## Ақпараттық қауіпсіздік жай-күйінің жедел мониторингін бағдарламалық қамтамасыз етуге қойылатын талаптар (SIEM)

### Жалпы талаптар

Жүйеде Ресей ФСБ-ның 2019 жылғы 6 мамырдағы № 196 бұйрығымен бекітілген компьютерлік шабуылдарды анықтауға, олардың алдын алуға және салдарын жоюға және компьютерлік инциденттерге ден қоюға арналған құралдарға қойылатын талаптарға сәйкестігі туралы қорытынды болуы тиіс.

### Жабдыққа қойылатын талаптар

• Жүйе компоненттері физикалық және виртуалды машиналарда орнатуды қолдауы тиіс.

• Негізгі компоненттер (оқиғаларды жинау, корреляциялау, оқиғаларды сақтау үшін жауап беретін модульдер) Linux жиынының операциялық жүйесінде орнатуды қолдауы тиіс:

o Astra Linux Special Edition 1.7.1-1.7.4;

o Oracle Linux 8.6, 8.7, 9.2 нұсқалары.

• Жүйе жоғары өнімділікті қамтамасыз етуі және бір серверде секундына 300 000 оқиғаға (EPS) дейінгі мөлшерде ағынды қабылдауды және өңдеуді қолдауы тиіс.

• Оқиғаларды сақтау үшін іздеудің жоғары жылдамдығын қамтамасыз ету үшін бағандық дерекқор пайдаланылуы тиіс.

Жүйенің архитектурасына қойылатын талаптар

• Жүйе оның негізгі компоненттерін: коллекторды, корреляторды және оқиғаларды сақтауды бағдарламалық қамтамасыз етуге қосымша лицензиялар сатып алудың қажеттілігінсіз көлденең масштабтауды қолдауға тиіс.

• SIEM барлық компоненттерінің желілік өзара іс-қимылы шифрланған байланыс арналары бойынша орындалуы тиіс

• Жүйе компоненттері Интернет желісіне қол жеткізудің қажеттілігінсіз бөлінген және оқшауланған желілерде орнатуды қолдауы тиіс.

• Жүйе оқиғаларды желінің оқшауланған сегменттерінен дата-диод арқылы, оның ішінде UDP-пакеттерді пайдалана отырып, оқиғаларды беру мүмкіндігі болмаған кезде жинау мүмкіндігін қолдауы тиіс.

• Жүйе әкімшінің АЖО-сына қосымша бағдарламалық жасақтама орнатпай веб-консоль арқылы орталықтандырылған басқаруды қамтамасыз етуі тиіс.

• Жүйе бірыңғай инсталляция шеңберінде жүйе пайдаланушыларының оқиғаларға, инциденттерге, корреляция, қалыпқа келтіру қағидаларына, сондай-ақ әртүрлі тенанттарға қатысты жүйенің белгілі бір баптауларына қол жеткізу құқықтарын ажырату мүмкіндігімен тәуелсіз тенанттар құруға мүмкіндік бере отырып, мультитенанттылықты қолдауға тиіс.

• Жүйе конфигурацияны орталықтандырылған жаңарту немесе компоненттерді, оның ішінде үдемелі компоненттерді қайта іске қосу мүмкіндігін қамтамасыз етуі тиіс.

• Жүйе компоненттер арасындағы оқиғаларды бағыттаудың икемді күйін сақтауы тиіс.

• Жүйе «ыстық» ауыстырып қосумен (High Availability) барлық компоненттер үшін істен шығуға төзімді кластердің жұмыс режимін қамтамасыз етуі тиіс;

• Жүйе географиялық бөлінген жүйелердің икемді схемаларын ұйымдастыру мүмкіндігі үшін оқиғалар қоймасының бірнеше тәуелсіз кластерлерімен жұмысты қолдауға тиіс.

• Шешімнің архитектурасы географиялық бөлінген инфрақұрылымда кем дегенде келесі көлемде өрістету мүмкіндігін қамтамасыз етуі тиіс:

o Жүйе белгілі бір оқиғаларды қашықтағы офистерден орталық корреляторларға беру мүмкіндігін қолдауы тиіс;

o Жүйенің жергілікті коллекторын орнату есебінен қашықтағы офистерде АҚ оқиғаларын жергілікті жинау, қалыпқа келтіру, агрегаттау, сүзу және байыту мүмкіндігі.

• Жүйе орталық тораптан алыс кеңселердегі оқиғалар бойынша іздеуді қолдауы тиіс.

• Жүйе активтерді, белсенді парақтарды басқару, тіркелген базалық және корреляциялық АҚ оқиғаларымен жұмыс істеу үшін RESTful API ұсынуы тиіс: іздеу, базалық және корреляциялық АҚ оқиғалары бойынша контекстік ақпаратты алу, өңдеу мәртебесін басқару.

• Жүйе өндіруші шығаратын нормалау ережелері мен корреляция ережелерін автоматты түрде жаңартуды қолдауға тиіс. Жаңа қолжетімді ресурстар туралы хабарламаны алғаннан кейін оператордың өзгерістерді тексеру мүмкіндігі іске асырылуы тиіс. Жүйе жаңартуды, оның ішінде «жаңарту айнасы» тетігін пайдалана отырып, интернетке тікелей қолжетімділіксіз қолдауы тиіс.

### Оқиғаларды жинауға, талдауға және сақтауға қойылатын талаптар

* Жүйе деректер көздерінен оқиғалардың белсенді де, пассивті де жиналуын қамтамасыз етуі тиіс.
* Жүйе деректердің біріздендірілген моделін қамтамасыз етуі тиіс.
* Жүйе келесі транспорттар арқылы оқиғаларды жинауды қамтамасыз етуі тиіс:
* Netflow (v9, v5), sFlow;
* IPFIX;
* TCP, UDP;
* HTTP;
* WEC, WMI;
* SNMP, SNMP-trap;
* FTP, NFS, filereader;
* API;
* SQL – сұранымдарды орындау, нәтижелерді өңдеу (ID-based және Time-Based кестелерін қолдайтын);
* Kafka, nats-jetstream.
* Жүйе оқиғаларды жинаушылардың (коллекторлардың) тізімін басқарудың орталықтандырылған интерфейсін ұсынуы тиіс.
* Жүйе бастапқы (raw) оқиғаны опциондық сақтау мүмкіндігін қолдауы тиіс. Баптаулар оқиғаны сөзсіз сақтауды және оқиғаны талдау қатесі болған жағдайда ғана сақтауды көздеуі тиіс.
* Жүйе оқиға көздерінің пайдаланушылық типтерін қосу және талдау және қалыпқа келтіру ережелерін сәйкес баптау мүмкіндігін қолдауы тиіс.
* Жүйе қолдау көрсетілетін форматтар мен деректерді жинау хаттамалары негізінде пайдаланушылық парсерстерді жасауды қамтамасыз етуі тиіс.
* Жүйе оқиғаларды талдау үшін жүйенің веб-интерфейсінен қалыпқа келтіру ережелерін жазу мүмкіндігін, оның ішінде тұрақты өрнектер арқылы және бастапқы оқиға мысалында оларды жазу синтаксисін тексеру мүмкіндігін қамтамасыз етуі тиіс.
* Қосымша талдау (қалыпқа келтіру) параметрлері жоқ жүйе Syslog, CEF пішімдерінде оқиғаларды алуды қолдауы тиіс.
* Жүйе еркін пайдаланушы таксономиясын іске асыру үшін пайдаланушы өрістерін құру мүмкіндігін қамтамасыз етуі тиіс. Өрістердің келесі түрлерін жасау қол жетімді болуы тиіс:

o Жолдық

o Сандық

o Қалқымалы нүктемен

o Жол жиыны

o Сандар жиыны

o Қалқымалы нүктелі сандар жиыны

* Жүйе оқиғаларды жүйелі иерархиялық талдау (қалыпқа келтіру) мүмкіндігін қолдауға тиіс.
* Оқиғаларды жинау компоненті (коллектор) оқиғаларды алушылар уақытша қол жеткізе алмайтын жағдайда жергілікті дискідегі оқиғаларды буферлеуді, сондай-ақ қосылысты қалпына келтіргеннен кейін буферленген оқиғаларды автоматты түрде жіберуді қамтамасыз етуі тиіс. Оқиғаларды сақтауға арналған буфер өлшемі теңшелетін болуы керек.
* Алынған оқиғаларды бастапқы өңдеу кезеңінде жинау компоненті (коллектор) қамтамасыз етуі керек:
  + Оқиғаларды қалыпқа келтіруді;
  + Оқиғаларды сүзуді;
  + Оқиғаларды агрегациялауды (математикалық функцияларды қолдану мүмкіндігімен);
  + Оқиғалардың модификациясын/мутациясын;
  + Оқиғалар уақытын түзетуді;
  + Байыту көздерінің тізбесіне сәйкес оқиғаларды ағындық байытуды (төменде қараңыз).
* Жүйе, атап айтқанда, әрбір дереккөз үшін мониторингтің берілген параметрлерінен ауытқыған жағдайда, көрсетілген уақыт аралығында оқиғалар санын қадағалай отырып және электрондық поштаға автоматты түрде хабарлай отырып, дереккөздерден оқиғалардың түсуін мониторингілеу мүмкіндігін қамтамасыз етуі тиіс;
* Жүйе оқиғаларды сақтау деңгейлерін бөлуді («ыстық» және «суық» деңгейлер) ұстап тұруы тиіс. Бұл ретте, деректер іздеу интерфейсінен «суық» сақтаудан оқиғаларды қосымша жүктеудің немесе іздеуді сақтау түрлері мен мерзімдері бойынша бөлудің қажеттілігінсіз ашық қол жетімді болуы тиіс. Сақтау мерзімдерінің параметрлерін пайдаланушы жүйенің графикалық интерфейсінде анықтауы тиіс.
* Оқиғаларды ұзақ сақтау мұрағатына түсіру мүмкіндігі.
* Жүйе оқиғаларды сақтау мерзімі әртүрлі және оқиғаларды пайдаланушы сүзгілеріне сәйкес осы топтар бойынша бөлу мүмкіндігі бар топтарға қойманың жалпы көлемін қисынды бөлуді қолдауы тиіс.
* Жүйе сұраулар конструкторының көмегімен оқиғалар базасы бойынша ерікті іздестіру негізінде оқиғалар базасы бойынша іздестіру мүмкіндігін қамтамасыз етуі тиіс;
* Жүйе сұранымдар тілінің SQL-like негізінде оқиғалар базасы бойынша топтамалар мен есептеу операцияларын жүргізу мүмкіндігімен іздеу мүмкіндігін қамтамасыз етуі тиіс;
* Жүйе оқиғалар базасы бойынша өрістер статистикасын шығару мүмкіндігін қамтамасыз етуі тиіс;
* Жүйе контент пен ресурстардың импортын/экспортын қолдауы тиіс: корреляция ережелері, парсерлер, коннекторлар және т.б..

### Оқиғаларды байыту функцияларына қойылатын талаптар

* Жүйе коллекторлардағы (оқиғаларды жинау және өңдеу кезеңінде), сондай-ақ коррелятордағы (корреляцияланған оқиғаларды байыту үшін) оқиғаларды байытуды қолдауға тиіс
* Threat Intelligence платформасымен ықпалдастыру жолымен оқиғаларды қауіп-қатерлер туралы деректер ағынымен салыстыру арқылы оқиғаларды ағындық байыту мүмкіндігі қамтамасыз етілуі тиіс. Табылған компрометация индикаторлары туралы деректер корреляция шеңберінде одан әрі пайдалану мүмкіндігімен бірден базалық оқиғаларға енгізілуі тиіс.
* Жүйенің лицензиясы KUMA-ға өндіруші компанияның да, сыртқы жеткізушілердің де компрометация индикаторлары туралы деректер ағынын қосу мүмкіндігін қамтуы тиіс (OSINT-дереккөздер және TAXII стандартты хаттамасы бойынша)
* Жүйе өндірушісінің деректер ағындары келесілерді қамтуы тиіс:
* ransomware url - «шифрлаушыларға» жататын URL мекенжайлары мен маскаларды
* botnet url - ботнет желілеріне қатысты командалық орталықтар мен веб-ресурстарды табуға арналған URL мекенжайлары мен маскаларды
* malicious url - зиянды URL мекенжайлары және зиянды веб-ресурстарды анықтауға арналған маскаларды
* phishing url - фишингтік веб-ресурстарды анықтауға арналған фишингтік URL және маскаларды
* ip reputation - күдікті және зиянды IP-мекенжайлары бар
* Жүйе онлайн қол жетімді беделді қызметке талдаушының сұранымы бойынша нақты оқиғаларды байыту мүмкіндігін қолдауы тиіс. Сұраным домендер, веб-мекенжайлар, IP-мекенжайлар және файлдардың хэштері бойынша орындалуы және қауіпті және зиянды, сондай-ақ заңды нысандар туралы мәліметтермен байытуды орындауы тиіс.
* Жүйе оқиғаларды байыту үшін келесідей тетіктер мен көздерді қолдауы тиіс:
* Активтердің кіріктірілген базасында бар активтер мен ақпараттық активтердің топтары туралы мәліметтер;
* Active Directory каталог қызметінде бар пайдаланушылар мен топтар туралы мәліметтер;
* DNS;
* IP-мекенжайлардың географиялық деректер базасы;
* Пайдаланушы жасайтын сөздіктер;
* Оқиға көзінің сағат белдеуі туралы мәліметтер;
* Threat Intelligence контекстік ақпараты (компрометация индикаторлары және тиісті хэш мәтіні, URL-мекенжайлары, сыртқы IP-мекенжайлары туралы мәліметтер).
* Жүйе IP-мекенжайы бар оқиғаларды геодеректердің жүктелген тізімдері негізінде географиялық деректермен байыту мүмкіндігін қолдауы тиіс.
* Жүйе MaxMind және IP2Location сервистерінен алынған геоданаларды пайдалану мүмкіндігін қолдауы тиіс.
* Жүйе оқиғаларды байыту үшін пайдаланушы сөздіктерін жасауды және оларды web-интерфейс және/немесе API арқылы толтыру мүмкіндігін қолдауы тиіс.
* Байыту үшін пайдаланылатын сөздіктер кемінде 50000 жазбаны қосу мүмкіндігін қолдауы тиіс.
* Жүйе дүниежүзілік үйлестірілген уақытқа (UTC) қатысты оқиға көзінің ауысу уақыты туралы ақпаратпен оқиғаларды байыту мүмкіндігін қолдауы тиіс.

### Оқиғаларды корреляциялау функцияларына қойылатын талаптар

• Жүйе нақты уақыт режиміне жақын режимде АҚ оқиғаларының ағымдық корреляциясын қамтамасыз етуі тиіс.

• Корреляция компоненті корреляция ережелерінде белсенді тізімдерді (Active List/Reference Set) қолдануды қолдауы тиіс.

• Белсенді тізімдер үшін кем дегенде келесідей операциялар қолданылуы тиіс:

o UI арқылы пайдаланушының тізімдерін жасау, жою;

o Корреляция ережесінің жұмыс нәтижесі ретінде жолдардың болуын тексеру, қосу, өзгерту және жою;

o Тізімдерді кестелік форматта импорттау және экспорттау;

o Белсенді тізімдегі жазбалар үшін теңшелетін өмір уақытын (TTL) қолдау;

o Белсенді тізімді қайта жасамай колонкалар жиынтығын өзгерту мүмкіндігін қолдау.

• Жүйе MITRE ATTACK матрицасының негізінде әзірленген өзекті қауіп-қатерлер мен шабуыл тәсілдерін зерттеу негізінде жасалған алдын ала белгіленген корреляция қағидаларының жиынтығымен жеткізілуі тиіс;

• Жүйе өзінің корреляция ережелерін құру мүмкіндігін қолдауы тиіс. Бұл ретте сүзгілер шарттарын және корреляциялық ережелерді код түрінде, сондай-ақ графикалық редакторда жазу қолжетімді болуы тиіс.

• Жүйе қосымша модульдерді орнатпай тарихи деректерге корреляция ережелерін тестілеу мүмкіндігін ұстап тұруы тиіс.

• Жүйе корреляция ережелерін көп деңгейлі қолдануды қолдауға тиіс, бұл ретте корреляцияның бір ережелерінің іске қосылу нәтижелері мынадай корреляция ережелері үшін көздер болып табылады.

• Жүйедегі корреляция ережелерін келесілерді қолдауы тиіс:

o Сандық белгісі бойынша корреляцияны;

o Оқиғалардың бірізділігі бойынша корреляцияны;

o Оқиға үзінділерін таңдау операцияларын (substring, regexp және т.б.);

o Корреляция ережесі іске қосылғанда автоматты хабарлауды;

o Жаһандық және жергілікті айнымалылар бойынша корреляцияны.

• Жүйе корреляция ережесінің сындылық деңгейін ескере отырып, сондай-ақ ақпараттық активтердің сындылығы мен санын ескере отырып, АҚ анықталған қауіп-қатерлерге автоматты түрде басымдық беруі тиіс.

• Жүйе активтің қандай да бір топқа кіруін ескере отырып, корреляция ережелерін жазу мүмкіндігін қамтамасыз етуі тиіс.

• Жүйе икемді теңшелетін пайдаланушы сүзгілері бойынша түзетілген оқиғаларды автоматты түрде біріктіруді қолдауы тиіс.

• Жаһандық ауыспалы корреляциялар олар жарияланған коррелятор шегінде әрекет етуі тиіс және корреляция ережелерінде қолданған кезде корреляция ережесінің (селектордың) іске қосылуының әрбір шарты шеңберінде әртүрлі мәндерді қабылдай алуы тиіс.

• Жергілікті ауыспалы корреляциялар корреляциялық ереже және олар жарияланған корреляция ережесінің (селектордың) іске қосылу шарттары шеңберінде ғана әрекет етуі тиіс.

• Ауыспалы корреляциялар келесі функцияларды қолдауы тиіс:

o Көрсетілген бағандағы мән туралы белсенді парақтан ақпарат алу;

o Көрсетілген сөздік бағанындағы мән туралы ақпарат алу;

o Жолдағы символдар санын қайтару;

o Жолдағы символдарды төменгі тіркелімге ауыстыру;

o Жолдағы символдарды жоғарғы тіркелімге ауыстыру;

o Жолдың соңына символдарды қосу;

o Жолдың басына символдарды қосу;

o Кіші жолдың басы мен соңының координаттары бойынша жолдан кіші жолды қайтару;

o Көрсетілген таңбаларды/кіші жолды жолдың басынан және/немесе соңынан жою;

o Барлық кіріс жолындағы А символдарының бірізділігін В символдарының бірізділігіне ауыстыру;

o Жолдағы жүйелі өрнекті қанағаттандыратын символдарды тұрақты өрнекті қармау тобы мен символдардың реттілігіне ауыстыру;

o Бастапқы жолдан тұрақты білдіру шартын қанағаттандыратын нәтиже алу;

o Epoch форматында уақытша белгі алу;

o Уақыттың атомарлық көріністерін (жыл, ай, күн, сағат, минут, секунд, апта күні түрінде) жолдар және уақыт айнымалыларынан epoch форматында алу;

o Уақытты RFC3339 пішімінен epoch пішіміне және керісінше түрлендіру;

o Уақытты epoch форматында дөңгелектеу (секундқа/минутқа/сағатқа/тәулікке дейін);

o Екі уақыт белгісі арасындағы уақыт аралығын epoch форматында алу (секунд/минут/сағат/күн);

o Негізгі математикалық операциялар:

* + - Қосу;
    - Шегеру;
    - Көбейту;
    - Бөлу;
    - Модуль бойынша бөлу;
    - Сандарды дөңгелектеу (үлкен/кіші жаққа);
    - Модуль бойынша санды алу;
    - Дәрежеге көтеру.

### Ден қою функцияларына қойылатын талаптар

• Жүйе корреляция ережелерінің іске қосылуы нәтижесінде автоматтандырылған ден қою функцияларын шақыруды қолдауы тиіс.

• Жүйе келесідей ден қою тетіктерін қолдауы тиіс:

* Пайдаланушы скрипттерін (серверлік) автоматты түрде іске қосу;
* Вирустарға кезектен тыс тексеруді немесе соңғы нүктелерді қорғау құралдарын басқару сервері арқылы базаларды жаңартуды мәжбүрлі түрде қолмен (актив карточкасынан) және автоматты түрде (корреляция ережесі іске қосылғанда) іске қосу;
* Соңғы нүктелерді қорғау құралдарын басқару сервері арқылы базаларды кезектен тыс жаңартуды қолмен де (актив карточкасынан), автоматты түрде де (корреляция ережесі іске қосылғанда) мәжбүрлі түрде іске қосу;
* EDR-агенттердің мүмкіндіктерін пайдалана отырып, қол режимінде де (актив карточкасынан), автоматты түрде де (корреляция ережесі іске қосылған кезде) ден қою. Келесі әрекеттер қолжетімді болуы тиіс:
* Хостты желілік оқшаулау;
* Хостта еркін командаларды іске қосу және орындау нәтижелерін алу;
* SIEM алатын оқиғалар параметрлерінің негізінде тыйым салу ережесін жасау
* Автоматты түрде веб-трафикті қорғау құралдарының мүмкіндіктерін пайдалана отырып әрекет ету (корреляция ережесі іске қосылғанда). Келесі әрекеттер қолжетімді болуы тиіс:
* E-mail бойынша бұғаттау;
* IP бойынша бұғаттау.
* Пошта серверлері үшін антивирустық қорғау құралдарының және спам сүзгісінің мүмкіндіктерін пайдалана отырып, автоматты түрде ден қою (корреляция ережесі іске қосылғанда). Келесі әрекеттер қолжетімді болуы тиіс:
* URL бойынша бұғаттау;
* IP бойынша бұғаттау;
* DOMAIN бойынша бұғаттау.
* Өнеркәсіптік кәсіпорындардың инфрақұрылымын қолмен (актив карточкасынан) де, автоматты түрде де (корреляция ережесі іске қосылған кезде) қорғау үшін шешімдердің мүмкіндіктерін пайдалана отырып ден қою. Активтің мәртебесін өзгерту мүмкін болуы керек.
* Active Directory тіркелгілерін қолмен (тіркелгі карточкасынан) және автоматты түрде (корреляция ережесі іске қосылғанда) басқару. Келесі әрекеттер қолжетімді болуы тиіс:
* Топтан тіркелгіні қосу және жою;
* Тіркелгі құпиясөзін арылту;
* Тіркелгіні бұғаттау.
* Есепке алу карточкасынан тиісті курстарды тағайындау арқылы қызметкерлердің хабардар болу деңгейін басқару.
* Активтер туралы мәліметтерді басқаруға қойылатын талаптар
  + Жүйе біріктірілген дерекқорда ақпараттық активтер туралы келесңдей түгендеу ақпаратын жинауды және автоматты түрде жаңартуды және сақтауды қамтамасыз етуі тиіс:
* IP
* MAC
* FQDN
* Белгіленген БҚ тізбесі
* БҚ-ның өзекті осалдықтары туралы ақпарат
* Аппараттық қамтамасыз ету туралы ақпарат
* САИ санаты
* Қорғаудың соңғы жаңартылған күні
* Активте белгіленген қорғау БҚ мәртебесі

• Жүйе актив карточкасына пайдаланушы өрістерін қосуға мүмкіндік беруі тиіс;

• Жүйе ақпараттық активтердің кіріктірілген базасын толықтырудың және жаңартудың мынадай тетіктерін қолдауы тиіс:

* Соңғы нүктелерді қорғау құралдарынан басқару серверімен интеграциялау арқылы ақпаратты автоматты түрде жинау және жаңарту;
* Өнеркәсіптік/технологиялық желілерді қорғау құралымен интеграциялау арқылы ақпаратты автоматты түрде жинау және жаңарту;
* Активтер мен осалдықтар туралы ақпарат бойынша есептерді сканерден қолмен қосу;
* Жүйенің графикалық интерфейсі арқылы активтер туралы ақпаратты қолмен қосу немесе редакциялау;
* REST API арқылы активтерді импорттау.
  + Жүйе пайдаланушы активтер топтарын (санаттарын) құруды қолдауға тиіс;
  + Жүйе бір немесе белгілердің комбинациясы негізінде активтерді автоматты түрде санаттау мүмкіндігін қамтамасыз етуі тиіс: ОЖ, IP адрестеу, FQDN, CVE ID болуы және ОЖ нұсқасы.
  + Активтерді автоматты санаттау шарттарын белгілеу кезінде жүйе ЖӘНЕ, НЕМЕСЕ, ЕМЕС логикалық операторларын, сондай-ақ олардың топтамасын қолдауы тиіс.
  + Активтерді автоматты санаттау шарттарын белгілеу кезінде жүйе ақпараттық активтердің қолда бар базасы бойынша берілген шарттарды тестілеу мүмкіндігін қамтамасыз етуі тиіс.
  + Жүйе кіріктірілген дерекқорда сақталған активтер бойынша іздеу мүмкіндіктерін қолдауы тиіс.
  + KSC немесе KICS-тен импортталған активтер үшін KUMA активтері мұрағаттық ретінде және пайдаланушы белгілеген кезең аяқталғаннан кейін белгіленетін және егер осы активтердегі агенттер KSC немесе KICS-ке енді қосылмаса, жойылуы мүмкін мұрағаттау тетігі қолданылуы тиіс.
  + Жүйе активтер аудитінің функциясын ұстап тұруы және келесі оқиғаларды қадағалауы тиіс:
* Активті жүйеге қосу;
* Актив параметрлерін өзгерту (аты, IP-мекенжайы, MAC-мекенжайы, FQDN, ОС);
* Активті жүйеден шығару;
* Активке осалдығы туралы мәліметтерді қосу;
* Активтің осалдығы туралы мәліметтерді жою/өзгерту;
* Актив санатын өзгерту (қосу/жою)

### Инциденттермен жұмыс істеу функцияларына қойылатын талаптар

* Жүйе табу оқиғасының карточкасын қалыптастыруды қамтамасыз етуі тиіс.
* Карточка келесі мүмкіндіктерді қолдауы тиіс:
* Инциденттің басымдығын өзгерту;
* Таңдалған талдаушыға инцидентті тағайындау;
* Инцидент карточкасынан байланысты базалық оқиғаларға көшу;
* Карточканың мәртебесін және орындалған іс-қимылдарын өзгерту журналын автоматты түрде жүргізу;
* Ақпараттық активтерді, инцидентпен байланысты пайдаланушыларды, сондай-ақ олар туралы қолжетімді контекстік ақпаратты көрсету;
* Активтерді табу оқиғасына байланысты және олардың құндылығын көрсете отырып, пайдаланушылар туралы ақпаратты бөлу;
* Инциденттің себебін талдау үшін қосымша оқиғаларды қолмен байлау;
* Бірнеше корреляция оқиғаларын қол режимінде де, автоматты түрде де: корреляция оқиғасын қалыптастырудың уақытша диапазоны негізінде, пайдаланушының есептік жазбасы негізінде бірыңғай инцидентке біріктіру мүмкіндігі іске асырылуы тиіс.
* Оқыс оқиғаны жіктеу мүмкіндігімен пайдаланушылар, активтер, корреляция оқиғалары бойынша - оқыс оқиғаға қосымша ақпаратты қолмен байланыстыру мүмкіндігі іске асырылуы тиіс.

### Визуализация мен есептілікке қойылатын талаптар

* Жүйе келесі нысандар үшін визуализация (дашбордтар) және есептілік құралдарын ұсынуы тиіс:
* Оқиғалар;
* Алерттар
* Инциденттер;
* Активтер;
* Оқиғалардың көздері;
* Белсенді парақтар.
* Жүйе графикалық панельдер (дашбордтар) мен есептердің алдын ала орнатылған жиынтығымен жеткізілуі тиіс.
* Жүйе оқиғалар мен оқыс оқиғалар туралы хабарламалардың пайдаланушы үлгілері мен ережелерін жасау мүмкіндігін қолдауы тиіс.
* Жүйе оқыс оқиғалар бойынша мынадай деректерді графикалық форматта (дашбордтар) көрсетуді қамтамасыз етуі тиіс:
* о құрылған тосын оқиғалар;
* кезең ішіндегі жабық инциденттер;
* сындылығы бойынша жабылмаған инциденттер;
* тосын оқиғаларды бөлу;
* сындылық деңгейі бойынша инциденттер;
* қозғалған активтер мен активтер топтары;
* инциденттердің ең көп саны бар оқиғалардың көздері;
* инциденттердің ең көп санымен корреляциялау ережесі;
* тенанттар бойынша инциденттерді бөлу (өткен кезеңмен салыстырғанда);
* тосын оқиғаларды табу уақыты бойынша бөлу (first seen);
* о инциденттермен қозғалған активтердің санын тенанттар бойынша бөлу.
* Жүйе графикалық форматта (дашбордтар) оқиғалар бойынша келесідей деректерді көрсетуді қамтамасыз етуі тиіс:
* Netflow-да жиі кездесетін ішкі IP мекенжайлары;
* Netflow-да жиі кездесетін сыртқы IP мекенжайлары;
* порттарға қатысты трафик көлемдерінің статистикасы;
* оқиғалар саны ең көп көздер бойынша статистика.
* Жүйе пайдаланушы дашбордтарын және есеп үлгілерін жасау мүмкіндігін қолдауы тиіс.
* Жүйе оқиғалар қоймасына пайдаланушы сұрауларының негізінде графикалық панельдер (дашбордтар) құруды қолдауы тиіс.
* Пайдаланушылық графикалық панельдерді (дашбордтарды) немесе есептерді қалыптастыру және теңшеу графикалық веб-интерфейсте толық орындалуы тиіс.
* Жүйе қолда бар үлгілердің құрамынан есептерді қалыптастыру мүмкіндігін қамтамасыз етуі тиіс:
* көздер бойынша;
* инциденттер бойынша;
* Жүйе инциденттер бойынша есептерді келесідей ақпаратпен құруды қамтамасыз етуі тиіс:
* белсенді оқыс оқиғалардың саны;
* бөлінбеген оқыс оқиғалардың саны;
* уақыт бойынша бөлінген тосын оқиғалар;
* уақыт бойынша соңғы инциденттер;
* сындылық деңгейі бойынша бөлумен оқыс оқиғалардың саны;
* орындаушылар бойынша тосын оқиғалар саны;
* мәртебесі бойынша бөлінетін оқыс оқиғалардың саны;
* қозғалған активтер мен активтер топтары;
* инциденттердің ең көп саны бар оқиғалардың көздері;
* инциденттердің ең көп санымен корреляциялау ережесі;
* қозғалған есепке алу жазбалары;
* құрастырушының көмегімен оқиғалар базасы бойынша еркін іздеу негізінде.
* Жүйе келесі ақпарат көздері бойынша есептерді құруды қамтамасыз етуі тиіс:
* Netflow-да жиі кездесетін ішкі IP мекенжайлары;
* Netflow-да жиі кездесетін сыртқы IP мекенжайлары;
* порттарға қатысты трафик көлемдерінің статистикасы;
* оқиғалар саны ең көп көздер бойынша статистика.
* Жүйе есептерді пошта арқылы жіберу, есепті желілік қоймаға орналастыру және есепті жүйені басқару консолы арқылы жариялау мүмкіндігін қамтамасыз етуі тиіс.
* Жүйе реттелетін кесте бойынша есептерді таратуды қолдауы тиіс.
* Жүйе HTML, CSV, бөлек CSV, XLSX форматында есептерді экспорттау мүмкіндігін ұсынуы тиіс.

**Өнімділік мониторингіне қойылатын талаптар**

* Жүйе Жүйенің барлық компоненттерінің өнімділік метрикаларын жинауды және сақтауды қамтамасыз етуі тиіс.
* Өнімділік өлшемдері Жүйенің графикалық интерфейсінде көрсетілуі тиіс.
* Жүйе кемінде келесі өнімділік өлшемдерін жинауы, сақтауы және көрсетуі тиіс:
* Жадты тұтыну;
* Көздер бойынша бөлумен секундына өңделетін (компонентке кіретін және компонентінен шығатын) оқиғалардың саны;
* Оқиғаларды өңдеудің әрбір кезеңінде уақыттың кідіруі (latency);
* Белсенді тізімдермен жұмыс істеу параметрлері (сұраулардың, кідірістердің саны);
* Сыртқы жүйелермен жұмыс істеу параметрлері (сұраулар саны, кідірістер).
* Жүйе сыртқы мониторинг жүйелеріне өнімділік метрикасын беруді қолдауы тиіс.
* Жүйе белгілі бір шекті мәндер бұзылған жағдайда, пошта хабарламаларын жіберу мүмкіндігін қолдауы тиіс.

### Қауіпсіздік талаптары

* Жүйе рөлдік модель негізінде қол жеткізу құқықтарының аражігін ажыратуды қамтамасыз етуі тиіс;
* Жүйе қол жеткізу оқиғаларын және конфигурацияның маңызды өзгерістерін тіркеуі тиіс;
* Жүйе келесідей тетіктерді пайдалана отырып, аутентификациялау мен авторизациялауды қолдауы тиіс:
* Пайдаланушылардың есептік деректерінің жергілікті базасы (логин-құпиясөз бойынша);
* AD, ADFS, FreeIPA.
* Жүйеде құпиясөзді таңдау әрекеттеріне қарсы әрекет етудің кіріктірілген тетіктері болуы тиіс.

## Пайдалану құжаттамасына қойылатын талаптар

* Жүйенің пайдалану құжаттамасы Пайдаланушы нұсқаулығы мен Әкімші нұсқаулығын қамтуы тиіс.
* Жүйемен жиынтықта жеткізілетін құжаттама тиісті құралды орнату, баптау және пайдалану процесін егжей-тегжейлі сипаттауы тиіс.

## Техникалық қолдауға қойылатын талаптар

Бағдарламалық қамтамасыз етуді техникалық қолдау келесідей талаптарға сәйкес болуы тиіс:

* орыс тілінде РК бүкіл аумағында шешім шығарушының сертификатталған мамандарымен оқыс оқиғалар бойынша ұсынылуы;
* өндірушінің web-сайты орыс тілінде болуы, толықтырылатын білім базасы, сондай-ақ бағдарламалық өнімдерді пайдаланушылардың форумы болуы тиіс;
* оқыс оқиғаларды жасау, жаңарту және мониторингілеу үшін пайдаланушының жеке есептік жазбасын пайдалану мүмкіндігін ұсыну;
* өнімді орнату, конфигурациялау және оның жұмыс істеуі процесінде оқыс оқиғаларды шешу бойынша техникалық қолдау мен кеңес беру;
* мәселенің бизнес-процестерге әсері негізінде техникалық қолдау қызметіне сұранымның басымдығын айқындау;
* стандартты сұраныстарға қатысты кеңейтілген техникалық қолдауды пайдаланушылардың сұраныстарына неғұрлым жоғары басымдық беру;
* сұранымдарды шешудің аралық нәтижелері мен барысы туралы ұдайы хабарлап отыру;
* қызмет көрсету сапасына өңірлік кеңсенің техникалық қолдау көрсету басшысының немесе корпоративтік клиенттермен жұмыс жөніндегі менеджердің деңгейіне наразылықтар мен шағымдар беру мүмкіндігін ұсыну;

Өнімді пайдалану мәселелері бойынша техникалық кеңес беру және оқыс оқиғалардың теріс салдарын жоюға сұранымдарды қабылдау:

* Пайдаланушыға 24x7x365 режимінде (демалыс және мереке күндерін қоса алғанда, тәулік бойы) сұранымдарды орналастыру мүмкіндігімен техникалық қолдау Интернет-порталына қол жеткізуді ұсыну;
* сыншылдық 1 деңгейі сұранымы үшін 24x7x365 режимінде бөлінген басым желінің телефоны бойынша сұраным қабылдау;
* сыншылдық деңгейі 2, 3 және 4 сұранымы үшін жұмыс күндері сағат 10: 00-18: 30 (Алматы уақыты) бойынша бөлінген басым желінің телефоны бойынша сұраным қабылдау;
* Интернет-портал арқылы сұраным салу мүмкін болмаған жағдайда, 24x7x365 режимінде (демалыс және мереке күндерін қоса алғанда, тәулік бойы) электрондық пошта арқылы сұранымды қабылдау;

Реакция уақыты шектілік деңгейіне сәйкес қамтамасыз етілуі тиіс:

|  |  |  |
| --- | --- | --- |
| **Сыншылдық деңгейі** | | **Жауап беру уақыты көп емес:** |
| Сыншылдық деңгейі 1 | Сыншылдық | 2 жұмыс сағатынан |
| Сыншылдық деңгейі 2 | Жоғары | 6 жұмыс сағатынан |
| Сыншылдық деңгейі 3 | Орта | 8 жұмыс сағатынан |
| Сыншылдық деңгейі 4 | Төмен | 10 жұмыс сағатынан |

Өнімге қатысты тосын оқиғалар сындылығының деңгейлері келесідей сипаттамаға сәйкес келуі тиіс:

**Сыншылдық деңгейі 1 (сыншылдық)** Өнімнің немесе Пайдаланушының операциялық жүйелерінің жұмыс қабілеттілігін тоқтату арқылы Пайдаланушы бизнесінің үздіксіздігіне әсер ететін немесе деректерді жоғалтуға, Пайдаланушының стандартты күйге келтіруін қауіпсіз емес режимге орнатуға немесе қауіпсіздікпен басқа да проблемалардың туындауына әкелетін Өніммен байланысты күрделі проблеманы білдіреді, бұл ретте айналма шешім жоқ.

Өнімге байланысты және 1-сындылық деңгейіне сәйкес келетін тосын оқиғалар тізбесі келесідей тосын оқиғаларды қамтиды:

• барлық жергілікті желі (немесе желінің сыншылдық бөлігі) жұмыс істемейді, бұл негізгі бизнес-процестерді тоқтатады.

**Сыншылдық деңгейі 2 (жоғары)** Өнiмнiң функционалдығына әсер ететiн, бiрақ деректердiң зақымдануын/жоғалуын немесе бағдарламалық қамтамасыз етудiң жұмыс қабiлеттiлiгiнiң үзiлуiн тудырмайтын жоғары деңгейдегi сындылық проблемасын бiлдiредi. Сыншылық деңгейі 1 айналма шешім белгілі болғанда Сыншылық деңгейі 2 ретінде қарастырылады.

Өнімге байланысты және Сыншылдық деңгейі 2 - ге сәйкес келетін тосын оқиғалар тізбесі келесідей тосын оқиғаларды қамтиды:

• өнім толығымен істен шықты, бірақ негізгі бизнес-процестердің үздіксіздігі бұзылмайды.

**Сыншылдық деңгейі 3 (орташа)** Өнімнің функционалдығын қозғамайтын күрделі емес проблеманы немесе қызмет көрсетуге сұранымды білдіреді.

Сыншылдық деңгейі 3 - ке сәйкес келетін тосын оқиғалар тізбесі келесідей тосын оқиғаларды қамтиды:

• Өнім ішінара істен шығарылған (сәйкес келмейтін түрде жұмыс істейді), бірақ Өнім жұмысының нәтижесінде Тапсырыс берушінің басқа бағдарламалық қамтамасыз етуі істен шығарылмаған.

**Сыншылдық деңгейі 4 (төмен)** қызмет көрсетуге арналған басқа да сындарлы емес сұранымдарды білдіреді. Жоғарыда аталмаған барлық оқыс оқиғалар осы сыни деңгейге жатады.

Техникалық қолдауға қойылатын қосымша талаптар:

• Бастапқыда Жүйенің стандартты жеткізілімінде қолдау таппайтын деректердің кемінде 10 (он) түрлі типтері үшін Парсерлер жүйесін өндіруші қосымша ақысыз әзірлеуді қамтамасыз ету.

## Әзірлеуші компанияға қойылатын жалпы талаптар

* Әзірлеуші бизнестің, аса маңызды инфрақұрылымның, мемлекеттік органдардың және қатардағы пайдаланушылардың қауіпсіздігін қамтамасыз ететін киберқауіпсіздік бойынша өнімдер, шешімдер мен сервистердің экожүйесіне ие болуы тиіс
* Әзірлеушінің өнімдерінің, шешімдерінің және қызметтерінің экожүйесінің тиімділігі MITRE жіктемесіне сәйкес шабуылды дамытудың барлық кезеңдерінде зерттеумен расталған қорғауға және қауіп-қатерлерді анықтауға ие болуы тиіс
* Әзірлеушінің өнімдерінің, шешімдері мен сервистерінің экожүйесі соңғы нүктелерде жаппай қауіп-қатерден анықтауды және қорғауды қамтамасыз ету жөніндегі шешімдерді қамтуы тиіс
* Әзірлеушінің өнімдері мен шешімдері әртүрлі халықаралық наградаларға ие болуы тиіс және детекторлау және қорғау сапасының деңгейіне тәуелсіз тестілеуге сәйкес көп жылдық көшбасшылық позицияға ие болуы тиіс
* Әзірлеушіде қауіп-қатерлерді зерттеу және талдау бойынша жаһандық сараптама орталықтары болуы тиіс, мысалы:
  + Зиянды бағдарламалық қамтамасыз етуді зерттеу және одан қорғау тәсілдерін жасау жөніндегі жаһандық орталық
  + APT-қатерлерді анықтайтын Жаһандық қауіп-қатерлерді зерттеу және талдау орталығы
  + Инциденттерді тексеру және оларға ден қоюға көмек көрсету жөніндегі жаһандық орталық
  + Өнеркәсіптік нысандарға шабуылдарды зерттеу, анықтау және тергеу жөніндегі жаһандық орталық
* Әзірлеуші Microsoft Active Protection Program, CVE тәрізді немесе ұқсас осалдықтар туралы деректермен алмасудың жаһандық бағдарламаларының қатысушысы болуы тиіс
* Әзірлеушінің портфолиосында сандық криминалистика, зиянды бағдарламаларды талдау және кері әзірлеу, сондай-ақ инциденттерге ден қою бойынша өзіндік оқыту курстары болуы тиіс
* Әзірлеуші Threat Intelligence саласында әлемдік талдау агенттіктерінің мойындауымен белгіленген жетекші жаһандық сараптамаға ие болуы тиіс, ол оның негізінде жұмыс істейтін өнімдердің, шешімдердің және сервистердің меншікті экожүйесіне терең ықпалдасуы тиіс