ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

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 имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

Инциденттерге жауап беруді автоматтандыру: Siem жүйелер қауіп-қатерге жауап берудің автоматтандырылған құралдарын барған сайын біріктіреді, бұл инциденттерге жауап беру уақытын қысқартады және әкімшілерге жүктемені азайтады.

Жақсартылған деректерді басқару және сақтау: деректерді ұзақ және дәл аналитикалық сақтауға мүмкіндік беретін Siem жүйелерінде деректерді тиімдірек сақтау және басқару технологиялары дамуда.

Қызметкерлерді оқыту және жаңарту: талдаушылар мен әкімшілерді Siem жүйелерін және талдаудың соңғы әдістерін пайдалану бойынша үздіксіз оқыту қауіпсіздік тиімділігін қамтамасыз етудің маңызды тренді болып табылады.SIEM жүйелерін дамытудағы трендтер ұйымдарға ақпараттық қауіпсіздіктің жоғары деңгейін сақтауға мүмкіндік беретін заманауи киберқауіптерді анықтау және оларға жауап беру қабілетін жақсартуға бағытталған.

Қорытынды

IBM QRadar SIEM-ең тиімді аналитикалық қауіпсіздік жүйелерінің бірі. Ең бастысы, шешім жетекші өндірушілердің 200-ден астам өнімімен жұмыс істеуді қолдайды және желілік шешімдер, қауіпсіздік құралдары, серверлер, хосттар, операциялық жүйелер мен қосымшаларды қоса алғанда, көптеген жүйелер арқылы деректерді жинауды, талдауды және корреляцияны жүзеге асырады. Сонымен қатар, шешімнің қосымша артықшылығы бастапқы деңгейдегі жүйенің төмен құны.

Пайдаланылған әдебиеттер тізімі

1. "Practical Machine Learning for Computer Security" by Dahua Xie and Xiaodong Lin (2019).

2. "A Systematic Literature Review on Machine Learning for Cyber Threat Intelligence" by Egehan Gökdemir, Emre Erturk, and Ali Doğanaksoy (2021).

3. "Threat Intelligence: A Comprehensive Survey" by Mohamed Ahmed Abdelraheem and Hossam El-Din Mostafa (2020).

4. David R. Miller. "Security Information and Event Management (SIEM) Implementation" (2010y). http://www.infobezpeka.com/publications/SIEM_osobennosti_siem/

5. Sam R. Alapati. "SIEM and Splunk Fundamentals" (2018y) .

6. Anton Chuvakin and Kevin Schmidt. "Log Management and Log Analysis: Security Information and Event Management". ((December 13, 2012 y).

7. "SIEM and Log Management: Operational Intelligence for Security" by David Miller, Shon Harris, and Allen Harper (2010 y).

8. "Security Information and Event Management (SIEM) – A Complete Guide" by Gerardus Blokdyk (2017y). https://softlist.com.ua/articles/chto-takoe-siem-sistema

ОӘК 004.056

SIEM ЖҮЙЕСІ ЗАМАНАУИ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ НЕГІЗГІ ҚҰРАЛЫ.

Атабек Қ.Ә., Абдураимова Б.К.

Қазақстан, Астана қаласы, Л.Н.Гумилев атындағы Еуразия Ұлттық Университеті

Аңдатпа

Бұл мақалада ақпараттық қауіпсіздік саласындағы өзекті мәселелер қарастырылады, мысалы, деректерді қорғау құралдарының тиімділігі және ықтимал қауіптерге жедел жауап беру. Ол оқиғаларға жауап беру уақытын қысқарту үшін қауіпсіздік бұзушылықтарын тіркеу процестерін автоматтандыру қажеттілігіне назар аударады. Кәсіпорындардың қауіпсіздігін қамтамасыз етудегі деректердің бұзылуын болдырмау жүйелерінің (DLP) және ақпараттық қауіпсіздік пен оқиғаларды басқару жүйелерінің (SIEM) рөлі сипатталған. Деректердің бұзылуындағы адам факторына және қызметкерлердің жеке саласының ықтимал бұзылуына қатысты мәселелерге ерекше назар аударылады. Жаңа технологиялардың қарқынды даму

дәуірінде ақпарат ең құнды активке ғана емес, сонымен қатар күнделікті өмірдің ажырамас бөлігіне айналады. Әрбір компанияның өзінің ерекше құпия ақпараты бар, оның таралуы қатаң бақылауда. Мұндай деректерді қорғау қауіпсіздіктің ажырамас шарасына айналады, оны барлық компаниялар қатаң сақтауы керек.

Кілт сөздер:

Ақпараттық қауіпсіздік, ақпаратты қорғау жүйелері, SIEM, машиналық оқыту, оқиғалардың корреляциясы, кибершабуылдар, GDPR, NIST

Ақпарат өмірдің ажырамас бөлігі болып табылатын және киберқауіптер сипатын үнемі өзгертіп отыратын қазіргі әлемде ақпараттық қауіпсіздікті қамтамасыз ету барған сайын қиындай түсуде. Бұл мақалада біз SIEM (Security Information and Event Management) жүйелерінің Компанияның құпия деректері мен активтерін қорғаудың негізгі құралы ретіндегі рөлін қарастырамыз.

Ақпаратты қорғау құралдары пайда болған сәттен бастап үнемі жетілдіріліп отырады. Алайда, бірқатар маңызды сұрақтар туындайды:

- Олардың тиімділігі мен үнемі өзгеріп отыратын киберқауіптерге қарсы тұру қабілетіне қалай кепілдік беруге болады?
- Ықтимал оқиғаларға қалай жедел әрекет ету керек?

Бұл сұрақтарға жауап беру үшін қауіпсіздік оқиғаларын тіркеу және талдау процестерін автоматтандыру қажет. SIEM (Security Information and Event Management) жүйелері автоматтандыру және тіркеу процестеріне жауап береді.

SIEM жүйесінің негізгі функционалдығы:

- Серверлерді, жұмыс станцияларын, желілік жабдықты, бұлттық қызметтерді, қолданбаларды қоса алғанда, әртүрлі құрылғылардан, жүйелерден және қолданбалардан қауіпсіздік журналдарын жинау және біріктіру.
- Оқиғаларды қалыпқа келтіру және санаттау, оларды табу мен талдауды жеңілдетеді.
- Өзара байланысты оқиғаларға негізделген күрделі қауіптерді анықтау үшін әртүрлі көздерден алынған оқиғалардың корреляциясы.
- Кибершабуылға байланысты күдікті әрекеттерді анықтау үшін машиналық оқытуды қолдану арқылы ауытқуларды анықтау.
- АТ мамандарына оқиғаларға жедел жауап беруге мүмкіндік беретін күдікті әрекеттер туралы ескертулер жасау.

Уақыт	Оқиға	Қауіп деңгейі
08:00 - 08:15	Кіру әрекеті	Орташа
08:20 - 08:35	Сәтсіз аутентификация	Төмен
09:00 - 09:10	Сәтті аутентификация	Төмен
09:30 - 09:45	Ерекше жоғары трафик	Жоғары
10:00 - 10:15	Зиянды бағдарламаны анықтау	Жоғары
10:30 - 10:45	Файлдарға әдеттен тыс қол жетімділік	Орташа

Кесте 1: Siem жүйесі арқылы талдау үшін пайдаланылуы мүмкін деректердің мысалы

SIEM барлық киберқауіптер үшін панацея емес.SIEM тиімді жұмыс істеуі үшін білікті қызметкерлер қажет. Алайда, артықшылықтары осы қиындықтардан бірнеше рет асып түседі. Қазіргі әлемдегі ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етудің таптырмас құралы.

SIEM-ден басқа, ақпараттық қауіпсіздікті қамтамасыз етуде маңызды рөл атқаратын басқа жүйелер бар:

- **DLP (Data Loss Prevention) жүйелері:** құпия деректердің ағып кетуіне жол бермеуге арналған.
- **Smart (Securitychchestration, Automation and Response) жүйелері:** оқиғаларға жауап беруге байланысты күнделікті тапсырмаларды автоматтандыру.
- **EDR (Endpoint Detection and Response) жүйелері**: соңғы құрылғыларды кибершабуылдардан қорғауды қамтамасыз етеді.

Бұл жүйелерді біріктірп пайдалану ақпараттық қауіпсіздікке кешенді көзқарас құруға сонымен қатар ақпараттық активтерін қорғау деңгейін айтарлықтай арттыруға мүмкіндік береді.

Бұрын қауіпсіздік мамандары көптеген журналдарды қолмен қарап, аномалияларды іздеуге қымбат уақыт жұмсауға мәжбүр болды. SIEM бұл процесті автоматтандырады, мамандарды маңызды мәселелерді шешуге босатады. Жоғарыда көрсетілген DLP жүйелері (Data Loss Prevention) – деректердің бұзылуына қарсы күресте біздің сенімді көмекшілеріміз. Олар құпия ақпараттың пошта, USB медиасы немесе басқа арналар арқылы компанияның шегінен шықпауын қамтамасыз етеді. SIEM, тәжірибелі детектив сияқты, әртүрлі көздерден алынған оқиғаларды салыстырады, күрделі ұрлау схемаларын анықтайды.

Мысалы: SIEM бухгалтерлік есеп жүйесіне кіру әрекеттерінің қалыптан тыс санын тіркеді. Сонымен қатар, DLP жүйесі үлкен файлды электрондық пошта арқылы жіберу әрекетін атап өтті. Осы оқиғаларды салыстыра отырып, мамандар бірден ұрлау әрекеті болуы мүмкін екенін түсінеді.

Адам факторы:

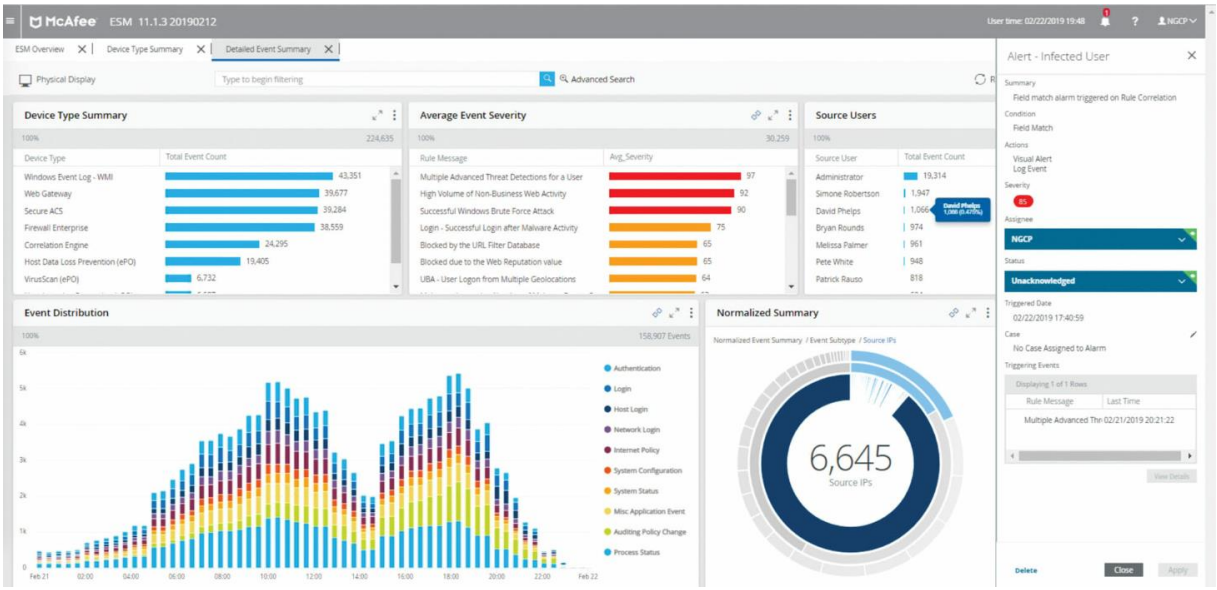
Барлық техникалық қорғаныс шараларына қарамастан, адам факторы ақпараттың негізгі көздерінің бірі болып қала береді. Қызметкерлер кездейсоқ немесе әдейі құпия деректерді, мысалы, дұрыс емес мекен-жайға электрондық пошта арқылы жіберу арқылы немесе шабуылдаушы әлеуметтік инженерия әдістерін қолдана отырып, құпия ақпаратқа қол жеткізе алады. Қызметкер маңызды қауіпсіздік журналының файлын кездейсоқ жойып жіберуі мүмкін. Қызметкер кездейсоқ маңызды серверді өшіруі мүмкін.

Оқиға түрі	**Сипаттама**	**Себебі**
Құпия ақпараттың ағуы	Қызметкер кездейсоқ құпия құжатты дұрыс емес мекен-жайға электрондық пошта арқылы жіберді.	Байқаусызда қате
Қауіпсіздік жүйелерінің жұмысын бұзу	Қызметкер маңызды қауіпсіздік журналының файлын кездейсоқ жойды.	Байқаусызда қате
Қызмет көрсетуден бас тарту	Қызметкер кездейсоқ маңызды серверді өшірді.	Байқаусызда қате
Рұқсатсыз кіру	Шабуылдаушы әлеуметтік инженерия әдістерін қолдана отырып, құпия ақпаратқа қол жеткізді.	Әдейі әрекет ету
Кибершабуыл	Шабуылдаушы Компанияның веб-сайтын бұзу үшін DDoS шабуылын жасады.	Әдейі әрекет ету

Кесте 2: Адам факторының ақпараттық қауіпсіздікке әсер ету мысалдары

Құпия деректерге рұқсатсыз қол жеткізуді болдырмау үшін бақылау шаралары қажет. Қызметкерлердің жеке саласын бұзбай, қауіпсіздік пен этика арасындағы тепе-теңдікті сақтау маңызды.

McAfee Enterprise Security Manager мысалын қарастырайық, ол қауіптерді кеңейтілген анықтауға, сәйкестікке қатысты әрекеттерді басқаруға және нақты уақыт режимінде есептер шығаруға мүмкіндік береді. Пайдаланушы интерфейсі әртүрлі төтенше жағдайлар сценарийлерін өңдеу үшін жаңа ресурстарды пайдалануға мүмкіндік береді. McAfee Enterprise Security Manager бұлтта да, жергілікті жерде де орналастырылуы мүмкін және деректер талаптарына сәйкес масштабталуы мүмкін.



Сурет 1: Ағымдағы қорғауды бақылау мониторы

McAfee Enterprise Security Manager жұмысы әртүрлі көздерден журналдарды жинауға негізделген, бұл желілік трафиктің айтарлықтай өсуіне әкелуі мүмкін. Белгіленген кемшіліктердің бірі-жүйенің журналдарды ең маңызды элементтерге дейін қысқартуы, бұл оқиғалардың толық мәнмәтінін алу үшін журналдарды қайта жинауды қажет етуі мүмкін. McAfee-дің кейбір кемшіліктері кеңейтілген қорғаныс конфигурациясын пайдалану кезінде нашар өнімділікті, сондай-ақ жұмыс үздіксіздігіне әсер етуі мүмкін жиі жаңартуларды қамтиды. Дегенмен, бұл кемшіліктерді оңтайлы қорғаныс конфигурациясын Орнату арқылы жоюға болады.

Қорытынды

Мақалада біз SIEM жүйелерінің қазіргі әлемдегі ақпараттық қауіпсіздікті қамтамасыз етудегі рөлін қарастырдық. SIEM-бұл жай ғана құрал емес, қауіпсіздік журналдарын орталықтандырылған басқаруға, оқиғалардың корреляциясына, ауытқуларды анықтауға және реттеушілердің сәйкестігін қамтамасыз етуге негізделген кешенді қауіпсіздік философиясы.

SIEM қолданудың артықшылықтары:

- Оқиғаларға жауап беру тиімділігін арттыру.
- Деректердің бұзылу қаупін азайту.
- Талаптарға сәйкестікті қамтамасыз ету.
- Киберқауіптер туралы хабардарлықты арттыру.

Еске сала кетсек:

- SIEM барлық киберқауіптер үшін панацея емес.
- SIEM тиімді жұмыс істеуі үшін білікті қызметкерлер қажет.
- SIEM енгізу көп уақытты қажет етеді және қымбатқа түседі.

Алайда, SIEM артықшылықтары осы қиындықтардан бірнеше рет асып түседі. Қазіргі әлемдегі ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етудің таптырмас құралы.

SIEM енгізу-бұл Сіздің компанияңыздың болашағына инвестиция. Бұл сіздің құнды деректеріңіздің қауіпсіздігінен қорықпай, тыныш дамуға мүмкіндік беретін сенімді қалқан. Сандық қауіп-қатер дәуірінде қауіпсіздік пен өркендеуге арналған нұсқаулық.

Пайдалынылған әдебиеттер тізімі

1. М. Синкве, Д. Котронео және А. Пеккия, "Ақпараттық қауіпсіздік және оқиғаларды басқару саласындағы қиындықтар мен бағыттар (SIEM)", 2018 ж.

2. К. М. Ахмед, М. Р. Гаутама Раман және А. П. Матур, " Нақты уақыттағы ауытқуларды анықтау үшін машиналық оқытуға негізделген тәсілдердегі проблемаларды өнеркәсіптік басқару жүйелерінде анықтау", 2020 ж.

3. 2020-2021 жылдардағы веб-қосымшалардың осалдықтары мен қауіптері , www.ptsecurity.com – 2022. - https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/
4. Хабр. [SIEM: жиі қойылатын сұрақтарға жауаптар]. [Электрондық ресурс]. Кіру режимі: https://habrahabr.ru/post/172389
5. Securitylab. [SIEM дегеніміз не?]. [Электрондық ресурс]. Кіру режимі: http://www.securitylab.ru/analytics/430777.php

УДК 004.056.5

ИСПОЛЬЗОВАНИЕ МЕТОДОВ И ИНСТРУМЕНТОВ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ДЛЯ ВОССТАНОВЛЕНИЯ ПОТЕРЯННЫХ ДАННЫХ

Балташева Назерке Төлегенқызы
Nazerke2810@gmail.com,
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Баж Мансия Уразбайқызы
mansiya.orz@gmail.com
студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л.Н. Гумилева
Научный руководитель Аймичева Гаухар Ислямовна

В эпоху цифровизации обеспечение целостности данных является одной из актуальных задач. Зачастую необходимые файлы могут быть удалены с компьютера или USB-носителя, как случайно, так и злоумышленно. Это особенно актуально в образовательной среде, где как обучающиеся, так и преподаватели могут столкнуться с потерей важных данных. По результатам проведенного опроса среди участников академической среды 80% респондентов сталкивались с необходимостью восстановления удаленных данных (рис.1). И всего лишь около 20% смогли восстановить удаленные файлы с использованием специального инструментария (рис.2). Предположительно это студенты, изучавшие инструменты криминалистического анализа, участвовавших также в опросе. В связи с этим, рассмотрение методов и инструментов восстановления потерянных данных, рассматриваемых в данной статье, является актуальным для участников образовательной среды и других пользователей цифровых устройств.

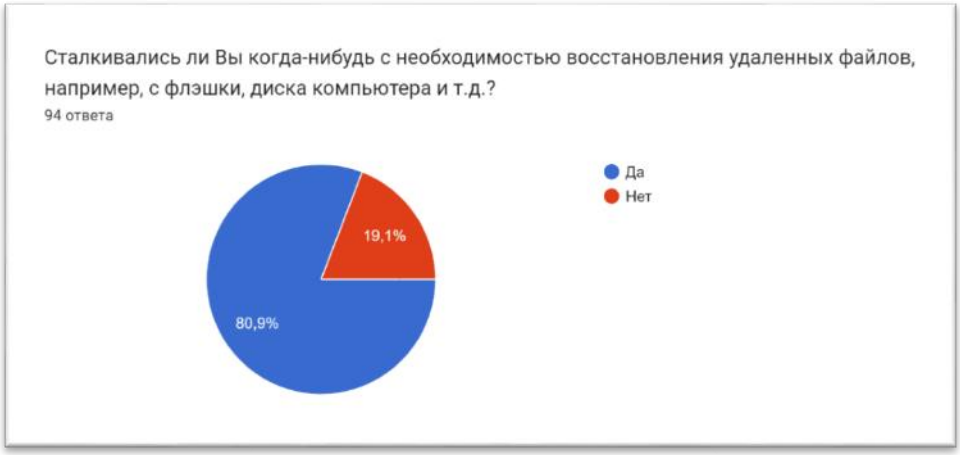


Рисунок 1. Результаты опроса 94-х респондентов на предмет выяснения факта необходимости восстановления удаленных данных