ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

Подсекция 1.7 Инфокоммуникациялық технологиялар мен электрониканың заманауи мәселелері

УДК 381.515.2

SIEM ЖҮЙЕСІ – АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚЫЗМЕТІНІҢ СЕНІМДІ ҚҰРАЛЫ

Ануарбек Аружан Асылбекқызы
Студент кафедры «Радиотехника, электроника и телекоммуникация»
ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Ғылыми жетекші – Наурызбаев .А.Е

Ақпараттық және телекоммуникациялық технологияларды қарқынды дамыту және енгізу жағдайында әлемнің жетекші мемлекеттері ірі гидротехникалық құрылыстарды, атом электр станцияларының желілерін, зиянды химиялық өндірістерді, көлік тораптарын, әуежайларды қамтитын аса маңызды объектілердің қауіпсіздігін қамтамасыз ету мәселелеріне ерекше назар аударады. Мұндай объектілердің істен шығуы ауыр және тіпті апатты салдарға әкелуі мүмкін. Маңызды объектілердің жиынтығы маңызды инфрақұрылым тұжырымдамасының мазмұнын құрайды.

Өнеркәсіп, ірі корпоративті орта және т.б. орталарда желі қауіпсіздігіне төнетін қатерлерді мониторингілеу жүйесін құрумен байланысты, оның негізгі мақсаты осы объектілерге әсер ету тәуекелінің ең төменгі деңгейіне дейін түсіру және туындайтын залалды барынша азайту болып табылады.

Маңызды аумақтарды қорғау міндеттерінің сипаты мен мазмұнын ескере отырып, SIEM жүйесінің тұжырымдамасын мониторинг жүйесін құрудың негізіне қою орынды болады. SIEM ақпараттық және қауіпсіздік оқиғаларын басқаруды (Security Information and Event Management) білдіретін қауіпсіздік жүйесін құру мен жұмыс істеудің негізгі мақсатын қалыптастырады. Нақты уақыт режимінде қауіпсіздік туралы ақпаратты талдау және қауіпсіздік оқиғаларын проактивті басқаруды жүзеге асыру мүмкіндігін қамтамасыз ету есебінен ақпараттық– телекоммуникациялық инфрақұрылымдағы ақпараттық қауіпсіздік деңгейін айтарлықтай арттыру жүйенің маңызды аспектісі болып табылады. Қауіпсіздік оқиғаларын белсенді басқару талданатын желілік оқиғалардың барлық ақпарат көздерін пайдаланатын автоматты механизмдерге, сондай– ақ оқиғаларды бақылау параметрлерін қорғалатын жүйенің ағымдағы күйіне автоматты түрде реттеуге негізделген.

Осы мақсатқа қол жеткізу үшін SIEM– жүйесі келесі міндеттер кешенін табысты шешу мүмкіндігіне ие болуы тиіс:

- жүйеге көптеген гетерогенді көздерден келетін қауіпсіздік оқиғаларын жинау, өңдеу және талдау;
- нақты уақыттағы шабуылдар мен қауіпсіздік критерийлері нормасын бұзушылықтарды анықтау;
- ақпараттық, телекоммуникациялық және басқа да маңызды ресурстардың қорғалуын жедел бағалау;
- желі қауіпсіздігінің тәуекелдерін талдау және басқару;
- инциденттерге тергеу жүргізу;
- маңызды ресурстар мен бизнес–процестердің ішкі қауіпсіздік саясатымен алшақтығын анықтау және оларды бір– біріне сәйкестендіру;
- ақпаратты қорғау бойынша тиімді шешімдер қабылдау;
- есеп беру құжаттарын қалыптастыру.

Аталған мәселелерді шешу үшін SIEM жүйесі пайдаланатын негізгі бастапқы деректер, қауіпсіздік оқиғаларын, жазатын әртүрлі журнал жазбалары (logs) болып

табылады. Бұл оқиғалар қауіпсіздікке әсер етуі мүмкін пайдаланушылар мен бағдарламалардың әрекеттерін көрсетеді. Қауіпсіздік оқиғаларының жалпы жиынтығынан SIEM жүйесі желідегі шабуылдарды немесе басқа да жағымсыз әрекеттерді көрсетуі керек.

Сурет 1 – SIEM жүйесінің архитектурасы

Деректер сақтау қорында жиналған ақпарат көздері деректерді талдау модельдерінің сұранысы бойынша беріледі. Үшінші деңгейде алынған SIEM– жүйеде ақпаратты өңдеу нәтижелері алдын ала анықталған және еркін нысандағы есептер, оқиғалар туралы деректердің жедел (on– line) корреляциясы, сондай– ақ on– line режимінде әзірленетін және электрондық пошта арқылы берілетін ескертулер болып табылады.

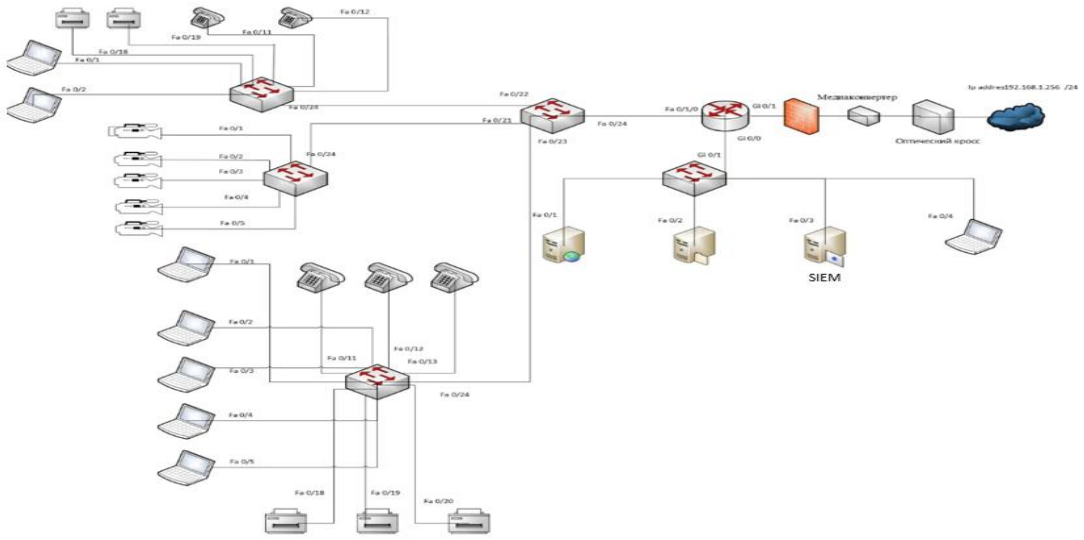
SIEM жүйесі SIM (Security Information Management) және SEM (security Event Management) ақпараттық қауіпсіздікті бақылау және басқару жүйелеріне жататын басқа екі жүйе класының функцияларын біріктіреді. Осы себепті SIEM жүйесі SIM және SEM жүйелеріне тән функцияларды орындайды. SIM жүйесінің функциялар тобына журнал жазбаларын жинау, сақтау және талдау, сондай– ақ қажетті есептілікті қалыптастыру кіреді. SEM жүйесінің функциялар тобына нақты уақыттағы қауіпсіздік оқиғаларын бақылау, оқиғаларды анықтау және оларға жауап беру кіреді. Жоғарыда аталған функцияларды SIEM жүйесінде іске асыру әртүрлі жұмыс механизмдерінің кешенін орындау негізінде жүзеге асырылады. Бірінші буын SIEM жүйелерінде мұндай механизмдердің қатарына әдетте қалыпқа келтіру, сүзу, жіктеу, агрегация, корреляция және оқиғаларға басымдық беру, есептер мен ескертулерді генерациялау жатады. Жаңа буын SIEM жүйелерінде оларға оқиғаларды және олардың салдарын талдау, шешім қабылдау және визуализация қосу керек. Көрсетілген механизмдердің SIEM жүйесіндегі иерархиясының деңгейлері бойынша таралуы 2– суретте көрсетілген.

Сурет 2 – SIEM жүйесінің иерархиялық моделі

SIEM жүйесінің архитектурасына тоқталсақ, ол "агенттер" — "деректер қоймасы" — "қолданбалар сервері" компонентінен тұрады. Агенттер қауіпсіздік оқиғаларын жинауды, оларды бастапқы өңдеуді және сүзуді жүзеге асырады. Қауіпсіздік оқиғалары туралы жиналған және сүзілген ақпарат деректер қоймасына немесе репозиторийге түседі, онда ол қолданба серверін кейінірек пайдалану және талдау мақсатында ішкі көрініс пішінінде сақталады. Қолданба сервері ақпаратты қорғаудың негізгі функцияларын жүзеге асырады. Ол репозиторийде сақталған ақпаратты талдайды және оны ескертулер немесе ақпаратты қорғау бойынша басқару шешімдерін әзірлеу үшін түрлендіреді. Осылайша, SIEM жүйесінде оның құрылысының 2– суретте көрсетілген келесі үш архитектуралық деңгейін ажыратуға болады: (1) деректерді жинау; (2) деректерді басқару; (3) деректерді талдау. Бірінші деңгейде деректерді жинау әр түрлі көздерден жүзеге асырылады. Оларға мыналар: файлдық серверлер, дерекқор серверлері, Windows серверлері, брандмауэрлер, жұмыс станциялары, шабуылға қарсы жүйелер (IPS, intrusion prevention systems), антивирустық бағдарламалар жатады.

Ірі кәсіпорындардың технологиялық жүйелері үнемі шабуылдарға ұшырайды. Шабуылдаушыларға тән антивирустық жүйелерді айналып өту модульдері бар ботнеттер мен зиянды бағдарламаларды пайдалануға болады.

Қазіргі заманғы жүйелер үшін көптеген коннекторлар жазылғанына қарамастан, кәсіпорындар әртүрлі "өздігінен жазылған" қосымшаларды қолдана алады әрі оларды бақылау қажет. Талдау ережелерінде журнал пішімі мен деректер өрістерінің мақсатын орнату арқылы біз бұл деректерді SIEM жүйесінде пайдалана аламыз. Siem жүйесінің өндірісінің негізгі көрсеткіштерінің бірі– уақыт бірлігінде өңделетін оқиғалардың саны (мысалы, журнал файлдарындағы жолдар). Жүйелердің саны неғұрлым көп болса, соғұрлым бұл көрсеткіш соғұрлым жоғары болады және, тиісінше, осы ақпаратты өңдеу және сақтау бөлігінде SIEM жүйесіне қойылатын талаптар аса маңызды. Аумақтық бөлінген компаниялар үшін жүйені масштабтау мәселесі өте маңызды, өйткені деректер көздері қашықтағы алаңдарда болуы және "тар" байланыс құралдарын пайдалануы мүмкін. Бұл жағдайда "алдын– ала өңдеу" модульдері қолданылады, олар қашықтағы жерлерде дамиды, ақпаратты алып, оны оңтайландырылған түрде жинақтау серверіне жібереді. Өңдеуден кейін ақпарат операторға қол жетімді болады, ол оны инциденттерді тергеу, ат жүйелерінің жұмысын статистикалық талдау немесе аудит үшін қолдана алады.



Сурет 3 – Корпоративтік желіге SIEM жүйесін орнату сұлбасы

Қорытындылай келе, кез келген кәсіпорын аумағында ақпараттық қауіпсіздік жүйесін SIEM негізінде қалыптастыру жұмысын жүргізу тиімді. Ақпараттар көзіне сүйеніп, SIEM

жүйесінің архитектурасы, оның тиімді қолданыстағы жақтары, негізгі сипаттамалары қарастырылды. Соның негізінде ақпараттық қауіпсіздік оқиғаларын жинау және корреляциялау жүйесі жасалды. SIEM жүйесінің енгізілуінен кейін корпоративтік желінің құрылымдық схемасы қалай бейнеленетіндігі көрсетілді. Ақпараттық қауіпсіздік тәуекелдері есептелініп, олардың міндеті нақты қауіптерді түсіну, тәуекелдерді есептеу, сондай– ақ оларды азайтуға және қорғауға бағытталған шараларды таңдау екендігіне көз жеткізілді. Осылардан шығатын негізге ой – SIEM жүйесі зерттеулердің жаңа бағыттарын айқындайтын өзекті ғылыми міндет болып табылатындығын көрсетеді.

Пайдаланылған әдебиеттер:

1. Канев А.Н. Мониторинг событий и обнаружение инцидентов безопасности с использованием SIEM – систем. Международный студенческий научный вестник. – 2015. – № 3;
2. Дмитрий Хамакев «SIEM: ответы на часто задаваемые вопросы», https://habrahabr.ru/post/172389/
3. Максим Гарусев. «Системы корреляции событий: революция или эволюция?», http://www.setevoi.ru/cgi– bin/text.pl/magazines/2003/7/30
4. Артем Медведев «самый безопасный SOC», http://www.jetinfo.ru/stati/samyj– bezopasnyj– soc

УДК 004.056.53

ОБЗОР СУЩЕСТВУЮЩИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Булкаиров Т.Т[1]., Оспанова С.Т[2]
[1]Л.Н.Гумилев атындағы Еуразия ұлттық университеті, «Радиотехника, электроника және телекоммуникациялар» кафедрасының магистранты, Астана, Қазақстан
[2]Л.Н.Гумилев атындағы Еуразия ұлттық университеті, «Радиотехника, электроника және телекоммуникациялар» кафедрасының лаборанты, Астана, Қазақстан
Научный руководитель – Казиева Н.М.
bulkairov.t@mail.ru

Аннотация: В статье рассматриваются методы защиты информации в телекоммуникационной сети. Проанализированы методы информационной безопасности которые используются для защиты информации в сети. Рассмотрены характеристики методов защиты информации.

Сегодня, когда телекоммуникационная сеть используются для приема и передачи электронной информации. Применение информационных технологий для приема и передачи электронной информации является фактором развития экономики и улучшения функционирование общественных и государственных учреждений, которые необходимо защитить от новых информационных угроз. В целом одним из основных направлений информационной безопасности является прогнозирование, обнаружение и оценка информационных угроз. Также надо отметить то, что применение больших данных привнесло больше науки, удобства и практичности в труде и жизнь людей. Популярность больших данных также делает телекоммуникационные сети объектами для серьезных угроз безопасности. Открытость самой сети позволяет любому пользователю войти в сеть, чтобы просматривать и запрашивать информацию, которая создает большую угрозу информационной безопасности сети. В связи с вышеизложенным существует необходимость более детально рассмотреть методы защиты информации в телекоммуникационной сети. В рамках статьи был произведен обзор статье по этому направлению.