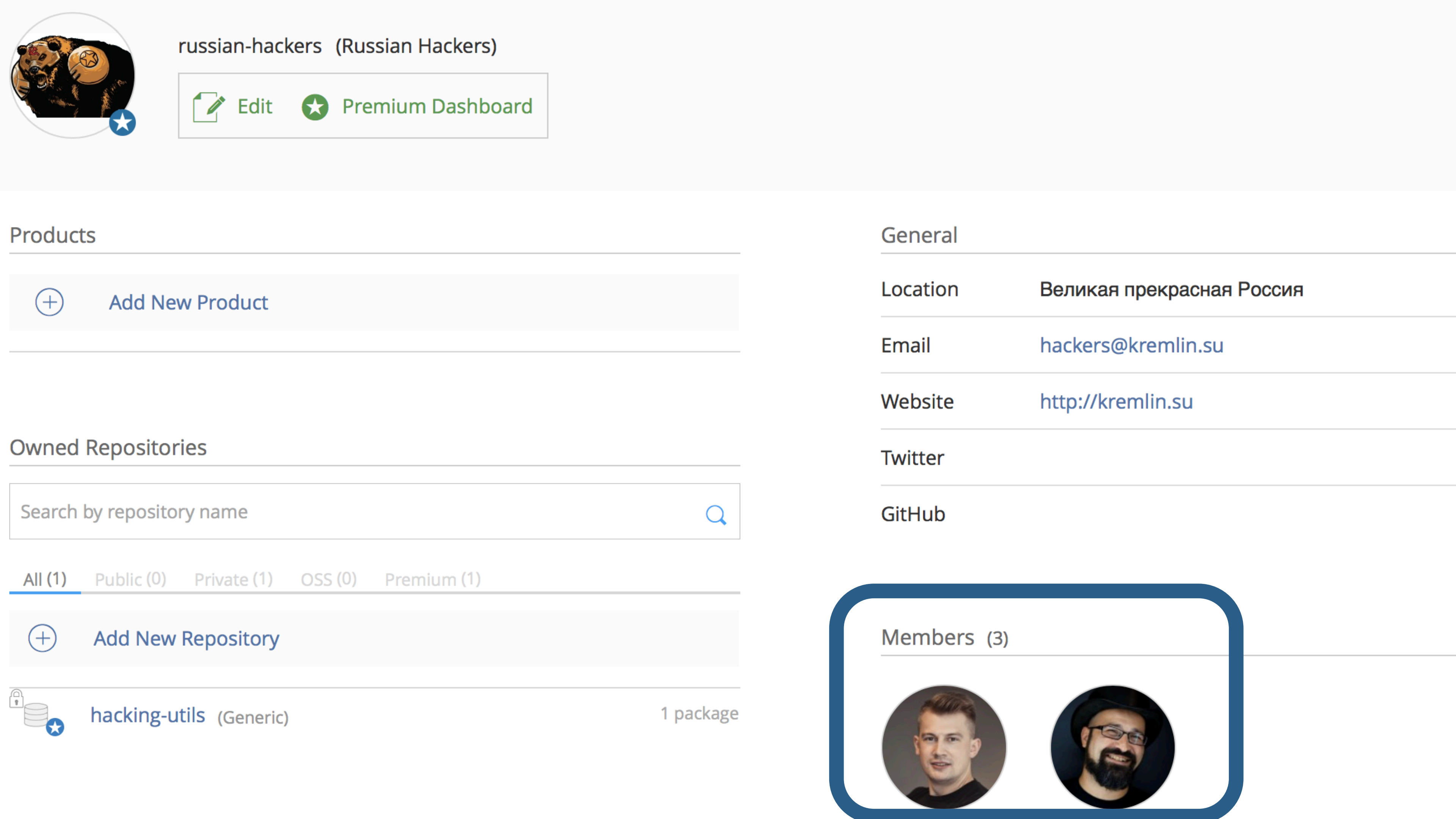
FIGHT CRIME WITH KAFKA STREAMS AND BINTRAY FIREHOSE API

Consuming liquid software from firehose like...



russian-hackers (Russian Hackers)

Products

Owned Repositories

hacking-utils (Generic) 1 package

General

Location	Великая прекрасная Россия
Email	hackers@kremlin.su
Website	http://kremlin.su
Twitter	
GitHub	

Members (3)

HACKERS? WAT?

- BARUCH SADOGURSKY
- HEAD OF DEVREL @JFROG
- @JBARUCH

- VIKTOR GAMOV
- DEVELOPER ADVOCATE @CONFLUENTINC
- @GAMUSSA

WTF IS FIREHOSE?!

FIREHOSE API

- TWITTER HAS IT, AWS HAS IT, BITNTRAY HAS IT
- STREAMING EVENTS FROM THE SOCKET
- A LOT OF INFORMATION

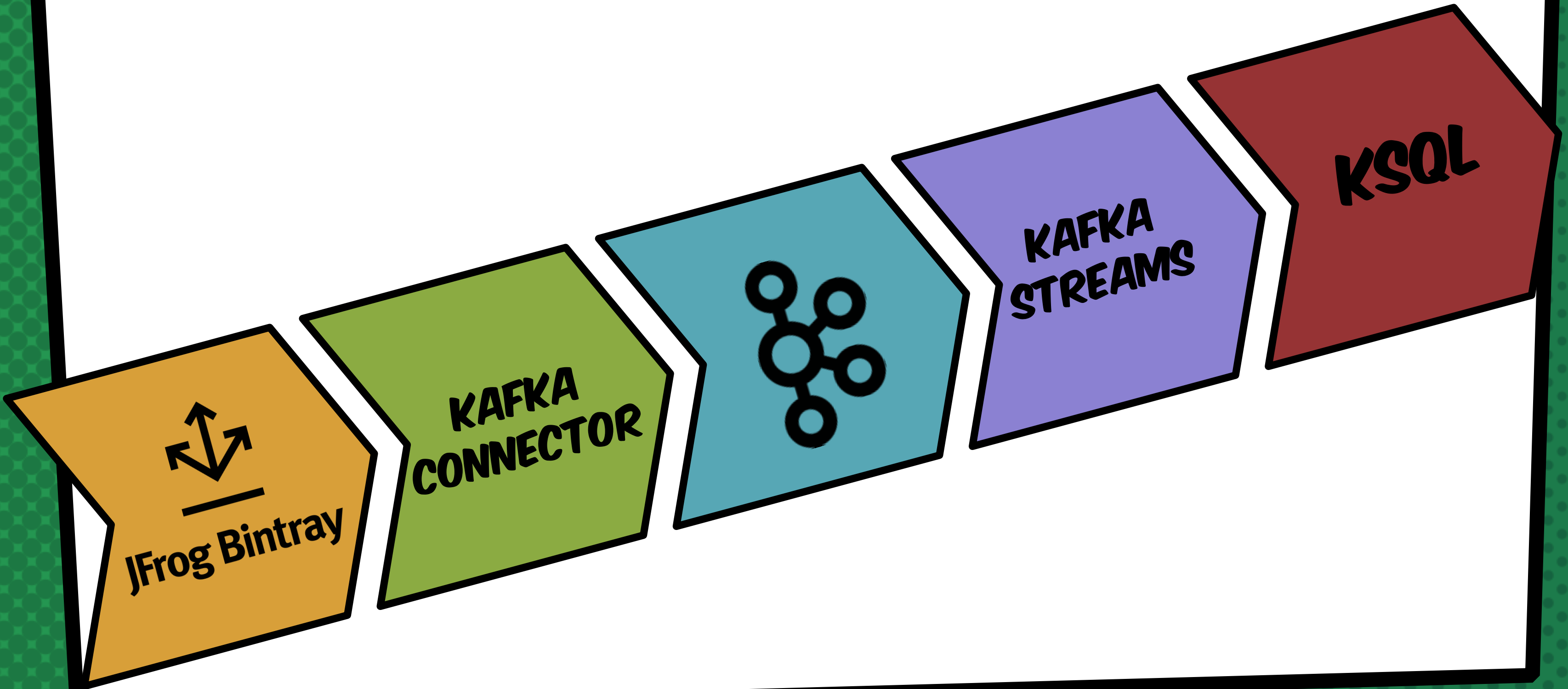
BINTRAY FIREHOSE API

- LOGIN SUCCESS
- LOGIN FAILURE
- FILE UPLOADED
- FILE DOWNLOADED
- FILE DELETED

CONSUMPTION

- JFROG CLI (PIPING ETC)
- REST API
- JAVA API (SOON)

OUR PROCESS IS EASY



JFrog Bintray

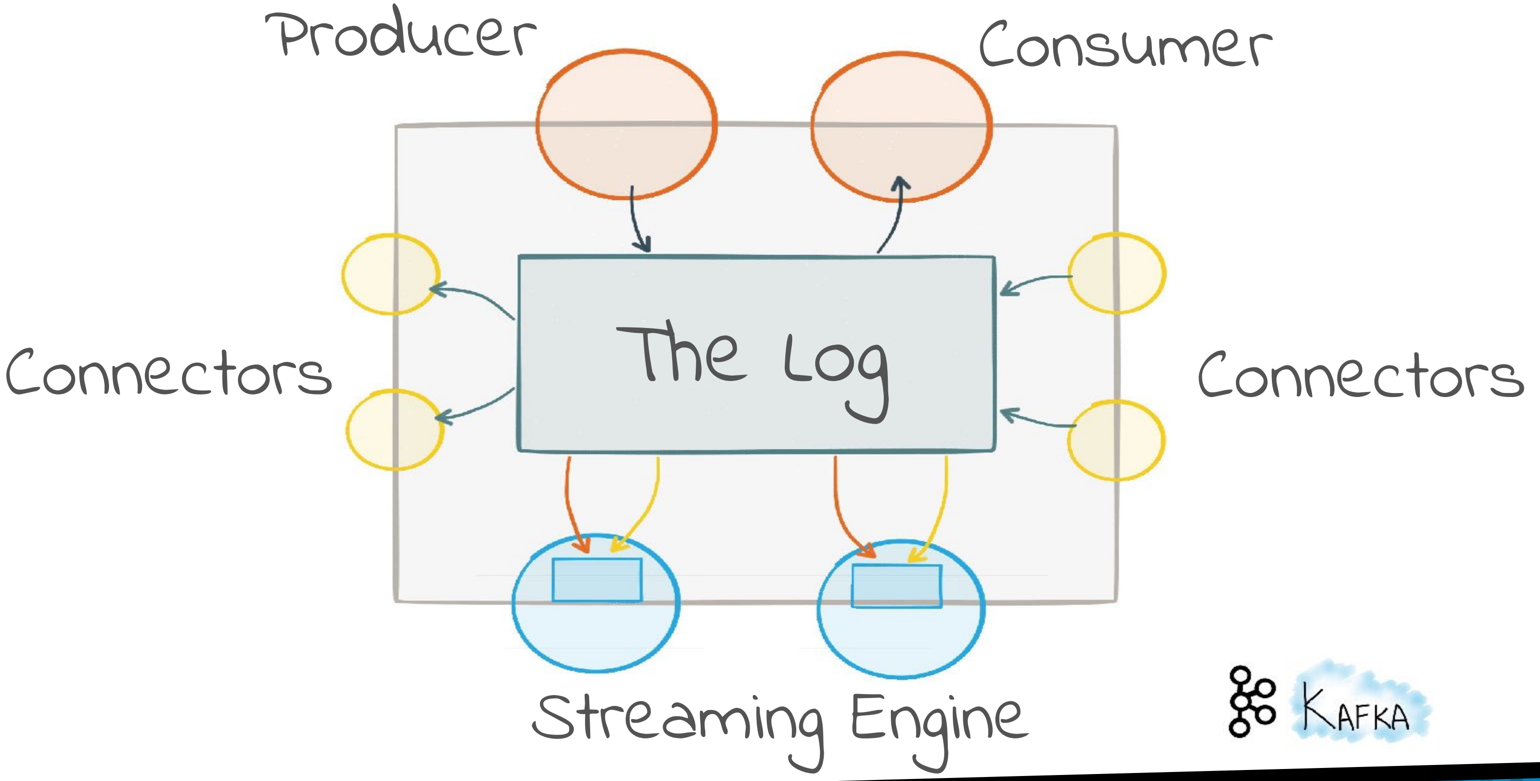
KAFKA CONNECTOR

KAFKA STREAMS

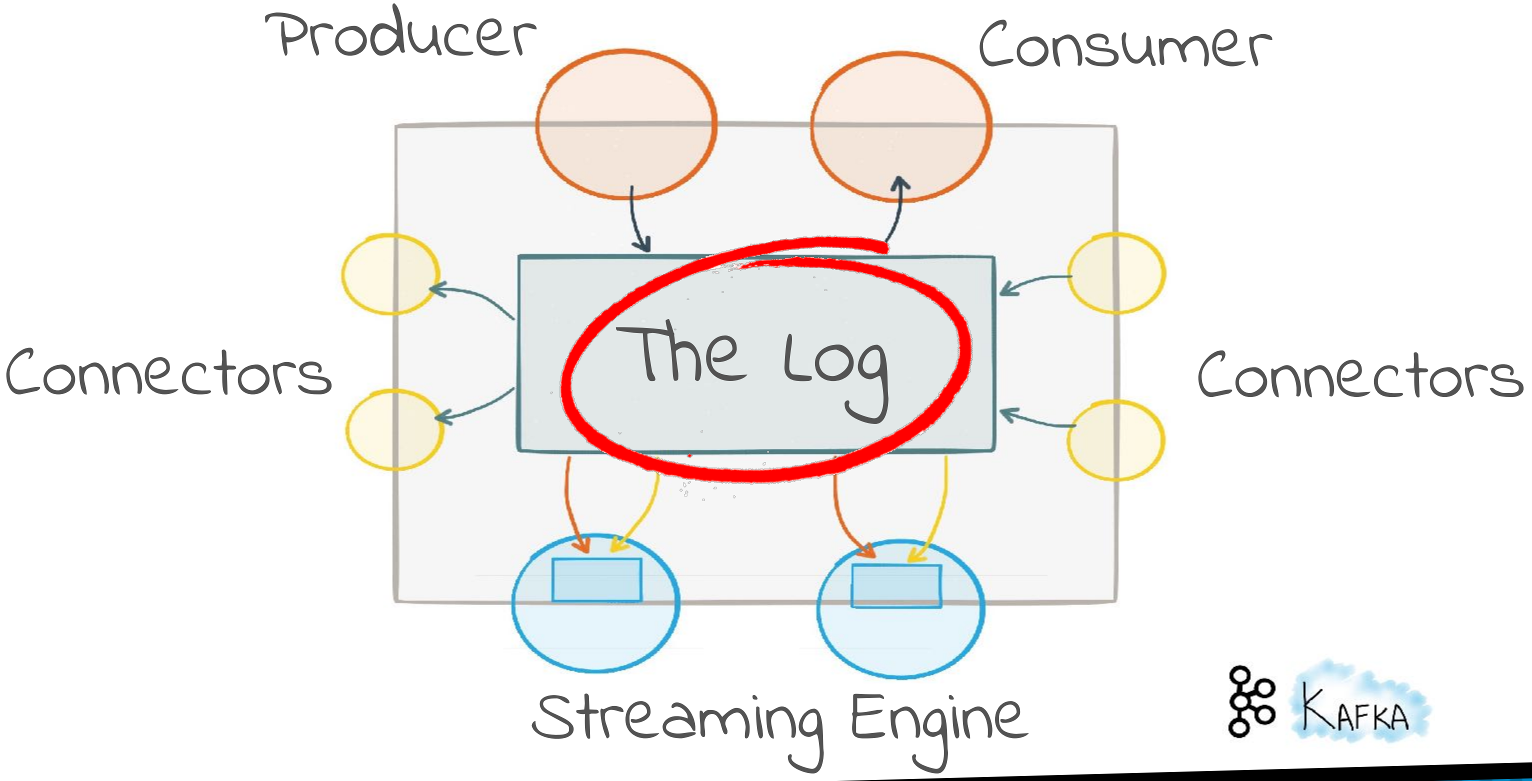
KSQL

KAFKA BASICS

WHAT IS A STREAMING PLATFORM?

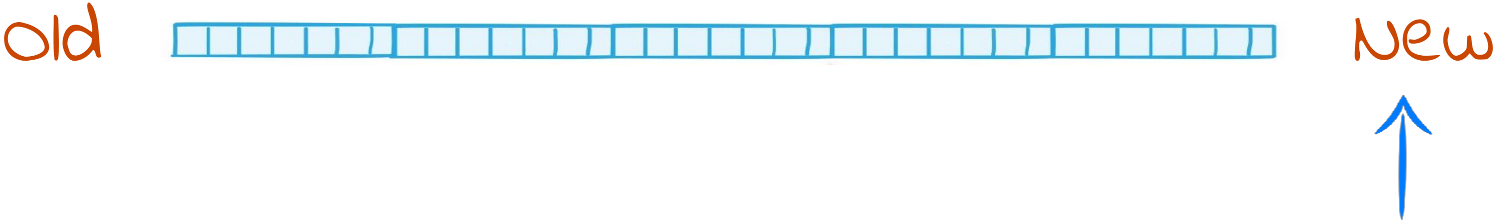


KAFKA'S DISTRIBUTED LOG



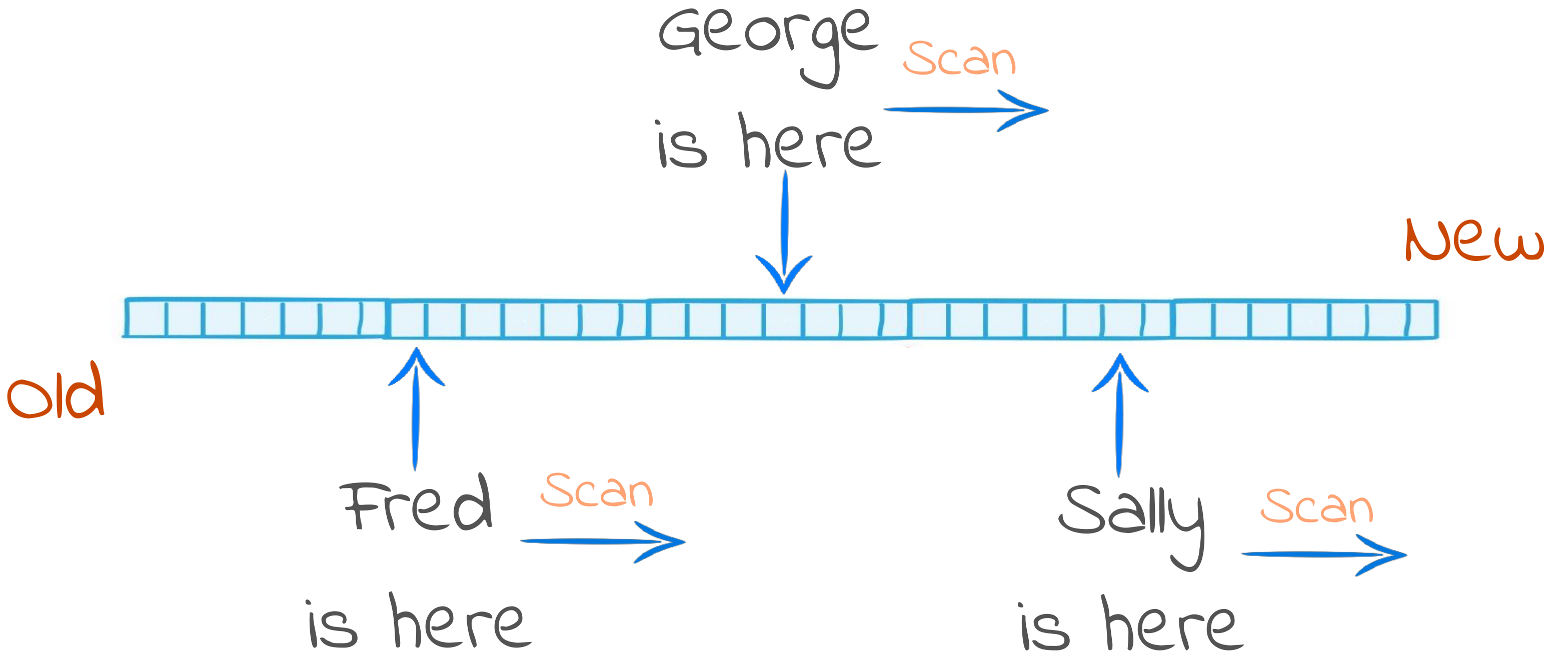
KAFKA

THE LOG IS A SIMPLE IDEA

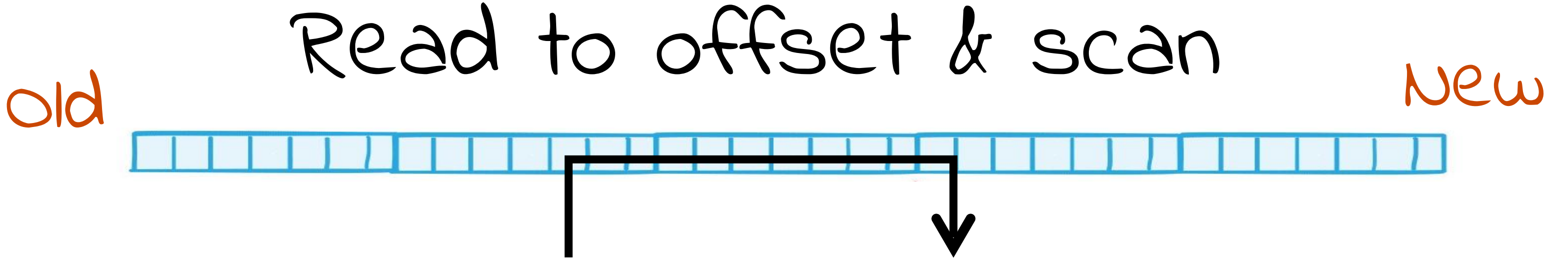


Messages are added at the end of the log

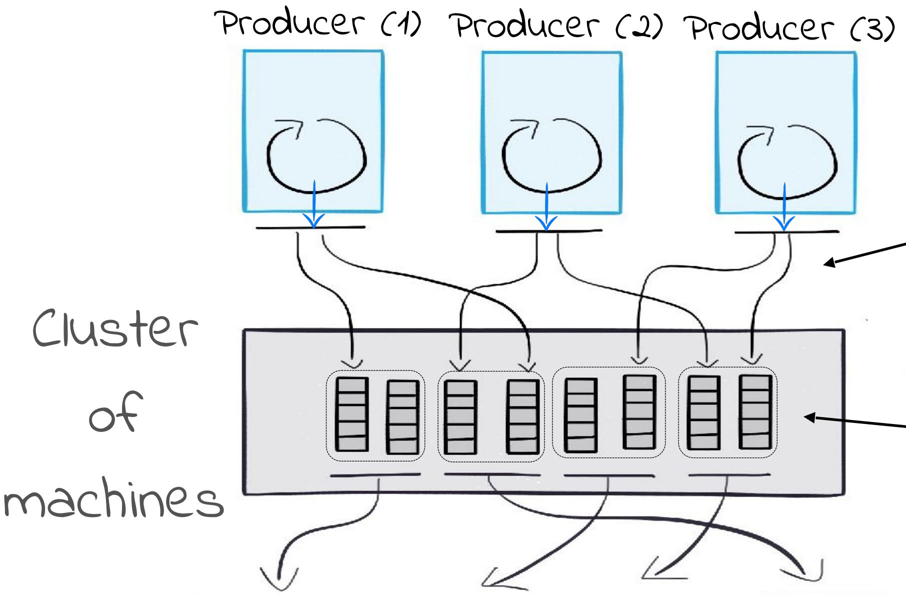
CONSUMERS HAVE A POSITION ALL OF THEIR OWN



ONLY SEQUENTIAL ACCESS



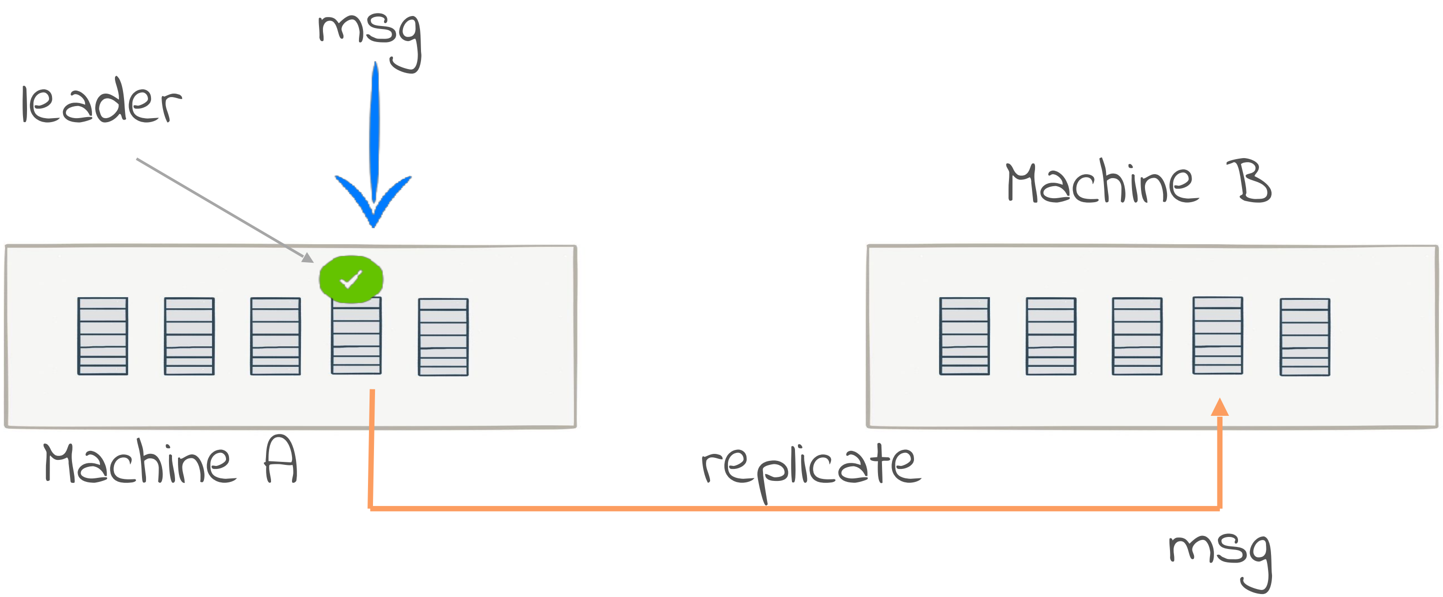
SHARD DATA TO GET SCALABILITY



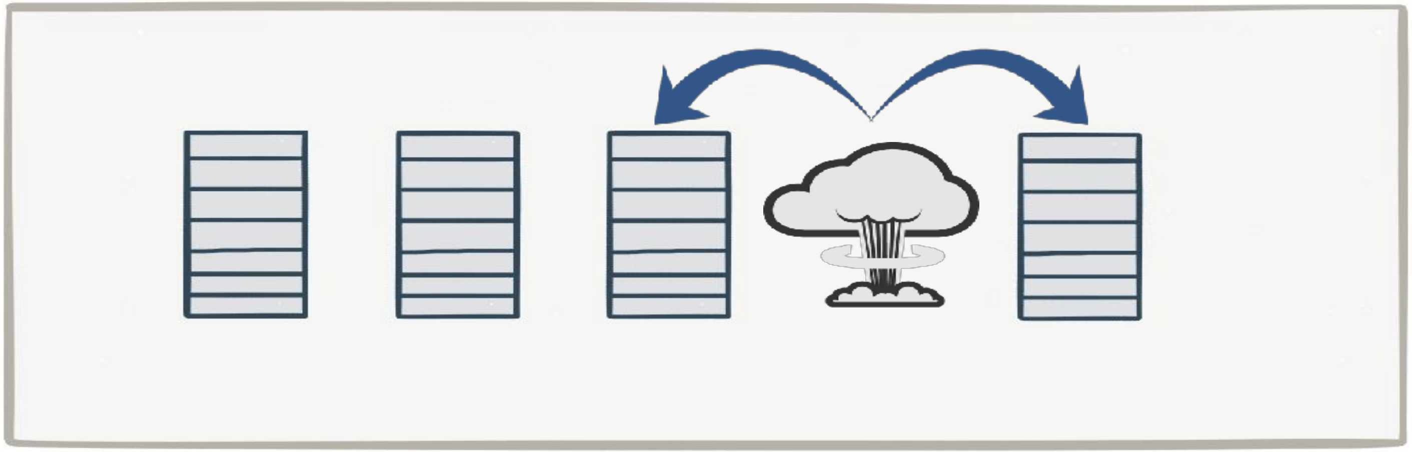
Messages are sent to different partitions

Partitions live on different machines

REPLICATE TO GET FAULT TOLERANCE

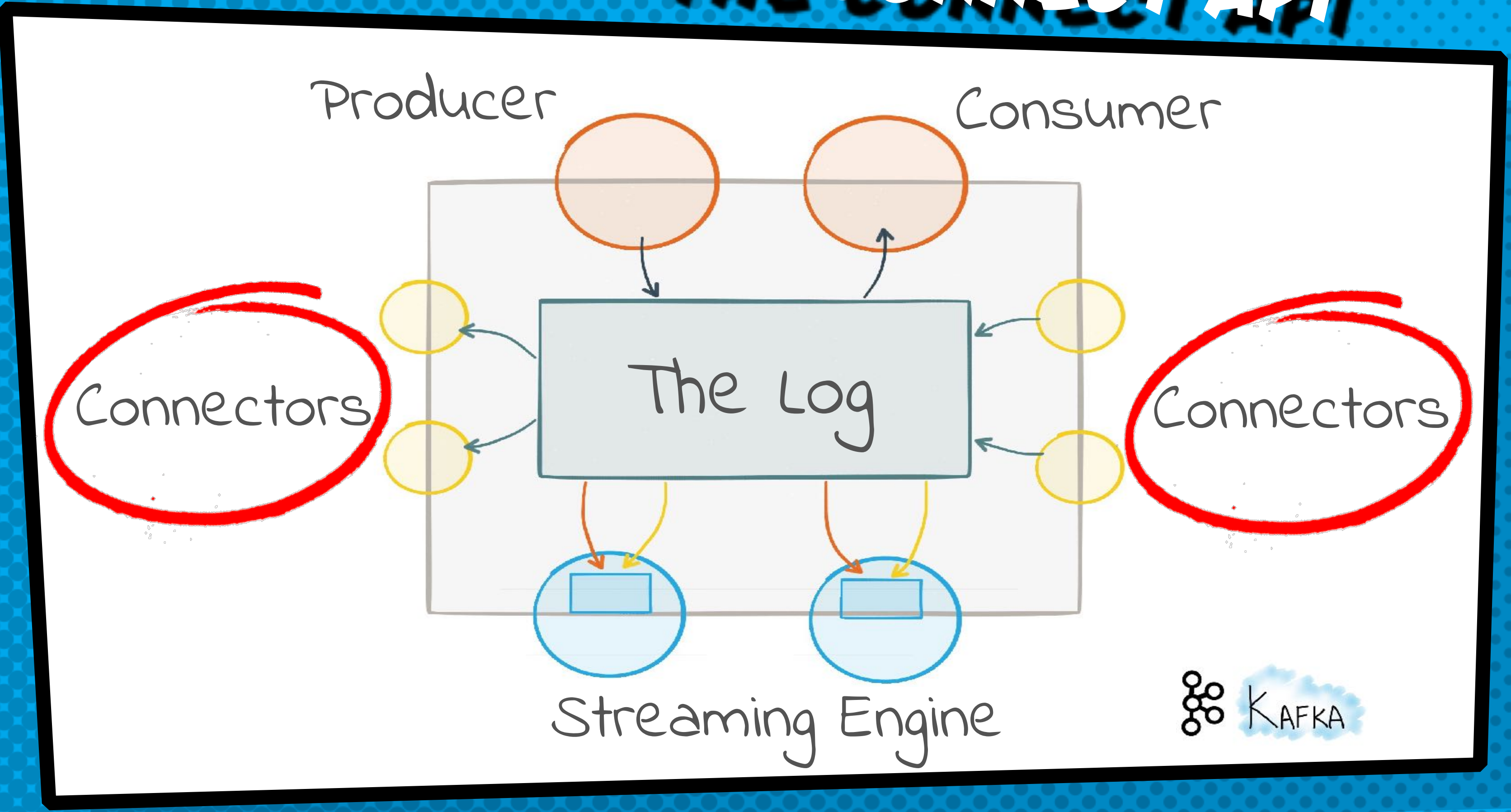


REPLICATION PROVIDES RESILIENCY

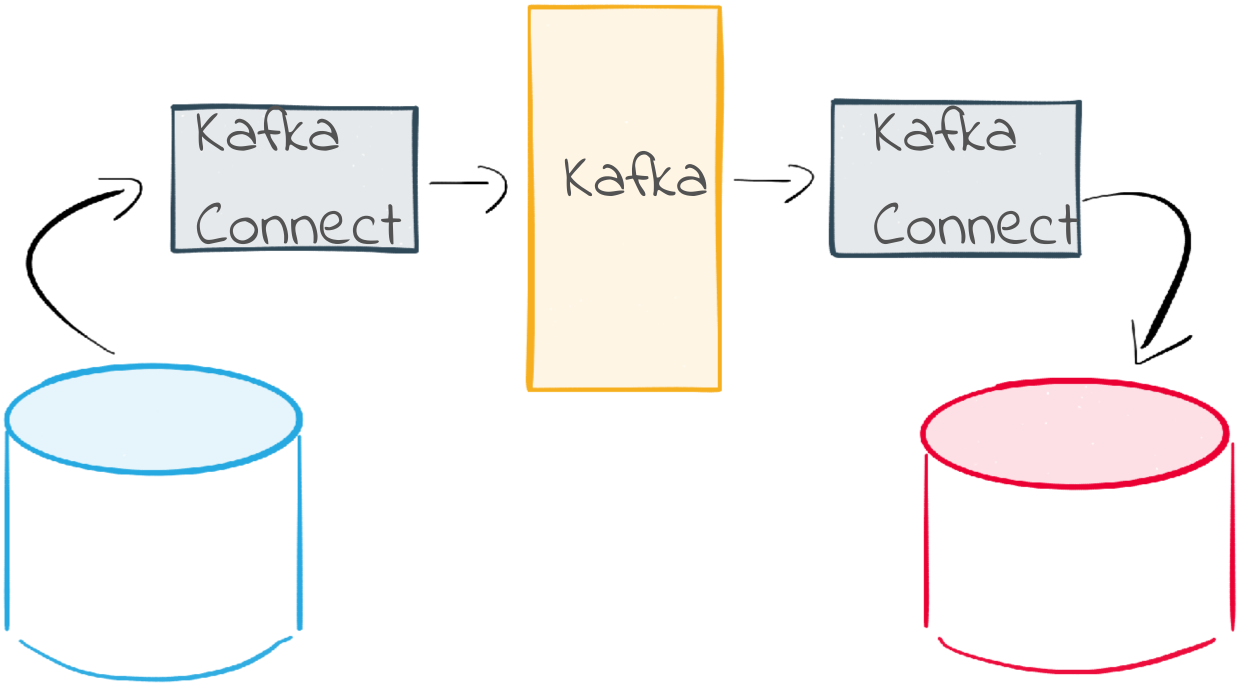


A 'replica' takes over on machine failure

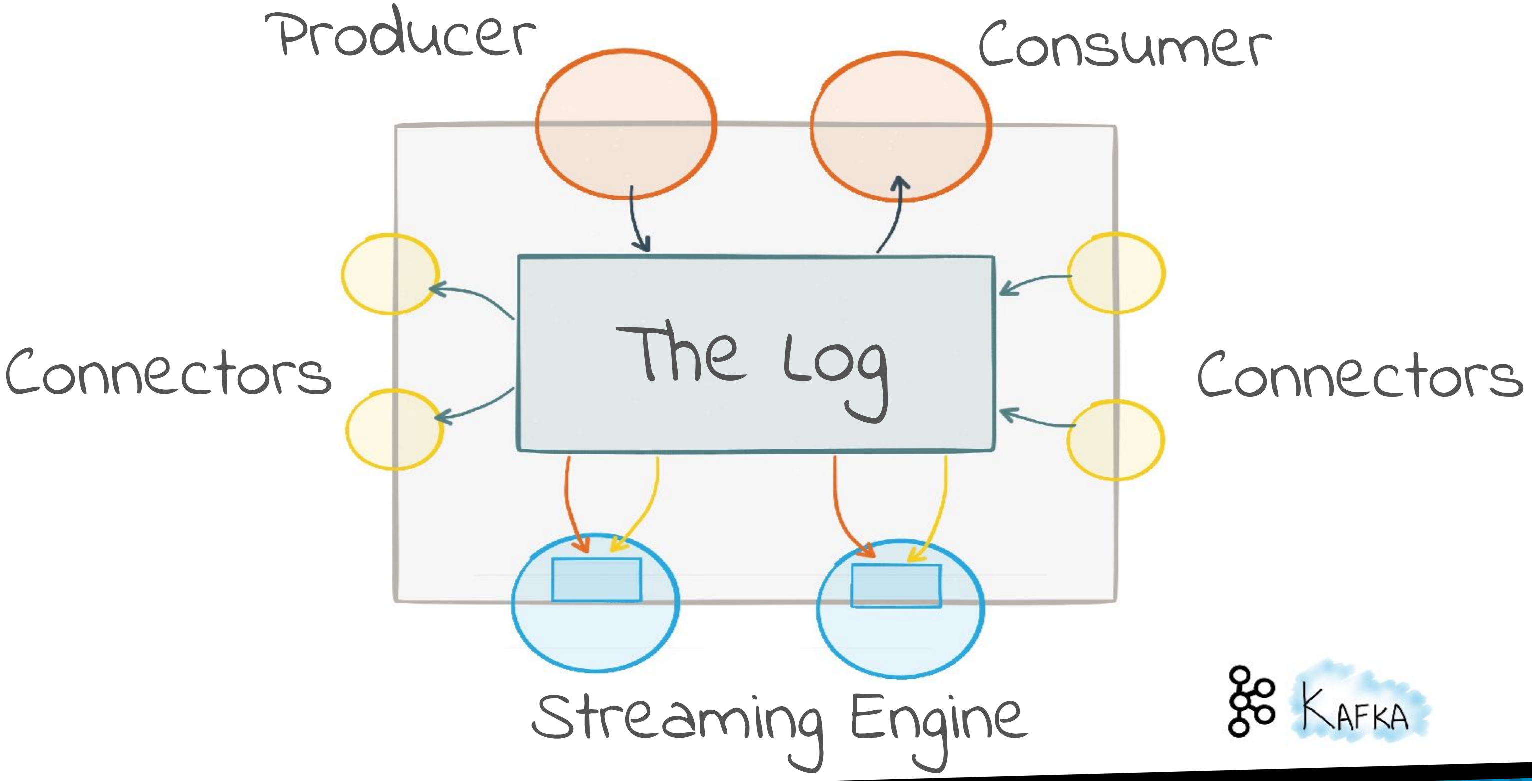
THE CONNECT API



INGEST / OUTPUT TO PRACTICALLY ANY DATA SOURCE

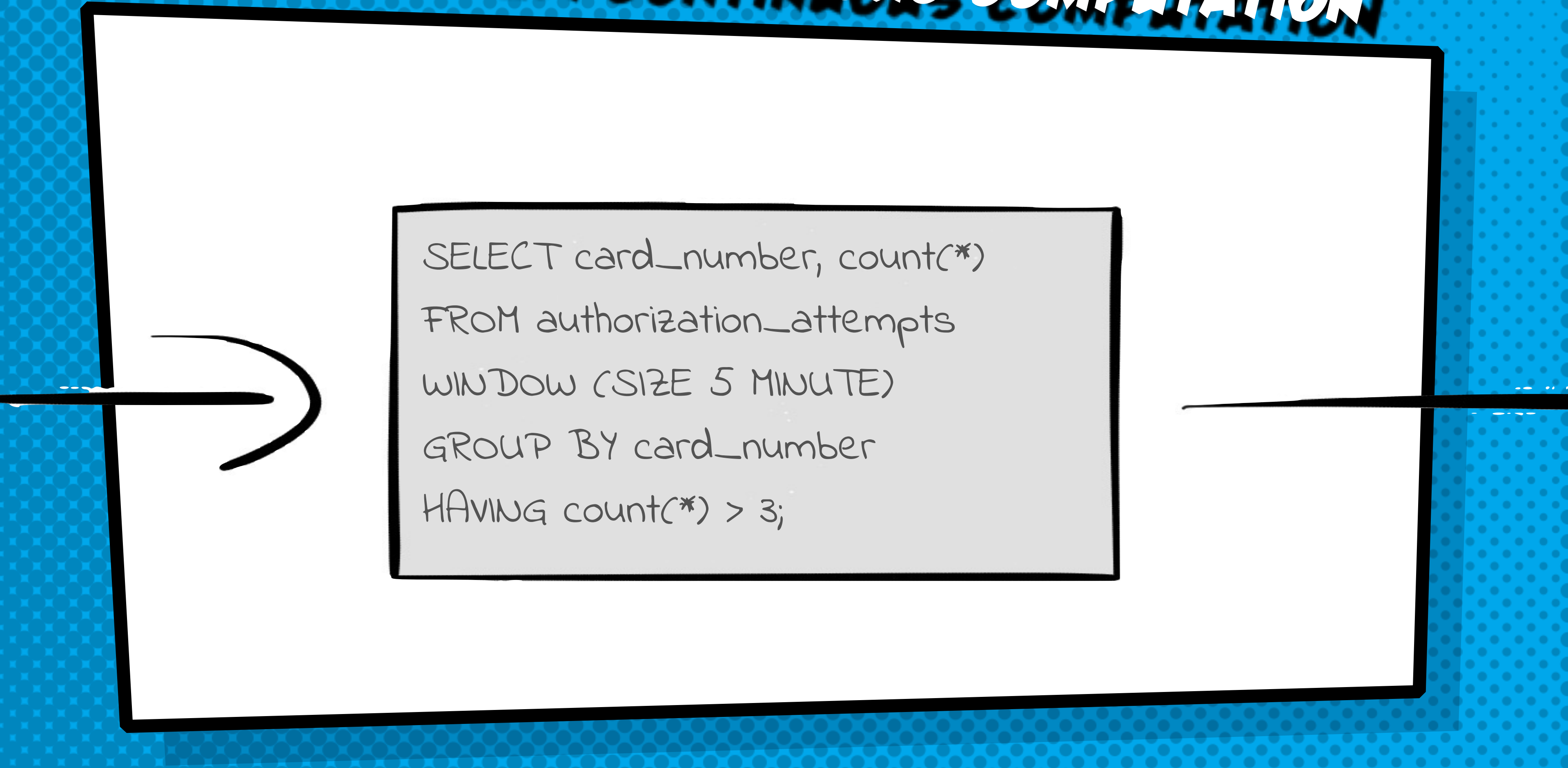


WHAT IS A STREAMING PLATFORM?



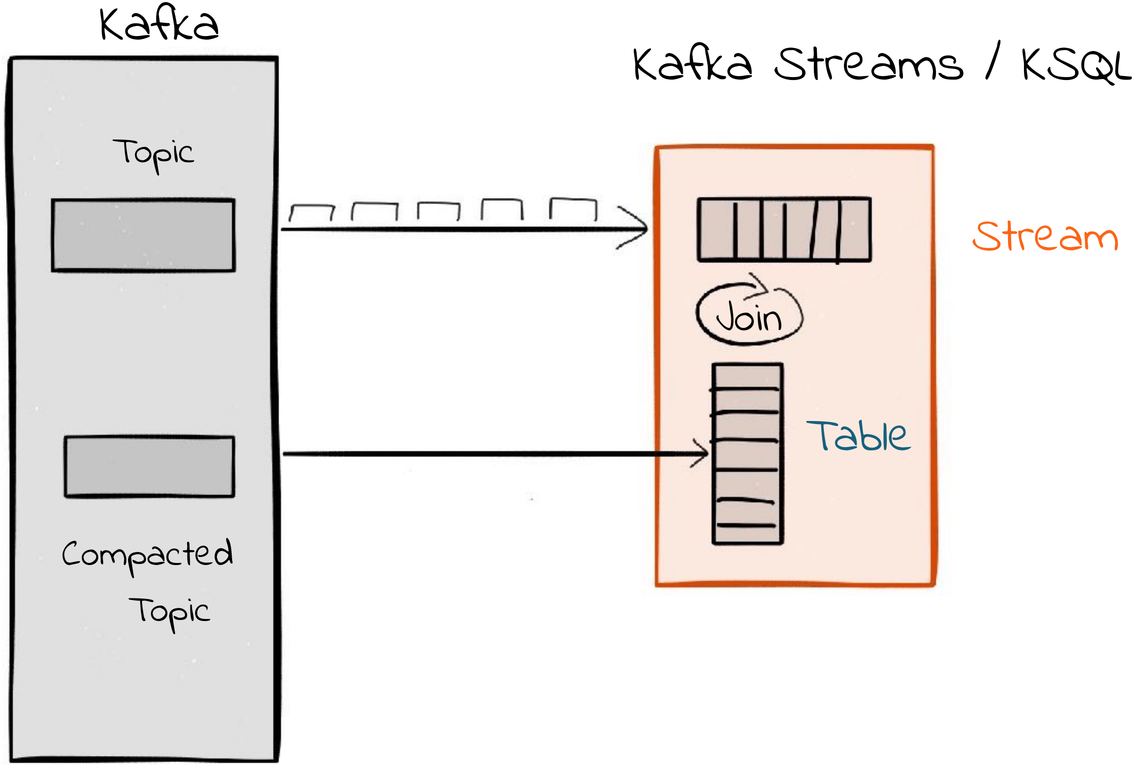
KAFKA

KSQL: CONTINUOUS COMPUTATION



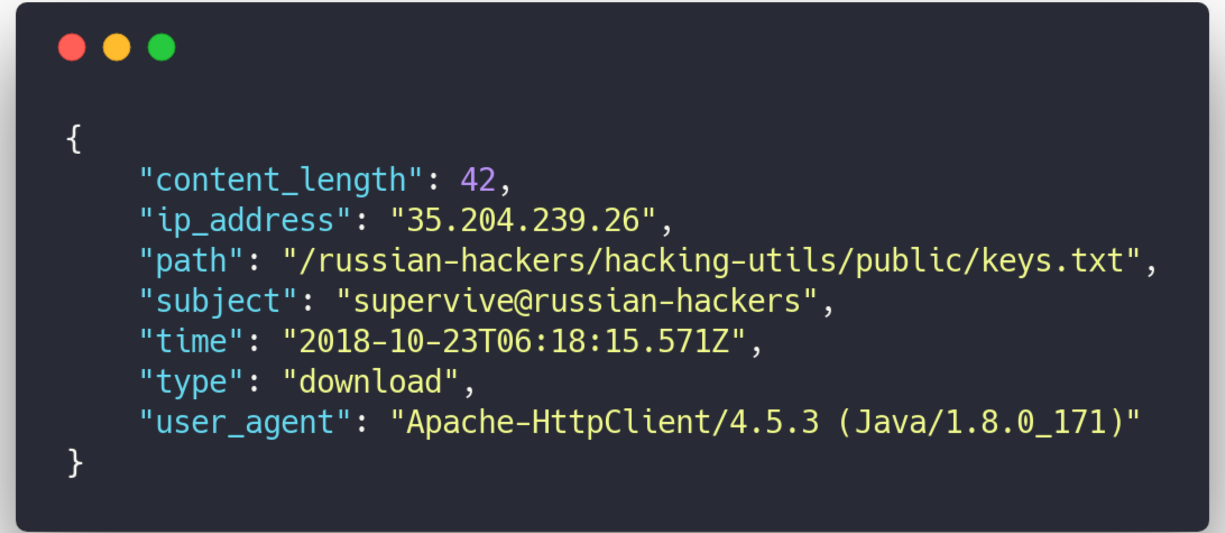
```
SELECT card_number, count(*)
FROM authorization_attempts
WINDOW (SIZE 5 MINUTE)
GROUP BY card_number
HAVING count(*) > 3;
```

JOIN STREAMS AND TABLES



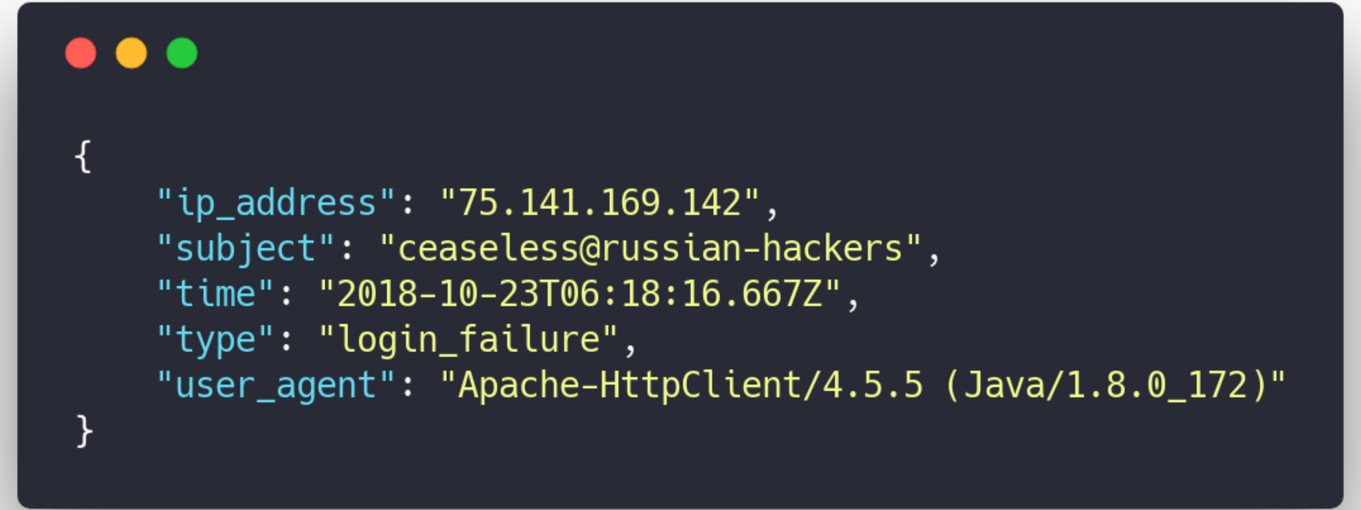
USE CASE
LOOKING FOR HACKERS

BINTRAY FIREHOSE API



```
{
    "content_length": 42,
    "ip_address": "35.204.239.26",
    "path": "/russian-hackers/hacking-utils/public/keys.txt",
    "subject": "supervive@russian-hackers",
    "time": "2018-10-23T06:18:15.571Z",
    "type": "download",
    "user_agent": "Apache-HttpClient/4.5.3 (Java/1.8.0_171)"
}
```

BINTRAY FIREHOSE API



```
{
    "ip_address": "75.141.169.142",
    "subject": "ceaseless@russian-hackers",
    "time": "2018-10-23T06:18:16.667Z",
    "type": "login_failure",
    "user_agent": "Apache-HttpClient/4.5.5 (Java/1.8.0_172)"
}
```

USE CASE: LOOKING FOR HACKERS!

1. HONEYPOT: SECRET FILE DOWNLOADS ATTEMPTS

2. BRUTE FORCE: LOGIN ATTEMPTS

3. * LEAKED PASSWORDS: USAGE OF THE SAME PASSWORD IN MULTIPLE PLACES

CODE IS ON GITHUB

- HTTPS://GITHUB.COM/RUSSIAN-HACKERS
- KAFKA CONNECT FOR BINTRY
- DOCKER COMPOSE AND STUFF

THANK YA'LL!

- @GAMUSSA
- @JBARUCH
- #ORACLECODEONE