Базовая архитектура безопасности контейнеров и kubernetes в BI-конструкторе Битрикс24

Александр Сербул,
руководитель больших данных, высоконагруженных систем
и машинного обучения, «1С-Битрикс»

Немного о себе

- Работал в Администрации Президента РФ
- Работал в Сбере, Softline, компаниях по разработке софта в ролях разработчика, руководителя подразделений разработки, IT-директора
- В Битрикс – с 2011 года.
- Архитектор и разработчик ядра BI-конструктора Битрикс24
- Веду инфраструктурные проекты на Python
- Веду внутренние высоконагруженные проекты на Java/Netty. Разработал плагин для Trino на Java для BI-конструктора Битрикс24
- Веду внутренние высоконагруженные проекты на Rust
- Участвую в сложных, крупных высоконагруженных внедрениях Битрикс24
- Много выступаю

О чем поговорим?

- Что на самом деле происходит сейчас с информационной безопасностью в IT?
- Где найти «специалистов по ИБ», умеющих программировать и понимающих более 1 ЯП?
- Почему так не любят обновлять софт и помогут ли тут контейнеры и k8s?
- ФСТЭК и эволюция ПО
- Как мы боремся за ИБ в BI-конструкторе Битрикс24

Кто создает книги?


БРАХМАНЫ
МУДРЕЦЫ
КШАТРИИ
ПРАВИТЕЛИ
ВОИНЫ
ВАЙШЬИ
ТОРГОВЦЫ
ЗЕМЛЕДЕЛЬЦЫ
ШУДРЫ
ДАЛИТЫ
ПРИСЛУГА
РАБОЧИЕ
НЕПРИКАСАЕМЫЕ
ОТВЕРЖЕННЫЕ

Что на самом деле происходит сейчас с информационной безопасностью в IT?

- Почему так важно использовать антивирус на рабочем месте сотрудников и многие до сих пор этого не понимают?
- Почему так медленно ротируют ключи и пароли или вообще не ротируют?
- Почему нет понимания важности двух и более факторной авторизации (пароль плюс «что-то еще»)?
- Почему уволенные сотрудники имеют доступ на сервера компаний много лет подряд?
- Почему в компаниях так неохотно обновляют софт: прикладной и серверный.
- Как мы боремся с этими векторами?

Где найти «специалистов по ИБ», умеющих программировать и понимающих более 1 ЯП?

- Почему специалист по ИБ часто не понимает код и технологии разработчика/системного администратора?
- Почему так важен аудит кода и настроек тимлидом?
- Как быстро прокачать сотрудников в контейнерах и k8s?
- Кто будет проверять на ИБ код на Java, Rust, Kotlin, Scala, экзотике и будет ли? Палка о двух концах.
- Как мы работаем с этими рисками?

Почему так не любят обновлять софт и помогут ли тут контейнеры и k8s?

- Почему в компаниях так много необновленных ОС? «Все же сломается и работа станет»?
- Контейнеры – помогают держать ОС обновленной.
- Как устроены современные MVP с контейнерами и разработка на их базе?
- Кто смотрит внутрь «open source» контейнеров и почему нет?
- Кто то смотрит внутрь километровых настроек helm-charts и почему нет?
- Обновление k8s у разных облачных провайдеров…

Архитектура BI-конструктора Битрикс24 и потоки данных

Docker-compose c Apache Superset + Trino

Containers

Give feedback

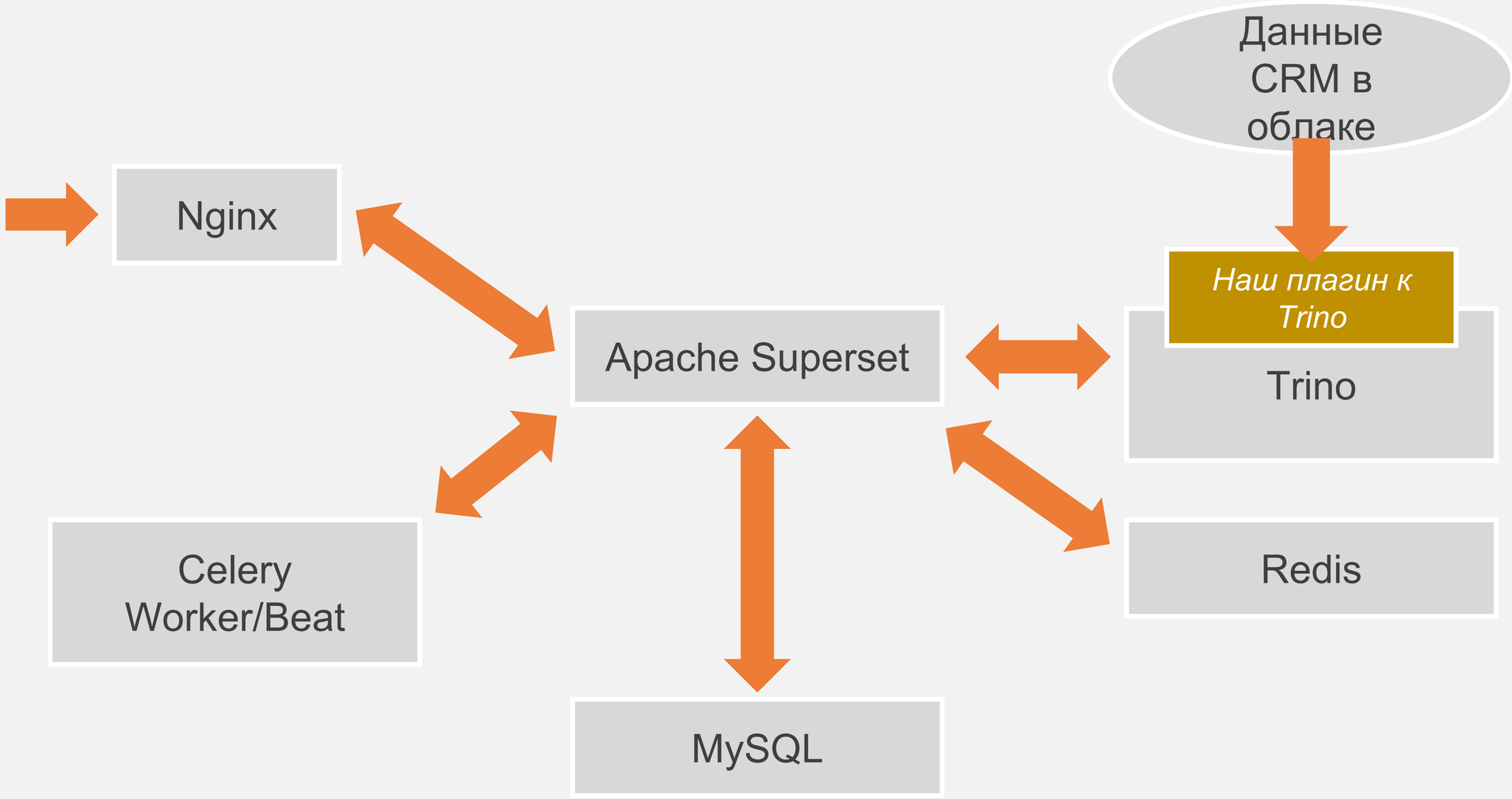
A container packages up code and its dependencies so the application runs quickly and reliably from one computing environment to another. Learn more

Search

Only show running containers

Name	Image	Status	Port(s)
fullfunct2products	-	Running (7/7)	
ss_celery_worker-1 f39fb839471c	fullfunct2products-ss_celery_worker	Running	
ss_nginx-1 a77fd5fe6845	fullfunct2products-ss_nginx	Running	1443:1443
ss_celery_beat-1 95972c0ed44e	fullfunct2products-ss_celery_beat	Running	
ss_superset-1 68b29f2681fa	fullfunct2products-ss_superset	Running	
ss_trino-1 f3ab546a7574	fullfunct2products-ss_trino	Running	
ss_redis-1 102c4813c14d	fullfunct2products-ss_redis	Running	
ss_mysql-1 b92396ea5970	fullfunct2products-ss_mysql	Running	

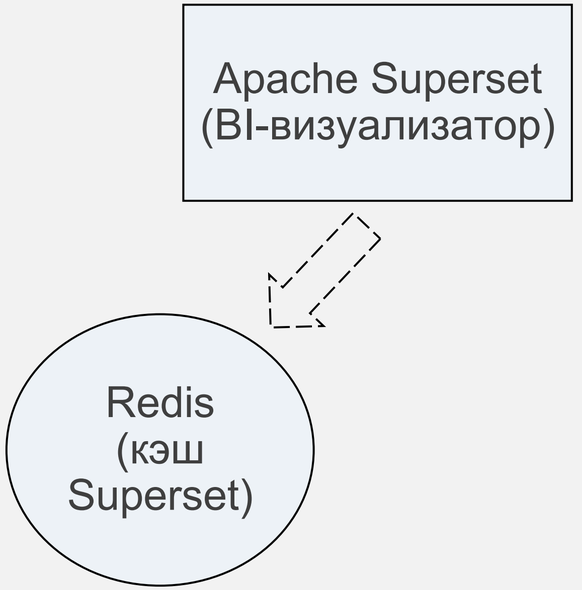
Архитектура Docker-контейнеров для BI



Потоки данных

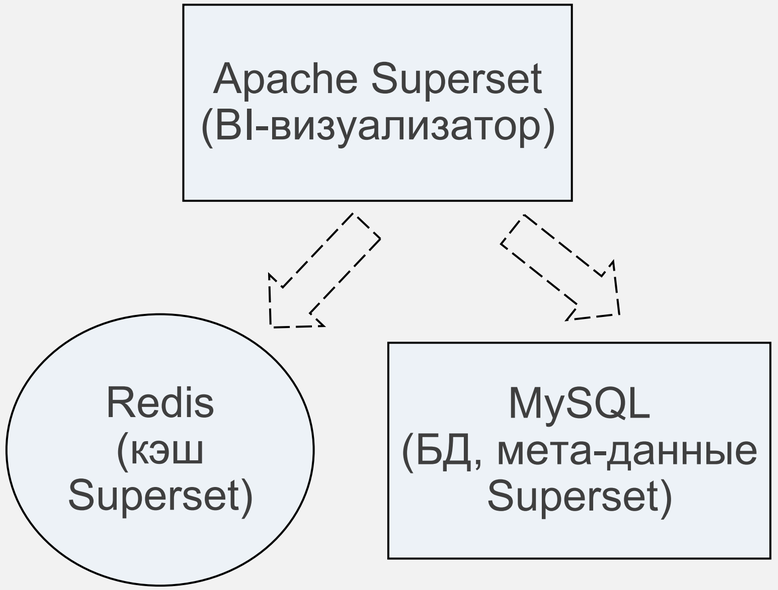
- Superset и Redis – внутри 1 пода, 1 под =

  1 клиент/компания



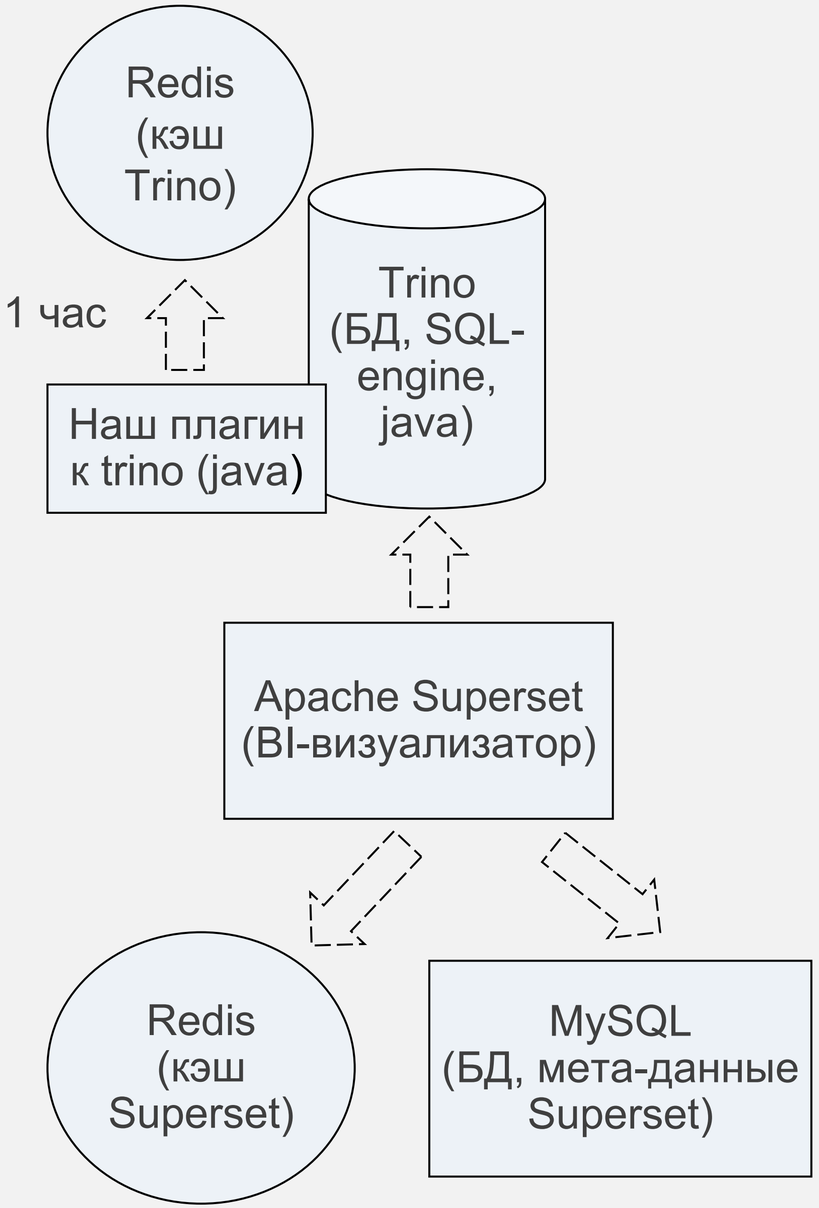
Потоки данных

- Superset и Redis – внутри 1 пода, 1 под = 1 клиент/компания
- MySQL – снаружи k8s, 1 клиент = 1 БД в MySQL



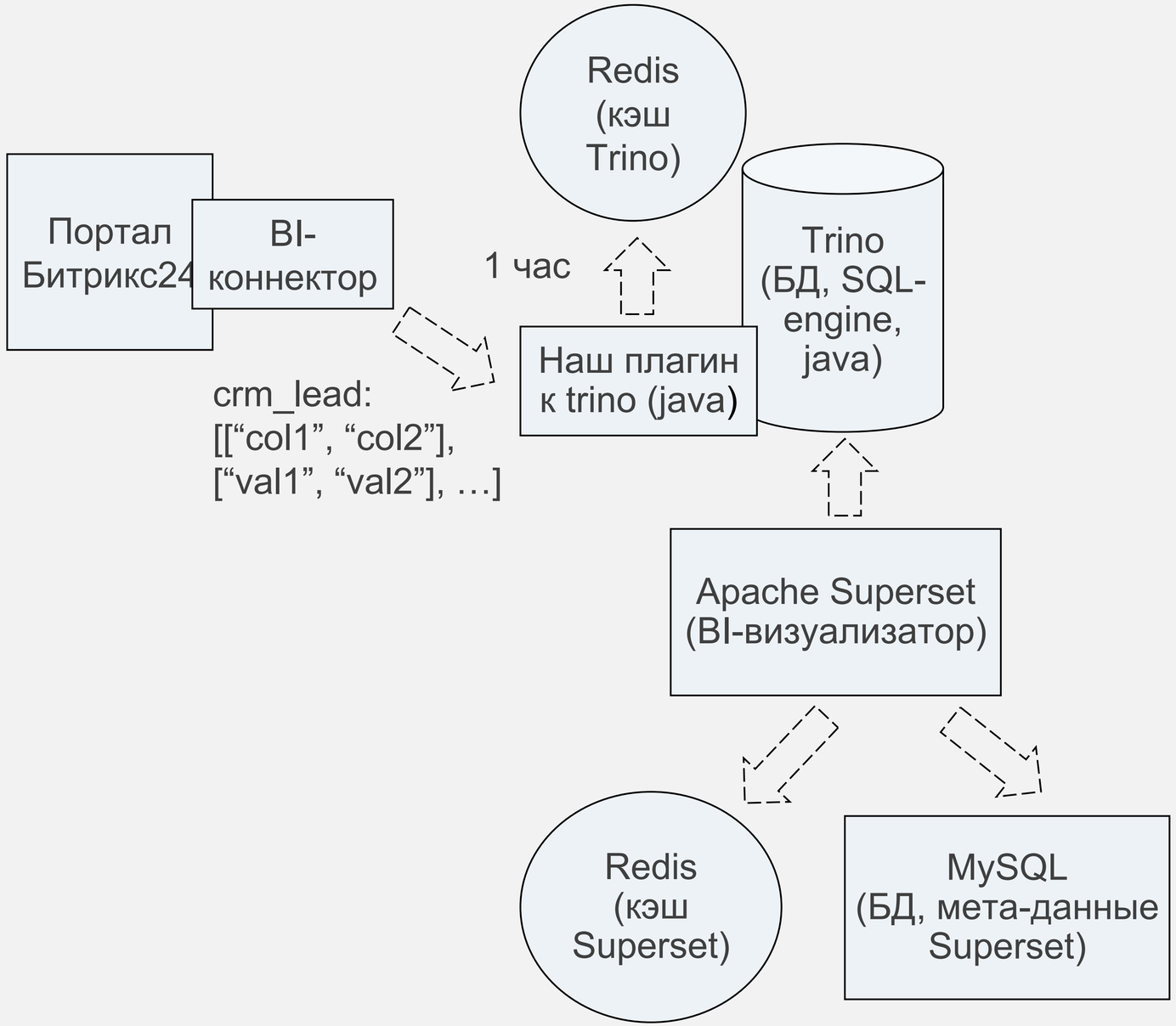
Потоки данных

- Superset и Redis – внутри 1 пода, 1 под = 1 клиент/компания
- MySQL – снаружи k8s, 1 клиент = 1 БД в MySQL
- Trino и ее кэш в Redis – снаружи k8s

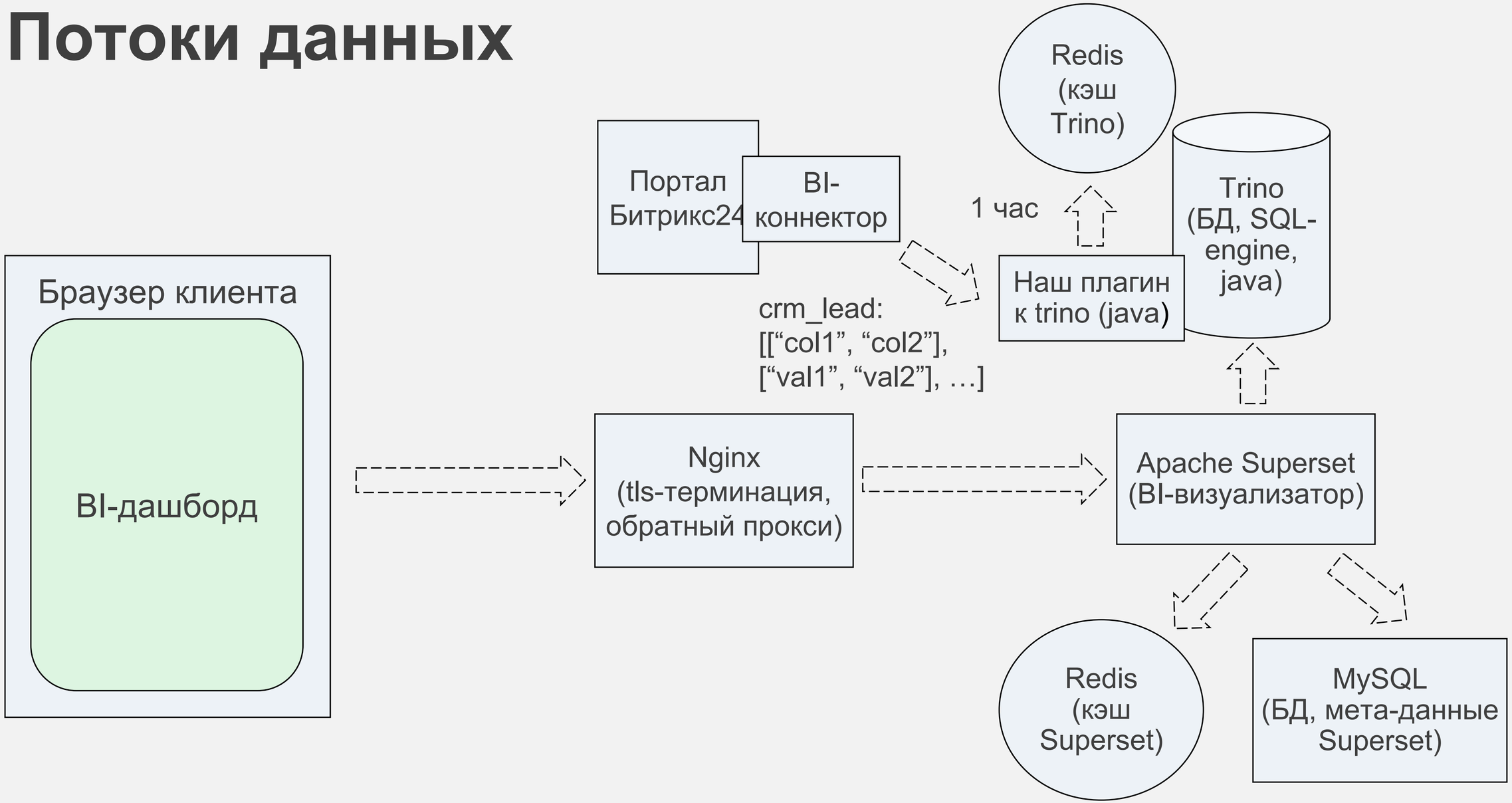


Потоки данных

- Данные клиентов – порталы Битрикс24, снаружи k8s



Потоки данных



Работа с векторами атак

- Каждый клиент – в своем namespace кубернетес в VK cloud. У нас - один из крупнейших облачных кластеров k8s в России.
- Порты redis в поде клиента – открыты на localhost (иначе были видны с любого пода). Vanila k8s – весь прозрачный!
- Контейнеры *постепенно* доработаны с запуском не от root
- Регулярно обновляем *постепенно свой* контейнер Apache Superset и раскатываем на десятки тысяч клиентов через «helm upgrade»
- Обычные секреты в k8s, никаких vaults и аддонов, kubernetes-replicator, «довольно длинные неплохие» (С) пароли
- Бекапа k8s нет и не хотим

Работа с векторами атак - 2

- Базы клиентов в MySQL – симметрично зашифрованы «на лету», MFA, защита от «слива»
- Файлы паролей в Trino – хэши с солью, пароли «довольно длинные неплохие» (C)
- Написали свой менеджер безопасности в плагине Trino на Java с логированием secure-операций
- TLS-терминация – за пределами k8s в nginx на балансерах, хотя начинали с секретов внутри k8s и TLS в ингресс-контроллере
- Ingress-контроллер был «ingress-nginx», сейчас «contour-envoy». Как мы его научились обновлять.

Спасибо за внимание!

Вопросы?

Александр Сербул,
руководитель больших данных, высоконагруженных систем и машинного обучения, «1С-Битрикс»