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

В эпоху цифровизации обнаружение стеганографии остаётся критически важной задачей для защиты конфиденциальной информации и предотвращения несанкционированного доступа к данным. Прогресс в разработке и применении методов стеганализа не только укрепит информационную безопасность, но и способствует развитию более безопасного и надёжного цифрового пространства.

Список использованных источников

1. Фридрих, Й. "Steganography in Digital Media: Principles, Algorithms, and Applications". – Кембридж: Издательство Кембриджского университета, 2009, 364 с.

2. Кокс, И. Дж., Миллер, М. Л., Блум, Дж. А., Фридрих, Й., Калкер, Т. "Digital Watermarking and Steganography". – Берлингтон: Морган Кауфманн, 2007, 624 с.

3. Провос, Н., Ханиман, П. "Hide and Seek: An Introduction to Steganography" // IEEE Журнал о безопасности и конфиденциальности, Т. 1, №3, 2003, С. 32-44.

4. Кер, А. Д. "A Review of Steganalysis Techniques: From Image to Audio" // Журнал математического изображения и зрения, Т. 26, №1, 2007, С. 83-102.

5. Бёме, Р., Кирхнер, М. "Counter-Forensics: Attacking Image Forensics" // В книге "Digital Image Forensics". Нью-Йорк, Нью-Йорк: Спрингер, 2015, С. 327-366.

ЖЕЛІДЕГІ ИНЦИДИЕНТТЕРДІ АНЫҚТАУ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕРДЕГІ БАҚЫЛАУДЫҢ ТИІМДІ АЛГОРИТМДЕРІНЕ ШОЛУ

Асатай Мардан Кунанбайұлы
mardan.asatay@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасы магистранты , Астана, Қазақстан
Ғылыми жетекші – Ташенова Ж.М.

Аннотация: Бақылау жүйелері өзгерістерге жедел жауап беруге, ауытқуларды анықтауға және жүйенің жұмысын жақсартуға мүмкіндік беретін деректерді үнемі бақылау мен талдауға мүмкіндік береді. Бақылау жүйелерінің маңызды құрамдас бөліктері сенсорлар, деректер жинаушылар, талдау алгоритмдері және есептер болып табылады. Бұл мақалада SIEM технологиясының маңызды аспектілері, киберқауіпсіздіктегі және оның құрамдас бөліктеріндегі рөлдер қарастырылады, қазіргі ақпараттық технологиялар әлеміндегі SIEM жүйесінің негізгі рөлі талқыланады, сонымен қатар Siem жүйесінің негізгі компоненттері, соның ішінде деректерді жинау, корреляция жүйелері, бақылау тақталары мен есептер қарастырылады. SIEM жүйелері қауіпсіздік стратегиясының бөлігі болып табылады және ұйымдарға цифрлық ортадағы қауіптерге тиімді қарсы тұруға мүмкіндік береді.

Кілт сөздер: ақпараттық қауіпсіздік, SIEM, IBM, QRadar, желілік қауіпсіздік.

Кіріспе: Қазіргі киберқылмыскерлер компаниялардың қорғаныс жүйелеріне шабуыл жасағанда барған сайын жетілдірілген әдістерді қолданады. Оларға қарсы тұру үшін ақпараттық қауіпсіздік департаменттері күніне көптеген оқиғаларды талдауға және түсіндіруге мәжбүр. IBM желілік қауіпсіздік қатерлерінен қорғау үшін IBM QRadar Security Intelligence Platform шешімін ұсынады, ол қауіпсіздік туралы ақпаратты және оқиғаларды басқаруды (SIEM) және журналдарды біріктіру, қалыптан тыс жағдайларды анықтау, оқиғаларды талдау, оларға жауап беру, параметрлерді басқару және осалдықтарды жою үшін бірыңғай архитектураны ұсынады.

QRadar Security Intelligence Platform бірыңғай архитектурасы журналдарды, желілік ағындарды, пакеттерді, осалдықтарды, сондай-ақ пайдаланушылар мен ресурстар туралы деректерді талдауға мүмкіндік береді. Sense Analytics-ті қолдану нақты уақыттағы ең үлкен қауіптерді, шабуылдарды және осалдықтарды анықтау үшін корреляциялық талдау жүргізуге мүмкіндік береді. Бұл бөлімдерге үлкен деректер ағынынан ең маңызды оқиғаларға басымдық беруге және бөлуге мүмкіндік береді. Шешім оқиғаларға автоматты түрде жауап береді және

деректерді жинау, олардың корреляциясын анықтау және есеп беру мүмкіндіктері арқылы реттеуші талаптарды орындайды.

IBM QRadar Security Intelligence Platform бірқатар әртүрлі модульдерді қамтиды. Шешімнің негізгі компоненттерінің бірі – IBM QRadar SIEM құралы-оқиғаларды жинау және талдау жүйесі. Ол желідегі құрылғылардан, соңғы нүктелерден және қолданбалардан келетін оқиғалар журналдарынан ақпаратты біріктіреді. QRadar SIEM қауіпсіздік қатерлерін анықтау үшін корреляцияны қалыпқа келтіреді және талдайды және қалыпты мінез-құлықты анықтау, ауытқуларды анықтау, озық қауіптерді ашу және жалған оң нәтижелерді жою үшін sense Analytics озық механизмін пайдаланады. Бұл бағдарламалық модуль барлық байланысты оқиғаларды бір оқиғаға жинауға мүмкіндік береді. QRadar SIEM IBM X-Force Threat Intelligence қауіп-қатерін ықтимал зиянды IP мекенжайларының, зиянды бағдарламалық жасақтама компьютерлерінің мекенжайларының, спам көздерінің және басқа қауіптердің тізімімен талдауды қамтуы мүмкін, бұл қауіпсіздікке белсенді көзқарасты енгізуге мүмкіндік береді. Сонымен қатар, басымдықтарды анықтау үшін өнім жүйелерге қауіп-қатерлерді желідегі оқиғалар мен деректермен салыстыра алады.

Пайдаланушылардың деректері мен әрекеттеріне қол жеткізу туралы егжей-тегжейлі есептер жасау мүмкіндігі қауіптерді басқаруды және стандарттарға сәйкестікті қамтамасыз етеді. Сондай-ақ, QRadar SIEM-ді жергілікті және бұлтты ортада қолдануға болатындығын атап өткен жөн.Сонымен қатар, IBM жақын арада Watson ai платформасын QRadar бағдарламалық жасақтамасымен және X-Force дерекқорымен біріктіре отырып, қауіпсіздік саласында пайдалануды жоспарлап отырғанын атап өткен жөн. Бұл қауіптердің сипатын анықтау үшін аналитика деңгейін арттыруға, сондай-ақ ақпараттық қауіпсіздік саласындағы ат персоналының жетіспеушілігін өтеуге мүмкіндік береді.

SIEM трендтері және болашағы

SIEM (ақпараттық қауіпсіздік пен оқиғаларды басқару жүйелері) жүйелерінің ағымдағы трендтері мен Даму бағыттары киберқауіптерді анықтау және оларға ден қою тиімділігін арттыруға бағытталған. Міне, SIEM дамуының ең маңызды трендтері мен бағыттары:

Жасанды интеллект және машиналық оқыту (AI/ML): жасанды интеллект пен Машиналық оқыту алгоритмдерін қолдану SIEM жүйелерінде жиі кездеседі. Бұл технологиялар қалыптан тыс әрекеттерді автоматты түрде анықтауға, қауіптерді жіктеуге және ықтимал оқиғаларды болжауға мүмкіндік береді.

Мінез-құлықты талдау(Behavior Analytics): SIEM жүйелер оқиғаларды талдаудан пайдаланушылар мен жүйелердің мінез-құлқын талдауға баса назар аударады. Бұл стандартты емес және күдікті белсенділік үлгілерін анықтауға мүмкіндік береді, бұл әсіресе ішкі қауіптерді анықтау үшін пайдалы.

Бұлтқа негізделген SIEM шешімдері: көптеген ұйымдар икемділікті арттыру және жергілікті инфрақұрылым жүктемесін азайту үшін бұлтқа негізделген SIEM шешімдеріне көшуде. Бұлтқа негізделген Siem шешімдері сонымен қатар заманауи технологиялар мен қауіпсіз деректер қоймаларына қол жеткізуге мүмкіндік береді.

DevOps интеграциясы: DevOps және контейнерлік технологияларды қолданудың артуымен, SIEM жүйелер қосымшаларды әзірлеу және пайдалану циклына енеді, бұл әзірлеу және енгізу кезеңінде қауіпсіздікті қамтамасыз етуге көмектеседі.

Деректер контекстін кеңейтілген пайдалану: SIEM жүйелер оқиғаларды дәлірек талдау және олардың маңыздылығын анықтау үшін пайдаланушы, ресурстар және орналасу ақпараты сияқты контекстік деректерді белсенді түрде пайдалануда.

Реттеулер мен стандарттарды сақтау: ақпараттық қауіпсіздік талаптарын күшейте отырып, Siem жүйелер GDPR, HIPAA және т. б. сияқты нормативтік талаптарды орындауды жеңілдетуге бағытталған.

Мамандардың қатерін талдауды күшейту (SOC): SIEM жүйелер нақты уақыттағы талдаушылар мен әкімшілердің ынтымақтастығы үшін Security Operations Center (SOC) - пен интеграциялануда.

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