ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Қаржылық құрылымдарға арналған ақпараттық қауіпсіздік қақтығыстарын басқару жүйелерін жобалау»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Тастемір Бекарыс Тобы: СИБк-15-1
Ғылыми жетекші: с.ғ.к., доцент Бердібаев Р. Ш.

Кеңесшілер:
Экономикалық бөлім бойынша:
э. ғ. к., профессор Аренбаева Ж. Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торгаев Э.Э.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «27» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
с.ғ.к., доцент Бердібаев Р.Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «07» 06 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Макарова Н.Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «07» мамыр 2019 ж.
(қолы)

Пікір беруші:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 201__ ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген

ТАПСЫРМА

Студент: Тастемір Бекарыс
(аты-жөні)

Жобаның тақырыбы: Картөлөк құрылымдарға арналған ақпараттық қауіпсіздік қатерлерін басқару жүйелерін жобалау

2018 ж. «26» 10 № 124 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «12» 06 2019 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Картөлөк құрылымдарға арналған ақпараттық қауіпсіздік қатерлерін басқару жүйелерін жобалау, үйлестіру, оның ішінде ақпараттық қауіпсіздік қатерлерін басқару жүйелері шешімдерін салыстыра отырып, картөлөк құрылымға сәйкес келетін шешімді таңдау

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: Картөлөк құрылымның ақпараттық қауіпсіздігінің ағымдағы тай-күй деңгейін бағалауға, SIEM жүйесін жобалау арқылы картөлөк және бедендік инфрақұрылымдарын ағайтуға, жүйеде байқалатын ақпараттық қатерлерге мүмкіндік беретін әдістерді, сол әдістердің негізінде жұмыс жасайтын бағдарламалық және құрамдық қамтамасыз ететін шешімдерді салыстыра отырып,

қартонық құрылым ақпараттық қауіпсіздігін
күшейтуге тиімді бағдарламамен шешу жасау

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі: 1. Ақпараттық активтердің жалпыздамық кестелері
2. Картонық құрылымның локалды желі түйінінің инфрақұрылымға сұлбасы
3. Ақпараттық қауіпсіздік қатынастарын басқару түйесінің инфрақұрылымдық сұлбасы
4. Шешім ағаштың салыстырмалық сұлбасы

Негізгі ұсынылатын әдебиеттер: 1. Миллер Р.Д., Харрис Ш., Харпер А.А. Security Information And Event Management Implementation. - Нью-Йорк: Network Pro Library, 2011. - 465 с.
2. В.Бондарев. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства. - М.: МГТУ им. Н.Э. Баумана, 2017. 228 с.
3. В. Бондарев. Введение в информационную безопасность автоматизированных систем. - М: Издательство МГТУ, 2016 - 46 с.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім			
экономикалық бөлім	Ерекбаева Ж.Г.	04.03.-31.05.	
өмірттіршілік қауіпсіздігі бөлімі	Торбаев Э.Т.	1.03-27.05	

Диплом жобасын дайындау
КЕСТЕСІ

№ р/с	Тарау аттары, әзірленетін сұрақтардың тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1.	Кіріспе	21.01.2019	
2.	Картоқоқ күрделенген ақпараттық Тәуекелдерін бағалау және Талдау	04.02.2019	
3	Картоқоқ күрделенген ақпараттық қауіпсіздікті қамтамасыз ету жәнелері	18.02.2019	
4.	Тәуекелдерді бағалаудың бағдарламалық құралын таңдау	04.03.2019	
	Картоқоқ күрделенген инфрақұрылымен танысу	26.03.2019	
5	SIEM шешімдерімен танысу, таңдау	02.04.2019	
6	Картоқоқ күрделенген тақырыбына сәйкес шешімді таңдау	16.04.2019	
7	SIEM жүйесін жобалау	17.04.2019	
8	Техникалық - экономикалық негіздеме	18.04.2019	
9	Өміртіршілік қауіпсіздігі	28.04.2019	
10	Қорытынды	15.05.2019	

Тапсырманың берілген уақыты «21» 01. 20 19 ж.

Кафедра меңгерушісі _____ (қолы) с.ғ.к., доцент Бердібаев Р. Ш.

Жоба жетекшісі _____ (қолы) с.ғ.к., доцент Бердібаев Р. Ш.

Орындалатын тапсырманы қабылдаған студент _____ (қолы) Тастемір Бекарыс

Андатпа

Берілген дипломдық жобада Алматы қаласындағы “American Food” жауапкершілігі шектеулі серіктестігі үшін Ақпараттық қауіпсіздік қақтығыстарын басқару жүйесін жобалау жүргізілді.

Жобалау барысында қаржылық құрылымның ақпараттық активтерін бағалау арқылы, қаржылық құрылымның бизнесінің мақсаттарына сай келетін Ақпараттық қауіпсіздік қақтығыстарын басқару жүйесінің шешімдері салыстырыла отырып, ең лайықты FortiSIEM шешімі жобалауға таңдалды.

Дипломдық жобада өмір тіршілік қауіпсіздігі және Ақпараттық қауіпсіздік қақтығыстарын басқару жүйесінің экономикалық тиімділігі қарастырылды.

Аннотация

В рамках данного дипломного проекта была проведена проектирование Системы управления конфликтами информационной безопасности для Товарищества с ограниченной ответственностью “American Food” в Алматы.

В процессе проектирования были сравнены решения Системы управления конфликтами информационной безопасности которые соответствуют бизнес-целям финансового учреждения, путем оценки информационных активов финансовой структуры. И наиболее подходящим решением был выбран FortiSIEM.

Дипломный проект исследует меры безопасности жизнедеятельности и экономическую эффективность Системы управления конфликтами информационной безопасности.

Abstract

As part of this graduation project, an Information Security Conflict Management System was designed for the American Food Limited Partnership in Almaty.

In the design process, decisions were made to compare Information Security Management System Conflicts that meet the business objectives of a financial institution, by evaluating the information assets of the financial structure. And the most suitable solution was chosen by FortiSIEM.

The graduation project examines the safety measures of life and the cost-effectiveness of the Information Security Conflict Management System.

Мазмұны

Кіріспе

Қаржылық құрылым - ҚР азаматтық заңнамасына сәйкес қызметінің негізгі мақсаты пайда табуды көздейтін заңды тұлға болып табылады.

Қазіргі әлемде ақпараттық технологиялар тез дамып келе жатқанда, қаржылық құрылымдардың ақпараттық құрылымын күтетін қауіп-қатерлер саны мен сапасы да олардан қалысар емес, сол себепті қаржылық құрылым ақпараттық қауіпсіздікті қамтамасыз етуі керек. Қаржылық құрылым жеткілікті мөлшерде үлкен болса, кейбір «қарапайым», мысалы, антивирус, оның ақпараттық қауіпсіздігін қамтамасыз ету үшін жеткіліксіз екенін түсінеді. Әрине, қаржылық құрылымда ақпараттық қауіпсіздік бойынша кем дегенде бір маман бола алады, бірақ ол кәсіпорында ақпараттық қауіпсіздік қызметкерін толық қорғай алмайды. Мамандарға SIEM жүйесі қолайлы көмекке айналады.

Осылайша, SIEM (Secunity Information and Event Management) ақпараттық технологиялардың эволюциялану барысында екі бағдарламалық қамтамасыз етуді құралдарының бірігуінен пайда болған: SIM (Security Infomation maast) ақпараттық қауіпсіздік менеджменті және SEM (Қауіпсіздік оқиғаларын басқару) қауіпсіздік оқиғаларын басқару. SIEM жүйелері класы ақпараттық қауіпсіздікті басқару құралдарының бірі болып табылады, бірақ олар тәуелсіз шешім ретінде ақпараттық қауіпсіздік оқиғаларын шоғырландыру үшін пайдаланылмайды, себебі олардың негізгі міндеті қаржылық құрылым ішіндегі инциденттерді анықтау. SIEM жүйелері көптеген қатерлерді анықтау үшін: DLP жүйелері, IDS / IPS жүйелері, антивирустық қосымшалар, серверлік және жұмыс станцияларының оқиғалар журналдары, брандмауэрлер, желі белсенді жабдықтары сияқты ақпаратты көздерін пайдалана алады: желілік шабуылдар, вирустық шабуылдар инфекциялар, құпия ақпаратқа рұқсатсыз қол жеткізу, ақпараттық жүйелердің қателіктері мен ақаулықтары, әрекеттер мен қолданыстағы мақсатты шабуылдар, осы тізімді көптеген заттармен жалғастыруға болады. Дәстүрлі түрде SIEM жүйесі бірнеше құрамдас бөліктерден тұрады: агенттер (SIEM жүйелері әртүрлі ақпарат көздеріне ие болғандықтан, ақпарат жинау және т.б.):

- сервер-коллекторлар (оқиғаларды алдын-ала жинақтау);
- сервер-коррелятор (алынған ақпаратты талдау);
- деректер базасының сервері және сақтау сервері. Бірақ ақпарат қауіпсіздігі саласындағы шығындары шектеулі компаниялар үшін жақында бірыңғай модулінде ақпаратты сақтау, іздеу және корреляциялау мүмкіндігі бар, барлығы бір-бірінде SIEM жүйесі пайда болды.

1 Жұмыс өзектілігі

Ақпараттық қауіпсіздік және оқиғаларды басқару (SIEM) ірі қаржылық құрылымдардың басты ақпараттық қауіпсіздікті қамтамасыз ету құралы болып табылады, себебі қаржылық құрылымның басты активі және мақсаты қаржы болып табылады. Бұл қаржылық құрылымның IT қауіпсіздігінің тұтас көзқарасын, сондай-ақ әртүрлі нормативтік талаптарға қатысты маңызды мәліметтерді беретін есеп беру құралы.

Бүгінде SIEM жүйелерінің көпшілігі деректерді жинау агенттерінің иерархиялық тұрғыдан соңғы пайдаланушы құрылғыларынан, серверлерден, желілік жабдықтан және брандмауэрлерден, антивирустық жүйелерден немесе кіруді болдырмау жүйелерінен қауіпсіздікке байланысты оқиғаларды жинау үшін жұмыс істейді. Жиналғандар оқиғаларды бағыттау орталықтандырылған басқару консоліне жібереді, мұнда қауіпсіздік талдаушылары шуды, қосылуға арналған нүктелерді және қауіпсіздік оқиғаларын басымдыққа бөледі.

SIEM өнімдерін жобалау кезінде ескерілетін маңызды ерекшеліктердің бірі:

1) Басқа басқару элементтерімен біріктіру. Жүйе шабуылдарды болдырмау немесе тоқтату үшін басқа кәсіпорынның қауіпсіздік құралдарын басқара алады ма?

2) Жасанды интеллект - жүйе машиналар мен терең оқу арқылы өз дәлдігін жақсарта алады ма?

3) Қауіптілік талдау арналары - жүйе ұйым таңдаған қауіп-қатер аналитикалық арналарын қолдана алады ма, әлде нақты арнаны пайдалану керек пе?

4) Сәйкестік туралы есептер. Жүйе жалпы талаптарға сәйкестік туралы кіріктірілген есептерді қамтиды ма және ұйымдар жаңа сәйкестік есептерін теңшеу немесе жасау мүмкіндігі бар ма?

5) Ақпараттық мүмкіндіктер. Жүйе қауіпсіздік оқиғалары туралы қосымша ақпарат жинайды ма?

Ақпараттық қауіпсіздік және оқиғаларды басқару (SIEM) желі қосымшалары мен жабдықтары арқылы туындаған қатерлер мен қауіпсіздік ескертулерін нақты уақыт талдауға мүмкіндік береді. Ол түрлі қауіпсіздік деректерін сақтау, басқару, талдау және есеп беруді басқарады және түрлі оқиғалар мен ескертулерді салыстыруға мүмкіндік береді.

SIEM нормативтік талаптарға сәйкестікте рөл атқарады және оны елемеуге болмайды. Жақсы қамтамасыз етілген ақпараттық қауіпсіздік және оқиғаларды басқару шешімі қауіпсіздік оқиғалары мен ақпараттың орталықтандырылған көзқарасын қамтамасыз ететін кибершабуылдардан бір қадам алдауға мүмкіндік береді.

2 Ақпараттық қауіпсіздік қақтығыстарын басқару жүйесін жобалау

2.1 SIEM компоненттері

SIEM-дің SIEM-ді табысты іске асыруға қатысуы қажет бірнеше негізгі компоненттері немесе маңызды функциялары бар:

- журналдар мен оқиғаларды басқаруды қамтитын деректерді біріктіру. SIEM бір маңызды қауіпсіздік оқиғасын өткізіп жібермеу үшін әртүрлі дереккөздерден деректер мен журналдарды жинау құралы;
- маңызды және пайдалы ақпарат алу үшін түрлі оқиғаларды бір-бірімен байланыстыратын жалпы тенденциялар мен атрибуттарды іздейтін корреляция құралы;
- байланысты оқиғаларды автоматты түрде талдауды қамтитын хабарландыру және IT-менеджерлеріне кез келген ықтимал мәселелер туралы хабарлау туралы ескертулер жасау құралы;
- өңделмеген ақпаратты түсінікті, мысалы, диаграммалар, сызбалар және сызба диаграммалар түрінде түсінуге оңайырақ түрге өңдеуге болатын құралдарды қамтитын бақылау тақталары;
- сәйкестікке қатысты деректерді автоматты түрде жинайтын әртүрлі құралдарды қамтитын талаптарға сәйкес болу, сондай-ақ компанияның нормативтік талаптарға сәйкестігін растайтын есептерді жасайтын құрал;
- деректер мен оқиғалар ұзақ мерзімді кезеңде қалай сақталатындығын, сондай-ақ тарихи деректермен не істейтінін сипаттайтын сақтау орны;
- оқиғаларға қол жеткізуге және түрлі түйіндерде әртүрлі уақыттан деректерді алуға мүмкіндік беретін құралдар.

2.2 SIEM жүйесін жобалау этаптары

SIEM жүйесін жобалау бірнеше кезеңдерден тұрады:

1) Анықтау және жоспарлау кезеңі. Кез-келген бизнес-үдерісте және IT-дегідей, SIEM жүйелерін енгізу мұқият жоспарлау мен талдаудан басталады.

Ұйым үшін SIEM-ді енгізуге кірісе отырып, алдымен бизнестің қайда екендігін және бизнес үшін SIEM-нің қандай мақсаттарға жетуі керектігін экономикалық тұрғыдан талдау керек. Бастапқы мақсаттар мен міндеттер тізімін құрастыра бастап және оларды ұйым үшін маңыздылығына қарай бағалау керек. Сондай-ақ іске асыруды қолдау үшін қандай міндеттер мен процестер маңызды екенін түсіну керек және тиісінше басымдықты белгілеу керек.

Қауіпсіздік саясатын да тексеріп, әдеттегідей, осы саясаттың қайсысы басымдықты болуы керек екенін білу керек:

- бизнестің қандай саясаты маңызды;
- компания ережелерін ұстану үшін қандай саясат маңызды;
- саясаттардың қайсысы қолданыста үздік болып табылады.

Сәйкестікті қамтамасыз етуге көмектесу үшін ағымдағы бақылау элементтерін (осы қауіпсіздік саясаттарын тексеру үшін пайдаланылады) түсінуі керек. SANS.org осы нұсқаулықтағы 20 маңызды бақылау элементін

сипаттайды, бұл қажеттіліктерді зерттеу және ресурстар, басқару құралдары және бизнес мақсаттары арасындағы қарым-қатынастарды анықтау үшін жақсы нүкте болып табылады. «Егер ұйым жалпы алғанда 20 сыни бақылауды жүзеге асыру жоспарын жасаса, SIEM енгізілген алғашқы бақылаудың бірі болуы керек», - деп түсіндіреді SANS.org. «Зияндылық сканерлері (SCAP-ге негізделген), ақ тізімді құралдар және басқа арнайы бақылау құралдары маңызды, бірақ олар SIEM-ге қарағанда тиімді бақылауды жүзеге асыру үшін нақты бақылауға сүйенбейді. Себебі SIEM осы құралдардың барлығынан деректерді жинай алады және тіпті ұйымдарға олардың осалдығын түсінуге, қауіпсіздік мәселелерін анықтауға және түзетуге және қауіпсіздікті арттыруға көмектесу үшін пайдалы».

Зерттеу кезеңінде әдетте SIEM жүйесін қолданыстағы технологиялар мен ұйымдастыру саясаттарының кішігірім, бірақ өкілдік жиынтығымен іске асыруға қолданады, ол сізге толығымен қолданар алдында өзгерістер мен жақсартулар туралы хабарлауға болатын маңызды деректерді жинауға мүмкіндік береді. Негізгі міндеттердің бірі – бақылау іс-шараларын жүзеге асырудағы әлсіз жақтар мен кемшіліктерді анықтау және оларды шешу жоспарларын жүзеге асыру. Дұрысында, бұл қауіпсіздік элементтері мен басқару элементтері SIEM іске асырылуында туындайтын кез келген бос орындарды жоюға мүмкіндік беруі керек. Әйтпесе, олар мониторинг және ескерту процестерінің мәнін арттырмайды.

2) Пилоттық кезең. Іске асыру сатысынан бастап екі мақсатты ескеру керек:

- SIEM жүйелерін көрсету инвестицияларды қайтаруды қамтамасыз етеді;

- жұмыс кітабы ретінде белгілі жұмыс үлгісі бар.

Зерттеу сатысында SIEM-ді ұйымыңыздың барлық құрылғылары мен саясаттарын көрсететін кішігірім жиынтықта пайдалану керек. Пилоттық кезеңге шыққанда, бірінші кезеңде жиналған деректерден алынған сабақты қолдана отырып және саясат пен құрылғылардың кең жиынтығына жасалған жақсартуларды іске асыру керек, бірақ пилоттық кезең мұнымен аяқталмайды.

Пилоттық сатыда анықтау кезеңінде жасаған барлық жорамалдар қамтылған құралдардың санының артуымен жұмыс істеу кезінде мұқият сынақтан өту керек. Қанағаттанарлық сынақ нәтижелеріне қол жеткізгеннен кейін, басқарылатын орналастыру кезеңіне өтуге қажетті барлық деректер мен мәліметтерге ие болу керек.

3) Басқарылатын орналастыру кезеңі. SIEM-ді орналастыруды бір жылдам қадамда аяқтауға тырыспау керек. Басқарылатын қондыру фазасы кезінде алдымен біртіндеп және бірте-бірте қуатты арттыру керек.

Басқарылатын орналастыру кезеңі сыйымдылықты арттыру арқылы толық орналастыруға дейін жету процесі және де ол юізге нақты өндірістік ортада сынақ кезеңі ретінде жұмыс істей алады. Бұл кезеңде барлық процестер, процедуралар мен операциялар тапсырма журналында нақты көрсетілуі керек.

4) Үздіксіз жақсарту фазасы. SIEM-ді табысты орнату - бұл бір жолғы нәрсе емес. Өйткені, хакерлер ешқашан шабуылдың күрделі әдістерін әзірлеуді тоқтатпайды, сол себепті әлеуетті қаскүнемдерден бір қадам алда тұруды жалғастыра беру керек.

Бақыланған орналастыру сатысынан кейін және SIEM жүйесін одан әрі пайдалану және орналастырудан кейін, өндірістегі заттардың қалай жұмыс істейтіні туралы қосымша мәліметтер ала аламыз. Бұл мәліметтер мен ақпаратты орналастыруды дәл баптау және ұйымның қауіпсіздік саясаты мен процестерін дамыту үшін пайдалану керек. Бұл SIEM қондырғыларын үнемі өзгеріп отырады дегенді білдіреді және бұл процесс ешқашан тоқтатылмауы керек.

5) SIEM жобалаудың ең үздік тәсілдері. SIEM іске асырудың ең жақсы тәсілі? Бірте-бірте. Қадамдық тәсіл қазіргі жүйелер туралы көбірек білуге және стратегияны бөлік арқылы жүзеге асыруға көмектеседі, бұл орнату кезінде түзетуге мүмкіндік береді. Егер осалдықтарды қараусыз қалса, жобалауда қателер немесе кемшіліктер бар болса, оларды қай жерде және қалай түзетуге болатынын оңай анықтауға болады. Сондай-ақ, әр қадам үшін қосымша деректерді алуға және болашақта қолдануды жақсарту үшін осы ақпаратты пайдалануға болады.

Бұл SIEM жобалаудың жалғыз үздік тәсілі емес. Басқа да озық тәжірибелерді қолдану үшін:

- шешімдерді қараудан және бағалаудан бұрын қолдану жағдайларын нақты түсіну керек;
- ең нашарына дайын болу керек, әрқашан ең нашар сценарийлерді ойластыру керек, сондықтан оларды жеңе алатын құралдарды тікелей таңдауға мүмкіндік болады;
- сыртқы немесеішкі желіден келетін осалдықтарды анықтауға көмектесу үшін IP мекенжайының беделі туралы деректерді пайдалану керек;
- құралдардың ең соңғы қауіп туралы ақпараты бар екеніне және жүйелі түрде жаңартылғанына көз жеткізу керек;
- бірнеше тапсырманы орындай алатын SIEM құралдарын таңдау керек. Әмбебап құрал-саймандар бақылау, қолдау және басқару үшін көптеген құралдар бар екенін білдіреді. Қазіргі уақытта осалдықты бағалау, активтерді анықтау, сымсыз кіруді анықтау, желіні талдау, журналды басқару және файлдардың тұтастығы мониторингі сияқты көптеген кіріктірілген қауіпсіздік құралдары бар. Мысалы, журналды басқару құралдары жиі SIEM санатына кіреді, бірақ журнал басқаруы мониторинг, метрикалар және оқиғалар туралы есептермен бірге маңызды деректерді тереңірек және толыққанды ұсынуды қамтамасыз етеді.

2.3 SIEM жобалауды жетілдіру тәсілдері

SIEM жүйесінің тек биылғы талаптарға ғана сәйкес келмейтіндігін қамтамасыз етудің ең тиімді жолы оны болашақ талаптарға сәйкес болуын жоспарлау болып табылады. Мұны істеудің үш жолы бар:

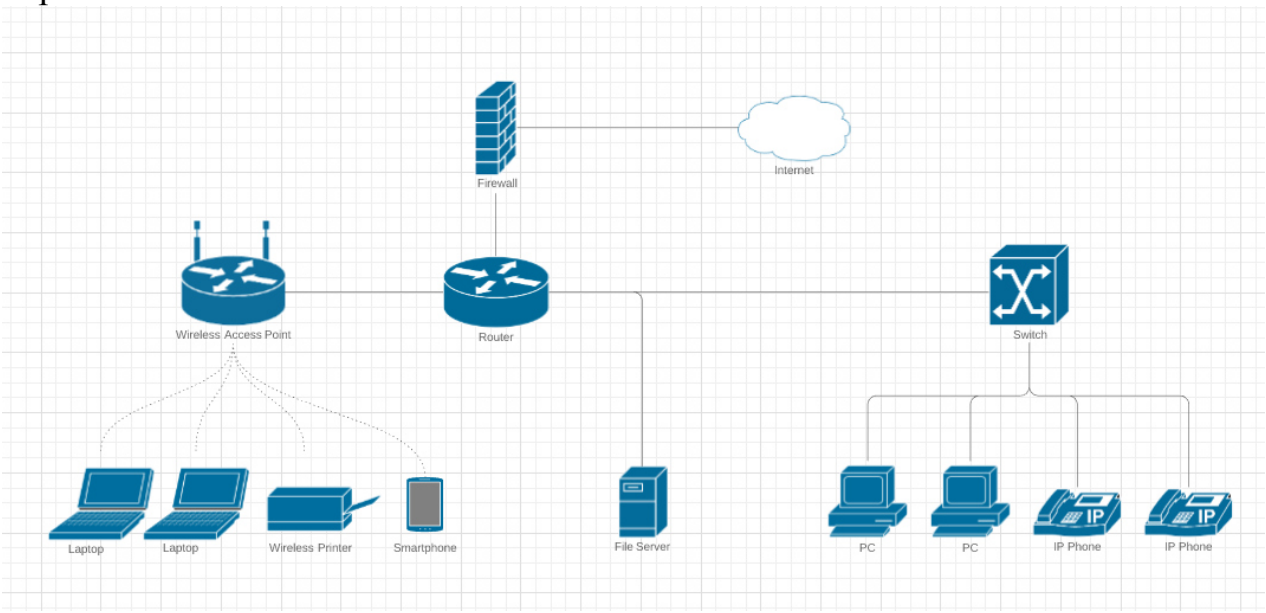
1) SIEM шектеулерін құрыңыз. SIEM - бұл кәсіпорынның қауіпсіздігі үшін пайдалы шешім. Дегенмен, жүйе техника мен қызметкерлерге қосымша қаражат салмаса ол оны тиімсіз ете алатын шектеулерге ие. SIEM-ді бастапқы нүкте ретінде қолдану және оны нәтижеге көп мәнмәтін беретін деректерді басқару шешімімен біріктіру арқылы осы шектеулерді айналып өтуге болады. Жиналған деректердің мағынасын жақсы түсіну арқылы келесі 5-10 жылда пайда болатын сақталу жағдайларына дайын болуға болады.

2) SIEM IT аудит шешімін толтықтыру. Көптеген IT мамандары SIEM шешімдерінде жүйенің аудит деректерінде деректер болмау кемшіліктері бар деп санайды. SIEM-ді табысты қадағалайтын және есеп беру журналында есеп беру үшін IT-аудит шешімімен біріктіру SIEM-ді желіңіздегі оқиғалар туралы сұраққа дұрыс жауап табуды жеңілдететін мүмкіндіктермен қосуы немесе ауыстыруы мүмкін. Бұл биылғы жылы қаншалықты үйлесімділікке қарамастан, сіз болашақта Сәйкестіктің басқа түріне қажетті деректерді жинап, жүйелеуге мүмкіндік береді.

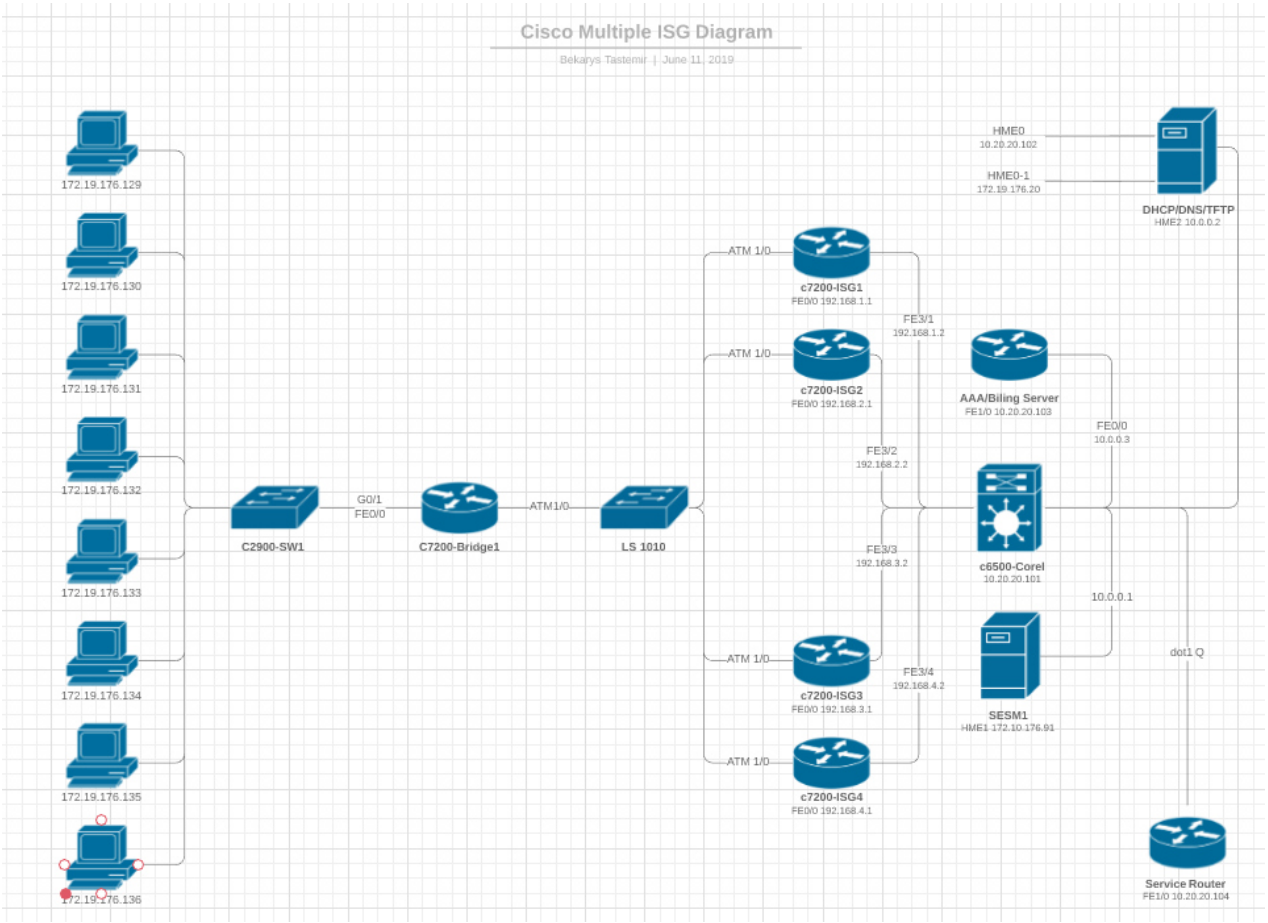
3) Алдымен қауіпсіздікке назар аудару керек. Технологиядағы жоспарлауды өзгерту тұрақты болып табылады, және сәйкестікті жоспарлау өзгеше емес. Сондықтан ең тиімді IT бөлімшелері болашақта SIEM шешімдерін жоспарлайды. Компания үшін сәйкестік үнемі кеңейтетін қозғалыстағы мақсат болуы мүмкін. Тек қана нақты сәйкестік түрлеріне назар аударудың орнына, тиімді SIEM жүйесі сіздің қажеттіліктеріңізге сәйкес икемді болуы керектігін есте сақтау керек.

2.4 SIEM жобаланатын құрылымның инфраструктурасы

Жобалау үшін мен ТОО «American Food» қаржылық құрылымын алдым. Компанияның желілік инфрақұрылымы төменде (2.1-сурет және 2.2-сурет) көрсетілген:



Сурет 2.1 – ТОО “American Food” желілік инфрақұрылымы



Сурет 2.2 – ТОО “American Food” ішкі инфрақұрылымы

Сызбадан көріп отқанымыздай компанияның ішкі инфрақұлымы көптеген дербес компьютерлерден, компьютерлерді біріктіретін компанияның ішкі желісіне біріктіретін желілік коммутаторлардан тұрады.

Сыртқы желісі ішкі желі мен серверді байланыстаратын Cisco 9336-PQ маршрутизаторынан, және Fujtsu RX2510 серверінен тұрады. Жобаланылататын ақпараттық қауіпсіздік қақтығыстарын басқару жүйесі серверге келіп түскен ақпараттың бәріне талдау жасап, оны өңдеп отыруы керек болғандықтан, жүйені серверден кейін орнатамыз.

Жобалау кезінде SIEM шешемінің екі құрылғысын орналастыруға шешім қабылдадым. Себебі, бір құрылғы оқиғалардың бәрін өңдеп үлгермесе немесе істен шыққан кезде, бүкіл түсіп отқан деректер ағыны екінші құрылғыға бағытталатын болады. Осы арқылы қатіліктерге қарсы тұруды күшейте аламыз.

2.5 Қаржылық ұйымның ақпараттық активтері

Ақпараттық актив – бұл сәйкестендіруге мүмкіндік беретін деректер. Белгілі бір ұйымға тиесілі және ол үшін құндылыққа ие. Кез-келген материалдық тасымалдаушыда оны өңдеуге, сақтауға немесе жіберуге мүмкіндік беретін пішінде сақталынады.

Қаржылық ұйымдағы ақпарат келесідей бөлінеді:

- экономикалық мәліметтер.
- сыртқы қаржылық мәліметтер.
- коммерциялық ақпарат.

Экономикалық ақпаратқа мыналар кіреді:
• қаржылық ақпарат (кәсіпорынның активтері мен міндеттемелері, айналымы, сату құны, кірістер мен шығыстар, салықтар және т.б.);
• кредиттік және талдамалық ақпарат (өтімділік, кірістілік коэффициенттері туралы ақпарат);
• төлем және аналитикалық ақпараттар (төлем мерзімдері және т.б.);
• қаржылық рейтингі.

Сыртқы қаржылық ақпарат мыналарды қамтиды:
• серіктестер мен бәсекелестердің қаржылық тұрақтылығы мен төлем қабілеттілігі туралы;
• бағалар, тарифтер, дивидендтер, тауарға, акцияларға, валюта нарықтарына деген қызығушылық;
• биржада және биржадан тыс нарықтардағы жағдай;
• кәсіпкерлік субъектілерінің қаржылық және коммерциялық қызметі;
• қаржылық болжамдар.

Коммерциялық ақпарат мыналарды қамтиды:
• нарық құрылымында;
• нарықтағы кәсіпорын сегменті;
• сұраныс;
• ұсыныс;
• бәсекелестер;
• тұтынушылар;
• бәсекелес тауарлар;
• жеткізушілер.

Ақпараттық қолдаудың маңызды бөлігі - ішкі және сыртқы нормативтік ақпараттар - заңды және нормативтік актілер туралы ақпарат және олардың практикалық қолданылуы, құқықтық емес реттеудің қолданыстағы әдістері, сондай-ақ мемлекеттік инновациялық инфрақұрылым - инновациялық технологиялық қызметті қолдау саласында жұмыс істейтін ұйымдар туралы ақпарат, оның ішінде инновацияларды қаржылық қолдау көрсететін ұйымдар.

Ақпараттың ерекше бөлігі табысты инновациялық жобалар туралы, сондай-ақ сәтсіз жобалар туралы, оларды талдау және өмірлік циклді бақылау нәтижелері туралы деректер болып табылады.

Мемлекеттік деңгейде инновациялық дамыған ақпараттық инфрақұрылыммен инновациялық процестің барлық қатысушылары ашық ақпарат тұжырымдамасын және бұлттық қызметтерді пайдалану арқылы осы ақпаратқа қол жеткізуге болады. Оларды болмаған жағдайда, инновациялық

қызметті жүзеге асыратын кәсіпорын ақпараттық-аналитикалық қызметпен айналысатын компаниялар қызметтерін пайдалана отырып, сыртқы ақпаратты беру және осы мәселелерді шешу үшін өз ресурстарын пайдалана алады.

Ақпараттық инфрақұрылымның негізгі функциялары:

• кәсіпорындардың ішкі ақпаратын сақтауды қамтамасыз ету;

• қызметкерлерді инновациялық қолдаудың сыртқы ақпараттық көздеріне қолжетімділікті қамтамасыз ету;

• әлеуетті пайдаланушыларға ақпарат беру;

• ақпараттың (әсіресе жаңа әзірлемелердің) пайдаланылуы бойынша кеңес беруді ұйымдастыру және оның көздерімен жұмыс істеу;

• ақпараттың аналитикалық өңдеуі;

• ақпаратты ыңғайлы түрде ұсыну.

Ақпараттық активтердің құндылығын анықтау үшін, алдымен ақпараттық активтерді алдымен санаттарға бөлуіміз керек:

- адам ресурстары;
- ақпараттық активтер (қоғамдық және құпия ақпарат);
- бағдарламалық қамсыздандыру ресурстары (бағдарламалық өнімдер, деректер базалары, корпоративтік қызметтер, мысалы, 1С, Банк-клиент және т.б., сондай-ақ тәуелді аппаратуралар);
- физикалық ресурстар (серверлер, жұмыс станциялары, желілік және телекоммуникациялық жабдықтар, мобильді құрылғылар қоса алғанда);
- қызметтік ресурстар (электрондық пошта, веб-ресурстар, онлайн-қоймалар, деректерді беру арналары және т.б.);
- үй-жайлар (онда ақпарат өңделеді және сақталады).

Ақпараттық ресурстардың құндылығын анықтау үшін келесі 2.1 кестені қолданамыз:

Кесте 2.1 – Активтерді бағалау шкаласы

Параметр/мағынасы	Ақпарат сыншылдығы		
Ақпарат түрінің құндылығы	Қауіпті (3балл)	Айтарлықтай (2 балл)	Елеусіз (1 балл)
Аса құпия ақпарат (4 балл)	7	6	5
Құпия ақпарат (3 балл)	6	5	4
Ішкі ақпарат (2 балл)	5	4	3
Ашық ақпарат (1 балл)	4	3	2

Енді қаржылық ұйымның ақпараттық активтерін құндылық коэффициентін анықтау үшін 2.2 кестені қолданамыз:

Кесте 2.2 – Активтердің құндылық коэффициенті

Ақпарат категориясы	Ашық ақпарат	Құпия ақпарат			
		Басқару, коммер.	Техникалық	Қаржылық. бухалтер.	Жеке ақпарат
Коэффициент	1	1.4	1.3	1.2	1.1

Ақпараттық активтің құндылығын анықтау үшін қауіптің пайда болу ықтималдылығын 2.3 кестеде анықтаймыз:

Кесте 2.3 – Жоғалтуларды анықтау және қауіптің орын алу ықтималдылығы

Жоғалтулар	Қауіптің орын алу ықтималдылығы		
	Елеусіз, < 1%	Елеулі, 1% бен 10 % арасында	Жоғары, 10% көп
Айтарлықтай емес	1	2	2
Айтарлықтай	2	2	2
Қауіпті	2	3*	3*

3* - қаржылық ұйымға қабылдауға келмейтін және қалайда болса жойылуға тиіс.

Қауіптердің пайда болу ықтималдылығын 2.4 кестеде белгілі бір периодта пайда болу жиілігіне айналдырамыз

Кесте 2.4 – Қауіптердің белгілі бір периодта пайда болу жиілігі

Жиілік (Ву)	Белгілі бір периодта қауіптің пайда болу ықтималдылығы	Ықтималдылық деңгейі
0,05	ешқашан іске асырылмайды	өте төмен
0,6	бес жылда 2-3 рет	өте төмен
1	жылына 1 бер	төмен деңгей
2	жарты жылда 1 рет	төмен деңгей
4	үш айда 1 рет	орташа деңгей

2.4-кестенің жалғасы

6	екі айда 1 рет	орташа деңгей
12	бір айда 1 рет	жоғарғы деңгей
24	айына 2 рет	жоғарғы деңгей
52	аптасына 1 рет	өте жоғарғы деңгей
365	күнделікті	өте жоғарғы деңгей

2.6 SIEM шешімін таңдау

SIEM шешімін таңдамастан бұрын алдымен бірнеше қадамдардан өтуіміз керек.

Ақпараттық қауіпсіздікті қамтамасыз ету үшін күрделі активтерді анықтаңыз. Біріншіден, ұйымның қауіпсіздікке қатысты тәуекелдерді басқару арқылы күрделі активтерді анықтау болып табылады. Сәйкестендіру басымдылыққа әкеледі. Ешбір компанияда бәрін бірдей қорғайтын ресурстар жоқ. Активтерді басым ету ұйымға өзінің қауіпсіздігін барынша ұлғайтуға мүмкіндік береді.

Активтерді басымдықты ету SIEM шешімін таңдауға да көмектеседі. Компаниялардың қажеттіліктерін түсіну сонымен қатар пайдаланылатын SIEM платформасын кеңейтуге мүмкіндік береді. SIEM технологиясы әлдеқайда теңдестірілмей, төмен деңгейлі талаптарға көмектеседі.

Кәсіпорынның көрінуі – тағы бір мақсат. Бұл орналастырудың әлдеқайда жоғары деңгейін талап етеді. Бұл мақсат арнайы конфигурацияны қажет етпейді. Сіздің компанияңыз сіздің мақсаттарыңызды біле ме? Инвестициядан бұрын толық стратегияны қалыптастыру үшін уақыт бөліңіз.

SIEM бағдарламалық жасақтамасын түсіну үшін қызметкерлерді оқыту Екінші қадам – толық уақытты қызметкерлердің SIEM-ті платформа ретінде түсінетініне көз жеткізу.

Жүйелік журналдар SIEM технологиясының шешімдерін бақылайды? Компанияңыз әртүрлі журналдарды пайдаланады ма? Деректерді түрлі бөлімдерде басқаша өңдей аласыз. SIEM сізге көмектескенге дейін бұл журналдарды қалыпқа келтіруіңіз керек. Түрлі журналдар жүйеге өзінің мүмкіндіктерін барынша арттыруға немесе тиімді есептер беруге мүмкіндік бермейді. Неліктен? Деректер сәйкес емес.

Масштабтау стратегиясын жасаңыз. Кейбір компаниялар кеңейтіле отырып, журнал жүргізу стратегияларын қайталайды. Серверге деген қажеттілік уақыттың ішінде артады. Сонымен қатар, компания тіркеу ережелерін қайта жасайды. Журнал файлдары уақыт өте келе көшіріледі. Ол

компания сатып алынған немесе басқа біріктірілген болса, жазбаларды сақтауға көмектеседі.

Серверлер әртүрлі уақыт белдеулерінде және орындарда таратылса, өміршең стратегия құру қиынға соғады. Ең дұрысы, ұйымыңыз пайдаланатын уақыт белдеуін стандарттау керек. Бұл қадамды елемеу нәтижесінде синхрондалмаған уақыт маркалары пайда болуы мүмкін. Ақырында, жүйедегі ықтимал оқиғаларды сұрыптауды теңшеңіз.

SIEM шешімі сіздің қажеттіліктеріңізге сәйкес келетінін тексеріңіз. Әрбір қауіпсіздік және оқиғаларды басқару туралы ақпарат журнал жинау талабымен бірге келеді. Мысалы, syslog журналдары сыртқы агенттер арқылы қосылады. Microsoft журналдары жергілікті орнатылған агенттермен жұмыс істейді. Журналдар кейін қашықтағы процедурадан немесе Windows басқару құралынан орталықтан жиналады. Тек содан кейін олар журналдарды жинайтын құрылғыларға ауыстырылады.

Басшылық әрбір басым активтің қауіпсіздік қажеттіліктерін анықтауға жауапты. Бұл өлшенетін және тиімді SIEM нәтижелерін алу үшін маңызды.
Тек маңызды активтерді тіркеңіз (бірінші). Толық журнал ортасын орнатқаннан кейін қосымша функциялар пайда болуы мүмкін. Бұл қадамды басқару қателерді болдырмауға көмектеседі. Сондай-ақ, SIEM тестіленгенше, жалпы міндеттемені төмендетуге көмектеседі.

2.7 SIEM шешімін таңдау критерийлері

SIEM шешімін таңдамастан бұрын алдымен бірнеше қадамдардан өтуіміз керек.

Ақпараттық қауіпсіздікті қамтамасыз ету үшін күрделі активтерді анықтаңыз. Біріншіден, ұйымның қауіпсіздікке қатысты тәуекелдерді басқару арқылы күрделі активтерді анықтау болып табылады. Сәйкестендіру басымдылыққа әкеледі. Ешбір компанияда бәрін бірдей қорғайтын ресурстар жоқ. Активтерді басым ету ұйымға өзінің қауіпсіздігін барынша ұлғайтуға мүмкіндік береді.

Активтерді басымдықты ету SIEM шешімін таңдауға да көмектеседі. Компаниялардың қажеттіліктерін түсіну сонымен қатар пайдаланылатын SIEM платформасын кеңейтуге мүмкіндік береді. SIEM технологиясы әлдеқайда теңдестірілмей, төмен деңгейлі талаптарға көмектеседі.

Кәсіпорынның көрінуі – тағы бір мақсат. Бұл орналастырудың әлдеқайда жоғары деңгейін талап етеді. Бұл мақсат арнайы конфигурацияны қажет етпейді. Сіздің компанияңыз сіздің мақсаттарыңызды біле ме? Инвестициядан бұрын толық стратегияны қалыптастыру үшін уақыт бөліңіз.

SIEM бағдарламалық жасақтамасын түсіну үшін қызметкерлерді оқыту Екінші қадам – толық уақытты қызметкерлердің SIEM-ті платформа ретінде түсінетініне көз жеткізу.

Жүйелік журналдар SIEM технологиясының шешімдерін бақылайды? Компанияңыз әртүрлі журналдарды пайдаланады ма? Деректерді түрлі бөлімдерде басқаша өңдей аласыз. SIEM сізге көмектескенге дейін бұл

журналдарды қалыпқа келтіруіңіз керек. Түрлі журналдар жүйеге өзінің мүмкіндіктерін барынша арттыруға немесе тиімді есептер беруге мүмкіндік бермейді. Неліктен? Деректер сәйкес емес.

Масштабтау стратегиясын жасаңыз. Кейбір компаниялар кеңейтіле отырып, журнал жүргізу стратегияларын қайталайды. Серверге деген қажеттілік уақыттың ішінде артады. Сонымен қатар, компания тіркеу ережелерін қайта жасайды. Журнал файлдары уақыт өте келе көшіріледі. Ол компания сатып алынған немесе басқа біріктірілген болса, жазбаларды сақтауға көмектеседі.

Серверлер әртүрлі уақыт белдеулерінде және орындарда таратылса, өміршең стратегия құру қиынға соғады. Ең дұрысы, ұйымыңыз пайдаланатын уақыт белдеуін стандарттау керек. Бұл қадамды елемеу нәтижесінде синхрондалмаған уақыт маркалары пайда болуы мүмкін. Ақырында, жүйедегі ықтимал оқиғаларды сұрыптауды теңшеңіз.

SIEM шешімі сіздің қажеттіліктеріңізге сәйкес келетінін тексеріңіз. Әрбір қауіпсіздік және оқиғаларды басқару туралы ақпарат журнал жинау талабымен бірге келеді. Мысалы, syslog журналдары сыртқы агенттер арқылы қосылады. Microsoft журналдары жергілікті орнатылған агенттермен жұмыс істейді. Журналдар кейін қашықтағы процедурадан немесе Windows басқару құралынан орталықтан жиналады. Тек содан кейін олар журналдарды жинайтын құрылғыларға ауыстырылады.

Басшылық әрбір басым активтің қауіпсіздік қажеттіліктерін анықтауға жауапты. Бұл өлшенетін және тиімді SIEM нәтижелерін алу үшін маңызды.

Тек маңызды активтерді тіркеңіз (бірінші). Толық журнал ортасын орнатқаннан кейін қосымша функциялар пайда болуы мүмкін. Бұл қадамды басқару қателерді болдырмауға көмектеседі. Сондай-ақ, SIEM тестіленгенше, жалпы міндеттемені төмендетуге көмектеседі.

3 SIEM шешімімен таныстыру

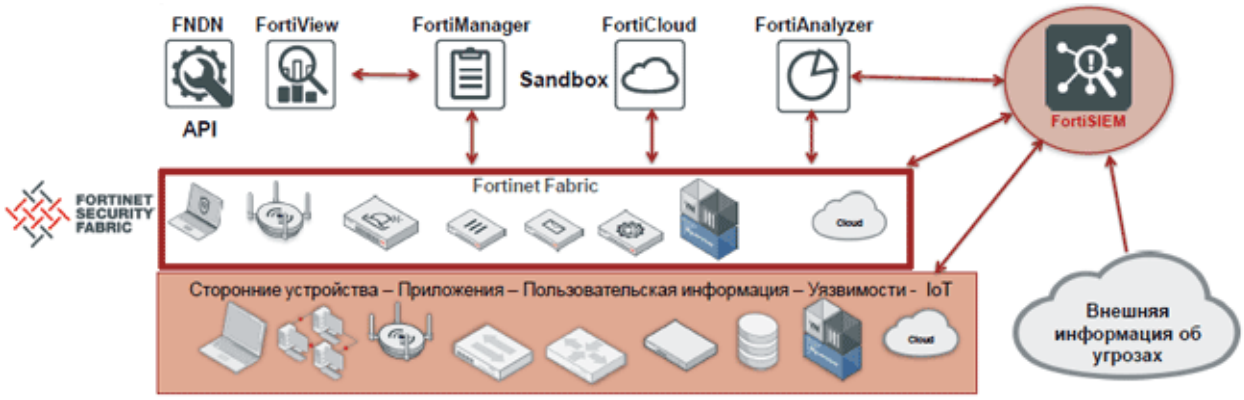
3.1 FortiSIEM жүйесімен таныстыру.

Fortinet компаниясы SIEM системалар нарығына ақпараттық қауіпсіздік оқиғаларын жинау және талдаудың біріңғай FortiSIEM жүйесін ұсынып отыр. Өнім тапсырыс берушіге толық функциональды мониторинг панелін, икемді логтар жинау, қауіптерді талдау функцияларын басқару, кәсіпорынның корпоративтік желісінің жағдайын қадағалау мүмкіндіктерін бере алады. FortiSIEM желілік құрылғылармен, басқа өндіріушілердің қауіпсіздік құрылғыларымен, обачный және виртуалды инфрақұрылымдармен, серверлармен және жұмыс станцияларымен өзара байланыс жасай алады.

FortiSIEM - интернетке қолжетімділікті қамтамасыз ететін, барлық инфрақұрылымдық компоненттердің, өнімділіктің, қауіпсіздіктің және қолдаудың. сондай-ақ облакалармен және Интернет заттарымен (IoT) жұмыс істей алатын кешенді, ауқымды басқаруы құралы. FortiSIEM шешімі жүйенің жұмысының осалдығын анықтауға бағытталған. SIEM жүйесі тек қана ақпаратты ғана емес, сонымен қатар клиенттің беделі, сыртқы келбетін де қорғауға , осы арқылы қауіптерден және жаңадан щабуылдардың зиянды салдарына қарсы әрекет етуге бағытталған. FortiSIEM, 2016 жылы Fortinet компаниясы сатып алған, SIEM жүйелері нарығында тынамыла және беделді AccelOps компаниясының SIEM жүйесінің дамуы болып табылады.. Fortinet ескі SIEM жүйесіне өзінің келесі патенттелінген технологияларын қосты:

- нақты уақыттағы оқиғалар ауқымиды корреляциясы;
- автоматтандырылған инфрақұрылым және қосымшаларды анықтау (CMDB);
- ыңғайлы логтарды өңдеу.

FortiSIEM инфрақұрылымды пайда болып жаьқан қауіпсіздік оқиғалары, логтар, жүйе өнімділігі және т.б. туралы сұрау арқылы үшінші тарап құрылғыларымен интеграцияланады. Сонымен қатар, FortiSIEM сыртқы осалдықтарды басқару жүйелерімен байланысуға және осалдықтар туралы ескертуге мүмкіндік береді, осылайша қарсы шаралар мен оларды қорғауды күшейтеді.



3.1 сурет - FortiSIEM Fortinet Security Fabric концепсиясында

FortiSIEM жүйесі ақпараттық қауіпсіздіктің инциденттерін тергеу уақытын қысқарта отырып, SOC (Қауіпсіздік операциялары орталығы) және NOC (Желілерді басқару орталығы) жеке технологияларының шекарасында орналасқан. Ол бір-бірінен ақпараттың өзара корреляциялық қатынасын пайдалануға мүмкіндік береді және SOC және NOC арасындағы өзара әрекеттестіктің тиімділігін арттырады. Оның артықшылықтары:

- желі жағдайын нақты уақыт режимінде талдаудың кеңейтілген құралы;
- нақты уақыттағы оқиғаларды талдаудың жоғары өнімділігі мен жылдамдығы;
- өнім қорапта болмаған кезде көптеген корреляция ережелері мен жасалған есептер қол жетімді болады;
- үшінші тарап құрылғыларымен және жүйелерімен көптеген интеграциялық хаттамалар;
- SOC және NOC талдауларының деректерінің өзара корреляциясы.
- іс жүзінде кез-келген қауіпсіздіктің бұзылуы сценарийін енгізу, дәйекті әрекеттер тізбегін анықтау мүмкіндігіне байланысты тергеу жүргізу;
- қауіпті және ауытқушылықтарды анықтауды автоматтандыру;
- инциденттерді тіркеу және бақылау үдерісін автоматтандыру, оларды кейіннен зерттеу мүмкіндігі;
- инфрақұрылымның күйін бақылау;
- Linux үшін Microsoft Windows және файл тұтастығын агенттері үшін деректерді жинау және бақылау агенттерінің болуы;
- көптеген орналастыру сценарийлерін қолдайды;
- масштабтау және виртуалданған архитектураны қолдау;
- гибридті дерекқордың архитектурасы;
- нақты уақыттағы оқиғалар корреляциясы таратылды;
- онлайндағы жеке журнал өңдеуі;
- тапсырыс берушінің қажеттіліктері мен инфрақұрылымына байланысты бірнеше орналастыру сценарийлері бар.

Кемшіліктері:

- орыс тілді локализациясының жоқтығы;
- FinSert немесе GosSOPKA-ға (ішкі нарыққа қатысты) қосылуға қолдау жоқ;
- FortiSIEM-дің ағымдағы нұсқасында пайдаланушылардың және UEBA субъектілерінің пайдаланушылық мінез-құлық аналитикасының мінез-құлық талдауларына қолдау жоқ, бірақ оны енгізу келесі шығарылымдарда жоспарланады.

3.1.1 Функциональдық мүмкіндіктері

FortiSIEM - IoT-тан облакоға дейін желілік қамтуды қамтитын кешенді және ауқымды кәсіпорындарға арналған шешім және нақты уақыт режимінде желінің қауіпсіздігін және өнімділігін тиімді басқаруға мүмкіндік беретін меншікті аналитикалық құралдарды қамтиды. FortiSIEM негізгі мүмкіндіктері:

1) үшінші тарап құрылғыларының және бағдарламаларының кең ауқымын қолдайды.

2) кең ауқымды және икемді лог жинау:

- секундына он мыңдаған оқиғаларды қолдау арқылы қауіпсіздік оқиғаларын жинау, өңдеу, сақтау, қалыпқа келтіру, индекстеу және корреляциялау (бір жетекші - 20 000 EPS-қа дейін, талап етілетін көлемге дейін масштабтау мүмкіндігі бар бір нұсқада);
- көптеген қауіпсіздік жүйелерін және жеткізушілердің API-лерін (жергілікті және бұлтты) қолдау;
- Windows агенттері арқылы оқиғаларды жинау, файлдардың тұтастығын бақылау, орнатылған бағдарламаларға өзгерістер мен тізілімін өзгерту;
- Linux агенттерімен файл тұтастығын бақылау;
- графикалық интерфейс ішіндегі талдау құралдарын (XML үлгілерін) жасау және өзгерту және экспорттау/импорттау функциясын пайдалану арқылы басқа пайдаланушыларға кіруді қамтамасыз ету.

3) Оқиға туралы хабарландыру және басқару:

- саясатқа негізделген оқиға туралы хабарлау инфрақұрылымын құру;
- белгіленген оқиға болған жағдайда жаңарту сценарийін іске қосу мүмкіндігі;
- сыртқы сұрау жіберу жүйелерімен API негізіндегі интеграция - ServiceNow, ConnectWise және Remedy;
- сұрауларды жіберудің кіріктірілген жүйесі.

4) Пайдаланушыны толыққанды функционалды бақылау панелімен қамтамасыз ету:

- негізгі жұмыс көрсеткіштерін көрсету үшін слайдшоуды айналдыру мүмкіндігі бар нақты уақыт режимінде реттелетін бақылау тақталары;
- ұйымдар мен пайдаланушылар қызметкерлерінің ұжымдық пайдалануы үшін қол жетімді есептерді және аналитикалық деректерді қалыптастыру;
- қиын мәселелерді жылдам анықтау үшін түсті таңбалау;
- бизнес қызметтері, виртуалданған инфрақұрылымдар және реттелетін қолданбалар үшін реттелетін, көп қабатты бақылау тақталары.

5) Сыртқы қауіп туралы деректерді біріктіру:

- қауіпті деректердің сыртқы көздерін интеграциялау үшін API - зиянды бағдарламалармен, IP мекенжайларымен, URL-мекенжайларымен, хэштермен, Tor тораптарымен домендер;
- танымал қауіпті дерек көздерінің интеграциясы - ThreatStream, CyberArk, SANS, Zeus;
- қатерлер туралы деректердің үлкен көлемін өңдеу технологиясы - кластерде қосымша жүктеу және тарату, нақты уақыт режиміндегі желілік трафикті сәйкестендіру.

6) Ауқымды талдау қызметін ұсыну:

- нақты уақыттағы оқиғаларды іздеу;

- кілт сөзбен және өңделген оқиғалар атрибуттарымен іздеу;

- тарихи оқиғаларды іздеу - логикалық сүзгілеу шарттарымен SQL түріндегі сұраулар, сәйкес жиынтықтар бойынша топтастыру, күннің уақытына байланысты сүзу, тұрақты өрнек сәйкестігі, есептелген өрнектер - графикалық интерфейс және API;

- нақты уақыттағы кешенді оқиға үлгілері үшін триггер;

- анықталған CMDB объектілерін, пайдаланушыны / жеке деректерді және іздеу және ереже жасау процесінде орын туралы ақпаратты пайдалану;

- есептерді жоспарлау және негізгі қызметкерлерге электрондық пошта арқылы нәтижелер беру;

- бүкіл корпоративтік желі бойынша оқиғаларды немесе жеке немесе логикалық есеп домені;

- сыни бұзушылықты анықтайтын динамикалық өзгеретін бақылау тізімдері - есеп беру ережелерін жасау үшін қадағалау тізімдерін қолдауға;

- жұмыс уақытының үзіліссіз жұмыс түйіндерін қосу арқылы аналитикалық деректер арналарын масштабтау;

- күрделі іскерлік қызметтерді пайдалану арқылы инциденттер туралы есеп беруде басымдықты анықтауды анықтау мүмкіндігі.

7) Негізгі ережелерді орнатыңыз және соңғы нүктенің/сервердің/ пайдаланушы әрекеттерінің статистикалық ауытқуларын анықтаңыз:

- сыртқы технологиялардың интеграциясы;

- IP-адресті табу үшін кез-келген сыртқы веб-сайтпен біріктіру;

- сыртқы қауіпті деректер көздері үшін API негізінде интеграция;

- қолдау қызметі жүйелерімен екі жақты API-негізделген интеграция - ServiceNow, ConnectWise және Remedy үшін жедел қолдау;

- сыртқы CMDB арқылы екі жақты интерфейске негізделген интеграция - ServiceNow және ConnectWise үшін жедел қолдау;

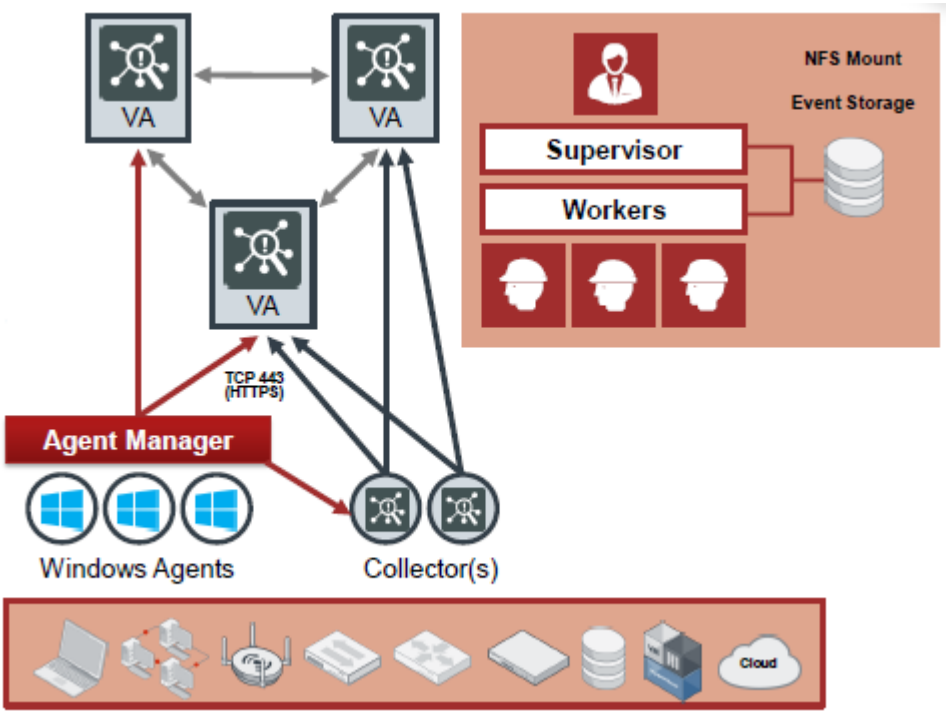
- кафка талдамалық есептілік құралдарымен (ELK, Tableau, Hadoop) интеграциялауды қолдайды;

- оқу жүйелерімен оңай біріктіру үшін API қамтамасыз ету;

- ұйымдарды қосу, тіркелгі деректерін жасау, анықтауды бастау, оқиға мониторингі процесіне өзгерістер енгізу үшін API ұсыну.

3.1.2 FortiSIEM архитектурасы және кіріс ақпарат көздері

FortiSIEM архитектурасы жүйенің орналасқан жеріне (өз инфрақұрылымы, бұлт, деректер орталығы) және өңделген деректердің көлеміне байланысты түрлі элементтер негізінде құрылған иерархиялық құрылым болып табылады.



3.2 сурет - FortiSIEM Архитектурасы

FortiSIEM-тің негізгі элементі - барлық өңдеу қызметтері, веб-сервер, қосымшалар сервері, дерекқор сервері, шешім интерфейсі бар жетекші. Одан кейін аналитикамен айналысатын өңдеушілер (жұмысшылар) болып табылады және кейбір қауіпсіздік оқиғаларына жауап береді, жетекшінің жүктемесін алып тастайды. Архитектураның келесі элементі - қашықтағы орындардағы оқиғаларды жинап, қалыпқа келтіретін коллекционер (коллекционер), ал деректерді инфрақұрылымнан деректерді басқарушыларға және супервайзерге беру.

Кесте 3.1 – FortiSIEM деректерді жинау технологияларын салыстыру

	Агентсіз технология	Агент
Табу	+	-
Өнімділікті бақылау	+	-
Жүйенің, бағдарламалардың, қауіпсіздіктің логтарын жинау (төмен өнімділік)	+	-
Жүйенің, бағдарламалардың, қауіпсіздіктің логтарын жинау (жоғары өнімділік)	-	+
DNS, DHCP, DFS,IIS логтарын жинау	-	+

3.1-кестенің жалғасы

Сервер ресурстарын жоғалтудың, кешігудің төмен деңгейі секундына 1800 оқиғаға дейін	-	+
Агенттер диспечерінде 500 агентке дейін	-	+
Уақытты жергілікті өңдеу және қалыпқа келтіру	-	+
Орнатылған бағдаламалық қамтамасыз етілулерді анықтау	-	+
Реестірдегі өзгерістерді бақылау	-	+
Файлдардың тұтастығын бвқылау	-	+
Клиенттердің лог файлдарын бақылау	-	+
WMI командаларының шығуын бақылау	-	+
PowerShell командаларының шығуын бақылау	-	+

FortiSIEM агентсіз деректерді жинау технологиясын қолдайды, бірақ толығырақ деректерді жинау және нақты мониторинг үшін пайдаланушы түпкілікті станцияларында және серверлерде орнатылған Fortinet Windows агенттері мен Fortinet Agent Manager құралдары пайдаланылады.

FortiSIEM үшін FortiOS (FortiGate, FortiMail, FortiSandbox, FortiWeb, FoetiAP, FortiManager, FortiSwitch) Fortinet-тің барлық Fortinet өнімдері FortiSIEM-тің іс-шарасы ретінде әрекет етеді. Байланыс SNMP, Telnet, SSH, Syslog және басқа да қолдау көрсетілетін хаттамалар арқылы жүзеге асырылады.

FortiSIEM Fortinet құрылғыларының операциялық жүйесіне администраторлық қатынасы бар:

- құрылғы конфигурацияларын жою және конфигурация стандарттарын сақтау;
- осы конфигурациялардағы өзгерістерге қатысты оқиғаларды салыстырып, кім, не, қашан және не істегені туралы сұрақтарға жауап беру;
- құрылғыларды, интерфейстерді, жадыларды, процессорларды және тректерді жүктеудің мәртебесі мен мәртебесінің тұрақты мониторингін жүргізеді;
- табылған осалдықтар туралы ақпаратты ортақ пайдалану үшін Fortinet Security Fabric қауіпсіздік фабрикасына біріктіру;

- FortiSIEM қазіргі уақытта конфигурацияға, ағымдағы өнімділікке және күйді бақылауға және жүктемені қадағалауға қол жеткізу үшін әртүрлі үшінші тарап өндірушілерінің 380-ден астам құрылғыларына қосылуды қолдайды. Құрылғылар мен қосымшалардың түрлері:

- қосқыштар, маршрутизаторлар, сымсыз кіру нүктелері және басқа жабдықтарды қоса алғанда, желілік құрылғылар;

- қауіпсіздік құрылғылары - брандмауэрлер, IPS желілік жүйелері, веб-шлюздар мен электрондық пошта шлюздері, зиянды бағдарламаларға қарсы құралдар, осалдық сканерлері және басқа жабдық;

- Windows, Linux, AIX, HP UX қоса серверлер;

- инфрақұрылымдық қызметтер, соның ішінде DNS, DHCP, DFS, AAA, домен контроллері, VoIP;

- веб-серверлерді, қосымшалар серверлерін, пошта жүйелерін, дерекқорларды қамтитын пайдаланушыға бағытталған бағдарламалар;

- NetApp, EMC, Isilon, Nutanix, Data Domain қоса алғанда, сақтау құрылғылары;

- AWS, Box.com, Okta, Salesforce.com;

- облакалық инфрақұрылымдар, соның ішінде AWS;

- қоршаған ортаны қорғау құрылғылары, UPS, HVAC, аппараттық құрылғылар;

- виртуалдандыру құралдары, соның ішінде VMware ESX, Microsoft HyperV.

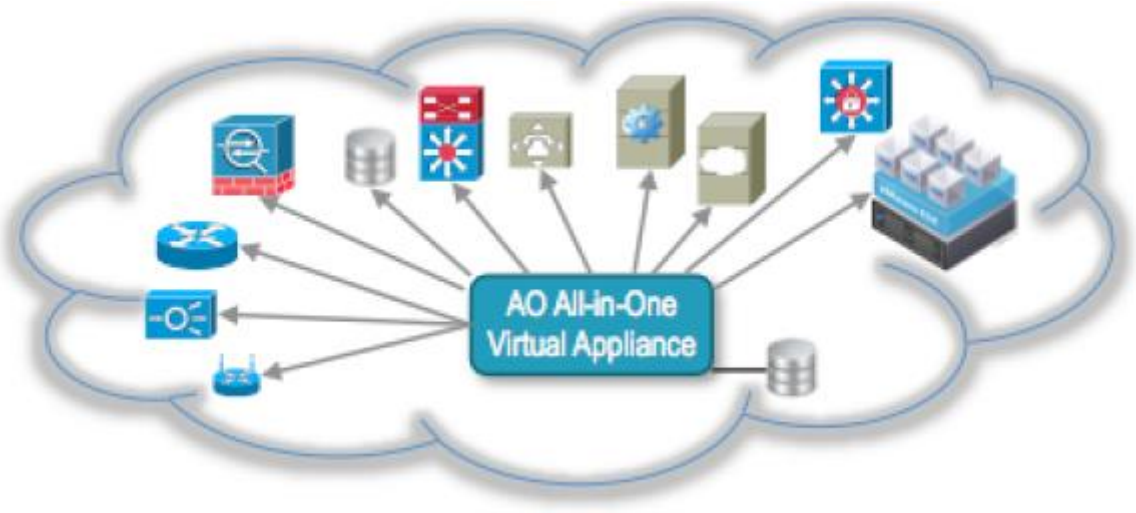
FortiSIEM үшінші тарап құрылғыларымен интеграциялау FTP (SSL арқылы FTP), HTTP, HTTPS, IMAP (SSL үстінен IMAP), JDBC, JMX, LDAP (LDAP іске қосу TLS), LDAPS, SMTP, SMTPS, SSH, TELNET, SNMP, VM SDK, Syslog.

3.2 FortiSIEM енгізу сценарийлері

FortiSIEM архитектурасы барлық өлшемдер мен бизнес-провайдерлердің бизнестеріне арналған бірнеше орналастыру опцияларын қамтиды.

1) Автономды қадағалаушыны енгізу - барлығы-біреу

Бұл бір қарапайым бақылаушы деректерді жинау, бақылау, өңдеу және талдауға және жаңа қауіпсіздік оқиғаларын қадағалауға мүмкіндік беретін ең оңай орналастыру нұсқасы. Оқиға деректерін сақтауға қойылатын талаптарға байланысты, супервайзер жергілікті немесе NFS сақтауды пайдалана алады. Жұмыс бекеттерінде және серверлерде бақылаудың дұрыстығын жақсарту үшін Windows агенттері мен агент менеджерін пайдалануға болады.



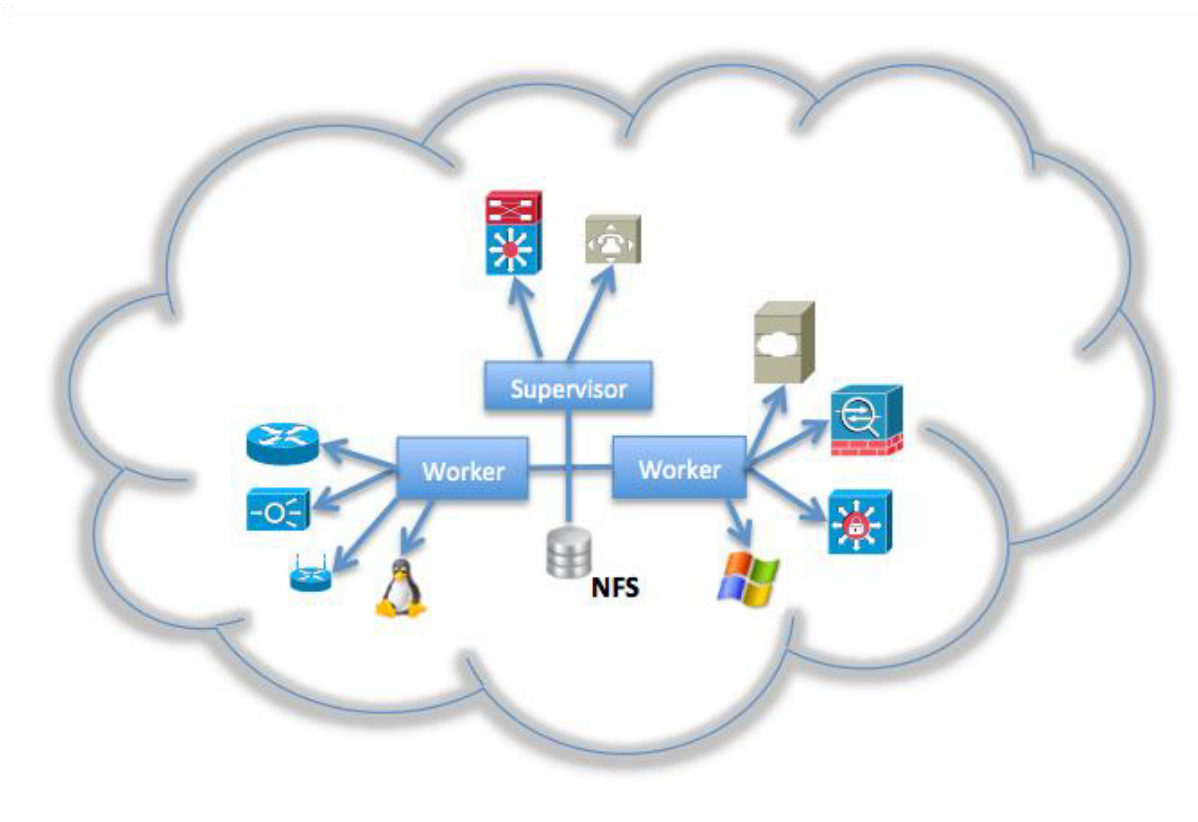
Сурет 3.3 – FortiSIEM енгізудің бір супервизормен «барлығы біреуінде» сценарийі

2) Жоспарлаушы мен жұмысшы кластерін енгізу - ішінара таратылған орналастыру

Мониторингтік құрылғылар саны немесе оқиғалардың өсу қарқыны арта түскен сайын, бір жетекші жүктемені жеңе алмайды. Бұл жағдайда ортақ дерекқор (NFS) арқылы супервайзермен деректермен алмасатын бір өңдеуші немесе өңдеушілердің кластері қолданылады. Қызметкерлер азаматтығы жоқ түйіндер болып табылады (олар алдыңғы өзара әрекеттер туралы ақпаратты сақтамайды, әр өзара әрекеттестік сұрауы тек онымен бірге келген ақпарат негізінде өңделеді) қажет болғанда кластерден оңай қосылуы немесе жойылуы мүмкін.

Кластерде жетекші мен өңдеушілердің түйіндері белгілі бір функцияларды орындайды:

- анықтау әрдайым супервайзерлер торабында орындалады;
- оқиғалар журналының талдауы супервайзерде немесе осы журналдарды алған өңдеушіде орындалады;
- өнімділікті бақылау жүктемені теңдестіру алгоритмін пайдалану арқылы барлық процессорлар арқылы қадағалаушы тарапынан таратылады.



Сурет 3.4 – FortiSIEM енгізудің өңдеушілер кластері – ішінара таратылған сценарийі

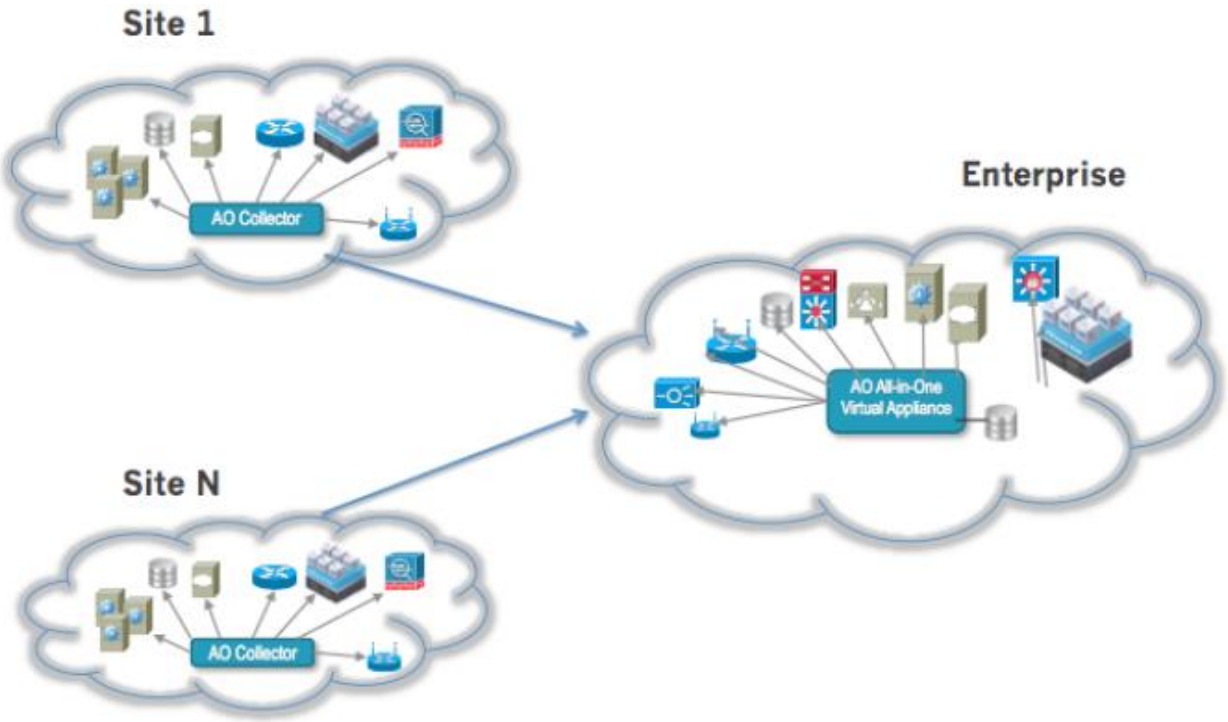
3) Супервайзер мен коллекторларды енгізу - бөлінген іске асыру

FortiSIEM-ті қолданған кезде бір жетекші жеткіліксіз екі жағдай бар:

- брандмауэрдің артында орналасқан құрылғыларды басқару үшін супервайзер пайдаланатын протоколдарды (мысалы, Windows басқару құралы, WMI) бұғаттайды;

- Supervisor бақыланатын құрылғыларды Wide Area Network (WAN) сияқты жоғары кідіріс желісі арқылы байланыстырады және бұл жағдайда SNMP немесе WMI сияқты протоколдар арқылы бақылау әдетте іске асырылмайды немесе жұмыс істемейді.

Мұндай жағдайларда супервайзермен HTTP (HTTPS) арқылы байланысатын қол жетімсіз құрылғыларды бақылау үшін коллекторларды пайдалану ұсынылады. Коллекторлар қашықтағы орындарда орналастырылады, құрылғылармен байланысады, оқиғалар мен журналдарды бастапқы өңдеуді жинайды және жүргізеді, деректерді қысады, содан кейін оқиғаларды қалыпқа келтіру, бақылау және қадағалау үшін супервайзерге жібереді. Коллекторларға хабарлау үзіліс болған жағдайда, сонымен қатар, оқиғаларды буферизациялауға болады.

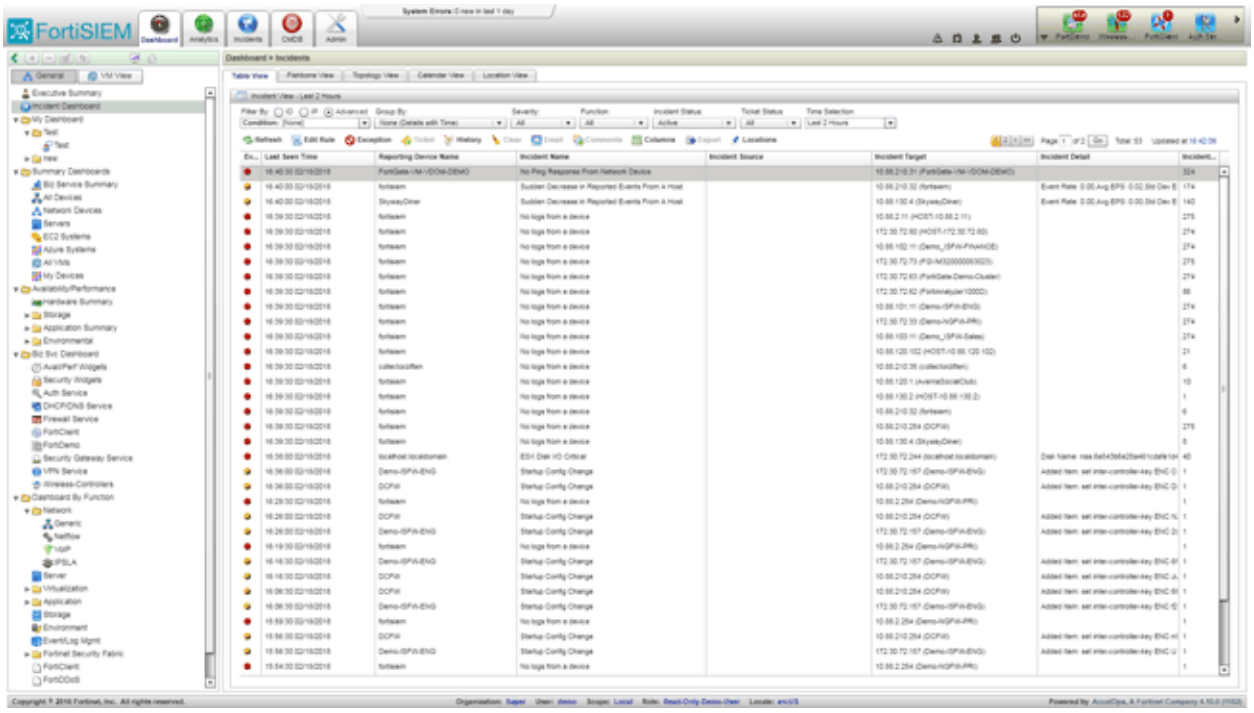


Сурет 3.5 – FortiSIEM енгузідің коллекторларды қолдану арқылы – таратылған енгізу сценарийі

4) Өңдеушілер арқылы таратылған орналастыру. FortiSIEM архитектурасының барлық элементтерін - супервайзерлерді, өңдеушілерді, коллекторларды қолданатын барлық түрлердің жиынтығы. Корпоративті инфрақұрылымның бөлігі ретінде, супервайзерден басқа, бір немесе бірнеше процессорлар және бір немесе бірнеше коллекторлар жалпы базаны қолдана отырып орналастырылады.

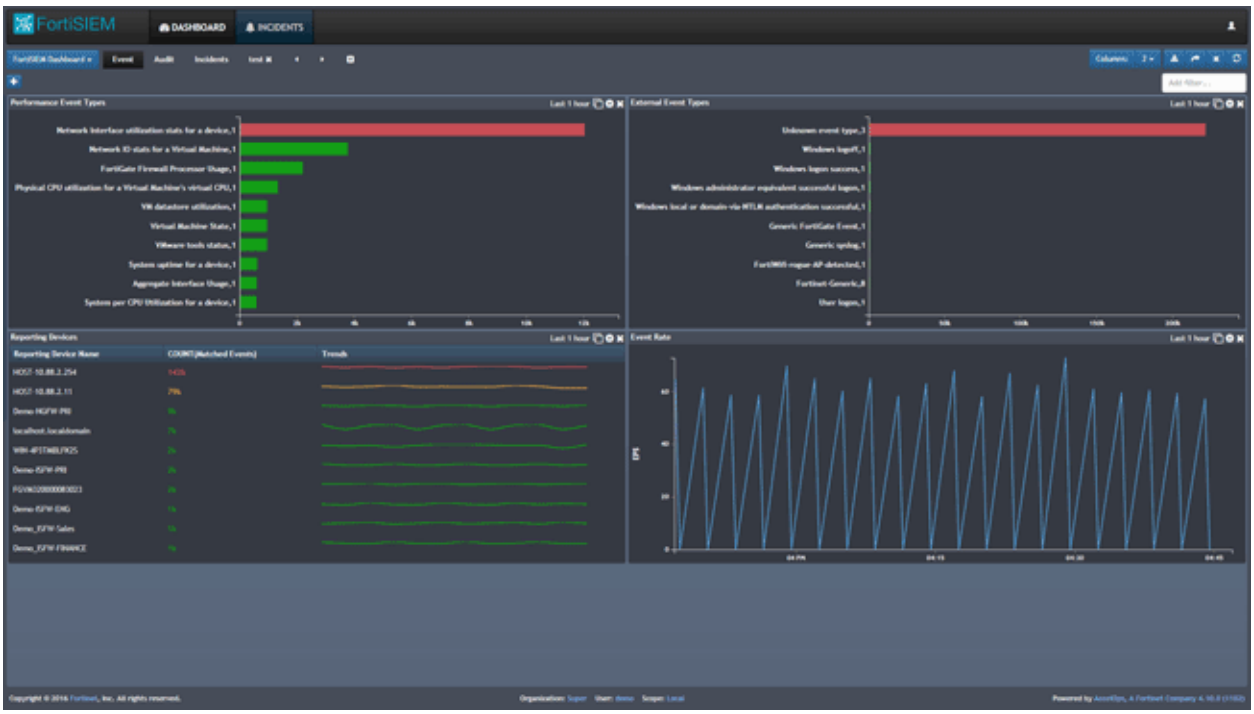
3.3 FortiSIEM ақпараттық қауіпсіздігін басқарудың негізгі мүмкіндіктері

Оқиғаларды бақылауы. FortiSIEM интерфейстердің екі түрін ұсынады. Біріншіде ақпаратты көрсету үшін иерархиялық бөлім құрылымы және жұмыс кеңістігі бар. Бұл интерфейс FortiSIEM басқаруға және ақпараттық қауіпсіздікті басқаруға, клиенттің инфрақұрылымы элементтерімен өзара әрекеттесуді реттеуге және орын алған оқиғалар туралы ақпаратты алуға мүмкіндік береді.

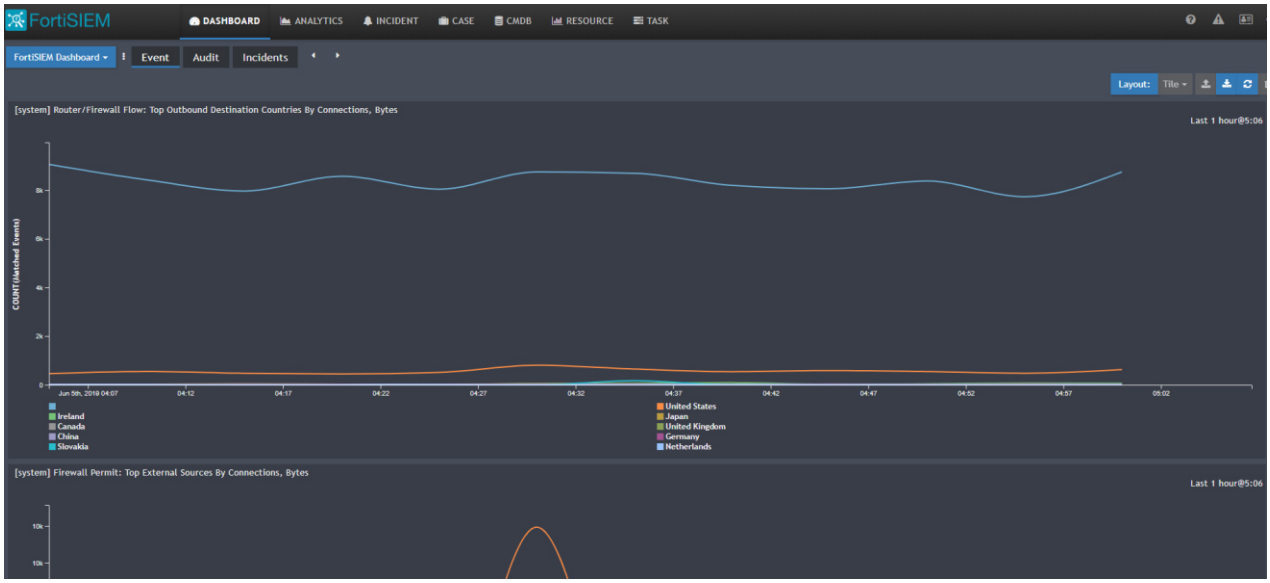


Сурет 3.6 – FortiSIEM администраторының интерфейсі, оқиғалар панелі

Екінші интерфейс кез-келген құрылғыда, үлкен экрандарда және плазмалық тақталарда оқиғаларды тұрақты бақылауға мүмкіндік береді. Карталарды панельдер (бақылау тақтасы) немесе инциденттер (инциденттер) және әр түрлі өлшемдер арқылы жасауға болады.

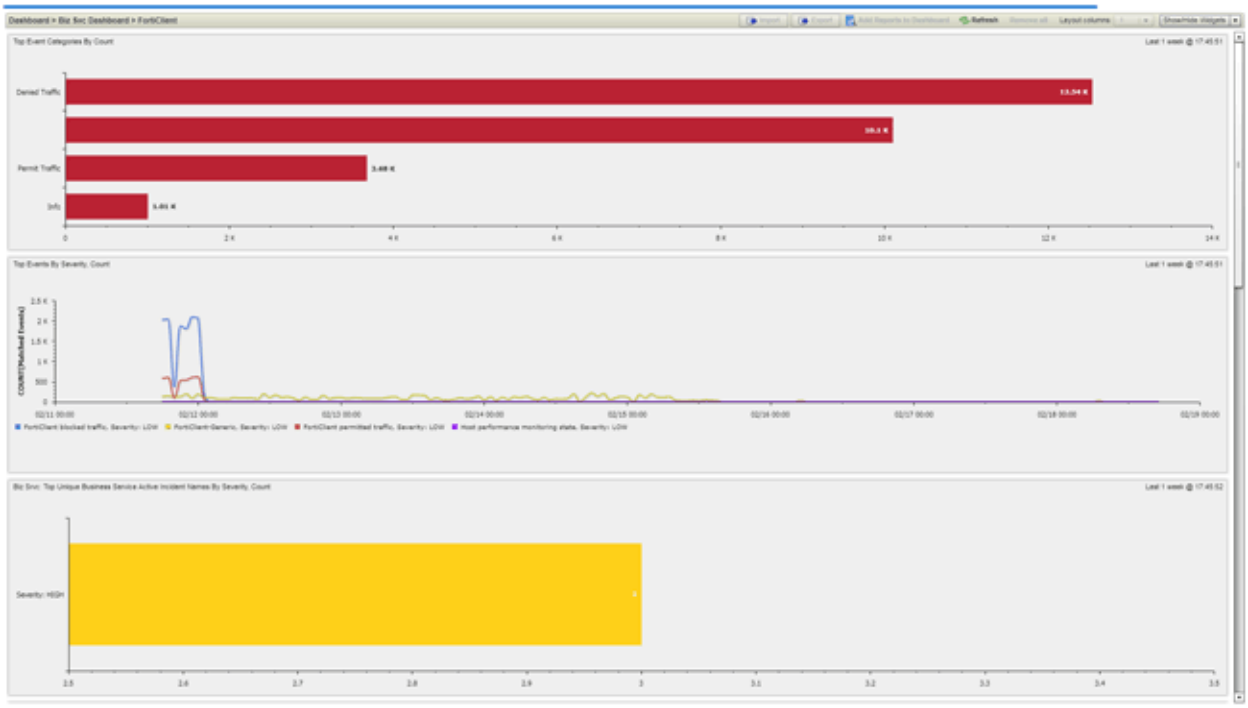


Сурет 3.7 – FortiSIEM администраторының интерфейсі, оқиғалар панелі



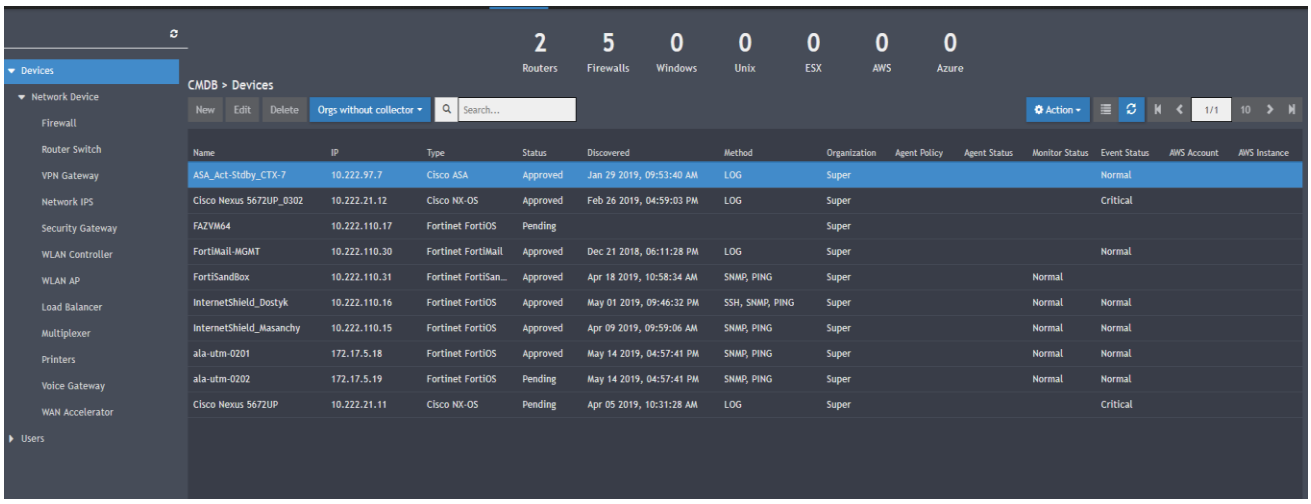
Сурет 3.8 – FortiSIEM администраторының интерфейсі, FortiSIEM панелінің виджеттері

Кілт индикаторларын көрсету үшін нақты уақыт режимінде реттелетін бақылау тақталарын слайдшоу арқылы көрсету мүмкіндігі бар.

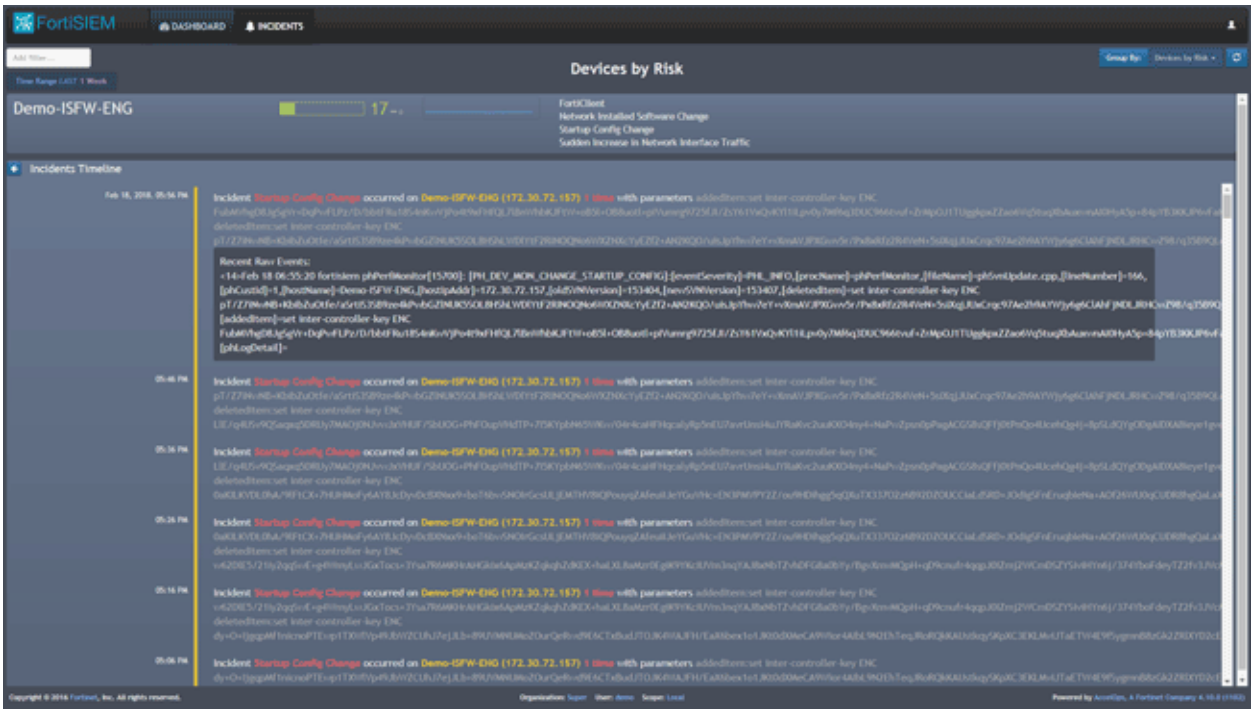


Сурет 3.9 – FortiSIEM бақылау панелінің слайд-шоу режимінде көру

Әрбір құрылғы үшін қауіпсіздік оқиғалары туралы егжей-тегжейлі ақпаратты қамтитын толық есептерді алуға болады.



Сурет 3.10 – FortiSIEM администраторлық интерфейсінде басқарылып отырылған құрылғылар тізімі.

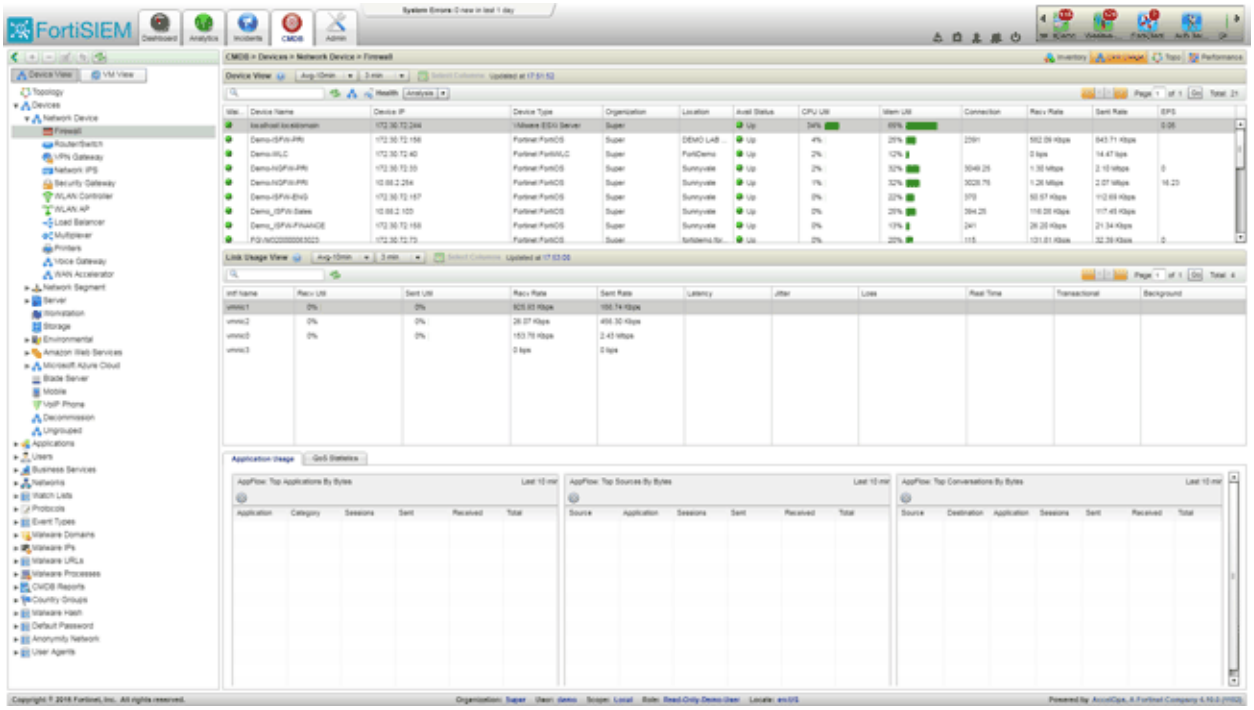


Сурет 3.11 – FortiSIEM администраторлық интерфейсінде басқарылып отырылған құрылғыда орын алған оқиғалар туралы есептер

Жүйе жағдайы мен өнімділігі мониторингі. FortiSIEM физикалық және виртуалды инфрақұрылымдардың топологиясын жергілікті және мемлекеттік/жеке бұлтқа сәйкестік деректерін пайдаланып салыстыруға мүмкіндік беретін құрылғыларды, қосымшаларды және конфигурацияларды табуды автоматтандыруды қолдайды.

Желінің периметрі бойынша, мысалы, брандмауэрлер мен маршрутизаторларға арналған, қандай интерфейстердің жұмыс істемейтіні және құрылғы трафигінің көп бөлігі қандай трафикті тұтынуы туралы ақпарат алу маңызды.

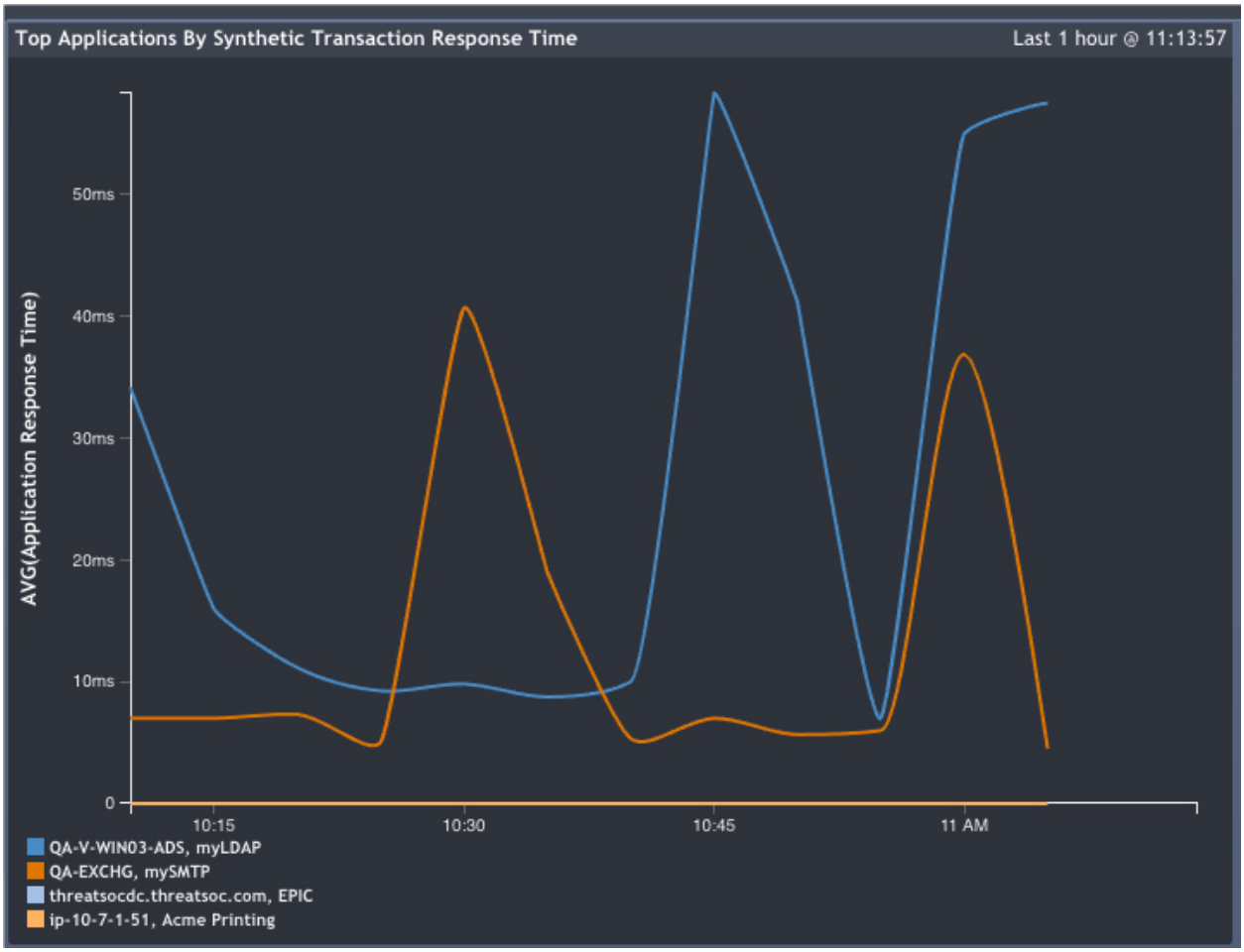
Арнайы бақылау тақтасы қажетті статистиканы қамтамасыз етеді және администторға қандай маршрутизатор интерфейстері жүктелетінін, қандай қосымшалар қолданатындығын және QoS статистикасы қандай екенін анықтауға мүмкіндік береді.



Сурет 3.12 – FortiSIEM администраторлық интерфейісінде желіаралық экрандардың жағдайларын бақылау

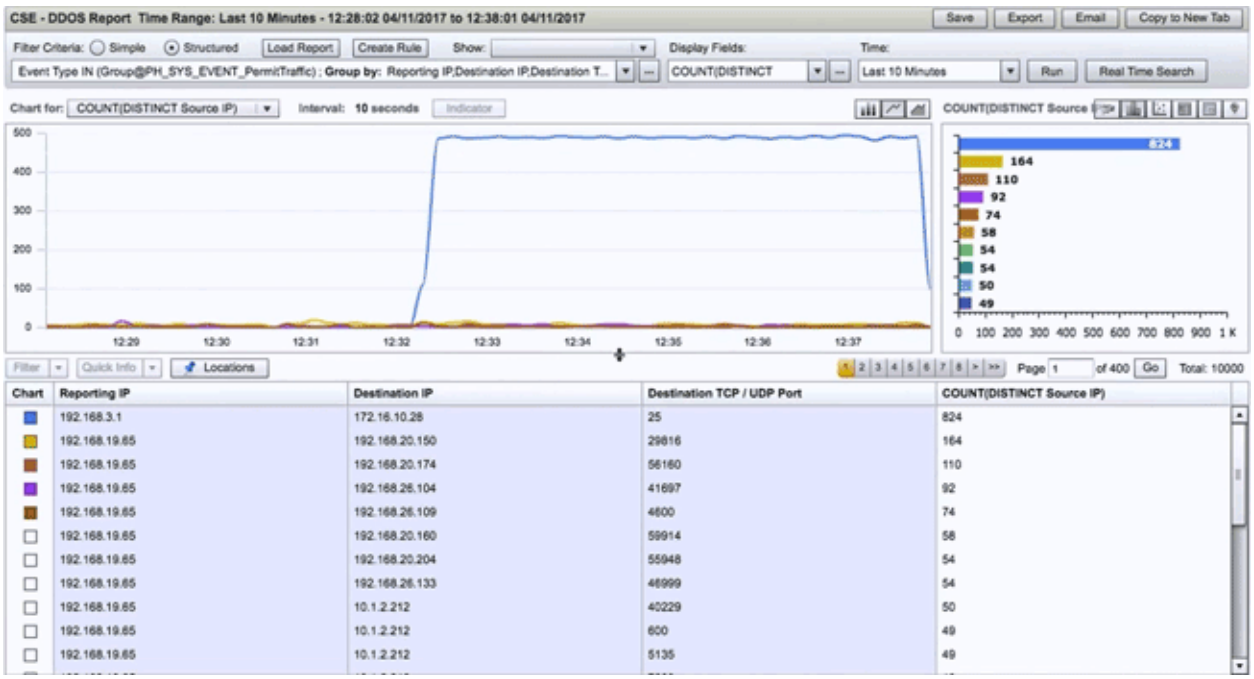
FortiSIEM арқылы анықталған құрылғылар үнемі бақыланады және жиналған деректер инфрақұрылымның жұмысына талдау жасауға мүмкіндік береді.

Ыңғайлылық үшін администратор құрылғының немесе қызметтің өнімділік бақылау тақтасын реттей алады. Мониторингтік жағдай бақыланады, корреляцияланады және FortiSIEM-де көрсетілген параметрлерге байланысты тиісті оқиғалар шығарылады.



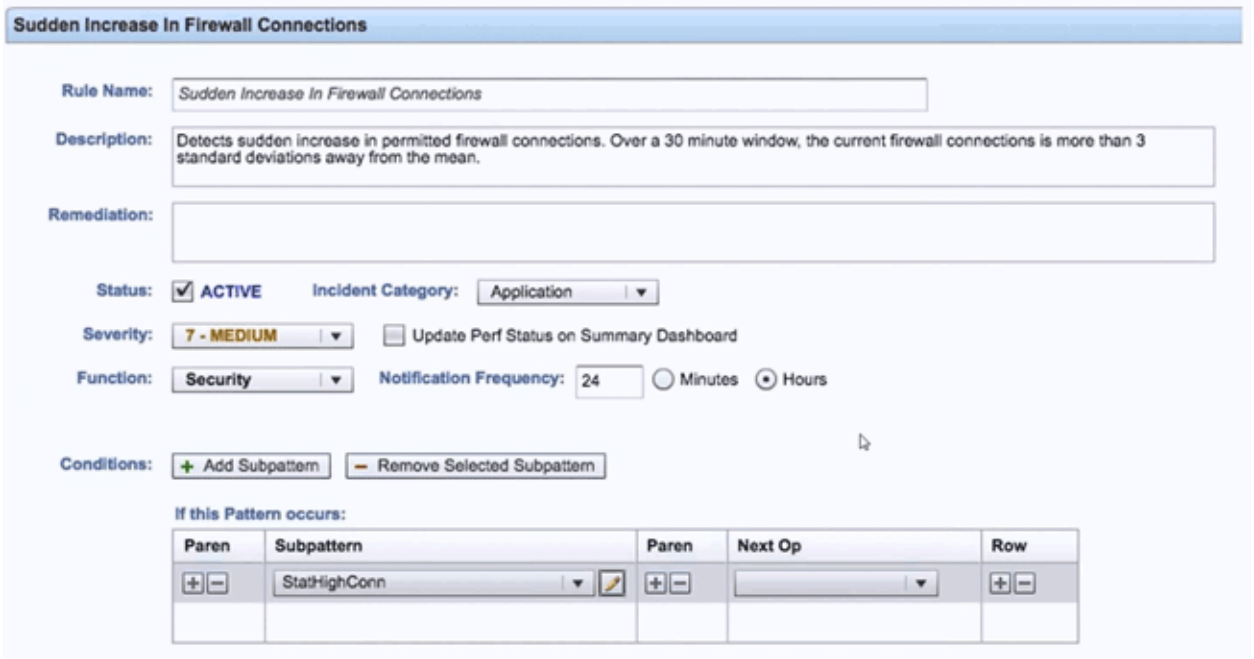
Сурет 3.13 – FortiSIEM құралдарымен басқарылатын құралдардың өнімділігін бақылау

Құрылғылар мен қызметтердің жағдайын талдап, сіз бірнеше шабуылды анықтай аласыз. Мысалы, желі ағынының күрт өсуі DDoS шабуылын білдіреді. Бұл оқиға бақылау тақтасында көрсетіледі және оқиғалар бақыланатын корреляция ережесі болады.



Сурет 3.14 – FortiSIEM құралдары арқылы басқарылып отырылған құрылғыдағы желелік ағынды бақылау арқылы DDoS шабуылды анықтау

Корреляция ережесі бірқатар параметрлерді (тәуекел деңгейін, ереженің әрекет етуін, осы ережеге сәйкес орын алған оқиғаны хабарлау жиілігін) және оқиғаға байланысты корреляциялық механизмдерді анықтайды.

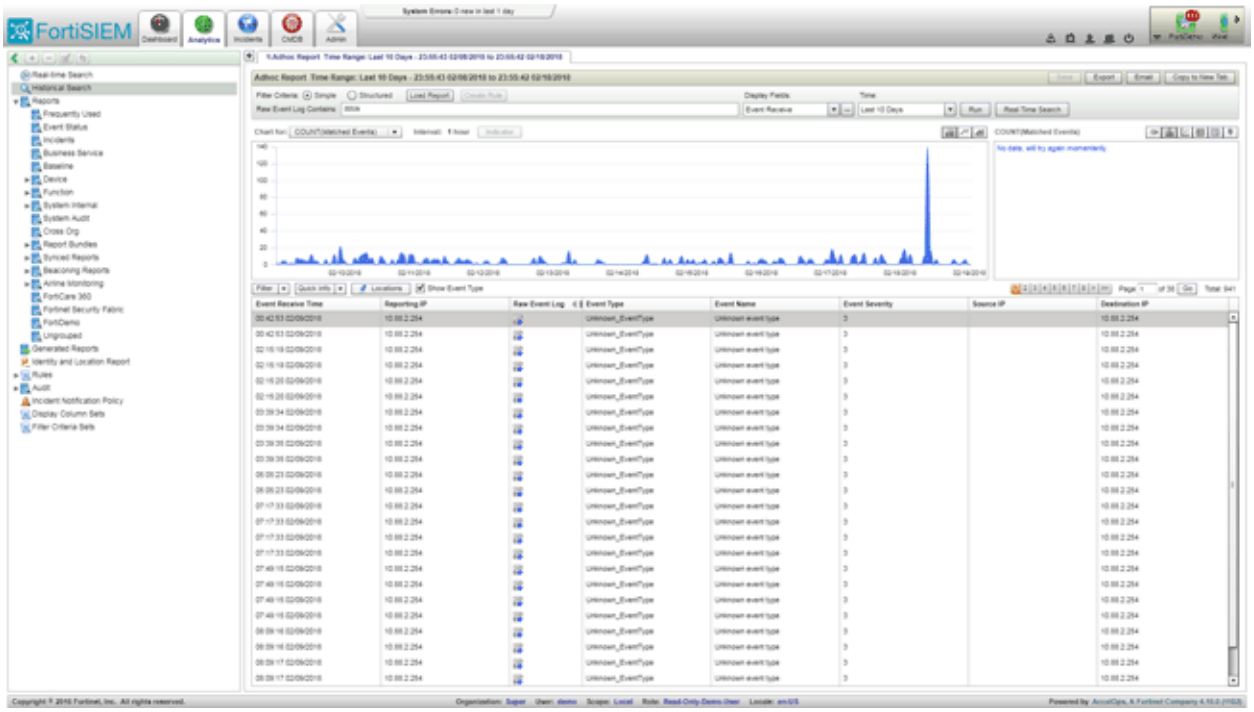


Сурет 3.15 – FortiSIEM корреляция ережелерін қалыптастыру

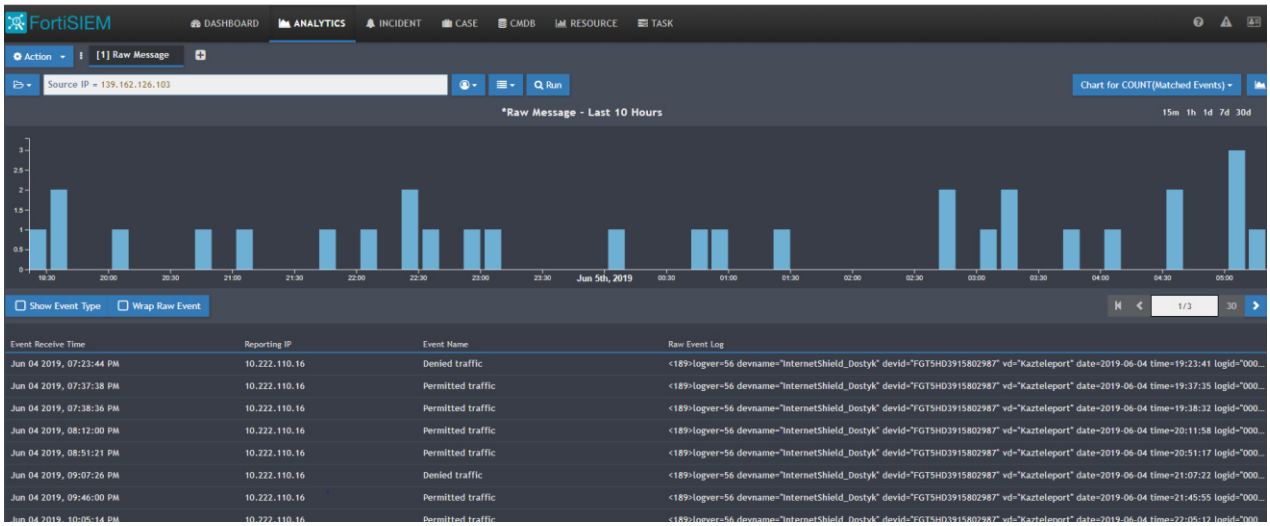
Бірнеше оқиғалар үшін сіз тиісті ережені жазу арқылы корреляция құра аласыз, бұл сіздің есепіңізді және ескертуді шығаратын жеке қауіпсіздік оқиғасы болады.

Оқиғаларды талдау. Сараптама FortiSIEM іздеу функцияларына, ережелерді орындау мен есепті жасауға негізделген.

FortiSIEM іздеу функциясы IT-инфрақұрылымынан алынған ақпараттарды нақты іздеу және тарихи іздеуді қамтиды. Нақты уақыттағы іздеулер оқиғаларды олар орын алған кезде көрсетеді, ал тарихи іздеу оқиға дерекқорында сақталған ақпаратқа негізделеді. Іздеудің екі түрі де белгілі бір атрибуттар мен оқиғалар мәндеріне негізделген іздеуге мүмкіндік беретін қарапайым кілт сөздерді іздеу және құрылымдық іздеу сұрауларын қамтиды, содан кейін нәтижелерді төлсипаттармен топтастырады.

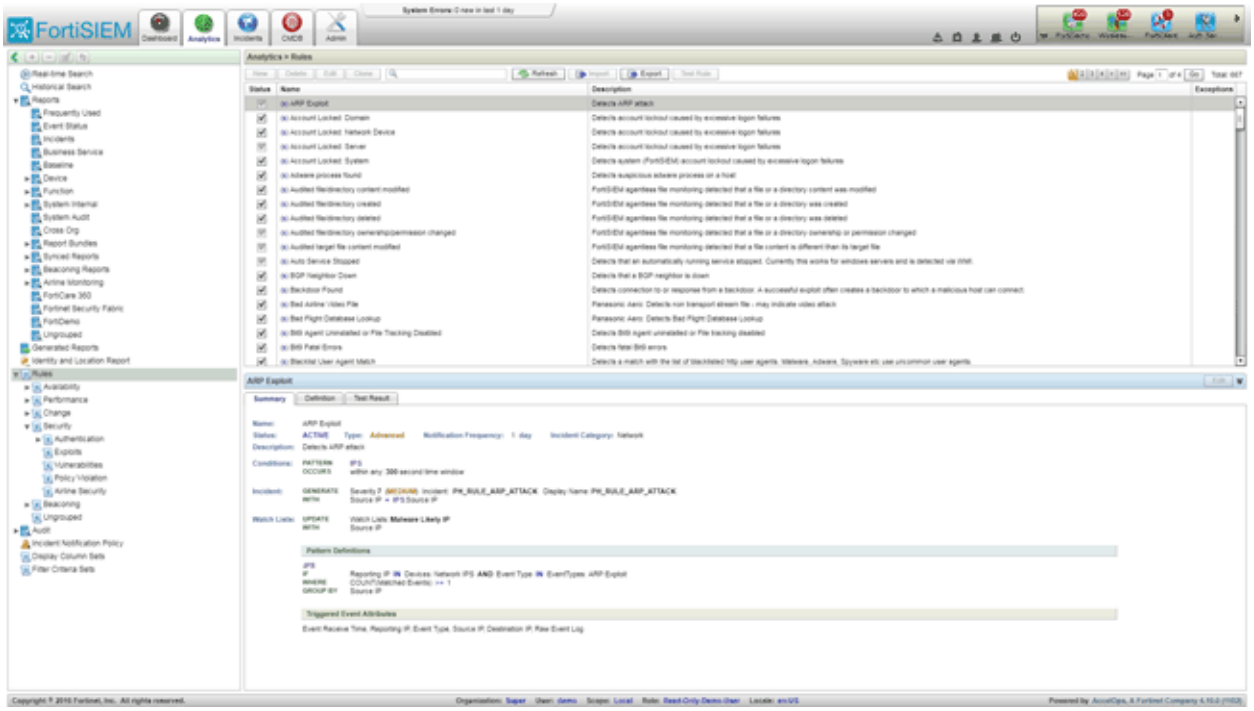


3.16 сурет - FortiSIEM уақыт бойынша іздеу

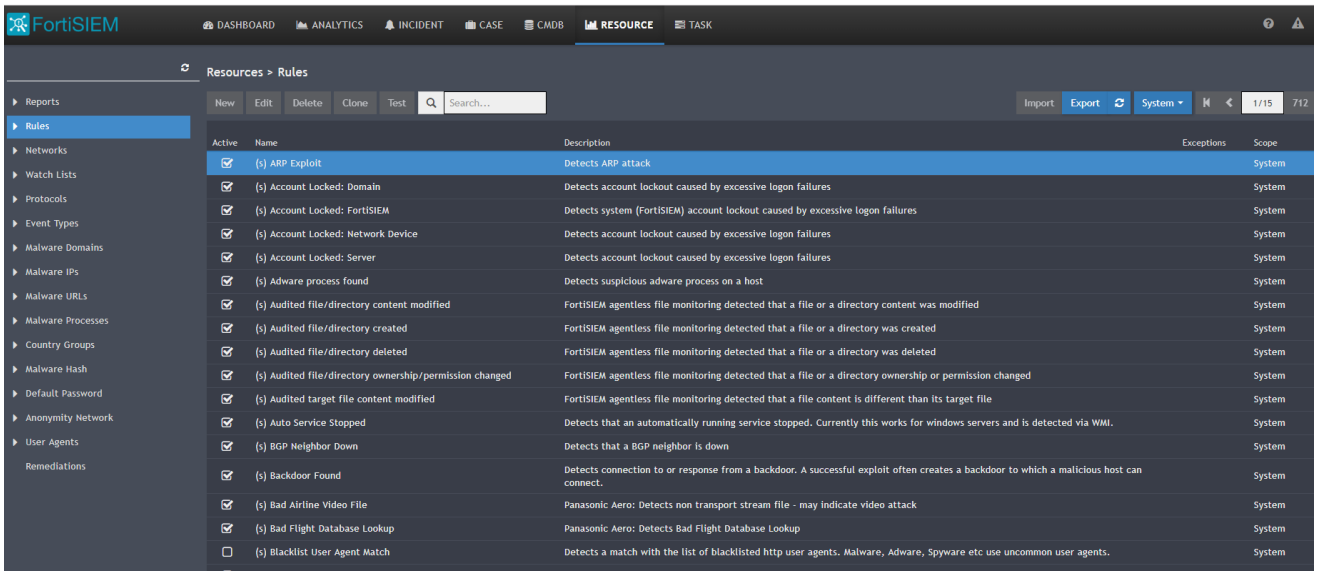


Сурет 3.17 – FortiSIEM уақыт бойынша іздеу

FortiSIEM тұрақты түрде инфрақұрылымды бақылайды және өнімділікті, қолжетімділікті және қауіпсіздікті талдау үшін пайдаланылатын ақпаратты ұсынады. Қауіпсіздік оқиғаларына тез жауап беру үшін айрықша, күдікті немесе әлеуетті қателер мен бұзушылықтардың пайда болуы туралы уақтылы ескертулер алу қажет. Мұны істеу үшін, назар аудару керек болатын жағдайларды анықтайтын ережелерді қолданыңыз және оқиғаны бастамаңыз. FortiSIEM 500-ден астам жүйелік ережелерді, сондай-ақ өз ережелеріңізді жасау үшін редакторды қамтиды.

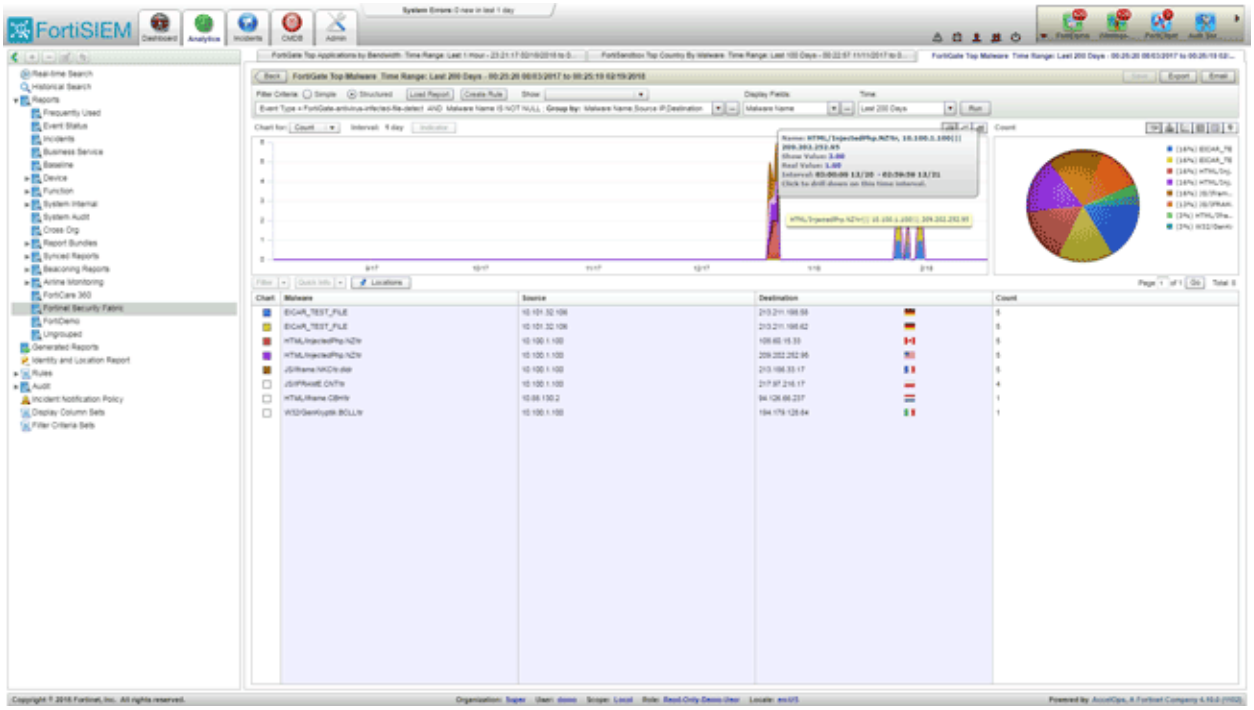


Сурет 3.18 – FortiSIEM ережелерді басқару панелі



Сурет 3.19 – FortiSIEM ережелерді басқару панелі

Есептер – алдын ала анықталған іздеу сұраныстарынан құралады. FortiSIEM сізге ортақ құрылғыларға арналған есептердің үлкен каталогын және сіздің қажеттіліктеріңізді қанағаттандыру үшін пайдалануға және реттеуге болатын талдау тапсырмаларын қамтиды.



Сурет 3.20 – Автоматты түрде қалыптастырылған есептің мысалы

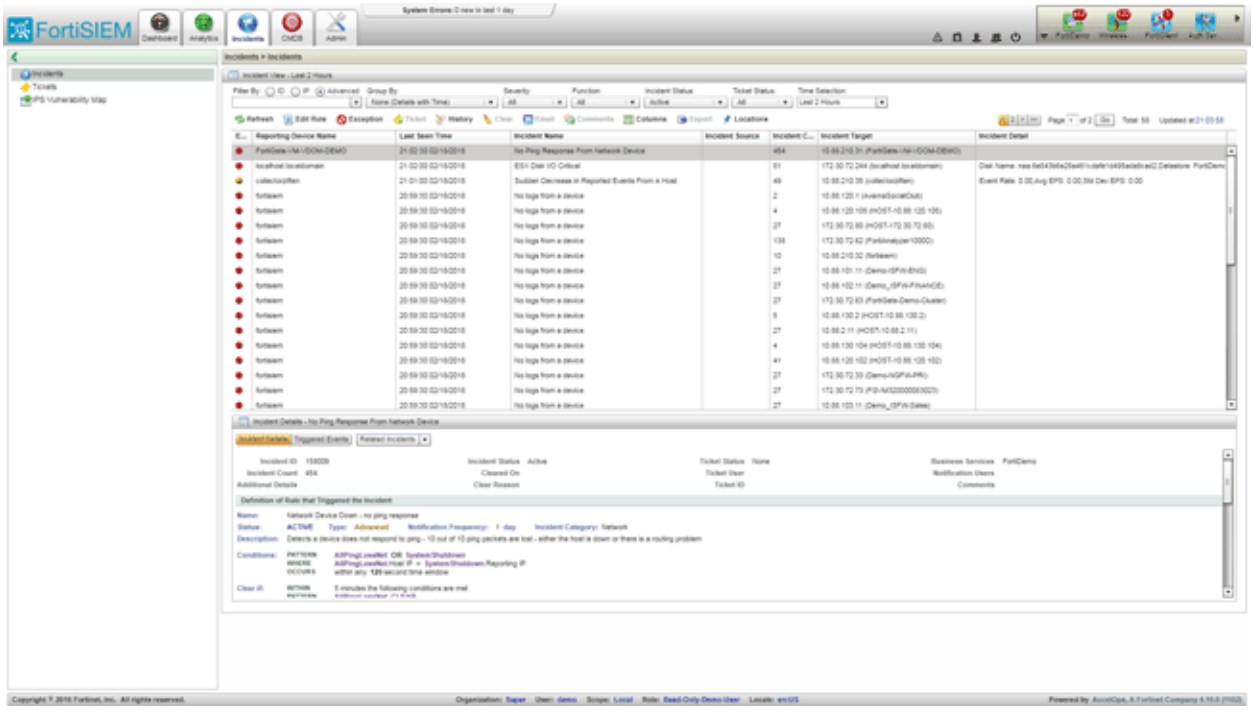
Зиянды бағдарламаларды анықтау. Зиянды бағдарламаларды анықтау FortiSandbox желісінің құм жәшігі арқылы орындалады. FortiSandbox кейбір зиянды әрекеттерді қолданады және FortiSandbox FortiSIEM үшін бақыланатын құрылғы болғандықтан, зиянды бағдарламаларды анықтау оқиғасы пайда болады, FortiSIEM бақылау тақтасы жаңартылады және ескерту ережесі жасалады. FortiSIEM ережесі зиянды әрекеттерді блоктау үшін құрылғыларға пәрмендер жіберуге мүмкіндік беретін автоматты түрде жасалуы мүмкін.

FSA - Sandbox Malware Detection - CSE — Last 15 minutes @ 11:34:24

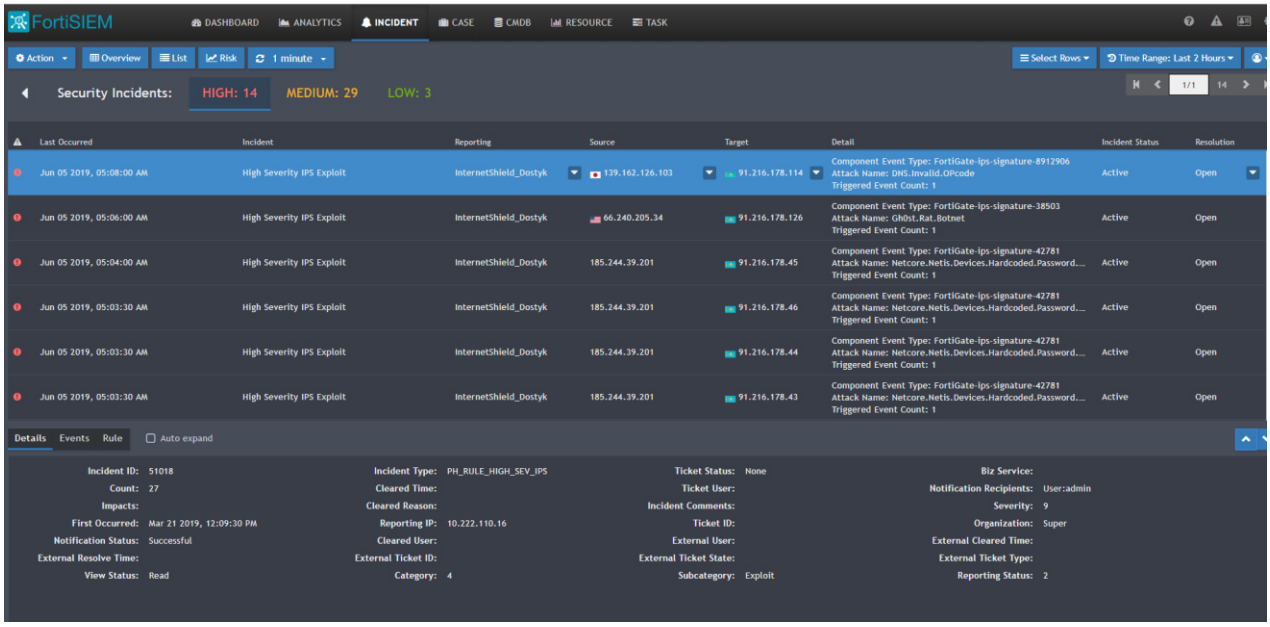
Reporting IP	Risk Name	Source IP	Destination IP	File Name
10.192.0.12	High Risk	10.40.0.151	31.169.73.70	fr.exe

Сурет 3.21 – FortiSIEM бақылау панелінің қауіпті файл табуы туралы хабарландыруы

Қауіптерді басқару. FortiSIEM құралдарының арқасында администратор оқиға туралы ақпаратты кім жібергені, оқиға болған қандай оқиға, оқиға болған бизнес қызметі, оқиғалардың саны туралы ақпаратты қамтитын оқиғаның қысқаша мазмұнын көре алады. Осы мәліметтерден біз бұл оқиғаның сыни екенін білеміз.

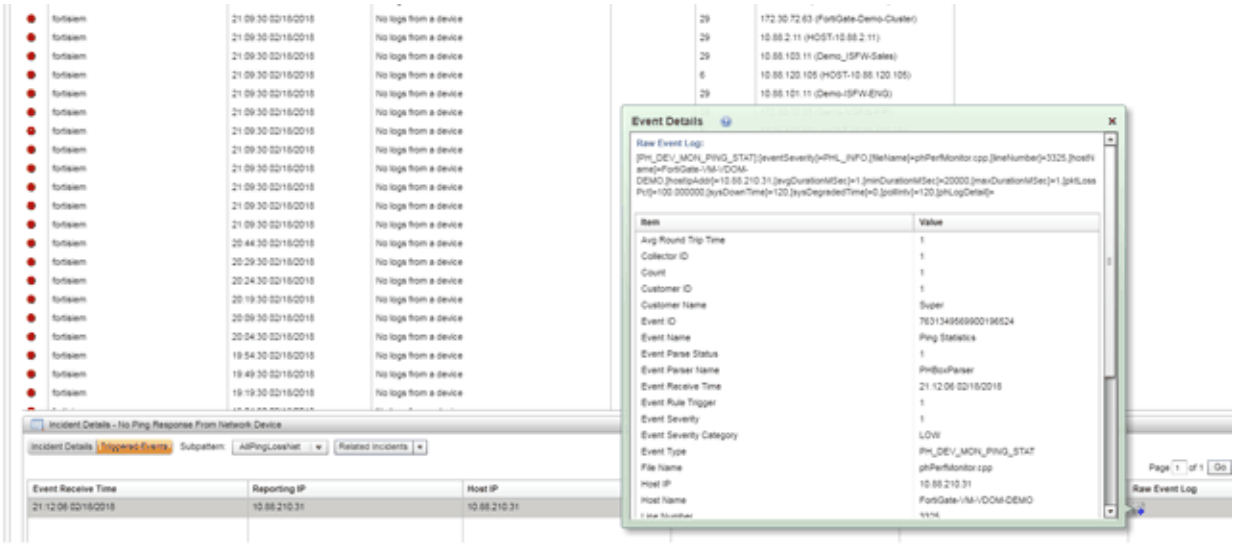


Сурет 3.22 – Орын алған оқиғаның резюмесі

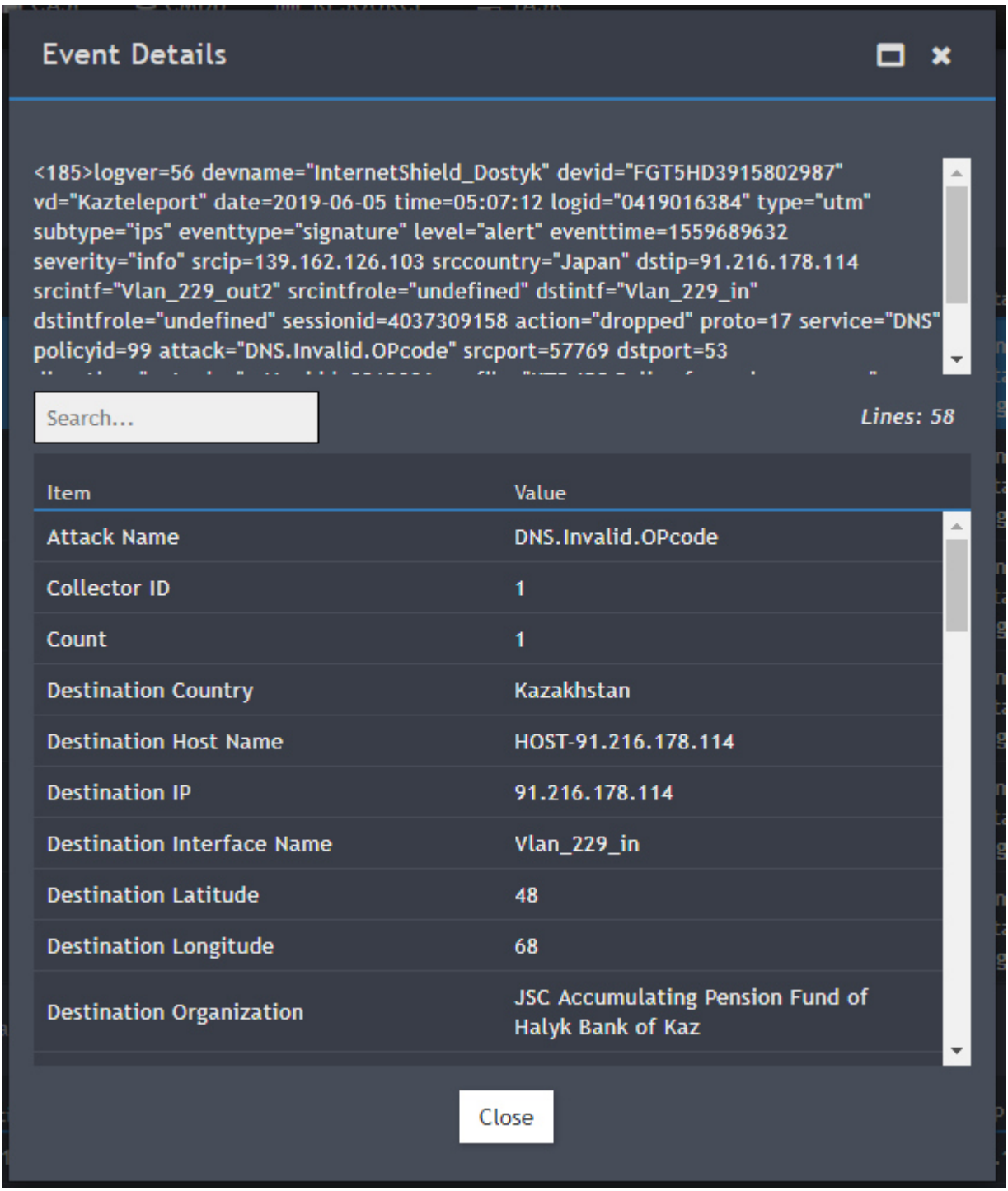


Сурет 3.23 – Орын алған оқиғаның резюмесі

Әрбір оқиға үшін оқиға туралы оқиғаларды қадағалауға болатын егжей-тегжейлі ақпараттар бар, оқиғалардың толық журналын көріңіз. Осылайша, қосымша корреляция ережесін қалыптастыруға болады. Ережелер критерийлердің көп мөлшерін салыстыра отырып, иерархиялық жолмен жасалады.



Сурет 3.24 – Орын алған оқиғаның резюмесі



Сурет 3.25 – Орын алған оқиғаның резюмесі

Белгілі бір қауіп-қатер түрін қадағалай алатын және белгілі бір уақыттағы нақты оқиғаларды көре алатын әкімшінің қауіп-қатерлерін уақыт бойынша іздестіруге болады.

3.4 FortiSIEM лицензиялау схемалары

FortiSIEM лицензиялары желілік құрылғылардың негізгі табу мүмкіндіктеріне қатынасу үшін пайдаланылады. Құрылғыларға ажыратқыштар, маршрутизаторлар, брандмауэрлер, серверлер және т.б. кіреді.

FortiSIEM тұрақты лицензия немесе жазылым ретінде таратылады. Әрбір лицензия мәліметтерді жинау мен байланыстыруды, ескертулер мен ескертулерді жасауды, есеп беруді, талдауды, деректерді сақтауды іздеуді және оңтайландыруды қамтиды, желілік құрылғыға (қосқыш, маршрутизатор, брандмауэр және т.б.) 10 EPS (секундтық оқиғалар) 2 EPS соңғы құрылғы үшін (Windows, Linux серверлері, пайдаланушының соңғы станциялары және т.б.). Инфрақұрылым клиенттері үшін FortiSIEM All-In-One лицензиясы ұсынылады. Windows Extended Monitoring Agents жеке лицензиясы бар, әр агент үшін 2 EPS есептеледі. FortiCare-ді қолдау бөлек сатып алынады (1-ден 5000 құрылғыға дейін).

FortiSIEM All-In-One сервисінің негізгі көлемі 50-ке дейін құрылғылар мен 500 EPS-ты қамтиды.

FortiSIEM жеткізу опциялары. Өнім физикалық немесе виртуалды құрылғы (FortiSIEM Virtual Appliance) немесе бұлтты қызмет ретінде қол жетімді (AWS Market Place-да FortiSIEM Cloud арқылы BYOL арқылы).

Сурет 3.26 – FortiSIEM физикалық құрылғылар желісі

Кесте 3.2 – FortiSIEM физикалық құрылғыларының характеристикалары

	FortiSIEM 500f Collector	FortiSIEM 2000F Supervisor	FortiSIEM 3500F Supervisor
Форм-фактор	1 бірлік	2 бірлік	4 бірлік
Процессор	Intel Xeon E3-1225V3 4C4T 3.2 ГГц	Intel Xeon E5-2620V3 6C12T 2.40 ГГц	2x Intel Xeon E5-2680V2 10C20T 2.80 ГГц
Желілік интерфестері	4 порт 1 Гбит Ethernet RJ45	4 порт 1 Гбит Ethernet RJ45	4 порт 1 Гбит Ethernet RJ452 слот 1 Гбит Ethernet SFP(оптика)
Жады көлемі	3 ТБ (1 x 3 ТБ)	36 ТБ (12 x 3 ТБ)	72 ТБ (24 x 3 ТБ)
Жедел жады	DDR3 16 Гб (2 x 8 ГБ)	DDR3 32 Гб (4 x 8 ГБ)	DDR3 64 Гб (8 x 8 ГБ)

3.2-кестенің жалғасы

Биіктігі*Ені*Ұзындығы(мм)	43 х 437 х 503	89 х 437 х 648	178 х 437 х 660
Салмағы(кг)	14	26,3	42,5

4 Техникалық-экономикалық негіздеме

Бұл дипломдық жобаның мақсаты - ақпараттық қауіпсіздікті қамтамасыз ету бастамаларын басқару жүйесін құру.

Жүйені жобалау кезінде мамандар тобы тартылатын болады, олар: техникалық менеджер, жүйелік әкімгер. Техникалық менеджердің міндеттері жұмыс кестелерінің сақталуы мен дамуы, оларды бақылау және оңтайландыру болып табылады. Жүйелік администратордың міндеттері компьютерлік және офистік техниканы орнату, қызмет көрсету, жүйелік әкімшілендіру, жүйелік бағдарламалық жасақтаманың (Windows ОЖ) қателерсіз жұмысын қамтамасыз ету, кеңсе және қолданбалы бағдарламалық қамтамасыз етуді (MS Office) орнату, баптау және жаңарту, компанияның желісінің жұмысын және қауіпсіздігін қамтамасыз етуді қамтиды. Техникалық-экономикалық негіздемені мынадай элементтер:

- SIEM жүйесін жобалаудың күрделілігін анықтау;
- жобаның құнын есептеу;
- жобаның нәтижелерін бағалау.

4.1 SIEM жүйесін жобалаудың күрделілігін анықтау

SIEM жүйесін жобалаудың күрделілігін дәл анықтау үшін, бүкіл тапсырманы қарапайым қадамдарға бөлу керек. Бұл SIEM жүйесі жобасын тиімді түрде бақылауға мүмкіндік береді, бұл кешенді тапсырманы жеңілдетілген тапсырмаларға бөле отырып. SIEM жүйесін жобалаудың күрделіліктік үлгілеуі 4.1-кестеде келтірілген.

Кесте 4.1 – SIEM жүйесін жобалау кезеңдері

Жобалау кезеңдері	Жұмыс түрі	Еңбек қарқындылығы
1 Кезең	Жоба бойынша ШСС жобасын әзірлеу және активті және пассивті желі жабдығын қосу	35
2 Кезең	Жабдықты таңдау және қосылатын магистралды ұйымдастыру және сыртқы әлем мен желі арасындағы маршрут	22
3 Кезең	Адрестік кеңістігін тарату	13
4 Кезең	Қызметтер мен жабдықтардың техникалық аспектілері қарастырылуда.	23
5 Кезең	Серверлерге арналған бағдарламалық қамтамасыз етуді таңдау, желіні басқару және мониторингі, операциялық жүйелер	34
6 Кезең	Жөндеу және ақаулықтарды жою	20

4.1-кестенің жалғасы

7 Кезең	Тестілеу және есеп беру	45
8 Кезең	Жобаны іске асыру және талқылау	80
Қорытынды: дипломдық жобаны іске асырудың күрделілігі		272

Жұмыс күнінің ұзақтығы - 8 сағат. Нәтижесінде бағдарламалық өнімді енгізу үшін 34 жұмыс күні қажет (272: 8 = 34).

4.2 SIEM жүйесін жобалау құнын есептеу

SIEM жүйесін жобалау үшін қажетті шығындарды анықтау келесі элементтерді қамтитын қол жетімді бағалауға негізделеді:

- материалдық шығындар;
- еңбекке ақы төлеу;
- әлеуметтік салық;
- негізгі құралдардың амортизациясы;
- басқа шығындар.

Материалдық шығындар SIEM жүйесін жобалау үшін қажетті материалдар, энергия және басқа шығындар үшін негізгі және қосымша шығындарға бөлінеді. Материалдық шығындарды есептеу 4.2 кестеде көрсетілген нысан бойынша жүзеге асырылады.

Кесте 4.2 – материалдық ресурстардың құны

Материал атауы	Маркасы	Өлшем бірлігі	Саны	Біреуінің бағасы	Құны, теңге
Офиске қағаз	SvetoCopy	Қаптама	1	1 500	1 500
Дәптер (96 парақ)	Abdi	Дана	1	250	250
Блокнот	Abdi	Дана	2	1 000	2 000
Қалам	Abdi	Дана	3	100	300
Компьютерлік пернетақта мен тышқан	HP	Дана	2	3 338	6 676
Қорытынды:					10 726

HP Helpdesk 3100 компьютері SIEM жүйесін жобалау үшін пайдаланылады, компьютердің қуаты тағайындалған тапсырмаларды орындау үшін жеткілікті. Компьютер мен бағдарламалық жасақтама үшін операциялық жүйені орнату қажет.

Материалдық ресурстар үшін талап етілетін жалпы сома ($З_м$) келесі формула бойынша есептеледі:

$$З_м = \sum P_i * Ц_i, \quad (4.1)$$

мұндағы P_i- і-ші материалдық ресурстардың, табиғи бірліктердің тұтынуы;

Ц$_i$- і-ші материалдық қордың бірлігіне баға, n;

i - материалдық ресурстардың түрі;

n - материалдық ресурстардың саны.

Қажетті жабдықтар мен бағдарламалық қамсыздандырудың құнын есептеу 4.3-кестеде келтірілген түрде жасалады.

Кесте 4.3 – Жоба үшін қажетті жабдықтар мен бағдарламалық қамтамасыз етудің құнын есептеу

Құрылғы атауы	Маркасы	Өлшем бірлігі	Саны	Біреуінің құны	Теңгедегі суммасы
Жеке компьютер	HP Helpdesk 3100	Дана	2	289 990	579 980
Монитор	HP22f 2XN58AA Black	Дана	2	46 990	93 980
Принтер	HP Color LaserJet Pro M254dw	Дана	1	88 900	88 900
Офистік БҚ	Microsoft Office Professional plus 2019 Лицензиясы	Дана	1	87 850	87 850
Барлығы:					850 710

$$З_м = 10\ 726 + 850\ 710 = 861\ 436 \text{ (тг)}$$

SIEM жүйелерінің жобаларын іске асыру үшін 861 436 теңге көлемінде материалдар қажет.

4.3 Электр энергиясының құнын есептеу

Желінің қауіпсіздігін жобалау электр энергиясын тұтынусыз жасай алмағандықтан, электр энергиясының құнын есептеу керек.

4.1-кестеге сәйкес, SIEM жүйесін жобалау үшін шамамен 272 сағат қажет, енді 272 сағат ішінде жұмсалатын электр энергиясын есептеу қажет.

$$Э = З_{эл.эн.обор.} + З_{доп.нужды.} \quad (4.2)$$

мұнда $З_{эл.эн.обор.}$ - электр жабдықтардың құны;

$З_{доп.нужды.}$ - қосымша қажеттіліктер үшін электр энергиясының құны.

Жабдықтарға қажетті электр энергиясын есептеу келесі формула бойынша анықталады:

$$З_{эл.эн.обор.} = \sum W * К_{исц} * S * T, \quad (4.3)$$

мұндағы W - энергия тұтыну, W;

$К_{исц}$ - пайдалану коэффициенті ($К_{исц}$ = 0.7 - 0.9);

Т - жұмыс уақыты;

S - тарифі (АлматыЭнергоСбыт ЖШС 01.01.19 ж. Заңды тұлғалар үшін 1 кВт / сағ = 23,85 теңге).

Тұтынылатын электр энергиясының құнын есептеу нәтижелері 4.4-кестеде келтірілген.

Кесте 4.4 - Электр шығындары

Құрал атауы	Номаинальды қуаты, кВт	Қуаттылық коэфициенті	Жұмыс жасау уақыты, сағ	ЭЭ бағасы тг/кВт сағ	Сумма, тг.
ДК	0,9	0,9	272	23,85	5 254,63
Монитор	0,6	0,7	272	23,85	2 724,62
Принтер	0,6	0,7	22	23,85	220,37
Жарықтандыру	0,3	0,7	136	23,85	636,07
Барлығы:					8 835,69

$$З_{эл.эн.обор.} = 8\,835{,}69 \text{ (теңге)}$$

Қосымша қажеттілік үшін шығындар электр энергиясының өзіндік құнын 5% мөлшерінде ұлғайту индикаторы негізінде есептеледі:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (4.4)$$

Формулаға сәйкес қосымша талаптардың құнын анықтаңыз (4.4):

$$З_{доп.нужды} = 0.05 * 8\,835{,}69 = 44{,}19 \text{ (теңге)}$$

Барлық есептеулер бойынша электр энергиясының жалпы шығындары:

$$Э = 44{,}19 + 8\,835{,}69 = 8\,879{,}87 \text{ (теңге)}$$

4.4 Еңбек шығындарын есептеу

Жоғарыда айтылғандай, SIEM жүйесін жасау үшін сізге екі қызметкер қажет:

- жоба жетекшісі - жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік саланы зерттеу;
- жүйелік администратор - компьютерлік және офистік техниканы, офистік техниканы, АТС-ны орнату және қызмет көрсету, жүйелік бағдарламалық қамтамасыз етудің қатесіз жұмысын қамтамасыз ету.

Еңбекке ақы төлеу шығындарының мөлшері мынадай формула бойынша есептелуі мүмкін:

$$З_{тр} = \sum ЧС_i * T_i \quad (4.5)$$

мұнда $ЧС_i$ і - і-ші қызметкердің сағаттық ставкасы, мр;

T_i - модельді дамытудың күрделілігі, адамдар × сағ ; і - қызметкер санаты;

n - ҚБ-ны дамытумен айналысатын қызметкерлердің саны.

Жобаны іске асыру кезінде қатысушыларға жұмыс уақыты біркелкі емес, сондықтан әр қызметкердің сағаттық мөлшерлемесін және жалпы жалақыны белгілеу маңызды.

Қызметкердің сағаттық ставкасы келесі формула бойынша есептеледі:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (4.6)$$

мұнда $ЗП_i$ - і-ші қызметкердің айлық жалақысы, мр;

$ФРВ_i$ - і-ші қызметкердің жұмыс уақытының айлық қоры, сағ.

Менеджердің айлық жалақысы 280 000 теңге, ал жүйелік әкімшінің айлық жалақысы 250 000 теңге. Әрбір қызметкердің (4.6) формуласына сәйкес сағаттық ставкасын есептеңіз:

$$ЧС_{руководитель} = \frac{280\,000}{22 * 8} = 1690{,}90 \text{ тг/ч}$$

$$ЧС_{сис.админ} = \frac{250\,000}{22 * 8} = 1420{,}45 \text{ тг/ч}$$

Техникалық жоба менеджерінің сағаттық жылдамдығы 1 690,90 (тг / сағ), дамудың күрделілігі - 127 сағат. Жүйелік администратордың сағаттық жылдамдығы 1420,45 (тг / сағ), жұмыс жүктемесі - 272 - 127 = 145 сағат. Формула бойынша (4.5) жұмысшылардың жалақысына жұмсалатын шығындардың мөлшерін есептеу мүмкін болады:

$$З_{тр} = 1690,90 * 127 + 1420,45 * 145 = 420\ 709,55 \text{ (тенге)}$$

Еңбек жалақы көрсеткіші бойынша есептеулер 4.5-кестеде көрсетілген.

Кесте 4.5 – Жалақыны есептеу

Қызметкер санаты	Біліктілігі	Жұмысшы атқаратын жұмыс, сағ.	Сағаттық жалақысы, тг/сағ	Сумма, тг.
Жетекші	Қоюшыинженер	127	1690,90	214 744,30
Жүйелік - администратор	Инженер	145	1420,45	205 965,25
Жалпы:				420 709,55

4.5 Әлеуметтік салықтық шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық жалақы жобасының 9,5% құрайды. Әлеуметтік салық келесі формула бойынша есептеледі:

$$С_н = (ФОТ - ПО) * 0,095 \quad (4.7)$$

онда ПО - зейнетақы қорына шегерім, олар жалақы қорының 10% құрайды.

$$ПО = 420\ 709,55 * 0,1 = 42,070,96 \text{ теңге}$$

$$С_н = (420\ 709,55 - 42\ 070,96\ ) * 0,095 = 35\ 970,67 \text{ тенге}$$

Есептеулердің нәтижелері кестеде келтірілген (4.6):

4.6-кесте - Әлеуметтік салықты есептеу

Қызметкер санаты	Қызметкерлер саны	Жалақысы, тг	Зайнетақы қорына шегерім, тг	Әлеуметтік салық, тг
Жетекші	1	214 744,30	21 474,43	18 360,63
Жүйелік - администратор	1	205 965,25	20 596,52	17 610, 04
Жалпы:				35 970,67

4.6 Негізгі құралдардың тозуы және басқа да шығыстар

Негізгі құралдар бойынша амортизация нормалары Қазақстан Республикасының салық кодексіне сәйкес анықталуы тиіс. ОБ құнсыздануы мынадай формула бойынша анықталуы мүмкін:

$$A_г = \frac{С_{об} * Н_а}{100} \quad (4.8)$$

мұндағы $С_{об}$- жабдықтың құны;

$С_{об}$- амортизация нормасы (амортизация нормасы = 25);

Формула (4.8) ДК үшін жыл үшін амортизацияны есептеу үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_{г} = \frac{289\ 990 * 25}{100} = 72\ 497 \text{ тенге}$$

Енді жобалау кезеңіндегі амортизация нормасын есептеу қажет:

$$A_{г} = \frac{72\ 497 * 34}{365} = 6\ 753 \text{ тенге}$$

Сол сияқты барлық жабдықтар үшін амортизация нормасын есептеу қажет. Есептеулердің нәтижелері кестеде келтірілген (4.7).

Кесте 4.7 - Құнсыздануы

Бағдарламлық қамтамасыз етудің атауы	Құралдың не бағдарламалық қамтамасыз ету құны, тг	Жылдық амортизация, %	Жылдыө амортизация құны, тг	Жобалау кезіндегі амортизация құны, тг
Жеке компьютер	289 990	25	72 497	6 753
Монитор	46 990	20	9 398	875
Принтер	88 900	20	17 780	1 656,2
Барлығы:				8 284,2

Сонымен қатар, Интернет шығындары 25 000,00 теңге болады.

SIEM жүйесін жобалауға арналған шығын сметасы.

Барлық ұсынылған есептердің негізінде кестеде келтірілген (4.8) нысан бойынша SIEM жүйесін жобалаудың өзіндік құнын бағалау қажет. 4.1-графикте операциялық шығыстардың кестесі келтірілген.

4.8-кесте - Жүйені жобалаудың болжамды құны

Шығыс түрі	Сумма, тг
Құрылғыға шығыс	861 436,00
Еңбекақыға шығыс	420 709,55
Әлеуметтік салықтар	35 970,67
Электрэнергиясына шығыс	8 879,87
Негізгі фондтардың амортизациясы	8 284,2
Басқа да (интернет)	25 000,00
Жалпы шығын:	1 360 280,29

4.7 Жобаның ықтимал бағасын анықтау

Бағдарламалық қамсыздандыру құны өнімнің сапасы, оны жасау мерзімдері және өнімнің сапасы негізінде айқындалады. Бағдарламалық қамтамасыз ету үшін $Ц_Д$құны келесі формула бойынша есептеледі:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (4.9)$$

мұнда $З_{нир}$ – бағдарламалық қамтамасыз етудің құны, тг;

Р – бағдарламалық қамтамасыз етудің орташа табыстылығы (%). Бұл параметр 25% деп есептеледі.

$$Ц_Д = 1\ 360\ 280{,}29 * \left(1 + \frac{25}{100}\right) = \ 1\ 700\ 350{,}36 \text{ теңге}$$

Бұдан әрі, ҚҚС-ты қоса алғанда, сатудың өзіндік құнын анықтау қажет, ҚҚС ставкасы Қазақстан Республикасының заңнамасымен белгіленеді. 2019 жылға ҚҚС ставкасы 12% құрайды. Сатылымның құны, ҚҚС қоса есептегенде, келесі формула бойынша есептеледі:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (4.10)$$

$$Ц_р = 1\ 700\ 350{,}36\ + 1\ 700\ 350{,}36\ * 0{,}12 = 1\ 904\ 392{,}40 \text{ теңге}$$

Сатып алушы үшін негізгі көрсеткіш желінің қауіпсіздігін және оның орындалуын жобалаудың оңтайлы бағасы болады. Жобаның құны мен пайдалылығы балансқа ие болу үшін сатып алушы жобаны сатып алуға мүдделі болуы керек. Сатып алушы үшін сапалы нәтиже сатып алынатын бағдарламалық қамтамасыз ету сатып алушыға қарсы барлық қажетті тапсырмаларды толығымен толтырады деп саналады. Сондай-ақ, соңғы тарауда жобаның шарттық бағасы есептелді, ол 1 904 392,40 теңгені құрайды, бұл экономикалық тиімділік тұрғысынан ұтымды. Жыл ішіндегі табыс: 340,070.07 теңге.

5 Өмір тіршілік қауіпсіздігі

5.1 Компьютердің жұмыс кезіндегі қауіпсіздігі

Компьютер – адам интеллектінің ең тамаша жетістіктерінің бірі. ЭЕМ және ДК үлкен ресурстары арқылы қолданушылардың тікелей диалог жүргізе алу мүмкіндігі миллиондаған адамдардың экран алдында көп уақыт өткізуіне алып келді. Уақыт өте келе компьютер пайдаланушыларында өздерін сезінуге байланысты шағымдар жиынтығы пайда болады.

Бұл компьютерден адамның денсаулығына сәулеленудің әсері туралы ойлаға алып келді. Мұндай ойлар үшін көптеген себептер бар. Бірқатар ғалымдар тұрмыстық АЖЖ көздерінен адамдарға электромагниттік сәулеленудің әсерімен байланыстырады.

Электрондық құрылғылар әртүрлі түрдегі сәуле шығарады – электромагниттік толқындар, электростатикалық кернеу және радиация. Электростатикалық кернеу электрді пайдаланатын барлық құрылғыларда болады, оның негізгі көздері – электр беру желілерін құрады. Қалада тұрып, одан құтылу мүмкін емес, компьютерлерден сәулелену осы әсерден аз көлемді құрайды. Сондықтан электромагниттік толқындарға толығырақ тоқтай кетсек.

Олар сезілмейді, денсаулыққа айтарлықтай зиян әкелмейді, бірақ дүниежүзілік денсаулық сақтау ұйымы экология үшін қауіпті факторлардың тізіміне электромагниттік сәулені енгізді. Электр желісінен жұмыс істеу кезінде аспаптар Жерді қоршаған физикалық өрісте импульстердің тербелісін жасайды. Бұл тербелістер экожүйенің жай-күйіне теріс әсер ете отырып, ғаламшардың жалпы электромагниттік өрісінің қозуын тудырады. Ал үйде компьютерден зиянды сәулелену денсаулыққа теріс әсер етуі мүмкін.

Әрбір дербес компьютерден электромагниттік сәуле шығады: төмен жиілікті және радиожиілікті. Дүниежүзілік денсаулық сақтау ұйымының пікірінше, толқындардың екі түрі де канцерогенді болып табылады – ол обыр ауруын тудыруы мүмкін.

5.1.1 Компьютер мониторынан бөлінетін сәулелер

Мониторлардың ішінде электронды – сәулелі түтікшелілері ең зиянды екені анықталды. Олады пайдаланған кезде, компьютер сәуле шағарады ма деген сұрақ туды. Иә – монитордан бөлінетін радиацияның зиянын рентген сәулелерінің зиянымен салыстыруға болады. Құрал 2 және одан да көп сағат компьютерді өшіргеннен кейін де сақталатын қуат өрістерін және жоғары электр кернеуін шығарады.

Сұйық-кристалды мониторлар айтарлықтай қауіпсіз, олар шамамен 50 Гц сәулелену қалыптастырады. Бұл доза ағзаға нақты зиян келтіру үшін аз, бірақ тұрақты әсер ету кезінде жағымсыз салдарлардан қашып құтылу мүмкін емес. Аналық плата мен корпустың қызуына байланысты ауаның деионизациясы және қоршаған ортаға зиянды заттардың бөлінуі орын алады. Міне, сондықтан тұрақты жұмыс істейтін есептеу техникасы бар бөлмелердегі ауа тыныс алу үшін өте ауыр. Тыныс алу жүйесі әлсіз адамдар үшін бұл

фактор демікпені тудырып, кері әсер етуі мүмкін. Ол компьютердің электростатикалық өрісінің және монитордың ауадағы өлшенген шаң бөлшектеріне әсерімен одан әрі күрделене түседі. Электрленіп алып, олар "тозаңды коктейль" құрайды, тыныс алуды ауырлатады.

Сенсорлы экранның болуы радиацияның жоқтығына кепілдік бермейді. Себебі, сіздің саусақтарыңыз экранда манипуляциялар жасай отырып, онымен, wi-fi-антеннадан бірнеше миллиметрде жанасады.

Әсіресе, жол жағдайында жұмыс істеуге арналған портативті құрылғы ретінде ойланған ноутбук сәуле шығару мәселесін де назарсыз қалдыруға болмайды. Бұл ыңғайлы және көпфункционалды құралдарды толық жұмыс күні ішінде пайдалану әртүрлі патологиялар мен аурулардың себебі болуы мүмкін. Өйткені, ол қарапайым компьютер сияқты электромагниттік сәулелену көзі болып табылады, бірақ ол адамға компьютерден айтарлықтай жақын орналасады. Сол себепті, олардың ада ағзасына зияны да көбірек.[2]

Жүйелік блок өзі айналасында электромагниттік өрісті белсенді жасайды. 2 мгтс (миллигаусс) минималды фондау ағзаға теріс әсер етеді. Ол адамнан 50-ден 100 см-ге дейінгі қашықтықта орналасқан құрылғы тудыра алады. Процессор неғұрлым жақынырақ болса, соғұрлым күшті әсер етеді.

Олар ерекше қауіп тудырады, өйткені әрқашан басқа тікелей киіледі. Сымсыз гарнитуралар мен Bluetooth жүйелері – бұл ең нашар нұсқа: олар арқылы адам ағзасына радио толқындары да енеді. Кабель айтарлықтай қауіпсіз, бірақ ұмытпаған дұрыс: оның ішінде металл – компьютер процессорынан тікелей кез келген сәулелер үшін тамаша өткізгіш. Жалпы, құлаққаптарды алып тастау және колонкадан дыбыс шығару мүмкіндігі пайда болған соң, оны бірден пайдаланған жөн.

Кейбір қуатты колонкалар, әсіресе вуферлер айналасында елеулі электромагниттік өріс жасайды. Олардан кемінде 50 см қашықтықта ұстаған жөн.

Мөлшері әртүрлі және тиісінше қуаты бар. Ең қарапайым, үй принтері 50 см қашықтықта ұстаған дұрыс. Үлкен кеңсе үшін арналған принтерді адамдардан 65 см арақашықтықта қалдыру керек.

Олардың радиожиілік магнит өрістері айнала көп метрге созылады. Бұлар сонысымен ыңғайлы, бірақ денсаулық үшін зиян. Тіпті егер оларды компьютерге кабель арқылы қосқан күнде де – төмен жиіліктер адамға әсер етеді. Сондықтан оларды 35 см кем емес қашықтықта қою керек.

Олар жоғарыда аталған барлық техника үшін өте қуатты төмен жиіліктерді шығарады. Оларды бір метр қашықтықта ұстау керек.

5.2 Компьютерден бөлінген сәулелердің адамға әсері

Компьютерден бөлінетін сәулелердің адам ағзасына неге зиянды екенін анықтайық.

Адам ағзасы да электрлік импульстерді шығарады. Олардың көмегімен ми мен жұлынға жүйке үштары арқылы сигналдар келіп түседі, қаңқа бұлшықеті мен жүрек бұлшықеттері азаяды. Жүйке үштары арқылы

секундына мыңдаған сигналдар беріледі, сондықтан компьютерден қандай зиян келетінін оңай түсінуге болады, сәулелер электрлік импульс жіберудің қиын жүйесіне әсер етіп, олардың өзара байланысына бөгет келтіруі мүмкін. Оның әсері бір сәтте сезілмейді,ол ағзада жинақталып, мүшелер мен жүйелердің жұмысын біртіндеп нашарлатады.

Екі маңызды жүйе ең осал болып табылады:

- жүйке жүйесі;
- жүрек – қан тамырлар жүйесі.

Бұның әсерінен ми сигналдары патологиялық түрде өзгеруі мүмкін. Бұл мидың және жүрек-тамыр жүйесі органдарының бұзылуына себеп болады. Жүрек-қантамыр жүйесінің қалыпты жұмыс істеуі импульстердің когеренттігіне және беріктігіне байланысты. Үйдегі бір немесе одан да көп құрылғылар жүрек жұмысын елеулі бұзылуға алып келмейді, бірақ үнемі сәулелену аритмия мен жүрек-тамыр қабілетінің бұзылуына әкелуі мүмкін. Ұзақ уақыт бойы әсер етуі бас ауруы, мигреньдер, иммунитеттің төмендеуі, депрессия, гормоналды теңгерімсіздік және ұйқының бұзылуына әкелуі мүмкін. Компьютерде көп жұмыс істеу Альцгеймер ауруы, Паркинсон ауруы, қатерлі ісік ауруы және ұрпақты болу жүйесінің бұзылу қаупін арттырады. Сонымен қатар миокард және перикард ауруларына, ағзаның жалпы гормональды фонының бұзылуына, су-тұз алмасуының нашарлауына, гомеостаздың бұзылуына алып келуі мүмкін.

Үй компьютері, ноутбук немесе смартфон зиянды сәуле көзі болып табылады. Компьютерден қанша сәуле алатынымыз түрлі факторларға байланысты: құралдың түрі, пайдалану уақыты, орналасуы.

5.3 Сәулеленуден қорғанудың іс – шаралары

Компьютерден қандай сәуле бөлінетінін және оның адам ағзасына калай әсер ететінін анықтаған соң, одан қорғану шараларын қарастыра кетсек.

Келесі кеңестерді орындай отырып, компьютерден бөлінетін сәулелердің әсерін бәсеңдетуге болады:

- егер бірнеше компьютер немесе ноутбуктер үнемі бір үй-жайда (мысалы, сыныпта, кеңседе) тұрса, оларды құрылғылар бөлменің периметрі бойынша тұратындай, ал орталық бос болатындай етіп орналастыру керек;
- мүмкіндігінше электрмагниттік сәулеленудің саны мен қарқындылығын азайтатын арнайы қорғаныс құралдары орнатылған мониторларды пайдаланған жөн. Әсіресе, бұл кеңес компьютер алдында көп уақыт жұмсайтын балаларға өзекті болып табылады;
- мониторды таңдау барысында, оның кеңеюіне, қорғау деңгейіне және радиациялық сәулелену мөлшеріне назар аудару керек. Low Radiain жазуы бар экрандарға көбірек назар адару қажет, себебі бұл ең аз радиация санын білдіреді;
- монитор көру үшін ыңғайлы қашықтықта, ал жүйелік блок пайдаланушыдан барынша алыста орналасуы тиіс;

- жұмыс аяқталғаннан кейін компьютерді өшіру керек, өйткені ол қаншалықты ұзақ жұмыс істесе, соғұрлым көп сәуле шығарады және ауаны арқылы қоршаған ортаға зиянды заттардың үлкен мөлшерін бөледі;

- арнайы қорғаныс пленкасын пайдалану электромагниттік сәуле шығару қарқындылығын және пайдаланушы ағзасына зиянды әсер ету мөлшерін азайтады;

- шаңды жүйелі түрде шығару, ылғалды жинау және мүмкіндігінше ионизаторларды қолдану компьютер жұмысының нәтижесінде алынған заттар әсер ететін дем шығаратын ауаның сапасын жақсартады, сондай-ақ адамның денесіне электромагниттік сәулеленудің зиянды факторларының әсерін азайтады;

- монитордың жандарынан және артқы бөлігінен шығатын сәулелер компьютермен бір бөлмеде, бірақ оны қолданбайтын адамға әсер етпеуі үшін, оны бөлменің бұрышына орналастырған жөн. Сондай-ақ, монитор көзге ыңғайлы жағдайда (бірақ кемінде 40 см) болуы тиіс, ал жүйелік блок пайдаланушыдан мүмкіндігінше алыс орналасуы тиіс.

5.4 Қолданушының компьютерден қауіпсіздік қашықтығын есептеу

Компьютер алдында жұмыс жасау барысында, барынша қауіпсіздікте болу үшін, монитордан көзге дейінгі ең аз арақашықтықты білу керек. Егер монитордың экраны қолданушыға қатысты дұрыс орналасса, қолданушының жақсы көру қабілетін ұзақ сақтап, остеохондроз және омыртқаның қисаюын болдырмайды.

Монитор мен көздің арасындағы қашықтық, ең алдымен, оның өлшемді параметрлеріне байланысты. Қазіргі уақытта ең танымал модельдер 14 – тен (ноутбуктар) 27 дюймге дейінгі диагоналдармен, ал ең үлкені диагоналі 30 – дан асатын экрандармен жабдықталған. Мониторлардың техникалық мүмкіндіктері мен қолдану салалары олардың дюйм өлшемдеріне байланысты.

Ең көп таралған модельдер келесі түрде болады:

1) 14-16''. Бұл бұқаралық ноутбуктар, олардың өлшемдері оңтайлы өнімділікті процессорларды ендіруге мүмкіндік береді. Кішкентай диагоналды портативті құрылғылардың қолданыс аясы тар.

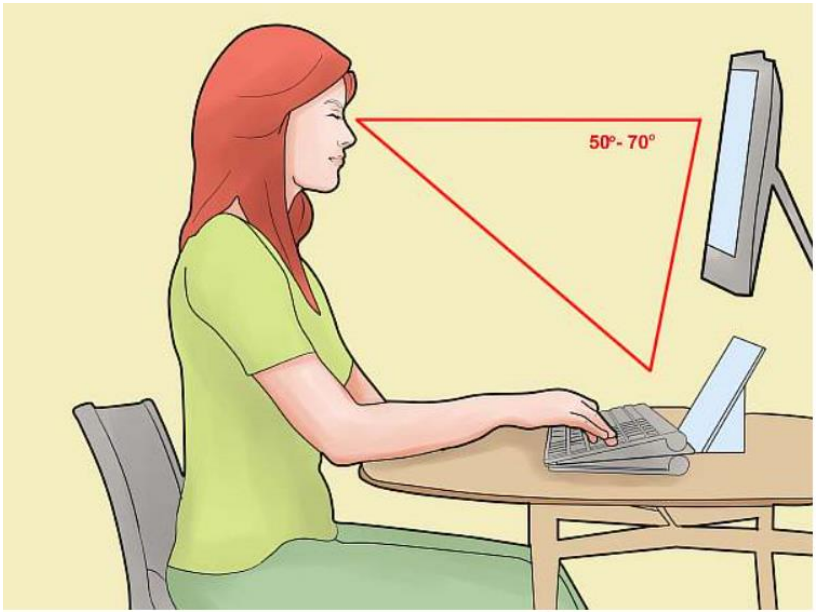
2) 17''. Көлемді ноутбуктар кеңсе үшін ыңғайлы нұсқа. Алып жүру ыңғайлы болмағанымен, жұмыс аймағында кеңістікті үнемдйді.

3) 18,5-20,1''. Шағын стационарлы модельдер, көбінде мәтін редакторында жұмыс жасау үшін пайдаданылады.

4) 21,5-24''. Орташа диагоналды бейнемониторлар қолданушыға ыңғайлы түрде мәтін теруге, бейнебаяндарды редакциялауға, бейнефильмдерді көруге мүмкіндік беретін әмбебап нұсқа болып табылады. 3D бейнесі бар ойынды қолдау үшін диагоналі кемінде 23 дюйм болуы керек.

5) 27'' және одан жоғары. Олар көбінесе фильмдер көруге, фото, бейне, аудио материалдырды редакциялау үшін қолданылады. Бұл мониторлар студияда, әсіресе, дыбыс жазу және фильм түсіру барысында таптырмас құрал

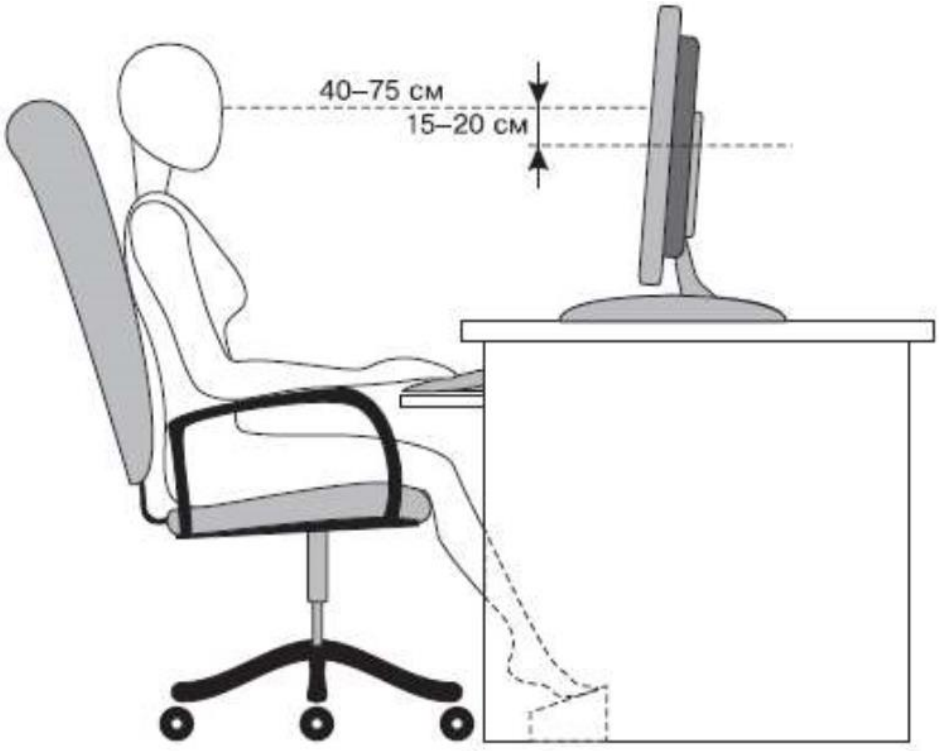
болып табылады. 32 және одан да жоғары дюймді мониторлар бейнебақылау үшін пайдаланылады. Ал қабырға мониторын теледидар ретінде пайдалану керек болса, оның диагоналі 31 – 34 дюйм болғаны жөн.



Сурет 5.1 – Оператордың компьютер алдындағы экономикалық жағдайы

Ғылыми зерттеулерге сүйенсек, адамның көзі 17 градус шеңберіндегі кескінді анық көре алады. Бұл жауап математикалық т.рде алынады: пайдаланушының беті мен экран арасындағы ең аз рұқсат етілген қашықтық оның диагональды ұзындығы болып табылады.

Көз бен бейне монитор арасының қанша сантиметр болу керек екенін анықтағанда, оның өлшемдерін ғана емес, сонымен қатар жобалау ерекшеліктерін де ескеру қажет. TFT панелі бар СК – дисплейді қолдану қауіпсіздірек.



Сурет 5.2 – Нормативті арақашықтық

Электронды – сәулелік түтікке негізделген дәстүрлі құрылғылармен салыстырғанда, СКД үлгілері мынадай артықшылыққа ие:

- элетромагниттік сәулеленудің өте аз мөлшерде болуы;
- көрінетін аймақтың үлкен өлшемі (15 дюймдік СКД мониторы 17 дюймдік CRT аналогы сияқты);
- сурет бұрмалауының жоқтығы;
- үлтелде үнемді орын алуы.

CRT бар болған жағдайда компьютер мониторынан 60 – 70 см қашықтықта болу керек, ал СКД барлық шарттарға қарамастан арақашықтықты 30 – 50 см қысқартуға мүмкіндік береді. Көзге түсетін жүктемені азайту үшін кескінді дұрыс бейідеу маңызды, сонымен қатар, бірінші мониторды арнайы бағдарлама арқылы тексеріп алған жөн.

Медициналық стандарттарға сәйкес, компьютерлік мониторға оңдайлы қашықтық – ең аз дегенде – бір жарымнан екі диагоналға дейін болуы керек. Есептеу үшін келесі формула қолданылады:

$$S – L * 2,54 * 1,75 \quad (5.1)$$

мұнда, L –диагональдың дюймдік ұзындығы;

2,54 – дюймді сантиметрге айналдыру коэффициенті;

1,75 – 1,5 және 2 диагоналі арасындары арифетикалық орта.

Формулаға сәйкес диагоналі 17 дюйм болатын кеңсе ноутбугынан оңтайлы қашықтықты есептесек:

$$S = 17 * 2,54 * 1,75 = 75 \text{ см} \quad (5.2)$$

Компьютерлердің әртүрлі модельдері бойынша есептеулердің нәтижелері 5.1 – кестеде келтірілген.

Кесте 5.1 – Диагоналдың өлшемі

Диагоналдың өлшемі, дюйм	Экраннан көзге дейінгі оңтайлы қашықтық, см
14	62
15	67
16	71
17	75
18	80
19	85
20	89
21	94
22	98
23	102
24	107
25	111
26	116
27	120
28	125
29	129
30	134
31	138
32	142
33	147

Студенттер мен оқушылардың, операторлардың, қызметкерлердің еңбекгін қорғау мақсатында олардың монитор алдындағы жұмыс орнын SanPiN 2.2.2.542 – 96 және SanPiN 2.4.2.1178 – 02 санитарлық нормалары және ережелеріне сай жабдықталуы керек. Бұл мәселеге құзіретті көзқарас визуалды шаршау мен басқа да аурулардың алдын алуға көмектеседі.

5.2.1 Бақылау жүйесі үшін мониторларды орналастыру

Қазіргі кезде кәсіпорындардың, мекемелердің немесе дүкендердің қорғалуы мен басқаруы бейнебақылау арқылы жүзеге асырылуда.

Тағы бір маңызды ерекшелігі – бір дисплейдің бірнеше камераларда жұмысы болып табылады, яғни, камералардың әрқайсысы белгілі бір аймақта орналасқан және әрбіреуі өз бейнесін көрсетеді (бейне өрісі). Дисплейді тиімді бақылау үшін 20 – 24 өріс болғаны жөн деп саналады.

Қажетті санына қарай бейнеқұрылғының диагоналын есептейді, шыққан мәнге сүйене отырып экранның бақылаушы көзіне дейінгі арақашықтықты есептейді. Барлық үш параметрдің дұрыс коэффициенттері 5.2 – кестеде келтірлген.

Кесте 5.2 – Диагональ ұзындығы дюймммен есебі

Өріс саны	Диагональ ұзындығы, дюйм (см)	Бақылаушы мен дисплей арасындағы қашықтық, м
4	Минималды – 17 (43)	1,7
9	19 – дан 22 – ге дейін (50 – 56)	2,0
16	19 – дан 40 – қа дейін (50 – 102)	2,0 – 3,0
20	Ең аз 32(81)	2,5

5.2.2 Компьютер аудиториясында мониторларды орналастыру ережесі

Аудиторияны жоспарлау кезінде копмьютерлік аудиторияның ішіндегі жұмыс орындарын шектеуді ұсынатын санитарлық норманың SanPiN 2.2.2.542-96 SanPiN 2.4.2.1178-02 пунктілері ескерілуі тиіс. Бір қолданушыға арналған алаң 2,5 – тен 3,5 – $м^2$ – ге дейін болуы керек. Бір компьютер үшін рұқсат етілген ең аз аймақ 6 $м^2$ жетеді.

Аудиторядағы жұмыс орындары үш жолмен ұйымдастырылады:

- қатар түрінде – қолданушылар бір – бірінің артында отырады, барлық дисплейлер бір бағытта бұрылады;
- кеңсенің ортасында компьютері бар үстелдердің екі қатары аудиторияның ортасыда бос орынсыз орналасады, ал компьютерлердің экрандары бір – біріне теріс бағытта айналдырылады;
- периметр бойынша – компьютері бар үстелдер қабырға бойымен орналастырылады.

Жұмыс орнын жабдықтау кезінде пайдаланушы көзінен монитор экраны кемінде 50 – 70 см қашықтықта болуы керек. Пайдаланушының үстелде дұрыс отырғаны жөн. Сонымен қатар, келесі ескертулердің де назарсыз қалмағаны дұрыс:

- дисплей жазықтығы тігінен орналасса, оның орталығы (немесе 2/3 биіктігіндегі нүктесі) көздің деңгейінде орналасу керек;
- көздің экранға 90 ˚ бұрышпен түскені жөн(перпендикулярдан 5 – 10˚ ауытқу рұқсат етіледі);
- бас аздап алға қарай қарағаны дұрыс – максималды 15˚.

Бұл шарттар үшін 5.3 – кестені қолданған дұрыс.

Кесте 5.3 – Үстел бетінің еденнен қашықтығы

Қолданушының бойы, см	Үстел бетінің еденнен қашықтығы,см	Орындықтың еденнен қашықтығы, см	Орындық тереңдігі, см
100 – 115	46	26	26
115 – 130	52	30	29

5.3-кестенің жалғасы

130 – 145	58	34	33
145 – 160	64	38	36
160 – 175	70	42	38
175 – тен көп	76	46	40

Жоғарыдағы ережелерге сүйене отырып, қолданушы өзіне сәйкестендіріп монитордың орналасу орнын жабдықтай алады. Келтірілген ережелерді сақтау омыртқаның тіктігіне және көз саулығына көп септігін тигізеді.

Қорытынды

SIEM жүйелерінің маңызды артықшылығы, ақпараттық қауіпсіздік оқиғаларын ескерту және ақпаратты нақты уақыт режимінде талдау, жүйенің дерекқорынан алынған дәлелдер құқық бұзушымен ішкі сынақтарға ғана емес, сотта да дәлел ретінде жарамды болып табылады.

Қорытындылай келе, SIEM класстық жүйесін енгізу - бұл өте қымбат оқиға, ол үлкен ұйым үшін ыңғайлы және кәсіпорынның жұмыс істеуі үшін кем дегенде бір білікті қызметкер оқиғаларды жинаудың үздіксіздігін бақылауды қамтамасыз ете алады, корреляция ережелерін басқарады, оларды ұйымның ақпараттық құрылымындағы жаңа қауіптердің немесе өзгерістердің пайда болуы. Кәсіпорын үшін дұрыс басқару болмаса, экономикалық дағдарыс жағдайында рұқсат етілмейтін ақпараттық қауіпсіздікті жүзеге асыруға көмек емес, ақша жұмсау болады. Ресейдегі SIEM класстық жүйелер нарығы өте кең және тапсырыс берушіге оңтайлы түрде қажетті функциялар жиынтығын таңдауға мүмкіндік береді. SIEM жүйелерінің дамуы үшін үлкен әлеует бар екені сөзсіз, себебі кәсіпорынның қауіпсіздігі туралы ақпарат үнемі өсіп келеді және оларды анықтау үшін бізге жақсартылған көмекші - SIEM қажет.

Қысқартулар тізімі

SIEM (Security information and event management) – ақпараттық қауіпсіздік қақтығыстарды басқару жүйесі

IDS (Intrusion Detection System) – интриграцияны анықтау жүйесі

IPS (Intrusion Prevention System) – интрузияны болдырмау жүйесі

DLP (Data Loss Prevention) – ақпараттың жоғалуын алдын алу

SOC (Security Orgnization Center) – қауіпсіздік операциялары орталығы

NOC (Network Organiztion Center) – желілерді басқару орталығы

Әдебиеттер тізімі

1 Миллер Р.Д, Хэррис Ш., Харпер А.А. Security Information And Event Management (Siem) Implementation. -Нью-Йорк: Network Pro Library, 2011. - 465 с

2 Щеглов А.Ю., Щеглов К.А. Анализ и построение защиты информационных систем. Контроль доступа к компьютерным ресурсам. Методы, модели, технические решения. -СПб.: Издательство Профессиональная Литература, 2017. - 416 с

3 В. Бондарев. Введение в информационную безопасность автоматизированных систем. -М.: Издательство МГТУ им.Н. Э. Баума, 2016. - 46 с

4 Громов В.И., Васильев Г.А. Энциклопедия безопасности-3 (с изменениями и дополнениями). -М.: Академия, 2000

5 SIEM жүйелерін жобалау кезеңдері, жүйе компоненттері туралы ақпарат. URL: https://stackify.com/siem-implementation-strategy-and-plan/ (кіру уақыты 15.05.19)

6 Маньков В.Д. Обеспечение безопасности при работе с ПЭВМ. -СПб.:: Политехника, 2004. - 277 с

7 Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: учебник для бакалавриата и магистратуры: -М.: Издательство Юрайт, 2017. - 309 с

8 А. Бабаш, Е. Баранова, Д. Ларин. Информационная безопасность. История защиты информации в России. -М.: Издательский Центр РИОР, 2015. - 283 с

9 FortiSIEM шешімі туралы толық ақпрат. URL: www.fortinet.com (кіру уақыты 21.04.19)

10 В. Бондарев. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства. -М.: МГТУ им. Н. Э. Баумана, 2017, 228 с.