Министерство науки и высшего образования Российской Федерации

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Научно-образовательный центр «Высшая ИТ школа»

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА**

СНИЖЕНИЕ КОГНИТИВНОЙ НАГРУЗКИ НА ИНЖЕНЕРОВ SOC ЧЕРЕЗ АВТОМАТИЗАЦИЮ ПРОЦЕССОВ ИНТЕГРАЦИИ ИСТОЧНИКОВ ДАННЫХ.

Шамов Егор Сергеевич

Направление подготовки 09.03.04 Программная инженерия

Направленность (профиль) «Программная инженерия»

Научный руководитель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ З.А. Полни Меня,

Заполни мои регалии и место работы

*подпись*

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_ г.

Научный консультант

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.С. Зоркин,

ведущий инженер, ООО "ТЦР"

*подпись*

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_ г.

Автор работы

студент группы № 972103

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е. С. Шамов

*подпись*

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_ г.

Оглавление

[1 Введение в предметную область 5](#_Toc191517706)

[1.1 Устройство SIEM 5](#_Toc191517707)

[1.1.1 Компоненты SIEM 5](#_Toc191517708)

[1.1.2 Процессы SIEM 5](#_Toc191517709)

[2 Анализ существующих процессов 6](#_Toc191517710)

[2.1 Процесс настройки сбора событий 6](#_Toc191517711)

[2.1.1 Создание коллектора 6](#_Toc191517712)

[2.1.2 Прямая интеграция с Kafka 6](#_Toc191517713)

[2.2 Процесс настройки нормализации событий 6](#_Toc191517714)

[2.2.1 Создание парсера 6](#_Toc191517715)

[2.2.2 Написание правил нормализации 6](#_Toc191517716)

[3 Автоматизация процесса 7](#_Toc191517717)

[3.1 Автоматизация поиска свободного порта 7](#_Toc191517718)

[3.1.1 Варианты решения проблемы 7](#_Toc191517719)

[3.1.2 Обоснование выбранного алгоритма 7](#_Toc191517720)

[3.2 Автоматизация создания топика 7](#_Toc191517721)

[3.2.1 Создание топика в собственном кластере 7](#_Toc191517722)

[3.2.2 Создание топика в кластере KaaS решения 7](#_Toc191517723)

[3.3 Автоматизация создания коллектора 7](#_Toc191517724)

[3.3.1 Требуемые параметры для запуска 7](#_Toc191517725)

[3.3.2 Генерация конфигурационного файла 7](#_Toc191517726)

[3.3.3 Развертывание сервиса 7](#_Toc191517727)

[3.3.4 Предоставление информации о развернутом экземпляре пользователю 7](#_Toc191517728)

[3.4 Автоматизация создания парсера 7](#_Toc191517729)

[3.4.1 Генерация конфигурационных файлов из шаблона 7](#_Toc191517730)

[3.4.2 Механизм развертывания парсера 7](#_Toc191517731)

Глоссарий

SOC (англ. Security Operations Center) – центр реагирования на инциденты информационной безопасности.

Введение

Security Operations Center – это специализированное подразделение, которое осуществляет мониторинг и реагирование на инциденты информационной безопасности в режиме реального времени.

Вся работа SOC построена на анализе данных с различных компонентов наблюдаемой системы. В этом команде аналитиков помогает система управления информацией и событиями безопасности (англ. SIEM). SIEM осуществляет сбор, агрегирование и анализ массивов данных в масштабах всего предприятия [4].

Каждый из этих процессов требует какой-то инфраструктуры, чтобы выполняться автоматически. Так, например, для сбора данных необходимы коллекторы – сервисы, собирающие информацию из различных источников.

Так как каждый источник уникален, под него необходимо создавать отдельный экземпляр коллектора с конфигурацией. Но файл конфигурации коллектора содержит много общих вещей, различия составляет лишь протокол взаимодействия с источником, а также место отправки данных в дальнейшем.

Для создания коллектора сейчас тратится много времени и когнитивной нагрузки инженера. Данная работа должна сократить время и нагрузку на инженера. Потому блаблабла

Целью настоящей работы является БЛАБЛАБЛА БЛАБЛАБЛА. Для достижения этой цели в работе решаются следующие задачи:

1. БЛАБЛА
2. БЛАБЛАБЛАБЛАБЛАБЛАБЛАБЛА.

# Введение в предметную область

## Устройство SIEM

### Компоненты SIEM

Блаблаблаблабла

### Процессы SIEM

# Анализ существующих процессов

## Процесс настройки сбора событий

### Создание коллектора

### Прямая интеграция с Kafka

Блаблаблабла

## Процесс настройки нормализации событий

### Создание парсера

Блаблаблабла

### Написание правил нормализации

#### Обогащение данных

Блаблабла

#### Исключение данных

Блаблабла

# Автоматизация процесса

## Автоматизация поиска свободного порта

блаблабла

### Варианты решения проблемы

Блаблабла

### Обоснование выбранного алгоритма

Блаблабла

## Автоматизация создания топика

### Создание топика в собственном кластере

Блаблаб

### Создание топика в кластере KaaS решения

Блаблабла

## Автоматизация создания коллектора

### Требуемые параметры для запуска

### Генерация конфигурационного файла

### Развертывание сервиса

### Предоставление информации о развернутом экземпляре пользователю

## Автоматизация создания парсера

### Генерация конфигурационных файлов из шаблона

### Механизм развертывания парсера

Заключение

В рамках данной работы …..

Список использованных источников и литературы

1. Site Reliability Engineering: How Google Runs Production Systems // Бетси Бейер, Нейл Ричард Мёрфи, Дэвид Рензин, Кент Кавахара и Стивен Торн, 2016.
2. UML. Основы. Третье издание. Краткое руководство по стандартному языку объектного моделирования // Мартин Фаулер, 2013.
3. Docker Documentation // Docker – [Б.м.]., 2024 – URL: [https://docs.docker.com](https://docs.docker.com/) (дата обращения: 20.06.2024).
4. What is SIEM? // Microsoft – [Б.м.]., 2025 – URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem