ТЕХНИКАЛЫҚ СИПАТТАМА

1047432 сатып алу бойынша
Төмендету баға ұсыныстарын сұрату тәсілімен

Лот № 1 (96-1 У, 3815155) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: «Karabatan Utility Solutions» жауапкершілігі шектеулі серіктестік

Ұйымдастырушы: «Karabatan Utility Solutions» жауапкершілігі шектеулі серіктестік

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	96-1 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензиялар беру жөніндегі қызметтер
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Атырау облысы, Атырау Қ.Ә., Атырау қ., трасса Атырау-Доссор, строение 295/2
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 15 жұмыс күніішінде
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

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

- Бағдарламалық қамтамасыз ету кез келген конфигурациядағы және күрделіліктегі желілердегі жұмысты қолдауы тиіс.
- Ұсыну 25 (жиырма бес) бағдарламалық қамтамасыз етуді пайдалану құқығына лицензиялар.
- Бағдарламалық қамтамасыз ету агенттердің серверге Интернет желісі арқылы қосылуын, оның ішінде VPN арқылы қосылуды ұйымдастырған жағдайда да қолдауы тиіс.
- Импортты алмастыру мақсатында серверлік және агенттік бөлімдер отандық операциялық жүйелерде (отбасында) орнату мүмкіндігін қолдауы керек Linux). Еркін таратылатын немесе отандық бағдарламалардың бірыңғай тізіліміне енгізілген мәліметтер базасы пайдаланылуы керек.
- Агенттерді басқару, жиналған ақпаратты сақтау және есеп беру функцияларын жүзеге асыратын бағдарламалық жасақтаманың серверлік бөлігі барлық қажетті компоненттерді бір серверге орнату мүмкіндігін қолдауы керек.
- Серверлік құрамдастарды бір қондырғыда қамтамасыз ету мүмкіндігі болуы керек ISO-суретте.
- ОЖ-де серверлік компоненттерді орнату мүмкіндігі қамтамасыз етілуі керек Ubuntu 16.04, 18.04, 20.04 қосымша тәуелділіктерді орнатпай.
- Ақпаратты жинау үшін бір компьютерге бір ғана бақылау агенті (модулі) орнатылуы керек.
- Агент жұмыс станциялары мен терминал серверлері үшін бірыңғай болуы керек.
- Өзінің жұмыс істеу процесінде жүйе (оның агенттері) қорғалатын жұмыс станциялары мен серверлердің жұмысына елеулі (елеулі) кері әсерін тигізбеуі керек.
- Жиналған ақпаратқа қол жеткізу, қауіпсіздік саясаттарын басқару, агенттің конфигурациясын конфигурациялау үшін өкілеттіктердің аражігін икемді ажырату мүмкіндігі бар бірыңғай әкімші консолі пайдаланылуы тиіс.
- Жүйе тік және көлденең масштабтау мүмкіндігіне ие болуы, заманауи виртуалдандыру жүйелерінде орнатылуы және өз функцияларын орындауы керек.

- Есептерді жаңартуды кідірту ұсынылған аппараттық конфигурацияда жүйені максималды пайдалану кезінде 15 минуттан аспауы керек.

Лицензиялауға қойылатын талаптар

- Лицензиялау бір уақытта белсенді жұмыс станцияларының және/немесе пайдаланушылардың саны бойынша жүргізілуі керек;
- Лицензияны бір жұмыс станциясынан немесе пайдаланушыдан басқа жұмыс станциясына немесе пайдаланушыға шектеусіз рет қайта орнату арқылы икемді лицензиялау мүмкіндігі болуы керек;
- Серверлік құрамдастар тапсырыс берушіден бағдарламалық қамтамасыз етуге арналған қосымша ақылы лицензиялардың міндетті түрде болуын талап етпеуі тиіс.
- Тағайындалған және қайтарып алынған лицензиялар сервер консолінде көрнекі және көрнекі түрде көрсетілуі керек.

Агент үшін қолдау көрсетілетін операциялық жүйелерге қойылатын талаптар

- Арналған агент Windows келесі операциялық жүйелерді қолдайтын 32 немесе 64 биттік нұсқада – Windows Vista SP2, Windows 7 SP2, Windows 8, Windows 8.1 SP1, Windows 10. Агент сонымен қатар келесі операциялық жүйелердегі терминалдық серверлердің жұмысын қамтамасыз етуі керек: Windows 2008, Windows 2008 R2, Windows 2012 R2, Windows 2016;
- Арналған агент Linux келесі операциялық жүйелерді қолдай отырып: CentOS, Ubuntu Dekstop, Debian, Gentoo linux, Astra linux, Arch linux, Rosa linux, AltLinux және басқалар Linux-like дистрибутивтер;
- Арналған агент MacOS операциялық жүйелерді міндетті түрде қолдай отырып: macOS 10.13, 10.14, 10.15, 11.x (Bigsur), 12.x(Montray), 13.x(Ventura).
- Операциялық жүйелерді қашықтан орнату утилитасымен қолдау: Windows Vista SP2, Windows 7 SP2, Windows 8, Windows1 SP1, Windows 10.

Бағдарламалық жасақтама архитектурасына қойылатын талаптар

- OLAP сұраныстарының нақты уақыт режимінде орындалуы қамтамасыз етілуі керек.
- Аналитикалық сұраныстарды нақты уақыт режимінде жоғары жылдамдықта орындау үшін жүйе қосымша типтегі мәліметтер базасын пайдалануға ауыса алатындай болуы керек columnar store, атап айтқанда, отандық ДБ бағдарламаларының бірыңғай тізіліміне енгізілген ClickHouse.
- Метадеректер дерекқорда, ал файлдар бөлек файл қоймасында сақталуы керек.
- Файлдарды сақтау "сақиналы буфер" түріндегі ротация режимінде ұзақ мерзімді сақтауға автоматты түрде көшу мүмкіндігімен қамтамасыз етілуі керек.
- Агент пен сервер арасындағы алмасу протоколы, сондай-ақ әкімші бақылау тақтасына кіру TLS тобының шифрлауымен (клиенттік сертификаттар негізінде) қорғалуы тиіс.
- API сұрауларын (REST API) қалыптастыру арқылы деректерді жинау серверінен ақпаратты алу мүмкіндігі қамтамасыз етілуі керек, Database API және деректер үлгісімен өзара әрекеттесу).
- Деректерді SIEM жүйелеріне жіберу мүмкіндігі болуы керек.
- Оқиғалар мен есептер негізінде жүйеде жиналған деректерді талдау мүмкіндігімен деректерді ҚББЖ-дан дерекқорға тасымалдау мүмкіндігі болуы керек.
- Күнтізбені құру үшін 1С-тен қызметкерлердің болмауына байланысты табельді импорттау мүмкіндігі болуы керек.
- Әкімші интерфейсі көпөлшемді принцип бойынша құрылымдалған деректердің үлкен массивтеріне негізделген жиынтық (жиынтық) ақпаратты шығаруды қамтамасыз етуі керек.
- Агент жиналған деректерді домендік атау бойынша да, IPv4 мекенжайлары бойынша да кемінде екі түрлі сервер мекенжайына жібере алуы керек және IPv6.
- Агент қажетті оқиғалар индекстелмейтін мониторинг ережелерін теңшеу мүмкіндігіне ие болуы керек;
- Агент әкімші құқықтары бар артықшылықты пайдаланушыдан қорғау үшін серверден құпия сөзді алу мүмкіндігіне ие болуы керек;
- Пайдалану мүмкіндігі болуы керек Rust деректерді өңдеу үшін;
- Негізінде мазмұнды талдаушыны пайдалану мүмкіндігі болуы керек Apache Tika.
- Трафикті сүзу арқылы деректерді жинауды конфигурациялау мүмкіндігі болуы керек ICAP-серверде.
- Кластерлік архитектураны, барлық кластерлердегі деректермен жұмыс істеуге арналған бір консольді және бір нүктені пайдалану арқылы серверді көлденең масштабтауды қамтамасыз ету қажет таралулар саясаткер.

Жүйені әкімшілендіруге қойылатын талаптар

Қатысуы тиіс **әкімшінің басқару тақтасы** ішінде web-келесі мүмкіндіктері бар сервер интерфейсіностармен:

- Әкімші интерфейсі рөлге негізделген өкілеттіктерді, соның ішінде берілген өкілеттіктерді бөлуді қолдауы керек Active Directory;
- Қосылымды орнату интерфейсі болуы керек Active Directory;
- Пайдаланушыларды немесе әкімшілерді консольдің веб-интерфейсінде авторизациялау, рөлдерді тағайындау, деректерге қол жеткізу құқықтарын тағайындау және бақылау конфигурациялары пайдаланушылар мен топтарды ескере отырып мүмкін болуы керек. Active Directory;
- Деректерге негізделген пайдаланушылар топтары ретінде деректерге қол жеткізу үшін әкімшілерге рұқсат беру Active Directory, сондай-ақ нақты шоттарға.
- Әкімшілердің атрибуттары негізінде белгілі бір деректер мен оқиғаларға қол жеткізуін шектеу мүмкіндігі.
- Агенттерді орнату және жою топтық саясаттар арқылы орталықтандырылғандай орындалуы керек Active Directory агент модулінің орнатушысын пайдалану арқылы немесе жергілікті түрде орнатушыны пайдаланушы машинасында іске қосу арқылы;
- Агентті бақылау утилитасын орнату мүмкіндігі болуы керек. Орнату жергілікті, топтық саясаттар арқылы және қашықтан орнату утилитасы арқылы жүзеге асырылуы керек.
- Пайдаланушыларды параметрлер бойынша басқаруды теңшеу мүмкіндігі OU.
- Деректерді синхрондау мүмкіндігі Active Directory бірнеше бойынша OU.
- Бірнеше домендерді қолдау Active Directory бірыңғай жүйе аясында.
- Агенттерді жергілікті желіде кесте бойынша орнатуды жоспарлау мүмкіндігі болуы керек.
- Алып тастау мүмкіндігі болуы керек IP - агентті қашықтан орнату үшін жергілікті желіні сканерлеу аясындағы мекенжайлар.
- Бақылау агенттерін орнату мүмкіндігі болуы керек VDI сервердің дерекқорында бірегей машина идентификаторын жасау мүмкіндігімен;
- Келесі әрекеттерді орындай отырып, белгілі бір немесе бірнеше жұмыс орындарын таңдау мүмкіндігімен белсенді немесе орнатуға дайын компьютерлерді қарау мүмкіндігі болуы керек: барлық компьютерлерді таңдау, лицензияны босату, лицензияны тағайындау, лицензияны автоматты түрде тағайындау, агентті жоюға шақыру, агентті жоюдан бас тарту, компьютерді құлыптау немесе құлпын ашу, агентті соңғы нұсқаға жаңарту, ағымдағы жаңартуды болдырмау, агентті орнату, агентті тексеру, сипаттарды тағайындау (конфигурация мен топтарды таңдау);
- ДК тізіміне сәйкес таңдау және орнату мүмкін болуы керек Active Directory орнатуға тағайындалған компьютерлерді таңдау үшін агент орнатушысын домен контроллеріне қосу арқылы;
- Ажыратылғандардан лицензияны автоматты түрде қайтарып алу болуы керек AD пайдаланушылардың.
- Жүйе әкімшісі растағаннан кейін агенттердің орталықтандырылған жаңартуларын автоматты түрде жүргізу мүмкіндігі болуы тиіс;
- Барлық анықталмаған агенттерді жою мүмкіндігі болуы керек;
- Деректер базасында ақпаратты сақтау ұзақтығын, оның ішінде мүмкіндікті теңшеу мүмкіндігі қамтамасыз етілуі керек автотазартқыштар дерекқордан деректерді жоймай файлдарды сақтауға арналған;
- Агенттің жергілікті дерекқорын шифрлау мүмкіндігі болуы керек.
- Агенттің жергілікті дерекқорын жойғаннан кейін оны сақтау мүмкіндігі болуы керек;
- Агенттерге деректерді тасымалдау үшін резервтік мекенжайды тағайындау мүмкіндігі болуы керек.
- Мәліметтер базасының дискілерін, қосымша мәліметтер базасын және файлдарды сақтауды толтыру туралы ескерту жасалуы керек;
- Жүйелік оқиғалар туралы жүйелік әкімшіге хабарламалар жасалуы керек (жүйелік қателер, ескертулер, қауіпсіздік саясатының іске қосылуы және т.б.).;
- Агенттен алынған деректердің бір реттік көлемінің максималды көлемін серверге жіберуді конфигурациялау қамтамасыз етілуі керек;
- Агенттен серверге деректерді тасымалдау жылдамдығын шектеу мүмкіндігі болуы керек.
- Жүйе әкімшілерінің әрекеттер журналы тікелей әкімші консолінде сақталуы керек;
- Орын алуы тиіс автосаменттер компьютердің атауын өзгерткен кезде агенттің аты-жөні;
- Агенттегі сервердің IP мекенжайын және портын оны қайта орнатпай-ақ өзгерту мүмкіндігі болуы керек;
- Агент пен сервердің бір портта және IP мекенжайында жұмыс істеуі үшін қолдау болуы керек, бірақ сертификатта басқа SNI болуы керек;
- Агенттердің нұсқаларын әкімшілік интерфейсінен жүктеу мүмкіндігі қамтамасыз етілуі керек Windows және Linux, сондай-ақ қашықтан орнату утилитасы;
- Веб-консольде орнату кезінде қолданылатын агенттердің нұсқалары көрсетілуі керек.
- Деректерді жинауды басқару пайдаланушылар мен компьютерлердің конфигурацияларын оларды қосу, өзгерту және жою мүмкіндігімен тағайындау арқылы жүзеге асырылуы тиіс;

- Алдын ала орнатылған (стандартты) конфигурациялар үшін бастапқы параметрлерге (әдепкі мәндер) қалпына келтіру мүмкіндігі болуы керек.;
- Пайдаланушы конфигурациялары онда анықталған пайдаланушыларға тағайындалуы және USB / CD құрылғыларын пайдалану ережелерінің параметрлері болуы керек: толық құлыптау, тек оқуға рұқсат беру және идентификаторлары бойынша осындай құрылғылардың тізімін орнату;
- Тағайындалған конфигурацияға қарамастан, барлық пайдаланушылар үшін бақылау модульдерін конфигурациялау мүмкіндігі бар жаһандық конфигурация болуы керек;
- Барлық есептерді жіберу үшін пайдаланылатын сервер параметрлерінде поштаны жіберу параметрлерін конфигурациялау мүмкіндігі болуы керек, бақылау тақталары және хабарламалар;
- Есептің нақты жіберілген уақытын көрсету мүмкіндігі болуы керек немесе бақылау тақтасы поштаға;
- Есептерді жіберу мүмкіндігі іске асырылуы керек, бақылау тақталары және форматтардағы хабарламалар PDF, HTML және EXCEL;
- Агенттерді веб-интерфейс арқылы орнату кезінде пайдаланылатын құпия сөздерді сақтау қоймасы құпия сөздерді сақтау және өңдеу мүмкіндігімен ұйымдастырылуы керек;
- Деректер базасын айлар бойынша бөлу мүмкіндігі болуы керек (шардалау) және әкімші интерфейсінен таңдалған айдағы деректерді жою функциясы;
- Веб-консольдегі әкімшілер жасаған параметрлер мен конфигурациялардағы өзгерістерді жазып алуы және көруге қолжетімді болуы керек;
- Белгілі бір ақпарат пен есептерді қарау үшін әкімші әрекеттері консольде жазылуы керек.
- "Жүйелік әкімшілердің соңғы әрекеттерін" жүктеу және сүзу мүмкіндігі қамтамасыз етілуі керек
- Саясаттар мен талдаушылардың атын көрсете отырып, сервер өңдейтін кезектегі оқиғалар санын көруге қолжетімді болуы керек;
- Сервер журналдарын, агент конфигурацияларын, бақылау ережелерін, сүзгілерді және саясаттарды жүктеп салу мүмкіндігі болуы керек;
- Лицензия, оның іске қосылу және жарамдылық мерзімі, серверге қосыла алатын компьютерлер саны және қосылған компьютерлер саны туралы ақпарат қолжетімді болуы керек;
- Барлық есептерді қайта есептеуді қолмен іске қосу функциясы болуы керек;
- Серверді бастапқы параметрлерге қайтара отырып, барлық пайдаланушы параметрлерін жою мүмкіндігі болуы керек;
- Барлық қызметтерді қайта іске қосу мүмкіндігі болуы керек;
- Веб-интерфейс тілін таңдау керек (орыс немесе ағылшын);
- Веб-интерфейстің көрнекі тақырыбын таңдау керек;
- Сервер нұсқасы, нұсқасы туралы ақпарат көрсетілуі керек Windows және Linux агенттің;
- Әкімші құпия сөзін өзгерту интерфейсі және интерфейспен жұмысты аяқтау функциясы (жүйенің ағымдағы пайдаланушысының сеансын аяқтау) болуы керек.
- Деректер базасынан деректерді нүктелік түрде жою мүмкіндігі, көрсетілген деректер параметрлеріне сәйкес, тікелей басқару консолінен.
- Инциденттер мен тұрақты жіберілімдер бойынша хабарламаларды бақылау мен баптаудың бірыңғай өрісі;
- Оқиғаларды айналдыру үшін пернелерді пайдалану;
- Сәтті және сәтсіз кіру әрекеттері көрсетілуі керек;
- Әкімшінің жүйеден шығуы көрсетілуі керек;
- Тиіс жүйеге кіру жүктелген деректерді егжей-тегжейлі көрсете отырып, жүйеден деректерді жүктеу фактісі;
- Тиіс жүйеге кіру жүйе әкімшісінің құпия сөзін өзгерту.
- Сессия аяқталуы тиіс, кезінде өзгерістер жүйенің әкімшісінің құпиясөзі.
- Синхрондау кезінде жоқ әкімшілер өшірілуі керек AD;
- Құпия сөз дұрыс енгізілмеген жағдайда, авторизациясы сәтсіз болған мекен-жайдан кіруге шектеу қойылуы керек.
- Тиіс бекітілуі және жүйеге кіру пайдаланушы үшін де, агент үшін де қайтарып алу себебін егжей-тегжейлі көрсете отырып, лицензияларды қайтарып алу және мониторинг тағайындау операциялары;
- Осы операцияны тіркей отырып, белсенді емес пайдаланушыларды бақылауға арналған лицензияны автоматты түрде босатуды немесе қайтарып алуды қосу мүмкіндігі болуы керек;
- Мониторингте жаңа машина пайда болған кезде хабарландыру мүмкіндігі;
- Ережелерді қарау және бақылау мүмкіндігі агенттің өз профиліндегі жұмысына қолданылатын;
- Белсенділік болмаған кезде әкімші сессиясынан шығу уақытын теңшеу мүмкіндігі;
- Веб-консольдегі деректерді өңдеудің белсенді элементтерін белгілеу;
- Құпия сөзді әлсіз құпия сөздерді пайдалануға жол бермей, әкімші құпия сөзін жасаудағы қиындықтардың бар-жоғын тексеру.
- Серверді веб-консольден басқару мүмкіндігі болуы керек, оның ішінде берілгендердің жоспарлы орындалуы аясында комманд.
- Сервер тарапынан агентке деректерді жіберу мекенжайын өзгерту мүмкіндігі болуы керек;

- Бақыланатын агенттер, пайдаланушылар және олардың мәртебесі туралы ақпаратты форматта жүктеп салу мүмкіндігі болуы керек CSV.
- Агент/пайдаланушы лицензия ала алмаған жағдайда жүйенің әкімшісінің поштасына хабарлама жіберу мүмкіндігі болуы керек.

Жүйенің функционалдық мүмкіндіктеріне қойылатын талаптар

Төмендегілер жазылуы керек **оқиғалардың түрлері** пайдаланушының іс-әрекеттері:

- жүйеге кіру/шығу;
- қашықтан жүйеге кіру/шығу
- қосымшалардағы және сайттардағы пайдаланушының белсенділігі;
- қашықтағы жұмыс үстеліне қосылу, басқаруды тоқтату;
- жұмыс үстеліндегі бейнені жазу;
- экран суреті;
- веб-камерадан алынған сурет;
- файлдармен жасалатын операциялар;
- ұсталған файлдардың көлеңкелі көшірмелері;
- құжаттарды басып шығару;
- алмасу буфері;
- пернетақтадан енгізу;
- жабдықтардың тізілімі;
- орнатылған бағдарламалардың тізілімі;
- микрофоннан жазу;
- веб-ресурстарға кіру;
- желілік қосылыстар;
- интернет-мессенджерлер;
- пошта;
- БҚ орнату;
- қосымшаны іске қосу және аяқтау;
- сыртқы дискілер мен құрылғылар;
- жұмыс орнында болуы.

Төмендегілер жазылуы керек **атрибуттар логияланатын ақпараттың**:

- агент;
- Тағайындалған конфигурация
- IP-мекен-жайы;
- қосымша белгі;
- ДК атауы;
- мәртебе;
- ОЖ нұсқасы;
- агент нұсқасы;
- пайдаланушының есептік жазбасы;
- түсініктеме;
- бөлім;
- ұйым;
- телефоны;
- толық аты-жөні;
- Топ AD;
- пошта;
- лауазымы;
- домен;
- басшы;
- пайдаланушы;
- қосымша;
- толық жол;
- атауы;
- сипаттамасы;

- сайт;
- толық домен;
- хаттама;
- URL;
- негізгі домен;
- мазмұн түрі;
- желілік белсенділік;
- желілік порт;
- файл;
- хэш файлдың;
- дереккөздің файл атауы;
- дереккөз жолы;
- дереккөзді кеңейту;
- операциялар;
- мазмұн түрі;
- файлдың аты;
- диск түрі;
- кеңейту;
- жол;
- құрылғылар;
- Құрылғы идентификаторы;
- диск түрі;
- құрылғы сыныбы;
- құрылғы түрі;
- хат алмасу;
- алушының домені;
- жіберуші;
- барлық алушылар;
- хабарлама форматы;
- бағыт;
- жіберушінің домені;
- алушы;
- чаттар;
- қарым-қатынас арнасы;
- күні;
- тәулік сағаты
- уақыт белдеуі;
- аптаның күні;
- жылдар бойынша;
- айлар бойынша;
- күндер бойынша;
- сағат бойынша;
- минуттар бойынша.

Тиіс **индекстелуі тиіс** жүйемен келесі форматтағы файлдар:

- Adobe Acrobat (*.pdf);
- Ansi Text (*.txt);
- ASCII Text;
- CSV (Comma-separated values) (*.csv);
- EML files (сақталған электрондық хаттар Outlook Express) (*.eml);
- HTML (*.htm, *.html);
- JPEG (метадеректер) (*.jpg);
- MHT-мұрағаттар (сақталған HTML-мұрағаттар Internet Explorer) (*.mht);
- MSG files (сақталған электрондық хаттар Outlook) (*.msg);
- Microsoft Excel (*.xls) Microsoft Excel 2003 XML (*.xml);
- Microsoft Excel 2007 және жоғары(*.xlsx);
- Microsoft Outlook Express 5 және 6: базалар хабарламалар (*.dbx);
- Microsoft PowerPoint (*.ppt);
- Microsoft Rich Text Format (*.rtf);

- Microsoft Word for DOS (*.doc);
- Microsoft Word for Windows (*.doc);
- Microsoft Word 2003 XML (*.xml);
- Microsoft Word 2007 және жоғары(*.docx);
- Multimate version 4 (*.doc);
- OpenOffice 1, 2 және 3 нұсқалары: құжаттар, электрондық кестелер және презентациялар (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (оазисті қоса алғанда Open Document Format кеңселік қосымшалар үшін).

Бақыланатын арналардағы ұстауға қойылатын талаптар

Бақылау мүмкіндігі қамтамасыз етілуі керек **электрондық поштаның**, атап айтқанда:

- Хаттамалар бойынша пошталық хабарламаларды ұстап қалу – SMTP/SMTPs, POP3/POP3s, IMAP/IMAPs, MAPI;
- IBM пошта хабарларын ұстау мүмкіндігі Lotus Notes IMAP пошта жәшігінен поштаны жинау арқылы.
- Арқылы алынған хабарламалар арасында байланыс болуы керек IMAP және жүйедегі домендік пайдаланушыларды;
- Пошта хабарламаларының файл-қосымшаларын ұстап қалу және талдау;
- Пошталық хабарламалар мен қосымшалардың мониторингі ақпараттың мазмұнымен және одан әрі ақпараттық қауіпсіздік үшін бір немесе бірнеше жауапты тұлғаларға хабарлама жіберу, егер көрсетілген критерийлер бойынша ақпарат табылса;
- Мәтіннің берілген параметрлері мен пошта хабарламаларының атрибуттары және олардың қосымшаларының мәтіні бойынша іздеу;
- Хаттарды келесі түрде түсіру мүмкіндігі: құжат Excel, HTML, CSV, PNG форматындағы кескін
- Хат алмасуды толығымен ZIP мұрағатында жүктеп алу немесе принтерде басып шығару мүмкіндігі;
- Көрсетілетін ақпараттың параметрлерін қолмен баптай отырып, хат алмасу графигін құру мүмкіндігі.

Ақпарат алмасуды мониторингілеу мүмкіндігі қамтамасыз етілуі керек **мессенджерлер (IM-клиенттер)**, оның ішінде, web-нұсқаларын, атап айтқанда:

- Мәтіндік хабарламаларды хаттамалар арқылы ұстап алу керек (Skype, Telegram, ICQ/QIP, Jabber, Mail.ru Агент, MS Teams, Bitrix 24 Desktop, Whatsapp, Express, VKTeams);
- Жіберілетін файлдарды ұстап қалу орын алуы керек (Skype, Telegram, Bitrix24 Desktop, Express, VKTeams);
- Мониторингтің арнайы критерийлерін белгілеу және мәтіндік хабарламалар мен файлдардың мониторингін ұйымдастыру мүмкіндігі болуы керек.
- Хабарламалар мен файлдарда мониторингтің белгіленген критерийлері бойынша ақпараттың жіберілгені анықталған жағдайда, ақпараттық қауіпсіздікке жауапты бір немесе бірнеше адамға хабарлама жіберуді ұйымдастыруға болады;
- Іздеу мәтіннің және хабарламалардың атрибутының және (мазмұнының) IM клиенттері арқылы жіберілген файлдардың көрсетілген параметрлері бойынша жүргізілуі керек.

Ақпаратты бақылау жүзеге асырылуы тиіс **HTTP хаттамалары бойынша/HTTPs**, атап айтқанда:

- HTTP/HTTPS хаттамалары бойынша деректерді ұстап қалу;
- Блогтарға, форумдарға, файл алмасу сервистеріне және өзге де веб-сервистерге жіберілетін хабарламалар мен файлдарды ұстап қалу және талдау;
- ВК шығыс хабарламаларын ұстап қалу;
- Веб-пошта қызметтері арқылы жіберілген немесе алынған шығыс электрондық пошталар мен тіркемелерді ұстау (кем дегенде, mail.yandex.ru, mail.google.com, mail.rambler.ru, e.mail.ru, outlook.com);
- Пайдаланушының іздеу сұрауларын ұстау және бақылау;
- Пайдаланушы кірген барлық беттердің (URL) мекенжайларын сақтау;
- Ақпараттың мазмұны бар хабарламалар мен файлдарды бақылау және көрсетілген критерийлер бойынша ақпарат табылған жағдайда ақпараттық қауіпсіздікке бір немесе бірнеше жауапты тұлғаларға хабарламаны одан әрі жіберу;
- HTTP(S) протоколы арқылы жіберілген және алынған хабарламалар мен файлдардың мәтіні мен атрибуттары бойынша іздеу;
- Веб-ресурстарға кіруді бұғаттау мүмкіндігі;
- Сайттардың мониторингін қара және ақ тізімдер бойынша алып тастау;
- Барлық кірген сайттарды және веб-беттерде өткізілген уақытты бақылау;

- ДК-де пайдаланушының жұмыс уақыты туралы әр түрлі есептер құру мүмкіндігі. Бір күнде кірген сайттардың рейтингі, жеке пайдаланушы немесе пайдаланушылар топтары немесе бүкіл ұйым үшін таңдалған уақыт аралығындағы оқиғалар хронологиясы келесі түрде: құжат Excel, HTML, CSV, PNG форматы;
- Есептерді толығымен ZIP мұрағатында жүктеп алу немесе принтерде басып шығару мүмкіндігі.

Берілетін ақпаратты бақылау мүмкін болуы керек **FTP хаттамасы бойынша**, атап айтқанда:

- FTP протоколы арқылы жүктелген немесе жіберілген, сондай-ақ шифрланған FTP протоколы арқылы жіберілген файлдарды ұстау (FTPs);
- Ақпараттың мазмұны бар файлдарды бақылау және көрсетілген критерийлер бойынша ақпарат табылған жағдайда ақпараттық қауіпсіздікке бір немесе бірнеше жауапты тұлғаларға хабарламаны одан әрі жіберу;
- FTP протоколы бойынша файлдар мен парольдерді бақылау және ұстап қалу/FTPs кейіннен ұсталған файлдарды контексттік талдаумен.

Ақпаратты бақылау мүмкіндігі болуы керек, **мөрге жіберілетін**, атап айтқанда:

- Басып шығаруға жіберілетін құжаттарды ұстап қалу;
- Баспаға жіберілген құжаттардың мәтінін шығару және талдау;
- Ақпараттың мазмұнымен басып шығаруға жіберілген құжаттарды бақылау және одан әрі ақпараттық қауіпсіздік үшін бір немесе бірнеше жауапты тұлғаларға хабарлама жіберу, егер ақпарат көрсетілген критерийлер бойынша табылса;
- Басып шығаруға жіберілген файлдардың мәтіні мен төлсипатының көрсетілген параметрлері бойынша іздеу;
- Құжат түрінде жүктеу мүмкіндігі Excel, HTML, CSV, PNG форматында;
- ZIP мұрағатында жүктеп алу немесе принтерде басып шығару мүмкіндігі.

Бақылау жүргізілуі керек **сыртқы жинақтағыштардың** келесі мүмкіндіктермен:

- Сыртқы тасымалдағыштарға, соның ішінде қатты дискілерге, жад карталарына және USB құрылғылары, CD/DVD дискілері сияқты жалғанған басқа алынбалы дискілерге жіберілген файлдарды көлеңкелі көшіру;
- USB-құрылғылардың қосылуын және ажыратылуын бақылау;
- Қосылымды, ажыратуды және операцияларды бақылау RuToken бірегейлікті беките отырып ID;
- USB құрылғыларының қол жеткізу ережелерін олардың бірегей идентификаторлары, соның ішінде тек оқуға арналған рұқсаты бар құрылғылар арқылы конфигурациялау мүмкіндігі;
- CD-жинақтағыштарды бұғаттау мүмкіндігі;
- USB-құрылғыларын қара немесе ақ тізімдер бойынша, құрылғылар кластары бойынша және топтар бойынша бұғаттау ережелерін теңшеу мүмкіндігі;
- Листингті ұстап қалу және көрсетілген файл кеңейтімдері бойынша ұстап қалу ережесін теңшеу мүмкіндігімен сыртқы тасымалдағыштарды қосқан кезде файлдарды көлеңкелі көшіру;
- Ақпараттың мазмұнымен файлдарды сыртқы тасымалдаушыларға тасымалдау жағдайларын бақылау және одан әрі ақпараттық қауіпсіздік үшін бір немесе бірнеше жауапты тұлғаларға хабарлама жіберу, егер ақпарат анықталған жағдайда көрсетілген критерийлер бойынша;
- Көрсетілген өлшемшарттар бойынша ақпарат анықталған жағдайда, көрсетілген параметрлермен сыртқы құрылғыларды пайдалану жағдайларын мониторингілеу және ақпараттық қауіпсіздік үшін бір немесе бірнеше жауапты тұлғаларға хабарламаны одан әрі жіберу;
- Файлдарды сыртқы жад дискілеріне көшіру оқиғаларының аудиті: файл атауы, пайдаланушы, күні, уақыты, қолданбасы, толық жолы және құрылғы деректері жазылады;
- Сыртқы тасымалдаушыларға жіберілген ұсталған файлдардың мәтіні мен атрибуттары бойынша іздеу мүмкіндігі.
- Пайдаланушылардың жергілікті компьютерлерінде көлеңкелі көшірмелер үшін сақтау көлемін теңшеу мүмкіндігі;
- Көлемі көрсетілген шекті мәннен асатын деректерді тасымалдау кезінде дискілерді құлыптау мүмкіндігі;
- Пайдаланушымен жұмыс істеу кезінде файлдық операцияларды басқару мүмкіндігі CD/DVD көлеңкелі көшірмелерді жасау мүмкіндігімен.

Берілетін ақпаратты бақылаудың келесі мүмкіндіктері болуы керек **бұлтты қоймалар** (файлдық арна):

- Келесі бұлттық қоймалар бойынша бақылауды жүзеге асыру мүмкіндігі – Dropbox, Яндекс.Диск, Google Drive, Nextcloud, ownCloud, OneDrive;

- Агент орнатылған қызметкердің жұмыс станциясынан бұлттық қоймаларға жіберілген файлдарды көлеңкелі көшіру;
- Көрсетілген параметрлермен файлдарды бұлттық қоймаларға тасымалдау жағдайларын бақылау және көрсетілген критерийлер бойынша ақпарат анықталған жағдайда ақпараттық қауіпсіздікке бір немесе бірнеше жауапты тұлғаларға хабарламаны одан әрі жіберу;
- Файлдарды бұлттық қоймаларға жіберу оқиғаларының аудиті: файл атауы, пайдаланушы, бұлттық қызметтің күні, уақыты және атауы жазылады;
- Бұлттық қоймаларға жіберілген ұсталған файлдардың мәтіні мен атрибуттары бойынша іздеу мүмкіндігі;
- Пайдаланушылардың жергілікті компьютерлеріндегі көлеңкелі көшірмелер үшін сақтау көлемін теңшеу мүмкіндігі.

Файлдарды бақылауды жүзеге асыру керек және **файлдық белсенділік**, атап айтқанда:

- Файлдық операцияларды басқару (Жазу, көшіру, дискінің мазмұны, ажырату, қоқыс жәшігін босату, қайта жазу, атын өзгерту, жылжыту, атын өзгерту және жылжыту, қосу, құру, жою, оқу);
- Алынбалы медиадан файлдарды және/немесе файлдар тізімін ұстау, соның ішінде CD/DVD-дискілер файлдарды кеңейтудің көрсетілген шаблондары бойынша жалғанған кезде;
- Бақыланатын жұмыс станциясының ақпараттық периметрінің артына жіберілген файлдардың көлеңкелі көшірмелерін сақтаңыз;
- Ұсталған файлдардың мәтіні мен атрибуттары бойынша кейінгі іздеулер;
- Көрсетілген өлшемшарттар бойынша ақпарат анықталған жағдайда, көрсетілген параметрлері бар файлдарды пайдалану жағдайларын мониторингілеу және ақпараттық қауіпсіздік үшін бір немесе бірнеше жауапты тұлғаларға хабарламаны одан әрі жіберу;
- Файлдық белсенділікті, оның ішінде алдын ала орнатылғандардан көшіру мүмкіндігін қоса, жеке бақылау саясаттарын жасау;
- Кез келген файлдық операциялар үшін көлеңкелі көшірмелерді жасау арқылы арнайы бақылауға арналған жолдар мен файлдарды анықтау мүмкіндігі.
- Крипто-бағдарламамен шифрланған файлдарды анықтау.

Жіберілетін ақпаратты бақылауды және өңдеуді жүзеге асыру мүмкіндігі болуы керек **жергілікті желілік** ресурстарды келесі жолдармен:

- Агент орнатылған пайдаланушының жұмыс станциясынан желілік ресурстарға жіберілген файлдарды көлеңкелі көшіру;
- Файлдарды көрсетілген параметрлермен желілік дискілерге тасымалдау жағдайларын бақылау және көрсетілген критерийлер бойынша ақпарат табылған жағдайда ақпараттық қауіпсіздікке бір немесе бірнеше жауапты тұлғаларға хабарлама жіберу;
- Желілік дискілерге файлдарды жіберу оқиғаларының аудиті: файл атауы, пайдаланушы, күні, уақыты және ресурсқа, қосымшаға желілік жол жазылады;
- Желілік ресурстарға жіберілген ұсталған файлдардың мәтіні мен атрибуттары бойынша іздеу мүмкіндігі;
- Жеке пайдаланушылар мен жұмыс станциялары үшін жеке ақпаратты басқару саясатын құру мүмкіндігі.

ДК-дегі пайдаланушылардың іс-әрекеттерін бақылау әдістеріне қойылатын талаптар:

БҚ мүмкіндік беруі тиіс **скриншоттар жасау** (кадрлар, қызметкердің жұмыс үстелі экранының кадрлары) кез келген экрандар саны үшін және түсіру процесін келесі жолдармен басқарыңыз:

- Скриншоттарды белгіленген аралықта түсіру;
- Белсенді терезені ауыстыру арқылы скриншоттарды түсіру;
- Жұмыс үстелін шолу немесе жұмыс үстелін қашықтан басқару кезінде қашықтан қосылу кезінде скриншоттарды түсіру;
- Белгілі бір қолданбалар мен сайттар үшін жиірек скриншот аралықтарын орнату;
- Пакеттердегі скриншоттардың қысылуын және түсін реттеу мүмкіндігімен белгілі бір кезеңдегі скриншоттарды бір файлға сақтайтын скриншоттар бумасын жасау.
- Алынатын скриншоттардың сапасын пайызбен реттеуді орындау;
- JPEG скриншот пішімін пайдалану;
- Үлкен өлшемді скриншоттарды талдау мүмкіндігі үшін веб-консоль ішінде скриншоттарды үлкейту мүмкіндігі.
- Келесі пішімдерде жүктеп салу: файл Excel, HTML, CSV, PNG форматы
- ZIP мұрағатына жүктеу немесе принтерге басып шығару;

БҚ қалыптастыруды және өңдеуді қамтамасыз етуі тиіс **белсенділік статистикалары** пайдаланушы мен компьютерді келесі жолдармен:

- Жиналған ақпаратты әртүрлі кестелер түрінде ұсына отырып, ДК-нің жұмыс уақыты мен тоқтап қалуы (қызметкердің іс-әрекетінің болмауы) туралы статистиканы жүргізу;
- Жиналған ақпаратты график түрінде ұсына отырып, қосымшаларда пайдаланушының жұмыс уақыты туралы статистиканы жүргізу (бұл процестердің басталуынан аяқталғанға дейінгі уақытты емес, пайдаланушының белсенді терезеде жұмыс істеген уақытын ескереді);
- Әрекетсіздік кезеңін орнату мүмкіндігі, содан кейін қызметкердің жұмыс уақыты бос уақыт болып саналады;
- Мониторингтен жекелеген процестердің ерекшеліктерін теңшеу мүмкіндігі;
- Белгілі бір оқиғаларды анықтау үшін жиналған статистиканы автоматты түрде талдау мүмкіндігі (мысалы, рұқсат етілмеген қосымшаларды іске қосу), пайдаланушылардың белгілі бір қосымшалармен жұмыс істеу ұзақтығын және компьютердің жұмыс/тоқтап қалу кезеңдерінің ұзақтығын бақылау – жауапты тұлғаға тиісті хабарлама жіберу арқылы;
- HTML пішімінде жеке пайдаланушы немесе бірнеше пайдаланушы үшін таңдалған уақыт аралығы үшін белсенділік бойынша жеке есептерді (ДК үшін пайдаланушы әрекеті, қолданба әрекеті) сақтау мүмкіндігі;
- ДК-дегі белсенді әрекеттерді жіктеуге арналған қосымшалар мен сайттардың алдын ала орнатылған жиынтығы;
- Қызметті өнімді/өнімсіз/бейтарап деп бөлу;
- Әртүрлі ұсыныстарға арналған есептердің және пайдаланушылардың белсенділігі бойынша жинақталған деректерді талдаудың болуы;
- Пайдаланушылардың белсенділігі бойынша жалпы және топтық есептер;
- Терминалдық жүйелердегі белсенділікті ұстап қалу linux-сеанстарда және кейіннен терминалды енгізу мен шығаруды GIF ретінде егжей-тегжейлі жазу.
- Пайдаланушылардың әрекеттерін ұстау және тіркеу Linux жүйелерде қолдану.
- Басқарманың пайдаланушының статистиканы белгіше арқылы жинау мүмкіндігі науа жүйелер.

Жүзеге асырылуы тиіс **алмасу буферін басқару**, және келесі мүмкіндіктер іске асырылды:

- Алмасу буферіне орналастырылған мәтіндік ақпаратты осы ақпарат алмасу буферіне орналастырылған процестің идентификаторын және оқиғаның уақытын көрсете отырып көшіру;
- Пайдаланушылар алмасу буферіне орналастырған мәтін бойынша іздеу.
- Алмасу буферіне орналастырылған белгілі бір ақпаратты бақылау және берілген критерийлер бойынша ақпарат табылған жағдайда ақпараттық қауіпсіздікке жауапты бір немесе бірнеше тұлғаға хабарлама жіберу;
- Алмасу буферіне орналастырылған графикалық ақпаратты, соның ішінде скриншоттарды басып шығару түймесін басу арқылы көшіру Screen
- Алмасу буфері арқылы деректерді бір қолданбадан екіншісіне тасымалдауды блоктау мүмкіндігі.

Іске асырылуы тиіс **кейллогер** (пернетақтадағы пернелерді басуды тоқтату), келесі ерекшеліктерге ие:

- Пайдаланушы осы ақпаратты және уақытты енгізген қосымшаны тіркей отырып, қызметкердің пернетақтадағы пернелерді басуын тіркеу;
- Пернетақтада енгізілген ақпаратты бақылау және берілген критерийлер бойынша ақпарат табылған жағдайда ақпараттық қауіпсіздікке бір немесе бірнеше жауапты тұлғаларға хабарлама жіберу;
- Жеке пайдаланушылар мен жұмыс станциялары үшін пернелерді басуды бақылауды басқарудың теңшелген саясаттарын жасау мүмкіндігі;
- Саясаттарды есептердегі деректермен тікелей толықтыру мүмкіндігі.
- Пайдаланушылар пернетақтадан енгізген мәтін бойынша іздеу мүмкіндігі.
- Диалогтық терезелерде парольдерді ұстап қалу мүмкіндігі Windows;
- Көмегімен бақылауға тыйым салу/рұқсат беру мүмкіндігі кейлоггердің қосымшалардың қара немесе ақ тізімдері бойынша;
- Жұмыс үстелінің құлпын ашу кезінде құпия сөзді ұстап қалу мүмкіндігі Windows (төмен деңгейлі кейллоггер).
- Алынған арнайы таңбаларды жасыру және көрсету мүмкіндігі кейлогер ретінде.

Жетекші функция болуы керек **аудиомониторинга**, атап айтқанда:

- Агент орнатылған қызметкердің жергілікті станциясындағы анықталған микрофондардан, ол пайдаланатын қолданбаға қарамастан, жазбаны жүргізу мүмкіндігі;
- Агент орнатылған қызметкердің жергілікті станциясындағы аудио құрылғыларға шығатын дыбысты жазу мүмкіндігі;

- Дыбыс жазбасының жазылатын үзінділерінің ұзақтығын реттеу мүмкіндігі;
- Жазу сапасын баптау мүмкіндігі;
- Дыбыстарды елемейтін шу шегін реттеу мүмкіндігі;
- Үнсіздік аралығын реттеу мүмкіндігі, содан кейін дыбыс жазбасы кідіртіледі;
- Дыбысты децибел бойынша жазуды баптау мүмкіндігі;
- Веб-интерфейс жүйесі арқылы жазба файлын ойнату мүмкіндігі;
- Жазылған жазбаларды жүктеу мүмкіндігі;
- Сөйлесулердің сәттерін визуалды түрде анықтау үшін жазылған жазбалардың толқын пішіні көрсетіледі.

Белсендіру мүмкіндігі болуы керек **бейнемониторинг**, келесі негізгі ерекшеліктерге ие:

- Қызметкердің компьютер мониторына қосылу және суретті нақты уақыт режимінде көру мүмкіндігі;
- Бір уақытта бірнеше пайдаланушының жұмыс үстелдерін бақылау мүмкіндігі;
- Қарау терезесін жеке экранға шығару мүмкіндігі;
- Қашықтан қосылған кезде қызметкерлердің жұмыс үстелдерінен ағынды бейнелерді жазу мүмкіндігі;
- Серверге қосылудың қолжетімсіз режимінде жұмыс үстелі бейнесін жазу мүмкіндігі;
- Бейне жазу үшін үзіндінің ұзақтығын реттеу мүмкіндігі;
- Бір уақытта бірнеше пайдаланушының жазбаларын сақтау мүмкіндігі;
- Жүйенің көмегімен жазба файлын ойнату мүмкіндігі.
- Қашықтан қосылуға болатын пайдаланушыларды сүзу мүмкіндігі.

Бақылау мүмкіндігі болуы керек пайдаланушыларды компьютерде жұмыс істейтіндер:

- Веб-камерадан суреттерді берілген аралықта түсіру мүмкіндігі;

- Белгілі бір қолданбалар мен сайттар үшін веб-камерадан суретке түсіру аралықтарын жиірек орнату;
- Веб-камерадан бейнежазба жасау мүмкіндігі;

- Компьютерде сеанс немесе белсенділік болмаған кезде веб-камерадан суретке түсіру мүмкіндігі;
- Нақты уақытта көру үшін веб-камераға қашықтан қосылу мүмкіндігі;

Модуль болуы керек, **файлдарды сканерлеуші**, ол:

- Көрсетілген параметрлер бойынша файлдарға рұқсатсыз кіруді блоктауға мүмкіндік береді;
- Берілген ережелер жиынтығына сәйкес пайдаланушылар мен қосымшалардың файлдарға қол жетімділігін басқаруға мүмкіндіктері бар;
- Оның кеңсе қолданбаларының негізгі түрлерінің файлдарына белгілерді қосу утилитасы бар:.docx, .xlsx, .pptx, .odt, . ods, .odp;
- Файлдардың мәтіндік мазмұнын талдау және ережелер жинағы бойынша оларға қолжетімділікті шектеу мүмкіндігі бар;
- Алынбалы сақтау құралдарына немесе одан файлдарды тасымалдауға тыйым салу мүмкіндігі бар;
- Тыйым салу мүмкіндігі бар белгілі бір операциялар файлдармен жасалған: көшіру, жылжыту, жою, атын өзгерту, оқу;
- Ережелер жиынтығы бойынша шифрланған архивтерге кіруді шектеу мүмкіндігі бар;
- Жұлдызшаланған файлдар бойынша жұмысты қадағалау мүмкіндігі бар;
- WEB-консольде басқару арқылы өз параметрлерінің баптауларына ие және белгіленген файлдар үшін пайдалану және бұғаттау ережелерін орнату мүмкіндіктеріне ие;
- Жергілікті файлдық жүйелерді сканерлейді және табылған нәтижелерді сақтайды;
- Ережелерді конфигурациялау кезінде операторларды қолдайды: not, or, and, xor, eq, matches, in;
- Пайдаланады кезінде баптауда қағидаларын атрибуттар: tag, tag_value, computer_name, user_name, user_domain, file_path, file_name, file_ext, exe_name, mine.

Жиналған ақпаратты көрсету мүмкіндіктеріне қойылатын талаптар

Қатысуы керек **ақпаратты оқиғалар түрлері бойынша қарау**, атап айтқанда:

- Іздеу сұраныстары, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, қолданушы, қосымша, домен, мәтін;
- Әрекет ету уақыты, ақпарат келесі түрде көрсетіледі: уақыт, оқиға түрі, компьютер, пайдаланушы, ұзақтығы (00 сағ 00 м 0
- Скриншот, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, тақырып, сурет;

- Дыбысты жазу, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, құрылғы, мазмұн (аудио файл);
- Ұсталған файл, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, мазмұн (файл, сурет және т.
- Құрылғылар, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, құрылғы түрі, құрылғы, идентификатор;
- Қосымшалардың аяқталуы, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, процесс идентиф
- Жүйелік журнал, ақпарат келесі түрде көрсетіледі: уақыт, оқиға түрі, компьютер, мәтін, мазмұн (журналды өзінен жүктеп
- Сымсыз байланыс, ақпарат келесі түрде көрсетіледі: уақыт, компьютерр, SSID;
- Веб-камерадан алынған сурет, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, сурет;
- Алмасу буфері, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, мәтін, алмасу буферінің фор
- FTP, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қолданба, оқиға;
- Пошта, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, жіберуші, алушылар, тақырып, мазмұн (тіркем
- Сайттарға кіру келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, сілтеме;
- Пернетақтадан енгізу, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, терезе тақырыбы, мәт
- Желі, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, розетка;
- Дабыл (сервер есептеген оқиға), ақпарат келесі түрде көрсетіледі: уақыт, тип, компьютер, пайдаланушы, уақыт, дабыл, мә
- Қосымшаны іске қосқан кезде ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, процесс идент
- Файлдармен жұмыс, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, операция, файл атауы,
- Сыртқы дискілер, ақпарат келесі түрде көрсетіледі – уақыт, компьютер, пайдаланушы, тип, құрылғы, идентификатор;
- Бағдарламалық жасақтаманы орнату, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, жұмыс, өнім, жеткізуші, нұсқа;
- Пакеттерді орнату және жою Linux жүйелерде қолдану.
- Орнатылған пакеттерді түгендеу Linux жүйелерде қолдану.
- Жұмыс үстеліндегі бейне, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қолданба;
- Жүйеге кіру
  /шығу, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, оқиға (жүйеге кіру, жүйеден шығу және т.б.)
- Қашықтан кіру
  /шығу, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, оқиға (жүйеге кіру, жүйеден шығу және т.б.)
- Нысанның деректері, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, қосымша, сайт;
- Жабдықтардың тізілімі, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, құрылғы түрі, құрылғы, жеке куәлік;
- Бағдарламалық жасақтама тізілімі, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, жұмыс, өнім жеткізушісі, нұсқа;
- Құжаттарды басып шығару келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, беттер (басылған беттер саны), мәт
- Интернет-
  пейджер, ақпарат келесі түрде көрсетіледі: уақыт, компьютер, пайдаланушы, жіберуші, алушылар, хабарлама.
- Қолданба логотипін көрсету оған сәйкес оқиғалар ұсталды.
- Оқиғалар бойынша егжей-тегжейлі ақпаратты көрсету пішімін көлденең немесе тікке өзгерту мүмкіндігі.
- Тізім элементі негізінде деректерді сүзу мүмкіндігі.

Жиналған ақпаратты жеке өлшемдер бойынша да, олардың өлшемдері бойынша да қарауды ұйымдастыру қажет **оқиғалар түрлерімен комбинацияларға және өлшемдердің ерікті жиынтығымен**:

- Агент өлшемі, таңдау келесі параметрлер бойынша қамтамасыз етіледі: IP мекенжайы, топ (агент тиесілі), қызметкер, компьютер, күй, ОЖ нұсқасы, агент нұсқасы;
- Пайдаланушыны өлшеу, таңдау келесі параметрлер бойынша қамтамасыз етіледі: бөлім, ұйым, телефон, толық аты-жөні, пошта, лауазым атауы, домен, пайдаланушы, пікір, (ақпарат пайдаланушы профилінде орнатылған);
- Өлшем қолданбасы, таңдау келесі параметрлер бойынша қамтамасыз етіледі: толық жол, терезе тақырыбы, тақырып, сипаттама;
- Сайтты өлшеу, таңдау келесі параметрлер бойынша қамтамасыз етіледі: толық домен, протокол, URL мекенжайы, негізгі домен, мазмұн түрі;
- Желілік белсенділікті өлшеу, таңдау келесі параметрлер бойынша қамтамасыз етіледі – IP мекенжайы, желілік порт;
- Файлды өлшеу, таңдау келесі параметрлер бойынша қамтамасыз етіледі: хэш файл, операция, файл атауы, алынған мазмұн (true немесе false), жапсырма, мазмұн түрі, диск түрі, кеңейтім, жол, бастапқы файл атауы, бастапқы жол, бастапқы кеңейтім;
- Өлшеу құрылғысы, таңдау келесі параметрлер бойынша қамтамасыз етіледі: құрылғы, құрылғы идентификаторы, маркер, диск түрі, құрылғы класы, құрылғы түрі;
- Корреспонденцияны өлшеу, таңдау келесі параметрлер бойынша жүзеге асырылады: алушының домені, жіберуші, барлық алушылар, хабарлама форматы, бағыт, жіберушінің домені, алушы, чаттар, байланыс арнасы. Деректердің үлкен көлемі болған жағдайда хат алмасудың бет-әлпеті көрсетілуі керек;
- Өлшеу күні, таңдау келесі параметрлер бойынша қамтамасыз етіледі: тәулік сағаты, уақыт белдеуі, апта күні, жыл, ай, күн, сағат, минут;
- Инсталляцияны өлшеу, таңдау келесі параметрлер бойынша ұсынылады: жеткізуші, жаңарту, нұсқа, операция, өнім;

- Іске қосылған сүзгілерді өлшеу, таңдау келесі параметрлер бойынша қамтамасыз етіледі: санат, тақырып.

Мүмкіндік болуы керек **есептерді ұсыну режимдерінің ауысуы** деректерді келесі критерийлер бойынша көрсете отырып:

- Белгілі бір оқиға түрлері мен өлшем түрлері туралы ақпаратты оларды біріктіру мүмкіндігімен көрсететін кесте;
- Тізім, белгілі бір оқиға түрлерінің және өлшем түрлерінің жалпы тізімімен, оларды біріктіру мүмкіндігімен ақпаратты қамтамасыз етеді;
- Суреттер, өлшеу түрлерін таңдау мүмкіндігімен веб-камера түсірілімдері мен скриншоттардың оқиға түрлері туралы ақпаратты беруге ыңғайлы болу үшін дисплей режимі;
- Белсенділік, ақпаратты жылулық диаграмма түрінде көрсетеді, ақпаратты оқиға түрлері мен өлшемдері бойынша көрсетуді таңдау мүмкіндігімен;
- Хат алмасу, қосымша өлшем түрлерін таңдау мүмкіндігімен оқиға түрі туралы ақпаратты пошта және интернет пейджер арқылы беруге ыңғайлы болу үшін дисплей режимі.

Жиналған мәліметтер бойынша статистиканы бақылау және талдау мүмкіндігі болуы керек (құру **сүзгілердің ішіндегі сүзгілер**), осылайша оны бейнелеудің келесі әдістерін қолдана отырып, ақпараттың қосымша бөлігін алады:

- Таңдалған ДК және сүзгі бойынша оқиғаларды кестелік түрде көрсету мүмкіндігі бар кесте;
- Таңдалған сүзгілер бойынша оқиғалар санын графиктің бағандары түрінде көрсету мүмкіндігі бар сызықтық график, сонымен қатар графикті сызықтық, гистограмма, жинақталған және жинақталмаған арасында ауыстыру мүмкіндігі бар;
- Оқиғалар санын кірістірілген сүзгілерді қолдайтын дөңгелек диаграмма ретінде көрсету мүмкіндігі бар дөңгелек диаграмма;
- Графикті диаграмма түрінде құру мүмкіндігі байланыстарды;
- Баспаға шығаруға болатын қатынастар ағашын құру мүмкіндігі және ағаш элементін басу арқылы оқиғаларға түсіп қалу мүмкіндігі;
- Деректерді келесі формаларда бейнелеудің қосымша мүмкіндіктері: радиолокация, оқиғалар өзені, статистика.
- Ақпаратты сандық өлшемдер бойынша көрсету мүмкіндігі: сөйлесу уақыты, беттер саны, белсенділік уақыты, оқиғалар саны, файл өлшемі.

Қатысуы керек **сүзгілер бөлімі** (мысалы, қойынды ретінде), ол топтастырылған өлшемдерді, саясаттарды қамтиды, бақылау тақталары және сөздіктер:

- Пайдаланушы өз бетінше жасаған сүзгілердің болуы;
- Әзірлеуші алдын ала орнатқан және жаңартқан сүзгілердің болуы;
- Есептерде де, нақты оқиғаларда да ақпаратты ұсыну мүмкіндігінің болуы;
- Тиімділік, қауіпсіздік және инциденттер бөлімшелерінің болуы;
- Қолданбалар мен сайттарды өнімділік санаттары бойынша белгілеу мүмкіндігі: өнімді әрекеттер, өнімсіз әрекеттер, бейтарап әрекеттер, премиум әрекеттер, оқиға. Кез келген санатқа орындалатын файлдардың немесе сайт атауларының кез келген санын қосуға/жоюға болады;
- Ішкі ақпаратты өңдеушілерді іске қосуға арналған сценарийлер болып табылатын жүйелік саясаттардың болуы және оларды өзгерту мүмкіндігі;
- Жаңа сүзгілерді жасау немесе бұрыннан барларын жою мүмкіндігі;
- Жасалған сүзгіге кез келген атауды орнату мүмкіндігі немесе бақылау тақтасына, оны кейіннен өзгерту мүмкіндігімен.
- Жасалған сүзгіге сипаттама қосу мүмкіндігі.
- Реттелетін шоғырландырылған есептерді жүйелі түрде жіберу мүмкіндігі html серверге қол жеткізусіз консольден есептермен жұмыс істеуге мүмкіндік беретін пішім.

Жұмыс істеген кезде **сүзгілермен және қауіпсіздік саясаттарымен**, пайдаланушыға келесі функционалдылық қол жетімді болуы керек:

- Жеке сүзгілерді және қауіпсіздік саясаттарын теңшеу, содан кейін оларды біріктіру мүмкіндігі бақылау тақталарықажетті көрсетілген ақпаратты бір жерде көруге мүмкіндік беретін;
- Бұрыннан бар сүзгінің көшірмесін жасау, жылдам өңдеу мүмкіндігі;
- Ақпараттық қауіпсіздікке жауапты тұлғаларға пошта арқылы хабарламаларды жіберу аралықтарын (іске қосылған кезде, күн сайын, апта сайын, ай сайын) және оқыс оқиға туралы алынған ақпаратты теңшеу мүмкіндігімен теңшеу мүмкіндігі;

- Мессенджерде хабарландыруларды теңшеу мүмкіндігі telegram ақпараттық қауіпсіздікке жауапты тұлғаларға жіберу аралықтарын (іске қосылған кезде, күнделікті, апта сайын, ай сайын) және оқыс оқиға туралы алынған ақпаратты конфигурациялау мүмкіндігімен;
- Кіріктірілген қауіпсіздік саясаттарының болуы, атап айтқанда, балағат сөздер сөздігі, нашақорлық жаргонының сөздігі, кері қайтару тақырыбының сөздігі, жұмыс іздеу сөздігі, несие карталарын іздеу, шифрланған мұрағаттар және т.б.;
- Ақпаратты және іске қосылған сүзгілерді кез келген уақыт аралығында қарау мүмкіндігі;
- Белгілі бір сүзгі немесе оқиға түрі бойынша іске қосылған инциденттер санын көрсете отырып, статистиканы қарау мүмкіндігі;
- Ақпараттық қауіпсіздікке жауапты тұлғаның поштасына хабарламаларды жіберуді теңшеу арқылы кірістірілген қауіпсіздік саясаттарын өзгерту мүмкіндігі және санаттарды келесі параметрлер бойынша өзгерту мүмкіндіктері: инцидент, өнімсіз, бейтарап, өнімді, премиалды түрде;
- Конфигурацияны автоматты түрде өзгерту мүмкіндігі, жасалған саясат, сөздік және шекті мән бойынша іске қосу саясаты арқылы анықталғанға реакция нәтижесінде.
- Сүзгілер тобы мен қауіпсіздік саясаттары үшін хабарландыру параметрлерін бір уақытта өңдеу мүмкіндігі;
- Жабдықтың конфигурациясын өзгерту туралы хабарламаларды алу мүмкіндігі;
- Таңдалған өлшемдер бойынша талдаудан фактілерге өту мүмкіндігі.

Оқиғалардан инциденттерді қалыптастыру құралы болуы керек (**оқиғалар консолі**). Оқыс оқиға туралы ақпаратты қарау кезінде web-интерфейсте келесі ақпарат қолжетімді болуы тиіс:

- Бұзушылыққа жол берген пайдаланушы;
- Оқиғаның күні мен уақыты;
- Сүзгіні немесе қауіпсіздік саясатын іске қосатын файл түрі (электрондық пошта, басып шығаруға жіберілген құжат және т.б.);
- Инцидентті тудырған файлдың мазмұны (электрондық пошта, басып шығаруға жіберілген құжат және т.б.);
- Басқа қосымша ақпарат (қажетті шығыс элементтерін алып тастау/қосу мүмкіндігімен).
- Инцидентте сыншылдық болуы және алдын ала белгіленуі тиіс.

Сервердің веб-консолінe қол жеткізбестен деректерді егжей-тегжейлі талдау мүмкіндігімен жұмыс уақытын есепке алу бойынша есептердің кешенді тобын күнделікті құрудың құралы болуы керек.

Икемді болу мақсатында **жұмыс уақытын есепке алу баптаулары** қатысуға тиіс:

- Қызметкерлердің жұмыс кестесін келесі критерийлер бойынша құру мүмкіндігі: аптаның күні, жұмыс күнінің басталуы, жұмыс күнінің аяқталуы, үзілістің басталуы, үзілістің аяқталуы, жұмыс уақыты;
- Жұмыс уақытын, мереке күндерін, ауру күндерін, демалыс және демалыс күндерін белгілеу мүмкіндігі бар күнтізбе;
- Кестелерді компьютерлер, топтар, бөлімдер, пайдаланушылар, толық пайдаланушы аттары және ұйым бойынша тағайындау мүмкіндігі.
- Әрекет немесе сөйлесу уақыты, файл өлшемі, белгілі бір қолданбалардағы, сайттардағы және басқа оқиғалар түрлеріндегі триггерлер саны асып кетсе, жауапты тұлғаларға пошта арқылы хабарламалар жіберу мүмкіндігі табалдырық бойынша іске қосылады.

Қатысуға тиіс **жұмыс уақытын есепке алу үшін ендірілген есептер**, атап айтқанда:

- Таңдалған пайдаланушылар бойынша таңдалған кезең туралы ақпаратты қамтитын, күндерге бөлінген және келесі ақпаратты көрсететін біріктірілген есеп: таңдалған кезеңнің күндері, пайдаланушы, пайдаланушының белсенділік шкаласы сағат бойынша, әрбір жұмыс күнінің басталуы мен аяқталуы, жалпы жұмыс уақыты, белсенді уақыт, тоқтау уақыты, кешігу және қосымша жұмыс уақыты туралы ақпарат, өнімді уақыт, өнімсіз уақыт және бейтарап уақыт, кесте. Өрістер таңдау мүмкіндігімен өлшем түрі бойынша топтастырылуы керек. Есепте белсенді емес қызметкерлерді көрсетуге қосу мүмкіндігі. Белгілі бір пайдаланушының біреуін таңдаған жағдайда, есеп өнімділік, пайдаланылған қолданбалардың жоғарғы жағы және кіргендердің жоғарғы жағы үшін уақыт пен пайыздық үлестермен біріктірілген статистикамен толықтырылады сайттардың күндердің әрқайсысы үшін уақыт шкалаларында көрсетіледі. Бұл ретте әрекеттерді сүзуге және осы әрекеттер бойынша фактілерге өтуге болады;
- Таспа диаграммасы, таңдалған пайдаланушылар бойынша таңдалған кезең туралы ақпаратты қамтитын, күндерге бөлінген және пайдаланушының әрекеттерін сағат бойынша көрсететін есеп. Белгілі бір бір пайдаланушы таңдалған жағдайда, есеп өнімділік, пайдаланылған қолданбалардың жоғарғы жағы және күндердің әрқайсысы

үшін уақыт шкалаларында көрсетілетін кірген сайттардың жоғарғы жағы, осы әрекеттердің үлестері бойынша біріктірілген статистикамен толықтырылады;

- Кесте - таңдалған пайдаланушылар үшін таңдалған кезең туралы ақпаратты қамтитын, күндерге бөлінген және келесі ақпаратты көрсететін есеп: таңдалған кезеңнің күндері, пайдаланушы, әр жұмыс күнінің басталуы мен аяқталуы, жалпы жұмыс уақыты, белсенді уақыт, бос уақыт, кешіктіру және қосымша жұмыс уақыты туралы ақпарат, өнімді уақыт, өнімсіз уақыт және бейтарап уақыт. Белгілі бір бір пайдаланушы таңдалған жағдайда, есеп өнімділік, пайдаланылған қолданбалардың жоғарғы жағы және күндердің әрқайсысы үшін кірген сайттардың жоғарғы жағы бойынша біріктірілген статистикамен толықтырылады;
- Таңдалған пайдаланушылар бойынша таңдалған кезеңдегі жиынтық ақпаратты қамтитын кезеңдегі белсенділік туралы есеп: пайдаланушы, жалпы жұмыс уақыты, белсенді жұмыс уақыты, тоқтау уақыты, кешігу туралы ақпарат, үстеме жұмыс, өнімді уақыт, бейтарап және өнімсіз уақыт. Есеп график түрінде күндердің әрқайсысы бойынша көрсетілетін өнімділік, пайдаланылған қолданбалардың жоғарғы жағы және кірген сайттардың жоғарғы жағы үшін уақыт пен пайыздық мөлшерлемелер бойынша жиынтық статистикамен толықтырылған. Бұл ретте есепті әрекеттердің, қолданбалардың немесе сайттардың таңдалған түрлері бойынша сүзуге болады.
- Таңдалған пайдаланушылар бойынша үзілістерге бөлінген интервалдар бойынша келесі ақпаратты қамтитын кезеңдегі үзілістер туралы есеп: қызметкер, күні, интервалдың басталуы мен аяқталуы, орындалған әрекеттер, есептелген жұмыс уақыты мен бос уақыт;
- Бөлімдер бойынша өнімді уақыт, жалпы жұмыс істеген уақыт шкаласы бойынша таңдалған уақыт аралығындағы жұмыс орындарындағы пайдаланушылардың жалпы өнімді/өнімсіз және бейтарап уақыттарын қамтитын есеп және олардың әрқайсысы үшін жалпы уақыт және оның жалпы санынан пайызы ретінде бөлек;
- Бөлімдер бойынша белсенді уақыт, жұмыс уақытының жеке және жалпы шкаласы бойынша жалпы белсенді уақытты, өңдеуді, жалпы жетіспеушілікті, таңдалған уақыт кезеңінде пайдаланушылардың жұмыс орындарында болмауын, оның ішінде жоспарланған уақытқа пайыздық қатынасты қамтитын есеп;
- Бөлім бойынша ең жақсы өнімсіз, таңдалған кезеңдегі ақпаратты қамтитын және өнімсіз қызметкерлерді бөлім бойынша сұрыптайтын есеп, келесілерді көрсетеді: компьютер, пайдаланушы, лауазым атауы, бөлім, әрекет түрінің атауы, әрекет уақыты;
- Кешіктірілген пайдаланушылар, кешіктірілген уақыттар, белсенді және белсенді емес, өнімді және өнімсіз пайдаланушылар туралы жиынтық статистиканы, сондай-ақ таңдалған пайдаланушылар бойынша таңдалған кезеңдегі жиынтық жиынтық ақпаратты қамтитын жиынтық есеп келесі түрде: пайдаланушы, жалпы уақыт, белсенді уақыт, тоқтау уақыты, өнімді уақыт, бейтарап өнімсіз уақыт, кешігулер саны, жалпы кешігулер және үстеме жұмыс уақыты;
- Ұйымдық бөлімшелер бойынша бөлінген әрбір қызметкер бойынша келесі ақпаратты қамтитын топтық жиынтық есеп: пайдаланушы, жалпы уақыт, белсенді уақыт, бос уақыт, өнімді уақыт, бейтарап және өнімсіз уақыт, кешігулер саны, жалпы кешігулер және үстеме жұмыс уақыты. Қызметкерлердің әрбір тобы бойынша сомалар есептеледі;
- Барлық таңдалған қызметкерлер бойынша келесі мәліметтер жиынтығын қамтитын жиынтық статистикалық есеп: пайдаланушы, белсенді күндер, жұмыс уақыты, жалпы уақыт, белсенді уақыт, өнімді уақыт, бейтарап уақыт, өнімді түзетілген уақыт, тәулігіне өнімді түзетілген уақыт, қатынас сағат 8-ге дейін өнімді түзетілген уақыт, өнімсіз уақыт, тәулігіне өнімсіз уақыт, тоқтау уақыты, тәулігіне тоқтау уақыты;
- Таңдалған пайдаланушылар бойынша таңдалған кезең үшін келесі ақпаратты қамтитын кешігулер туралы есеп: уақыт кезеңі, пайдаланушы, кешігулер саны, жалпы кешігулер, жалпы уақыт, белсенді уақыт және тоқтау уақыты – егер бір пайдаланушы таңдалса, және бірнешеу үшін қосымша статистикалық ақпарат: кешігулердің жалпы уақытының жалпы уақытқа қатынасы, кешіктірілгендердің жоғарғы жағы және кешігулердің жоғарғы жағы;
- Ерте кетулер мен келулерді есепке алу, күндермен бөлінген және таңдалған пайдаланушылар бойынша таңдалған кезең үшін келесі ақпаратты қамтитын есеп: уақыт кезеңі, пайдаланушы, кешігу ұзақтығы, түскі асқа ерте кету және түскі асқа кешігу, жұмыстан ерте кету, жұмыста ұстау және жұмысқа ерте келу;
- Топтар бойынша ерте кетулер мен келулерді есепке алу, таңдалған пайдаланушылар бойынша таңдалған кезең үшін келесі ақпаратты қамтитын күндер мен ұйымдық бірліктерге бөлінген есеп: уақыт кезеңі, пайдаланушы, кешігу ұзақтығы, түскі асқа ерте кету және түскі асқа кешігу, жұмыстан ерте кету, жұмыста ұстау және жұмысқа ерте келу;
- Кеңейтілген уақыт кестесі, барлық таңдалған пайдаланушылар үшін ай сайынғы есептердің жиынтығы болып табылатын есеп, мұнда әрбір пайдаланушы үшін келесі толтырылған өрістер қарастырылған: ұйым, бөлім, лауазым, қызметкер және жұмыс уақыты. Бұл жағдайда жұмыс уақыты әр күн үшін келесі өлшемдерде ескеріледі: кіру, шығу, кеңседе болу уақыты, рұқсат етілген бағдарламалық жасақтамада жұмыс уақыты, тыйым салынған бағдарламалық жасақтамада жұмыс уақыты, үзіліс. Әрбір өлшем бойынша әрбір ай бойынша қорытындылар шығарылады: жұмыс және демалыс күндеріндегі күндер мен сағаттар;
- Т13 формасындағы кестелер ("1С-тегідей" есептер): жұмыс уақыты, белсенді уақыт, жұмыс орнында болмау, принтерді пайдалану.
- КББЖ-дан жиналған мәліметтер негізінде үй-жайға кіру, шығу және болу туралы есеп.

- Таңдалған кезең ішінде серверге деректерді жібермеген машиналар туралы ақпаратты қамтитын кезеңдегі оқиғалардың болмауы туралы есеп.
- Есептерде көрсетілетін ақпаратты редакциялау мүмкіндігінің болуы;
- Талданатын деректер кезеңін өзгерту және бекіту мүмкіндігі;
- Есептердегі талдау объектісін өзгерту мүмкіндігі: компьютерлер, пайдаланушылар, пайдаланушылардың толық аты-жөндері, қызметкерлер.
- Есеп шеңберінде жұмыс күнінің басталуы мен аяқталуын талдау үшін белсенділіктің минималды уақытын белгілеу мүмкіндігі.
- Қашықтағы сессияның уақыты бойынша есепте деректерді көрсету мүмкіндігі.

Орнатылған БҚ мен жабдықтарды түгендеу мүмкіндіктеріне қойылатын талаптар

- Кірістірілген жұмыс станциясының құрылғыларын түгендеу туралы есеп келесі параметрлермен бірге болуы керек: күйі (бар немесе жоқ), компьютер (жұмыс станциясының атауы), өндіруші, құрылғы түрі, HWID және қолжетімділігі соңғы тексерілген күні, компьютерлер бойынша топтастыру және есепті жүктеп салу мүмкіндігі бар. html, pdf және excel форматтарда жүзеге асырылады.
- Жұмыс станциясы қолданбаларының кірістірілген түгендеу есебі келесі шығыс деректерімен бірге болуы керек: күй (бар немесе жоқ), компьютер (жұмыс станциясының атауы), өнім, жеткізуші, нұсқасы және соңғы қолжетімділікті тексеру күні, компьютерлер бойынша топтастыру және есепті жүктеп салу мүмкіндігімен. html, pdf және excel форматтарда жүзеге асырылады.
- Ұйымның жұмыс станцияларындағы қосымшалар туралы кіріктірілген есеп келесі шығыс мәліметтерімен бірге болуы керек: Қосымшаның атауы, ол табылған станциялардың тізімі БОЙЫНША, бастап мәртебесі, жеткізуші бойынша ақпаратпен, нұсқасы және қол жетімді күні. Есепті жүктеу мүмкіндігі болуы керек html, pdf және excel форматтарда

Талдау және тану мүмкіндіктеріне қойылатын талаптар

Бағдарламалық жасақтама жиналған ақпаратты талдаудың кеңейтілген мүмкіндіктерін қамтамасыз етуі керек **контенттік талдау**бар болса:

- Кілт сөздер мен сөз тіркестері бойынша іздеу мүмкіндігі
- Ұсталған файлдарда немесе құжаттарда анықтау үшін сүзгіге сөздерді немесе сөз тіркестерін қосу мүмкіндігі;
- Жеке сөздіктерді құрастыру мүмкіндігі;
- Әртүрлі сөздіктерден табылған сәйкестіктерді әртүрлі түстермен бөлектеу мүмкіндігі.
- Конструктор жасаған сұрауды тексеру мүмкіндігімен тұрақты өрнек құрастырушысы арқылы мазмұнды іздеу мүмкіндігі.
- Оқиғаға әрекет еткен барлық саясаткерлер бойынша егжей-тегжейлі ақпарат.

Бағдарламалық жасақтама функционалдылыққа ие болуы керек **суреттер мен құжаттарды тану**қамтамасыз ететін:

- Өзіңіздің тегін кірістірілген OCR құрылғыңыздың болуы Tesseract4-тен ескі емес;
- 2 немесе одан да көп тану серверлерін пайдалану мүмкіндігі.
- Төңкерілген кескіндерді тану мүмкіндігі;
- Келесі тілдерді - орыс және ағылшын тілдерін таңдау мүмкіндігі;
- Келесі форматтарды - PDF, JPEG, PNG тану мүмкіндігі;
- Бұлтты ABBYY қосылу мүмкіндігі Cloud OCR SDK.
- Машиналық оқытуды пайдалана отырып, нейрондық желілер арқылы төлқұжаттар мен мөрлердің мөрлерін тану мүмкіндігі.
- Машиналық оқытуды пайдалана отырып, веб-камера түсірілімдері арқылы беттерді тану мүмкіндігі.

Функционалдық талаптар

- Жабдықтаушы орнатуға және конфигурациялауға байланысты техникалық жұмыстарды орындауы керек

тапсырыс берушінің аппараттық құралдарында, оның ішінде:

- Орнату және баптау (қосымшалар сервері);
- - Лицензиялар санына сәйкес клиенттік орындарды орнату және қосу;
- Клиенттік орындарды баптау және қосу нысанда тапсырыс берушілер тапсырыс берушінің инженерін қоса отырып.
- Тапсырыс берушіні техникалық қолдау және сүйемелдеу күннен бастап жүзеге асырылады 12 ай ішінде шартқа қол қою.
- Әлеуетті өнім беруші беретін лицензиялардың қолданылу мерзімі: мерзімсіз.
- **Сапаға қойылатын талаптар:** Көрсетілетін қызметтердің сапасы Қазақстан Республикасында қолданылып жүрген қолданыстағы стандарттарға, техникалық және өзге де нормаларға сәйкес келуге тиіс.

- Әлеуетті өнім берушіден құжаттарды шетелдік форматта ұсынған жағдайда тілінде қазақ немесе орыс тілдеріндегі нотариалды куәландырылған аудармасы ұсынылуы тиіс. орыс тілінде).
- Лицензияларды жеткізу, орнату және жеткізу мерзімі баптаулар: 15 (он бес) мерзім ішінде
- Шартқа қол қойылған күннен бастап жұмыс күндері.
- Шарттың жалпы сомасына жеткізуге байланысты барлық шығындар кіреді лицензияларды, орнатуды және баптауды бойынша.

3. Техникалық стандарттар

№ р/с	ҚР тіркелген	Белгіленуі	Құжат нөмірі	Санаты	Атауы	Қолдану саласы	Әзірлеуші	Беттер	МКС	Мәртебесі	Бұйрық	Енгізу күні бастап	К б
						Настоящий стандарт распространяется на процессы разработки и документирования программного обеспечения (ПО) встроенных систем реального времени. Стандарт распространяется на все действия, имеющие отношен					Приказом		

1	Иә	СТ РК ГОСТ Р 51904-2011	347668	Қазақстан Республикасының ұлттық стандарты	Программное обеспечение встроенных систем. Общие требования к разработке и документированию Дата введения с 2013.01.01	ие к разработке программного обеспечения. Настоящий стандарт применяют полностью ко всему поставляемому программному обеспечению, включая среду разработки, если контрактом не предусмотрено использование специальных стандартов для определенных заказчиком типов ПО. Стандарт неприменим для аппаратных элементов программно-аппаратного обеспечения	Нет ()	186	Программное обеспечение	Действует	Председателя Комитета технического регулирования и метрологии Министерства индустрии и новых технологий Республики Казахстан от 17 ноября 2011 года № 625-од	01.01.2013

Қол қойған Муратов Арман Халелұлы

Қол қойылған күні 11.11.2024

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1047432
способом Запрос ценовых предложений на понижение

Лот № 1 (96-1 У, 3815155) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Karabatan Utility Solutions"

Организатор: Товарищество с ограниченной ответственностью "Karabatan Utility Solutions"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	96-1 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Атырауская область, Атырау Г.А., г.Атырау, трасса Атырау-Доссор, строение 295 /2
Условия поставки	-
Срок поставки	С даты подписания договора в течение 15 рабочих дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

- Программное обеспечение должно поддерживать работу в сетях любой конфигурации и сложности.
- Предоставление 25 (двадцать пять) лицензий на право использования программного обеспечения.
- Программное обеспечение должно поддерживать подключение агентов к серверу через сеть Интернет, в том числе в случаях организации подключения через VPN.
- В целях импортозамещения серверная и агентская части должны поддерживать возможность установки на отечественные операционные системы (семейство Linux). Должны использоваться базы данных либо свободного распространения, либо включенные в Единый реестр отечественных программ.
- Серверная часть программного обеспечения, реализующая функционал управления агентами, хранения собираемой информации и формирования отчётов должна поддерживать возможность установки всех необходимых компонентов на одном сервере.
- Должна быть возможность предоставления серверных компонентов в едином установочном ISO-образе.
- Должна предоставляться возможность установки серверных компонентов на ОС Ubuntu 16.04, 18.04, 20.04 без установки дополнительных зависимостей.
- Для сбора информации должен устанавливаться только один агент (модуль) мониторинга на один ПК.
- Агент должен быть унифицирован для рабочих станций и терминальных серверов.
- В процессе своего функционирования, система (её агенты) не должна оказывать значимого (существенного) негативного влияния на функционирование защищаемых рабочих станций и серверов.
- Для доступа к собранной информации, управления политиками безопасности, настройки конфигурации агента должна использоваться единая консоль администратора с возможностью гибкого разграничения полномочий.
- Система должна иметь возможность вертикального и горизонтального масштабирования, устанавливаться и выполнять свои функции на современных системах виртуализации.

- Задержка обновления отчётов не должна превышать 15 минут при максимальной загрузке системы на рекомендованной аппаратной конфигурации.

Требования к лицензированию

- Лицензирование должно производиться по количеству одновременно активных рабочих станций и/или пользователей;
- Должна присутствовать возможность гибкого лицензирования с переустановкой лицензии с одной рабочей станции или пользователя на другую рабочую станцию или пользователя неограниченное количество раз;
- Серверные компоненты не должны требовать обязательного наличия у заказчика дополнительных платных лицензий на программное обеспечение.
- Назначенные и отозванные лицензии, должны наглядно и визуально отображаться в консоли сервера.

Требования к поддерживаемые операционным системам для агента

- Агент для Windows в 32-х или 64-х битном варианте с поддержкой следующих операционных систем – Windows Vista SP2, Windows 7 SP2, Windows 8, Windows 8.1 SP1, Windows 10. Агент так же должен поддерживать работу терминальных серверов в следующих операционных системах: Windows 2008, Windows 2008 R2, Windows 2012 R2, Windows 2016;
- Агент для Linux с поддержкой следующих операционных систем: CentOS, Ubuntu Dekstop, Debian, Gentoo linux, Astra linux, Arch linux, Rosa linux, AltLinux и другие Linux-like дистрибутивы;
- Агент для MacOS с обязательной поддержкой операционных систем: macOS 10.13, 10.14, 10.15, 11.x(Bigsur), 12.x (Montray), 13.x(Ventura).
- Поддержка операционных систем утилитой удалённой установки: Windows Vista SP2, Windows 7 SP2, Windows 8, Windows1 SP1, Windows 10.

Требования к архитектуре программного обеспечения

- Должно обеспечиваться выполнение OLAP запросов в реальном режиме времени.
- Для высокоскоростного исполнения аналитических запросов в реальном режиме времени система должна иметь возможность переключения на использование дополнительной базы данных типа columnar store, в частности, включенную в Единый реестр отечественных программ БД ClickHouse.
- Метаданные должны храниться в БД, а файлы в отдельном файловом хранилище.
- Хранение файлов должно обеспечиваться в режиме ротации типа «кольцевой буфер» с возможностью автоматического перемещения на долговременное хранилище.
- Протокол обмена между агентом и сервером, а также доступ в панель администратора должен быть защищен шифрованием семейства TLS (на основе клиентских сертификатов).
- Должна обеспечиваться возможность получения информации от сервера сбора данных посредством формирования API-запросов (REST API, Database API и взаимодействие с моделью данных).
- Должна существовать возможность передачи данных в SIEM-системы.
- Должна иметься возможность передачи данных со СКУД в БД с возможностью анализировать собранные данные в системе на основе событий и отчетов.
- Должна иметься возможность импорта табеля по отсутствию сотрудников из 1С для формирования календаря.
- Интерфейс администратора должен обеспечивать вывод суммарной (агрегированной) информации на основе больших массивов данных, структурированных по многомерному принципу.
- Агент должен уметь отправлять собранные данные не менее, чем на два различных адреса сервера как по доменному имени, так и по адресам IPv4 и IPv6.
- Агент должен иметь возможность настройки правил мониторинга, по которым необходимые события не будут индексироваться;
- Агент должен иметь возможность получения пароля от сервера, для защиты от привилегированного пользователя с правами администратора;
- Должна быть возможность использовать Rust для обработки данных;
- Должна быть возможность использовать парсер контента на основе Apache Tika.
- Должна присутствовать возможность настройки сбора данных посредством фильтрации трафика на ICAP-сервере.
- Должно быть предусмотрено горизонтальное масштабирование сервера за счет использования кластерной архитектуры, единая консоль для работы с данными на всех кластерах и единая точка распространения политик.

Требования к администрированию системы

Должна присутствовать **панель управления администратора** внутри web-интерфейса сервера со следующими возможностями:

- Интерфейс администратора должен поддерживать распределение полномочий, основанных на ролях, в том числе заданных в Active Directory;
- Должен быть интерфейс настройки подключения Active Directory;
- Авторизация пользователей или администраторов в веб-интерфейсе консоли, распределение ролей, назначение прав доступа к данным и конфигураций мониторинга должны быть возможны с учётом пользователей и групп из Active Directory;
- Предоставление доступа администраторам для доступа к данным как к группам пользователей, на основе данных из Active Directory, так и к конкретным аккаунтам.
- Возможность ограничения доступа администраторам к конкретным данным и событиям на основе их атрибутов.
- Установка и удаление агентов должны производиться как централизовано с помощью групповых политик Active Directory с помощью инсталлятора модуля агента, так и локально, путём запуска инсталлятора на машине пользователя;
- Должна быть возможность установки утилиты мониторинга агента. Установка должна производиться как локально, групповыми политиками, так и через утилиту удаленной установки.
- Возможность настройки контроля пользователей по параметрам OU.
- Возможность синхронизации данных с Active Directory по нескольким OU.
- Поддержка нескольких доменов Active Directory в рамках единой системы.
- Должна быть возможность планировки установки агентов в локальной сети по расписанию.
- Должны быть возможность исключения IP - адресов в рамках сканирования локальной сети для удаленной установки агента.
- Должна иметься возможность установки агентов контроля на VDI с возможность генерации уникального идентификатора машины в базе данных сервера;
- Должна быть возможность просмотра активных или готовых к установке компьютеров, с возможностью выбора конкретного или нескольких рабочих мест с выполнением следующих действий: выбор всех компьютеров, освобождение лицензии, назначение лицензии, автоматическое назначение лицензии, вызов деинсталляции агента, отмена деинсталляции агента, заблокировать или разблокировать ПК, обновить агента до последней версии, отменить текущее обновление, установить агента, проверить агента, назначить свойства (выбор конфигурации и группы);
- Должны быть возможны выбор и установка согласно списку ПК из Active Directory путём подключения инсталлятора агентов к контроллеру домена для выбора компьютеров, назначенных на установку;
- Должен присутствовать автоматический отзыв лицензии с отключенных в AD пользователей.
- Должна существовать возможность после подтверждения администратором системы проводить централизованное обновление агентов автоматически;
- Должна присутствовать возможность удаления всех неустановленных агентов;
- Должна обеспечиваться возможность настройки длительности хранения информации в базе данных, в том числе возможность автоочистки файлового хранилища без удаления данных из базы данных;
- Должна иметься возможность шифрования локальной базы данных агента.
- Должна иметься возможность сохранить локальную базу данных агента после его удаления;
- Должна присутствовать возможность назначения агентам резервного адреса для передачи данных.
- Должно формироваться предупреждение о заполнении дисков БД, дополнительной БД и файлового хранилища;
- Должны создаваться уведомления администратору системы о системных событиях (системные ошибки, предупреждения, срабатывания политик безопасности и т.д.);
- Должна обеспечиваться настройка передачи на сервер максимального размера единовременного объёма перехваченных данных от агента;
- Должна быть возможность ограничения скорости передачи данных от агента серверу.
- Должен вестись журнал действий администраторов системы непосредственно в консоли администратора;
- Должна происходить автосмена имени агента, при смене названия компьютера;
- Должна быть возможность сменить IP-адрес и порт сервера на агенте без его переустановки;
- Должна быть поддержка работы агента и сервера на одном порту и IP-адресе, но с разными SNI в сертификате;
- Должна обеспечиваться возможность скачать из интерфейса администрирования агенты версии Windows и Linux, а также утилиту удалённой установки;
- В веб-консоли должны указываться версии агентов, которые будут использоваться при установке.
- Управление сбором данных должно осуществляться путём назначения конфигураций пользователей и компьютеров с возможностью их добавления, изменения и удаления;

- Для предустановленных (стандартных) конфигураций должна быть возможность сброса на изначальные параметры (значения по умолчанию);
- Конфигурации пользователей должны назначаться для определяемых в ней пользователей и иметь настройки правил использования USB/CD устройств: полную блокировку, разрешать только чтение и задавать перечень таких устройств по их идентификаторам;
- Должна присутствовать глобальная конфигурация с возможностью настройки модулей мониторинга для всех пользователей, независимо от назначенной им конфигурации;
- Должна быть возможность настройки параметров отправки почты в настройках сервера, которая используется для отправки всех отчётов, дашбордов и уведомлений;
- Должна быть возможность указывать точное время отправки отчёта или дашборда на почту;
- Должна быть реализована возможность отправки отчетов, дашбордов и уведомлений в форматах PDF, HTML и EXCEL;
- Должно быть организовано хранилище паролей, использующихся при установке агентов через веб-интерфейс, с возможностью сохранения и редактирования паролей;
- Должна быть возможность разбиения базы данных по месяцам (шардирование) и функционал удаления данных за выбранный месяц из интерфейса администратора;
- Должны фиксировать и быть доступными для просмотра изменения в настройках и конфигурациях, производимые администраторами в веб-консоли;
- Должны фиксироваться в консоли действия администратора по просмотру определенной информации и отчетов.
- Должна предоставляться возможность выгрузки и фильтрации «последних действий администраторов системы»
- Должен быть доступен просмотр количества событий в очереди на обработку сервером с указанием названия политик и парсеров;
- Должна быть возможность выгрузки логов сервера, конфигураций агентов, правил мониторинга, фильтров и политик;
- Должна быть доступна информация о лицензии, сроках её активации и истечения, количестве компьютеров, которые могут подключаться к серверу и количестве подключенных компьютеров;
- Должна быть функция ручного запуска пересчёта всех отчётов;
- Должна присутствовать возможность удаления всех пользовательских настроек, с возвращением сервера к первоначальным настройкам;
- Должна быть возможность перезапуска всех служб;
- Должен быть выбора языка веб-интерфейса (русский или английский);
- Должен быть выбор визуальной темы веб-интерфейса;
- Должна выводиться информация о версии сервера, версии Windows и Linux агента;
- Должен быть интерфейс смены пароля администратора и функция завершения работы с интерфейсом (завершения сеанса текущего пользователя системы).
- Возможность точечного удаления данных из БД, согласно заданным параметрам данных, напрямую из консоли администрирования.
- Единое поле контроля и настройки уведомлений по инцидентам и регулярным рассылкам;
- Использование клавиш для прокрутки событий;
- Должны отображаться удачные и неудачные попытки входа в систему;
- Должен отображаться выход администратора из системы;
- Должен логироваться факт выгрузки данных из системы с детализацией выгруженных данных;
- Должна логироваться смена пароля администратора системы.
- Должна завершаться сессия, при изменеии пароля администратора системы.
- Должны отключаться отсутствующие администраторы при синхронизации с AD;
- При неверном вводе пароля должен ограничиваться доступ с адреса, с которого была неуспешная авторизация.
- Должны фиксироваться и логироваться операции снятия и назначения лицензий для мониторинга как для пользователя так и для агента с детализацией причины отзыва;
- Должна иметься возможность включить автоматическое освобождение или отзыв лицензии мониторинга неактивных пользователей с логированием данной операции;
- Возможность уведомления при появлении новой машины под мониторингом;
- Возможность просмотра и контроля правил применяемых к работе агента в его профиле;
- Возможность настройки времени выхода из сессии администратора, при отсутствии активности;
- Обозначение активных элементов обработки данных в веб-консоли;
- Проверка пароля на сложность при создании пароля администратора, не позволяющая использовать слабые пароли.
- Должны иметься возможность управления сервером из веб консоли, в том числе и в рамках планового выполнения заданных комманд.
- Должна иметься возможность на стороне сервера изменить агенту адрес для передачи данных;
- Должна иметься возможность выгрузки информации по контролируемым агентам, пользователям и их статусом в формате CSV.

- Должна иметься возможность отправки уведомления на почту администратора системы при невозможности получения лицензии агентом\пользователем.

Требования к функциональным возможностям системы

Должны фиксироваться следующие **типы событий** действий пользователя:

- вход/выход из системы;
- удаленный вход/выход из системы
- активность пользователя в приложениях и на сайтах;
- подключение к удаленному рабочему столу, перехват управления;
- запись видео рабочего стола;
- снимок экрана;
- снимок с веб-камеры;
- операции с файлами;
- теневые копии перехваченных файлов;
- печать документов;
- буфер обмена;
- ввод с клавиатуры;
- реестр оборудования;
- реестр установленных программ;
- запись с микрофона;
- посещение веб-ресурсов;
- сетевые подключения;
- интернет-мессенджеры;
- почта;
- установка ПО;
- запуск и завершение приложения;
- внешние диски и устройства;
- присутствие на рабочем месте.

Должны фиксироваться следующие **атрибуты логируемой информации**:

- агент;
- Назначенная конфигурация
- IP-адрес;
- дополнительная метка;
- название ПК;
- статус;
- версия OS;
- версия агента;
- учетная запись пользователя;
- комментарий;
- отдел;
- организация;
- телефон;
- полное имя;
- Группа AD;
- почта;
- должность;
- домен;
- руководитель;
- пользователь;
- приложение;
- полный путь;
- название;
- описание;
- сайт;
- полный домен;

- протокол;
- URL;
- основной домен;
- тип контента;
- сетевая активность;
- сетевой порт;
- файл;
- хеш файла;
- имя файла источника;
- путь источника;
- расширение источника;
- операции;
- тип контента;
- имя файла;
- тип диска;
- расширение;
- путь;
- устройства;
- ID устройства;
- тип диска;
- класс устройства;
- тип устройства;
- переписка;
- домен получателя;
- отправитель;
- все получатели;
- формат сообщения;
- направление;
- домен отправителя;
- получатель;
- чаты;
- канал общения;
- дата;
- час суток
- часовой пояс;
- день недели;
- по годам;
- по месяцам;
- по дням;
- по часам;
- по минутам.

Должны **индексироваться** системой файлы следующих форматов:

- Adobe Acrobat (*.pdf);
- Ansi Text (*.txt);
- ASCII Text;
- CSV (Comma-separated values) (*.csv);
- EML files (электронные письма, сохраненные Outlook Express) (*.eml);
- HTML (*.htm, *.html);
- JPEG (метаданные) (*.jpg);
- MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht);
- MSG files (электронные письма, сохраненные Outlook) (*.msg);
- Microsoft Excel (*.xls) Microsoft Excel 2003 XML (*.xml);
- Microsoft Excel 2007 и выше(*.xlsx);
- Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx);
- Microsoft PowerPoint (*.ppt);
- Microsoft Rich Text Format (*.rtf);
- Microsoft Word for DOS (*.doc);
- Microsoft Word for Windows (*.doc);

- Microsoft Word 2003 XML (*.xml);
- Microsoft Word 2007 и выше(*.docx);
- Multimate version 4 (*.doc);
- OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений).

Требования к перехвату в контролируемых каналах

Должна обеспечиваться возможность контроля **электронной почты**, в частности:

- Перехват почтовых сообщений по протоколам – SMTP/SMTPs, POP3/POP3s, IMAP/IMAPs, MAPI;
- Возможность перехватывать почтовые сообщения IBM Lotus Notes посредством сбора почты из IMAP-почтового ящика.
- Должна присутствовать связь между сообщениями полученными посредством IMAP и доменными пользователями в системе;
- Перехват и анализ файлов-вложений почтовых сообщений;
- Мониторинг почтовых сообщений и вложений с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Поиск по заданным параметрам текста и атрибутам почтовых сообщений, и тексту их вложений;
- Возможность выгрузки писем в следующих видах: документ Excel, HTML, CSV, изображение в формате PNG
- Возможность скачать переписку целиком в ZIP архиве или распечатать на принтере;
- Возможность построения графа переписки, с ручной настройкой параметров отображаемой информации.

Должна обеспечиваться возможность мониторинга обмена информацией посредством **мессенджеров (IM-клиентов)**, в том числе, web-версий, в частности:

- Должен происходить перехват текстовых сообщений по протоколам (Skype, Telegram, ICQ/QIP, Jabber, Mail.ru Агент, MS Teams, Bitrix 24 Desktop, Whatsapp, Express, VKTeams);
- Должен происходить перехват отправляемых файлов для (Skype, Telegram, Bitrix24 Desktop, Express, VKTeams);
- Должна быть возможность задания особых критериев мониторинга и организация мониторинга текстовых сообщений и файлов.
- В случае обнаружения передачи информации по заданным критериям мониторинга в сообщениях и файлах должна быть возможность организовать отправку уведомления одному или нескольким ответственным за информационную безопасность лицам;
- Должен осуществляться поиск по заданным параметрам текста и атрибута сообщений и (содержимого) файлов, переданных через IM-клиенты.

Должен осуществляться контроль информации **по протоколам HTTP/HTTPs**, в частности:

- Перехват данных по протоколам HTTP/HTTPS;
- Перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
- Перехват исходящих сообщений VK;
- Перехват исходящих электронных писем и вложений, переданных или полученных через почтовые веб-сервисы (как минимум, mail.yandex.ru, mail.google.com, mail.rambler.ru, e.mail.ru, outlook.com);
- Перехват и мониторинг поисковых запросов пользователя;
- Сохранение адресов всех страниц (URL), посещенных пользователем;
- Мониторинг сообщений и файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Поиск по тексту и атрибутам сообщений и файлов, переданных и перехваченных по протоколу HTTP(S);
- Возможность блокировки посещения веб-ресурсов;
- Исключение мониторинга сайтов по чёрным и белым спискам;
- Мониторинг всех посещённых сайтов и времени, проведённого на веб-страницах;
- Возможность формирования различных отчётов по времени активности пользователя за ПК. Рейтинг посещенных сайтов за день, хронология событий за выбранный временной интервал для отдельного пользователя или для групп пользователей или всей организации в следующих видах: документ Excel, HTML, CSV, формат PNG;

- Возможность скачать отчёты целиком в ZIP архиве или распечатать на принтере.

Должен быть возможен контроль информации, передаваемой **по протоколу FTP**, в частности:

- Перехват файлов, загруженных или переданных по FTP-протоколу, а также переданных по зашифрованному FTP-протоколу (FTPs);
- Мониторинг файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Мониторинг и перехват файлов и паролей по протоколу FTP/FTPs с последующим контекстным анализом перехваченных файлов.

Должна быть возможность контроля информации, **отправляемой на печать**, а именно:

- Перехват документов, отправляемых на печать;
- Извлечение и анализ текста отправленных на печать документов;
- Мониторинг документов, отправленных на печать с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Поиск по заданным параметрам текста и атрибута отправленных на печать файлов;
- Возможность выгрузки в виде документа Excel, HTML, CSV, в формате PNG;
- Возможностью скачать в ZIP архиве или распечатать на принтере.

Должен происходить контроль **внешних накопителей** со следующими возможностями:

- Теневое копирование файлов, отправляемых на внешние носители, в том числе, жёсткие диски, карты памяти и другие съёмные накопители, подключенные, как USB-устройства, CD/DVD;
- Контроль подключений и отключений USB-устройств;
- Контроль подключения, отключения и операций с RuToken с фиксацией уникального ID;
- Возможность настройки правил доступа для USB-устройств по их уникальным идентификаторам, в том числе с разрешением только для чтения;
- Возможность блокировки CD-накопителей;
- Возможность настройки правил блокировки USB-устройств по чёрным или белым спискам, по классам устройств и по группе;
- Перехват листинга и теневое копирование файлов при подключении внешних носителей, с возможностью настройки правила для перехвата по указанным расширениям файлов;
- Мониторинг случаев передачи файлов на внешние носители с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Мониторинг случаев использования внешних устройств с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Аудит событий копирования файлов на внешние накопители: фиксируется имя файла, пользователь, дата, время, приложение, полный путь и данные устройства;
- Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных на внешние носители.
- Возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- Возможность блокировки накопителей при передаче данных, объемом превышающие заданное пороговое значение;
- Возможность контроля файловых операций при работе пользователя с CD/DVD с возможностью создания теневых копий.

Должны присутствовать следующие возможности контроля информации, передаваемой в **облачные хранилища** (файловый канал):

- Возможность осуществления контроля по следующим облачным хранилищам – Dropbox, Яндекс.Диск, Google Drive, Nextcloud, ownCloud, OneDrive;

- Теневое копирование файлов, отправляемых в облачные хранилища с рабочей станции сотрудника с установленным агентом;
- Мониторинг случаев передачи файлов в облачные хранилища с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, пользователь, дата, время и имя облачного сервиса;
- Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных в облачные хранилища;
- Возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей.

Должен осуществляться контроль файлов и **файловой активности**, а именно:

- Контроль файловых операций (Запись, Копирование, Оглавление диска, Отключение, Очистка корзины, Перезапись, Переименование, Перемещение, Переименование и перемещение, Подключение, Создание, Удаление, Чтение);
- Перехват файлов и/или списка файлов со съёмных носителей, включая CD/DVD-диски при их подключении по заданным шаблонам расширений файлов;
- Сохранять теневые копии файлов, отправленных за информационный периметр контролируемой рабочей станцией;
- Последующий поиск по тексту и атрибутам перехваченных файлов;
- Мониторинг случаев использования файлов с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Создание индивидуальных политик контроля за файловой активностью, в том числе с возможностью копирования из предустановленных;
- Возможность определять пути и файлы для особого контроля с созданием теневых копий при любых файловых операциях.
- Детектирование файлов, зашифрованных крипто-про.

Должна быть возможность осуществления контроля и обработки информации, отправляемой на **локальные сетевые** ресурсы, следующими способами:

- Теневое копирование файлов, отправляемых на сетевые ресурсы с рабочей станции пользователя с установленным агентом;
- Мониторинг случаев передачи файлов на сетевые диски с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Аудит событий отправки файлов на сетевые диски: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу, приложение;
- Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных на сетевые ресурсы;
- Возможность создавать индивидуальные политики контроля информации для отдельных пользователей и рабочих станций.

Требования к методам мониторинга действий пользователей на ПК:

ПО должно позволять **создавать скриншоты** (снимки, кадры экрана рабочего стола сотрудника) для любого количества экранов и управлять процессом съёмки следующими способами:

- Снятие скриншотов с заданным интервалом;
- Снятие скриншотов по переключению активного окна;
- Снятие скриншотов во время удалённого подключения при просмотре рабочего стола или удалённом управлении рабочим столом;
- Настройка для определенных приложений и сайтов более частых интервалов снятия скриншотов;
- Создание пакета скриншотов, сохраняющего скриншоты за определенный период в один файл с возможностью настройки сжатия и цветности скриншотов в пакетах.
- Выполнение настройки качества получаемых скриншотов в процентах;
- Использование формата скриншотов JPEG;
- Возможность увеличения снимков экрана в рамках веб-консоли для возможности анализа снимков экрана большого размера.

- Выгрузка в следующих форматах: файл Excel, HTML, CSV, формат PNG
- Скачивание в ZIP архиве или печать на принтере;

ПО должно обеспечивать формирование и обработку **статистики активностей** пользователя и компьютера следующими способами:

- Ведение статистики по времени работы и простоя (отсутствия действий сотрудника) ПК с представлением собранной информации в виде различных графиков;
- Ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);
- Возможность настройки периода неактивности, после которого рабочее время сотрудника будет считаться простоем;
- Возможность настройки исключений отдельных процессов из мониторинга;
- Возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу;
- Возможность сохранения отдельных отчётов по активности (активность пользователя за ПК, активность приложений) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в формате HTML;
- Предустановленные наборы приложений и сайтов, для классификации активной деятельности за ПК;
- Разделение деятельности на продуктивную/непродуктивную/нейтральную;
- Наличие отчётов для различных представлений и анализа накопленных данных по активности пользователей;
- Общий и групповые отчёты по активности пользователей;
- Перехват активности в терминальных linux-сессиях и последующая детализированная запись терминального ввода и вывода в виде GIF.
- Перехват и логирование действий пользователей на Linux системах.
- Возможность управлением сбора статистики пользователем, посредством иконки в трее системы.

Должен осуществляться **контроль буфера обмена**, и реализованы следующие возможности:

- Копирование помещаемой в буфер обмена текстовой информации с фиксацией идентификатора процесса, из которого данная информация была помещена в буфер обмена, и времени события;
- Поиск по тексту, помещаемому пользователями в буфер обмена.
- Мониторинг определенной информации, помещенной в буфер обмена, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Копирование графической информации, помещаемой в буфер обмена, включая скриншоты посредством нажатия Print Screen
- Возможность блокировки передачи данных посредством буфера обмена из одного приложения в другое.

Должен быть реализован **кейллогер** (перехват нажатий клавиш на клавиатуре), имеющий следующие особенности:

- Регистрация нажатий сотрудником клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию и времени;
- Мониторинг информации, вводимой на клавиатуре, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Возможность создавать индивидуальные политики контроля перехвата нажатий клавиш для отдельных пользователей и рабочих станций;
- Возможность дополнять политики данными напрямую из отчетов.
- Возможность поиска по тексту, вводимому пользователями с клавиатуры.
- Возможность перехвата паролей в диалоговых окнах Windows;
- Возможность запрета/разрешения отслеживания при помощи кейлоггера по чёрным или белым спискам приложений;
- Возможность перехвата пароля в момент разблокировки рабочего стола Windows (низкоуровневый кейллоггер).
- Возможность скрывать и отображать спецсимволы полученные кейлогером.

Должна быть функция ведения **аудиомониторинга**, в частности:

- Возможность вести запись с обнаруженных микрофонов на локальной станции сотрудника с установленным агентом, независимо от используемого им приложения;
- Возможность записи звука, выводимого на аудиоустройства на локальной станции сотрудника с установленным агентом;
- Возможность настройки длительности записываемых отрывков записи звука;
- Возможность настройки качества записи;
- Возможность настройки шумового порога, при котором будут игнорироваться звуки;
- Возможность настройки интервала тишины, после которого запись звука будет приостановлена;
- Возможность настройки записи звука по децибелам;
- Возможность воспроизведения файла записи средствами системы веб-интерфейса;
- Возможность скачать записанные записи;
- Отображаться осциллограмма записанных записей для визуального определения моментов разговоров.

Должна быть возможность активировать **видеомониторинг**, имеющий следующие ключевые особенности:

- Возможность подключения к монитору компьютера сотрудника и просмотра изображения в режиме реального времени;
- Возможность мониторинга рабочих столов нескольких пользователей одновременно;
- Возможность вывода окна просмотра на отдельный экран;
- Возможность записи потокового видео с рабочих столов сотрудников при удаленном подключении;
- Возможность записи видео рабочего стола в режиме недоступности подключения к серверу;
- Возможность настройки длительности отрывка для записи видео;
- Возможность сохранения записей нескольких пользователей одновременно;
- Возможность воспроизведения файла записи средствами системы.
- Возможность фильтрации пользователей, к которым возможно удаленное подключение.

Должна присутствовать возможность контролировать пользователей работающих за компьютером:

- Возможность создания снимков с веб-камеры по заданному интервалу;
- Настройка для определенных приложений и сайтов более частых интервалов снятия снимков с веб-камеры;
- Возможность производить видеозапись с веб-камеры;
- Возможность делать снимки с веб-камеры при отсутствии запущенной сессии или активности за компьютером;
- Возможность удаленного подключения к веб-камере для просмотра в реальном времени;

Должен присутствовать модуль, **сканирующий файлы**, который:

- Позволяет блокировать несанкционированный доступ к файлам по заданным параметрам;
- Имеет возможности управления доступом пользователей и приложений к файлам согласно задаваемому набору правил;
- Обладает утилитой добавления меток к файлам основных типов офисных приложений: .docx, .xlsx, .pptx, .odt, .ods, . odp;
- Имеет возможность анализировать текстовый контент файлов и ограничивать доступ к ним по набору правил;
- Имеет возможность запрещать передавать файлы на или с съемных носителей информации;
- Имеет возможность запрещать определенные операции производимые с файлами: копирование, перемещение, удаление, переименование, чтение;
- Имеет возможность ограничивать доступ к шифрованным архивам по набору правил;
- Имеет возможность отслеживания работы над помеченными файлами;
- Имеет настройки собственных параметров через управление в WEB-консоли и обладает возможностями выставления правил использования и блокировок для помеченных файлов;
- Сканирует локальные файловые системы и сохраняет найденные результаты;
- Поддерживает при настройке правил операторы: not, or, and, xor, eq, matches, in;
- Использует при настройке правил атрибуты: tag, tag_value, computer_name, user_name, user_domain, file_path, file_name, file_ext, exe_name, mine.

Требования к возможностям отображения собранной информации

Должен присутствовать **просмотр информации по типам событий**, а именно:

- Поисковые запросы, информация выводится в следующем виде: время, компьютер, пользователь, приложение, домен, текст;
- Время активности, информация выводится в следующем виде: время, тип события, компьютер, пользователь, длительность (в формате 00 ч 00 м 00 с), приложение, сайт, заголовок;
- Снимок экрана, информация выводится в следующем виде: время, компьютер, пользователь, заголовок, снимок;
- Запись звука, информация выводится в следующем виде: время, компьютер, пользователь, устройство, контент (аудиофайл);
- Перехваченный файл, информация выводится в следующем виде: время, компьютер, пользователь, приложение, контент (файл, изображение и т.д.), связь с событием, страницы (перехват печати отображает количество страниц), получатели;
- Устройства, информация выводится в следующем виде: время, компьютер, пользователь, тип устройства, устройство, ID;
- Завершение приложений, информация выводится в следующем виде: время, компьютер, пользователь, приложение, ID процесса, ID пользовательской сессии;
- Системный лог, информация выводится в следующем виде: время, тип события, компьютер, текст, контент (с возможностью скачать сам лог из web-интерфейса);
- Беспроводное подключение, информация выводится в следующем виде: время, компьютер, SSID;
- Снимок с веб-камеры, информация выводится в следующем виде: время, компьютер, пользователь, приложение, снимок;
- Буфер обмена, информация выводится в следующем виде: время, компьютер, пользователь, приложение, текст, формат буфера обмена (текст или изображение);
- FTP, информация выводится в следующем виде: время, компьютер, пользователь, приложение, событие;
- Почта, информация выводится в следующем виде: время, компьютер, пользователь, отправитель, получатели, заголовок, контент (файлы, изображение и т.д. с нумерацией по номеру вложения);
- Посещение сайтов, выводится в следующем виде: время, компьютер, пользователь, приложение, ссылка;
- Ввод с клавиатуры, информация выводится в следующем виде: время, компьютер, пользователь, приложение, заголовок окна, текст;
- Сеть, информация выводится в следующем виде: время, компьютер, пользователь, приложение, сокет;
- Алерт (вычисленное сервером событие), информация выводится в следующем виде: время, тип, компьютер, пользователь, время, алерт, текст. При обнаружении алерта должна быть возможность автоматически сформировать и отправить уведомление по e-mail;
- Запуск приложения, информация выводится в следующем виде: время, компьютер, пользователь, приложение, ID процесса, ID пользовательской сессии;
- Операция с файлами, информация выводится в следующем виде: время, компьютер, пользователь, приложение, операция, имя файла, устройство, тип диска;
- Внешние диски, информация выводится следующем виде – время, компьютер, пользователь, тип, устройство, ID;
- Установка ПО, информация выводится в следующем виде: время, компьютер, операция, продукт, поставщик, версия;
- Установка и удаление пакетов на Linux системах.
- Инвентаризация установленных пакетов на Linux системах.
- Видео рабочего стола, информация выводится в следующем виде: время, компьютер, пользователь, приложение;
- Вход/выход из системы, информация выводится в следующем виде: время, компьютер, пользователь, событие (вход в систему, выход из системы и т.д.)
- Удаленный вход/выход из системы, информация выводится в следующем виде: время, компьютер, пользователь, событие (вход в систему, выход из системы и т.д.)
- Данные формы, информация выводится в следующем виде: время, компьютер, пользователь, приложение, сайт;
- Реестр оборудования, информация выводится в следующем виде: время, компьютер, тип устройства, устройство, ID;
- Реестр софта, информация выводится в следующем виде: время, компьютер, операция, продукт поставщик, версия;
- Печать документов, выводится в следующем виде: время, компьютер, пользователь, страницы (количество распечатанных страниц), текст;
- Интернет-пейджер, информация выводится в следующем виде: время, компьютер, пользователь, отправитель, получатели, сообщение.
- Отображение логотипа приложения по которому были перехвачены события.
- Возможность изменять формат отображения детализированной информации по событиям на горизонтальный или вертикальный.
- Возможность производить фильтрацию данных на основе элемента список.

Должен быть организован просмотр собранной информации как по отдельным измерениям, так и по их **комбинациям с типами событий и произвольным набором измерений**:

- Измерение Агент, выбор предоставляется по следующим параметрам: IP адрес, группа (к которому относится агент), сотрудник, компьютер, статус, версия OS, версия агента;
- Измерение пользователь, выбор предоставляется по следующим параметрам: отдел, организация, телефон, полное имя, почта, должность, домен, пользователь, комментарий, (информация задаётся в профиле пользователя);
- Измерение приложение, выбор предоставляется по следующим параметрам: полный путь, заголовок окна, название, описание;
- Измерение сайт, выбор предоставляется по следующим параметрам: полный домен, протокол, URL, основной домен, тип контента;
- Измерение сетевая активность, выбор предоставляется по следующим параметрам – IP-адрес, сетевой порт;
- Измерение файл, выбор предоставляется по следующим параметрам: хеш файла, операция, имя файла, контент извлечен (true или false), метка, тип контента, тип диска, расширение, путь, имя файла источника, путь источника, расширение источника;
- Измерение устройство, выбор предоставляется по следующим параметрам: устройство, ID устройства, маркер, тип диска, класс устройства, тип устройства;
- Измерение переписка, выбор предоставляется по следующим параметрам: домен получателя, отправитель, все получатели, формат сообщения, направление, домен отправителя, получатель, чаты, канал общение. В случае большого объема данных должно присутствовать постраничное отображение переписки;
- Измерение дата, выбор предоставляется по следующим параметрам: час суток, часовой пояс, день недели, по годам, по месяцам, по дням, по часам, по минутам;
- Измерение инсталляции, выбор предоставляется по следующим параметрам: поставщик, обновление, версия, операция, продукт;
- Измерение сработавшие фильтры, выбор предоставляется по следующим параметрам: категория, название.

Должна быть возможность **смены режимов предоставления отчётов** с отображением данных по следующим критериям:

- Таблица, выводящая информацию определенных типов события и типов измерения, с возможностью их комбинирования;
- Список, предоставляет информацию общим списком определенных типов события и типов измерения, с возможностью их комбинирования;
- Снимки, режим отображения для удобства предоставления информации по типам события снимков с веб-камеры и снимков с экрана, с возможностью выбора типов измерения;
- Активность, выводит информацию в виде тепловой диаграммы, с возможностью выбора отображения информации по типам события и измерениям;
- Переписка, режим отображения для удобства предоставления информации по типам события почта и интернет-пейджер, с возможностью выбора дополнительных типов измерения.

Должна присутствовать возможность наблюдать и анализировать статистику по собранным данным (строить **фильтры внутри фильтров**), тем самым, получая дополнительный срез информации при помощи следующих способов её отображения:

- Таблица с возможностью отображения в табличном виде события по выбранным ПК и фильтру;
- Линейный график с возможностью отображения количества событий по выбранным фильтрам в виде столбцов графика, а также возможность переключения графика между: линейным, гистограммой, с накоплением и без накопления;
- Круговая диаграмма с возможностью отображения количества событий в виде круговой диаграммы с поддержкой вложенных фильтров;
- Возможность построения графа в виде диаграммы связей;
- Возможность построения дерева взаимосвязей, которое возможно выгрузить на печать, и возможностью провалиться в события, кликнув на элемент дерева;
- Дополнительные возможности отображения данных в следующих видах: радар, река событий, статистика.
- Возможность отображать информацию по количественным измерениям: время разговора, число страниц, время активности, количество событий, размер файла.

Должен присутствовать **раздел фильтров** (например, в виде вкладки), включающий в себя сгруппированные измерения, политики, дашборды и словари:

- Наличие фильтров, создаваемые пользователем самостоятельно;
- Наличие фильтров, предустановленных и обновляемых разработчиком;
- Наличие возможности представления информации как в отчётах, так и конкретных событиях;
- Наличие подразделов эффективности, безопасности и инцидентов;
- Возможность маркировки приложений и сайтов по категориям продуктивности: продуктивная деятельность, непродуктивная деятельность, нейтральная деятельность, премиальная деятельность, инцидент. В любую из категорий можно добавить/удалить любое количество имён исполняемых файлов или сайтов;
- Наличие системных политик, являющимся скриптами для запуска внутренних обработчиков информации и возможность их изменения;
- Возможность создание новых фильтров или удаление уже имеющихся;
- Возможность задать любое имя созданному фильтру или дашборду, с возможностью его последующего изменения.
- Возможность добавить описание к созданному фильтру.
- Возможность регулярной рассылки настраиваемых консолидированных отчетов в html формате, позволяющими работать с отчетами из консоли без доступа к серверу.

При работе с **фильтрами и политиками безопасности**, пользователю должен быть доступен следующий функционал:

- Возможность настройки индивидуальных фильтров и политик безопасности, с последующим комбинированием их в дашборды, позволяющие просматривать необходимую выводимую информацию в едином месте;
- Возможность создавать копию фильтра из существующего, редактировать на лету;
- Возможность настройки уведомлений на почту ответственным лицам за информационную безопасность, с настройкой интервалов отправки (при срабатывании, ежедневно, еженедельно, ежемесячно) и возможностью настройки получаемой информации об инциденте;
- Возможность настройки уведомлений в мессенджер telegram ответственным лицам за информационную безопасность, с настройкой интервалов отправки (при срабатывании, ежедневно, еженедельно, ежемесячно) и возможностью настройки получаемой информации об инциденте;
- Наличие встроенных политик безопасности, а именно словарь ненормативной лексики, словарь наркоманского сленга, словарь откатной тематики, словарь поиска работы, поиск кредитных карт, шифрованных архивов и т.д.;
- Возможность просмотра информации и сработавших фильтров за любой промежуток времени;
- Возможность просмотра статистки с указанием количества сработавших инцидентов по определенному фильтру или типу события;
- Возможность изменения встроенных политик безопасности, с настройкой отправки уведомлений на почту ответственному лицу за информационную безопасность и возможности изменения категорий по следующим параметрам: инцидент, непродуктивно, нейтрально, продуктивно, премиально;
- Возможность автоматического изменения конфигурации, как следствие реакции на обнаруженный посредством созданной политики, словаря и политики срабатывания по пороговому значению.
- Возможность одновременного редактирование настроек уведомлений для группы фильтров и политик безопасности;
- Возможность получения уведомлений по изменению конфигурации оборудования;
- Возможность перейти из анализа к фактам по выбранным измерениям.

Должно присутствовать средство формирования инцидентов из событий (**консоль инцидентов**). При просмотре информации об инциденте в web-интерфейсе должна быть доступна следующая информация:

- Пользователь, допустивший нарушение;
- Дата и время инцидента;
- Тип файла, вызывающего срабатывания фильтра или политики безопасности (электронное письмо, документ, отправленный на печать и т.д.);
- Содержание файла, породившего инцидент (электронного письма, документа, отправленного на печать и т.д.);
- Другая дополнительная информация (с возможностью исключения/добавления необходимых пунктов вывода).
- У инцидента должна присутствовать и предустанавливаться критичность.

Должно присутствовать средство ежедневной генерации комплексной группы отчетов по учету рабочего времени с возможностью детального анализа данных без доступа к веб-консоли сервера.

С целью гибкой **настройки учёта рабочего времени** должны присутствовать:

- Возможность настройки рабочего расписания сотрудников, по следующим критериям: день недели, начало рабочего дня, конец рабочего дня, начало перерыва, конец перерыва, рабочее время;
- Календарь с возможностью проставления рабочих часов, праздников, больничных, отгулов и отпусков;
- Возможность назначения расписаний по компьютерам, группам, отделам, пользователям, полным именам пользователей и организации.
- Возможность отправки уведомлений ответственным лицам на почту, при превышении времени активности или разговора, размеру файла, количеству срабатываний в определенных приложениях, сайтах и других типах событий - срабатывание по порогу.

Должны присутствовать **встроенные отчёты для учёта рабочего времени**, а именно:

- Комбинированный отчёт, содержащий информацию за выбранный период по выбранным пользователям, разбитый на дни и выводящий следующую информацию: даты выбранного периода, пользователь, шкала активностей пользователя по часам, начало и окончание каждого рабочего дня, общее время работы, активное время, время простоя, информацию по опозданию и сверхурочным, продуктивное время, непродуктивное время и нейтральное время, расписание. Поля должны быть сгруппированы по типу измерения с возможностью выбора. Возможность включения в отображении в отчете неактивных сотрудников. В случае выбор одного определённого пользователя отчёт дополняется комбинированной статистикой в долях по времени и процентам для продуктивности, топу используемых приложений и топу посещаемых сайтов, отображаемых на временных шкалах по каждому из дней. При этом становится возможным отфильтровать активности и перейти к фактам по этим активностям;
- Ленточный график, отчёт, содержащий информацию за выбранный период по выбранным пользователям, разбитый на дни и выводящий шкалы активностей пользователя по часам. В случае выбора одного определённого пользователя отчёт дополняется комбинированной статистикой по продуктивности, топу используемых приложений и топу посещаемых сайтов, отображаемых на временных шкалах по каждому из дней, долями этих активностей;
- Таблица - отчёт, содержащий информацию за выбранный период по выбранным пользователям, разбитый на дни и выводящий следующую информацию: даты выбранного периода, пользователь, начало и окончание каждого рабочего дня, общее время работы, активное время, время простоя, информацию по опозданию и сверхурочным, продуктивное время, непродуктивное время и нейтральное время. В случае выбора одного определённого пользователя отчёт дополняется комбинированной статистикой по продуктивности, топу используемых приложений и топу посещаемых сайтов по каждому из дней;
- Отчёт по активности за период, содержащий суммарную информацию за выбранный период, по выбранным пользователям: пользователь, общее время работы, активное время работы, время простоя, информацию по опозданию, сверхурочные, продуктивное время, нейтральное и непродуктивное время. Отчёт дополнен комбинированной статистикой в долях по времени и процентам для продуктивности, топу используемых приложений и топу посещаемых сайтов, отображаемых по каждому из дней в виде графика. При этом отчёт можно отфильтровать по выбранным типам активностей, приложений или сайтов.
- Отчёт по простоям за период, содержащий поделённую простоями на интервалы следующую информацию по выбранным пользователям: сотрудник, дата, начало и окончание интервала, совершённые действия, учтённые часы работы и часы простоя;
- Продуктивное время по отделам, отчёт, содержащий суммарное продуктивное/непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени на шкале общего отработанного времени и отдельно по каждому из них в виде суммарного времени и его проценте от общего;
- Активное время по отделам, отчёт, содержащий на индивидуальных и общей шкалах отработанного времени суммарное активное время, переработку, суммарную недоработку, отсутствие пользователей на рабочих местах за выбранный период времени, в том числе по отношению к плановому времени в процентах;
- Топ непродуктивности по отделам, отчёт, содержащий информацию за выбранный период и сортирующий непродуктивных сотрудников по отделу, отображая следующее: компьютер, пользователь, должность, отдел, название типа активности, время активности;
- Сводный отчёт, содержащий как обобщённую статистику об опоздавших пользователях, времени опозданий, активных и неактивных, продуктивных и непродуктивных пользователях, так и сводную суммарную информацию за выбранный период по выбранным пользователям в следующем виде: пользователь, общее время, активное время, время простоя, продуктивное время, нейтральное непродуктивное время, количество опозданий, общее время опозданий и сверхурочные;
- Сводный отчёт по группам, содержащий следующую информацию по каждому сотруднику с разбиением по организационным единицам: пользователь, общее время, активное время, время простоя, продуктивное время, нейтральное и непродуктивное время, количество опозданий, общее время опозданий и сверхурочные. Вычисляются суммы по каждой группе сотрудников;
- Сводный статистический отчёт, содержащий следующий набор информации по всем выбранным сотрудникам: пользователь, активные дни, рабочие часы, общее время, активное время, продуктивное время, нейтральное время,

продуктивное корректированное время, продуктивное корректированное время в день, отношение продуктивного корректированного времени к 8 часам, непродуктивное время, непродуктивное время в день, время простоя, время простоя в день;

- Отчёт по опозданиям, содержащий следующую информацию за выбранный период, по выбранным пользователям: период времени, пользователь, количество опозданий, общее время опозданий, общее время, активное время и время простоя – если выбран один пользователь, и дополнительную статистическую информацию для нескольких: отношение общего времени опозданий к общему времени, топ опоздавших и топ по времени опозданий;
- Учёт ранних уходов и приходов, отчёт, разделённый датами и содержащий следующую информацию за выбранный период по выбранным пользователям: период времени, пользователь, длительность опоздания, ранний уход на обед и опоздания с обеда, ранний уход с работы, задержание на работе и ранний приход на работу;
- Учёт ранних уходов и приходов по группам, отчёт, разделённый датами и организационными единицами, содержащий следующую информацию за выбранный период по выбранным пользователям: период времени, пользователь, длительность опоздания, ранний уход на обед и опоздания с обеда, ранний уход с работы, задержание на работе и ранний приход на работу;
- Расширенный табель учёта рабочего времени, отчёт, который представляет собой совокупность ежемесячных отчётов по всем выбранным пользователям, где для каждого пользователя предусмотрены следующие заполненные поля: организация, отделение, должность, сотрудник и рабочее время. При этом рабочее время учитывается в следующих измерениях для каждого дня: вход, выход, время нахождения в офисе, время работы в разрешённом ПО, время работы в запрещённом ПО, простой. По каждого месяца по каждому измерению подводятся итоги: дни и часы в рабочие и выходные дни;
- Табели по форме Т13 (отчёты "как в 1С "): рабочего времени, активного времени, отсутствия на рабочем месте, использования принтера.
- Отчет по входу, выходу и пребыванию в помещении на основе данных собранных со СКУД.
- Отчет по отсутствию событий за период, содержащий в себе информацию по машинам, которые за выбранный период не присылали данных на сервер.
- Наличие возможности для редактирования отображаемой информации в отчетах;
- Возможность изменения и фиксации периода анализируемых данных;
- Возможность изменения объекта анализа в отчетах: компьютеры, пользователи, полные имена пользователей, сотрудники.
- Возможность установки минимального времени активности для анализа начала и окончания рабочего дня в рамках отчета.
- Возможность отображения данных в отчете по времени удаленной сессии.

Требования к возможностям инвентаризации установленного ПО и оборудования

- Должен присутствовать встроенный отчёт инвентаризации устройств рабочей станции со следующими выводимыми параметрами: статус (в наличии или нет), компьютер (имя рабочей станции), производитель, тип устройства, HWID и дата последней проверки на наличие, с возможностью группировки по компьютерам и выгрузки отчёта в html, pdf и excel форматах.
- Должен присутствовать встроенный отчёт по инвентаризации приложений рабочей станции со следующими выводимыми данными: статус (в наличии или нет), компьютер (имя рабочей станции), продукт, поставщик, версия и дата последней проверки на наличие, с возможностью группировки по компьютерам и выгрузки отчёта в html, pdf и excel форматах.
- Должен присутствовать встроенный отчет по приложениям на рабочих станциях организации со следующими выводимыми данными: Название приложения, список станций на которых обнаружено данное ПО, с информацией по статусу, поставщику, версии и дате наличия. Должна присутствовать возможность выгрузки отчета в html, pdf и excel форматах

Требования к возможностям анализа и распознавания

В программном обеспечении должны быть предусмотрены расширенные возможности аналитики собираемой информации посредством **контентного анализа**, имеющего:

- Возможность поиска, по ключевым словам, и словосочетаниям
- Возможность добавления слов или словосочетаний в фильтр для их обнаружения в перехваченных файлах или документах;
- Возможность составления собственных словарей;
- Возможность подсветки разными цветами найденных совпадений из разных словарей.

- Возможность поиска контента посредством конструктора регулярных выражений с возможностью проверки запроса, сформированного конструктором.
- Детальная информация по все политикам, среагировавшим на инцидент.

Программное обеспечение должно обладать функционалом **распознавания изображений и документов**, которые обеспечивает:

- Наличие собственного бесплатного встроенного модуля OCR не старее Tesseract4;
- Возможность использования 2х и более серверов распознавания.
- Возможность распознавания перевернутых изображений;
- Возможность выбора следующих языков - русский и английский;
- Возможность распознавания следующих форматов - PDF, JPEG, PNG;
- Возможность подключения облачного ABBYY Cloud OCR SDK.
- Возможность распознавать Паспорта и Штампы печатей через нейронные сети с использованием машинного обучения.
- Возможность распознавания лиц через снимки с веб-камеры с использованием машинного обучения.

Функциональные требования

Поставщик должен провести технические работы, связанные с установкой и настройкой на аппаратных средствах Заказчика, в том числе:

- Установка и настройка (сервер приложений);
- Настройка и подключение клиентских мест в соответствии с количеством лицензий;
- Настройка и подключение клиентских мест на обьекте заказчики с приствуем инженера заказчика.
- Техническая поддержка и сопровождение Заказчика осуществляется с даты подписания договора в течение 12 месяцев.
- Срок действия предоставляемых потенциальным поставщиком лицензий: бессрочно.
- **Требования к качеству:** качество Услуг должно соответствовать существующим стандартам, техническим и иным нормам, действующим в Республике Казахстан.
- В случае предоставления документов от Потенциального поставщика на иностранном языке, должен быть предоставлен нотариально заверенный перевод на казахском или русском языке).
- Срок поставки лицензий, установки и настройки : в течение 15 (пятнадцать)рабочих дней с даты подписания Договора.
- Общая сумма Договора включает в себя все расходы, связанными с поставкой лицензий, установкой и настройкой ПО.

3. Технические стандарты

№ п/п	Зарегистрирован в РК	Обозначение	Номер документа	Категория	Наименование	Область применения	Разработчик	Страницы	МКС	Статус	Приказ	Дата введения с
						Настоящий стандарт распространяется						

1	Да	СТ РК ГОСТ Р 51904-2011	347668	Национальный стандарт Республики Казахстан	Программное обеспечение встроенных систем. Общие требования к разработке и документированию Дата введения с 2013.01.01	на процессы разработки и документирования программного обеспечения (ПО) встроенных систем реального времени. Стандарт распространяется на все действия, имеющие отношение к разработке программного обеспечения. Настоящий стандарт применяют полностью ко всему поставляемому программному обеспечению, включая среду разработки, если контрактом не предусмотрено использование специальных стандартов для определенных	Нет ()	186	Программное обеспечение	Действует	Приказом Председателя Комитета технического регулирования и метрологии Министерства индустрии и новых технологий Республики Казахстан от 17 ноября 2011 года № 625-од	01.01.2013

						заказчиком типов ПО. Стандарт неприменим для аппаратных элементов программно-аппаратного обеспечения							

Подписал Муратов Арман Халелұлы

Дата подписания 11.11.2024