жүйе жүйелік дерекқорда орналасқан ақпаратқа қол жеткізу үшін API қамтамасыз етуі керек.  • Жүйеде басқа жүйелермен біріктіру үшін API болуы керек  • API тегін берілуі керек.  • Автоматты жаңарту  • Жүйе пайдаланушының қосымша уақыт шығынынсыз конфигурацияларды автоматты түрде жаңартуды қамтамасыз етуі керек. Мысалы, жеке жүйе құрамдастары үшін осалдық дерекқорларын жаңарту.  • Автоматты жаңартулар мыналарды қамтуы керек, бірақ олармен шектелмейді:  • Жоспарланған жаңартулар;  • Қолмен жаңарту;  • Жаңартуды жүктеп алу және қажетті уақытта орнату мүмкіндігі.  • Сақтық көшірме жасау және қалпына келтіру  • Жүйе конфигурацияның автоматты сақтық көшірмесін және конфигурацияны бір графикалық веб-интерфейстен сақтық көшірмеден қалпына келтіру мүмкіндігін қамтамасыз етуі керек.  • Жүйе конфигурацияның көшірмесін шешімнен бөлек сақтай алуы керек.  • Масштабтау  • Жүйе сатып алынған функциядан қосымша инвестицияны қажет етпестен қарапайым, жылдам масштабтауды және функционалдылықты кеңейтуді қамтамасыз етуі керек.  • Жүйе қосымша техникалық қызмет көрсету шығындарынсыз географиялық алыс модульдердің өзара әрекеттесуін қамтамасыз етуі керек.  • Жүйе сканерлеу жұмысында сканердің қолжетімділігіне негізделген сканерлер арасында жүктемені динамикалық түрде бөлу арқылы осалдық сканерлері бойынша жүктемені теңестіруді, ақауларды қалпына келтіруді қолдауы керек.  Сканерлеу  • Жүйе келесі мүмкіндіктерді жүзеге асыруы керек: Кесте бойынша сканерлеу; Белгіленген сканерлеу тапсырмаларында қажетті сынақтарды қосу/өшіру; Тапсырманы қажетті уақытқа кідірту; Кестеге сәйкес қызмет процестерімен бос емес болса, маңызды ресурстарды сканерлеуден автоматты түрде алып тастау мүмкіндігі; Оқшауланған желі сегментін сканерлеу, содан кейін нәтижелерді бір консольге жүктеп салу; Сканерлеу үшін осалдықтарды таңдау; Арнайы порттарды сканерлеу; Есептік жазбаларды пайдалану.  • Жүйе сканерлеу кезінде кем дегенде келесі аутентификация түрлерін орындай алуы керек:  • Windows операциялық жүйесі үшін: логин мен құпия сөз, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, NTLM Hash, LM Hash;  • Unix жүйелері үшін: логин мен құпия сөз, Kerberos, CyberArk Vault, Lieberman, Thycotic Secret Server, Arcon, Centrify, BeyondTrust, Hashicorp Vault, сертификат, ашық кілт;  • Желілік жабдық үшін – SNMP;  • Жүйе әртүрлі пішімдерде сканерлеу мақсаттарын қабылдай алуы керек: активтер, IP мекенжайлары, IP желілері, атаулар.  • Сканерлеу модулі кем дегенде келесі амалдық жүйелерде орнатылуы керек: Windows; Linux; MacOS; Amazon Linux; FreeBSD; Федора.  • Жүйе пайдаланушыларға өздерінің сканерлеу тексерулерін жазуға және пайдалануға мүмкіндік беруі керек.  • Жүйеде ipv4 және ipv6 желілері үшін жүйелерді белсенді сканерлеусіз пакеттік деңгейде желілік трафикті бақылау арқылы активтерді пассивті ашу мүмкіндігі болуы керек. Бұл жағдайда жүйе кем дегенде мыналарды анықтауы керек: Ашық порттардың тізімі; Пайдаланылған хаттамалар тізімі; Хост атрибуттарының тізімі.  Осалдықты анықтау  • Жүйе проблемаларды, тәуекелдерді және осалдықтарды анықтауы және жіктеуі керек. Ол сондай-ақ тәуекелдердің сипаты туралы егжей-тегжейлі ақпаратты және оларды азайту бойынша ұсыныстарды қамтуы керек.  • Жүйе қауіпсіздік бойынша кеңес беретін ұйымдар анықтауы тиіс активтегі белгілі осалдықтар туралы есеп беруі керек (мысалы, Жалпы осалдықтар және әсер ету деректері дерекқоры (CVE) немесе Open Source осалдық дерекқоры (OSVDB) немесе SecurityFocus Bugtraq (BID) немесе кез келген комбинациясы. бұл).  • Өнімнің осалдығы дерекқоры тексерулерді қамтуы керек: ОЖ қауіпсіздігі және патч; CISCO; Брандмауэрлер; DNS; FTP; SMTP; RPC; SNMP; LDAP; ШОБ; CGI; Веб-серверлер; Мәліметтер базасы; Backdoors; Қызмет көрсетуден бас тарту; Әдепкі тіркелгілер; Пиринг жүйесі; Remote Shell;  Жүйе істей алуы керек:  • стандартты емес порттарда жұмыс істейтін қызметтерді анықтау.  • қосылым баннерлерін көрсету үшін конфигурацияланбаған қызметтерді анықтау.  • әртүрлі порттарда жұмыс істейтін бір қызметтің бірнеше данасын тексеру.  • «өлі түйіндерді» сканерлеу («ping» пәрменіне жауап бермейтін құрылғылар).  • Аудит  • Жүйе жүйелердегі патчтардың конфигурациясын және қолжетімділігін тексеру мүмкіндігін қамтамасыз етуі керек: Windows; Unix/Linux; Adtran NetVanta; Alcatel TiMOS; Arista EOS; ArubaOS; BlueCoat ProxySG; Brocade FabricOS; GAiA бақылау нүктесі; Cisco ACI; Cisco Firepower; Cisco IOS; Citrix қолданбасын жеткізу; Мәліметтер базасы; ExtremeXOS; F5; FireEye; FortiGate FortiOS; HP ProCurve; Huawei VRP; IBM DB2 DB; IBM iSeries; Juniper Junos; MongoDB; MS SQL МБ; NetApp API; OpenShift контейнер платформасы; Oracle DB; Palo Alto желілері; PostgreSQL DB; RHEV; Salesforce.com; SonicWALL SonicOS; Sybase DB; VMware vCenter/vSphere; WatchGuard; ZTE ROSNG;  Жүйе аудит саясатын қамтамасыз етуі керек, оның ішінде ең аз дегенде: ТМД эталондары; Microsoft үздік тәжірибесі; DISA STIGs; NIST; PHI/PII мазмұны; Теңшелетін конфигурациялар.  • Жүйенің қосымша зияткерлік басымдылық мүмкіндігі болуы керек, ол арқылы жүйе шабуыл кезінде әрқайсысын пайдалану ықтималдығына негізделген осалдықтарға басымдық беруі керек және жеке меншікті пайдалану арқылы жеткізушінің осалдық деректері мен үшінші тараптың осалдық деректері мен қауіптерін қоса, тәуелсіз деректер көздерін біріктіруі керек. жақын болашақта пайдаланылуы мүмкін осалдықтарды анықтау үшін машиналық оқыту алгоритмі. Бұл функция жүйеде Интернетке қосылуды қажет етпей жұмыс істеуі керек.  Ескертулер мен хабарландырулар  • Жүйе осалдықты сканерлеу немесе конфигурация аудиті нәтижелеріне негізделген ескертулерді қолдауы керек.  • Есеп беру  • Жүйе барлық оқиғалар туралы есеп беруді қамтамасыз етуі керек, есеп беру веб-интерфейс арқылы қолжетімді болуы керек.  • Жүйе есеп беруді дербес конфигурациялауға және өз есептерді жасауға мүмкіндік беруі керек.  • Жүйе сұраныс бойынша есептерді шығара алуы керек.  • Жүйе пайдаланушының жаңа есептерді оңай пайдалануы және жасауы үшін жасалған есептердің мысалдарын қамтамасыз етуі керек.  • Жүйеде кірістірілген есептер болуы керек.  • Жүйеде кірістірілген немесе жылдам қол жеткізуге болатын дайын үздік тәжірибе есеп беру пакеттері (NIST, CIS, ISO) болуы керек.  • Жүйе желідегі әртүрлі сегменттер мен жүйелер үшін белгілі бір уақыт аралығында есеп беруді қамтамасыз етуі керек.  • Жүйе жасаған есептер кем дегенде келесі ақпаратты қамтуы керек:  • Жеткізуші шкаласы мен CVSS сәйкес осалдықтың атауы және оның маңыздылық деңгейі;  • осал жүйелер немесе қызметтер тізімі;  • осалдық жағдайы;  • осалдықты жою бойынша ұсыныстар немесе егер бар болса, патчқа сілтеме;  • Осалдықтарға басымдық берудің қосымша критерийлері: эксплуат, зиянды кодтың болуы және т.б.  • Осалдықты басқару  • Жүйе осалдықтың анықталған күнін және инфрақұрылымда осалдықтың болған уақыты туралы есептерді сүзу және жасау үшін соңғы табылған күнді қадағалауы керек.  • Жүйе патчтардың жоқтығын, қызметтердің қолжетімділігін тексеруді, аудит файлдарына сәйкестікті тексеруді және т.б. қолдау көрсетуі керек.  • Жүйе үшінші тараптың осалдықты сканерлеу жүйелерінен ақпаратты импорттай алуы керек.  • Жүйе қажет болған жағдайда агенттерсіз агенттер арқылы желі ішіндегі және сыртындағы ресурстарды сканерлеу мүмкіндігін қамтамасыз етуі керек.  • Кеңейту опциялары  • Жүйе өндірушінің ресми веб-сайтынан қосымшаларды қосу арқылы өзінің функционалдығын кеңейте алуы керек.  • Жүйе бір өндірушінің осалдықтарын іздеу үшін пассивті сканерді қосу арқылы өзінің функционалдығын кеңейте алуы керек. Пассивті сканер жүйені белсенді сканерлеусіз желілік трафикті бақылау арқылы хосттарды пассивті табу мүмкіндігін қамтамасыз етуі керек.  Лицензиялау  • Жүйені лицензиялау жеке жүйе құрамдастарын лицензиялауға қарамастан, IP санына негізделуі керек.  • Лицензия мыналарды қамтуы керек: сканерлердің шектеусіз саны; Толық функционалдығы бар агенттердің шектеусіз саны; Халықаралық стандарттарға (DISA STIG, CIS, MSCT және т.б.) сәйкестікке жүйелік аудит саясаты;  • Rest API.  Интеграциялар  • Жүйе келесі шешімдермен интеграцияны қолдауы керек: VMware AirWatch – MDM; APCON – желіні бақылау; Apple - MDM; Аруба, Hewlett Packard Enterprise компаниясы – NAC; Аксониус - CMDB; Atlassian - Қауіпсіздік операциялары; BeyondTrust - артықшылықты қол жеткізуді басқару; Bomgar/Liberman - артықшылықты рұқсатты басқару; BMC – патчтарды басқару; Brinqa – TVM; Cisco - NAC; CyberArk - артықшылықты қол жеткізуді басқару; Цимуляция – симуляция; Dell - патчтарды басқару; ForeScout - NAC; Garland Technology – Networking; Gigamon – желілік байланыс; Blackberry – MDM арқылы жақсы қуатталған; HCL BigFix - патчтарды басқару; IBM - SIEM; Infoblox - IP мекенжайын басқару; Кенна – TVM; LogRhythm - SIEM; Microsoft - SIEM; Red Hat - патчтарды басқару; Redseal – TVM; ServiceNow - Қауіпсіздік операциялары; Splunk - SIEM; Symantec - патчтарды басқару; ThreatConnect – қауіп барлау; Thycotic - артықшылықты есептік жазбаны басқару.  • Барлық тізімделген интеграцияларға Жүйе өндірушісі қолдау көрсетуі керек.  • Орналастыру  • Жүйенің барлық құрамдас бөліктері Интернетке қосылуды қажет етпестен жергілікті жерде орнатылуы және қолдауы болуы керек  • Жүйе желіден тыс белсендіруді қолдауы керек.  • Жүйе Интернетке қосылудың қажетінсіз Жүйенің жаңартуларын және осалдықтар туралы ақпаратты қолдауы керек.  Өнімді лицензиялау талаптары  • Бағдарламалық құрал пакеті келесі схемаға сәйкес лицензиялануы керек:  Пайдаланушылар санын шектеместен кемінде 1200 ресурстарды қосуға лицензия.   * + 1. **Бастапқы кодты талдау жүйесі**   Жалпы талаптар  «Қосымшаның қауіпсіздігін тексеру жөніндегі бағдарламалық жасақтама лицензиясы» (бұдан әрі - Өнім) келесі мүмкіндіктерді және функцияларды қамтуы керек:  - бағдарламалық жасақтаманы (бұдан әрі – бағдарламалық қамтамасыз ету) бастапқы кодтың ақпараттық қауіпсіздік талаптарына сәйкестігін талдау;  - бағдарламалық жасақтамада жарияланбаған мүмкіндіктерді (бұдан әрі - NDV) іздеу;  Өнім жалған позитивті және жалған теріс мәндердің санын автоматты түрде азайту мүмкіндігін қамтамасыз етуі керек.  Ақпараттық жүйенің немесе автоматтандырылған ақпараттық жүйенің (бұдан әрі - АЖ немесе ААЖ) қосымшаларын талдау нәтижелері бойынша ол пайдаланылуы осындай осалдықтар мен NDV үшін ақпараттық қауіпсіздік құралдарын (бұдан әрі - АЖҚ) орнату бойынша ұсынымдар беруі керек. ISIS орнату арқылы алдын алуға болады;  Өнім бағдарламалық жасақтамада ресурстарды шектеусіз кемінде бір серверде/жұмыс станциясында/виртуалды машинада және кемінде бес пайдаланушыға бір жыл бойы пайдалану құқығын қамтамасыз етуі керек.  Өнімнің бастапқы кодын талдау функциясы келесі талаптарға сай болуы керек:  - келесі бағдарламалау тілдерінде жазылған бастапқы кодты талдау керек: C/C++, C#, Java, Android үшін Java, JavaScript, .NET Core, ASP.NET, TypeScript, Kotlin, Swift, COBOL, SAP ABAP, Scala, VB.NET , Go, Ruby, PHP, Python.  - өнім жаңа бағдарламалау тілдері мен фреймворктарын қоса алуы керек;  - өнім келесі бағдарламалау орталарында жазылған кодты сынай алуы керек: AngularJS, Node.js, Vue.js, Apache Struts, .NET 4.5, ASP .NET MVC, ASP .NET, Django, EJB 2, Ionic, J2EE , JJSF 2, Jax – RS, Jax – WS, Objective C, React Native, SAP ABAP, Spring MVC, Xamarin, Symphony.  Өнім мыналармен интеграцияны қолдауы керек: Azure DevOps Services, Azure DevOps Server (TFS), Apache Ant/Uunce, Apache Maven, Gradle, Jenkins, MSBuild.  Өнім Visual Studio Code IDE ішінде нақты уақыттағы сканерлеу мүмкіндіктерін қамтамасыз етуі керек.  Өнім бастапқы кодты және байт-кодты (құрастырылған) сканерлеуді, соның ішінде деректер ағынын талдауды сканерлеу мүмкіндігін қамтамасыз етуі керек.  Өнім осалдықтар үшін веб-бағдарламалар трафигін бақылау және оларды орталық консольге хабарлау мүмкіндігін қамтамасыз етуі керек.  Өнім Java, .NET және Node.js қосымшаларының интерактивті сынақтарын қолдауы керек.  Өнім Git нұсқасымен және тапсырмаларды басқару жүйелерімен біріктірілуі керек: Jira, Azure DevOps.  Өнім келесі ақпараттық қауіпсіздік талаптарына сай болуы керек:  - өнім орталық консольде пайдаланушы рөлдерін анықтау және пайдалану мүмкіндігін қамтамасыз етуі керек. Бұл рөлдер пайдаланушының жұмыс үстеліндегі жергілікті сканерлеу құралдарына да кеңейтілуі керек.  - пайдаланушының ресурстарға қол жеткізуін бақылау қауіпсіздік қызметкері конфигурациялаған пайдаланушы құқықтарына сәйкес жүзеге асырылуы тиіс;  - ресурстарға қол жеткізу тек жеке логин мен пароль арқылы жүзеге асырылуы тиіс;  - пайдаланушы құпия сөздері шифрланған түрде сақталуы керек;  - қауіпсіздік қызметкерінің функцияларына қол жеткізу тек қауіпсіздік қызметкерінің жеке логині мен паролін пайдалану арқылы жүзеге асырылуы керек;  - иерархиялық деңгейлер бойынша функционалдылыққа қол жеткізуді бөлу қамтамасыз етілуге ​​тиіс;  - Орталық консольдегі, сондай-ақ жергілікті сканерлеу құралдарындағы пайдаланушы, әкімші және жүйелік әрекеттер журналға тіркеліп, орталықта сақталуы керек.  - Орталық консольдің бір рет кіру жүйесі Microsoft, Okta және PingFederate идентификациялық провайдерлерімен біріктіру үшін SAML пайдалануды қолдауы керек.  Өнім келесі функцияларды қамтамасыз етуі керек:  - барлық ақпаратты орыс және/немесе ағылшын тілдерінде ұсыну;  - Өнім беретін ақпаратқа қол жеткізудің бірыңғай нүктесін қамтамасыз ету;  - Уақыт өте келе барлық қосымшалардың қауіпсіздік күйін және олардың күйін көруді қамтамасыз ету үшін бақылау тақталары бар орталық консоль қамтамасыз етілуі керек.  Өнім қауіпсіздік қатерлерінің рейтингтері, сынақ күйі, ашық мәселелер, негізгі мәселе түрлері және мәселенің маңыздылығы туралы ақпаратты қамтамасыз етуі керек.  Осалдықтардың дерекқорына және ереже үлгілеріне қойылатын талаптар  Өнім дерекқорды теңшеу және пайдаланушы осалдықтарын біріктіру үшін пайдаланушы ережелерін жасай алуы керек.  Осалдықты сипаттауға/түзетуге қойылатын талаптар  Әрбір анықталған осалдық туралы техникалық ақпарат мыналарды көрсетуі керек:  • осалдық түрі  • қалай, қайда және қашан анықталды,  • түзетілмесе, ықтимал пайдаланудың ауырлығы  • осалдықтардың анық жіктелуі  • түзету/жеңілдету бойынша ұсыныстар мен ұсыныстар  • орынды және орынсыз шешімдердің мысалдары  Есеп беру талаптары  Өнім PDF және HTML пішімінде есептерді шығара алуы керек:  • CWE/SANS Top 25 2011 ж  • DISA қолданбасының қауіпсіздігі және дамуы STIG  •Open Web Application Security Project (OWASP) Mobile Top 10  •Open Web Application Security Project (OWASP) Топ 10 2013, 2017, 2021  • Төлем картасы индустриясының деректер қауіпсіздігі стандарты (PCI DSS) 3.2 нұсқасы  • Бағдарламалық жасақтаманың қауіпсіздік профилі  SSL және TLS (Transport Layer Security) хаттамаларына қолдау көрсету қажет.  Тапсырыс берушінің және Орындаушының уәкілетті өкілдері Қызметті пайдалануға беру актісіне қол қойған күннен бастап кемінде 12 (он екі) ай ішінде Орындаушыдан техникалық қолдау көрсетілуі тиіс.  Орындаушы өнім үшін есептеу қуатын қамтамасыз етуі, оған жеткізілетін қызметті орнатуы және конфигурациялауы керек;  Тапсырыс беруші қызметкерлерін құралды пайдалануға үйрету;   * + 1. **Артықшылықпен қол жеткізуді басқару және мониторингтеу жүйесі**   Артықшылықты қол жеткізуді басқару және бақылау жүйесі келесі функцияларды қамтамасыз етуі керек:  Шешімдер PAM шешімімен қорғалған жүйелерде әкімші агенттерді орнатуды қажет етпей, PROXY режимінде жұмыс істеуі керек.  Шешім ауыстырылатын кластерге жиналуы керек  Шешім балансты жүктей алуы керек  Артықшылықты пайдаланушылардың сеанстарын (командалар мен орындалған әрекеттер) жазу және бақылау, орындалған әрекеттердің сөзсіздігін және дәлелдемелік база үшін материалды қорғауды қамтамасыз ету үшін қауіпсіздік функцияларын пайдалануға мүмкіндік береді.  Шешім Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure сияқты бұлттық платформаларда іске асыруды қолдауы керек. Ол сондай-ақ виртуалды орталарды қолдауы керек: ядроға негізделген виртуалды машина (KVM), Microsoft Hyper-V, OpenStack, VMware vSphere. Оқшау аппараттық платформаны пайдалану мүмкіндігін де қолдау керек.  Шешім SSH және RDP протоколдары үшін PROXY және SSH / TELNET / RLOGIN / RDP / HTTP / HTTPS / VNC үшін PROXY жүйесінен қорғалған жүйелерге қосылымдарды табиғи түрде қолдауы керек.  Стандартты емес протоколдар үшін (бастапқыда шешім қолдамайды) орнату серверінде пайдаланушыға тек клиент пен оның ресурстары көрінетіндей етіп осындай протоколды қолдайтын клиентті шақыру мүмкіндігі болуы керек.  Стандартты емес хаттамалар және оларды клиент шақыруы үшін шешім Microsoft Remote қолданбасына арналған технологияларды қолдауы керек.  Профиль параметрлеріне байланысты әкімшіге, пайдаланушыға, аудиторға кіру құқықтарын тағайындау мүмкіндігі.  Аудитор рұқсаты болған жағдайда, пайдаланушы профилі кем дегенде таңдалған пайдаланушы топтары мен жүйенің мақсатты топтарының жазбаларына және олар үшін конфигурацияланған артықшылықты тіркелгілерге қол жеткізуді шектеу мүмкіндігін ұсынуы керек.  Пайдаланушы профилінің конфигурациясы бастапқы IP мекенжайы негізінде кіріс қосылымдарды сүзу мүмкіндігін қамтуы керек, яғни тағайындалған профилі бар пайдаланушылар үшін қатынасты басқару тізімдерін (ACL) жасау. Шектеу анықтамасы пішімге рұқсат беруі керек: IP мекенжайы, желі мекенжайы және желі маскасы немесе толық жарамды домен атауы (FQDN).  Шешім мақсатты жүйелердің белгіленген тобына таңдалған пайдаланушылар тобын тағайындау арқылы қатынас саясатын анықтауға мүмкіндік беруі керек.  Жазылған деректерді алдын ала қарау сессияның бейнежазбасын және барлық сеанс метадеректерін (RDP) көрсететін жазбаның транскриптін, сондай-ақ консоль үшін көрсетілген деректердің толық жазбасын (SSH) қамтуы керек.  Нақты уақыттағы қосылымды бақылау, оның ішінде сеансты бірден тоқтату мүмкіндігімен нақты уақытта көру мүмкіндігі.  Жергілікті пайдаланушылар мен әкімшілердің құпия сөздеріне арналған ережелер жинағын (саясаттарын) басқарыңыз.  Таңдалған пайдаланушы топтары үшін сеанс жазуын қосу/өшіру опциясы.  Шолғышқа арнайы плагинді орнатуды қажет етпей, кем дегенде SSH және RDP сеанстары үшін веб-портал, браузер арқылы қол жеткізуді орнату мүмкіндігі.  Шешім пайдаланушы ақпаратын синхрондау қажеттілігінсіз Microsoft Active Directory бағдарламасымен интеграцияны қамтамасыз етеді. Бұл Active Directory пайдаланушысы PAM шешімімен танылған кезде пайдаланушылар тобына автоматты түрде қосылатынын білдіреді.  RDP сеанстары үшін, мақсатты Microsoft Windows сервер жүйесінде қысқартылатын TCP қосылымдарын блоктау мүмкіндігі.  RDP сеанстары үшін мақсатты Microsoft Windows сервер жүйесінде таңдалған процестерді блоктау мүмкіндігі.  SSH және RDP сеанстары үшін орындалатын пәрмендер үшін тұрақты өрнек үлгілерін жасау мүмкіндігі және мұндай үлгі анықталса, сеансты аяқтау немесе үлгі табылған кезде хабарландыру жіберу әрекеттерінің бірін орнату мүмкіндігі.  Орындалатын SSH және RDP пәрмен үлгілерін орнату қол жеткізу жасалған пайдаланушы топтарын құру деңгейінде немесе кіру PAM шешімімен қорғалған және басқарылатын мақсатты жүйелер тобы деңгейінде орындалуы керек.  Құпия сөз енгізу өрістерінде немесе пайдаланушы тіркелгісін басқару терезесінде енгізу курсорын анықтау арқылы сеанстар кезінде енгізілген құпия сөздерді қорғаңыз.  Логин/пароль, X.509 сертификаты, SSH кілті арқылы пайдаланушы аутентификациясы.  Аутентификация протоколын қолдау: KERBEROS, RADIUS, Microsoft Active Directory, LDAP, TACACS+.  Бекітушілердің белгіленген саны бар мақсатты жүйелердің таңдалған тобына қосылымдар үшін қосымша жұмыс үрдісін бекітуді орнату мүмкіндігі.  Жүйеге кіру уақытына негізделген қосымша рұқсатты орнату мүмкіндігі, мысалы, дүйсенбіден жұмаға дейін 8:00-ден 16:00-ге дейін мақұлдау қажет емес, ал барлық басқа күндер мен уақыттар үшін мақұлдау қажет.  Белгілі бір хосттар немесе тіркелгі топтары үшін құпия сөздер мен SSH кілттерін автоматты түрде айналдыру мүмкіндігі.  Автоматты құпия сөздер мен SSH кілттеріне ерекше жағдайлар жасау мүмкіндігі.  Мақсатты жүйелерде құпия сөзді автоматты түрде өзгерту кестелерін жасау.  Бір реттік құпия сөздерді жасаңыз және оларды пайдаланғаннан кейін автоматты түрде ауыстырыңыз.  Құпия сөздерді өзгертуге арналған жеке саясаттарыңызды/талаптарыңызды жасау мүмкіндігі:  а. Қажетті таңбалардың ең аз саны  б. Әкімші көрсеткен таңбаларды қоспағанда  в. Бас және кіші әріптерді міндетті түрде пайдалану,  г. Арнайы таңбаларды міндетті түрде пайдалану,  Хосттардың әртүрлі топтары немесе тіркелгілер топтары үшін әртүрлі құпия сөзді өзгерту саясаттарын орнату мүмкіндігі.  Құпия сөзді белгілі бір уақыт кезеңіне жарамдылық мерзімі аяқталатын етіп орнатыңыз.  Файлдардағы құпия сөздерді жасыру немесе шифрын шешу арқылы басқарыңыз.  Келесі жүйелер үшін құпия сөздерді немесе SSH кілттерін өзгертуге мүмкіндік беретін плагиндерді қамтамасыз ету: AIX, F5 BIG IP, SAP, SAP IQ, AWS IAM, Checkpoint, ESX, Fortinet Fortigate, HP iLO, MS SQL Server, ORACLE, Stormshield, Teradata, Unix, Micorsoft Windows, Cisco, Dell iDRAC, IBM 3270, Juniper SRX, LDAP, MySQL, Palo Alto, Графана.  Шешім кем дегенде REST API арқылы құпия сөзді өзгертуге рұқсат беруі керек.  Өнімді лицензиялау талаптары  Бағдарламалық қамтамасыз ету пакеті келесі схемаға сәйкес лицензиялануы керек:  Пайдаланушылар санын шектемей 1000 ресурстарды қосуға арналған мәңгілік лицензия.   * + 1. **Енуге тестілеу жүргізу қызметі.**   Орындаушы жыл сайын:   * жылына бір рет сыртқы ену сынақтары, кемінде 30% пайдаланылған IP мекенжайлары және Тапсырыс берушінің сыртқы периметрінде кемінде 10 веб-қосымшалар; * ену сынағы және веб-қызметтердің, жеке түйіндер мен қосымшалардың ақауларға төзімділігі.   Қолданылатын ену сынақтарының сценарийлері мен құралдары Тапсырыс берушімен келісіледі. Нәтижелер бойынша Орындаушы анықталған осалдықтарды жоюдың кейінгі мониторингі бар есепті ұсынады.  Барлық жұмыстар Қазақстан Республикасының нормативтік құқықтық актілерінің талаптарына және «ҚТЖ» ҰК» АҚ ақпараттық қауіпсіздік және ақпараттандыру саласындағы ішкі нормативтік құжаттарына сәйкес жүргізілуі тиіс.   * + 1. **Пайдаланушыларды хабардар ету қызметіне қойылатын талаптар**   Тапсырыс беруші қызметкерлерінің хабардарлығын арттыру шеңберінде Орындаушы шарттың барлық мерзіміне келесі электрондық материалдар мен қызметтерді ұсынады:   * Ақпараттық қауіпсіздік негіздері туралы кітапша; * Ақпараттық қауіпсіздік негіздері бойынша суреттер (кемінде 15 дана); * Әрбір көрсетілетін қызмет бойынша оқытуды өткізу; * Ақпараттық қауіпсіздік негіздері нұсқаулығы.   Теориялық курс материалы келесі форматтарда ұсынылуы керек:   * мәтін; * суреттер (фото/графика/иллюстрация); оқу бейнелері; * циклдік анимациялар   Практикалық курс материалы келесі форматтарда ұсынылуы керек:   * тесттер (pickone). Функционалдық талаптар * Курс төмендегілерді қамтамасыз ететін ақпараттық жүйеде (Жүйеде) қайта шығарылуы керек   мүмкіндіктер:   * Жүйе курстық оқу материалдарына орнатусыз веб-браузер арқылы қол жеткізуді қамтамасыз етуі керек   үшінші тарап бағдарламалық жасақтамасы (Flash, Java, ActiveX және т.б.) және HTTP немесе HTTPS хаттамасы арқылы қол жетімді болуы;   * Жүйе синхрондау үшін LDAP каталог қызметтеріне қосыла алуы керек   пайдаланушылар, пайдаланушы топтары және пайдаланушының аутентификациясы;   * Жүйеде каталог қызметінен пайдаланушы есепке алуын авторизациялау функциясы болуы керек   LDAP;   * Жүйе курс құрылымын, оның материалдары мен іс-шараларын теңшеу функциясын қамтамасыз етуі керек; * Жүйе жүзеге асыру үшін үшінші тарап қызметтерімен интеграциялық функцияны қамтамасыз етуі керек   вебинарлар;   * Жүйе курстың кезеңін есте сақтап, пайдаланушыға тоқтаған жерінен жалғастыруға мүмкіндік беруі керек; * Жүйеде студенттердің курсты аяқтау жағдайы туралы есептер болуы керек; * Жүйе тек лекцияны 100% орындағаннан кейін және тестілеу мүмкіндігін қамтамасыз етуі керек   әрекеттердің шектеулі саны;   * Жүйе дәрісті өту мәртебесіне қарамастан тестілеуден өту мүмкіндігін қамтамасыз етуі керек; * Жүйе сұрақтар банкін құру және пайдалану мүмкіндігі болуы керек; * Жүйе әрекеттерде сұрақтардың бірдей құрамын жою үшін тест сұрақтарын кездейсоқ таңдай алуы керек; * Жүйе тест сұрақтарын кездейсоқ ретпен көрсете алуы керек; * Жүйе тестілеу аяқталғаннан кейін сынақ нәтижелерін автоматты түрде шығарады және нәтижені түзету мүмкіндігін бермейді; Жүйе пайдаланушының есепке алуын LDAP анықтамалық қызметінде, егер ол талап етілетін сынақтан өту баллына жетпесе, автоматты түрде құлыптай алуы керек; * Жүйеде барлық курс қатысушыларының тестілеу күйі туралы кірістірілген аралық есептер болуы керек; * Жүйе оқу топтары мен ағындарын құру мүмкіндігін қамтамасыз етуі керек; * Жүйе пайдаланушылар тобын курсқа тіркей алуы керек; * Жүйеде курсты аяқтаған студенттер тобының үлгерімі туралы есеп - әрбір студенттің курсты аяқтау пайызы және топтың күн бойынша үлгерімінің графигі болуы керек; * Жүйе өзінің курстық сертификат үлгісін (конструкторын) құра алуы керек; * Жүйе автоматты және қолмен режимде курсты аяқтағаны туралы сертификат бере алуы керек; * Жүйе жалпы және әрбір пайдаланушы үшін мәртебесі бойынша іске қосылған компаниялар туралы ақпаратпен интерактивті есепті (бақылау тақтасын) қамтамасыз етуі керек. * Әрбір қызметкер LMS жүйесіне кіріп, Active Directory есепке алу арқылы оқытуды бастай алады. * Жүйе әкімшісі курсты қабылдауды бастау үшін пайдаланушыларды курсқа тағайындауы керек.   Тапсырыс беруші қызметкерлерінің хабардарлығы мен біліктілігін арттыру шеңберінде келесі қызметтер көрсетіледі:   * Жыл сайынғы тағылымдамадан 5 күннен кем емес, Орындаушының СОК-да кемінде 5 адам.   + 1. **Компьютерлік криминалистика (форензика) қызметіне қойылатын талаптар**   Ақпараттық қауіпсіздіктің сыни инциденттерін тергеп-тексеру жөніндегі қызметтер көрсету. Қызметтерді көрсету шеңберінде желілік белсенділікті, журналдарды, параметрлердің өзгерістерін талдау, жойылған ақпаратты қалпына келтіру, шабуыл векторын іздеу және локализациялау бойынша жұмыстар жүргізіледі.   * + 1. **Консалтингтік қызметке қойылатын талаптар**   Консультациялық қызметтердің тізімі:   * Ақпараттық қауіпсіздіктің техникалық саясаты саласында кеңес беру: * Активтерді жіктеу саясатын әзірлеуде кеңес беру * Техникалық бақылау әдістерін таңдау саласында кеңес беру * Бағдарламалық және аппараттық қорғау құралдарын таңдау саласында кеңес беру * Ақпараттық қауіпсіздік шешімдерін пайдалану бойынша кеңес беру * Ақпараттық активтерді есепке алу және ақпараттық қауіпсіздік активтерін орталықтандырылған басқару саласында кеңес беру. * Ақпараттық өзара іс-қимыл бойынша кеңес беру: * Әртүрлі жүйелер үшін пайдаланушылардың әртүрлі санаттары (соның ішінде сыртқы Орындаушылер) үшін рұқсат етілген қол жеткізу деңгейі бойынша оңтайлы ұсыныстарды әзірлеу. * АЖ/АС қол жеткізуді басқаруды енгізудің техникалық құралдары мен әдістерін таңдау бойынша ұсыныстарды қалыптастыру * Әртүрлі ақпараттық өзара іс-қимыл үшін қабылданатын шаралар бойынша ұсыныстар (блоктау режимдерін таңдау, бақылау, қосымша қолмен тексеру) * Іскерлік кеңес беру: * АҚБЖ ақпараттық жүйелерімен және осы АЖ деректерімен байланысты АЖ тәуекелдеріңізді бағалау. * Тапсырыс беруші қызметкерлерінің АҚБЖ-ға қол жеткізуі үшін нормативтік құжаттарды әзірлеу бойынша ұсынымдар.   + АҚБЖ құрамдастары бар бизнес-процестерді сипаттау бойынша ұсыныстар     1. **DDoS шабуылдарын тазалау жүйесіне қойылатын талаптар**   Бұл жүйені енгізудің негізгі мақсаттары:  DDoS шабуылы кезінде заңды пайдаланушылардың жұмысын қамтамасыз ету;  Автоматты режимде нақты уақыт режимінде желіні көпвекторлы DDoS шабуылдарынан қорғау, яғни. қызметкерлердің белсенді қатысуынсыз;  Ақпараттық қауіпсіздік қызметін шабуылдар туралы хабарлау ақпаратымен қамтамасыз ету.  Орындаушы авторизацияны немесе серіктес мәртебесін жазбаша растауды (тиісті дилерлік келісімнің немесе өндірушіден, ресми дистрибьютордан алынған құжаттың көшірмелері, осы Жабдықты жеткізуге рұқсаттың/серіктес мәртебесінің болуын растайтын рұқсат хаттың көшірмесін қоса бере отырып) беруге міндеттенеді. мөрмен және/немесе қолмен немесе факсимильмен расталған Бағдарламалық қамтамасыз етудің көшірмелері).  Бағдарламалық жасақтама жеткізілетін жабдықпен толық үйлесімді болуы және осы Техникалық сипаттаманың функционалдық талаптарына сәйкес болуы керек.  Аппараттық және бағдарламалық қамтамасыз ету талаптары  Жабдық ағымдағы болуы және қолдаусыз болмауы керек және өндірушінің зауыттарында сынақтан өткен болуы керек. Барлық қажетті техникалық құжаттама мен пайдаланушы нұсқаулығы өндіруші ұсынған толық көлемде берілуі керек. Жеткізу пакетінде жеткізілетін Жабдықтың функционалдығын қамтамасыз ету үшін барлық қажетті керек-жарақтар болуы керек.  Жабдық жеткізу шартының әрекет ету мерзімі ішінде өндірістен, қолдаудан (пайдалану мерзімінің аяқталуы) жойылған немесе басқа жағдайға байланысты Тапсырыс берушіге жеткізу мүмкін болмаған жағдайда, Орындаушы мұндай Жабдықты баламалы ауыстыруды ұсынуға міндетті болады. оның құнын арттырмай немесе функционалдығын төмендетпей.  Бағдарламалық жасақтама немесе оның нұсқалары жеткізу шартының әрекет ету мерзімі ішінде өндірістен, қолдаудан (қолдану мерзімінің соңы) тоқтатылған немесе басқа жағдайға байланысты Тапсырыс берушіге жеткізу мүмкін болмаған жағдайда, Орындаушы баламалы ауыстыруды ұсынуға міндетті болады. мұндай Бағдарлама үшін оның құнын арттырмай және функционалдығын төмендетпей.  Берілген Жабдық Тапсырыс берушінің орнында құрастыру және іске қосу және орнату жұмыстарын жүргізу үшін қажетті барлық құрамдас бөліктермен (бекіткіштер, қуат көзі және жерге қосу кабельдері) жабдықталуы керек.  Жабдық және Бағдарламалық жасақтама шартқа қол қойылған күннен бастап 5 жұмыс күнінен кешіктірмей толық көлемде жеткізілуі тиіс.  Жабдықты жеткізу мекенжайына жеткізу, жабдықты түсіруді және тиеуді (тиегіштерді және қажет болған жағдайда арнайы техникалық құралдарды бере отырып) Орындаушы жүргізеді және оның есебінен жүзеге асырылады. Түсіру Тапсырыс беруші белгілеген үй-жайлар мен орында жүргізіледі.  Жүйенің модульдік құрылымы болуы және кемінде екі ішкі жүйеден тұруы керек:  10 Гбит/с дейінгі шабуылдарды басудың жалпы мүмкіндігімен кірістірілген режимде жұмыс істейтін DDoS шабуылдарын басу ішкі жүйелері (бірнеше құрылғылар мүмкін). DDoS шабуылын азайтудың ішкі жүйесі ақауларға төзімді жұмыс режимін қамтамасыз етуі керек.  Бақылау және талдаудың ішкі жүйелері  Сауда-саттыққа қатысушының ұсынысына енгізілген әрбір шабуылды азайту құрылғысы келесі талаптарға жауап беруі немесе одан асуы керек:   |  |  | | --- | --- | | Талап | Мағынасы | | Режимде шағылысқан шабуыл мөлшері (Гбит/с), | 10 | | Жүйемен қорғалған жалпы заңды трафик, кем емес (Гбит/с) | 5 | | Өңделген пакеттер саны (PPS), кем емес | 7,2 млн | | Максималды кідіріс енгізілді, артық емес | 60 мс | | Шабуыл векторындағы өзгерістерге жауап беру жылдамдығы, артық емес | 18 секунд | | Шабуылдардың барлық түрлерін анықтау және қорғау автоматты түрде жүзеге асырылуы керек. | Міндетті түрде | | Параметрлер шабуылсыз трафик параметрлерін есептеу негізінде қолмен де, автоматты түрде де жасалуы керек | Міндетті түрде | | Жүйе дұрыс емес пакеттерді (қате бақылау сомасымен, дұрыс емес тақырыптармен, толық емес немесе қайталанатын фрагменттермен, қысқа пакеттермен) блоктауы керек. | Міндетті түрде | | Қолдау көрсетілетін интерфейстер (бір құрылғыда) | 8x1G Copper Ethernet және 4x 10GE (SFP+) | | Қосымша қуат көзінің болуы | Міндетті түрде | | Бөлек басқару интерфейсінің болуы | Міндетті түрде | | Мөлдір режимде жұмыс істеу мүмкіндігі (L2 мөлдір) | Міндетті түрде | | IP режимінде жұмыс істеу мүмкіндігі (L3) | Міндетті түрде | | Негізгі жұмыс режимі: In-line | Міндетті түрде | | Бір бағытты да, екі бағытты да қозғалыс режимдерінде жұмыс істеу мүмкіндігі | Міндетті түрде | | Бір бағытты және екі жақты трафик еркін түрде араласқан кезде аралас режимде жұмыс істеу мүмкіндігі | Міндетті түрде | | Шабуылға жауап берудің әртүрлі нұсқаларының мүмкіндігі (пакеттерді блоктау және ақпараттық қауіпсіздік әкімшісіне хабарлау, тек ақпараттық қауіпсіздік әкімшісіне хабарлау). | Міндетті түрде | | IPv4 және IPv6 протокол стектерін толық қолдау | Міндетті түрде | | OSI моделінің (2-7) әртүрлі қабаттарына бір уақытта бағытталған көп векторлы DDoS шабуылдарынан қорғау | Міндетті түрде | | TCP тасқын шабуылдарынан қорғау (соның ішінде SYN, SYN-ASK, PUSH, FIN, RST, ASK су тасқыны, mirai тасқыны, TCP фрагменті тасқыны, қате TCP пакеттері арқылы жасалған тасқын) | Міндетті түрде | | TCP қосылымын су тасқынынан қорғау | Міндетті түрде | | ICMP су тасқынынан қорғау (жаңғырық сұрау, қол жетімсіз, көзді өшіру) | Міндетті түрде | | GRE туннельдерінің ішіндегі су тасқынынан қорғау | Міндетті түрде | | IGMP су тасқынынан қорғау | Міндетті түрде | | HTTP қосылымының тасқынынан қорғау (соның ішінде Java-скрипті, 302 қайта бағыттау және т. | Міндетті түрде | | HTTPS қосылымының тасқынынан қорғау (соның ішінде Java-скрипті, 302 қайта бағыттау және т. | Міндетті түрде | | Тек бірінші HTTPS сұрауының шифрын ашу мүмкіндігі | Міндетті түрде | | HTTPS трафигінің шифрын толық ашу мүмкіндігі | Міндетті түрде | | SMTP және FTP су тасқынынан қорғау | Міндетті түрде | | HTTP және FTP дөрекі күш шабуылдарынан қорғау | Міндетті түрде | | UDP су тасқынынан қорғау (соның ішінде кездейсоқ порт тасқыны, үлкен пакеттік су тасқыны, мирайдан туындаған су тасқыны) | Міндетті түрде | | Күшейту шабуылдарынан қорғау | Міндетті түрде | | DNS қорғауы, соның ішінде  қатал қорғаныс деп атаңыз  жалған бастапқы мекенжай  Кездейсоқ ішкі домендерге шабуыл  Күшейтудің рефлексиялық шабуылы  Сөздік шабуылдары және қатал күш шабуылдары | Міндетті түрде | | Қолмен өңдеу мүмкіндігі бар домендердің ақ тізімін автоматты түрде құрастыруға негізделген оң модель арқылы DNS қорғауы |  | | SIP су тасқынынан және SIP қатал күшінен қорғау | Міндетті түрде | | Дұрыс емес SIP пакеттерінің шабуылынан қорғау | Міндетті түрде | | Баяу шабуылдардан қорғау (Slow Loris, Slow Read, т.б.) | Міндетті түрде | | Пульсациялық (жарылу) шабуылдардан қорғау | Міндетті түрде | | SSL/TLS бағытталған шабуылдардан қорғау (қайта келіссөздер, қол алысу, су тасқынын қоса) | Міндетті түрде | | Трафиктің шифрын шешпей SSL шабуылдарынан қорғау (соның ішінде L7 қосылымының тасқыны, яғни SSL туннелі ішіндегі су тасқыны) | Міндетті түрде | | Белгісіз шабуылдардан қорғау (нөлдік күн), нақты уақытта шабуылдардың сипаттамаларын (қолтаңбаларын) автоматты түрде жасау | Міндетті түрде | | Нақты уақытта белгілі осалдықтардан қорғау (тұрақты және апаттық сипаттама жаңартулары) | Міндетті түрде | | Қолмен шабуылдардың сипаттамасын (қолтаңбаларын) жасау мүмкіндігі | Міндетті түрде | | Соңғы 24 сағатта бот желілеріне қатысқан хосттарды блоктау мүмкіндігі (қосымша лицензияларды пайдалану арқылы мүмкін) | Міндетті түрде | | Әкімшінің өз қорғау саясаттарын жасау және оларды жылдам өзгерту мүмкіндігін қамтамасыз ету мүмкіндігі. | Міндетті түрде | | Зиянды бағдарламалық құралдан (зиянды бағдарлама) қорғау | Міндетті түрде | | Қара және ақ тізімдерді жасау мүмкіндігі | Міндетті түрде | | Географиялық шабуылдардан қорғау (қосымша лицензиялармен мүмкін) | Міндетті түрде | | Белгілі бір көзден, алушыға дейін немесе протокол, қолданба, желі сегменті, физикалық порт, топ деңгейінде екеуінің тіркесімі (жылдамдықты шектеу, қосылымды шектеу) арқылы трафик жылдамдығын шектеу. | Міндетті түрде | | Зиянды/зиянды трафикті нақты уақытта анықтау үшін хаттама аномалиясын анықтау | Міндетті түрде | | Портты тік және көлденең сканерлеуден қорғау. | Міндетті түрде | | L3, L4, L7 ақпараты негізінде пакеттерді фильтрлеу мүмкіндігі. | Міндетті түрде | | Үшінші тарап жүйелерімен өзара іс-қимылді ұйымдастыруға арналған API интерфейсін қолдау. | Міндетті түрде |   DDoS қорғау құрылғыларын басқару жүйесінің функционалдық және техникалық талаптары  Жүйені аппараттық шешім ретінде немесе VMware немесе KVM (кез келген) виртуалдандыру ортасында виртуалды машиналар ретінде орналастырылған бағдарламалық құрал ретінде орналастыруға болады.  Жүйелік бағдарламалық жасақтаманың бір данасы кемінде 2 аппараттық немесе виртуалды құрылғыны бақылауды және басқаруды қамтамасыз етуі керек.  Басқару жүйесінің интерфейсіне кіру веб-браузер арқылы болуы керек.  Жүйе рөлдер мен пайдаланушы топтары негізінде жүйеге пайдаланушының қол жеткізуін саралауды қолдауы керек, соның ішінде құрылғыларға шектеулі қол жетімділікпен Active Directory-мен біріктіру арқылы.  Ағымдағы және өткен шабуылдар туралы ақпаратты визуализациялау;  Шабуыл статистикасы бойынша есептерді жасау және оларды электрондық почта арқылы автоматты түрде тарату арқылы CSV, XML, PDF форматтарында жүктеп алу.  Жүйе DDoS қорғау құрылғыларын басқару тұрғысынан келесі функцияларды орындауы керек:  CPU пайдалану сияқты құрылғы ақпаратын көрсету;  Құрылғылардың орнатылған бағдарламалық жасақтамасының нұсқасы және олардың орталықтандырылған жаңартылуы туралы ақпаратты көрсету;  Құрылғы лицензиясын басқару;  Құрылғы конфигурация файлдарының сақтық көшірмелерін жасау;  Жүйе DDoS қорғау құрылғыларын бақылау тұрғысынан келесі функцияларды орындауы керек:  Негізгі көрсеткіштердің жай-күйін мониторингтеу және шекті мәндерден асып кеткен жағдайда ескерту;  Есепке алу жазбаларына және өзгерістер қашан енгізілгеніне бақылау жасау мүмкіндігімен конфигурация өзгерістерін мониторингтеу.  **2.5.18 Веб-қосымшалардың трафигін фильтрлеу жүйесіне қойылатын талаптар** Жабдыққа қойылатын талаптар Жүктемені бөлу жүйесі (ADC – қосымшаларды жеткізу контроллері) және веб-қосымшалар трафигін қорғау (WAF) Тапсырыс берушінің желілік инфрақұрылымында орналастыруға арналған.  Жүктемені бөлу жүйесін енгізудің негізгі мақсаты (ADC - қосымшаларды жеткізу контроллері) және шабуылдардан қорғауқолданба деңгейі: - TLS шифрлаудың 1.0/1.1/1.2/1.3 нұсқалары арқылы шифрланған трафикті шешу; - веб-трафикті оңтайландыру; - Web-қосымшаларды қолданбалы деңгейдегі шабуылдардан қорғау, мысалы: OWASP TOP-10; - қолданбалы серверлер және т.б. сияқты сервистік құрылымдардың құрамдас бөліктері арасындағы жүктемені бөлу; - Клиенттің жалпы IP мекенжайын реттелетін http тақырыбы өрісінде жазу.  **Өткізу қабілеті және өнімділік**  Ұсынылған шешім виртуалды бағдарламалық кешен түрінде жеткізілуі және кем дегенде 1 Гбит/с жалпы өткізу қабілеті бар HTTP/HTTP трафигін өңдеуді қамтамасыз етуі керек.  Жеткізілген лицензиялар бір жылдық техникалық қолдау құнын қамтитын жаңартылатын жылдық жазылым ретінде ұсынылуы керек. Ең аз жазылу мерзімі - 1 жыл.  Ұсынылған бағдарламалық-виртуалды кешен VmWare vSphere, KVM, Microsoft Hyper-V сияқты жалпы виртуалдандыру платформаларында орналастыру мүмкіндігін қолдауы керек.  Бағдарламалық-виртуалды кешендердің көшірмелерінің жалпы саны кемінде 8 дана болуы керек.  TLS 1.0/1.1/1.2/1.3 хаттамаларының аппараттық шифрлау өңдеуін қолдау;  Әрбір физикалық құрылғыдағы артық қуат көздері.  Виртуалды машиналарды пайдалану кезінде үлгі алу.  Бағдарламалық және аппараттық құралдарға қойылатын функционалдық талаптар.  Протоколды қолдау (қосымша лицензияларсыз): IEEE 802.3ad (LACP) сілтемелерді біріктіру; OSPFv2/3, BGP; GSLB.  Шешім IPv4, IPv6 желілеріндегі жұмысты қолдауы керек  Егер пакеттер теңгерімдеуге арналмаған болса, Layer2 және Layer3 Forwarding қолдауы;  STP хаттамасы н қолдау: MST, RSTP  Сілтемелерді біріктіру хаттамаларын қолдау (кемінде 4 порт)  Статикалық жинақтау  Динамикалық біріктіру (LACP)  VLAN технологиясын қолдау (802.1q, әр құрылғыға кемінде 1000)  Ақауларға төзімділік:  VRRP хаттамасын қолдау  Сыртқы жабдықты басқару (OOBM) үшін кем дегенде бір тәуелсіз интерфейстің болуы;  Басқару интерфейсі мен деректер интерфейстері арасындағы трафикті жіберудің техникалық мүмкін еместігі.  Жұмыс режимдерін қолдау: Кері прокси; Мөлдір прокси сервер.  Кластердегі элементтердің қолдау көрсетілетін саны - кемінде 2 құрылғы. Кластер құрамдастарының кез келгені тұтастай кластердің функционалдығын жоғалтпай техникалық қызмет көрсету режиміне кіруі керек.  Белсенді күту режимінде ақауларға төзімділікті қолдау; Белсенді-белсенді режимде ақауларға төзімділікті қолдау (кемінде 8 құрылғы); Құрылғылар арасында жүктемені тапсырма бойынша қолмен тасымалдау мүмкіндігімен белсенді күту режимінде ақауларға төзімділікті қолдау.  Белсенді/күту режимі арасында ауысу кезінде сеанс күйін сақтауды қолдау (күй-жұмыс істемеуі);  Географиялық бөлінген GSLB кластерлік жүйелерін құру мүмкіндігі.  SSL сертификатын басқаруға қолдау көрсету.  Сервер атауын анықтауға (SNI) байланысты әртүрлі сертификаттарды қамтамасыз етуді қолдау.  HTTP трафигін манипуляциялау үшін құрылғыдағы тоқтатуды ескере отырып, SSL трафигін теңестіру мүмкіндігі.  TLS 1.0/1.1/1.2/1.3 хаттамаларын қолдау; TLS 1.0 және 1.1 хаттамаларын толығымен өшіру мүмкіндігі;  Жеке таңдалған шифрларды пайдалану мүмкіндігі;  Сыртқы және ішкі интерфейстерде бір уақытта әртүрлі шифрлау профильдерін қолдайды (Front End & Back End);  TLS қайта келіссөздер мүмкіндігін өшіру мүмкіндігі.  Денсаулықты тексеру арқылы кемінде 4000 нақты серверді теңестіру мүмкін болуы керек.  Аппараттық ресурстарды (CPU, RAM және т.б.) және физикалық порттарды бөлу арқылы виртуалдандыруды қолдау;  Рөлдік басқару үлгісінің болуы.  Сыртқы NTP көздерінен контроллерлерде уақытты синхрондау  Ақауларды жою үшін tcpdump утилитасына ұқсас құрылғылар арқылы өтетін трафикті талдауға арналған кірістірілген механизмдерге қолдау көрсету қажет.  Функционалды теңестіруге қойылатын талаптар  Серверлер мен қосымшалардың өнімділігі мен қолжетімділігін тексеру мүмкіндігі:  Алдын ала орнатылған L3 тексерулерінің (ICMP) болуы;  Алдын ала орнатылған L4 тексерулерінің болуы (TCP/UDP портын тексеру);  Алдын ала орнатылған L7 қолданба деңгейін тексерулердің болуы.  Жүктемені бөлу механизмдерін қолдау: Round Robin; бастапқы/тағайындалған мекенжай бойынша; қолданба мазмұнына негізделген; өтінімге жауап беру уақытына байланысты; өңделген трафик көлеміне негізделген; қосылымдар санына қарай; сервердің салыстырмалы салмағының күрделі таралуына (екінші реттік ерекшелігіне) негізделген; тұрақты, үзіліссіз L4 сеансын сақтау (табандылық);  Бір серверге сеанс бағыты (жабысқақтығы): IP мекенжайы немесе IP+Port негізінде; cookie негізіндегі; SSL сеансының идентификаторына негізделген; HTTP пакет тақырыбының деректеріне негізделген; XML тегіндегі деректерге негізделген.  L7 деңгейінде өзгертуге қолдау көрсету, соның ішінде пайдаланушы сценарийлерін пайдалану.  **Оңтайландырудың функционалдығына қойылатын талаптар**  Веб-ресурстарды (Web Performance Optimization (WPO)) жеделдетуге қолдау көрсету: Тиісті оңтайландырумен браузер/мобильді браузер платформасын анықтау; Платформалардағы жүктемені азайту үшін деректерді кэштеу; Кескінді оңтайландыру, оның ішінде кескінді прогрессивті өңдеу, қысу және біріктіру; CSS, Java сценарийлері мен кескіндері үшін ресурстарды біріктіру;  Модификация: JavaScript және CSS.  **Веб-қосымшаларды (WAF) қорғау функционалдығына қойылатын талаптар**  Жұмыс режимдерін қолдау:  Монитор режимі (out-of-path/заңсыз сұрау салулар туралы хабарландыру арқылы айналы трафикті қарау);  Мөлдір прокси режимі (Transparent Proxy). Бұл режимде жүйе трафикті өңдеудің келесі нұсқаларын қолдауы керек: заңсыз сұрау салуларды блоктау; өту және заңсыз сұраулар туралы хабарлау.  Толық прокси режимі (Full Proxy). Бұл режимде жүйе трафикті өңдеудің келесі опцияларын қолдауы керек: заңсыз сұрау салуларды блоктау; өту және заңсыз сұраулар туралы хабарлау.  Белгілі шабуылдарды блоктайтын жағымсыз қауіпсіздік моделі де, қорғалатын трафиктің қалыпты қолданылуын зерттеуге және қалыптан тыс әрекеттерді анықтауға негізделген оң модель де сақталуы керек.  Жүйе қолдауды, тануды және HTTP хаттамасының және Websocket хаттамасының стандарттарына сәйкестігін тексеруді қамтамасыз етуі керек;  Өз тақырыптарыңызды қосу мүмкіндігін қоса алғанда, жалпы HTTP хаттамасының тақырыптарын қолдау;  HTTP тақырып өрістерінің толып кетуінен қорғау;  Жүйе қосымшаларды OWASP Top 10 осалдықтарынан қорғауы керек;  Жүйе Session hijacking, Buffer overflows, Forceful browsing, Hidden fields manipulation, Remote File Inclusion, Directory/Path traversal, XXE Injection, Request Header Filtering, Request Method Filtering, Response Header Filtering, SQL Injection, NoSQL Injection қоса алғанда, әдеттегі шабуылдарға қарсы мақсатты іс-қимыл функционалын қолдауы тиіс.  Жүйе алдын ала белгіленген метрикадан асып кеткенде веб-ресурсқа қол жеткізуді шектеу мүмкіндігімен автоматтандырылған жаппай шабуылдардан және параллель шабуылдардан қорғауды қамтамасыз етуі керек, соның ішінде:  Қолданба деңгейінде қызмет көрсетуден бас тарту шабуылдарынан (DoS, DDoS) қорғау;  Веб-қосымшалар аккаунтарына (Brute Force) құпия сөздерді қолдануға әрекеттенетін сұрау салуларды анықтау және блоктау;  Жүйе баяу шабуылдардан (Slow Loris, Slow Read, т.б.) қорғауды қамтамасыз етуі керек.  Жүйе олардың әрекеттерін талдау негізінде сыртқы периметрлік қорғаныс құрылғыларында (мысалы, DefensePro) шабуылдаушыларды блоктауды қамтамасыз етуі керек. «Заңсыз әрекет» ұпайларын есептеу және блоктау уақыты шабуылдардың ауырлық деңгейі мен санына байланысты болуы керек.  Жүйе шабуылдаушы NAT немесе проксидің артында болса да, анықталған шекті мәндердің нәтижелері бойынша фильтрлеу үшін әрбір анықталған шабуыл көзі үшін бағалау ұпайларын есептеуі керек. Бір NAT немесе проксидің артында орналасқан заңды пайдаланушыларды блоктауға болмайды;  Жүйе көзге тағайындалған тәуекелді индикаторлармен тыйым салынған URL/URI мекенжайларына немесе қолданба файлдарына сұрауларды блоктауы керек;  Жүйе бір-бірінен толығымен тәуелсіз қорғау саясаттарын пайдалана отырып, бір жарияланған IP мекенжайында бірнеше хосттарды (веб-қосымшаларды) бір уақытта қорғау мүмкіндігін қамтамасыз етуі керек (яғни, бір саясатқа өзгертулер бір IP мекенжайында орналасқан басқаларына әсер етпейді).  Жүйе репутация тізімдерінің тұрақты, теңшелетін жаңартуларын қамтамасыз ете отырып, ықтимал сенімсіз мекенжайлардан қорғау механизмдерін қамтамасыз етуі керек;  Жүйе белгілі бір елдерге қатысты географиялық орынға негізделген мекенжайларды блоктау механизмдерін қамтамасыз етуі керек  Жүйе сервер қателерін ұстауға және реттелетін қызмет беттерін көрсетуге арналған функционалдылықты қамтуы керек;  Жүйе құпия ақпаратты (несие картасының нөмірлері, телефон нөмірлері және төлқұжат деректері) жария етуден қорғауды қамтамасыз етуі керек.  Жүйе бір-бірінен толығымен тәуелсіз қорғау саясаттарын (яғни, бір саясаттағы өзгерістер сол IP-мекенжайындағы қалғандарына әсер етпейді) пайдалана отырып, сол жарияланған IP мекенжайындағы веб-қосымшалардың (хосттардың) кез келген саны үшін интеллектуалды автоматтандырылған оқыту механизмдерін қолдануды/іске қосуды қамтамасыз етуі керек.  Жүйе автоматтандырылған оқытудың интеллектуалды механизмдерін, ауытқуларды анықтауды және заңсыз белсенділіктерді блоктауды қолдануды қамтамасыз етуі тиіс, оның ішінде:  Әрбір қорғалатын веб-бағдарлама үшін жеке-жеке бастапқы оқытуды аяқтағаннан кейін қорғау режимін қолмен қосу немесе өшіру мүмкіндігі;  Әрбір веб-бағдарлама үшін жеке-жеке қорғаудың модуліне/түріне бастапқы оқыту аяқталғаннан кейін қорғау режимін қолмен қосу немесе өшіру мүмкіндігі;  Тестілеу (staging) жағдайында оқыту және алынған саясатты өнімді жағдайға көшіру мүмкіндігі.  Жүйе қосымшаның әрбір/кез келген деңгейі үшін әртүрлі саясаттарды жасау мүмкіндігін ұсынуы тиіс (URI);  Жүйеде автоматты түрде қолданылатын сайт пен одан шығатын есептерді өңдеу мүмкіндігі құрылымы өзгерген кезде сыртқы қауіпсіздік сканерін автоматты түрде іске қосу функционалы болуы тиіс.  Жүйенің HTTP тақырыбының еркін түрдегі өрісінен көздің нақты IP-мекенжайларын шығарып алу мүмкіндігі болуы керек;  Жүйе анықталған және блокталған қауіптердің егжей-тегжейлі журналдарын жүргізуі керек;  Жүйе L4 немесе L7 (мысалы, XFF) ақпаратына негізделген, блокталуы тиіс, нақты шабуылдаушылар туралы ақпаратты қамтитын хабар алмасу мүмкіндіктерін қамтамасыз етуі керек;  Жүйе қателер туралы пайдаланушылар беттерін жасауды қолдауы керек. Бұл бетті қорғау құрылғысының өзінде де, сыртқы веб-серверде де орналастыру мүмкіндігі болуы керек;  **Мониторингтеу және басқару**  HTTPS, SSH хаттамалары арқылы басқаруды қолдау; telnet  TACACS+, RADIUS, LDAP хаттамалары арқылы аутентификацияны қолдау;  Қауіпсіз емес Telnet & HTTP хаттамаларын өшіру мүмкіндігін қолдау (бар болса);  Басқару интерфейстеріндегі кіру тізімдерін қолдау;  SNMP v3 хаттамалары арқылы кеңейтілген статистиканы алу мүмкіндігін қолдау;  Syslog, SNMP Traps көмегімен хабарландыруларды орнатуды қолдау;  Орталықтандырылған мониторингтеу және басқару үшін бағдарламалық жасақтаманың болуы.  Әр түрлі SNMP хабарлама жинаушыларына SNMP ескертулерін (SNMP тұзағы) жіберудің икемді баптауларының мүмкіндігі.  RESTful API қолданбалы интерфейсінің қолдауы.  Әкімшілендірудің рөлдік моделін қолдау  Орталықтандырылған мониторингтеу жүйесі (жеке лицензия болған кезде мүмкін болады) келесілерге қолдау көрсетуі керек:  Реттелетін есептерді жасауға арналған кіріктірілген утилиталар.  Пайдаланушы қосымшаларының жұмыс өнімділігі туралы есептерді ұсыну: ЦОД-тағы кідіріс, желілік кешігу, клиент жағындағы кідіріс, соның ішінде клиент жағында пайдаланылатын браузерге байланысты.  Кірістірілген мониторингтеу құралдары кемінде 90 күн бойы барлық көрсеткіштерді көруге, сондай-ақ барлық құрылғылар үшін тарихи есептерді беруге мүмкіндік беруі керек.  Жүйеде әдеттегі операцияларды автоматтандыруға қолдау көрсету керек.  конфигурацияны сақтау және қалпына келтіру;  кесте бойынша конфигурация өзгерістері;  сертификаттардың жарамдылық мерзімі туралы ескертулер  барлық құрылғылардың конфигурацияларының дұрыс қолданылуын және құрылғылардың тұрақты жадында сақталуын тексеру;  пайдаланылатын SSL саясаттарының ұйым саясаттарына сәйкестігін тексеру.  Әрбір құрылғы үшін жүйеде мониторингтеу функциясы болуы керек: интерфейстердің статусы; процессорды, жадтарды, дискілік кеңістікті пайдалану жүктемелері; кластердің жай-күйі;  Жүйенің әрбір құрылғы үшін апаттардың тізімін көрсете алатын мүмкіндігі болуы керек;  Жүйенің барлық жүйе пайдаланушыларының іс-әрекеттерін тексере алатын мүмкіндігі болуы керек.    **2.6 Есеп беру құжаттарына қойылатын талаптар**  Орындаушы келесілерге міндеттенеді:   * Шарт жасалғаннан кейін 10 жұмыс күні ішінде Тапсырыс берушіге бекітуге береді, ал Тапсырыс беруші өз кезегінде ұсынылғаннан кейін 5 күн ішінде мәтіндік, кестелік және графикалық (диаграммалар, графиктер) бар тоқсандық жиынтық есептің нысанын келіседі. Шартты орындаудың негізгі көрсеткіштері туралы ақпарат және дәл: * есепті кезеңдегі сұраныстар мен оқиғалар бойынша статистикалық деректер; * ақпараттық қауіпсіздік инфрақұрылымының жай-күйін талдау; * проблемалық мәселелердің тізбесі және оларды шешу және ақпараттық қауіпсіздік инфрақұрылымының жұмысын жақсарту бойынша ұсынымдар; * Қызметтер көрсетуге жауапты мамандардың өзекті байланыс деректері. * Тапсырыс берушінің сұрау салуы бойынша жылына бір реттен жиі емес сүйемелденетін қорғау құралдары жөніндегі, ақпараттық қауіпсіздік оқиғалары және тіркелген ақпараттық қауіпсіздік инциденттері туралы ақпараттың негізінде проблемалық мәселелер тізбесін, ақпараттық қауіпсіздік инфрақұрылымының жұмысын жақсарту бойынша талдаулар мен және ұсыныстарды қоса алғанда, ақпараттық қауіпсіздік инфрақұрылымының жай-күйін талдайтын аналитикалық есепті ұсынуға; * тоқсан сайын және Тапсырыс берушінің сұрау салуы бойынша, бірақ айына бір реттен жиі емес Тапсырыс берушіге Қызметтер/Сервис көрсетуге жауапты мамандардың жиынтық есебін және өзекті байланыс деректерін ұсыну.  Сервиске қойылатын талаптар Жобаны іске асыру барысында сервистік қызметтерді енгізу бойынша келесі әрекеттерді орындау қажет:   * барлық жүйелер Тапсырыс берушінің аумағында орналасуы керек; * берілген қауіпсіздік құралдарына лицензияларды орнату және іске қосу жүзеге асырылды; * келесілерден тұратын жобалық құжаттаманы қалыптастыру:   ○ түсіндірме жазба: түсіндірме жазбада әр сервистің процесін, оның іргелес жүйелермен интеграциясын сипаттайтын ақпарат болуы керек, физикалық (желілік, жабдықты шкафтарға орналастыру, кабельдік журнал), логикалық, құрылымдық және басқа өзара іс-қимыл схемалары болуы керек, түсіндірме жазбада әр сервистің енгізілген функционалы сипатталуы керек;   * сервис әкімшісінің нұсқаулығы – сервис әкімшілігі механизмдерінің сипаттамасын, оның баптауларының өзгерістерін, қызметті қайта конфигурациялауды, сервистің бағдарламалық жасақтамасын немесе оның құрамдас бөліктерінің жаңартылуын, белсенді желілік, есептеу жабдықтарын немесе сайттағы Тапсырыс беруші алаңындағы деректерін сақтау жүйелерін орнатуды көздейтін сервистер үшін регламенттік іс-шараларды жүргізуді қамтуы тиіс – сондай-ақ монтаждау және орнату жөніндегі нұсқаулық болуы тиіс; * сервисті пайдаланушы нұсқаулығы – сервисті пайдаланушы нұсқаулығы сервисті қолданатын пайдаланушының типтік тапсырмаларының сипаттамасын, типтік проблемалардың сипаттамасын және оларды шешу тәсілдерін, жүйе интерфейсінің сипаттамасын қамтуы тиіс; * PMI - сынақтар бағдарламасы мен әдістемесі техникалық ерекшеліктерге сәйкес сынақтар жинағын қамтуы керек; * Жабдықтарды орнату қызметтері: * тіреуде жабдықты орнату орнын белгілеу; * қоректендіру көздеріне, байланыс желілеріне және технологиялық LAN сегменттеріне қосылуларды келісу; * жабдықты тіреулерге орнату және қоректендіру көздеріне қосу; * физикалық схемалар мен кабельдік журналдар бойынша жабдықты коммутациялау; * Жүйені баптау жөніндегі қызметтер: * инфрақұрылымның қажетті нүктелерінде серверлік жабдықты және фильтрлеу жабдығын орнату, қолданыстағы ақпараттық жүйеге АҚБЖ қызметтерінің әсерін жою мақсатында Тапсырыс берушінің өкілдерімен бірге барлық жүйелердің байланыста болуын және дұрыс жұмыс істеуіне тексеру жүргізу; * техникалық ерекшеліктерге және ақпараттық инфрақұрылымның және Тапсырыс берушінің LAN желісінің өзекті мүмкіндіктеріне сәйкес қажетті функционалды қамтамасыз ету үшін барлық сервистерді орнату. Тапсырыс берушінің алаңдарында қажетті интеграциялық қуаттардың болмауына байланысты қажетті функционалдылықты баптау мүмкін болмаса, осы тармақ бойынша қызметтер мүмкіндігінше тезірек орындалады; * агенттердің таратылу тапсырмаларын іске қосу (өз тарату жүйесі бар агент қызметтері үшін), орталықтандырылған AD саясаттары арқылы орнату үшін агент дистирбутивтерін Тапсырыс берушінің пайдалану қызметінің жауапты қызметкерлеріне жіберу. Агенттік бағдарламалық жасақтаманы таратудың оңтайлы әдісін таңдау бойынша консультациялар, бағдарламалық жасақтаманы орнатуды қамтамасыз ету үшін желілік инфрақұрылымның, AD инфрақұрылымының және жұмыс станциясының параметрлерінің дұрыс баптаулары бойынша Тапсырыс беруші өкілдерімен кеңесу; * сервистерді олардың дұрыс жұмыс істеуі мен алынуын қамтамасыз ету үшін қолданыстағы жүйелермен интеграциялау; * ақпараттық қауіпсіздіктің ахуалдық орталығының қызметін қолданыстағы АҚБЖ жүйелерімен интеграциялау, логтар мен оқиғалар журналдарын, деректер базасының деректерін экспорттауды баптау, интеграциялау (сервиске байланысты); * сервистерді пайдаланушыларды басқарудың рөлдік үлгісін құру, Тапсырыс беруші мен Орындаушы қызметкерлері арасында жауапкершілік аймақтарын бөлу, шамадан көп артықшылықтар алуды болдырмау үшін жүйенің әрбір әкімшісі мен пайдаланушысына жүйелерге тек ең аз қажетті қолжетімділік құқықтарын беру.   **3. Жауапкершілік аймақтарын бөлу.**  Осы техникалық ерекшелікке сәйкес қызметтер көрсету кезінде 7-кестеге сәйкес Орындаушы мен Тапсырыс берушінің келесі жауапкершілік аймақтары белгіленеді.  7-кесте. Жауапкершілік аймақтарын бөлу:   | **№** | **Параметр** | Тапсырыс беруші | Орындаушы | | --- | --- | --- | --- | | 1.1 | Тіркелген және Мониторингтеу аймағына кіретін Клиенттердің инфрақұрылымдық элементтеріне қатысты ақпараттық қауіпсіздік оқиғаларын мониторингтеу және талдау (инциденттерге әрекет ету бойынша ұсыныстар беруді қоса алғанда). |  | + | | 1.2 | Тіркелген немесе Мониторингтеу аймағына кірмейтін Клиенттердің инфрақұрылымдық элементтеріне қатысты ақпараттық қауіпсіздік оқиғаларын мониторингтеу және талдау. | + |  | | 1.3 | Тапсырыс берушінің алаңында да, Орындаушының алаңында да орнатылған ақпараттық қауіпсіздік оқиғаларын басқарудың кіші жүйесінің құрамдас бөліктерінің жай-күйін мониторингтеу |  | + | | 1.4 | Ақпараттық қауіпсіздік оқиғаларын басқарудың кіші жүйесінің дұрыс жұмыс істеуін қамтамасыз ету |  | + | | 1.5 | Логтарды жіберу үшін көздерде агенттерді орнату | + |  | | 1.6. | Орындаушының ұсынымдарына сәйкес оқиғалардың/ағындардың коллекторларын және ақпараттық қауіпсіздік оқиғаларын басқарудың кіші жүйесінің басқа инфрақұрылымдық элементтерін орналастыру үшін қажетті технологиялық мүмкіндіктерді қамтамасыз ету. Қателерге төзімділікті және тиісті инфрақұрылымның қолжетімділігін қолдау |  | + | | 1.7 | Көздерден коллекторларға желі ағындарын бағыттау | + |  | | 1.8 | Орындаушы ұсынған ұсынымдарға сәйкес ақпараттық қауіпсіздік инциденттеріне ден қою, оларды оқшаулау, салдарын жою және қалыпты жұмысты қалпына келтіру | + |  | | 1.9 | Тапсырыс беруші мен Орындаушы алаңдары арасындағы қауіпсіз ақпарат беру арналарының функционалдығын қамтамасыз ету | + | + | | 1.10 | Ақпараттық қауіпсіздік орталығының ұсынымдарын орындау және ақпараттық қауіпсіздік инциденттеріне дер кезінде ден қою | + |  | | 1.11 | Мониторингтеу аймағына енгізілген серверлік, коммуникациялық және компьютерлік техниканың, сондай-ақ ақпараттық жүйелердің өзекті тізбесін ұсыну | + |  | | 1.12 | Қайталанатын инциденттің туындау ықтималдығын жою мақсатында Орындаушының ұсынымдарын қолдану | + |  | | 1.13 | Мониторингтеу аймағындағы барлық өзгерістер туралы жедел ақпарат ұсыну. | + |  | | 1.14 | Көздерді мониторингтеу жүйесіне қосу (желілік байланысты қамтамасыз ету, көздерді мониторингтеу жүйесіне қосу жөніндегі нұсқаулықтардың тармақтарын орындау, агенттерді орнату) | + |  | | 1.15 | Мониторингтеу жүйесіне көздерді қосу бойынша нұсқаулықтар беру, ақпараттық қауіпсіздік оқиғаларының дұрыс келіп түсуін тексеру. |  | + | | 1.16 | Мүкәммалдық түгендеу саясатын баптау | + |  | | 1.17 | Мүкәммалдық түгендеу/интеграциялау үшін есептік жазбаларды ұсыну | + |  | | 1.18 | Сыртқы жүйелермен интеграцияны баптау |  | + | | 1.19 | Коллекторлардың архитектурасын баптау |  | + | | 1.20 | Атрибуттарды тағайындау саясаттарын баптау | + |  | | 1.21 | Пайдаланушыларды қосу | + |  | | 1.22 | Қол жеткізу деңгейлерін/пайдаланушы рөлдерін баптау |  | + | | 1.23 | Осалдықтар мен тәуекелдерді басқару | + |  | | 1.24 | Ден қою сценарийлерін баптау | + | + | | 1.25 | Инциденттер баптауларын басқару |  | + | | Желілік периметрді қорғау жүйесі | | | | | 2.1. | ПАК NGFW бағдарламалық жасақтамасын орнату және жаңарту, қауіптердің деректер базасы мен жабдық сигнатураларын жаңарту, жұмыс қабілеттілігін мониторингтеу. |  | + | | 2.2 | Электрондық почта, телефон, қашықтан қол жеткізу құралдары арқылы конфигурациялар мен қауіпсіздік ережелерін баптау, оңтайландыру, NGFW ПАК желілік өзара іс-қимыл құралдары бойынша кеңестер беру |  | + | | 2.3. | Жүйеге қол жеткізуді және Тапсырыс берушінің тиісті бөлімшелерімен өзара іс-қимылды ұйымдастыру, серверлік үй-жайларды беру, инфрақұрылымға қажетті құқықтарды ұсыну (шоттарды немесе басқа жазбаларды құру). | + |  | | 2.4. | Қағидаларды, саясаттарды және қауіпсіздік профильдерін әзірлеу және баптау, маршруттау және желіні сегменттеу, веб-фильтрлеу ережелері, VPN топтары және қол жеткізу ережелері, басып кіруді блоктау ережелері, NGFW ПАК желісінің және жүйе параметрлерінің конфигурациялары. | + |  | | Почта трафигін фильтрлеу жүйесі | | | | | 3.1 | ОЖ-ны, сондай-ақ серверлерде KSMG бағдарламалық пакетін орнату және баптау. Жүйенің және оның барлық компоненттерінің дұрыс жұмыс істеуін қамтамасыз ету |  | + | | 3.2 | Почта трафигін фильтрлеу ережелерін орнату және енгізу |  | + | | 3.3 | Тапсырыс берушінің бастамасы бойынша фильтрлеу ережелерін өзгерту |  | + | | 3.4 | Жүйені табу оқиғалары бойынша есеп жасау |  | + | | 3.5 | Оқиғалардың SIEM жүйесіне жіберілуін баптау |  | + | | 3.6 | Кабельдік байланыс желілерін монтаждау және платформа серверлері үшін Тапсырыс берушінің аумағында маршруттауды баптау | + |  | | Вирусқа қарсы қорғау жүйесі | | | | | 4.1 | ОЖ-ны орнату және баптау, сондай-ақ серверлердегі антивирустық қорғау жүйесіне арналған Әкімшілендіру орталығы бағдарламалық кешенін орнату.  Жүйенің және оның барлық компоненттерінің дұрыс жұмыс істеуін қамтамасыз ету |  | + | | 4.2 | best practice тәжірибеге сәйкес құрылғылардың барлық түрлері үшін қауіпсіздік саясаттарын орнату |  | + | | 4.3 | Тапсырыс берушінің бастамасы бойынша қауіпсіздік саясатына өзгерістер енгізу | + |  | | 4.4 | Вирусқа қарсы бағдарламалық жасақтаманы орнату немесе баптау кезінде Тапсырыс беруші құрылғыларымен жергілікті өзара іс-қимылды талап ететін мәселелерді шешу. | + |  | | 4.5 | Тапсырыс беруші құрылғыларында антивирустық бағдарламалық жасақтаманы орнату немесе баптау және қауіпсіздік саясаттарын баптау бойынша техникалық қолдау көрсету |  | + | | 4.6 | Соңғы нүктелерде антивирустық бағдарламалық жасақтаманы орнату | + |  | | Осалдықты сканерлеу жүйесі | | | | | 5.1 | Мақсатты түйін мен осалдық сканері арасындағы желі қосылымын қамтамасыз ету | + |  | | 5.2 | Сканерлеу үшін мақсатты түйінді баптау. | + |  | | 5.3 | Мақсатты түйіндерді сканерлеу, сканерлеу профильдерін орнату |  | + | | 5.4 | Есептерді қалыптастыру, есептерді жіберу, есеп беруден жалған оң осалдықтарды алып тастау |  | + | | 5.5 | Сканерлеу процесі кезінде табылған осалдықтарды өңдеу және жою | + |  | | 5.6 | Осалдықтарды сканерлеу жүйесінің жұмысқа қабілеттілігін сақтау, жаңарту және резервтік көшіру |  | + | |

**Ақпараттық қауіпсіздік**

**қызметінің бастығы О.Жүнісбеков**

Кесте 2

**Әлеуетті өнім берушіге қойылатын талаптар**

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Талап** | **Растау** |
|  | Әлеуетті өнім берушінің соңғы 5 (бес) жыл ішінде, сатып алынатын біртекті жұмыстар, көрсетілетін қызметтер нарығында немесе белгілі бір салада жұмыс тәжірибесінің болуын көздейтін біліктілік талаптары | - |
|  | Әлеуетті өнім берушіде растайтын құжаттарды ұсына отырып, жабдықтардың, техниканың (техникалық құрылғылардың), ғимараттардың (құрылыстардың), үй-жайлардың болуы туралы талаптар | - |
|  | Әлеуетті өнім берушілердің тендерлік өтінімдерді ашу күніне дейін сатып алынатын тауарлардың үлгілерін ұсынуы туралы талап | - |
|  | БҚҚ-да айқындалған әлеуетті өнім берушілердің біліктілігіне қойылатын талаптар | - |
|  | Тиісті лицензияны (лицензияларды) және өзге де рұқсат құжаттарын, сондай-ақ Қазақстан Республикасының заңнамасына сәйкес рұқсат беруге(лицензиялауға) жататын қызмет түрлерін(кіші түрлерін) көрсете отырып, Қазақстан Республикасының Рұқсаттар және хабарламалар туралы заңнамасына сәйкес берілген рұқсатты (лицензияны) беру туралы талап.  Қазақстан Республикасының заңнамасына сәйкес айқындалатын құрылыс объектілерінің жауапкершілік деңгейі туралы ақпарат. | Әлеуетті өнім беруші конкурсқа қатысуға өтінім шеңберінде «Рұқсаттар және хабарламалар туралы» Қазақстан Республикасының заңнамасына сәйкес берілген рұқсаттың (лицензияның) электрондық көшірмесін немесе электрондық құжат немесе электрондық көшірме форматындағы электрондық рұқсат (лицензиялау) жүйесін пайдалана отырып, рұқсатты (лицензияны) берген мемлекеттік органның ресми интернет көзіне (веб-сайтына) сілтемесі бар әлеуетті өнім беруші: қызмет көрсетуге лицензия ақпараттың шығуының техникалық арналарын және арнайы техникалық құралдарды анықтау; жедел-іздестіру іс-шараларын жүргізуге арналған. |