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

- **SMS-тен бөлек аутентификация әдістерін қосу** (мысалы, Email арқылы растау немесе аутентификатор қолданбаларын пайдалану).
- **UI/UX жақсарту**, пайдаланушылар үшін 2FA процесін жеңілдету.
- **Қауіпсіздікті одан әрі күшейту**, мысалы, логин әрекеттерін бақылау және күдікті әрекеттерді анықтау алгоритмдерін енгізу.

Жоғарыда айтылғандарды талдай отырып, екі факторлы аутентификацияны қолдану қажет деген қорытынды жасауға болады. Дегенмен, қолданылатын факторлар әртүрлі болуы керек екенін ескеру қажет, яғни сенімділік үшін әртүрлі растау әдістерін қолдану қажет. Біздің жағдайда сәйкестендіру тек SMS-код арқылы жүзеге асырылады, ол жүйенің қауіпсіздік деңгейіне белгілі бір шектеулер қояды.

SMS аутентификациясы жеке басын растау үшін ыңғайлы, бірақ ол хабарламаларды ұстау, фишингтік шабуылдар және SIM картасын ауыстыру сияқты бірқатар қауіптерге сезімтал. Мұндай тәуекелдерді азайту үшін кодты енгізу әрекеттерінің санын шектеуді, оның жарамдылық мерзімін қысқартуды және күдікті кіру әрекеттерін талдауды қоса алғанда, қосымша қауіпсіздік шараларын қолдану ұсынылады.

Кейбір осалдықтарға қарамастан, SMS аутентификациясы қарапайымдылығы мен қолжетімділігіне байланысты сәйкестендіруді тексерудің танымал және кеңінен қолданылатын әдісі болып қала береді. Дегенмен, қауіпсіздік деңгейін арттыру үшін биометриялық сәйкестендіру немесе аппараттық кілттер сияқты балама әдістерді енгізу мүмкіндігін қарастырған жөн.

Қолданылған әдебиеттер тізімі

1. Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., & F. Gómez-Skarmeta, A. (2007). A Survey of Electronic Signature Solutions in Mobile Devices. Journal of Theoretical and Applied Electronic Commerce Research, 2(3), 94–109. MDPI AG”
2. Albesher AS. Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites. Sustainability. 2023; 15(14):11043.
3. Risk Analysis Research on SMS Verification Code and Biometric Recognition Technology (Likun Yu (2024))
4. Django/Flask ресми құжаттамалары. (https://flask.palletsprojects.com/en/stable/)
5. Mobizon.kz API құжаттамасы. (https://mobizon.kz/help/api-docs)

УДК 004

АВТОМАТИЗАЦИЯ ВНЕДРЕНИЯ АЛЬТЕРНАТИВНОЙ SOAR ПЛАТФОРМЫ НА ОСНОВЕ СРЕДСТВ СО СВОБОДНОЙ ЛИЦЕНЗИЕЙ

Кадринов Даулет Маулетович
kadrinov23@mail.ru
Магистрант второго курса кафедры информационной безопасности, ену им. Л. Н. Гумилева, Астана, Казахстан
научный руководитель – Оспанова А. Б.

Введение

Рост числа кибератак делает автоматизацию реагирования критически важной, но существующие SOAR-решения остаются дорогими и сложными для малого и среднего бизнеса. Угрозы затрагивают не только IT-сектор, но и другие сферы, включая госструктуры

и образование. Цель работы — разработка доступной SOAR-платформы с автоматическим развертыванием, что упростит её интеграцию и снизит затраты на внедрение.

Методы и технологии

Для эффективного управления инцидентами используется Elastic Stack (Elasticsearch, Logstash, Kibana) для сбора и анализа логов, выявления угроз и передачи алертов в TheHive. IRP-платформа TheHive автоматически создаёт кейсы, а Cortex анализирует артефакты (IP, хэши, URL). Python-скрипты обеспечивают автоматизацию реагирования: связывают сервисы, выполняют плейбуки, блокируют IP, изолируют хост и отправляют уведомления в Telegram. Система контейнеризована в Docker, а Docker Swarm управляет балансировкой. Развёртывание автоматизировано с помощью Terraform (создание ВМ) и Ansible (настройка сервисов). Такой подход обеспечивает масштабируемость, гибкость и доступность, делая платформу эффективной альтернативой коммерческим решениям.

Схема на рисунке 1 представляет работу альтернативной SOAR-платформы, объединяющей SIEM, IRP и автоматизированное реагирование на инциденты. Весь процесс начинается с того, что компьютеры и другие системы отправляют логи в SIEM, где Logstash нормализует данные и передает их в Elasticsearch для хранения и анализа, а Kibana используется для визуализации. Если в логах выявляется подозрительная активность, система генерирует алерты, которые затем поступают в специальные скрипты. Эти скрипты анализируют входящие события и передают обработанные алерты в IRP-систему TheHive, где создаются кейсы для расследования инцидентов. Если угроза подтверждается, система автоматически инициирует реагирование, выполняя блокировку IP-адресов атакующего или изоляцию скомпрометированного хоста. По результатам предпринимаемых действий формируется отчет, а для оперативного информирования администратора запускаются скрипты, которые отправляют уведомления, например, в Telegram. Вся эта архитектура обеспечивает автоматическое выявление, обработку и нейтрализацию угроз, минимизируя ручной труд и сокращая время реагирования на инциденты.

Рисунок 1. Схема инфраструктуры SOAR

Так же есть определенные шаблоны с помощью которых идет отработка инцидентов. Рисунок 2 отражает процесс реагирования на инцидент, связанный с Malware Alert из SIEM.

1. Malware Alert поступает в SIEM, анализируется факт запуска PowerShell или CMD.
   - Если запуск был, проверяется наличие исполняемых файлов с расширениями .exe, .bat, .dll.
   - Если файлы найдены, выполняется удаление вируса.
   - Если файлы не найдены, хост изолируется для предотвращения распространения угрозы.
2. Если запуска PowerShell/CMD не было, проверяется, был ли файл скачан из браузера.
   - Если да, анализируется загруженный файл. Если он вредоносный — выполняется удаление вируса.
   - Если файл не найден, хост изолируется как потенциально скомпрометированный.

Схема помогает быстро классифицировать угрозу и принять решение о дальнейших действиях.

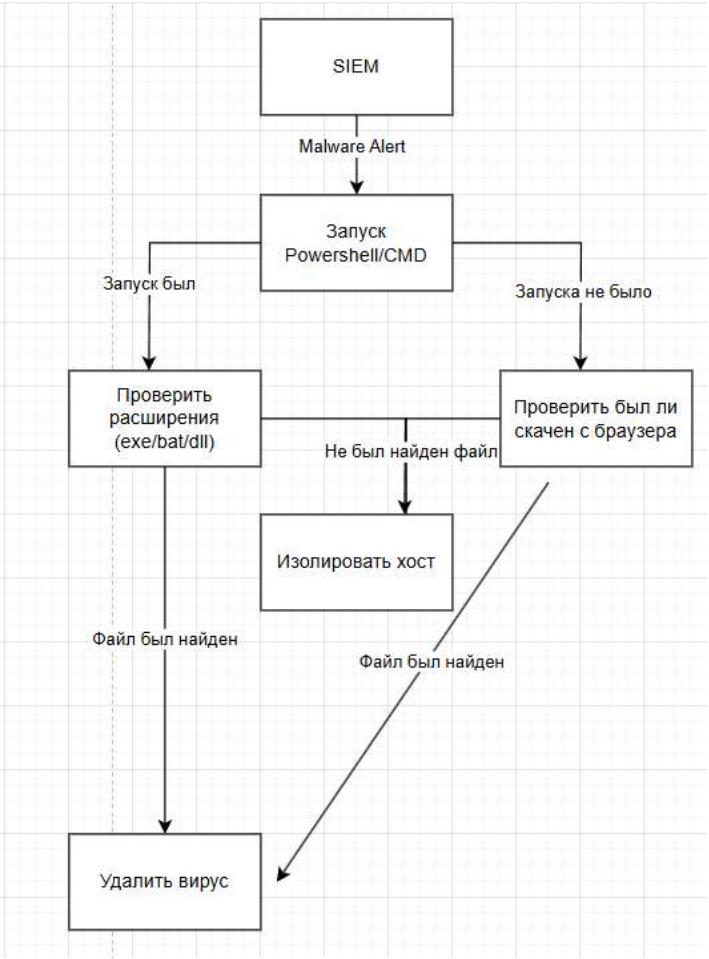

Рисунок 2. Схема работы автоматического реагирования

Код на рисунке 3 реализует автоматизированную обработку инцидентов, соответствующую ранее представленной схеме реагирования.

1. **Проверка запуска PowerShell/CMD**
   - Запрос в Elasticsearch анализирует логи, выявляя запуск powershell.exe или cmd.exe.

- Соответствует этапу "Запуск PowerShell/CMD" в схеме.

2. **Проверка подозрительных расширений**
   - Анализируются файлы с расширениями .exe, .bat, .dll.
   - Отражает этап "Проверить расширения (exe/bat/dll)".
   - Если найден подозрительный файл, возможна его изоляция или удаление.

```
from elasticsearch import Elasticsearch
import requests

# Конфигурация
ELASTIC_HOST =
ELASTIC_INDEX = "logs*"  # Индекс логов
TELEGRAM_BOT_TOKEN = '
TELEGRAM_CHAT_ID = '

# Подключение к Elasticsearch
es = Elasticsearch([ELASTIC_HOST])

def search_logs(query):
    """Поиск логов в Elasticsearch."""
    response = es.search(index=ELASTIC_INDEX, body=query, size=10)
    return response.get("hits", {}).get("hits", [])

def check_powershell_cmd():
    """Проверка запуска PowerShell/CMD."""
    query = {
        "query": {
            "bool": {
                "should": [
                    {"match": {"process.name": "powershell.exe"}},
                    {"match": {"process.name": "cmd.exe"}}
                ]
            }
        }
    }
    return search_logs(query)

def check_file_extension():
    """Проверка наличия подозрительных расширений файлов."""
    query = {
        "query": {
            "bool": {
                "should": [
                    {"match": {"file.extension": "exe"}},
                    {"match": {"file.extension": "bat"}},
                    {"match": {"file.extension": "dll"}}
                ]
            }
        }
    }
    return search_logs(query)
```

Рисунок 3. Скрипт

Разработанная SOAR-платформа превосходит коммерческие аналоги FortiSOAR, R-Vision и Splunk SOAR по ключевым параметрам которые отражены в таблице 1. Разработанная платформа быстрее, дешевле и гибче существующих решений, делая её оптимальным выбором. Таблица была основана на официальных данных от документаций продуктов

Таблица 1

Критерий	**Проект SOAR**	**FortiSOAR**	**R-Vision**	**Splunk SOAR**
Лицензия	Полностью открытая, без ограничений	Закрытая, привязка к Fortinet	Закрытая, привязка к экосистеме R-Vision	Закрытая, требует лицензии Splunk

Стоимость	Бесплатно, платишь только за ресурсы на которых будет работать	Дорого, подписка и поддержка	Дорого, скрытые платежи	Очень дорого, цена зависит от логов
Гибкость интеграций	Полностью кастомизируемая, любые API и сервисы	Ограничена продуктами Fortinet	Ограничена только R-Vision	Хорошая, но сложная в настройке
Развертывание	Автоматическое (Terraform + Ansible), готово за минуты	Долгая ручная настройка	Долгая настройка, нужны инженеры	Сложное, требует специалистов Splunk
Автоматизация	Полная, любые скрипты на Python	Ограниченная, только через Fortinet	Ограниченная, кастомизация сложная	Есть, но требует дорогостоящих специалистов

Заключение

Разработанная SOAR-платформа на основе open-source решений обеспечивает эффективное управление инцидентами, автоматизацию реагирования и интеграцию с SIEM. Благодаря контейнеризации и автоматизированному развертыванию система легко масштабируется и адаптируется под нужды организации, предлагая доступную альтернативу коммерческим продуктам.

Список использованных источников

1. Elastic. Deployment guide. – URL: https://www.elastic.co/guide/en/enterprise-search/current/deployment.html (дата обращения: 23.03.2025).

2. R-Vision. SOAR — Автоматизация реагирования на инциденты. – URL: https://rvision.ru/products/soar (дата обращения: 23.03.2025).

3. Splunk. Splunk Security Orchestration and Automation (SOAR). – URL: https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html (дата обращения: 23.03.2025).

4. Fortinet. FortiSOAR. – URL: https://www.fortinet.com/products/fortisoar (дата обращения: 23.03.2025).

УДК 004

WIRESHARK БАҒДАРЛАМАСЫН ПАЙДАЛАНЫП ЖЕЛІЛІК ТРАФИКТІ ТАЛДАУ ЖӘНЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ.

Казбаганбетова Мейрагуль Асылхановна
mira_85k@mail.ru
Қ.Жұбанов атындағы Ақтөбе өңірлік университеті, магистрант, Ақтөбе, Қазақстан
Ғылыми жетекшісі-Г.А.Шангытбаева

Аннотация. *Қазіргі ақпараттық технологиялар дәуірінде желілік қауіпсіздік маңызды орын алады. Кибершабуылдар мен зиянды бағдарламалардан қорғану үшін желілік трафикті*