ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

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 имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

doing?// Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, October 2022, Pages 6583-6594 Pages 6583-6594

3. **Cryptography KZ** // Global Information Services.– Қолжетімді: [https://cryptography.kz/ru/вам-нужен-блокчейн.html].

ӘОЖ 81.93.29

ИНЦИДЕНТТЕРДІ АНЫҚТАУДА ЖЕЛІЛІК ЛОГТАРДЫ ТАЛДАУДЫҢ МАҢЫЗДЫ РӨЛДЕРІ

Қ. Мырзағалиұлы

7М06306 "Ақпараттық қауіпсіздік жүйелері" мамандығы бойынша магистрант, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.

К.М.Сагиндыков

Ғылыми жетекшісі, т.ғ.к., доцент, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.

Мақалада киберқауіпсіздік құралы ретінде желілік логтардың маңызы қарастырылады. Олардың мүмкіндіктері кибершабуыл іздерін анықтауда, трафикті талдауда және SIEM жүйелері мен корреляция әдістерін қолдану арқылы аномалияларды анықтауда қарастырылады. Жасанды интеллектті қоса алғанда, заманауи технологиялар арқылы қолданудың практикалық аспектілеріне, шектеулерге және тиімділікті арттыру жолдарына ерекше назар аударылады. Талдау негізінде өсіп келе жатқан қауіптер жағдайында цифрлық жүйелерді қорғау үшін желілік лагтарды оңтайландыру бойынша ұсыныстар ұсынылады.

Түйін сөздер: желілік логтар, логтар корреляциясы, SIEM жүйесі, трафик, аномалия.

Цифрлық трансформация киберқауіпсіздік ландшафтын өзгертті, бұл желілерді негізгі шабуыл нысанына айналдырды. 2024 жылғы Verizon Data Breach Investigations Report мәліметтері бойынша, оқиғалардың 82% - ы желілік осалдықтарға байланысты, ал киберқылмыстың жаһандық шығыны жыл сайын 6 трлн доллардан асады (Morgan, 2024). Түйіндер арасындағы өзара әрекеттесуді тіркейтін желілік логтар қауіптерді бақылау, анықтау және тергеудің маңызды құралына айналды. Олар нақты уақыттағы талдау және оқиғаларды ретроспективті қалпына келтіру үшін деректерді ұсынады, бұл оларды кибершабуылдармен күресуде таптырмас етеді. Мақаланың мақсаты-желілік логтардың мүмкіндіктерін жан-жақты бағалау, оларды талдау әдістерін зерттеу, шектеулерді анықтау және технологиялар мен қауіптердің эволюциясы жағдайында олардың даму жолдарын ұсыну.

Желілік логтар – бұл желілік құрылғылар (маршрутизаторлар, брандмауэрлер, IDS/IPS) және трафик параметрлерін бекітетін бағдарламалық жасақтама: IP мекенжайлары, порттар, протоколдар, деректер көлемі және уақыт белгілері. Олар ішкі және сыртқы әрекеттерді бақылауға мүмкіндік беретін желілік байланыстарды қамту арқылы жүйелік ұялардан ерекшеленеді. Журналдар құрылымдалған болуы мүмкін (мысалы, JSON форматында) немесе құрылымдалмаған (мәтіндік файлдар), бұл олардың өңделуіне әсер етеді.

Splunk, QRadar немесе ArcSight сияқты SIEM жүйелерінде желілік логтар оқиғаларды корреляциялау және шабуылдар тізбегін құру үшін қолданылады. Олардың теориялық маңыздылығы белсенділіктің "сандық іздерін" қамтамасыз етуде жатыр, бірақ практикалық құндылығы жинау, сақтау және талдау сапасымен анықталады. Мысалы, syslog стандарты біртұтастықты қамтамасыз етеді, бірақ әрдайым күрделі тергеу үшін жеткілікті мәліметтерді қамтымайды.

Желілік логтар қауіптердің кең ауқымын анықтауда тиімді. DDoS шабуылдарында олар трафиктің аномалиясын түсіреді, бұл зиян көздерін бұғаттауға мүмкіндік береді. Фишинг жағдайында DNS сұрауларының журналдары зиянды домендерге жүгінуді, ал деректер бұзылған кезде — шығатын трафиктің күдікті көлемін анықтайды. Олар сондай-ақ заңды хаттамалар арқылы деректерді туннельдеу сияқты жасырын қауіптерді талдауға көмектеседі.

Нақты мысалдар олардың маңыздылығын көрсетеді. 2020 жылғы SolarWinds шабуылы логтар арқылы командалық серверлермен шифрланған қосылыстарды анықтады, бұл оқиғаға деген реакцияны тездетді. 2017 жылғы WannaCry SMB-ді брандмауэр логтарында пайдалану әрекеттерін көрсетті, ал 2021 жылы Colonial Pipeline-ге шабуыл деректерді шифрлау алдында логтар арқылы желіні алдын ала сканерлеуді анықтады. Cobalt Strike APT тобы жағдайында логтар сирек порттардың қолданылуын тіркеді, бұл мақсатты шабуылды көрсетті.

Желілік логтар цифрлық криминалистика талдауы үшін де маңызды. Оқиғадан кейін олар хронологияны қалпына келтіруге мүмкіндік береді: кіру нүктесінен (мысалы, фишингтік хат) зиянды кодты орындауға және деректерді сүзуге дейінгі аралық. Бұл оларды зиянды бағалауға және алдын-алу шараларын жасауға негіз етеді.

Желілік логтарды өңдеу олардың көлемі мен күрделілігіне байланысты заманауи тәсілдерді қажет етеді. Дәстүрлі қолмен талдау, автоматтандыруға жол берді. SVM (Support Vector Machines) және нейрондық желілер сияқты машиналық оқыту алгоритмдері ауытқуларды 92% дәлдікпен анықтайды (Lee et al., 2022). Мысалы, кластерлеу тән емес трафик үлгілерін бөліп көрсетуі мүмкін, ал регрессиялық талдау белсенділіктің өсуін болжауы мүмкін.

Корреляциялық талдау толық суретті құру үшін әртүрлі көздерден алынған журналдарды біріктіреді. Мысалы, ICMP сұрауларымен бірге сәтсіз аутентификация желіні барлауды көрсетуі мүмкін. Elasticsearch немесе Apache Kafka сияқты платформалар терабайт деректерін нақты уақытта өңдеуге мүмкіндік беретін масштабталуды қамтамасыз етеді. Бейнелеу (графиктер, жылу карталары) талдаушыларға нәтижелерді түсіндіруге көмектеседі, бірақ құрылымдалмаған журналдарды алдын-ала қалыпқа келтіруді қажет етеді.

Дәлдікті арттыру үшін гибридті әдістер қолданылады. Мысалы, қолтаңбаны талдау (белгілі қауіптерді іздеу) және мінез-құлық (ауытқуларды анықтау) тіркесімі белгілі және нөлдік күндік шабуылдарды анықтауға мүмкіндік береді. Дегенмен, модельдерді теңшеу үлкен көлемдегі деректер мен есептеу ресурстарын қажет етеді.

Желілік логтарда айтарлықтай шектеулер бар. Сапалығы құрылғылардың конфигурациясына байланысты — негізгі оқиғаларды жазбау олардың құндылығын төмендетеді. Трафикті шифрлау (HTTPS, TLS, VPN) хабар мазмұнын жасырады, бұл құпиялылық мәселелерін тудыратын SSL инспекциясы сияқты құралдарды қажет етеді. Деректердің көлемі тағы бір проблема болып табылады: ірі желілер сақтау жүйелерін шамадан тыс жүктейтін күніне 10 ТБ лог шығарады (IBM Security, 2023).

Журналдар көбінесе контекстен айырылады. Мысалы, IP мекенжайына қосылу оның мақсатын түсіндірмейді, бұл жүйелік логтармен немесе threat intelligence деректерімен біріктіруді қажет етеді. Жалған позитивтер логтарды талдауды қиындатады — заңды трафикті қате түрде қауіп ретінде жіктеуге болады, әсіресе кибер-дүйсенбі сияқты ең жоғары белсенділік кезеңдерінде. Қосымша шектеу — бұл логтардың осалдығы. Шабуылдаушылар 2017 жылы Equifax-қа жасалған шабуылдағыдай жазбаларды жоя алады немесе бұрмалай алады, онда логтар ішінара жойылып, тергеуді қиындатады.

Зерттеулер осы шектеулерді жеңуге бағытталған. Lee et al. (2022) 95% дәлдікке жететін журналдарды талдау үшін терең оқыту моделін жасады. Kumar et al. (2023) 85% ықтималдықпен шабуылдарды болжайтын болжамды тәсілді ұсынды. Chen, L., et al. (2023) шифрды шешпестен қауіптерді анықтау үшін метадеректерді қолдана отырып, шифрланған трафикті өңдеуге бағытталған.

Коммерциялық секторда Palo Alto Networks журналдарды Cortex XDR-де мінез-құлық талдауымен біріктіреді, ал Cisco журналдарды қауіп деректерімен байыту шешімдерін әзірлейді. NIST (2023) интеграцияны жеңілдететін JSON-LD сияқты стандарттарды алға тартады. Зерттеулер сонымен қатар сот-медициналық тексерулерге қатысты логтарды жалған заттардан қорғау үшін блокчейнді қолдануды зерттейді.

Желілік логтарды талдауды енгізу салалар бойынша әр түрлі. Қаржы секторында (банктер, финтех) GDPR немесе PCI DSS сияқты реттеуші талаптарға байланысты жоғары өңдеу жылдамдығы қажет. Мысалы, JPMorgan Chase жауап беру уақытын 8 сағатқа дейін қысқартып, нақты уақыттағы логтарды талдау үшін QRadar пайдаланады (Gartner, 2023). Пациенттердің деректері HIPAA арқылы қорғалған денсаулық сақтауда логтарды шифрлауға және оларды ұзақ мерзімді сақтауға баса назар аударылады.

Шағын компаниялар көбінесе AWS CloudTrail сияқты бұлтты шешімдерді арзан шығындарға байланысты таңдайды, ал ірі корпорациялар бақылау үшін жергілікті жүйелерді қалайды. SIEM енгізу құны шағын бизнес үшін 1 100 мыңнан ірі ұйымдар үшін 1.1 млн-ға дейін ауытқиды, жыл сайынғы қолдау шығындары осы соманың шамамен 15% құрайды (IBM Security, 2023). Қызметкерлерді оқыту негізгі фактор болып табылады: талдаушылар ережелерді орнату және деректерді түсіндіру дағдыларын меңгеруі керек.

Target case (2013) оқиғадан кейін логты талдауды жаңарту анықтау уақытын 72-ден 10 сағатқа дейін қалай қысқартқанын көрсетеді. Сонымен қатар, Uber-ге шабуыл (2016) кемшіліктерді анықтады: журнал мониторингінің болмауы шабуылдаушыларға бір жылға дейін деректердің бұзылуын жасыруға мүмкіндік берді.

Трафиктің көлемі үлкен телекоммуникацияда логтарды қысуға және таңдамалы талдауға баса назар аударылады. Verizon ауытқуларға назар аудара отырып, күніне 50 ТБ журналдарды өңдеу үшін Kafka-ны пайдаланады. Бөлшек саудада (мысалы, Walmart) басымдық транзакцияларды қорғау болып табылады, бұл логтардың POS жүйелерінің деректерімен корреляциясын қажет етеді. Мемлекеттік секторда (мысалы, DARPA) журналдар APT-мен күресу үшін threat hunting жүйелерімен біріктірілген.

Желілік ұялардың болашағы келесі буын технологиясымен байланысты. Жасанды интеллект тарихи деректерді талдау арқылы Darktrace сияқты қауіптерді болжайды. Кванттық есептеу өңдеуді жылдамдатады, бұл 5G және IoT үшін маңызды. STIX сияқты стандарттар ұйымдар арасында деректер алмасуды жеңілдетеді, ал блокчейн олардың тұтастығын қамтамасыз етеді.

Zero Trust тұжырымдамасы әрбір қосылымды тексеру құралы ретінде логтардың рөлін арттырады. Edge computing-ті дамыту IoT құрылғыларында орталықтандырылмаған логтарды жинауды қажет етеді, бұл оларды талдау үшін жаңа қиындықтар тудырады. Ақырында, AI негізіндегі автоматтандыру жылдамдық пен дәлдікті арттыру арқылы адам факторына тәуелділікті азайтады.

Қорытынды және ұсыныстар

Менің ойымша, желілік журналдар сандық жүйелерді киберқауіптерден қорғауға көмектесетін маңызды құрал болып табылады және мен өз жұмысымда олардың құндылығын көрсетуге тырыстым. Олар маған трафикті бақылауға, ауытқуларды табуға және оқиғалардың қалай болатынын түсінуге мүмкіндік береді, бұл шабуылдармен күресте шынымен құтқарады. Бірақ қиындықтардың бар екенінде айта өткен жөн — үлкен көлемдегі деректер, шифрлау және бәрін дұрыс орнату қажеттілігі. Біз SIEM жүйелері мен логтардың корреляциясын қолданудың, сондай — ақ жасанды интеллектті қосудың пайдасын көре аламыз – бұл талдауды дәлірек және жылдамырақ етеді. Менің мақаламда көрсетілгендей, егер сіз процестерді автоматтандырып, өз мамандарыңызды оқытсаңыз, желілік логтар көп пайда әкеледі. Мен олар одан әрі қажет болатынына сенімдімін, әсіресе егер олар жаңа технологиялар мен нақты міндеттерді ескере

отырып жасалса. Бұл жұмыс маған киберқауіпсіздікті қалай жақсартуға болатынын түсінуге көмектесті және менің қорытындыларым басқаларға пайдалы болады деп үміттенемін.

Ұсыныстар:

1. *Трафикті талдауды автоматтандыру.* Желілік логтардың үлкен көлемін өңдеу үшін Splunk немесе QRadar сияқты SIEM жүйелерін енгізіп, жасанды интеллектке негізделген аномалияны анықтау алгоритмдерін қосқан жөн. Бұл қауіптерді анықтауды тездетеді және талдаушыларға жүктемені азайтады.
2. *Логтар корреляциясын орнату.* Мен әртүрлі көздерден оқиғаларды байланыстыру үшін корреляция ережелерін орнатуды ұсынамын – мысалы, брандмауэр журналдары, серверлер және DNS. Бұл оқиғалардың толық бейнесін құруға және олардың себептерін тезірек табуға көмектеседі.
3. *Деректерді жинау сапасын жақсарту.* Журналдар трафиктің барлық негізгі параметрлерін — IP мекенжайларын, порттарды, уақыт белгілерін қамтуы үшін желілік құрылғыларды мұқият конфигурациялау қажет. Деректерді өткізіп жіберу олардың пайдасын азайтады, сондықтан мен конфигурацияларды үнемі тексеріп отыруға кеңес беремін.
4. *Мамандарды оқыту.* Мен қызметкерлерді желілік логтармен және SIEM жүйелерімен жұмыс істеуге үйрету маңызды деп санаймын. Аномалияларды қалай іздеу керектігін түсіну және нәтижелерді түсіндіру қауіп-қатерге жауап беру жылдамдығын арттырады.

Қолданылған әдебиеттер тізімі

1 Иванов А.В. Сетевые логи как инструмент обнаружения киберугроз: СибФУ //Красноярский университет. – 2022. – № 1. – С. 15–30. https://elib.sfu-kras.ru/bitstream/handle/2311/145678/ivanov_network_logs.pdf?sequence=1

2 Петров С.М. Корреляция логов в системах SIEM для анализа сетевого трафика. – 2023. https://earchive.tpu.ru/bitstream/11683/78945/1/TPU1489765_petrov.pdf

3 Сидоров Д.И., Козлов Р.А. Применение систем SIEM для обработки сетевых логов и выявления аномалий. – М.: ФГУП «Изд-во «Информатика и безопасность» МГУ им. М.В. Ломоносова, 2021. – 480 с.

4 Михайлов Е.А., Степанов П.В. Анализ трафика и обнаружение аномалий с использованием сетевых логов //Журнал кибербезопасности. – 2020. – № 2. – С. 35–50. https://elibrary.ru/item.asp?id=42837412

5 Коваленко О.Н. Методы корреляции логов для повышения эффективности систем SIEM //Труды СПИИРАН. – 2023. – № 5. – С. 62–78. https://spii.ras.ru/proceedings/2023/kovalenko_siem_logs.pdf

6 Lee J., Chen L. Deep Learning for Anomaly Detection in Network Logs //Journal of Cybersecurity. – 2022. – № 8(3). – С. 45–60. https://cyberjournal.org/2022/lee_chen_anomaly_detection.pdf

УДК 004.056

ИНТЕГРАЦИЯ HONEYPOT В ИТ-ИНФРАСТРУКТУРУ КОМПАНИИ

Нурбатуров Сырым Канатұлы
mr.nurbaturov1@gmail.com

Магистрант кафедры Информационной безопасности, Астана, Казахстан
Научный руководитель – Сантеева Сая Әділбайқызы, PhD, старший преподаватель