**Отчет по выполнению задания №1**

Целью данной работы было создание системы централизованного сбора и анализа логов для контроля активности сотрудников отдела F и мониторинга внутреннего сетевого трафика с целью выявления аномалий и своевременного реагирования на критические события.

**Задачи**:

* Организовать сбор логов действий пользователей (авторизация, доступ к ресурсам, изменения данных).
* Обеспечить централизованное хранение и быстрый анализ логов.
* Настроить мониторинг внутреннего сетевого трафика и реализовать оповещения при обнаружении подозрительных событий.

**ПО.** Для реализации поставленных задач была выбрана следующая архитектура:

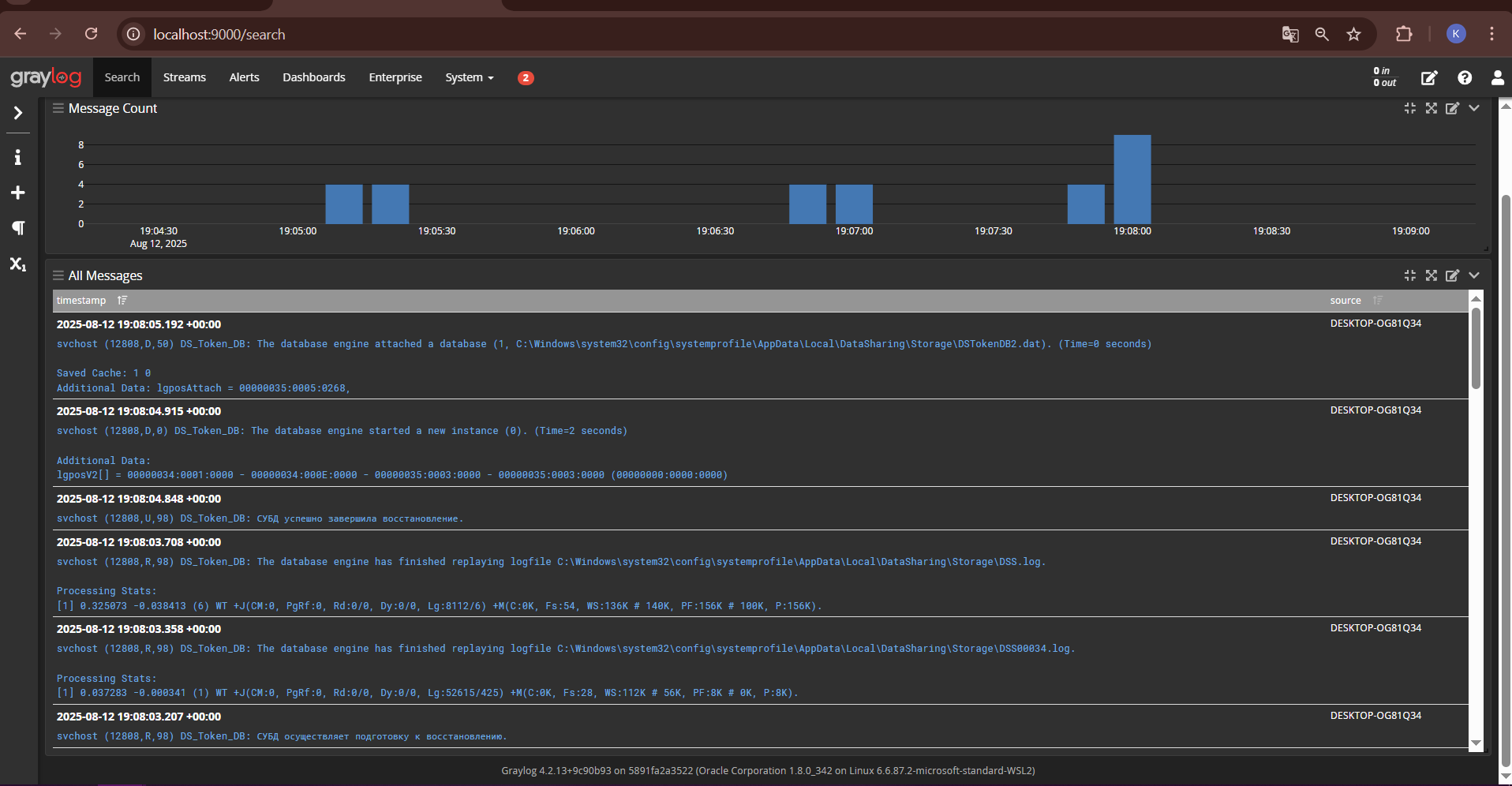
* Winlogbeat — агент сбора событий журналов Windows (Application, Security, System).
* Graylog — платформа для централизованного сбора, хранения и анализа логов.
* Elasticsearch — хранилище и поисковый движок для логов.
* MongoDB — база данных для метаданных Graylog.
* Docker Compose — для удобного развертывания всех компонентов в контейнерах.

*(были использованы данные сервисы и программы, поскольку некоторые программы запрашивают корпоративную сеть или недоступны в РФ)*

Был создан файл docker-compose.yml с описанием сервисов и конфигурация winlogbeat.yml для сбора журналов Windows и отправки в Graylog по порту 5044. Winlogbeat запущен как сервис на клиентской машине.

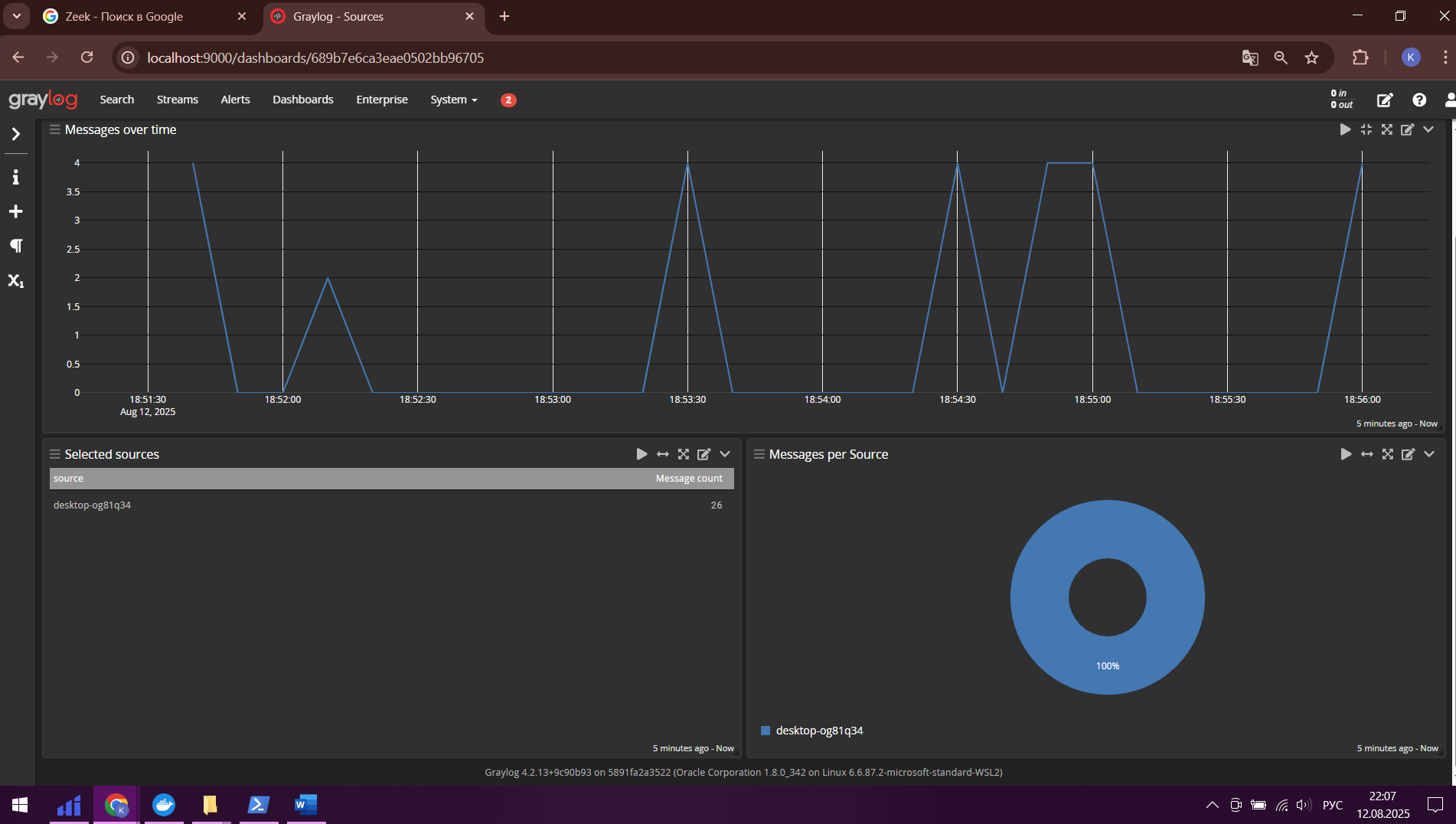
**Демонстрация результатов**

В Graylog успешно настроен прием логов от Winlogbeat. Логи с компьютера отображаются в разделе "All messages" с подробной информацией о событиях (пример на скриншоте 1).



Скриншот 1. Мониторинг событий пользователей отдела F.

Создан дашборд графиком, отображающими события входа, активности пользователей и системные уведомления (пример на скриншоте 2).



Скриншот 2. Мониторинг входов пользователей отдела F

**Рекомендации по развитию системы**

1. Добавить мониторинг сетевого трафика с использованием специализированных инструментов (например, Zeek, Suricata).
2. Настроить оповещения (alerts) в Graylog для критических событий, например, неудачные попытки входа, аномальный сетевой трафик.
3. Внедрить систему ротации и архивации логов для хранения данных за длительный период.
4. Обеспечить отказоустойчивость сервисов Graylog и Elasticsearch.
5. Регулярно обновлять и тестировать систему на предмет новых видов атак и угроз.

**Отчет по выполнению задания №2**

**Цель работы:** настроить систему мониторинга внутренних подключений сотрудников, выявлять аномальные и подозрительные события (например, изменение системных настроек, нестандартные действия в реестре Windows), а также реализовать визуализацию и аналитику в Graylog.

**Использованы компоненты:**

* Sysmon — агент для расширенного аудита событий Windows (отслеживание процессов, файловых изменений, работы с реестром и сетевой активностью).
* Winlogbeat — средство доставки событий Windows (в том числе Sysmon) в систему централизованного логирования.
* Graylog — платформа для анализа и визуализации логов.
* Logstash — промежуточный обработчик данных, получающих логи от Winlogbeat и отправляющий их в Graylog.

**Схема работы:**  
Sysmon → Winlogbeat → Logstash → Graylog → Дашборды (скриншот 3)

**Ход выполнения**

1 Настройка Sysmon

* Установлен Sysmon на рабочую станцию.
* Конфигурация Sysmon настроена для логирования ключевых событий безопасности (в том числе — запись изменений в реестре).

2 Настройка Winlogbeat

В конфигурационном файле winlogbeat.yml добавлен раздел для сбора логов *Sysmon:*

*yaml*

*КопироватьРедактировать*

*winlogbeat.event\_logs:*

*- name: Microsoft-Windows-Sysmon/Operational*

*ignore\_older: 72h*

*output.logstash:*

*hosts: ["127.0.0.1:5044"]*

*logging.level: debug*

*logging.to\_files: true*

*logging.files:*

*path: C:\winlogbeat\logs*

*name: winlogbeat.log*

*keepfiles: 7*

*permissions: 0644*

Winlogbeat успешно запущен и отправляет события в Logstash.

3 Прием и обработка логов в Graylog

* Настроен прием входящих сообщений через Beats Input (порт 5044).
* Создан поток для фильтрации событий Sysmon, содержащих "Registry value set".
* Логи корректно поступают в систему (пример на скриншоте).

4 Построение дашбордов

На основе полученных событий Sysmon в Graylog создана панель мониторинга:

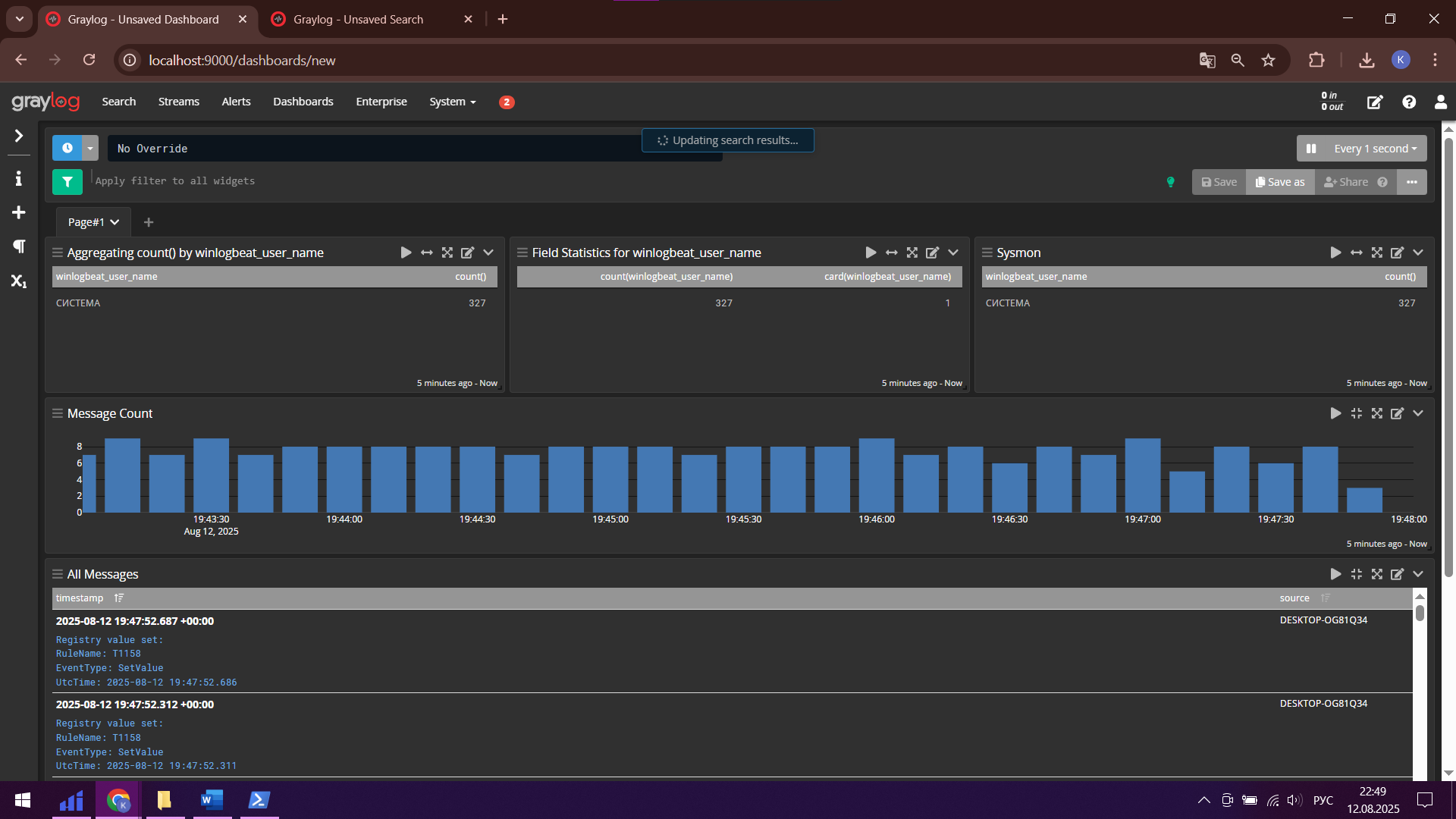
* Агрегация count() по winlogbeat\_user\_name — отображает количество событий по каждому пользователю.
* Message Count — график интенсивности событий по времени.
* Список всех сообщений — для оперативного анализа деталей инцидента.

4. Результаты

* Система собирает и отображает события Sysmon в реальном времени.
* Есть возможность быстро выявлять подозрительную активность в реестре (в т.ч. RuleName: T1158).
* Построены визуализации для анализа и выявления аномалий.
* Настроено автоматическое обновление дашборда каждые 1 секунду.

5. Рекомендации по развитию

1. Добавить мониторинг сетевого трафика через Zeek (через ВМ) или Suricata для выявления нестандартных соединений и объемов передачи данных.
2. Настроить alerts в Graylog для автоматического уведомления администраторов о критических событиях.
3. Реализовать ротацию и долгосрочное хранение логов (архивация в S3 или NAS).
4. Обеспечить отказоустойчивость и резервирование Graylog и Elasticsearch.
5. Регулярно обновлять правила и конфигурацию Sysmon в соответствии с новыми угрозами.



Скриншот 3. Изменения в реестре — пользователи.

Система внедрена, работает в реальном времени.