006

Практическая работа

Информационно-аналитические технологии поиска угроз инорфмационной безопасности

Использование технологии Yandex DataLens для анализа данных сетевой активности

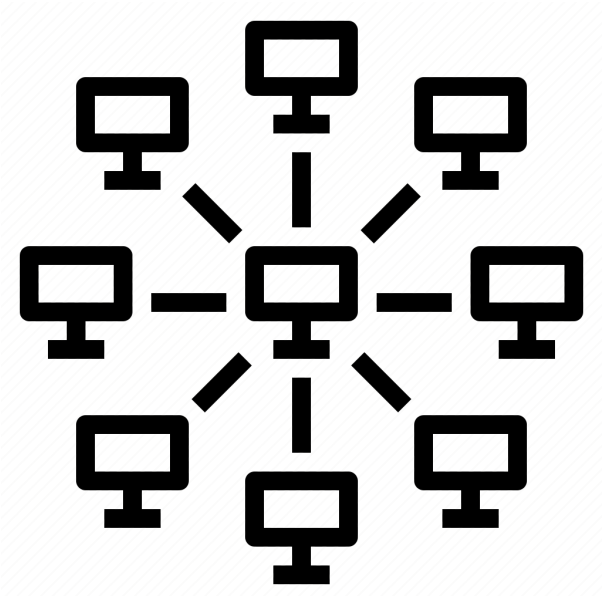
Цель работы

1. Изучить возможности технологии Yandex DataLens для визуального анализа структурированных наборов данных
2. Получить навыки визуализации данных для последующего анализа с помощью сервисов Yandex Cloud
3. Получить навыки создания решений мониторинга/SIEM на базе облачных продуктов и открытых программных решений
4. Закрепить практические навыки использования SQL для анализа данных сетевой активности в сегментированной корпоративной сети

Общая ситуация

Для понимания сетевой обстановки и принятия решений по управлению информационной безопасностью Вам необходимо визуально представить результаты анализа информации, выполненной в YandexQuery с помощью продукта DataLens. Конкретнее – serverless решение в облаке YandexCloud.

Как и прежде, у Вас есть данные сетевой активности в корпоративной сети компании XYZ. Данные хранятся в Yandex Object Storage. Вы провели разведочный анализ данных и имеете представление о структуре данных.



Yandex
DataLens

Вам необходимо построить observability решение – средство визуального представления информации для мониторинга и оценки сетевой активности.

Задание

Используя сервис Yandex DataLens настроить доступ к Yandex Query, который Вы использовали в ходе ранее выполненных практических работ, и визуально представить результаты анализа данных.

Задачи

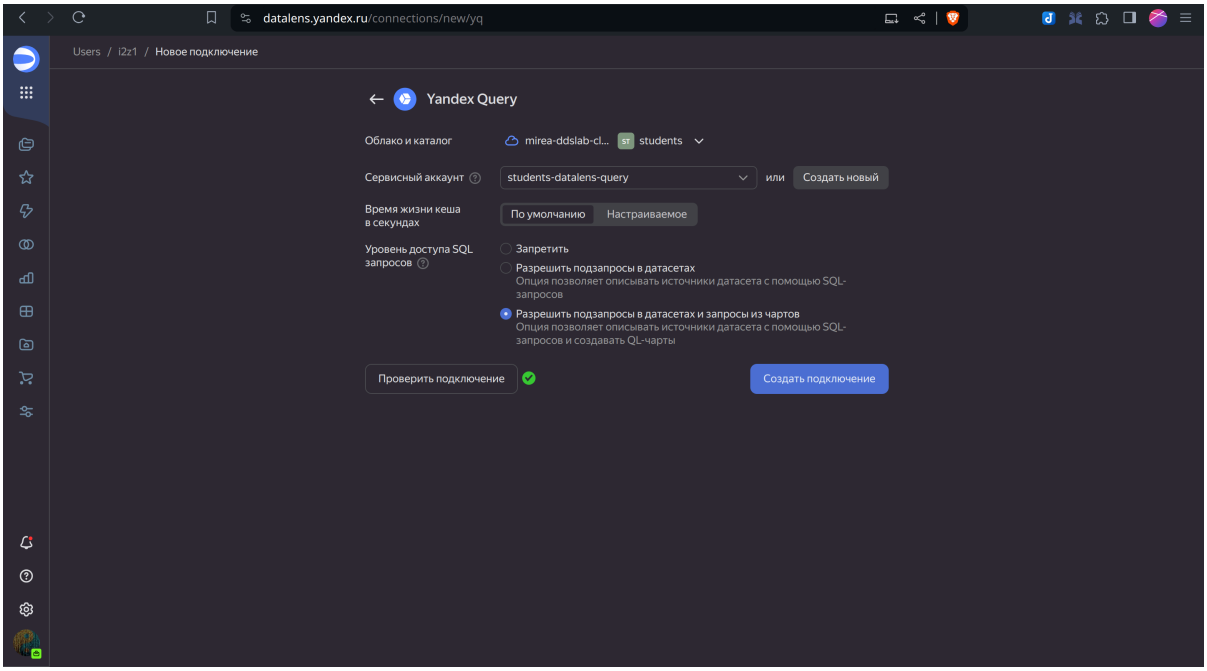
1. Представить в виде круговой диаграммы соотношение внешнего и внутреннего сетевого трафика.
2. Представить в виде столбчатой диаграммы соотношение входящего и исходящего трафика из внутреннего сетвого сегмента.
3. Построить график активности (линейная диаграмма) объема трафика во времени.
4. Все построенные графики вывести в виде единого дашборда в Yandex DataLens.

Ход работы

Для выполнения предложенного задания Вам необходимо последовательно проделать следующие шаги:

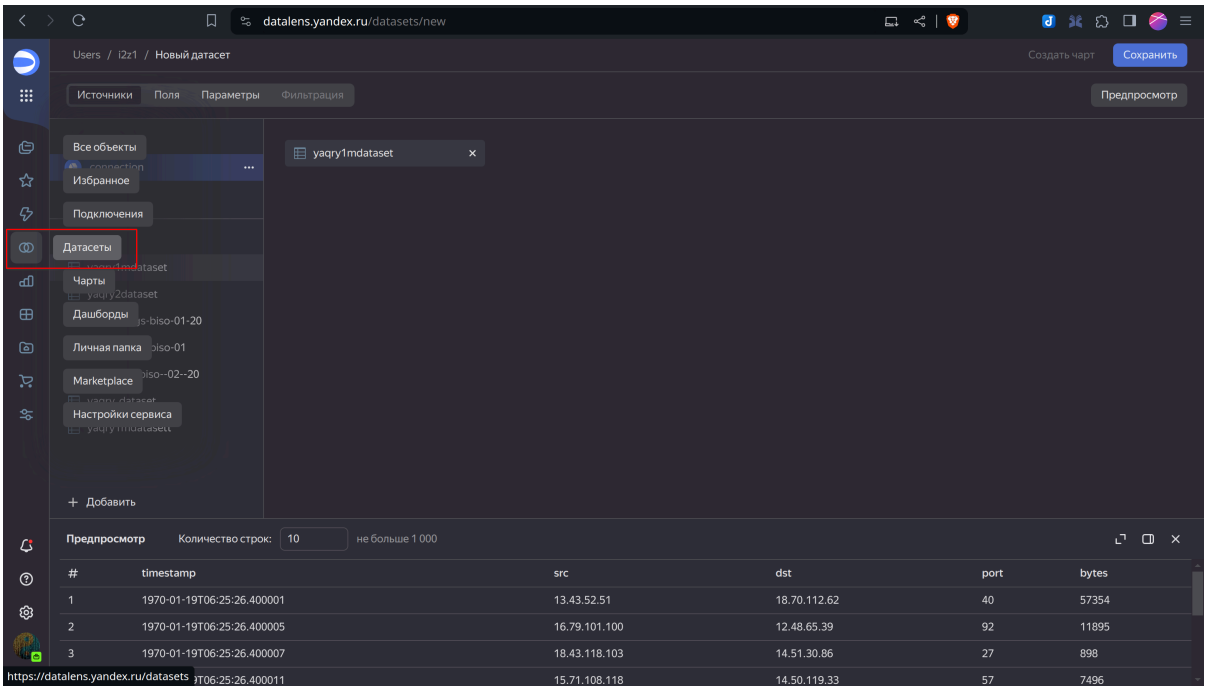
1. Настроить подключение к Yandex Query из DataLens

1. Перейти в соответствующий сервис – https://datalens.yandex.ru/
2. Выбрать “Подключения” – “Создать новое подключение”
3. Выбрать в разделе “Файлы и сервисы” Yandex Query
4. Настроить и проверить подключение



> ⚠ **Может подключение уже есть:)**
>
> Перед началом настройки, проверьте, доступно ли уже готовое подключение через сервисный аккаунт `stud2425grpsa`

2. Создать из запроса YandexQuery датасет DataLens



Перетащите из левой колонки результаты доступных запросов как датасет в правую часть экрвна. Внизу доступен предпросмотр датасета.

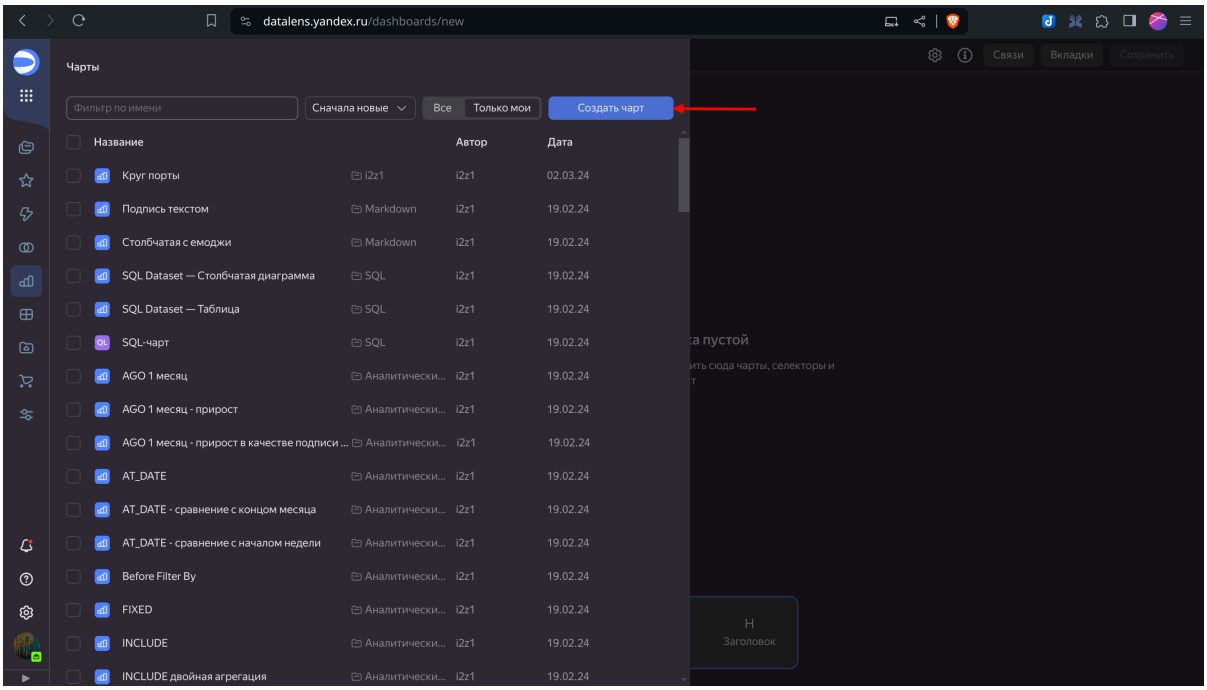
Разумеется датасет у Вас уже заранее должен быть подготовлен. Как это сделать, уже знаете – Вы ведь помните практическую работу по Yandex Query, не так ли?)

> **Как сделать SQL запрос в YandexQuery в котором будут все данные**
>
> Наверное все и так знают основы SQL, но повторение – мать ученья!
>
> Например:
>
> ```
> SELECT * FROM yaqry2dataset
> ```

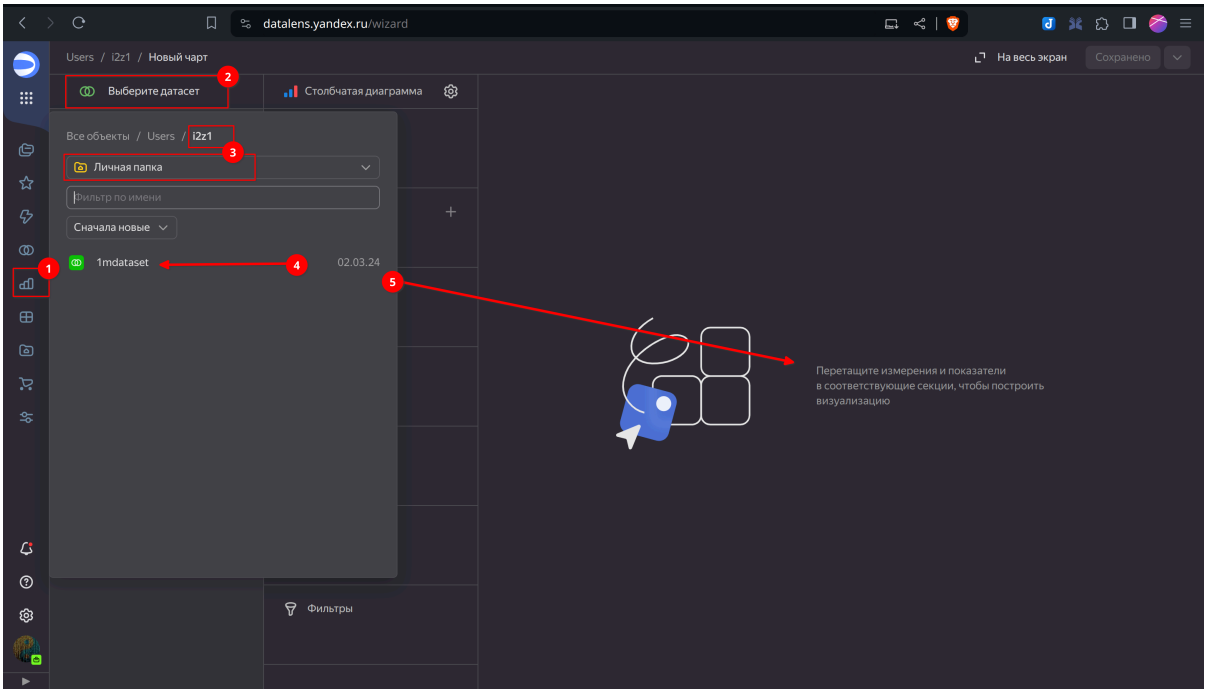
3. Делаем нужные графики и диаграммы

В DataLens они называются чартами.

Выбираем “Создать чарт – Чарт”.



Тут все элементарно: выбираем данные, тип диаграммы и данные. Все как в Excel и даже проще!

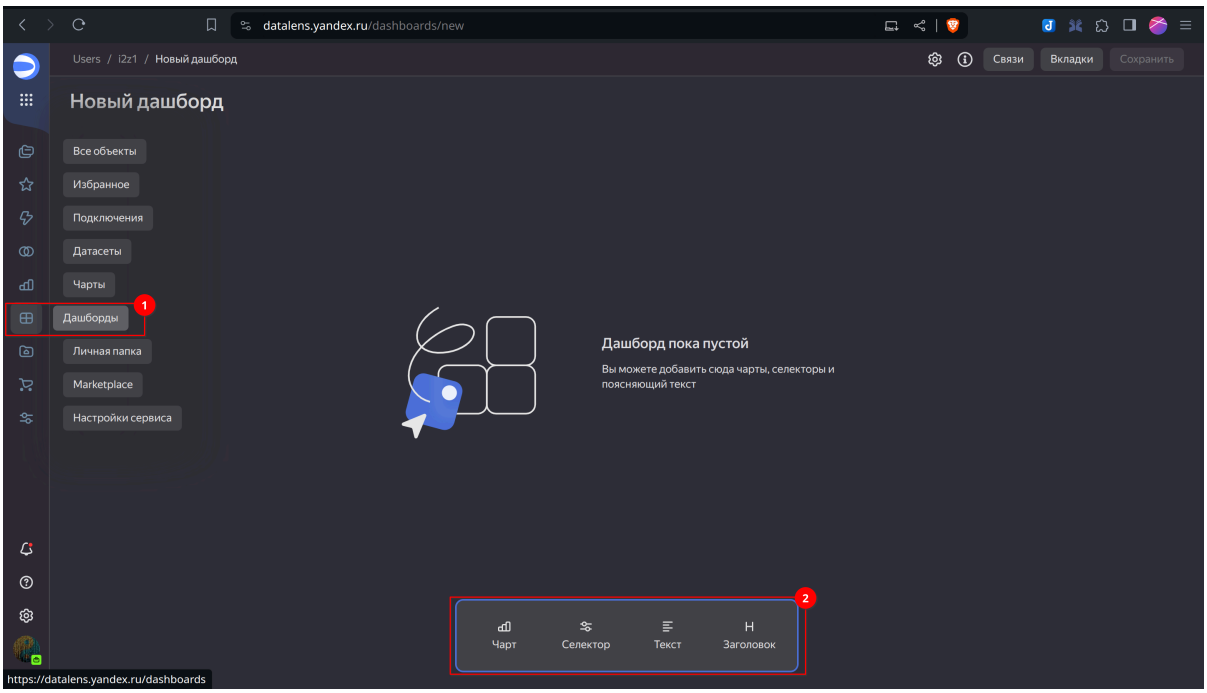


Не забудьте каждому чарту дать имя, легенду (если необходимо) и СОХРАНИТЬ

Всего у нас по заданию должно быть 3 чарта

4. Составляем дашборд

Переходим в нужный раздел и создаем новый дашборд.



Оформляем дашборд в соответствии со своим чувством прекрасного и заданием. Сохраняем!

Конкурс!!!

Конкурс!

Лучший дашборд потока – билет его создателю в кандидаты на **экзамен автоматом**!

Учитывается корректность выполнения задания, композиция, уровень оформления. Вдохновение можно брать из интернета и различных коммерческих решений.

Это ваше будущее портфолио. Труд должен вознаграждаться!:)

Tip

Дополнительные материалы можно найти в Telegram https://t.me/datadrivencybersec

Отчет

Для оформления отчета используйте следующие материалы:

1. https://i2z1.ddslab.ru/posts/lab_recommendations/
2. https://i2z1.quarto.pub/checklab/criteria.html
3. https://github.com/i2z1/Report_template

Сайт курса

https://i2z1.ddslab.ru/IAMCTH